KLAVYE DİNLEME VE ÖNLEME SİSTEMLERİ
ANALİZ, TASARIM VE GELİŞTİRME

Gürol CANBEK

YÜKSEK LİSANS TEZİ
BİLGİSAYAR MÜHENDİSLİĞİ

GAZİ ÜNİVERSİTESİ
FEN BİLİMLERİ ENSTİTÜSÜ

Eylül 2005
ANKARA

Gürol CANBEK tarafından hazırlanan KLAVYE DİNLEME VE ÖNLEME SİSTEMLERİ ANALİZ, TASARIM VE GELİŞTİRME adlı bu tezin yüksek lisans tezi olarak uygun olduğunu onaylarım.

Doç. Dr. Şeref SAĞIROĞLU

Tez Yöneticisi

Bu çalışma, jürimiz tarafından oybirliğiyle Bilgisayar Mühendisliği Anabilim Dalında Yüksek Lisans tezi olarak kabul edilmiştir.

Başkan: : Prof. Dr. Hayri SEVER

Üye : Prof. Dr. Volkan ATALAY

Üye : Doç. Dr. Şeref SAĞIROĞLU

Üye : _____

Üye : _____

Tarih : 13/09/2005

Bu tez, Gazi Üniversitesi Fen Bilimleri Enstitüsü tez yazım kurallarına uygundur.

TEZ BİLDİRİMİ

Tez içindeki bütün bilgilerin etik davranış ve akademik kurallar çerçevesinde elde edilerek sunulduğunu, ayrıca tez yazım kurallarına uygun olarak hazırlanan bu çalışmada orijinal olmayan her türlü kaynağa eksiksiz atıf yapıldığını bildiririm.

Gürol CANBEK

KLAVYE DİNLEME VE ÖNLEME SİSTEMLERİ
ANALİZ, TASARIM VE GELİŞTİRME
(Yüksek Lisans Tezi)

Gürol CANBEK

GAZİ ÜNİVERSİTESİ
FEN BİLİMLERİ ENSTİTÜSÜ
Eylül 2005

ÖZET

Bu tez çalışmasında, bilgi ve bilgisayar güvenliğini son zamanlarda tehdit eden kötücül ve casus yazılımlar ile, bu tür yazılımları önlemeye yönelik geliştirilen casus savar yazılımlar kapsamlı olarak incelenmiştir. Bu kapsamda, özellikle bu çalışmanın temelini teşkil eden klavye dinleme ve önleme sistemleri araştırılmış; incelenmiş; karşılaştırılmış ve bu sistemlerin sahip oldukları özellikler ve kullanılan yöntemler ve yaklaşımlar açıklanmıştır. Elde edilen bulgular çerçevesinde günlük hayatımızda, işyeri gözetleme, çocukların İnternet ve bilgisayar güvenliğinin sağlanması, otomatik kişisel bilgisayar faaliyet günlüğünün çıkarılması, eğitim ve başka kişilerin bilgisayar ve İnternet faaliyetlerinin gizlice izlenmesi gibi farklı amaçlar için kullanılabilecek, TürkSpyware adı verilen ileri özelliklere sahip bir casus yazılım geliştirilmiştir. Bu tez çalışmasında ayrıca, casus yazılımlar ve klavye dinleme sistemleri tarafından oluşturulan tehditleri ortadan kaldırmak amacıyla kullanılabilecek, TürkAntiSpyware adında bir klavye dinleme önleme sistemi yazılımı da geliştirilmiştir. Geliştirilen bu yazılımlar ile ülkemizdeki çevrimiçi İnternet bankacılığı, popüler web tabanlı e-posta sağlayıcılarının güvenliği araştırılmıştır. Sonuç olarak araştırılan, incelenen ve değerlendirilen konular ve geliştirilen yazılımların, ülkemizde bilgi ve bilgisayar güvenliği konusunda kişisel ve kurumsal güvenliğin ve verimliliğin oluşturulmasına büyük katkı sağlaması ve yeni ufuklar açması beklenmektedir.

Bilim Kodu : **908**
Anahtar Kelimeler : **Klavye dinleme, önleme, etkinlik izleme, kötücül yazılım, casus yazılım, bilgi, bilgisayar, güvenlik, gizlilik, işyeri gözetleme, çocuk güvenliği**
Sayfa Adedi : **305**
Tez Yöneticisi : **Doç. Dr. Şeref SAĞIROĞLU**

ANALYSIS, DESIGN AND IMPLEMENTATION OF KEYLOGGERS AND ANTI-KEYLOGGERS
(M.Sc. Thesis)

Gürol CANBEK

GAZI UNIVERSITY
INSTITUTE OF SCIENCE AND TECHNOLOGY
September 2005

ABSTRACT

In this thesis, malware and spyware threatening information and computer security and anti-spyware developed for preventing this kind of malicious software have been examined. In this context, the main subject of the study, keyloggers or activity monitoring systems and anti-keyloggers were studied; available commercial off-the-shelf software were compared and their capabilities and possible methods were explained. Making use of those findings, an advanced activity monitoring system based on key logging called TürkSpyware has been developed. The system that is considered the first Turkish keylogger can be used for workplace monitoring, ensuring the child safety on the Internet, education purpose, automatic personal logging of all the computer and Internet activities, and monitoring the computer activities secretly. In this study, also an anti-keylogger system, called TürkAntiSpyware was developed for blocking the threats of spyware and keyloggers. The security level of Turkish online Internet banking and popular web based e-mail suppliers were tested with the developed systems. It is expected that this thesis will contribute to personal and institutional information and computer security and productivity and bring new visions and awareness.

Science Code : **908**
Key Words : **Keylogger, anti-keylogger, activity monitoring, malware, spyware, information, computer, security, privacy, workplace monitoring, child safety**
Page Number : **305**
Adviser : **Assoc. Prof. Dr. Seref SAĞIROĞLU**

TEŞEKKÜR

Bilgi ve bilgisayar güvenliği konusunda beni yönlendiren ve çalışmalarım sırasında değerli katkılarını ve teşviklerini eksik etmeyen kıymetli hocam, Doç. Dr. Şeref SAĞIROĞLU'na ve vermiş oldukları desteklerinden ötürü annem Nesrin ve babam Mustafa CANBEK'e teşekkürlerimi bildirmeyi bir borç bilirim.

İÇİNDEKİLER

Sayfa

Sayfa

Sayfa

Sayfa

Sayfa

Sayfa

Sayfa

Sayfa

Sayfa

Sayfa

ÇİZELGELERİN LİSTESİ

Çizelge **Sayfa**

Çizelge **Sayfa**

ŞEKİLLERİN LİSTESİ

Şekil **Sayfa**

Şekil **Sayfa**

Şekil **Sayfa**

Şekil **Sayfa**

Şekil **Sayfa**

RESİMLERİN LİSTESİ

Resim **Sayfa**

SİMGELER VE KISALTMALAR

Bu çalışmada kullanılmış bazı simgeler ve kısaltmalar, açıklamaları ile birlikte aşağıda sunulmuştur.

Simgeler **Açıklama**

Bu çalışmada kullanılan bir simge yoktur.

Kısaltmalar **Açıklama**

A.Ş.	Anonim Şirketi
ABD	Amerika Birleşik Devletleri
AIM	(AOL Instant Messenger), AOL Anlık Haberci
AMA	(American Management Association), Amerikan Yönetim Birliği
AOL	America Online
API	(Application Programming Interface), Uygulama Programlama Arayüzü
ATM	(Automatic Teller Machine), Otomatik Vezne
BAT	(Batch File), Toplu İşlem Dosyası
BHO	(Browser Helper Object), Tarayıcı Yardımcı Nesnesi
BIOS	(Basic Input/Output System), Temel Girdi/Çıktı Sistemi
BSD	(Berkeley Software Distribution), Berkeley Yazılım Dağıtımı
CD-ROM	(Compact Disk-Read Only Memory), Kompakt Disk-Salt Okunur Bellek
CGI	(Common Gateway Interface), Ortak Ağgeçidi Arayüzü
COM	Haberleşme kapısı, MS-DOS çalıştırılabilir komut dosya tipi uzantısı
CPU	(Central Processing Unit), Merkezi İşlem Birimi
CSI	(Computer Security Institute), Amerikan Bilgisayar Güvenliği Enstitüsü

Kısaltmalar	Açıklama
DDK	(Driver Developer Kit), Sürücü Geliştirici Takımı
DDoS	(Distributed Denial of Service), Dağıtık hizmet aksattırma saldırıları
DLL	(Dynamic-Link Library), Dinamik Bağlantı Kütüphanesi
DNS	(Domain Name Server), Bölge Ad Sunucusu
DoS	(Denial of Service), Hizmet aksattırma saldırıları
DVD-ROM	(Digital Versatile Disk-Read Only Memory), Sayısal Çok yönlü Disk-Salt Okunur Bellek
EULA	(End-User License Agreement), Uç Kullanıcı Lisans Anlaşması
EXE	(Executable), Çalıştırılabilir dosya uzantısı
FBI	(Federal Bureau of Investigation), Amerikan Federal Soruşturma Bürosu
FTC	(Federal Trade Commission), Amerikan Federal Ticaret Komisyonu
FTP	(File Transfer Protocol), Dosya Aktarım Protokolü
G/Ç	Girdi/Çıktı
GB	Giga bayt
GHz	Giga hertz
GIF	(Graphics Interchange Format), Grafik Değiştirme Biçemi
GUID	(Globally Unique Identifier), Küresel Benzersiz Tanıtıcı
HTA	(HTML Applications), HTML uygulama dosya uzantısı
HTML	(Hypertext Markup Language), İleri Metin İşaretleme Dili
HTTP	(Hypertext Transfer Protocol), İleri Metin Aktarım Protokolü
HTTPS	(Secure Hypertext Protocol), Güvenli İleri Metin Protokolü
IAT	(Import Address Table), İçeri Aktarma Adres Tablosu
IBM	(International Business Machines), Uluslararası İş Makineleri firması
ICQ	(I Seek You), sohbet programı
IDC	(International Data Corporation), Uluslararası anket ve araştırma şirketi
IDS	(Intruder Detection System), Saldırı Tespit Sistemi
IM	(Internet Messaging), İnternet Mesajlaşma
INF	(Windows Information File), Windows kurulum bilgi dosyası
IP	(Internet Protocol), İnternet Protokolü

Kısaltmalar	Açıklama
IPD	(Integrity Protection Driver), Bütünlük Koruma Sürücüsü
IRC	(Internet Relay Chat), İnternet Aktarmalı Sohbet
IRP	(I/O Request Packet), G/Ç İstem Paketi
IRQ	(Interrupt Request), Kesme İsteği
ISM	(Industrial, Scientific and Medical), Endüstriyel, Bilimsel ve Tıbbi
ISO	(International Standards Organization), Uluslararası Standartlar Örgütü
ISP	(Internet Service Provider), İnternet Servis Sağlayıcısı
JPG	(Joint Photographic Expert Group), Ortak Fotoğraf Uzman Grubu
JS	(JScript File), JScript dosya uzantısı
JSE	(JScript Encoded Script File), JScript kodlu betik dosyası uzantısı
KB	Kilo bayt
KHz	Kilo hertz
LNK	(Shortcut), Kısayol dosya tipi uzantısı
LSP	(Layered Service Provider), Katmanlı Hizmet Sağlayıcı
MAC	(Media Access Control), Ortam Erişim Denetimi
MacOS	(Macintosh Operating System), Macintosh İşletim Sistemi
MB	Mega bayt
MHz	Mega hertz
MP3	(MPEG-1 audio layer 3), MPEG-1 ses katmanı 3
MPEG	(Moving Pictures Expert Group), Film Uzman Grubu
MSDN	(Microsoft Developer Network), Microsoft Geliştirici Ağı
MS-DOS	(Microsoft Disk Operating System), Microsoft Disk İşletim Sistemi
MSN	Microsoft Network
NCSA	(National Cyber Security Alliance) Amerikan Ulusal Siber Güvenlik Birliği
NT	((Windows) New Technology), Yeni Teknoloji
OLE	(Object Linking and Embedding), Nesne Bağlama ve Katıştırma
OEM	(Original Equipment Manufacturer), Orijinal Malzeme Üreticisi
P2P	(Pear to Pear), Eşten Eşe
PBX	(Private Branch Exchange), Özel Telefon Santralı

Kısaltmalar	Açıklama
PDA	(Personal Digital Assistant), Kişisel Sayısal Asistan
PE	(Portable Executable), Taşınabilir Çalıştırılabilir
PHP	(Hypertext Preprocessor), İleri Metin Ön İşlemci betik dili
PIF	MS-DOS programlarına ait kısayol dosyasının uzantısı
PIN	(Personal Identification Number), Kişisel Tanımlama Numarası
PING	(Packet Internet Groper), Paket İnternet Yoklayıcı
PKI	(Public Key Infrastructure), Açık Anahtar Altyapısı
PS/2	IBM'in ikinci kuşak kişisel bilgisayar serisi
RAR	Dosya sıkıştırma algoritması
RAT	(Remote Administration Tool), Uzaktan Yönetim Aracı
RF	(Radio Frequency), Radyo Frekansı
SAK	(Secure Attention Key), Güvenli Dikkat Tuşu
SCM	(Service Control Manager), Hizmet Kontrol Yöneticisi
SCR	(Screen Saver), Ekran koruyucu dosya uzantısı
SCT	(Windows Script Component), Windows betik bileşen dosya uzantısı
SDK	(Software Developer Kit), Yazılım Geliştirme Takımı
SDL	(Security Development Lifecycle), Güvenlik Geliştirme Yaşam Döngüsü
SHB	(Document Shortcut), Belge kısayol tipi dosya uzantısı
SHS	**(**Shell Scrap Object), Kabuk atık nesnesi dosya uzantısı
SMS	(Short Message Service), Kısa Mesaj Hizmeti
SMTP	(Simple Mail Transport Protocol), Basit Posta İletim Protokolü
SQL	(Structured Query Language), Yapısal Sorgulama Dili
SSL	(Secure Socket Layer), Güvenli Soket Katmanı
T.A.O	Ticaret Anonim Ortaklığı
TCP	(Transmission Control Protocol), İletim Denetim Protokolü
TSR	(Terminate and Stay Resident), Bitince Yerleşik Kalan
TÜBİTAK	Türkiye Bilimsel Ve Teknik Araştırma Kurumu
URL	(Uniform Resource Locator), Birörnek Kaynak Konumlayıcı
USB	(Universal Serial Bus), Evrensel Seri Veriyolu
VB	Visual Basic, VBScript dosyası

Kısaltmalar	Açıklama
VBS	(Virtual Basic Script), VBScript dosyası
VPN	(Virtual Private Network), Sanal Özel Ağ
WAP	(Wireless Application Protocol), Kablosuz Uygulama Protokolü
WH	(Windows Hook), Windows Çengeli
WHQL	(Windows Hardware Quality Lab), Windows Donanım Kalite Laboratuarı
WiFi	Kablosuz yerel alan ağı
WSC	(Windows Script Component), Windows betik bileşeni dosya uzantısı
WSF	(Windows Script File), Windows betik dosya tipi uzantısı
WSH	(Windows Scripting Host Settings), Windows betikleme konak ayarı dosya uzantısı
WWW	(World Wide Web), Dünya Çapında Ağ
ZIP	Dosya sıkıştırma algoritması

1. GİRİŞ

Bilim ve teknolojide son yıllarda kat edilen aşamalar ve süre gelen araştırma ve çalışmalar, insanlık hayatında oldukça önemli ve kökten değişikliklere yol açmıştır. Bilgisayar ve haberleşme teknolojilerinde yaşanan baş döndürücü gelişmeler ve özellikle İnternet'in katalizör etkisi ile insanların çalışma, iletişim kurma ve her türlü günlük ihtiyaçlarını karşılama biçimi sürekli bir dönüşüm halindedir (1). Günümüz toplumunda insanlar artık, bilgisayarla küçük yaşlarda tanışmakta; evde ve okulda gerek ödevleri için ve gerek eğlence için bilgisayardan yoğun bir şekilde istifade etmektedir (2). Hayatının geri kalanında ve özellikle iş sahasında, bilgisayar ve bilgisayar sistemlerini olabildiğince etkin bir şekilde kullanmaktadır (3). Bir çok işi hızlı, doğru, daha ucuz ve etkin bir şekilde gerçekleştiren bilgisayar sistemlerinden, gerçekten bilinçli bir şekilde yararlanıldığını kabul etmek doğru değildir (4, 5). Bilgisayar sistemlerine sıradan bir makine, bir veri deposu veya hızlı hesap yapan bir araç gözü ile bakmak; yani bu sistemleri bilinçsizce kullanmak, belki belli bir süre için bir ilerleme sağlasa da; bu ilerleme gittikçe cılızlaşacak ve ömrü kısa olacaktır. Özellikle iş hayatında yer alan kurum, kuruluş ve çalışanların kendisi için rekabetin yerelden küresele gittiği ve zayıf olanın ve ilerlemeye ayak uyduramayanın silindiği günümüz şartlarında; bilgi ve bilgisayar sistemlerinin doğru bir şekilde tanımlanması ve bilginin ve bilgi ile ilişkili bütün kavram, yöntem ve stratejilerin taşımakta olduğu önemin özümsenmesi gerekmektedir. Bunu özümseyen toplum ve devletlerin nerelere ulaştığı; bu konuya yeterince önem vermeyenlerin ise nerede kaldığı gözler önündedir.

Bilgisayarlar, veri işleyen, depolayan, ileten ve alan sistemlerdir. Bu sistemler üzerinde işlenen ve taşınan verilerin, yukarıda belirtilen sebeplerden dolayı, güvenliğinin sağlanması şarttır. Bu güvenliğin sağlanması, "veri nedir?", "bilgi nedir?" ve "özbilgi nedir?" gibi basit gibi gözüken soruların cevaplanmasıyla başlar. Bu sorulara verilecek cevapların altında binlerce yıllık bir insanlık medeniyeti ve gelecek yatmaktadır (6). Bu kavramların önemini kavrayamayan toplumlar gerilemeye ve başka toplumlara bağımlı kalmaya mahkumdurlar. Bu yüzden bu

kavramların ve bilginin öneminin ve taşıdığı potansiyelle toplumları götüreceği noktanın doğru bir biçimde tespit edilmesi gerekmektedir.

Bunların bilinmesi ve sistemli bir şekilde değerlendirilmesi önemlidir; ama tek başına yeterli değildir. Bilginin değerinin olması, bu değeri elde etmek için emek ve zamanın harcanması ve kazanılan bilginin fark yaratması nedeniyle bilgi, korunması gereken bir varlık olarak görülmelidir (7). Bilginin paylaşılması bile belirli kurallar çerçevesinde yapılmalıdır. Bu paylaşım esnasında bilgiyi gönderen, alan veya saklayan hiç bir taraf zarar görmemelidir. Bilgi ve bilgi sistemlerinin öneminin artması ile, ona karşı yönelen kötü niyetli yaklaşımlar artmıştır. Saldırı veya atak olarak adlandırılan bu tehditlerin önüne geçip; bilgi ve bilgisayar güvenliğinin temininde gerekli olan yöntemlerin belirlenmesi ve uygulanması son derece kritik bir konu olarak karşımıza çıkmaktadır. Kullanılan bilgisayar sistemine yönelik var olan tehdit durumu, bakış açısına göre değişebilirse de; tehlikeler son derece açıktır (8).

Özellikle ülkemizde bir çok kurum ve kuruluşun ve her seviyeden bilgisayar kullanıcısının bilgi ve bilgisayar sistemlerine ve bilgi güvenliğine bakış açısı ne yazık ki yeterli seviyede değildir (9, 10). Hele bilgi ve bilgisayar güvenliği konusunda oldukça yetersiz bilgi seviyesine ve tecrübeye sahibiz. İnternet'te sadece "boy göstermek" adına site açan şirketler aslında ne gibi fırsatları tepiyor? Bir çok firma neden elektronik ticaret yapamıyor? Çevrimiçi bankacılık gerçekten yeterli güvenlik koruması sunuyor mu? Bir bilgisayar sistemi alırken veya tasarlarken konu ile ilgili her türlü boyut düşünülüyor mu? Bilgisayar sisteminde yer alan veri ve bilgilerin doğru bir analizi yapılmış mı? Eldeki bilginin değerinin farkına varılmış mı? Ticari sırlar bu sistemlerde yeterince korunuyor mu? İşyerinde çalışan kişilerin performanslarının doğru bir biçimde tespiti mümkün mü? Gerçekten çalışanlar çalıştığı süreyi verimli bir şekilde kullanıyorlar mı? Bilinçli bir bilgisayar kullanıcısı güvenli bir şekilde bilgisayar kullanımı için neleri yerine getirmesi gerekir? "Bedava öğle yemeği" olmadığı gibi "bedava yazılım" var mıdır? Çocuğuna ders çalışması için bir bilgisayar hediye eden kişi, sadece bunu yapmak ile üzerine düşen görevi yapmış sayılır mı? İnternet'e bağlı olmayan bir bilgisayar güvenli midir? gibi bir çok soru ne yazık ki cevaplanmayı beklemektedir.

Bilgi ve bilgisayar güvenliği konusunda üniversitelerin de yeterli çabayı gösterdiği söylenemez. Bu çalışma sırasında çok sayıda üniversitenin bilgisayar mühendisliği bölümlerinde kabul edilen yüksek lisans tezleri, çevrim içi kütüphanelerinden taranmış; bu tezler arasında, bilgi ve bilgisayar güvenliği konusunu ele alan tez sayısının yok denecek kadar az olduğu görülmüştür. Kötücül yazılım, casus yazılım ve klavye dinleme sistemlerine yönelik bir çalışmaya da rastlanılmaması da oldukça şaşırtıcı bir bulgu olarak değerlendirilmektedir. Bunun nedeni olarak ya konunun küçümsendiği ya da konunun öneminin farkında olunmadığı anlamı çıkmaktadır.

Türkiye Bilimsel ve Teknik Araştırma Kurumu TÜBİTAK'ın, Yönlendirme Kurulu, yapmış olduğu "Bilim ve Teknoloji Strateji Belgesi" çalışmasında, ülkemizin 2023 yılına ışık tutacak bilim, teknoloji ve yenilik vizyonunu, "Sürekli yeni bilgi ve teknoloji üreterek; küresel rekabet gücü ve sürdürülebilir kalkınmanın temeli olan nitelikli işgücüne dayalı yüksek katma değeri yaratacak; bilgi temelli bir refah toplumu olma hedefine uygun şekilde tüm topluma yayılmış; etkin işleyen ve küresel sistem ile etkileşim içinde olan bir bilim, teknoloji ve yenilik sistemine sahip olmaktır" şeklinde tanımlamaktadır (11).

Bu belgede, bilgi toplumuna geçiş için, teknolojik altyapının güçlendirilmesi hedefi doğrultusunda yapılması gerekenler,

- Kullanımı eğitim gerektirmeyen bilgisayarların geliştirilmesi,
- Bilgi yönetimi ve iletiminde yüksek hizmet kalitesinin sağlanması,
- Bilgi toplumunda bilgi güvenliğinin sağlanması,
- Bilgi savaşlarına, elektronik savaşlara hazır olunması,
- Taşıyıcı sistemlerde 4. kuşak gezgin iletişim sistemlerinin geliştirilmesi,
- Geniş Bant İletişim Ağı'nın kurulması,
- Biyoelektriksel insan-bilgisayar arabirimlerinin geliştirilmesi ve
- İletişimde uydu uygulamalarında yetkinleşmek

şeklinde belirlenmiştir. Burada, bilgi güvenliği konusunun göz ardı edilmeyip çeşitli stratejilerin belirlenmiş olması ümit vericidir. Belgede bilgi toplumunda bilgi güvenliğinin sağlanması için gerekenler,

- Bilgi güvenliğini, kişilere ilişkin bilgiyi saklı tutma ve iletilen herhangi bir bilginin alıcısından başkasına gitmemesini sağlama şeklinde iki ayrı alanda ele almak gerekir. Birincisi için yetkilendirme ve yetkisizleri dışında tutan "kalkan"lar, ikincisi için ise "kriptolama teknikleri" öne çıkmaktadır.
- Yetkili kişileri tanıma (authentication) için kullanılabilecek yöntemler arasında, biyolojik olanların yanı sıra, günümüzde kullanılmayan, ancak kullanılması için gerekli teknolojilerin yeterli yetkinliğe ulaştığı yöntemler de bulunmaktadır.

şeklinde sıralanmaktadır. Elbette bu konuda yapılması gerekenler bunlarla sınırlı değildir. Çok sayıda ayrıntının bulunduğu bilgi ve bilgisayar güvenliği için, devlet, üniversite ve araştırma kuruluşları ile sanayinin bir arada çalışacağı, geniş bir katılımın sağlanması şarttır. Yurtdışında, özellikle ileri bilgi teknolojilerini kullanan ülkelerde, bilgi güvenliği konusu en güncel, üzerinde en çok durulan, çalışmalar yapılan ve büyük meblağlarda yatırımların gerçekleştirildiği konulardan biridir. Hazırlanan bu tez çalışmasının, ülkemizde de bilgi ve bilgisayar güvenliği ile ilgili tüm kişi ve kuruluşlara ışık tutmasına ve konunun öneminin doğru bir şekilde kavranmasına yardımcı olması ümit edilmektedir.

Bilgi ve bilgisayar güvenliği konusunda yapılan bir çok çalışma daha çok "makine-makine arayüzüne" yönelik saldırılara karşı alınan tedbirlere odaklanmaktadır. Örneğin, bilgisayarlar ve ağlar arasındaki güvenlik üzerine bir çok çalışma yapılmış; çeşitli uygulama ve protokoller geliştirilmiştir. Uzun yıllardır "insan-makine arayüzünde" var olan güvenlik açıkları ise çoğunlukla göz ardı edilmiştir. Bir "insan-makine arayüzü" olarak bilgisayar kullanırken en çok etkileşimde bulunduğumuz donanımların başında gelen klavyeler, bilgisayar sistemlerinin belki de en az değişen ve üzerinde en az durulan bileşenlerinden biridir. İşlemciler, bellekler, ekranlar, disk birimleri ve diğer çevre birimlerde yaşanan baş döndürücü yenilik ve ilerlemeler

klavyelerde ve biraz da “onun pabucuna dama atan” farelerde gözlenmemektedir. Bugün kullanılan klavyeler, çok az farklılıklarla yirmi yıl önce de kullanılmaktaydı. Belki de bu yüzden bilgi ve bilgisayar güvenliği konusunda da çok aşina olduğumuz klavyelerin, daha doğrusu klavyeden girilen bilgilerin, ne gibi bir güvenlik açığı oluşturduğu son zamanlara kadar ülkemizde gözden kaçmıştır.

Klavye dinleme sistemleri, kullanıcının sisteme klavyedeki tuşları kullanarak, şifre ve kişisel bilgiler gibi sağladığı bütün bilgileri, daha işin başında, sistemden elde edebilen yapılardır. Böylelikle bu aşamadan sonra sergilenen bütün güvenlik önlemlerinin pek de önemi olmayacaktır. Çünkü korunmak istenen bilgi çoktan ele geçmiştir. Genelde iyi niyetli olmayan ve çok ciddi tehdit oluşturan bu sistemlerin, çalışmanın ilerleyen bölümlerinde incelendiği gibi oldukça yarar sağlayabilecek şekilde kullanımlarının da mümkün olduğunun vurgulanmasında fayda vardır. Bu faydalı yönler, bu çalışmada gerçekleştirilen özgün klavye dinleme ve önleme yazılımlarının daha uygun bir şekilde, çeşitli alanlarda kullanılabileceği düşüncesini oluşturmuştur. Şu an klavye dinleme sistemleri, ilk çıktıkları zamana göre oldukça geniş bir kapsamda işlev sergileme yeteneğindedirler. Öyle ki klavye, artık tek başına üzerine eğilinen bir bileşen değildir. Fare tıklamalarının izlenmesi, İnternet’te gezilen sitelerin izlenmesi, çalışan programların izlenmesi, kullanılan dosyaların izlenmesi ve belli aralıklarla ekran görüntüsünün alınması gibi bir çok işlev, çoğu klavye dinleme sistemlerinde bulunmaktadır. Bu yönüyle “klavye dinleme sistemi” tamlaması yeterli görülmeyip; “elektronik faaliyet izleme” gibi adlandırmalara rastlansa da; “klavye dinleme sistemi” tamlamasının, bilgisayar üzerinde yapılan elektronik faaliyet izleme anlamında bütün bu işlevleri kapsadığının belirtilmesinde fayda vardır.

Bu tez çalışması, her ne kadar klavye dinleme sistemlerine yönelik olsa da; kötücül ve casus yazılımlarla beraber klavye dinleme ve önleme sistemlerinin araştırılması, incelenmesi, tasarımı ve doğrudan geliştirilmesi ile ilgili konular, geniş bir kapsam içinde sunulmuştur.

Bu tezin 2. bölümünde, çalışmanın özünü teşkil eden, bilgi ve bilgi güvenliği konusu en genel hatları ile incelenmektedir. Veri ve bilgi gibi, birbirleri ile karıştırılan ve birbirleri yerine söylenen terimler, açıklanmış ve bundan daha "rafine" anlam ve önem ifade eden "özbilgi" kavramı incelenmiştir. Gerçeklik ile hikmet arasında yer alan veri, bilgi ve özbilgi basamakları, konunun özünü belirtecek şekilde verilmiştir. Bilgi ve bilgisayar güvenliği ve güvenli bir sistemin taşıdığı bütün unsurlar yine bu bölümde açıklanmaktadır. Sistematik bilgi güvenliği sürecinin en temel safhaları olan önleme, saptama ve karşılık verme süreçleri, genel hatları ile bu bölümde özetlenmektedir. Güvenliği zafiyete düşüren saldırıların çeşitli şekillerde sınıflandırılmasının sunulmasından sonra; en genel saldırı türleri olan, kaynak kod istismarı, gizli dinleme, sosyal mühendislik ve insan hatası, hizmet aksattırma saldırıları, dolaylı saldırılar, arka kapılar, doğrudan erişim saldırıları ve kriptografik saldırılar açıklanmış ve bilgi ve bilgi güvenliği konusunda önemli ve üzerinde gerçekleşen tartışmaların hala devam ettiği bir konu olan, kişisel gizlilik (mahremiyet), temel özellikleri ile beraber sunulmuştur. Bölümün sonunda ülkemizde yeni Türk Ceza Kanunu ile tanımlanan ve konu ile ilişkili olan "Bilişim Suçları" kanunları konunun yasal boyutunu da sergilemek amacıyla sunulmaktadır.

Bölüm 3'de en tehlikeli türlerinden biri, "klavye dinleme sistemleri" olan, kötücül yazılım (malware) ve casus yazılımlar (spyware) incelenmiştir. Virüsler, solucanlar, Truva atları, casus yazılımlar, arka kapılar, klavye dinleme sistemleri, tarayıcı soyma, telefon çeviriciler, kök kullanıcı takımları, korunmasızlık sömürücüleri ve tavşanlar olarak adlandırılan en genel kötücül yazılım türleri; sergiledikleri özelliklerle ve sahip oldukları çeşitliliklerle özetlenmeye çalışılmıştır. Ayrıca bu bölümde kırk kadar diğer kötücül yazılım türü gözden geçirilmiştir. Uzun araştırmalar sonucu elde edilen böyle bir sınıflamanın, ülkemizde yapılması beklenen araştırmalara bir temel oluşturacağı düşünülmektedir. Bu bölümde ayrıca; virüs, casus yazılım, mesaj sağanağı (spam), bilgisayar solucanı (worm), Truva atı (Trojan), reklam yazılım (adware) ve sazan avlama (phishing) gibi kötücül yazılımların bir birleri ile olan ilişkisinden ve bilgisayar sistemlerine karşı sergiledikleri "bir nevi dayanışmadan" bahsedilmiştir. Casus yazılımların nasıl geliştiğine dair geçmişten günümüze bir zaman yolculuğunun yapıldığı 3. bölümün

son kısmında; şu an için en yaygın bir şekilde rastlanan casus yazılımlardan bazıları, temel özellikleri ile beraber aktarılmıştır. Bu bölümü hazırlarken onlarca yabancı kötücül yazılım teriminin Türkçe karşılıkları varsa araştırılıp kullanılmış; Türkçe karşılığı henüz önerilmeyenlere ise birer karşılık önerilmiştir. Bu bölüm ile, "bilgi ve bilgisayar güvenliğinin" karşı tarafında cephe alan bütün tehdit ve olguların gözler önüne serilmesi sonucunda, saldırı durumunda karşılaşılacak durumlar ve bunlara karşı alınabilecek önlemlerin daha doğru bir şekilde belirlenmesi amaçlanmıştır.

Casus yazılımlara yönelik tedbirler ve casus savar yazılımların anlatıldığı Bölüm 4'de, öncelikle bir bilgisayar sistemine her hangi bir casus yazılımın bulaşıp bulaşmadığını saptamaya yarayan bulgular gözden geçirilmiştir. Bu bölümün kayda değer bir diğer kısmı, casus yazılımların ne gibi "kirli veya zararlı" taktiklerle sistemlere sızdığının, ayrıntılarıyla açıklanmasıdır. Bu sayede kullanıcıların ileride karşılaşılabilecek durumlara karşı bilinçlenmesi ve gerekli tedbirleri almasının sağlanması amaçlanmıştır. Bunlar arasında; uç kullanıcı lisans anlaşması, kaçak indirme kavramı ve casus yazılımların özellikle çocukların istismarı ile sistemlere bulaşma girişimlerinin, gereken ilgi ve tepkiyi alması ümit edilmektedir. Bölüm 4'de geniş araştırmalar ve bizzat yaşanan tecrübeler ışığında, kullanıcıların kendi başlarına alabilecekleri önlemler, madde madde listelenmektedir. Bu bölümde ayrıca bilgisayar sistemi yöneticilerinin alması gereken tedbirlerden de bahsedilmiştir. Casus yazılımların "yumuşak karnı" olarak nitelendirilebilecek, bulaştıkları bilgisayar sisteminin açılışı ile beraber, kendi kendini otomatik olarak başlatabilmek için kullandıkları teknikler, yine bu bölümde örnekleriyle açıklanmaktadır. Bu önemli bilgi dışında; bit sonlandırma yöntemi ile ActiveX engelleme, İnternet Gezgini'nin ağ kullanıcıları için güvenli bir şekilde yapılandırılması ve casus yazılım bulunan konak sunucuların önlenmesi gibi pek bilinmeyen; fakat oldukça etkili yöntemlerden bahsedilen bu bölümün sonunda, hali hazırda piyasada yer alan ve aralarında Microsoft Antispyware beta sürümü ve bedava olarak sunulanlar dahil, bir çok önemli casus savar yazılımın, karşılaştırılması yapılmış ve üstünlükleri ve zayıf yönleri listelenmiştir.

Bölüm 5'de klavye dinleme sistemlerinin sergilediği yaklaşımlar, kullandıkları yöntemler ve sahip oldukları özellikler genel olarak açıklanmıştır. Bu bölümün başında, en temel girdi/çıktı bileşenlerinden biri olan klavye çevre biriminin, işlevi, yapısı, genel özellikleri ve çalışma prensibinden bahsedilmiştir. MS-DOS işletim sisteminde kullanılan klavye kesmelerinin yerini Windows işletim sisteminde üstlenen Windows mesaj mekanizmasının ve tuş basımı mesajlarının açıklandığı bu bölüm ile en çok kullanılan işletim sistemlerinden biri olan Windows işletim sisteminde, klavye dinleme sistemlerinin üzerinde bulunduğu alt yapı gözler önüne serilmiştir. Klavye dinleme sistemi türlerinden biri olan donanım klavye dinleme sistemlerinin, pek de bilinmeyen veya görmezden gelinen etkileyici yeteneklerinin gözler önüne sergilendiği kısmı, yazılım klavye dinleme sistemlerinin Windows işletim sistemine yönelik sergilediği, üç ana "ortadaki adam" (man-in-the-middle) saldırısının ayrıntıları ile incelendiği kısım izlemektedir. Özellikle, Windows çengelleri (hook) konusunda oldukça önemli ayrıntılar sunulmaktadır. Çekirdek tabanlı klavye süzgeç sürücülü klavye dinleme sisteminin alt yapısının anlatıldığı bu bölümde, ayrıca Linux/BSD/UNIX benzeri işletim sistemlerinde klavye dinlemenin nasıl yapıldığı, örnek kod ile açıklanmaktadır. Klavye dinleme sistemlerinin sahip oldukları işleyiş esasları ve sahip olabilecekleri yetenekler sıralanmış; casusluk, çevrimiçi bankacılık, ebeveynlerin çocuklarının İnternet ve bilgisayar kullanımını kontrolü ve işyeri gözetleme gibi bir çok sahada klavye dinleme sistemlerinin nasıl kullanılabileceği ayrıntıları ile anlatılmıştır. Bölümün sonunda, piyasada mevcut bulunan yüzlerce klavye dinleme sistemi ve türevinden, bu konuda derecelendirme yapan kuruluşlar tarafından en üst seviyede kabul edilen yazılımlar için yapılan incelemelerin sonuçları aktarılmıştır.

Bölüm 6'da klavye dinleme sistemlerine karşı alınabilecek tedbirlerden bahsedilmektedir. Donanım klavye dinleme sistemlerine karşı kullanılabilecek kablosuz, kızıl ötesi, bluetooth ve lazer klavyeler bu bölümde tanıtılmaktadır. Birçok yazılım klavye dinleme sistemlerine karşı kullanılmasında fayda görülen sanal klavyelerin anlatıldığı bu bölüm, bilgisayar sistemlerinde güvenli bilgi girişinin nasıl yapılacağı konusunu, sunulabilecek çözüm önerileri ve bu önerilerin olumlu ve olumsuz yönlerini sıralayarak incelemektedir. Çok az sayıda sunulan mevcut klavye

dinleme önleme sistemi yazılımlarının özelliklerinin incelendiği bölümün son kısmında, API izleme ile klavye dinleme önleme yöntemleri ve çekirdek tabanlı klavye ve fare sürücülerini önleme konuları genel hatları ile açıklanmaktadır.

Bölüm 7'de bu tez çalışması için gerçekleştirilen klavye dinleme sistemi, TürkSpyware yazılımının tasarımından, sahip olduğu modüllerden ve programın kullanım durumlarından bahsedilmektedir. Program Gmail, Hotmail ve Yahoo mail gibi web tabanlı e-posta sağlayıcıların giriş sayfalarının güvenliğini ve Türkiye'de İnternet üzerinde bankacılık faaliyeti gösteren tüm bankaların İnternet şubelerinin giriş sayfalarının güvenliğini test etmek amacıyla kullanılmıştır. Yapılan denemelerin ayrıntılı sonuçları verilmiştir. Bu bölümde Türkiye'de faaliyet gösteren bankaların klavye dinleme sistemlerine karşı aldıkları güvenlik önlemleri derecelendirilmiş ve sonuçlar değerlendirilmiştir. Bölümün son kısmında, TürkSpyware klavye dinleme sistemi ile Bölüm 6.5'de bahsedilen klavye dinleme önleme sistemleri, birlikte test edilerek; her iki gruptaki yazılımların başarılı ve başarısız noktaları belirtilmektedir.

Bölüm 8'de tez çalışması için gerçekleştirilen klavye dinleme önleme sistemi TürkAntiSpyware yazılımı açıklanmaktadır. Bu yazılımın tasarım özellikleri, kullanıcı arabirimi ve kullanım açıklamaları bu bölümde sunulmaktadır.

Son kısım Bölüm 9'da ise, yapılan tez çalışmasından elde edilen sonuçlar ve bunlara yönelik değerlendirmeler, çalışma sırasında karşılaşılan güçlükler ve sunulan öneriler aktarılmaktadır.

2. BİLGİ VE BİLGİ GÜVENLİĞİ

Klavye dinleme ve önleme sistemleri, diğer kötücül ve casus yazılımlar gibi, bilgi ve bilgi güvenliği ile doğrudan ilişkili olan bir konudur. Bilgi güvenliğine yönelik son derece ciddi bir saldırı türü olan klavye dinleme sistemlerini ve bu sistemlere karşı geliştirilen klavye dinleme önleme sistemlerinin neden çok büyük bir önem taşıdığını kavramak için, öncelikle bilginin ne olduğunun doğru bir şekilde tanımlanması gerekmektedir. Bu bölümde, bilgi, bilgi ile ilişkili kavramlar, bilgi ve bilgisayar güvenliğinin kapsamı, önemi ve bilgi güvenliğini oluşturan unsurlar, güvenli bir bilgi sistemini meydana getirmek için uygulanması gereken süreçler, bilgi ve bilgisayar sistemlerinin güvenliğine yönelik saldırılar, klavye dinleme sistemlerinin de ilişkili olduğu kişisel gizlilik konusu ve ülkemizde bilişim suçlarına yönelik yasal çerçeve incelenmiştir.

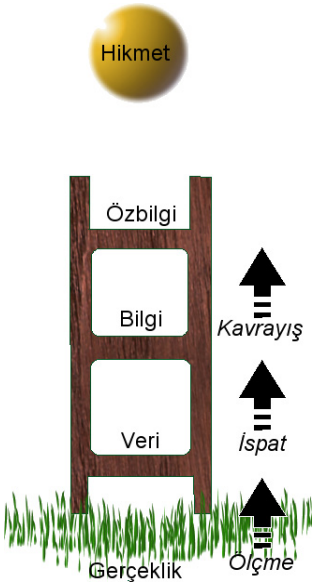
2.1. Bilgi

"Bilgi çağında yaşıyoruz" şeklinde ifadelere rastlamamış olmak nerdeyse imkansızdır. Bulunduğumuz dönemi farklı şekillerde adlandırmak mümkünse de; bilginin yaşadığımız çağa damgasını vuran bir varlık olduğu artık su götürmez bir gerçektir. Bu açıdan bakıldığında, çağımızın altın değerindeki hammaddesi olan bilgiyi tanımlamak, kavramak ve bilgi ile ilgili hususları incelemek, insanlığın başlangıcından itibaren geçen süreçte ileriye yönelik gelişimimizi şekillendirmenin en önemli anahtarıdır. Günümüzde ön plana çıkmış gibi gözükse de; bilgi, dünün, bugünün ve geleceğin anahtarıdır.

Bilgi ile ilgili bir çok şey söylenebilir. Bilginin doğası ile ilgili aşağıda derlenen sözler, konunun ufuklarını bir kez daha gözler önüne sermek açısından faydalı olabilir (12):

- Bilgi boşlukta ve zamanda yer kaplar.
- Bilgi gürültü çıkarmadan hareket edemez.
- Bilginin hareket etmesi için enerji gerekir.

- Bilgi yaşam ve herhangi bir düzenli etkinlik için gereklidir.
- Bilgi hem maddesiz biçim; hem biçimsiz maddedir.
- Işık gibi, bilgi'nin de ağırlığı vardır. Bir giga bayt, bir parmak izinden daha az ağırlıktadır.
- Bilgi zaman içinde hareketli veya donmuş olabilir.
- Bilgi, bir soruya tatmin edici, belki de rahatsızlık verici cevaptır.
- Bir taşın ağırlığı ile bunu tanımlamak için gerekli bilgi birbirine eşittir.
- Bilgi, katı hale sahiptir; donarak katılaşır (depolama).
- Bilgi, sıvı hale sahiptir; akar (iletişim).
- Bir yerlerde bilgi hareket eder; evren gümbürder ve gerçeği gürler.
- Maddeden farklı olarak bilgi aynı anda birden fazla yerde olabilir.
- El sıkışma bir bilgidir. Bir baş sallama, bir bakış, bir iç çekiş.
- Bilgi, rastsallık denizinde parlar.
- Ben merkeziyetçiliklerinde insanlar bilginin yalnız kendileri için var olduğunu düşünür. Öyle değildir.



Şekil 2.1. Gerçeklikten özbilgiye ulaşmak için aşılması gereken basamaklar

Bilgi çağında ilerlemek, bir merdivenin basamaklarını kullanarak bir üst seviyeye çıkmaya benzetilebilir (13). Şekil 2.1'de gerçeklik (reality) ile hikmet (wisdom) arasında gösterilen bu merdivenin basamakları: veri (data), bilgi (information),

özbilgi (knowledge) basamaklarıdır. Çoğu durumda her basamak, atlanmadan teker teker geçilir. Yukarıya çıktıkça elimizdeki şeyin miktarı azalırken; değeri artar. Yine yukarıya çıktıkça bir sonraki basamağa adım atmak daha da zorlaşır ya da daha çok çaba ister. Genel olarak bilimin getirdiği yöntemlerden ölçme ile, eldeki gerçeklikten veriye ulaşılır; ispat ile, veriden bilgiye ulaşılır ve kavrayış ile, bilgiden özbilgiye ulaşılır (14). Bir özbilginin gerçeklik haline dönüştürülmesi de mümkündür. Bunun için yönetim biliminden yararlanılır.

Kullanımda çoğu kez bu basamakların adları birbirleri ile karıştırılır. Bu kavramları sırası ile aşağıdaki gibi açıklamak mümkündür.

Verinin İngilizce karşılığı olarak kullanılan "data", Latince "datum" kelimesinden (çoğul şekli "data" ve "vermeye cesaret etmek" fiilinin geçmiş zamanı, dolayısıyla "verilen şey") gelmektedir. Latince "data" (dedomena) kavramının M.Ö. 300 yıllarında Öklid'in bir çalışmasında geçtiği bildirilmektedir (15). Dilimizde de verilen şey anlamında, "veri" olarak kullanılmaktadır. Bilişim teknolojisi açısından veri, bir durum hakkında, birbiriyle bağlantısı henüz kurulmamış bilinenler veya kısaca, sayısal ortamlarda bulunan ve taşınan sinyaller ve/veya bit dizeleri olarak tanımlanabilir.

Bilgi, verinin belli bir anlam ifade edecek şekilde düzenlenmiş halidir. Veri ve ilişkili olduğu konu, bağlamı içinde bilgi üretecek şekilde bir araya getirilir. İşlenmiş veri olarak da ifade edilebilecek bilgi, bir konu hakkında var olan belirsizliği azaltan bir kaynaktır. Veri üzerinde yapılan uygun bütün işlemlerin (mantığa dayanan dönüşüm, ilişkiler, v.s., formüller, varsayımlar, basitleştirmelerin) çıktısı bilgidir.

Özbilgi, tecrübe veya öğrenme (sonsal) şeklinde veya iç gözlem şeklinde (önsel) elde edilen gerçeklerin, doğruların veya bilginin, farkında olunması ve anlaşılmasıdır. Verileri bir araya getirip, işlemek bilgiyi oluştursa da; özbilgi, kullanılan bilgilerin toplamından daha ileride bir kavramdır. Bir güç oluşturabilecek, katma değer sağlayabilecek veya bir araç haline dönüşmek üzere, daha fazla ve özenli olarak işlenmiş bilgi, asıl değerli olan özbilgidir.

2.2. Bilgi ve Bilgisayar Güvenliği

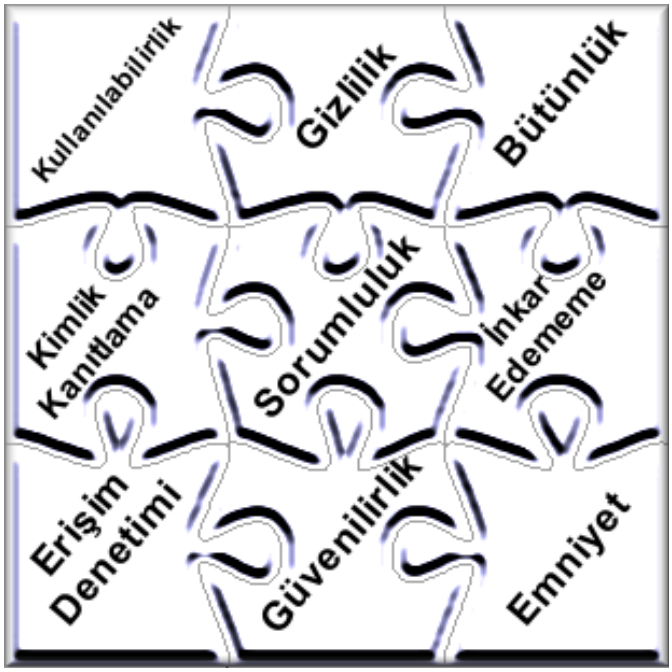
Bilginin üretilme, depolanma, korunma, kullanılma, paylaşma, yayılma, etkileşme ve artma hızı, teknolojinin getirdiği hızlı bilgi işleme ve iletişim araçları ile baş döndürücü bir hal almıştır. Günümüz insanı, günlük yaşamında bile yoğun bir bilgi bombardımanı altındadır. Bu yüzden bilgiye erişimde seçici yöntemler kullanılarak doğrudan ulaşılmak istenilen bilgiye eriştirecek yöntemler geliştirilmelidir. Bir başka önemli konu da bilginin taşıdığı değerdir. Bilginin değerli veya değersiz olduğunu belirlemek veya bilginin taşıdığı değeri ölçmek, en az bilginin kendisi kadar önemlidir. Elde edilen bilgiyi değerlendirirken bilginin kalitesini gösteren özelliklere bakılması gerekir. Doğruluk, güncellik, konuyla ilgili olma, bütünlük ve öz, gereksinimlere uyum gösterme, iyi sunulma ve fiziksel ve idrak yolu ile erişim gibi ölçütler bilginin kalitesini belirleyen etmenlerden bazılarıdır.

Bilginin çok önemli bir varlık olması, ona sahip olma ile ilgili bazı konuların düzenlenmesi ve yeni şartların getirdiği özelliklere göre ayarlanmasını gerekmektedir. Bilgi en basit benzetme ile para gibi bir metadır. Kişiler, kurumlar ve ülkeler için bilgi, elde edilmesi zor; aynı zamanda elde tutulması zor bir metadır. Entelektüel mülk olarak bilginin sahibinin korunması, hayati bir önem arz etmektedir. Bu korunma, hem bilgi kullanımındaki karmaşayı, yozlaşmayı ve kötüye kullanımı önleyeceği gibi; hem de bilgiyi bir çaba göstererek elde eden tüzel veya gerçek kişilerin haklarının korunmasını da sağlayacaktır. İşte bu yüzden patent gibi haklar, entelektüel mülkü korumak amacıyla oluşturulmuştur. Fakat, bilginin korunması, daha doğrusu bilginin güvenliği, çok daha kapsamlı bir konudur.

Bilgi güvenliği, bilginin bir varlık olarak hasarlardan korunması, doğru teknolojinin, doğru amaçla ve doğru şekilde kullanılarak bilginin her türlü ortamda, istenmeyen kişiler tarafından elde edilmesini önleme olarak tanımlanır. Bilgisayar teknolojilerinde güvenliğin amacı, kişi ve kurumların bu teknolojilerini kullanırken karşılaşabilecekleri tehdit ve tehlikelerin analizlerinin önceden yapılarak gerekli önlemlerin alınmasıdır.

Bilgisayar güvenliği, aracıların (kullanıcılar veya programların) sadece müsaade edilen faaliyetleri icra edecek şekilde tasarlanmış olan güvenli bir bilgi işleme platformunu oluşturma çabalarıdır. Bu, güvenlik politikasının belirlenmesini ve gerçekleştirilmesini içermektedir. Sorgulanan faaliyetler, erişim, değiştirme ve silme işlemlerine indirgenebilir. Bilgisayar güvenliği, daha geniş güvenlik konularına bakan güvenlik mühendisliğinin bir alt alanı olarak görülebilir.

2.2.1. Güvenlik unsurları



Şekil 2.2. Güvenlik unsurları

Şekil 2.2'de gösterildiği gibi, gizlilik (confidentiality), bütünlük (integrity), kullanılabilirlik (availability), kimlik kanıtlama (authentication) ve inkar edememe (non-repudiation) bilgi güvenliğinin temel unsurlardır. Bunun dışında sorumluluk (accountability), erişim denetimi (access control), güvenilirlik (reliability) ve emniyet (safety) etkenleri de bilgi güvenliğini destekleyen özelliklerdir.

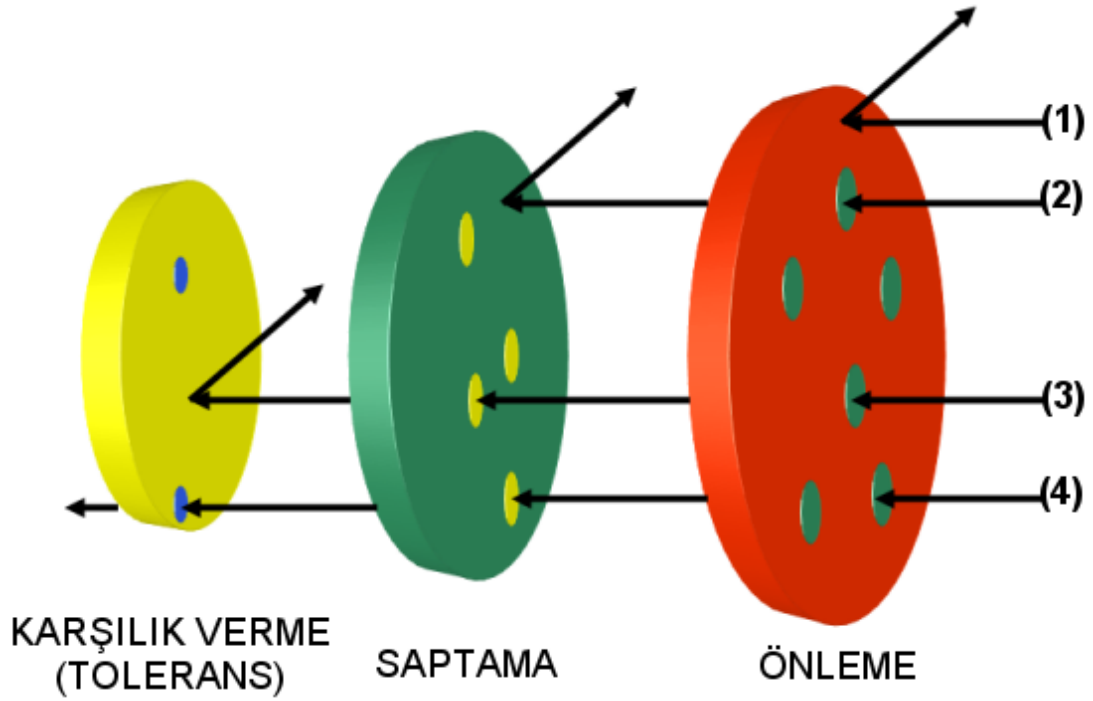
ISO tarafından ISO-17799 "Bilgi Güvenliği Yönetim Standardı" belgesinde, gizlilik, "bilginin sadece erişim hakkı olmaya yetkili kişilerce erişilebilir olmasının temini" olarak; bütünlük, "bilgi ve bilgi işleme yöntemlerinin doğruluğunun ve

eksiksizliğinin korunması" olarak; kullanılabilirlik, "yetkili kullanıcıların ihtiyaç duyulduğunda bilgi ve ilişkili varlıklara erişme hakkının olmasının temini" olarak tanımlanmıştır (16). Kimlik kanıtlama, geçerli kullanıcı ve proseslerin tanıması ve doğrulanması ve bir kullanıcının veya prosesin hangi sistem kaynaklarına erişme hakkının olduğunun belirlenmesi sürecidir. İnkar edememe, Alıcı ve vericinin gerçekte bilgiyi (mesajı) sırasıyla, alan ve veren taraf olduğunun doğrulanabilmesi demektir.

Sorumluluk, belirli bir eylemin yapılmasından kimin veya neyin sorumlu olduğunu belirleme yeteneğidir. Tipik olarak etkinliklerin kayıtlarını tutmak için bir kayıt tutma (logging) sistemine ve bu kayıtları araştıracak bir hesap inceleme (auditing) sistemine ihtiyaç duyar. Erişim denetimi, bir kaynağa erişmek için belirli izinlerin verilmesi veya alınması olarak tanımlanabilir. Güvenilirlik, bir bilgisayarın, bir bilginin veya iletişim sisteminin şartnamesine, tasarım gereksinimlerine sürekli ve kesin bir şekilde uyarak çalışması ve bunu çok güvenli bir şekilde yapabilme yeteneğidir. Emniyet, bir bilgisayar sisteminin veya yazılımın işlevsel ortamına gömülü olduğunda, kendisi veya gömülü olduğu ortam için istenmeyen potansiyel veya bilfiil tehlike oluşturacak etkinlik veya olaylara sebep olmamayı gösteren bir niteliktir.

2.2.2. Güvenlik süreçleri: önleme, saptama ve karşılık verme

Bilgi güvenliği çerçevesinde kurulacak güvenlik politikası ve altyapısının doğru şekilde belirlenebilmesi için, korunmak istenen bilginin değerlendirilmesi ve güvenlik risk analizinin doğru ve eksiksiz bir şekilde yapılması gerekir. Kurulacak güvenlik sistemin maliyeti, dikkate alınması gereken bir başka önemli husustur. Güvenlik sisteminin maliyeti, korunan bilginin değeri ve olası tehditlerin incelenmesiyle belirlenen risk ile sınırlı olmalıdır. %100 güvenliğin olmayacağı ilkesi ile beraber, bilgi güvenliğinin ideal yapılandırılması üç süreç ile gerçekleştirilir. Bu süreçler, önleme (prevention), saptama (detection) ve karşılık vermedir (response).



Şekil 2.3. Güvenlik süreçleri ve saldırılara tepkileri

Şekil 2.3'de gösterildiği gibi her bir süreç, sisteme yapılan saldırılara çeşitli aşamalarda cevap verebilmektedir. 1 numaralı saldırı, hemen önleme safhasında engellenirken; 2, 3 ve 4 numaralı saldırılar bu safhada önlenememiştir. Önleme sürecini atlatan bu saldırılardan 2 numaralı saldırı, saptama aşamasında tespit edilip, bertaraf edilirken; 3 ve 4 numaralı saldırılar, saptama aşamasından da geçebilmiştir. Belirlenen tolerans ile tasarlanmış son aşama olan karşılık verme safhasında, 3 numaralı saldırı önlenirken; bütün aşamaları atlatıp geçen 4 numaralı saldırı, bütün güvenlik süreçlerini geçip, sisteme zarar vermiştir. Takip eden kısımda güvenlik süreçlerinin her biri, temel özellikleri ile açıklanmaktadır.

1. Önleme

Önleme, güvenlik sistemlerinin en çok üzerinde durduğu ve çalıştığı süreçtir. Bir evin bahçesine çit çekmek, çelik kapı kullanmak gibi güncel hayatta kullanılan emniyet önlemleri gibi, bilgisayar sistemlerine yönelik tehdit ve saldırılara karşı, sistemin yalıtılmış olması için çeşitli önlemler geliştirilmektedir. Kişisel bilgisayar güvenliği ile ilgili, virüs tarama programlarının kurulu olması, bu programların ve

işletim sistemi hizmet paketlerinin ve hata düzeltme ve güncellemelerinin düzenli aralıklarla yapılması, bilgisayarda şifre korumalı ekran koruyucu olması, bilgisayar başından uzun süreliğine ayrı kalındığında sistemden çıkılması, kullanılan şifrelerin tahmininin zor olacak şekilde belirlenmesi, bu şifrelerin gizli tutulması ve belirli aralıklarla değiştirilmesi, disk paylaşımlarında dikkatli olunması, İnternet üzerinden indirilen veya e-posta ile gelen dosyalara dikkat edilmesi, önemli belgelerin parola ile korunması veya şifreli olarak saklanması, gizli veya önemli bilgilerin e-posta, güvenlik sertifikasız siteler gibi güvenli olmayan yollarla gönderilmemesi, kullanılmadığı zaman İnternet erişiminin kapatılması, önemli bilgi ve belgelerin düzenli aralıklarla yedeklerinin alınması gibi önlemler, basit gibi gözükebilecek ama hayat kurtaracak önlemlerden bazılarıdır.

Kurumsal ortamlarda bilgisayar güvenliğinde uygulanması gereken önleme adımları daha geniş ve karmaşıktır. Güvenlik ile ilgili uzmanlaşmış kişilerin çalıştığı bu tür sistemlerde, önleme ile ilgili yapılanlardan bazıları şunlardır: işletim sistemi ve yazılımların servis paketlerinin ve güncellemelerin düzenli aralıklarla incelenmesi, kullanıcı haklarının asgari seviyede tutulması, kullanılmayan protokol, servis, bileşen ve proseslerin çalıştırılmaması, veri iletişiminde şifreleme tekniklerinin kullanılması, korunmasızlık tarayıcıları, VPN (Virtual Private Network, Sanal Özel Ağ) kullanımı, PKI (Public Key Infrastructure, Açık Anahtar Altyapısı) ve biyometrik kullanımı.

2. Saptama

Güvenlik, sadece önleme ile sağlanabilecek bir mesele değildir. Örneğin bir müzede iyi bir korunmanın sağlanmış olması, müzenin çevresinin çitlerle çevrili olması, kapıların kapalı ve kilitli olması, o müzede geceleri bekçi kullanılmamasını gerektirmez. Aynı şekilde bilgisayar sistemlerinde de saldırı girişimlerini saptayacak yöntemlerin de kullanılması şarttır. Önleme, saldırıları güçleştiren (ama imkansız kılmayan) veya saldırganların cesaretini kıran (ama yok etmeyen) bir engel inşa etmeyi sağlar. Saptama ve karşılık verme olmadan önlemenin ancak sınırlı bir faydası olabilir. Sadece önleme ile yetinilseydi; yapılan çoğu saldırıdan haberdar bile olunamazdı. Saptama ile, daha önce bilinen veya yeni ortaya çıkmış saldırılar, rapor

edilip, uygun cevaplar verebilir. Saptamada ilk ve en temel basamak, sistemin bütün durumunun ve hareketinin izlenmesi ve bu bilgilerin kayıtlarının tutulmasıdır. Bu şekilde ayrıca, saldırı sonrası analiz için veri ve delil toplanmış olur. Güvenlik duvarları, IDS (Intruder Detection System, Saldırı Tespit Sistemi), ağ trafiği izleyiciler, kapı (port) tarayıcılar, honeypot (bal çanağı) kullanımı, gerçek zamanlı koruma sağlayan karşı virüs ve casus yazılım araçları, dosya sağlama toplamı (checksum) kontrol programları ve ağ yoklayıcı (sniffer) algılayıcıları, saptama sürecinde kullanılan en başta gelen yöntemlerden bazılarıdır.

3. Karşılık Verme

Bekçiler, köpekler, güvenlik kameraları, algılayıcılarla donatılmış bir yerin, hırsızları çekmesi gibi; gerçek zamanlı saptama sistemlerine sahip bilgisayar sistemleri de saldırganlara cazip gelir. Hızlı karşılık verme, bu saldırıları püskürtmek için güvenlik sistemini tamamlayan esaslı bir öğe olarak ortaya çıkmaktadır. Karşılık verme, önleme süreci ile baş edilemeyen ve saptama süreçleri ile belirlenmiş saldırı girişimlerini, mümkünse anında veya en kısa zamanda cevap verecek eylemlerin ifa edilmesi olarak tanımlanabilir. Saldırı tam olarak önlenmese bile; sistemin normal durumuna dönmesine, saldırıya sebep olan nedenlerin belirlenmesine, gerektiği durumlarda saldırganın yakalanmasına, güvenlik sistemi açıklarının belirlenmesine ve önleme, saptama ve karşılık verme süreçlerinin yeniden düzenlenmesine olanak verir. Saldırı tespit edilince yapılması gereken işlerin, daha önceden iyi bir şekilde planlanması, bu sürecin etkin bir şekilde işlemesini ve zaman ve para kaybetmemeyi sağlayacaktır. Yıkım onarımı (disaster recovery) bu aşama için gerçekleştirilen ve en kötü durumu ele alan esaslı planların başında gelir.

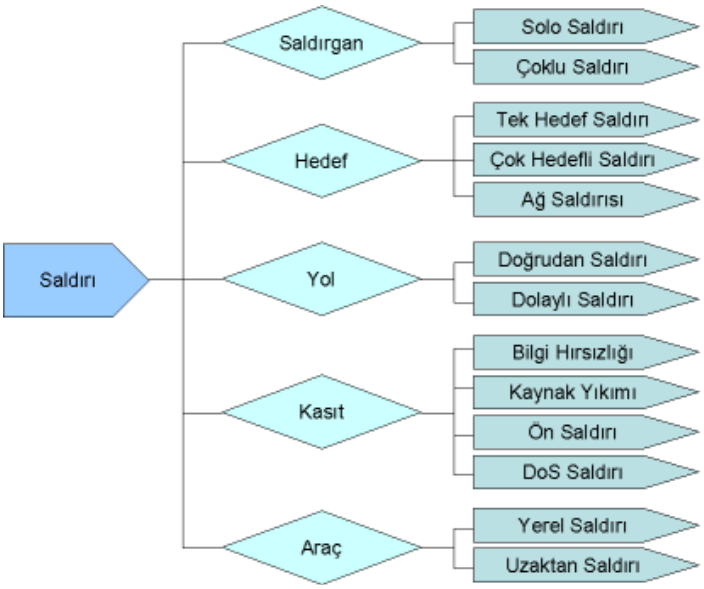
2.3. Sistemlere Yapılan Saldırılar ve Türleri

Güvenlik süreçlerinin belirlenmesinde yapılan ön teorik çalışmalar dışında; var olan sistemlere yönelik gerçekleşmiş veya gerçekleşebilecek olan saldırıların çok doğru bir şekilde belirlenmesi ve analiz edilmesi gerekmektedir. Sonuçta bütün güvenlik süreçleri afaki saldırıları önlemekten çok; gerçekten karşılaşılabilecek saldırılara

yönelik tasarlanmalıdır. Yani oluşturulacak güvenlik sistemine sadece kendi tarafımızdan değil; dışardan, saldırganın tarafından bakılması gereklidir. Resim 2.1'de esprili bir şekilde gözler önüne serildiği gibi, aslında bilgisayar sistemlerine yapılan saldırılar, çoğunlukla doğrudan güvenlik sistemini hedef alacak şekilde değil; güvenlik sistemine fark etmeden istenileni elde edecek şekilde yapılmaktadır. Bunun için saldırgan, sistemin korunmasızlıklarını araştırır ve ona göre hareket eder. Korunmasızlık (vulnerability), ilgili sistem, ağ, uygulama veya protokolün güvenliğini tehlikeye atan; beklenmeyen ve istenmeyen bir olaya sebep olabilecek bir zayıflığın varlığı, tasarım veya gerçekleme hatası olarak tanımlanmaktadır (17). Bilgisayar sistemlerinin güvenliği ile ilgili geliştirilen yöntemlerin anlaşılması için bu korunmasızlıkları hedefleyen saldırı (atak) türlerinin belirlenmesi ve bu saldırılara karşı alınabilecek önlemlerin geliştirilmesi gerekmektedir.

Resim 2.1. "Güvenlik atlatılır, saldırılmaz", Adi Shamir (18)

Saldırılar çeşitli şekillerde sınıflandırılarak incelenebilir. Saldırgan sayısına, hedef türüne, kullanılan yola, kasıt ve araçlara göre saldırılar, Şekil 2.4'de gösterildiği gibi sınıflanmaktadır.



Şekil 2.4. Saldırıların sınıflandırılması

Tek bir saldırgan tarafından yürütülen solo saldırı, en genel türde saldırıların başında gelir ve saptanması daha kolaydır. Sistem korunmasızlık saldırıları ve yetkisiz erişim, solo saldırı türündedir. Birden fazla saldırganın karıştığı saldırılar, çoklu saldırı olarak adlandırılır. IP kandırma (spoofing), e-posta bombardımanı ve ağ taşkını (flooding) bu tür saldırılardır. "Back Orifice" ve Winnuke saldırıları gibi saldırılar tek hedefe yönelik saldırılardır. Anormal paket yayınlama saldırısı, tarama saldırısı ve anonim FTP saldırısı çok hedefli saldırılardır. DNS kandırma (DNS Spoofing), yönlendirici (router) saldırısı ve ağ DoS (Denial of Service, hizmet aksattırma) saldırısı, ağ saldırı türüdür. Doğrudan saldırılar arasında arabellek taşması, "ölümüne ping" (ping of death) saldırılarını saymak mümkündür. Yerel saldırılar sisteme giriş (login) yapıldıktan sonra gerçekleştirilmektedir.

Başlıca saldırı türleri arasında, kaynak kod istismarı, gizli dinleme (eavesdropping), sosyal mühendislik ve insan hatası, hizmet aksattırma saldırıları (DoS), dolaylı saldırılar, arka kapılar (backdoor), doğrudan erişim saldırıları ve kriptografik

saldırıları saymak mümkündür. Bu saldırılar takip eden kısımlarda sırasıyla açıklanmaktadır.

2.3.1. Kaynak kod istismarı

Sistemde kullanılan (işletim sistemi için hazırlanan sistem programları dahil) tüm yazılımlarda var olabilecek arabellek taşması (buffer overflow), CGI betikleme (scripting) hataları ve şifreleme hataları gibi yazılım kusurları, bir bilgisayar sisteminin kontrolünün ele geçirilmesine veyahut o bilgisayarın beklenmedik bir şekilde çalışmasına neden olabilir. Bu, son yıllara kadar gözden kaçırılan bir konu olarak, bir çok saldırıya açık kapı bırakmış bir korunmasızlıktır. Özellikle işletim sistemi yazılımları tasarlanırken, geliştirilirken ve test edilirken, güvenliği hiç bir şekilde göz ardı etmeyecek çalışmalara ihtiyaç vardır. En çok kullanılan işletim sistemi olarak belirtilen Microsoft Windows işletim sisteminde, bu tür kaynak kod kusurları, hazırlanan güvenlik bültenleri ile kullanıcılara duyurulmakta; çok önemli düzeltmeler ("hot-fix") ve belirli aralıklarda çıkan hizmet paketleri, kullanıcılara gerek çevrimiçi gerekse CD gibi ortamlarda sunulmaktadır. Bu düzeltmelerin çokluğu, işletim sistemi geliştirilmesi sırasında öngörülmeyen veya dikkat edilmeyen yazılım kusurlarının çokluğuna işaret etmektedir. Bu konuda Microsoft firması, piyasaya çıkardığı işletim sistemi yazılımları için güvenliği merkeze alan çalışmalara hız vermiştir. "Güvenlik Geliştirme Yaşam Döngüsü" (SDL, Security Development Lifecycle) yaklaşımı ile geliştirilen Windows Server 2003'ün, Windows 2000'e göre çok daha az güvenlik bülteni ile piyasaya sürüldüğü belirtilmektedir (19). Microsoft, güvenliğin önemini algılamış ve bu konudaki yatırımlarını ve çalışmalarını artırmaya başlamıştır (20).

2.3.2. Gizli dinleme

Bir ağ veya kanal üzerinden iletilen verinin, kötü niyetli üçüncü kişiler tarafından araya girilerek alınması; hatta kaynaktan hedefe giden verinin arada elde edilip, değiştirilerek hedefe gönderilmesi bile mümkündür. İngilizce "eavesdropping" (saçak damlası) olarak adlandırılan bu saldırının, sanıldığının aksine çok farklı

uygulama alanı bulunmaktadır. Hiç bir bilgisayarla etkileşimi olmayan tek başına çalışan bir bilgisayar bile, mikroçip, ekran veya yazıcı gibi elektronik parçalarından yayılan elektrik veya elektromanyetik yayılım takip edilerek gizlice dinlenebilir. Bu cihazların bu tür dinlemelere olanak vermemesi için, Amerikan hükümeti 1950'li yılların ortasından başlayarak TEMPEST adında bir standart geliştirmiştir.

2.3.3. Sosyal mühendislik ve insan hatası

İnsan faktörü, her işte olduğu gibi güvenlik işinde de en önemli etken olarak karşımıza çıkmaktadır. Bilgisayar sistemlerinde karşılaşılan güvenlik ile ilgili bir çok olay, insan faktörünün kasten veya bilerek devreye girmesiyle meydana gelmektedir. Bilgisayar güvenliğinde sosyal mühendislik, bir bilgisayar korsanının, ilgilendiği bilgisayar sistemini kullanan veya yöneten meşru kullanıcılar üzerinde psikolojik ve sosyal numaralar kullanarak, sisteme erişmek için gerekli bilgiyi elde etme tekniklerine verilen genel addır. Özellikle telefon ile kullanıcı ve şifre bilgilerini elde etme, buna en tipik örnektir. Korsan sıradan bir şirket kullanıcısı gibi sistem yöneticilerinden bu tür bilgileri edinebilir. Bu konuda bir çok taktik düşünebilir ve tüm bu taktiklerden yara almadan çıkmak için yapılması gereken en önemli şey, kullanıcıların düzenli olarak eğitilmesi ve uyarılması ve sistem yöneticileri dahil tüm kullanıcıların istisnası olmadan güvenlik ile ilgili politikalara uymasıdır (21).

Bilgisayar sistemlerinde gerçekleşen bir çok hasar insan hatası ile meydana gelmektedir. Kurum içi kullanıcıların aslında bizzat kendileri, kullandıkları sisteme en çok hasar veren kişilerdir. Bir diğer dikkat edilmesi gereken husus, bir şirketten ayrılan veya çıkartılan kişinin, daha sonradan çalışmış olduğu bu şirkete zarar vermesi veya saldırması olasılığıdır. Bunun için şirketten ayrılan kişiler için çeşitli güvenlik politikaları oluşturulmalıdır. Sosyal mühendislikte kullanılan ilginç yöntemler, risk alanı, korsanın uyguladığı taktik ve bunlara karşı mücadelede yapılması gerekenler Çizelge 2.1'de listelenmektedir. Listeden de görülebileceği gibi sosyal mühendislik, bir bilgisayar kullanıcısını, bilgisayarını kullanırken arkasından hissettirmeden gözetlemekten, iş yerinde kağıt atıkları arasında işe yarar belge aramaya kadar, akla gelmeyecek çeşitli yöntemleri kullanmaktadır.

Çizelge 2.1. Yaygın sosyal mühendislik taktikleri ve önlemler (22)

Risk Alanı	*Korsan Taktiği*	*Mücadele Stratejisi*
Telefon (Yardım Masası)	Taklit ve inandırma	Çalışanların ve yardım masasının telefonla hiç bir şekilde şifre veya diğer gizli bilgilerin verilmemesi için eğitilmesi
Binaya giriş	Yetkisiz fiziksel erişim	Sıkı kimlik kartı güvenliği, çalışanların eğitilmesi ve güvenlik görevlilerin çalıştırılması
Ofis	Omuz sörfü[1]	Sizden başka birinin ortamda bulunduğu durumlarda şifrenizi girmeyin. Zaruri durumlarda hızlı bir şekilde tuşlara basınız.
Telefon (Yardım Masası)	Yardım masası aramalarında taklit etme	Bütün çalışanlara yardım masası desteği alabilmesi için tekil bir PIN numarası atanması.
Ofis	Kimsenin olmadığı açık odalar bulabilmek için koridorlarda dolaşma	Bütün misafirlere işyerinden bir refakatçi sağlanması
Posta odası	Sahte notların sokulması	Posta odasını kilitle ve izlemeye tabi tut
Makine odası – Santral	Erişmeye teşebbüs, cihazların kaldırılması ve gizli bilgileri elde edebilmek için bir protokol analizcisi eklenmesi	Santral, sunucu odaları v.s. her zaman kilitli tut ve cihazların güncel envanterini tut
Telefon ve PBX	Telefon görüşme ücreti erişimi çalma	Şehirlerarası, milletlerarası ve cep telefonu aramalarını kontrol et, konuşmaları izle, aktarmaları reddet
İş yeri atık deposu (dumpster)	Çöplük karıştırma	Bütün çöp kutularını güvenli ve izlenen alanlarda tut. Önemli belgeleri kesme makinesiyle yok et, manyetik ortamdaki verileri sil.
İntranet - İnternet	Şifre araklamak için İntranet veya İnternet üzerinde sahte yazılımların oluşturulması ve konulması	Sistem ve ağ değişikliklerinden sürekli haberdar olma, şifre kullanımı eğitimi
Ofis	Hassas belgelerin çalınması	Belgelere gizlilik derecesi ver ve bu belgeleri kilitli yerlerde sakla
Genel - Psikolojik	Taklit ve ikna	Bütün çalışanları sürekli uyanık tutarak ve eğitim programlarına tabi tutarak bilinçlendirme

2.3.4. Hizmet aksattırma saldırıları

Hizmet aksattırma saldırıları, yetkisiz erişim veya sistem kontrolünü ele geçirmeye yarayan saldırılardan farklı bir amaç için gerçekleştirilen saldırılardır. Bu saldırının tek amacı bir bilgisayar, sunucu veya ağın kaldırabileceğinden daha fazla yük bindirilmesi sağlanarak, sistemin kullanılmaz hale getirilmesidir. Bu tip saldırılar genelde bant genişliği, boş disk alanı veya CPU zamanı gibi bilgi işlem

[1] Omuz sörfü: Klavye ile yazı yazarken çevredeki birinin sizi gözetlemesi (shoulder surfing)

kaynaklarının tüketilmesi; yönlendirme (routing) bilgileri gibi yapılandırma bilgilerinin bozulması ve fiziksel ağ bileşenlerinin bozulması şeklinde yapılmaktadır. Ağ üzerinde kilit önem taşıyan bir sunucuya yapılan bu tip bir saldırı, tüm ağın işlemez hale gelmesine yol açabilir. Bu saldırıları önlemek için tüm ağın analizi gerektiğinden, saldırıların önüne geçilmesi çok zordur. Dağıtık hizmet aksattırma saldırıları (DDoS, Distributed Denial of Service), tek bir kaynaktan değil de birden fazla ele geçirilmiş konak bilgisayardan, tek bir hedefe doğru yapılan hizmet aksattırma saldırısıdır. Yeterli sayıda saldırgan bilgisayar kullanarak, çok büyük ve iyi ağ bağlantılı web sitelerinin hizmetleri bile aksattırılabilir.

2.3.5. Dolaylı saldırılar

Bu tür saldırılar, uzaktan erişilerek devralınmış üçüncü parti bir bilgisayardan başlatılan değişik türde saldırıları kapsamaktadır. Hayalet bilgisayar (zombie computer) olarak adı geçen başka bir bilgisayarın saldırıda kullanılması, saldırıyı gerçekleştiren asıl kaynağın belirlenmesini güçleştirir. Mesela, Türkiye aleyhinde haksız ve kötü yayın yapan siteleri çökertmek iddiasıyla bir araya gelen insanların kurduğu bir sitede, buna katılan kişilere bir program vererek yapılacak saldırıya kendi bilgisayarlarının desteği istenmesi, dolaylı saldırı türünde bir örnek olarak verilebilir (23).

2.3.6. Arka kapılar

Bilgisayar üzerinde sıradan incelemeler ile bulunamayacak şekilde, normal kimlik kanıtlama süreçlerini atlatan veya kurulan bu yapıdan haberdar olan kişiye o bilgisayara uzaktan erişmeyi sağlayan yöntemler, arka kapı olarak adlandırılmaktadır. Arka kapı, kurulu bir program şeklinde (örneğin Back Orifice) olabileceği gibi; var olan meşru bir programın bizzat kendisinde, o programı yazan kişi tarafından belgelendirilmemiş bir biçimde, kasten bırakılmış olabilir. Bu tür saldırılarda özellikle Truva atı (Trojan horse) programları yoğun bir şekilde kullanılmaktadır.

2.3.7. Doğrudan erişim saldırılarını

Bir bilgisayar sistemine doğrudan fiziksel erişime sahip olan bir kişinin yaptığı saldırılar bu grupta toplanmaktadır. Bilgisayara fiziksel erişim sağlayan kişi, işletim sistemlerinde kendisi için bir kullanıcı belirlemek gibi ileride kullanılabilecek çeşitli değişiklikler yapabilir; yazılım solucanları, klavye dinleme sistemleri ve gizli dinleme cihazlarını sisteme kurabilir. Doğrudan erişime sahip olan saldırgan ayrıca, CD-ROM, DVD-ROM, disket gibi yedekleme ünitelerini; bellek kartları, sayısal kameralar, sayısal ses sistemleri, cep telefonu ve kablosuz/kızılötesi bağlantılı cihazları kullanarak, büyük miktarda bilgiyi kendi tarafına kopyalayabilir. Bu açıdan, bir bilgisayar sistemi üçüncü şahısların kullanımına kısa süreliğine bile olsa bırakılmamalıdır.

2.3.8. Kriptografik saldırılar

Şifrelenmiş bilgilerin şifresini kırmak veya çözmek için yapılan saldırılardır. Bu saldırılar, kriptoanaliz yöntemleri ile gerçekleştirilmektedir. Bunlar arasında kaba kuvvet saldırısı (brute force attack), sözlük saldırısı (dictionary attack), ortadaki adam saldırısı (man in the middle attack), sade şifreli metin (chipertext only), bilinen düz metin (known plaintext), seçilen düz metin veya şifreli metin (chosen plaintext, chipertext), uyarlanır seçili düz metin (adaptive chosen plaintext) ve ilişkili anahtar (related key attack) saldırılarını saymak mümkündür (6).

2.4. Kişisel Gizlilik

Bilgi güvenliği ile ilgili bir başka önemli kavram, mahremiyet ya da kişisel gizliliktir. Genel anlamda kişisel gizlilik, temel bir insan hakkıdır. Birleşmiş Milletler Genel Kurulu'nda 1948 yılında ilan edilen ve ülkemizde 27 Mayıs 1949'da Resmi Gazete'de yayınlanan İnsan Hakları Evrensel Beyannamesi'nin 12. maddesi, kişisel gizliliği "özel yaşam" olarak şu şekilde ifade etmektedir (24):

“Madde 12- Kimsenin özel yaşamına, ailesine konutuna ya da haberleşmesine keyfi olarak karışılamaz, şeref ve adına saldırılamaz. Herkesin bu gibi karışma ve saldırılara karşı yasa tarafından korunmaya hakkı vardır.”

Mahremiyet, insan itibarının ve değerlerinin temelini oluşturur. Modern çağın en önemli haklarından biri haline gelen kişisel gizlilik, daha ayrıntılı olarak “kesintisiz bir biçimde, müsaadesiz bir şekilde araya girme, mahcubiyet veya sorumluluk olmadan, her bireye, fiziksel bir alan sağlama isteği ve kişilerin kendileri ile ilgili bilgilerinin açıklanması zamanını ve şeklini denetleme girişimi” şeklinde tanımlanabilir (25). Kişisel gizliliğin dört yüzü bulunmaktadır. Genetik testler, ilaç deneyleri gibi zorlayıcı prosedürlere karşı, kişilerin doğrudan fiziksel bünyelerinin korunmasını ele alan, bedensel mahremiyet; posta, telefon, e-posta ve diğer iletişim şekillerinin güvenliğini ve gizliliğini kapsayan, iletişim mahremiyeti; ev ve iş yeri veya umuma açık yerler gibi diğer ortamlara müdahalenin sınırlarının belirlenmesini ele alan, yaşam alanı mahremiyeti ve kredi kartı bilgileri ve tıbbi ve hükümet kayıtları gibi kişisel verilerin toplanması ve işlenmesini yöneten kuralların tespitini ele alan, bilgi mahremiyetidir (“veri koruma”).

Bilgisayar sistemlerinde güvenlik, kişisel gizliliğe dayanmaktadır. Güvenlik ile ilgili uygulanan yöntem ve tedbirlerin kişisel gizliliği çiğnemeyecek şekilde hazırlanması gerekmektedir.

2.5. Ülkemizde Bilişim Suçlarına Yönelik Yasal Düzenlemeler

Bilgi ve bilgisayar güvenliği ve kişisel gizlilik, klavye dinleme sistemleri ve diğer casus yazılımlar konusunda tartışılan en önemli konulardan biri de, bilgi ve bilgisayar güvenliği ve kişisel gizliliğe karşı yapılan saldırıları caydırmak amacıyla yasalarda ne gibi önlemler alındığıdır. Bu konuda yurtdışında yapılan yasal çalışmalar ayrıca Bölüm 5.7.6 “İşyeri gözetleme” kısmında açıklanmaktadır. Ülkemizde ise, bilgi ve bilgisayar güvenliği ve kişisel gizlilik konusunda yapılan yasal düzenlemeler oldukça yenidir. Bilişim suçları tanımlaması bile bulunmayan eski kanunlar, 12 Ekim 2004’de Resmi Gazete’de yayımlanan yeni Türk Ceza

Kanunu ile, ilk defa bu açıdan bakılarak düzenlenmiştir (26). Konu, ülkemizde özellikle çevrimiçi bankacılık ve elektronik ticaret açısından oldukça önemlidir. Ülkemizde İnternet üzerinden kredi kartı ile yapılan e-ticaret hacmi, son yıllarda oldukça hızlı bir şekilde artmaktadır. Bankalararası Kart Merkezi'nin raporlarına göre, 2005 yılında ilk altı aylık e-ticaret, 563,5 milyon YTL'ye ulaşmaktadır (27). İleride daha da artacak çevrimiçi işlemlerde güvenliğin sağlanmasına yönelik yasal durumun incelenmesi, bilinçli kullanıcıların sahip oldukları hakları öğrenmesi ve bu tür suçların caydırılması açısından önemlidir.

5237 sayılı kanunun Onuncu Bölüm, "Malvarlığına Karşı Suçlar" başlığında, "nitelikli hırsızlık", 142. Madde 2 (e) bendinde, "Hırsızlık suçunun, bilişim sistemlerinin kullanılması suretiyle, işlenmesi hâlinde, üç yıldan yedi yıla kadar hapis cezasına hükmolunur." şeklinde cezalandırılmaktadır. Yine "nitelikli dolandırıcılık", Madde 158'de 1 (f) bendinde "Dolandırıcılık suçunun; bilişim sistemlerinin, banka veya kredi kurumlarının araç olarak kullanılması suretiyle, işlenmesi halinde, iki yıldan yedi yıla kadar hapis ve beş bin güne kadar adlî para cezasına hükmolunur." şeklinde tanımlanmaktadır (26).

Yeni Türk Ceza Kanunun Onuncu Bölümünde Madde 243, 244, 245 ve 246, "Bilişim Alanında Suçları" ilk defa tanımlamaktadır. Bu dört maddenin içerikleri konu ile doğrudan ilişkili olması sebebiyle aşağıdaki alt başlıklarda sunulmaktadır. Bilişim alanında suçlarla "korunmak istenen hukuki yarar" bilgisayarın dokunulmaz olması ve sistemin istendiği şekilde hizmet görmesi gereğidir (28).

2.5.1. Bilişim sistemine girme

MADDE 243. - (1) Bir bilişim sisteminin bütününe veya bir kısmına, hukuka aykırı olarak giren ve orada kalmaya devam eden kimseye bir yıla kadar hapis veya adlî para cezası verilir.

(2) Yukarıdaki fıkrada tanımlanan fiillerin bedeli karşılığı yararlanılabilen sistemler hakkında işlenmesi halinde, verilecek ceza yarı oranına kadar indirilir.

(3) Bu fiil nedeniyle sistemin içerdiği veriler yok olur veya değişirse, altı aydan iki yıla kadar hapis cezasına hükmolunur.

Casus yazılımlar ve klavye dinleme sistemleri açısından önemli olan bu maddeye göre, sisteme hukuka aykırı olarak girip; orada kalmaya devam etmekle suç tamamlanır. Açıklanan şekilde sisteme girmeye çalışmak veya girdikten sonra orada kalmayı başaramamak, teşebbüs halidir. Sisteme hukuka aykırı olarak giren ve orada kalmaya devam eden kimsenin ilgiliye zarar vermek veya yarar elde etmek ya da belirli verileri elde etmek amacına yönelmiş veya bu türden sonuçlara ulaşmış olmasının, suçun oluşumu bakımından önemi yoktur (28).

2.5.2. Sistemi engelleme, bozma, verileri yok etme veya değiştirme

MADDE 244. - (1) Bir bilişim sisteminin işleyişini engelleyen veya bozan kişi, bir yıldan beş yıla kadar hapis cezası ile cezalandırılır.

(2) Bir bilişim sistemindeki verileri bozan, yok eden, değiştiren veya erişilmez kılan, sisteme veri yerleştiren, var olan verileri başka bir yere gönderen kişi, altı aydan üç yıla kadar hapis cezası ile cezalandırılır.

(3) Bu fiillerin bir banka veya kredi kurumuna ya da bir kamu kurum veya kuruluşuna ait bilişim sistemi üzerinde işlenmesi halinde, verilecek ceza yarı oranında artırılır.

(4) Yukarıdaki fıkralarda tanımlanan fiillerin işlenmesi suretiyle kişinin kendisinin veya başkasının yararına haksız bir çıkar sağlamasının başka bir suç oluşturmaması halinde, iki yıldan altı yıla kadar hapis ve beş bin güne kadar adlî para cezasına hükmolunur.

2.5.3. Banka veya kredi kartlarının kötüye kullanılması

MADDE 245. - (1) Başkasına ait bir banka veya kredi kartını, her ne suretle olursa olsun ele geçiren veya elinde bulunduran kimse, kart sahibinin veya kartın kendisine

verilmesi gereken kişinin rızası olmaksızın bunu kullanarak veya kullandırtarak kendisine veya başkasına yarar sağlarsa, üç yıldan altı yıla kadar hapis cezası ve adlî para cezası ile cezalandırılır.

(2) Sahte oluşturulan veya üzerinde sahtecilik yapılan bir banka veya kredi kartını kullanmak suretiyle kendisine veya başkasına yarar sağlayan kişi, fiil daha ağır cezayı gerektiren başka bir suç oluşturmadığı takdirde, dört yıldan yedi yıla kadar hapis cezası ile cezalandırılır.

2.5.4. Tüzel kişiler hakkında güvenlik tedbiri uygulanması

MADDE 246. - (1) Bu bölümde yer alan suçların işlenmesi suretiyle yararına haksız menfaat sağlanan tüzel kişiler hakkında bunlara özgü güvenlik tedbirlerine hükmolunur.

Bütün bu maddelerin hazırlanmış olması, bilgi ve bilgisayar güvenliğindeki yasal açıkları önlemek için önemli bir adımdır. Fakat konunun oldukça hızlı değişen yapısı sebebi ile; bilgi ve bilgisayar güvenliğindeki mevcut durumun yasal çerçevede karşılığının bulunup bulunmadığı, yetkili kişiler tarafından sürekli olarak takip edilmesi ve gerekli durumlarda yapılması gereken düzenlemelerin bir an önce alınması gerekmektedir.

2.6. Değerlendirme

Kişisel gizlilik ve bilginin korunmasında güvenliğin ne kadar önemli olduğunun herkes tarafından akılda tutulması ve bilgi güvenliğine yönelik uygulama politikalarının doğru bir şekilde belirlenmesi ve titizlikle uygulanması şarttır. Bilgi ve bilgisayar güvenliğe yönelik saldırıların en başında gelen ve şu sıralar oldukça güncel bir konu olarak karşımıza çıkan casus yazılımların ne olduğunun, doğru bir şekilde öğrenilmesi gerekmektedir. Antik Çinli filozof Sun Tzu, 2500 yıl önce Savaş Sanatı adlı kitabında muhaberede anahtar olarak sunduğu düşünceyi “kendinizi tanımak, savunma durumunda olmanıza imkan verir; düşmanı tanımak, saldırıya

geçmenizi kolaylaştırır" ve "düşmanınızı ve kendinizi tanırsanız, zaferiniz kesinleşir" olarak özetlemektedir (29). Veri, bilgi ve özbilgi gibi kavramları doğru bir şekilde tanımlayıp, bilgi ve bilgisayar güvenliğini ve saldırıları inceledikten sonra, en azılı bilgi güvenliği düşmanlarından casus yazılımların her yönüyle incelenmesi gerekmektedir.

Yukarıda açıklananlar ışığında ve belirtilen gerekçe ve sebeplerden dolayı, bu tez çalışmasında sonraki iki bölümde casus yazılımlar ve casus savar yazılımlar her yönüyle incelenmiş; dikkat edilmesi gerekenler konular açıklanmış; konunun daha iyi anlaşılması için klavye dinleme yaklaşımı sunan bir casus yazılım ile bir casus savar yazılım sistemi geliştirilmiş ve bu yazılımlar ile karşılaşılabilecek tehlikeler farklı uygulama örnekleri ile ortaya konulmaya çalışılmıştır.

3. CASUS YAZILIMLAR

Casus yazılım (spyware) olarak ifade edilen yazılımlar, kötücül yazılım (malware) adı verilen yazılımların bir türü olarak tanımlanmaktadır. On bir adet ana sınıf kötücül yazılım dışında, yapılan geniş araştırmalar sonucunda bir araya getirilen 35 adet diğer türde kötücül yazılım, 3.1.12 kısmında açıklanmıştır. Kötücül yazılımlarla ilgili bütün türler derlenmeye çalışılarak, varolan tehdidin tamamının gösterilmeye çalışılmasının, ülkemizde bu konuda ortaya çıkan bilgi ve kaynak eksikliğini kapatmaya yönelik fayda sağlayacağı düşünülmektedir.

Ayrıca, mantar gibi çoğalan kötücül yazılımları adlandırırken sonu "ware" ile biten oldukça fazla sayıda birbirinden ilginç İngilizce isim kullanılmaktadır. Bu çalışmada, bu tür terimlere en uygun Türkçe karşılıklar verilmeye çalışılmıştır. Bunlar arasında "phishing" terimine karşılık olarak düşünülen "sazan avlama" ifadesi, Türk Dil Kurumu'nun Bilgisayar Terimleri Karşılıklar Kılavuzu'na öneri olarak bildirilmiştir. Bu karşılık dışında, tarayıcı soyma (browser hijacking), telefon çevirici (dialer), kök kullanıcı takımı (rootkit), korunmasızlık sömürücüleri (exploit), püsküllü bela yazılım (pestware), web böcekleri (web bugs), bot ağı (botnet), ağ taşkını (flooder), aldatmaca (hoax), telefon kırma (phreaking), kapı tarayıcı (port scanner), sondaj aracı (probe tool), turta (PIE), damlatıcı (trickler) ve savaş telefon çeviricileri (war dialer) gibi kötücül yazılımların İngilizce isimlerine Türkçe karşılıkları da, bilindiği kadarıyla ilk olarak bu çalışmada bulunup, metin içinde kullanılmıştır. İleride sıkça gündeme gelecek olan antispyware terimine karşı da yine bu çalışmada ilk olarak "casus savar yazılım" karşılığı da önerilmiştir. Bilim dilinde Türkçe'nin kullanılmasında bilgi ve bilgisayar güvenliği konularında destek olmayı da amaçlayan bu çalışmada önerilmiş olan karşılıkların, hem ülkemiz akademik camiası ile bilgi ve bilgisayar güvenliği uzmanları arasında; hem de bu konuda zaten yeterince bilgisi olmayan ve İngilizce bilmeyen kullanıcıları daha kolay bilinçlendirebilmek adına yaygınlaşması ümit edilmektedir.

Bu bölümde ayrıca, kötücül yazılım ve bu tür yazılımlara karşı alınabilecek tedbirlere ilişkin ana unsurlar, casus yazılımların tarihi gelişimi ve çalışmanın

yapıldığı tarihe kadar bilinen en yaygın casus yazılımların neler olduğu açıklanmaktadır.

3.1. Kötücül Yazılım (malware)

Kötücül yazılım (malware, İngilizce "malicious software"in kısaltılmışı), bulaştığı bir bilgisayar sisteminde veya ağ üzerindeki diğer makinelerde zarara yol açmak veya çalışmalarını aksatmak amacıyla hazırlanmış yazılımların genel adıdır. Şekil 3.1'de şema şeklinde gösterilen virüsler, solucanlar (worms), Truva atları (Trojan), casus yazılımlar (spyware), arka kapılar (backdoor), klavye dinleme sistemleri (keylogger), tarayıcı soyma (browser hijacking), telefon çeviriciler (dialer), kök kullanıcı takımları (rootkit), korunmasızlık sömürücüleri (exploit) ve tavşanlar (wabbit) en genel kötücül yazılımlardır. Kötücül yazılımlar için (daha çok argo olarak) kullanılan başka bir ismin de scumware (kirli yazılım) olduğunu belirtmekte fayda vardır.

Şekil 3.1. Kötücül yazılım ana türleri

3.1.1. Bilgisayar virüsleri

En tehlikeli ve en eski kötücül yazılım olarak kabul edilebilir. Organizmalardaki hücrelere bulaşan küçük parçacıklar olarak tanımlanan biyolojik virüslerden esinlenerek adlandırılan bilgisayar virüsleri, kendi kopyalarını çalıştırılabilir diğer kodlara veya belgelere yerleştirilerek yayılan ve kendi kendine çoğalan bir programdır. Ekranda rahatsız edici, çalışmaya kısa süreliğine de olsa mani olan mesajlar göstermek gibi zararsız sayılabilecek türlerinin de bulunmasına karşın; çoğu virüs programlarının, önemli dosyaları silmek veya konak (host) sistemini tamamen çalışmaz hale getirmek gibi yıkıcı etkileri bulunmaktadır. Bir bilgisayar solucanın bir parçası olarak ağ üzerinden yayılabilir olmalarına rağmen; tanım olarak virüsler, yayılmak için ağ kaynaklarını kullanmazlar. Bunun yerine disket, CD veya DVD gibi ortamlarla veya e-posta eklentileri ile hedef sistemlere bulaşırlar.

Virüsler yaygınlaştıkça virüs korunma programları da gelişmeye başlamış ve McAfee ve Symantec gibi firmaların öncülüğünü yaptığı virüs korunma programları bir bilgisayar güvenlik sisteminin ayrılmaz bir parçası olmuştur. Bu firmalar kötü niyetli kişiler tarafından geliştirilen "vahşi" ("the wild") olarak tabir ettikleri virüslere karşı önlemler üretmek yanında; "hayvanat bahçesi" ("zoo") tabir ettikleri laboratuarlarında ileride çıkması muhtemel virüslere için de çeşitli çalışmalar yürütmektedirler. Bilgisayar virüsleri dört sınıfta incelenebilirler:

- Dosya virüsleri
- Önyükleme (boot) virüsleri
- Makro virüsleri
- Betik (script) virüsler

Dosya virüsleri, yayılmak için kendilerini çeşitli dizinlere kopyalayarak veya virütik kodlarını çalıştırılabilir dosyalara bulaştırarak, işletim sistemi dosya sistemini kullanan virüs türleridir. Önyükleme (boot) virüsleri, sabit disk veya disketin "Ana Önyükleme Kaydını" (Master Boot Record) değiştirerek bilgisayarın her açılışında virütik kodun çalışmasını sağlayan virüslerdir. 26 Nisan 1986'da yaşanan Çernobil

faciası üzerine Çernobil virüsü olarak adlandırılan ve bu tarihte bulaştığı konak sisteme zarar veren W95/CIH virüsü, önyükleme virüsleri arasında en çok tanınan ve oldukça zararlı olan virüslerden biridir. Makro virüsleri, Microsoft Word ve Excel gibi güçlü makro desteği olan masaüstü programları kullanan ve bunlara ait belgelerin açılışında çalışan makrolar ile yayılan virüs türleridir. Çalıştırılabilir dosyalar dışındaki dosyalara bulaşan ilk virüs olan WinWord/Concept (30) ve Microsoft Excel çalışma sayfalarına bulaşan XM/Laroux, bu tür makro virüslerine örnek olarak verilebilir. Betik (script) virüsler, VB (Visual Basic), JavaScript, BAT (toplu işlem dosyası), PHP gibi betik dilleri kullanılarak yazılan virüslerdir. Bu virüsler ya diğer Windows veya Linux komut ve hizmet dosyalarına bulaşır ya da çok bileşenli virüslerin bir parçası olarak çalışırlar. Betik desteği olan ve zararsız gibi görünen HTML, Windows yardım (help) dosyaları, toplu işlem dosyaları ve Windows INF dosyaları, bu tür virüslerin yerleştiği dosyalar olarak karşımıza çıkabilir.

3.1.2. Bilgisayar solucanları (worms)

Bilgisayar virüslerine benzer yapıda olan solucanlar, virüsler gibi bir başka çalıştırılabilir programa kendisini iliştirmez veya bu programın parçası olmaz. Solucanlar, yayılmak için başka bir programa ihtiyaç duymayan, kendi kendini çoğaltan bir yapı arz ederler. Bir solucanın yayılmasında kullandığı en yaygın yöntemler arasında, e-posta ve FTP ve HTTP gibi İnternet hizmetlerini kullanmaktadır. Solucanları yaymak için, hedef sistemdeki korunmasızlıklardan faydalanma veya kullanıcıların solucanları çalıştırabilmeleri için sosyal mühendislik yöntemlerini kullanma gibi yöntemler kullanılmaktadır. Solucanlar, başka dosyaları değiştirmezler; fakat etkin bir şekilde bellekte dururlar ve kendilerini kopyalarlar. Solucanlar otomatik olarak gerçekleştirilen ve genellikle kullanıcılara gözükmeyen işletim sistemi yapılarını kullanırlar. Solucanların kontrol dışı çoğalmaları, sistem kaynaklarını aşırı kullandığında veya diğer işlemekte olan görevleri yavaşlattığında veya bu görevlerin sonlanmalarına neden olduğunda farkına varılabilir. Solucan ismi, 1975 yılında John Brunner tarafından yazılan “Shockwave Rider” (Şok Dalgası

Binicisi) adında bir bilim kurgu romanında, bir bilgisayar ağı üzerinden kendi kendini yayan bir programa verdiği isimden gelmektedir.

Bilgisayar solucanları dört grupta incelenebilir:

- E-posta solucanları
- IM solucanları
- İnternet solucanları
- Ağ solucanları

E-posta solucanları, kötücül yazılımların en çok tercih ettikleri yayılma yöntemi olan e-postaları kullanmaktadır. Genellikle bir fotoğraf veya metin dosyası gibi tek bir eklenti içerecek şekilde gönderilen e-postalar içerinde bulunurlar. Kullanıcı eklentiyi çalıştırdığında solucan kendini başlatır ve konak makineye bulaşır. Solucanlar genellikle bulaştıkları makinede kullanıcının adres defterinden e-posta adreslerini toplar ve kendini bulduğu her bir adrese gönderir.

"İnternet Mesajlaşma" (IM, Internet Messaging) Microsoft'un MSN Messenger, AOL'nın AIM, IRC, ICQ, KaZaA gibi yaygın mesajlaşma hizmetleri ve ağ paylaşımları IM solucanlarının yayılması için kullanılırlar. Hedeflenen hizmeti kullanan tüm kullanıcılara, solucan bulaşmış bir dosya veya solucanın kendisinin yer aldığı bir web sitesine yönelen İnternet bağlantısı gönderirler. Bağlantıya tıklandığında solucan indirilir ve çalışır. Solucan kendini konak makineye kurar ve kullanıcının haberleşme listesindeki tüm kullanıcılara aynı türde mesajlar göndererek kendini yaymaya devam eder.

İnternet solucanları, sadece İnternet'e bağlı olan makinelere bulaşabilen solucanlardır. Bu tür solucanlar, İnternet üzerinde tarama yapar ve en son güvenlik güncellemelerini kurmamış olan, açık kapıları olan veya güvenlik duvarı olmayan korunmasız bilgisayarları bulmaya çalışırlar. Solucan böyle bir bilgisayar bulununca, kendini bu makineye kopyalar ve kendini kurar. W32/Blaster ve W32/Deloder bu tür solucanlara örnektir.

Bir başka ilginç solucan türü olan ağ solucanları, paylaşılan bir klasöre, isimlerini faydalı veya ilginç gözükebilecek bir uygulama veya dosya ismine dönüştürerek kendilerini kopyalarlar. Bu dosyaları çalıştıran kullanıcılar kendi bilgisayarlarına solucanı bulaştırmış olur.

3.1.3. Truva atları (Trojan horses)

Yunan antik şairlerinden Homeros'un yazmış olduğu, Odise adlı eserde: Yunanlıların Truva şehrini on sene boyunca kuşatmalarına rağmen şehri ele geçiremedikleri; bunun üzerine içine bir kaç askerin saklandığı dev boyda bir atı (Resim 3.1) hediye olarak kalenin içine sokmayı başardıkları ve gece geç vakitte at içinde saklanan askerlerin kalenin kapılarını içerden açarak şehrin ele geçirilmesini sağladıkları yazılmaktadır.

Resim 3.1. Çanakkale'de bulunan Truva atı

Tarihte bir çok örneği görülen bu kamuflaj hilesini kullanan kötücül yazılımlar, bu efsanenin ismi ile anılmaktadır. Truva atları meşru yazılım gibi gözüken kötücül yazılımlardır. Son zamanlarda tersi de geçerli olan örnekler bulunsa da Truva atları virüsler gibi kendi kendini çoğaltmayan yazılımlardır. Bir Truva atı faydalı bir

programa “bohçalanabileceği” (bundling) gibi; kullanıcıları, faydalı bir işleve sahip olduğunu ikna edip, bizzat kullanıcı tarafından çalıştırılmaları ile de etkinleştirilirler. Sisteme çeşitli şekillerde zarar veren genel Truva atları dışında, aşağıdaki türlerde Truva atları bulunmaktadır:

Truva arka kapıları (Trojan backdoor)

En yaygın ve tehlikeli Truva atı türüdür. Bulaştığı makinenin uzaktan kontrolünü sistem yöneticisinin farkına varmadan saldırgana veren araçlar içerir.

PSW Truva atları (PSW Trojan)

Kişisel bilgisayarda bulunan şifreleri çalmak için kullanılan Truva atlarıdır.

Truva tıklayıcılar (Trojan clickers)

İnternet tarayıcıların ayarlarını değiştirerek veya İnternet adresleri ile ilgili işletim sistemi dosyalarını değiştirerek hedef kullanıcının belirli bir siteye veya İnternet kaynağına yöneltmeyi sağlayan Truva atıdır. Bu tür Truva atları bir İnternet sitesinin ziyaretçi sayısını artırarak fark edilmesini sağlamak için veya ileride yapılacak olan bir saldırı için hedef bilgisayarın kullanılmasını sağlamak amacıyla kullanılmaktadırlar. Truva tıklayıcılar DoS (Hizmet Aksattırma) saldırıları için kullanılmaktadır.

Truva indiriciler (Trojan downloaders)

Bu tür Truva atları, hedef makineye yeni bir kötücül yazılım veya reklam yazılımı indirip ve kurmak için bir ara basamak oluşturur. İndirici, kullanıcının haberi olmadan yeni kötücül yazılımı indirip çalıştırır veya sistem açıldığında otomatik olarak başlatır. İndirilecek kötücül yazılımın adresi Truva atı içinde bulunmaktadır.

Truva damlalıkları (Trojan droppers)

Truva indiricileri gibi damlalıklar da başka bir kötücül yazılımın sisteme yerleşmesini sağlayan bir ara basamak vazifesi görür. Bu tür Truva atları içinde muziplik içeren bir dosyayı sadece sisteme yüklediğini hissettirerek programın sebep olduğu etkinliğin zararsız olduğunu düşündürür. Halbuki bu Truva atının asıl amacını yerine getiren diğer yükler için bir maskedir.

Truva vekilleri (Trojan proxies)

Bu Truva atları hedef makinenin İnternet erişimini bir vekil sunucu (Proxy server) gibi saldırganın hizmetine açar. Mesaj sağanağı oluşturmak isteyen kötü niyetli kişiler bu tür yoğun mesajlaşma için hedef bilgisayarın kaynaklarını kullanmaktadır.

Truva casusları (Trojan spies)

Tuş basımları, ekran görüntüleri, etkin uygulama kayıtları ve diğer kullanıcı faaliyetlerini toplayan ve bu bilgileri saldırgana gönderen Truva atlarıdır.

Truva bildiriciler (Trojan notifiers)

Saldırgana Truva atının bulaştığını bildiren yapılardır. Hedef bilgisayara ait IP adresi, açık kapı numaraları ve e-posta adresleri gibi bilgiler e-posta, ICQ v.s. ile veya saldırganın web sitesine gönderilir.

Arşiv bombaları (ArcBombs)

Bu tür Truva atları sıkıştırılmış arşiv dosyalarını açan programları sabote etmek için kodlanmış arşiv dosyalarıdır. Çalıştırıldığında hedef bilgisayar yavaşlar ve çöker veya disk ilgisiz verilerle doldurulur. Gelen verilerin otomatik olarak işlendiği sunucular için bu tür Truva atları çok tehlikeli olabilir. Arşiv dosyasında hatalı başlık bilgisi oluşturarak; arşiv içindeki verileri tekrar ederek ve aynı dosyaların arşivlenmesi ile bu tür Truva atları oluşturulmaktadır. Tekrar eden verilerden oluşan

büyük bir dosya çok küçük bir arşiv dosyası olarak paketlenebilir. Örneğin 5 giga baytlık bir veri RAR biçiminde 200 kilo bayta (ZIP biçiminde 408 kilo bayt) kadar sıkıştırılabilir. Yine 10100 adet eş dosya RAR biçiminde 20 kilo bayta (ZIP biçiminde 230 kilo bayta) kadar sıkıştırılabilir.

3.1.4. Casus yazılımlar (spyware)

Kullanıcılara ait önemli bilgilerin ve kullanıcının yaptığı işlemlerin, kullanıcının bilgisi olmadan toplanmasını ve bu bilgilerin kötü niyetli kişilere gönderilmesini sağlayan yazılımlardır. Bazı kaynaklarda dar manada "snoopware" (burun sokan yazılım) olarak da adlandırılan casus yazılımlar, ileriki kısımlarda ayrıntılı olarak incelenecektir.

3.1.5. Arka kapılar (backdoor)

Bilgisayar üzerinde sıradan incelemelerle bulunamayacak şekilde, normal kimlik kanıtlama süreçlerini atlamayı veya kurulan bu yapıdan haberdar olan kişiye o bilgisayara uzaktan erişmeyi sağlayan yöntemler, arka kapı olarak adlandırılmaktadır. Arka kapılar Bölüm 2.3.6'da açıklanmıştır.

3.1.6. Klavye dinleme sistemleri (keyloggers)

Ortaya çıkan ilk türleri açısından ve en temel işlevi bakımından, kullanıcının klavye kullanarak girdiği bilgileri yakalayıp, tutan ve bunları saldırgana gönderen casus yazılımlardır. Klavye dinleme sistemleri, "keycatcher" (tuş yakalayıcı) ve "screen scraper" (ekran kazıyıcı) olarak da adlandırılmaktadır. Tezin ana konusu olan klavye dinleme sistemleri Bölüm 5'de tüm ayrıntıları ile incelenecektir.

3.1.7. Tarayıcı soyma (browser hijacking)

URL enjeksiyonu (URL injection) olarak da adlandırılan tarayıcı soyma, İnternet tarayıcı ayarlarını her zaman veya sadece belirli bölgeler için, kullanıcının belirlediği tarzın dışında davranmasına yol açan yazılımlardır. Bu, en basit olarak, tarayıcı

açıldığında gösterilen başlangıç sayfasını (home page) istenilen sitenin adresi yapmak olabilir. Bunun dışında uygunsuz içerik veya reklam içeren çıkıveren pencereler gösteren tarayıcı soyma türleri de bulunmaktadır.

3.1.8. Telefon çeviriciler (dialers)

Telefon çeviriciler, kurbanlarına büyük miktarlarda telefon ücreti ödetmek amacıyla, genellikle milletler arası uzak mesafe telefon numaralarını, hedef bilgisayar modeminin İnternet servis sağlayıcısının bağlantı numarası ile değiştirirler. Her zamanki gibi İnternet'e bağlanan kişi aslında farklı bir hattı kullandığının farkına vardığında çok büyük miktarlarda telefon faturası ile karşılaşabilirler. Bazı telefon çeviriciler ise, tuş basım bilgilerini ve şifre gibi önemli bilgileri, kullanıcı belli bir süre aktif olmadığı bir anda, korsana telefon hattı kullanarak gönderirler.

3.1.9. Kök kullanıcı takımları (rootkit)

UNIX işletim sistemlerinde yönetici anlamına gelen "root" isminden gelen kök kullanıcı takımları, saldırganın bir sistemin kontrolünü ele geçirdikten sonra, bilgisayar sistemine eklenen yazılımlardır. Takımda yer alan araçlar arasında, kayıt (log) girdilerini silerek veya saldırgan proseslerini gizleyerek saldırının izlerini gizleyen araçlar ve saldırganın sisteme daha sonraki girişlerini kolaylaştıracak arka kapıları düzenleyen araçları sayabiliriz. Kök kullanıcı takımları, işletim sistemine çekirdek (kernel) seviyesinde çengel (hook) attıklarından, fark edilmeleri oldukça güçtür.

3.1.10. Korunmasızlık sömürücüleri (exploit)

Belirli bir güvenlik korunmasızlığını hedef alan türde saldırılar üretebilen kötücül yazılımlardır. Bu tür yazılımlar sadece bu korunmasızlığın varlığını bütün dünyaya göstermek amacıyla yazıldığı gibi; ağ solucanları gibi zararlı programların bulaşma yöntemi olarak da kullanılabilirler.

3.1.11. Tavşanlar (wabbit)

Virüs ve solucanlar dışında daha az yaygın olan “tavşanlar”, kendi kendine çoğalan diğer bit tür kötücül yazılım türüdür. Virüsler gibi konak program veya belgelerine bulaşmazlar ve solucanlar gibi diğer bilgisayarlara yayılmak için ağ yeteneklerini kullanmazlar. UNIX komutu “fork” ile çok miktarda proses üreten “fork bombası” en basit wabbit örneğidir. İngilizce önerilen isim, “Buggs Bunny” çizgi filminde, Elmur Fudd adındaki tavşanı avlamaya çalışan çizgi roman kahramanının, “rabbit” (tavşan)’ı söyleme şeklinden gelmektedir. Doğada bulunan tavşanlar gibi, bu kötücül yazılımlar da hızlı bir şekilde çoğalma yeteneğine sahiptir.

3.1.12. Diğer kötücül yazılımlar

Yukarıda açıklanan kötücül yazılımlar dışında bir çok çeşit kötücül yazılım türü bulunmaktadır. Yeni yeni kötücül yazılımlar, teknolojinin getirdiği yenilikleri takip ederek ortaya çıkmakta veya şekil değiştirmektedir. Uzun süre güvenilir olarak adlandırılan bir çok ortamın, bitmek tükenmek bilmeyen güdülerle hareket eden bilgisayar korsanlarının cirit attığı alanlar haline dönüşmesi, çok kısa bir süre almaktadır. Örneğin, ilk olarak Haziran 2004’de ortaya çıkan, EPOC.cabir ve Symbian/Cabir olarak da adlandırılan “Cabir” isimli bir bluetooth solucanı, Symbian OS işletim sisteminin bulunduğu cep telefonlarında da saldırı yapılabileceğini gösterdiğinden, cep telefonlarında da bilgi güvenliğine yönelik çalışmaların yapılması gerektiğini ortaya çıkarmıştır (31).

Diğer kötücül yazılımlar arasında, reklam yazılım (adware), parazit yazılım (parasiteware), hırsız yazılım (thiefware), püsküllü bela yazılım (pestware), web böcekleri (web bugs), ciltçi (binder), tarayıcı yardımcı nesnesi (browser helper object (BHO)), uzaktan yönetim aracı (remote administration tool, RAT), ticari RAT (commercial RAT), bot ağı (botnet), ağ taşkını (flooder), aldatmaca (hoax), saldırgan ActiveX kontrolleri (hostile ActiveX), saldırgan Java (hostile Java), saldırgan betik (hostile script), IRC (ele geçirme) savaşı (IRC (takeover) war), anahtar üreticiler (key generator), e-posta bombardımanı (mail bomber), kitle postacısı (mass mailer), nuker

(nuke: nükleer silah), paketleyici (packer), şifre yakalayıcılar (password capture) - şifre soyguncular (password hijacker), şifre kırıcılar (password cracker), telefon kırma (phreaking, phone breaking), kapı tarayıcılar (port scanner), sondaj aracı (probe tool), arama motoru soyguncusu (search hijacker), koklayıcı (sniffer), kandırıcı (spoofer), casus yazılım çerezleri (spyware cookie), iz sürme çerezleri (tracking cookie), turta (PIE), damlatıcı (trickler) ve savaş telefon çeviricilerini (war dialer) saymak mümkündür. Bu yazılım türler hakkında özet bilgiler aşağıda verilmiştir:

1. Reklam yazılım (adware)

Kötücül yazılım olması şart değildir fakat bir bedava veya paylaşımlı yazılımdan (freeware, shareware) beklenebilecek reklam anlayışının ötesinde yöntemler kullanırlar. Normalde yazılımlarda kullanılan reklamların, programlama maliyetini karşılamaya; kullanıcılara daha düşük fiyat sunmaya ve programcılara yeni uygulamalar geliştirmesi ve yaptıkları uygulamaları idame etme ve güncellemesi için cesaret vermeye yönelik yararlı yönleri bulunmaktadır. Bu tür programlar reklamlarını, çıkıveren pencerelerde (pop-up windows) veya ekranda bir şeritte (banner) yer alacak şekilde yapmaktadır. Kötücül yazılım olarak nitelendirilen reklam yazılımlar ise, kullanıcıya reklam yazılım ile beraber sunulan asıl programı çalıştırmasa da devrede olan programlardır. Bölüm 4.2'de reklam yazılımlar ve sistemlere bulaşma teknikleri ile ilgili ayrıntılı bilgiler verilmektedir.

2. Parazit yazılım (parasiteware)

Parazit yazılım, üyelik (affiliate) yöntemi ile gelir elde eden sitelerdeki iz sürme bağlantılarını silen reklam yazılımı türüdür. Bu davranış, üyelikle elde edilecek komisyon ve kredilerini yanılttığından, "parazit" olarak nitelendirilmektedir. Kullanıcı açısından bakıldığında parazit yazılımlar, önemli bir güvenlik tehdidi olarak görülmez.

3. Hırsız yazılım (thiefware)

İz sürme çerezlerinin üstüne yazarak veya İnternet tarayıcılarında o anki trafiği, yeni tarayıcı pencereleri açarak farklı sitelere de yönlendiren ve bu şekilde üyelik komisyonlarını çalan uygulamalardır.

4. Püsküllü bela yazılım (pestware)

Reklam yazılım türünde bir kötücül yazılımdır. Çoğunlukla iki yüzlü üreticiler tarafından, kullanışlı bir program olarak sunulan ve kurulması önerilen yazılımlardır. Sisteme büyük zararlar vermeyen bu tür programlar, bilgisayar kullanımı sırasında verdikleri rahatsızlıklarla "püsküllü bela" olarak adlandırılabilecek, can sıkıcı bir hal alabilirler. Normalde bütün yazılım üreticileri, kurulan ürünü daha fazla kullanmak istemeyen kişilerin, programı sistemlerinden çıkartabilmeleri için bir program kaldırıcıyı (uninstaller) program menülerine ve/veya "Program Ekle/Kaldır" bölümüne eklerler. İşte püsküllü bela yazılımın en tipik belirtisi, programı diğer sıradan programlarda olduğu gibi otomatik olarak bilgisayardan kaldıracak bir yöntemin kasten sunulmamasıdır.

Püsküllü bela yazılımlar müşteri çekmek amacıyla, sistemde yer işgal eden işe yaramayan artık dosyaları kolayca veya otomatik olarak temizleme, sistemin güvenliğini artırma, sistemin bilgi işleme gücünün etkinliğini geliştirme, eğlenceli oyunlar, çok özellikli İnternet tarayıcı, daha ilginç fare işaretçi imgeleri ve ekran koruyucuları ve daha iyi arama motoru sunma vaadinde bulunmaktadırlar. Bir dereceye kadar vaatlerini yerine getirseler de; bu işe kendini adayan profesyonel programların daha ilerisine gidemeyen bu programların asıl amaçları, masaüstünüzde çeşitli şekillerde reklamlar çıkartabilmektir. Belki bu reklamların bir zararı olmayacağı düşünülse de bu yazılımların CPU, bellek ve bant genişliği gibi sistem kaynaklarını hoyratça kullandığı veya kullanım sırasında anormal sıkıntılarla günlük çalışma verimliliğini düşürdüğü bir gerçektir.

5. Web böcekleri (web bugs)

İz sürme böceği (tracking bug), piksel etiketi (pixel tag), web feneri (web beacon) veya temiz gif (clear gif) olarak da bilinen web böceği, HTML tabanlı bir e-posta mesajını veya bir web sayfasını kimlerin, kaç kez görüntülediği ve mesajla ne kadar süre ilgilendiği gibi bilgileri elde etmek amacıyla kullanılan ilginç ve sıradan kullanıcı tarafından pek bilinmeyen bir tekniktir. Web böceği, saydam veya artalan renginde ve genelde 1 x 1 piksel boyutunda küçük bir resimdir. Bu resim, mesajın içine gömülmediğinden, e-posta programının mesaj penceresinde gösterilebilmesi için harici bir adresten indirilmektedir. Resmin dosya olarak bulunduğu bu bağlantının hareketlerinin kaydını tutan web sunucusu, mesajı okuyan kişinin IP adresini, resmin gösterilme süresini ve buna benzer bir çok bilgiyi elde edebilmektedir. Bu tür bir mesajı açan kişi, en azından kendi e-posta adresinin geçerli ve kullanılan bir adres olduğunu karşı tarafa ifşa etmektedir. Bu şekilde ileride bir çok mesaj aynı e-posta adresine gönderilebilir.

6. Ciltçi (binder)

Dosya yönetimi açısından "binder", Microsoft'un ciltçi yazılımı gibi, türleri farklı da olabilecek birden fazla dosyayı tek bir dosya haline getiren yazılımlardır. Fakat ne yazık ki bu tip dosyaların içine Truva atları gibi kötücül yazılımların da paketlenmesi mümkündür. Bu yüzden Microsoft dahil bir çok yazılım üreticisi bu tip yazılımları üretmeyi bırakmışlardır (32).

7. Tarayıcı Yardımcı Nesnesi (Browser Helper Object (BHO))

İnternet Gezgini (Internet Explorer) her açıldığında otomatik olarak çalışan küçük programlar olarak üretilen BHO, genel olarak tarayıcıya diğer yazılım programları tarafından yerleştirilir ve tipik olarak araç çubuğu donatıları tarafından kurulur. Kötücül amaçlarla yazılmış bir BHO nesnesi İnternet tarayıcısına kurularak o kullanıcıya ait İnternet'de erişilen her bilgiyi toplayabilir ve kullanım verilerini gizlice izleyebilir.

8. Uzaktan Yönetim Aracı, RAT (Remote Administration Tool)

Saldırgana, hedef makine çevrim içi olduğu zaman bu makineye sınırsız erişim hakkı veren en tehlikeli kötücül yazılımlardan biridir. Saldırgan, bu araçları kullanarak dosya aktarımı, dosya ve programların eklenme ve silme işlemleri ve fare ve klavyeyi kontrol altına alma gibi işlemleri kolaylıkla yapabilir.

9. Ticari RAT (commercial RAT)

Normalde uzaktan yönetim aracı olarak üretilen her hangi bir ticari RAT programının, kullanıcının izni veya bilgisi olmadan kötü amaçlarla kullanılmasıdır.

10. Bot Ağı (botnet)

"Bot" terimi, bilgisayar teknik dilinde, özerk olarak çalışan ve bir kullanıcı veya program için, bir insan faaliyetini benzetmeye çalışan "yazılım robotlarının" yerine kullanılmaktadır. Örneğin, bir çok arama motorunun İnternet üzerindeki sayfaları ortaya çıkarmak amacıyla kullandığı ve web sayfalarını inceleyip sayfanın içerdiği bağlantılara yönelip diğer sayfaları tarayan örümcekler (spider) ve tırtıllar (crawler), en yaygın bot'lar arasındadır. Uzaktan yönetim yazılım türü olan bot ağı (botnet), kötü niyetli kişiler tarafından mesaj sağanağı (spam) göndermek, izinsiz daha fazla casus yazılım kurmak gibi kötü amaçlara yönelik kontrol altına aldıkları, bilgisayar solucanları ve Truva atları gibi kötücül yazılımların çalıştırıldığı, ele geçirilmiş bilgisayarlardan oluşmaktadır.

11. Ağ taşkını (flooder)

DoS saldırılarına sebep olacak şekilde, seri PING (Packet Internet Groper, Paket İnternet Yoklayıcı) göndermek gibi yöntemlerle, bir ağ bağlantısına kasten aşırı yük bindiren yazılımlardır.

12. Aldatmaca (hoax)

Kullanıcıları, olmayan bir şeyin varlığına ikna etmeyi amaçlayan her türlü "numara", aldatmaca olarak sınıflandırılmaktadır. Aldatmacanın en yaygın biçimde gerçekleşen türü, aslında olmayan bir virüs hakkında insanları uyaran mesaj sağanaklarıdır. Bunun dışında inanılması zor hayali olaylar, dini veya insani konular içeren çeşitli aldatmaca mesajları sık sık kullanıcılara iletilmektedir. Bu mesajın aldatmaca olduğunun farkına varamayan kişiler, mesajı yardımcı olmak amacıyla başka kişilere de ileterek, aldatmacanın daha da fazla yayılmasına alet olurlar. Bu tip aldatmacalar, gereksiz İnternet trafiğine ve zaman kaybına yol açmaktadır. Bunun dışında örneğin önemli bir işletim sistemi dosyasını, zararlı bir dosya gibi gösteren aldatmacaya inanan kişi, belirtilen dosyayı silerse sistemin tamamen çalışmamasına neden olabilmektedir. Bu yüzden, aldatmaca türünde mesajları hiç dikkate almamak yerinde bir davranış olacaktır.

13. Saldırgan ActiveX kontrolleri (hostile ActiveX)

Genellikle indirilerek kurulan sürücülerle (drive-by-download) İnternet Gezginine kurulan yazılımlardır. Bu uygulama bir kez kurulunca, bilgisayar üzerinde normal bir program gibi, genelde kullanıcıdan gizli olarak çalışabilir ya da diğer kötücül yazılımları indirip, kurabilir.

14. Saldırgan Java (hostile Java)

İnternet tarayıcıları, Java programını sarmalayan (encapsulate) ve yerel makineye erişimi önleyen bir "sanal makineye" (virtual machine) sahiptir. Bir Java küçük uygulamasının (applet) arkasında yatan teori; çalıştırılan uygulamanın, büsbütün bir uygulama olmasından ziyade, tıpkı ekran üzerinde gösterilen yazı ve şekiller gibi bir içerik sunacak şekilde çalışmasıdır. 2000 yılında, bilinen bütün tarayıcıların, bu "kum torbalarını" (sandbox) aşacak açıklara sahip olduğu anlaşıldı. Bir çok güvenlik uzmanı bu durumda, ya Java seçeneğini etkisiz kılmayı ya da daha ileri kum torbaları ve sanal makinelerle küçük uygulamaları sarmalamayı önermektedir.

15. Saldırgan betik (hostile script)

.VBS, .WSH, .JS, .HTA, JSE ve .VBE uzantılı metin dosyalarından oluşan ve Microsoft WScript veya Microsoft Betikleme Konak Uygulaması (Microsoft Scripting Host Application) tarafından yürütülen metin dosyaları, istenmeyen faaliyetleri icra etmek amacıyla kullanılabilmektedir. Bu tür betikler, içerdikleri kötücül niyet açısından saldırgan betik olarak adlandırılmaktadır.

16. IRC (ele geçirme) savaşı (IRC (takeover) war)

IRC savaşları uzun süre IRC şebekesini rahatsız etmiştir. İki sunucu bir birleri arasındaki bağlantıyı kaybedince, her iki tarafta kısaca "op" olarak adlandırılan ve o kanalı idare eden kanal operatörlerinin sahip oldukları konumlar korunmalıdır. Eğer oluşan kopma sırasında sunucuların herhangi birinde bir kullanıcı bulunmuyorsa; kanala o sırada tekrar katılan insanlar, kanal operatörü konumunu kazanabilirler. Sunucular daha sonra birleşince de asıl operatörler kanaldan "tekmelenebilir" ("kick out"). Bu, daha ileri saldırılar için iyi bir zemin sağlayabilir. Verilen bu örnek dışında, IRC üzerinden yapılan her türlü saldırıyı kolaylaştırmak amacıyla kullanılan tüm araçlar, IRC savaşı olarak sınıflandırılmaktadır.

17. Anahtar üreticiler (key generator)

Yazılımların yasal olmayan yollarla kopyalanmasını önleyerek, lisanslı yazılım kullanıma sevk etmek amacıyla oluşturulan anahtar (yazılım lisans numarası) tabanlı yazılım korumalarını, meşru anahtarlar üreterek kıran araçlardır. Bu araçları kullanan kişiler, yazılımı satın almadan kopyalayıp kurdukları programlardan, yetkili kullanıcı gibi faydalanabilirler.

18. E-posta bombardımanı (mail bomber)

Hedef kişinin e-posta gelen kutusunu, binlerce e-posta ile bombardıman eden kötücül yazılımlardır. Gönderilen e-postalardan, gönderen kaynağın bilgisini elde etmek mümkün değildir.

19. Kitle postacısı (mass mailer)

E-posta yolu ile virüs gönderen kötücül yazılımlardır. 1987'de yaşanan ilk CHRISTMA EXEC solucanı ve 1999 yaşanan Melissa virüsü, bu tür yazılımlarla üretilmiştir.

20. Nuker (nuke: nükleer silah)

Uygun şekilde yamalanmamış veya güvenlik duvarı olmayan Windows işletim sistemli makinelere yapılan WinNuke DoS saldırısı için kullanılan "nuke" terimi, şu an için çeşitli TCP/IP DoS saldırılarının genel adı olarak da kullanılmaktadır. Ticari yazılımların yasal olmayan biçimde dağıtıldığı "warez" adı verilen bilgisayar dünyasında "Nuker", warez grubunun kurallara uymasını denetleyen kişilere verilen addır.

21. Paketleyici (packer)

Bir prosesin içine bir dosyayı şifreleyerek sıkıştıran yardımcı programlardır. Program çalıştırıldığında, bellekteki dosyayı kendiliğinden açan bir başlığı prosese ekler. Paketleyiciler Truva atı geliştiricileri tarafından, çalışmalarının virüs korunma ürünleri tarafından saptanmasını önlemek için kullanılmaktadır.

22. Şifre yakalayıcılar (password capture), şifre soyguncular (password hijacker)

Sistemde girilen şifreleri yakalayıp kaydetmeye yönelik casus programlardır.

23. Şifre kırıcılar (password cracker)

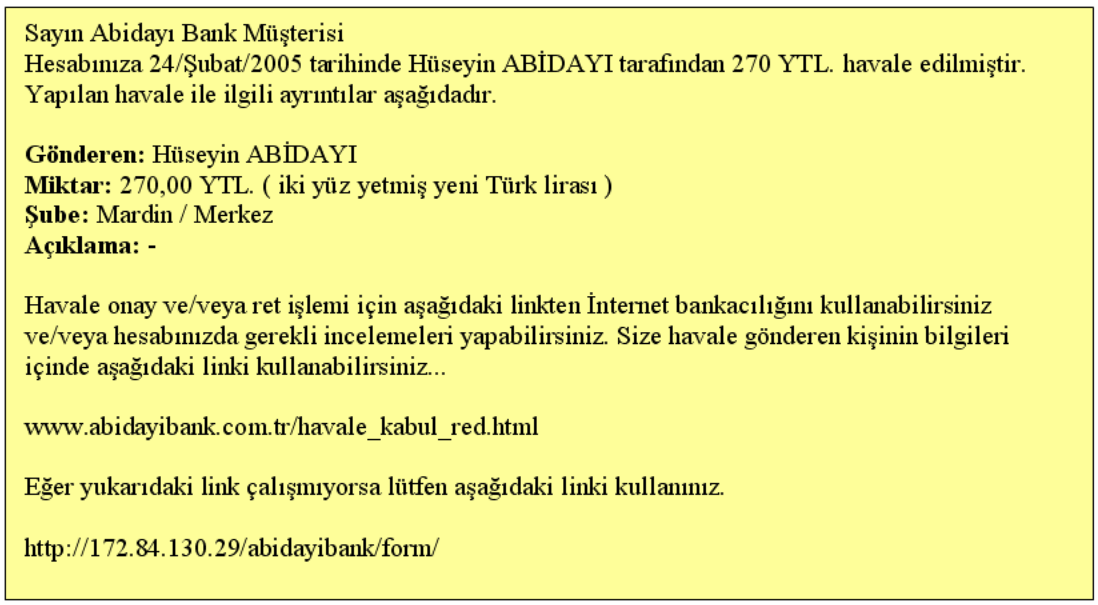
Kaba kuvvet ve sözlük tabanlı deneme yanılma yöntemlerini de içeren; bir şifreyi veya şifreli bir dosyanın şifresini çözen araçlardır. Şifre kırıcılar, güvenlik yöneticileri tarafından meşru bir biçimde, kullanıcılar tarafından tanımlanmış olan zayıf şifrelerin bulunması ve bu şifrelerin değiştirilmesinin, daha güvenilir bir sistem oluşturmak için, kullanıcıdan talep edilmesi için de kullanılabilmektedir.

24. Sazan avlama (phishing)

Bu tez çalışmasında, dilimizde kullanılmak amacıyla "sazan avlama" olarak bir karşılık önerilen phishing, kimlik hırsızlığı ("identity theft") adı verilen banka hesap numaraları, kredi kartı numaraları v.s. gibi kişisel bilgilerin, banka gibi resmi bir kurumdan gerçekten gönderilen resmi bir mesaj gibi gözüken e-postalarla kişilerden elde edilmesidir. Sosyal mühendisliğin bir uygulama alanı olan bu tür sahte e-postalarını alan kişi, istenilen gizli bilgileri göndererek, bu bilgilerin kötü niyetli üçüncü şahısların eline geçmesine ve akabinde oluşabilecek zararlara maruz kalınmasına neden olacaktır (33). Phishing için İngilizce "password harvesting fishing"in (şifre toplama avcılığının) bir kısaltması olduğu ya da 1980'de ilk kez psikolojik teknikler kullanarak kredi kartı bilgilerini elde eden Brien Phish'e bir atıf olduğu söylenmektedir.

Aşağıda Şekil 3.2'de bir örneği gösterilen e-posta'ya benzer bir çok mesaj, bugünlerde ülkemizde de insanlara gönderilmektedir. Örnek e-posta'da, (varolan hiç bir bankayı ima etmemek adına burada "Abidayı" olarak isimlendirilen) bir bankadan gelen mesajda, gönderilen kişinin hesabına bir para havalesinin yapıldığı müjdeleniyor! Kurbandan bu havaleyi kabul edip etmediğini, bankanın resmi İnternet adresinden girerek doğrulaması isteniyor. Bunun için verilen adres ise (www.abidayibank.com.tr/havale_kabul_red.html) gerçekte bankanın resmi İnternet sitesinde var olmayan bir sayfayı işaret ettiğinden, mesajda ek olarak verilen ve bahse konu bankanın sunucusunun değil de sazan avlamaya çıkan kötü niyetli kişinin sunucunun bulunduğu adres verilmektedir. Bu adres, bölge adı şeklinde değil de IP numarası (http://172.84.130.29) şeklinde, rakamlarla veriliyor. Burayı bankanın resmi bir adresi olarak algılayıp belirtilen adrese giden kişi, hesap bilgileri ve şifrelerini, korsanın daha önce hazırladığı sahte banka sayfasından, korsana bizzat kendi elleriyle verebiliyor. Mesajın, sazan avlama amacıyla kullanıldığını gösteren bu bilgiler dışında, aslında mesajın kendisi biraz dikkatlice incelendiğinde, mesajın kötü bir amaç için hazırlandığını gösteren bir çok husus göze çarpmaktadır. Öncelikle kullanılan dil, profesyonel bir bankanın resmi üslubunun dışındadır. Dilbilgisi ve noktalama hataları vardır. Ve en önemlisi, mesajın gönderildiği kişinin

tam adı yerine "Sayın Abidayı Bank Müşterisi" şeklinde genel bir ifade kullanılmaktadır.



Sayın Abidayı Bank Müşterisi
Hesabınıza 24/Şubat/2005 tarihinde Hüseyin ABİDAYI tarafından 270 YTL. havale edilmiştir.
Yapılan havale ile ilgili ayrıntılar aşağıdadır.

Gönderen: Hüseyin ABİDAYI
Miktar: 270,00 YTL. (iki yüz yetmiş yeni Türk lirası)
Şube: Mardin / Merkez
Açıklama: -

Havale onay ve/veya ret işlemi için aşağıdaki linkten İnternet bankacılığını kullanabilirsiniz ve/veya hesabınızda gerekli incelemeleri yapabilirsiniz. Size havale gönderen kişinin bilgileri içinde aşağıdaki linki kullanabilirsiniz...

www.abidayibank.com.tr/havale_kabul_red.html

Eğer yukarıdaki link çalışmıyorsa lütfen aşağıdaki linki kullanınız.

http://172.84.130.29/abidayibank/form/

Şekil 3.2. Örnek bir sazan avlama e-postası (34)

Bu tür e-postalara karşı kullanıcılar bilinçli ve uyanık olmalıdır. Sazan avlamak isteyen kişilerin attıkları oltaya yem olunmalı ve hiç bir şekilde kişisel bilgileri bu yolla isteyen mesajların söyledikleri yapılmamalıdır. Sazan avlamaya yönelik e-postalar, ilgili bankalara gönderilerek bankaların gerekli tedbirleri alması ve diğer müşterilerini bilinçlendirmesi sağlanmalıdır.

25. Telefon kırma (phreaking, phone breaking)

Telefon dinleme, bedava telefon görüşmesi yapma amacıyla veya telefon şebeke ve santrallerine saldırı yapmak amacıyla, ses kartı ve modem kartı gibi donanımları kullanılan araçlara verilen addır.

26. Kapı tarayıcılar (port scanner)

Herhangi birinin bir kapıyı dinleyip dinlemediğini görmek amacı ile bir makine üzerinde tanımlı olan 65 536 adet kapının hepsini otomatik olarak sınayan araçlardır.

27. Sondaj aracı (probe tool)

Olası korunmasızlıkları aramak amacıyla başka bir sistemi araştıran araçlardır. Sondaj araçları, güvenlik durumlarını desteklemek isteyen güvenlik yöneticileri tarafından meşru bir biçimde kullanılabileceği gibi; bir sisteme ne tür bir saldırı yapılabileceğini araştırmak isteyen saldırganlar tarafından da kötü amaçlarla kullanılabilir. Bu tür araçlara örnek olarak NT Güvenlik Tarayıcı (NT Security Scanner) verilebilir.

28. Arama motoru soyguncusu (search hijacker)

İnternet tarayıcıların varsayılan olarak ayarlı olan arama motoru ayarlarını değiştirmek amacıyla hazırlanan kötücül yazılımlardır. Bu şekilde arama yapmak isteyen kullanıcının sorguları veya olmayan veyahut yanlış girilen bir adres sonucu açılacak varsayılan arama sayfası, başka bir siteye yönlendirilmektedir.

29. Koklayıcı (sniffer)

Bir ağ üzerindeki IP paketlerini "koklamak" için kullanılan donanım ve yazılımlar, koklayıcı olarak adlandırılmaktadır. Koklayıcı yazılım veya donanım, bütün paketleri dinleyen ayrımsız kipe (promiscuous mod) geçerek bütün ağ trafiğini dinler ve kaydeder. Bu paketler içinde yer alan şifre bilgileri gibi önemli bilgiler, paket içeriği taranarak elde edilebilir. Ağ üzerinde kullanılan aktif ağ cihazları (hub), paketleri sadece ulaşılması istenen adrese yönlendirerek, koklayıcıların paketleri elde etmesinin önüne geçebilmektedir.

30. Kandırıcı (spoofer)

Kandırıcılar, saldırganın IP adreslerinin sahtelerini üretmek (IP kandırma, IP spoofing) amacıyla kullanılır. Şirinler (Smurf, çizgi film) ve Fraggle (Muppet şov'daki yaratıklara verilen ad) saldırıları, bugünlerde kullanılan kandırma saldırılarının en başında gelenleridir. Saldırılmak istenen hedef makinenin adresi, paketi gönderen adres olarak yazıldığı bir sahte paketin, bir yayın (broadcast)

adresine gönderilmesi ile bu saldırılar başlatılır. Yayın bölgesinde var olan bütün makineler hedef makineye cevap paketlerini gönderir. Bu da hedef makinenin İnternet bağlantısına aşırı yük bindirir.

31. Casus yazılım çerezleri (spyware cookie)

Sitelerin İnternet üzerinde daha kullanışlı bir hizmet vermek amacıyla kullandıkları çerezler, kötü amaçlara da hizmet verebilmektedir. Kişisel kullanıcı bilgilerinin elde edilmesi ve paylaşılması amacıyla bu çerezler kullanılabilmektedir.

32. İz sürme çerezleri (tracking cookie)

Bir kullanıcının İnternet üzerinde gezinme geçmişini izlemek amacıyla iki veya daha fazla web sayfasında paylaşılan çerezler iz sürme çerezleri olarak adlandırılmaktadır.

33. Turta (PIE)

PIE (Persistent Identification Element, İnatçı Kimlik Elamanı) olarak adlandırılan yapılar, bir çok tarayıcı ve casus savar yazılımların iz sürme çerezlerini engellemeleri sonucunda ortaya çıkan arayışın son örneklerinden biridir. Hali hazırda kullanılan bu yöntemlerin başında, Macromedia Flash MX uygulamasının yerel paylaşılan nesneleri (local shared objects) gelmektedir. Flash canlandırmaları son zamanlarda web sayfalarında oldukça yaygın bir şekilde kullanılmaktadır. Bu tür canlandırmaları oynatabilen programlar arasında Macromedia Flash Player, Mart 2005'e göre % 98 ile birinci sırada bulunmaktadır (35). Flash biçeminde bir reklam içeren bir web sayfası, bir çerez gibi işlev gören SOL uzantılı bir dosyayı genellikle \Documents and Settings\{kullanıcı_adı}\Application Data\Macromedia\Flash Player\ klasöründe alt klasörlerin altında tutmaktadır. İşte bu dosyalar kullanılarak kullanıcıların İnternet'te gezinme alışkanlıkları rahatlıkla izlenebilmektedir.

34. Damlatıcı (trickler)

Otomatik yazılım indirme tekniklerini kullanan bu casus yazılım, arka planda gizli ve çok yavaş bir şekilde (damla damla) bir yazılımın, hedef bilgisayara indirilmesini ve indirilen bu yazılımın kullanıcının haberi olmadan kurulmasını sağlar. Damlatıcılar, bir casus yazılımın bilgisayara sessizce kurulumuna olanak sağladığı gibi; kullanıcı o casus yazılıma ait bazı bileşenleri, casus savar yazılımlar kullanarak veya bizzat silerek kaldırdığında, eksik öğeleri tekrar indirerek casus yazılımın bilgisayardaki ikametini sürdürmesine de yol açması açısından tehlikeli yapılardır.

35. Savaş telefon çeviricileri (war dialer)

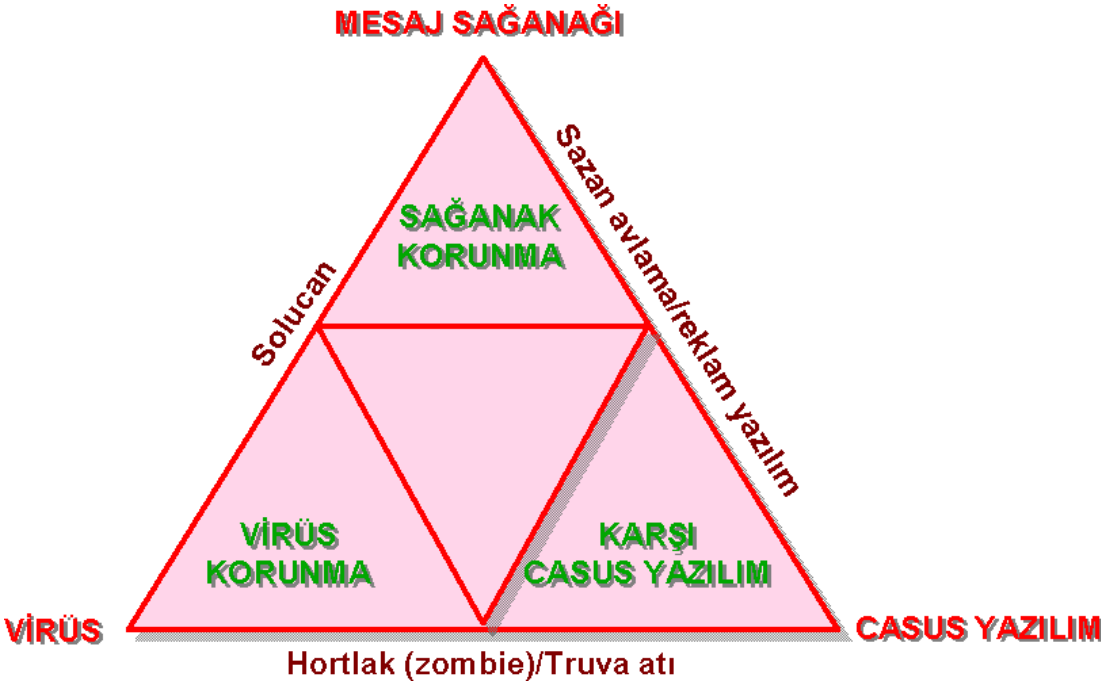
Hayalet program telefon çevirme (demon-dialing) ve taşıyıcı tarama (carrier-scanning) olarak da adlandırılan savaş telefon çeviricileri, 1983'de yapılan "Savaş Oyunları" (War Games) filmi ile popülerlik kazanmıştır. Bir aralıktaki telefon numaraları çevrilir ve çağrıyı otomatik olarak cevaplayan bir makine aranır. Bir çok kuruluşun bu tür çağrıları cevaplaması için kullandığı modem takılı makineleri bulunmaktadır. Bu makinelere yapılacak saldırılar bu araçlarla saptanmaktadır.

3.2. Kötücül Yazılım ve Önlemlere İlişkin Ana Unsurlar

Kötücül yazılımların kesin sınırlarla sınıflandırılması günümüzde zorlaşmaktadır. Yukarıda bahsedilen birden fazla türde kötücül yazılım içeren melez yazılımlar bulunmaktadır. Kötücül yazılımların, İnternet üzerinden oluşturduğu üç ana tehdit bulunmaktadır (36). Şekil 3.3'de gösterildiği gibi bu tehditler: mesaj sağanağı (spam), virüsler ve casus yazılımlardır. Bu üç ana risk, ikili olarak birleşerek ikincil riskleri oluşturmaktadır:

- Sağanak + Virüsler = Solucanlar
- Sağanak + Casus Yazılımlar = Sazan avlama/Reklam yazılım
- Virüsler + Casus Yazılımlar = Hortlaklar (zombie)/ Truva atları

Her bir riske karşı oluşturulan önlemler: sağanak korunma (antispam), virüs korunma (antivirus) ve casus savar yazılım (antispyware) olarak düzenlenmektedir.



Şekil 3.3. Kötücül yazılım tehdit üçgeni

3.3. Casus Yazılımlar

Casus yazılımları daha doğru anlayabilmek için bu yazılımların nasıl ortaya çıktığını incelemekte fayda vardır. Bu kısımda casus yazılımların hangi zaman sürecinde ve ne şekilde ortaya çıktığı ve geliştiği incelenecektir.

İnternet'in ortaya çıkması ve HTTP protokolünün yaygınlaşması ile bir çok şirket "com" uzantılı siteler edindiler. Bu sitelerle dünyanın her köşesinden insanlara erişmek mümkün olmuştur. Zamanla bu sitelerden para kazanmanın en basit yolunun, gazete, dergi, radyo ve televizyon gibi diğer kitle iletişim araçlarında olduğu gibi reklam vererek yapılabileceği anlaşılmıştır. Reklamlar "banner" olarak adlandırılan ve genellikle hareketli GIF resimlerinden oluşan reklam şeritleri üzerinde web sitelerinde boy göstermeye başlamıştır. Çoğu İnternet kullanıcısı, bu reklam şeritlerine pek aldırmasa da; bir çok site bu reklamlarla yeni ziyaretçileri kendi sitelerine çekip, pazarladıkları ürünleri satabilmişlerdir. Bir çok web yöneticisi,

başka firmaların reklam şeritlerini hazırladıkları sitenin sayfalarında göstererek önemli gelirler elde ettiler. Sistem biraz daha düzeltilerek, yalnızca reklam şeridini göstermek ile kazanılan para azaltılırken; o reklamın gösterdiği etkiyi ölçebilecek tek eylem olan "şeride tıklama" ile reklam veren şirketin sitesine yönlendirilen kullanıcı başına, site sahibine daha fazla ödeme yapılmaya başlanmıştır. Tıklama başına ödeme ("pay-per-click") olarak adlandırılan bu yöntemle sayfalarında reklam gösteren site sahipleri, ne kadar çok İnternet kullanıcısı bu reklama tıklayıp, reklam verenin sitesine giderse, o kadar çok para kazanıyordu. İşte bu noktada vekil tıklama ("Proxy clicking") adı verilen programlar, bu sisteme el atıp; sanki her defasında farklı kullanıcı bu reklamlara tıklıyormuş gibi davranarak, reklam yöntemini kullanan denetleme yapılarını şaşırttılar. Bu programlar, bir çok İnternet reklam şirketinin zarar etmesine neden olmuştur. Reklamcıların elini kolunu bağlayan başka bir etken de reklam şeritlerini bloke ederek gösterilmemesine neden olan güvenlik duvarı yazılımlarının ortaya çıkmasıdır.

Reklam şirketleri ve İnternet üzerinden para kazanmak isteyen pazarlama şirketleri bunun üzerine, sadece anlaşmalı oldukları firmalara ait sitelere, reklam şeridine tıklayarak yönlendirilen müşteri adayları için değil; -daha büyük pay olarak- yönlendirilen müşterinin, gerçekte çevrim içi olarak sipariş verip satın aldığı alışverişlerden ödeme yapmayı sağlayan, üyelik (affiliate) programlarına başladılar. Bir diğer grup reklamcı ise reklam vermenin yeni, fakat iş ahlakına ters düşen yöntemlerinin peşine düştüler. Pazarlamasının yapılması istenen ürününün reklamını yapmak için her hangi bir web sitesine veya reklam olarak hizmet veren sunucuya ihtiyaç duymayacak bu yol, casus yazılımların doğmasına sebep olmuştur (37).

Beraberlerinde istenen reklamın açık bir şekilde gösterildiği reklam yazılımlarının (adware) boy göstermesine rağmen; casus yazılımlar, ilk olarak bedava ve paylaşılan yazılımlar içine bohçalandılar. Gitgide bu yazılımlar daha cüretkar davranarak daha büyük zararlar verme yoluna gittiler. İlk önceleri rahatsız eden çıkıveren pencereler ve programların işleyişini kesen mesajların yerini, İnternet üzerinde gezerken istenmeden açılan tarayıcı pencereleri ve kendi kendine değişen İnternet başlangıç sayfaları almıştır. Daha sonra, kişisel gizliliği çiğneyen casus yazılımlar ortaya

çıkmaya başlamıştır. Kullanıcının haberi olmadan, bir şekilde sisteme yerleşen casus yazılımlar, bir yandan kullanıcının İnternet üzerinde gezdiği sitelerin adreslerini sessizce kaydederek, gezinme alışkanlıklarını toplayıp, haksız rekabete yol açacak şekilde reklam stratejilerinin daha uygun olarak geliştirilmesini sağlarken; diğer yandan kullanıcıların İnternet üzerinden yaptıkları alışveriş veya çevrim içi bankacılık gibi işlemlerinde kullandıkları şifre ve özel bilgileri ele geçirip, casus yazılımı kullanan kötü niyetli kişilerin ellerine teslim ettiler. Böylece, işin boyutlarının ne kadar ciddi olduğu gözler önüne serilmiştir. Bazı yazılımlar daha da ileri gidip, telefon çeviriciler (dialer) olarak adlandırılan yazılımlarla, tecrübesiz kullanıcıların, bilgisayarlarını İnternet'e bağladıkları İnternet Servis Sağlayıcılarını (ISP, Internet Service Provider) daha pahalı ücret talep eden bir servis sağlayıcı ile değiştirerek veya milletler arası pornografik telefon hatlarını aratarak büyük meblağlarda telefon faturaları ödemelerine neden oldular.

Casus yazılımların sebep olduğu yıkım bu kadarla kalmamaktadır. Bu yazılımlar, sızdıkları sistemin dengesini de bozmaktadırlar. Normal programların özen gösterdiği bir çok programlama ilkesi, bu tür programları yazan kişiler tarafından dikkate alınmaz. Onlar için, istedikleri amaca ulaştıracak programların hızlı bir şekilde geliştirilmesi önemlidir. Bu amaca ulaşırken, programın barındığı sistemin durumunun ne olduğu veya olacağı önemli değildir. Bu yüzden casus yazılımın bulaştığı sistemler, normal başarımlarından daha düşük bir seviyede faaliyet gösterebilirler. Bazı casus yazılımların etkisi sistemin çökmesine, hatta sistemin yeni baştan kurulmasına neden olabilmektedir.

Bu tür programlara karşı ileri seviyede tecrübeli bir kullanıcı olmak bile fayda vermeyebilir. Casus yazılımı kaldırmak amacıyla yapılan müdahaleler, daha da kötü sonuçlar doğurabilir. Bu açıdan ortalama bir kullanıcı için casus savar yazılımların (antispyware) geliştirilmesinin, bu koruma yazılımların kullanılmasının şart olduğu görülmüş; sistemde var olan casus yazılımları tarayıp bulan ve/veya dinamik olarak bu tür yazılımların sisteme bulaşmasını önleyen yazılımlar geliştirilmeye başlamıştır.

Casus savar yazılım oldukça yeni bir olgudur. Piyasada artan sayıda bu konuda iddialı yazılımlar geliştirilmeye başlansa da; gelinen nokta, olması gerekenin gerisindedir. Öyle ki virüs korunma ürünleri üreten firmaların piyasaya virüs yayıp virüs korunmalarını (antivirus) satmaları nasıl abesse; casus yazılım ürünleri çıkaran firmaların, aynı zamanda casus savar yazılım ürünlerini üretip satıyor olması da o kadar vahimdir. Birinci durum "bilindiği kadarı" ile yoktur; fakat ne yazık ki ikinci duruma karşılık gelen birçok üretici bulunmaktadır.

Özellikle 2004 yılına gelindiğinde, casus yazılım konusunda önemli bir kamuoyu ve piyasa oluşmuştur. O zamana kadar casus yazılım denilince, İnternet ve güvenlik konusunda hemen hemen her şeyi ifade eden muğlak bir terim akla gelmekteydi. Bu yüzden casus yazılımın hukuki sebeplerle bir tanımının yapılması gerekiyordu. Bunun için Federal Ticaret Komisyonu (FTC, Federal Trade Commission) ve ABD Kongresi, Nisan 2004'de casus yazılımı, "Bir kişi ve örgüt hakkındaki bilginin, kendilerinin bilgisi olmadan elde edilmesine yardım eden ve böyle bilgileri başka bir tarafa tüketicinin rızası olmadan gönderen veya yine tüketicinin rızası olmadan bir bilgisayar üzerinde kontrolü elde eden yazılım" olarak tanımladı. Casus yazılımı azaltmayı hedefleyen çeşitli bildirilerin ABD Kongresi tarafından taslakları yapılmış ve bazıları 2004 Ekim ayına kadar yürürlülüğe sokulmuştur.

Casus savar yazılım ürünleri arasında, ilk örnekleri olmasının avantajıyla en başta gelen yazılımlardan, Bölüm 4.11.8'de incelenen Spybot Search & Destroy yazılımı ve Lavasoft şirketinin çıkartmakta olduğu Ad-Aware yazılımı sayılabilir. Bedava sürümü de bulunan bu yazılımlar, bir çok ihtiyacı karşılamaktadır.

Casus savar yazılım pazarına ilgi gösteren bazı firmaların, işlerini ciddiye almamaları nedeniyle, kendi yazılımlarını sattırabilmek için müşterilerini kandırma yoluna bile gittiği bile görülmüştür. Böyle bir kandırmacanın, Seismic Entertainment Productions Inc. ve SmartBot.Net Inc. şirketleri tarafından denendiği FTC tarafından saptanmış ve Ekim 2004'de bu şirketler hakkında, "çıkıveren pencereli reklamlarla sistemin başarımını ve verimli çalışmayı zorlaştıran ve kullanıcılar tarafından talep edilmeyen yazılımları gizli bir şekilde bilgisayarlara bulaştırmak ve sonra bu

bilgisayarlarda kullanıcılara, 30$'a "Spy Wiper" veya "Spy Deleter" adlarında ürünleri almaları gerektiğine dair mesajlar göndermekten" dava açılmıştır (38). Amerika'da "siber alemde" işlenen suçlarla ilgili hükme bağlanan bir çok cezalandırma ve yürütülen bir çok dava bulunmaktadır (39). Amerika'da National Cyber Security Alliance (NCSA)'ın verdiği rapora göre, kişisel bilgisayarların %80'inde casus yazılım olma ihtimali vardır (40).

IDC ve Wachovia Securities'deki endüstri analizcileri, casus savar yazılım pazarının, şu an itibariyle sahip olduğu 90 milyon ABD $'lık büyüklüğünden, 2008'e kadar 305-400 milyon ABD $'ı büyüklüğe ulaşacağını beklemektedir (41). Güvenlik yazılımı "suaygırları" olarak adlandırılan McAfee ve Symantec, ürün yelpazelerine casus savar yazılım çözümlerini uzun süredir eklemiş bulunmaktadırlar. Yahoo, EarthLink ve son zamanlarda Microsoft gibi diğer ağır toplar da pazara adım atmışlardır. Özellikle Microsoft'un casus savar yazılımı işine girişi, ana müşterileri masaüstü tüketici pazarı olan bu firmaların durumunu da etkileyecektir.

Casus yazılımların gelişimini inceledikten sonra çalışmanın yapıldığı 2005 yılında çok sayıda bilgisayarda tespit edilen casus yazılımların neler olduğu ve bu yazılımların ne tür amaçlar güttüğünün incelenmesinde fayda vardır.

3.4. En Yaygın Casus Yazılımlar

Günümüzde binlerce casus yazılım, İnternet üzerinde hızla yayılmaktadır. Bunlar arasında en yaygın olanlarının, üç casus savar yazılım organizasyonu tarafından derecelendirildiği liste Çizelge 3.1'de verilmektedir. Özellikle bu tür yaygın casus yazılımlar yakın bir şekilde takip edilmeli ve kullandıkları yöntemler kullanıcılar tarafından öğrenilmelidir.

Çizelge 3.1. En yaygın casus yazılımlar. Kaynaklar: Webroot Inc. (42), Computer Associates (43), The Network Administrator (44)

Casus Yazılım	*Webroot Inc.*	*Computer Associates*	*The Network Administrator*
Ezula		X	X
Gator/GAIN/Claria	X		X
ISTbar/Aupdate	X	X	
180search Assistant	X		
Advance Keylogger	X		
BargainBuddy		X	
BlazeFind	X		
BonziBuddy			X
CoolWebSearch (CWS):	X		
Cydoor			X
GameSpy Arcade			X
Hot as Hell	X		
Hotbar			X
IBIS Toolbar		X	
Internet Optimizer	X		
KaZaA		X	
LinkGrabber 99			X
TIBS Dialer	X		
TOPicks			X
Transponder (vx2):	X		
WeatherCast			X

Bu programlardan farklı özellikler gösteren bir kaçının açıklamaları aşağıda sunulmaktadır. Bu örneklerin kullanıcılar tarafından bilinmesi ve kavranması, ileride bu tür programlarla karşılaşıldığında daha temkinli olmayı ve benzer programları bilgisayara kopyalamamayı sağlayacaktır.

eZula isminde bir şirket tarafından aynı isimle çıkarılan Ezula programının, İnternet üzerinde gezinmeyi ve referans bilgi alınımını kolaylaştırdığı iddia edilmekteyse de bu programın izinsiz olarak başlangıç sayfası dışında diğer tarayıcı ayarlarını değiştirdiği belirlenmiştir.

En bilinen casus yazılımlardan biri de Gator'dur. Gain ve Claria adlarını da kullanan bu casus yazılımın 2001 yılı itibariyle 8 milyon bilgisayarda kurulu olduğu belirtilmektedir (45). Program, kullanıcısının ad, soyadı, ülke ve posta kodu gibi bilgilerini Gator'un kendi web sitesine göndermektedir. Kullanıcı İnternet üzerinde

gezdikçe, ziyaret ettiği siteler, ilgilendiği ürünler ve programın gösterdiği reklamlara olan tepkisi izlenmekte ve bütün bu bilgiler firmanın sunucusuna gönderilmektedir. Firma bu bilgileri reklamcılara satmakta; reklam veren şirketler bu program aracılığıyla o anda kullanılan anahtar sözcüğe göre reklamlarını Gator üzerinden gösterebilmekte; dahası program ile anlaşan reklam veren şirketin rakibine ait bir siteye girildiğinde çıkıveren pencerelerle kullanıcı çeldirilmek istenmektedir. Bu program genellikle KaZaa gibi popüler dosya paylaşım programları ve bir çok bedava yazılımla bohçalanmış bir şekilde yayılmaktadır.

ISTbar/AUpdate, pornografik sitelerde arama yapmak için kullanılan bir araç çubuğudur. Başlangıç sayfaları gibi İnternet tarayıcı ayarlarını izinsiz olarak değiştirmektedir.

BargainBuddy, gezilen siteleri ve arama motorlarına girilen anahtar sözcükleri tutan ve bunlara göre reklam gösteren bir Tarayıcı Yardımcı Nesnesidir (BHO).

IBIS Toolbar, kullanıcıdan izinsiz, tarayıcı ayarlarını değiştirir. IP, GUID, e-posta adresi, isim, telefon numarası, kredi kartı bilgileri gibi bilgileri gizlice izler. Bazı belirli sitelere girilmesini engeller.

Bu tür yazılımların sürekli olarak değişik şekillere bürünmesi ve yeni yöntemlerle gelişmesi nedeniyle güvenlik konusu ile ilgili güvenilir ve farklı kaynaklardan yeni tehditler hakkında güncel bilginin edinilmesi ve bu kaynakların takip edilmesi gerekmektedir.

Casus yazılımların şu an için var olan bütün türlerinin sunulduğu bu bölümde, ne kadar değişik casus yazılım türünün olduğu gözler önüne serilmeye çalışılmıştır. Yeni çıkan casus yazılım türlerinin ve var olan türlerin kullanacağı yeni tekniklerin sürekli bir şekilde takip edilip, öğrenilmesi çok önemlidir. Casus yazılımların en genel özelliklerinin tanıtıldığı bu bölümden sonra bu yazılımlara karşı alınabilecek tedbirlerin belirlenmesi gerekmektedir. Bölüm 4'de casus yazılımlardan korunma ile ilk başta alınacak tedbirleri belirlemek adına, casus yazılımların bilgisayar

sistemlerine nasıl sızdıkları, örneklerle incelenmektedir. Bu tekniklere göre alınacak tedbirler, işin başında bir çok yazılımın sisteme bulaşmasını önlemektedir. Bu bölümde ayrıca alınabilecek genel ve ileri tedbirler, casus yazılımların her sistem açılışında çalışabilmeleri için uyguladıkları yöntemler ve casus savar yazılımlar tanıtılmaktadır.

4. CASUS YAZILIMLARA YÖNELİK TEDBİRLER VE CASUS SAVAR YAZILIMLAR

Virüslerin yaygın bir biçimde bilgisayarlara yayılıp, sistemlere zarar vermesi üzerine ortaya çıkan virüs koruma (antivirus) programlarının, bilgisayar sistemlerinin güvenliğini sağlamada ayrılmaz bir araç olarak karşımıza çıkmasına benzer bir şekilde; 70 000'in üzerinde farklı türlerde casus yazılıma karşı, kullanıcıların ve sistem yöneticilerin kullanabileceği "casus savar yazılım" (antispyware) ürünleri geliştirilmeye ve sunulmaya başlamıştır. Virüs tanım dosyalarının uygun aralıklarla düzenli bir şekilde güncellenmesi gerektiği gibi; casus savar yazılımlar da gerek kullandıkları tanım dosyalarını gerekse yazılımın kendisini otomatik olarak güncelleyecek sistemlere sahiptir.

Casus savar yazılımları incelemeden önce, bilgisayar kullanıcılarının ve sistem yöneticilerinin bizzat kendilerinin alabileceği tedbirleri incelemede fayda vardır. Kullanılan her bilgisayarda casus savar yazılımı mevcut olmayabileceğinin yanında; düşmanını (casus yazılımları) iyi bir şekilde tanımak bir çok zararı gerçekleşmeden önlemeyi sağlayacağı gibi; bazı basit alışkanlıkların öğrenilip uygulanması, casus yazılımların elini kolunu bağlamaya yetecektir. Bunun için ilk olarak, kullanılmakta olan bilgisayar sisteminde casus yazılımın olup olmadığını anlamaya yarayacak bulgular incelenmiş; casus yazılımların sistemlere bulaşmak için kullandıkları yöntemlerin en önemlileri açıklanmıştır. Bu tür bulgulara ve bulaşma tekniklerine dikkat edilmesi ve düzenli takip edilmesi, ileride karşılaşılacak bir çok problemi önleyecektir.

4.1. Bir Bilgisayarda Casus Yazılımın Olduğuna İşaret Eden Bulgular

Casus yazılımlar, bir bilgisayar sistemine bulaştıktan sonra işlerini gizlice yapmaya çalışıp; ulaşacakları amaca sessizce erişmek isterler. Fakat çoğu kez, casus yazılım tanısını koymada bazı önemli ve yaygın belirtiler, biraz dikkatli olunduğunda oldukça kayda değer deliller sunmaktadır. Eğer,

- Bilgisayarınızın her zamanki başarımı düşüyorsa ya da kısa süreli olarak durduk yere bilgisayarınız nerdeyse sürünmeye başlıyorsa
- İnternet üzerinde tarayıcınızla sörf ederken istemediğiniz siteler karşınıza çıkıyorsa
- İnternet tarayıcınızdaki arama çubuğu bölümünde aramak istediğiniz anahtar kelimeyi girdiğinizde normalde kullanmak üzere ayarladığınız arama motoru yerine başka bir arama motoru arama sonuçlarını gösteriyorsa
- İnternet tarayıcınızdaki Sık Kullanılanlar (Favorites) veya Yer İmi (Bookmark) bölümünde sizin eklemediğiniz yabancı sitelere bağlantılar eklenmişse
- İnternet tarayıcınızın başlangıçta gösterdiği site olan "Başlangıç Sayfanız" (Home Page), sizin ayarladığınızdan başka bir siteyi gösteriyorsa ve bu ayarı tekrar değiştirseniz de yine ayarladığınızdan farklı siteler açılışta ortaya çıkıyorsa
- İnternet tarayıcınızda daha önce görmediğiniz araç çubukları varsa
- Sistem tepsinizde (system tray) daha önce görmediğiniz bir simge varsa
- İnternet'e bağlantınız olmadığı durumlarda bile size adınızla hitap eden çıkıveren (pop-up) reklamlar görüyorsanız
- İnternet sayfanızda bazı tuşlar çalışmıyorsa (örneğin bir web formu doldururken bir sonraki yazım alanına geçmek için kullandığınız sekme (tab) tuşu çalışmıyorsa)
- Bilgisayarınızla faal olarak çalışmadığınız bir sırada bilgisayar kasanızdaki sabit disk hareketini gösteren lamba sürekli yanıp sönüyorsa
- İnternet'e erişim olmadığı sırada sistem tepsisindeki ağ bağlantınızı gösteren (iki bilgisayar şeklinde gösterilen) simgede veri aktarımını gösteren hareketler görüyorsanız
- CD sürücünüz kendi kendine açılıp kapanıyorsa
- Rasgele hata mesajları alıyorsanız
- İnternet'e modem ile bağlanıp da büyük meblağlarda telefon faturası aldıysanız

sisteminizde çok büyük ihtimalle casus yazılım bulunmaktadır. Sistemine bir casus yazılımın bulaştığını bu tür bulgularla farkına varan bir kullanıcının aklına gelen ilk soru "Acaba bu yazılım sistemime nasıl bulaştı?" olacaktır. Bu yerinde sorunun cevabı, takip eden kısımda örneklerle verilmeye çalışılacaktır.

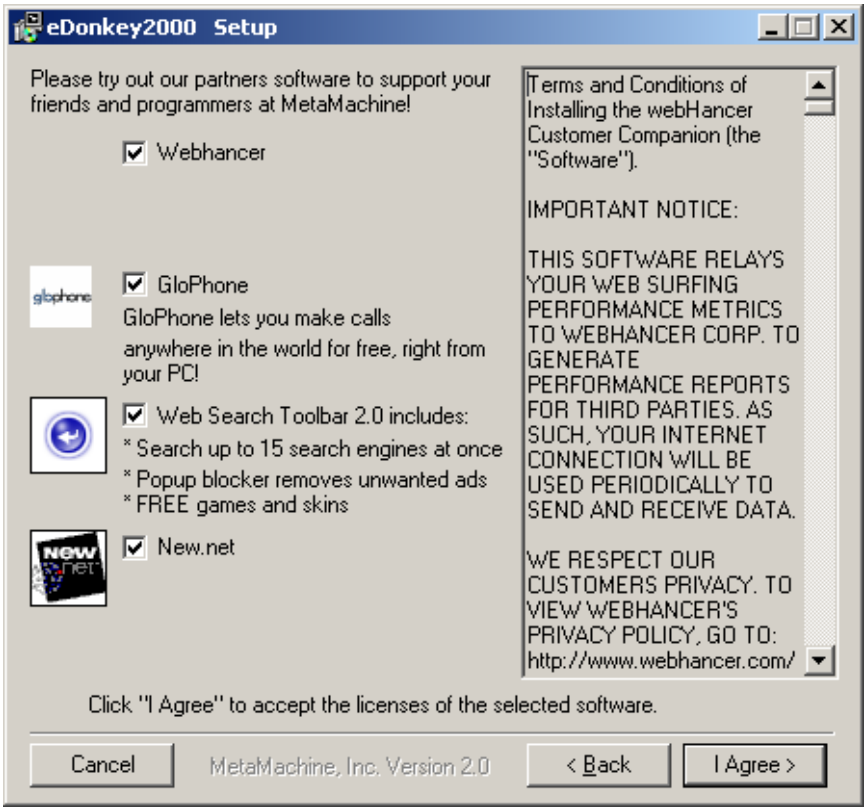
4.2. Casus Yazılımların Müşteri Çekme Teknikleri

Casus yazılımların bir bilgisayar sistemine bulaşması çeşitli şekillerde olabilmektedir. Casus yazılımlar bilgisayarlara bulaşmak ve yayılmak için, İnternet üzerinde pek de dürüst olmayan bir çok teknik kullanmaktadır. Genelde, oldukça faydalı bir işe yarayacak gibi gösterilmeye çalışan ve "bedava" olduğu sürekli vurgulanan programlar, kullanıcılara çeşitli şekilde önerilmektedir. Bazı teknikler, çok dikkat çekmeden kullanıcıların bilinç altını bile etkileyebilmektedir. Faydalı olabileceğini düşünen, üstelik de bedava olan bu yazılımları kendi bilgisayarlarına kuranların, karşılaşabileceği tehlikelerin boyutlarının neler olabileceğini kestirmek zordur.

Dahası, aslında casus yazılım olan bir programı kurmaya ikna olan veya ikna edilen kişiye, bir de o programla beraber başka casus yazılımlar kurdurma yoluna da gidilerek, daha çok casus yazılım bir birleri ile işbirliği içinde sistemlere sızabilmektedir. Şekil 4.1'de bunu gösteren çok tipik bir örnek verilmiştir. Burada bir şekilde eDonkey2000 adında bir dosya paylaşım programını sistemine kurmayı düşünen kişiye, kurulum sırasında dört adet başka programın kurulması, onay kutuları da kullanıcının zahmet etmesini önlemek amacıyla varsayılan olarak seçili olacak şekilde sunulmaktadır. "Bir taşla dört kuş vurmak" şeklinde özetlenebilecek bu yöntem, bu sıralar hemen hemen bütün casus yazılımların kurulum safhasında karşımıza çıkmaktadır.

Bu tür casus yazılımlar, herhangi bir bilgisayara kurulduktan sonra, kendi temel amacı dışında işlev görmeye başlamaktadır. Öyle ki, kullanıcının gezdiği sitelerin HTML kodlarının asıllarını bile kullanıcının haberi olmadan, dinamik olarak

değiştirip anlaşmış oldukları kendi firmaların reklamlarını bile vermeye cüret etmektedir.



Şekil 4.1. Örnek bir dosya paylaşım programı kurulumunda ilave program kurulumları

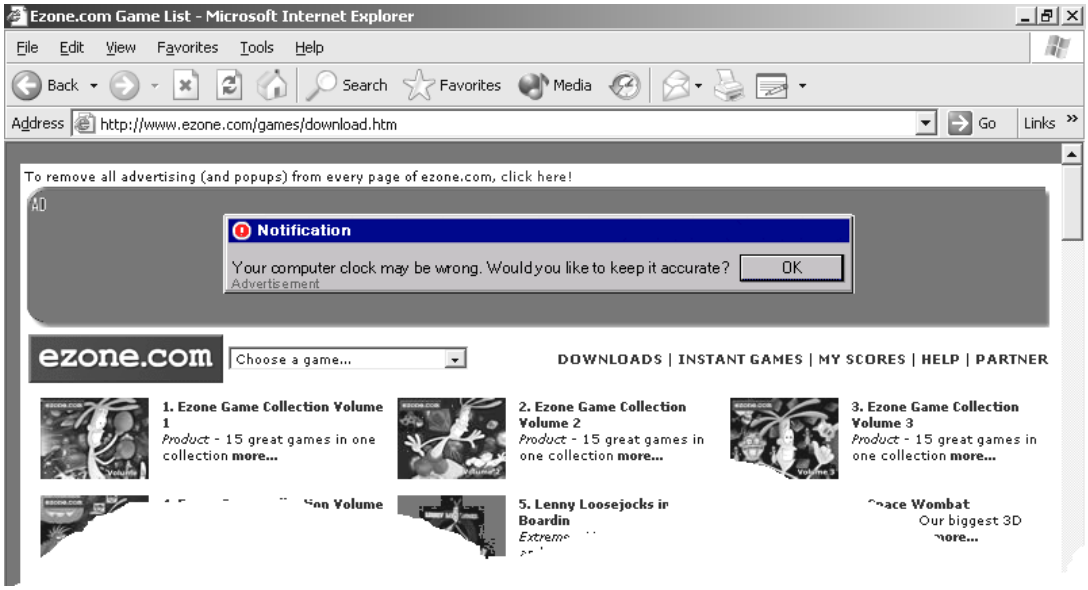
HTML kodu değişen sayfada Şekil 4.2'de görüldüğü gibi bir çok şey vadeden, çeşitli reklamlarla kullanıcılar kandırılmaya ve reklamda sunulan ürünleri almaya özendirilebilmektedir.

Sunulan reklamlar, kumar, bahis, faiz karşılığında ödünç para verme, seyahat (uçak biletleri, oteller, araç kiralama, deniz gezisi), kredi kartları, elektronik ve haberleşme, cinsel sağlık, sigorta, çöpçatanlık, sağlık ve ilaçlar (diyet, vitaminler, saç onarımı, kalp krizi önleme), müzik, kitaplar ve filmler (kitap klüpleri, CD klüpleri, DVD kiralama, bilet temini), bankacılık ve yatırım, ev ve ev ürünleri, giysi ve aksesuarlar, eğitim (çevrimiçi derece alma, uzaktan eğitim, diploma alma, tatil eğitimi), çiçekler, yazıcı sarf malzemeleri, açık artırma ve sigara gibi bir çok konuda olabilmektedir. Görüldüğü gibi her bir konu, bir çok insanı cezp edecek türdendir.

Şekil 4.2. Casus yazılımların çıkıveren reklamlarına örnekler

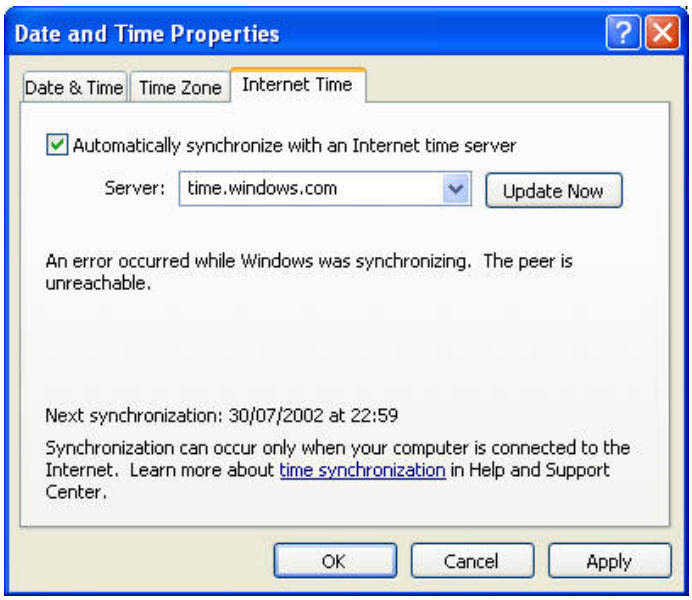
Casus yazılımların, sisteme sızabilmek için kullandığı ve aslında oldukça "zavallı" olarak nitelendirilebilecek bir başka taktik de, sahte pencere veya diyaloglar kullanmaktır. Kullanıcılar, İnternet sayfalarında gezinirken İnternet tarayıcısına ait çıkıveren pencerelere karşı az da olsa daha çekimserdirler. Bu tür pencereler, kullanıcılar tarafından görülür görülmez, genelde içeriğine bakılmadan hemen kapatılırlar. İşletim sisteminden gelen mesaj ve diyalog kutuların ise kullanıcılar tarafından daha önemsendiği düşünülmektedir. Bu gerçeği kullanan casus yazılımlar, İnternet sitelerinde standart işletim sistemi diyalog kutularına benzeyen mesajlar göstermektedirler.

Şekil 4.3'de bir örneğinin görüldüğü gibi, bir sitede geniş bir alanda bilgisayarınızın sistem saatinin tam doğru olmadığını gösteren bir ileti, sanki bir sistem mesajı gibi gösterilmektedir. Aslında resim olan bu mesaj, değişik şekillerde gezilen diğer sayfalarda gösterilerek kullanıcının dikkati çekilmek istenir. Kullanıcı bu resme tıkladığında (OK düğmesine basıp basmadığının bir önemi de yoktur) önerilen saat düzeltici programını, indireceğini düşünebilir fakat aslında bu diğer casus yazılımların kurulabilmesi için sunulan ve aslında oldukça bayağı olan bir yemdir.



Şekil 4.3. Sahte diyalog kutuları

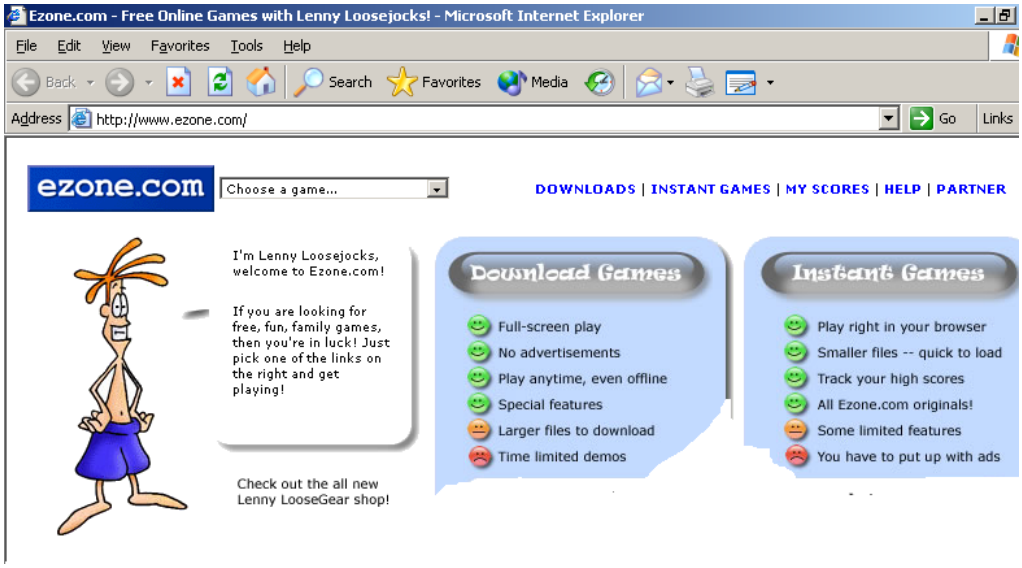
Sistem saatinin doğruluğu konusuna biraz daha eğilinirse; aslında Microsoft, Windows XP ile, kullanıcılarının doğru ve hassas sistem saatine sahip olmaları için otomatik saat senkronizasyonu özelliğini işletim sistemine bütünleştirmiştir. Şekil 4.4'de görüldüğü gibi, kullanıcılar bu özelliği etkinleştirerek saatlerini hiç bir harici programa ihtiyaç duymadan doğrulatabilirler.



Şekil 4.4. Windows XP ile birlikte gelen otomatik saat senkronizasyonu penceresi

Normalde bir web sunucusu sitesine bağlanan kişinin hangi işletim sistemini kullandığı, sunucu tarafında çok kolay bir şekilde algılanılabilmektedir. Dolayısıyla Windows XP yüklü bir bilgisayar için böyle bir sayfada sunucunun "saatiniz yanlış olabilir" diye bir mesajı göstermesi, art niyet dışında hiç bir şeyle ifade edilemez. Fakat casus yazılımların böyle gereksiz programlarla sistemlere bulaşabilmesi için kötü niyetli web sitelerinde, hiç ayırt etmeden kullanıcıların hepsine böyle bir mesaj verilebilmektedir.

Bir başka ciddi konu da İnternet sitelerinden casus programın kurulabilmesini sağlamak için çocukların suiistimal edilmesidir.

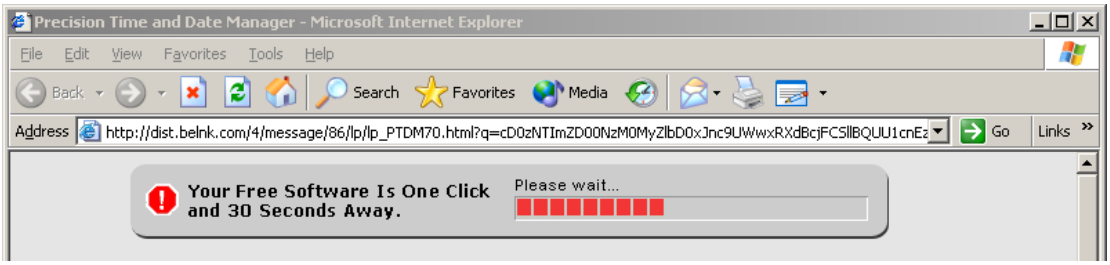


Şekil 4.5. Çocukları program indirmeye özendiren örnek bir İnternet sayfası

Şekil 4.5'de gösterilen sayfada, çocukları özendirici bir tarz göze çarpmaktadır. Çocukların hoşuna gidecek çizgi kahraman, resim ve canlandırmalarla, oyun v.s. gibi yazılımlar içinde casus yazılımlar bilgisayara kopyalanabilmektedir. Bu tür sitelerden program indiren çocuklara, EULA'nın (EULA (End-User License Agreement, Uç Kullanıcı Lisans Anlaşması) gösterilmesi de bir şey ifade etmez. Çünkü erişkinler gibi çocuklar da bu tür yazıları hiç okumaz ya da okusalar da anlamaları güçtür. Ebeveynlerin bu konuda dikkatli olmaları ve gerekli tedbirleri almaları gerekmektedir. Bölüm 5'de, klavye dinleme sistemleri anlatılırken ayrıntılarına

girileceği gibi çocukların, bilgisayar ve İnternet üzerinden casus yazılımlarla kandırılmaları ve güvenliklerinin tehdit edilmesi mümkündür.

Bazı İnternet sitelerine erişimi veya bu sitelerden yazılım kurulumunu engelleyen Bölüm 5.7.6'da "İşyeri gözetleme" başlığında ayrıntıları ile açıklanan WebSense gibi İnternet filtreleme yazılımları, bu tür adresleri engelleyebilmektedir. Fakat casus yazılım üreticileri, programlarını yeni satın aldıkları rasgele isimler içeren bir bölgeye taşıyarak, bu tür casus savar yazılımlardan bir süreliğine de olsa kaçabilmektedirler. Şekil 4.6'da görülebileceği gibi mesela "ezone.com" sitesi, saat senkronizasyonu yaptığını iddia eden yazılımın dağıtımını "dist.belnk.com/..." gibi "ezone.com" ile hiç alakası olmayan bir adresten yapmaktadır.



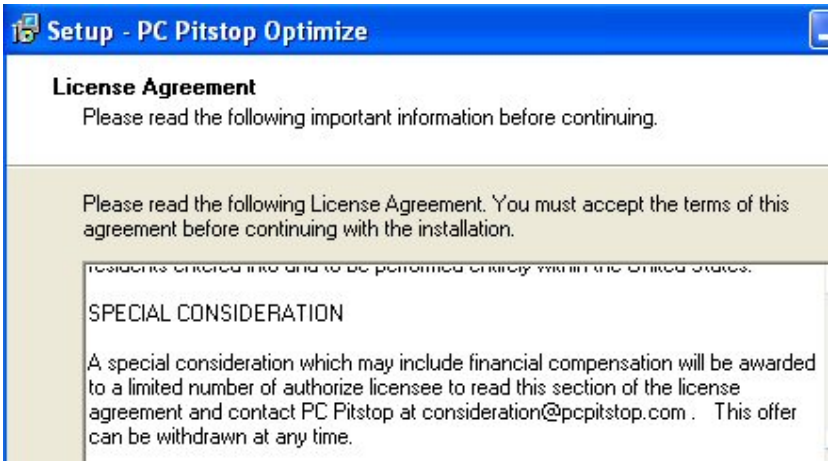
Şekil 4.6. Ana bölge adresinden farklı adres kullanarak casus yazılım dağıtımı

4.3. Uç Kullanıcı Lisans Anlaşması (EULA)

Programların kurulması sırasında normalde bir çok kurulum programı veya sihirbazı, İngilizce EULA adı verilen bir anlaşma ile başlamaktadır. Anlaşma okunduktan sonra "Kabul Ediyorum" ("I agree") düğmesine tıklanarak kurulum başlatılır. Bu durumda, anlaşmada belirtilen her şeyin kullanıcı tarafından kabul edildiği anlamı çıkmaktadır. Diğer durumda program kurulamaz. Ülkemiz için lisans anlaşması ile ilgili bir başka olumsuzluk, bu metinlerin genelde İngilizce olmasıdır. İngilizce bilmeyen veya yeterli seviyede bilmeyen kişiler, bu anlaşmaları anlamadan kabul etmek zorunda kalmaktadır.

Ne yazık ki lisans anlaşmasında yazılan metne, ya şöyle bir göz atılır ya da çoğunlukla yapıldığı gibi hiç okunmadan anlaşma kabul edilir. Bunun böyle olduğu

yaşanan bir olayla çok güzel bir şekilde gözler önüne serilmiştir. Bu olayda, casus savar yazılım ürünleri çıkaran bir firma lisans anlaşmalarına gösterilen ilgisizliği gözler önüne sermek amacıyla, kendi casus savar yazılım lisans anlaşmasının içerisinde ve metnin ortalarında yer alan bir paragrafta, "bahse konu olan paragrafı okuyup; firmaya başvuranlara mali bir ödül vereceğini" beyan etmesine rağmen; 3000 adet program indirilmesinden sonra, ancak dört ay geçince bunu okuyan tek bir kişi çıkmış ve firmaya anlaşmada belirtilen e-posta adresinden başvurmuştur. Bu kişinin 3000$ ödül kazandığı firmanın İnternet sitesinde ifade edilmektedir (46). Anlaşmanın örneği Şekil 4.7'de gösterilmektedir. Durumun vahametini gösteren bu örnek, bir çok casus yazılımın aslında programın yapmakta olduğu kirli işleri lisans anlaşmalarında "çoğu kez" belirttikleri; fakat kullanıcıların bunları okumadan kabul etmeleri nedeniyle yasa önünde suçlu bulunmamalarının sağlandığının en güzel delilidir.



Şekil 4.7. Lisans anlaşmalarının okunmadığını göstermek amacıyla hazırlanan ödüllü bir uç kullanıcı lisans anlaşması

Anlaşmaları okumayı prensip haline getirseniz bile çeşitli güçlükler sizi beklemektedir. Casus yazılımlar, kurulumları sırasında bu tür anlaşmaların okunmasını bazı numaralarla daha da zor hale getirmektedirler. GAIN casus yazılımın 2004 Ekim sürümünün Uç Kullanıcı Lisans Anlaşması, 2550 kelimeden yani yedi sayfadan oluşmaktadır. Bu kadar bol metin içinde programın yaptığı işler, Çizelge 4.1'de görüldüğü gibi net bir şekilde anlatılmaktadır:

Çizelge 4.1. Gizli bilgi toplama ve reklam gösterme ile ilgili bilgi veren örnek bir EULA anlaşması

“GAIN Publishing offers some of the most popular software available on the Internet free of charge ("GAIN-Supported Software") in exchange for your agreement to also install GAIN AdServer software ("GAIN"), which will display Pop-Up, Pop-Under, and other types of ads on your computer based on the information we collect as stated in this Privacy Statement. We refer to consumers who have GAIN on their system as 'Subscribers.'”	“GAIN Yayıncılık, bu Kişisel Gizlilik Bildirisinde ifade edildiği şekilde bilgisayarınızda topladığımız bilgilere dayanan Üste Çıkıveren, Altta Çıkıveren ve diğer türde reklamlar gösteren, İnternet üzerinde var olan en popüler yazılımların bazılarını GAIN Reklam Sunucusu yazılımını da (“GAIN”) ayrıca kurmak karşılığında ücretsiz olarak teklif eder. Sistemlerinde GAIN olan müşterilerden ‘Aboneler’ olarak bahsedilir.”

Bunun dışında bir çok ilginç ifade bu tür anlaşmaların satır aralarında var olabilir. Çizelge 4.2’de görüldüğü gibi aynı anlaşmada, program kaldırılmasının (uninstall), casus savar yazılımlarla bile mümkün olmadığı çok rahat bir şekilde belirtilmektedir.

Çizelge 4.2. Casus yazılım anlaşmasında programın kaldırılmasının yasaklanması

"You agree that you will not use, or encourage others to use, any unauthorized means for the removal of the GAIN AdServer, or any GAIN-Supported Software from a computer."	“Bir bilgisayardan GAIN Reklam Sunucusunun veya GAIN-Destekli herhangi bir yazılımın sistemden kaldırılması için hiç bir yetkisiz yöntem kullanmayacağınızı veya diğer kişileri buna teşvik etmeyeceğinizi kabul etmektesiniz.”

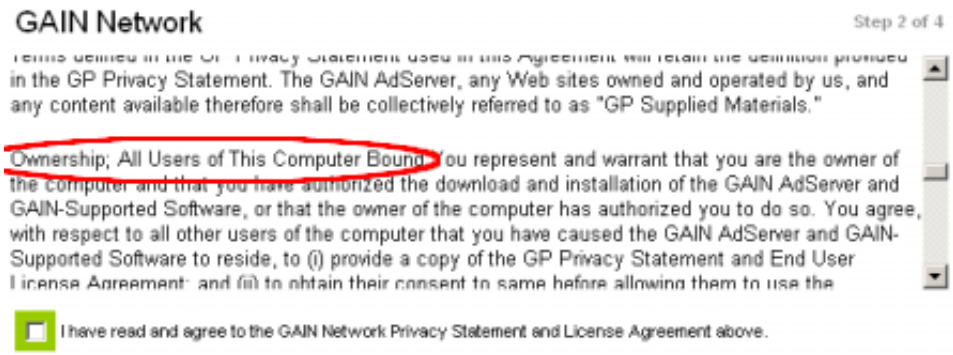
Çizelge 4.3’de yine aynı program ile ilgili ilginç bir ifade, net bir şekilde lisans anlaşmasında bulunmaktadır. Buna göre, programın yüklü olduğu bilgisayar ile programın sunucusu arasında ne gibi bir haberleşmenin olduğunu bulmaya çalışmak ve bu şekilde programın kullanıcı hakkında topladığı bilgilerin gerçekte neler olduğunu öğrenmek bile önlenmek istenmektedir (47).

Çizelge 4.3. Casus yazılımın anlaşmasında kendi topladığı ve gönderdiği bilgilerin incelenmesinin yasaklanması

"Any use of a packet sniffer or other device to intercept or access communications between GP and the GAIN AdServer is strictly prohibited."	“GP ve GAIN Reklam Sunucusu arasındaki haberleşmeleri, araya girip kesmek veya bunlara erişmek için bir paket koklayıcı veya diğer tür cihazların herhangi şekilde kullanımı kesinlikle yasaktır.”

Kullanılan başka bir numara da anlaşmanın okunurluluğunu azaltmaktır. Şekil 4.8'de GAIN programının önceki ve sonraki sürümleri için kullanılan EULA'nın ekran görüntüsü gösterilmektedir. İkinci örnekte okunurluk azdır ve kullanıcı muhtemelen o bölümü okumadan atlayacaktır.

(a) EULA'nın bölüm başlıkları koyu ve ayrı yazılmış önceki hali

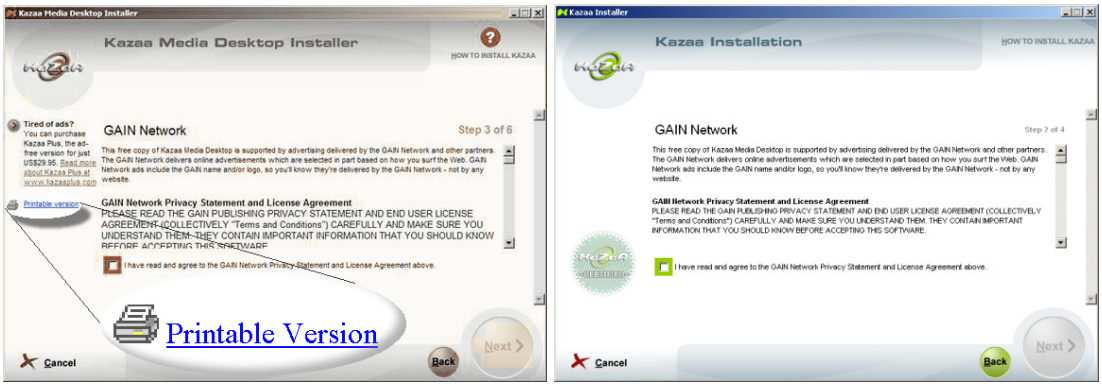


(b) Bölüm başlığı normal şekilde yazılmış sonraki hali

Şekil 4.8. EULA'nın kullanıcı tarafından anlaşılmasının güçleştirilmesine bir örnek

Bu tür programlarda çok uzun olan anlaşma metni, bir de daha düşük genişlikte bir kutuya yazılarak kullanıcının anlaşmayı okuma hevesinin kırılması istenmektedir. Kullanıcı arabirimi ile ilgili yapılan bir araştırmada, 10 ile 12 cm arasında genişlikte pencerelere yazılan yazıların, en hızlı okumayı sağladığı belirtilmektedir (48). Çoğu casus yazılımın kurulum programlarında, lisans anlaşması daha kısa genişlikte yazılarak daha çok kaydırmaya sebep olunup metnin okunma hızı düşürülmektedir. Şekil 4.1'de böyle bir kurulum ekranı gözükmektedir.

Çoğu kurulum ekranında, hem bütün anlaşmanın daha rahat okunabilmesi için hem de arşiv olarak saklanabilmesi için anlaşmanın yazıcı çıktısını alma seçeneği konulmaktadır. Kötücül yazılımların bir kısmında bu seçenek de kaldırılmıştır. Şekil 4.9'da görülebileceği gibi KaZaa programının ilk sürümlerinde yer alan Yazıcı Sürümü (Printable Version) seçeneği sonraki sürümlerinde "her nedense" gerek görülmeyerek kaldırılmıştır (47).



Şekil 4.9. Önceki sürümlerde yer alan "Printable Version" seçeneği (soldaki resim) sonraki sürümlerde kaldırılmış (sağdaki resim)

Bunun gibi bir çok kandırmaca, kullanıcıları tuzağa düşürmek ve yıldırmak için yapılmaktadır. Bazı taktikler ise "bu kadarı da olmaz" dedirtecek türdendir. Mesela lisans anlaşmasının tamamını görmeye yarayan dikey kaydırma çubukları çalışmaz hale getirilmiş veya kaydırıldığında geride hiç bir şey bulunmayan kurulum programlarına bile rastlamak mümkündür.

Çizelge 4.4'de görüldüğü gibi bir programın kuruluşunun altında bir çok gizli faaliyet yatmaktadır: sayfalarca lisans anlaşması metni, gizlenen diğer "bonus" kurulumlar ve sisteme eklenen yüzlerce sistem kütüğü (registry) eklentileri (kütük anahtarları ve değerleri) ile dosya sistemini dolduran yüzlerce eklentiler (klasörler ve dosyalar). Bu kadar eklenti ve gizlenme çabalarının, sadece dosya paylaşımını gerçekleştirmek; sistem saatini doğru tutmak veya hava durumunu anlık öğrenmek v.s. amacıyla yapılıyor olduğunu düşünmek, fazla iyimserlik olacaktır.

Çizelge 4.4. P2P (Pear to Pear, Eşten Eşe) dosya paylaşım programlarının lisans anlaşmaları, kurdukları diğer yazılımlar ve sistem kütüğüne ve dosya sistemine ekledikleri öğelerin dökümü (49)

P2P Dosya Paylaşım Programı	*Ana kurulum ekranında ifşa edilen gerekli kurulumlar*	*Ana kurulumda ifşa edilen seçimlik kurulumlar*	*Sadece lisans anlaşması içinde ifşa edilen kurulumlar*	*Bohçalanmış yazılım*		*Sistem kütüğü (registry) eklentileri*		*Dosya sistemi eklentileri*	
				İnternet gezintilerinin izini sürme	*Tarayıcı içinde veya çevresinde reklam gösterme*	*Anahtarlar*	*Değerler*	*Klasörler*	*Dosyalar*
eDonkey		Webhancer, GloPhone, Web Search Toolbar, New.net		Evet	Evet	280	944	23	353
	7767 kelime, 90 ekran sayfası. Satır başına3-5 kelime gösteren dar lisans penceresi. Birden fazla lisans tek bir metin kutusuna birleştirilmiş.								
iMesh			AskJeeves (MySearch) araç çubuğu	Hayır		488	1589	30	214
	5493 kelime, 56 ekran sayfası. Bir web araç çubuğu kurmasına rağmen “toolbar” (araç çubuğu) kelimesi asla kullanılmıyor. Lisans anlaşmasında kırık bağlantılar.								
Kazaa	Cydoor, GAIN, Instafinder, My Search Toolbar	Skype	Masaüstü simge eklentisi ("Your Free Casino Chips!" ve "Play Poker Now!")	Evet	Evet	845	1477	112	638
	22606 kelime, 182 ekran sayfası. Çok az başvurulan birden fazla lisans gösterilmiyor. Birden fazla lisans tek bir metin kutusuna birleştirilmiş. Harici belgelere anonim başvuru yapan birden fazla atıf. Ayrık bölüm başlıkları ana metin gövdesiyle birleştirilmiş. İzin verilen kaldırma yöntemlerinde sınırlama.								
LimeWire	"ads" (reklam) ve "nagware"			Hayır	Hayır	134	527	61	864
	Hiç lisans gösterilmiyor veya başvuru belirtilmiyor.								
Morpheus			DirectRevenue	Evet	Evet	85	312	15	384
	4492 kelime, 44 ekran sayfası. Lisans anlaşmasında kırık bağlantı. İzin verilen kaldırma yöntemlerinde sınırlama. Diğer programları kaldırma izninin manalı bir şekilde verilmesi. Toplanan belirli bilgilerin açığa vurulmasında ihmal.								

Kullanıcılar, sistemlerine kurdukları bütün programların lisans anlaşmalarını dikkatlice okumalı ve bu tür taktiklere karşı uyanık olmalıdır.

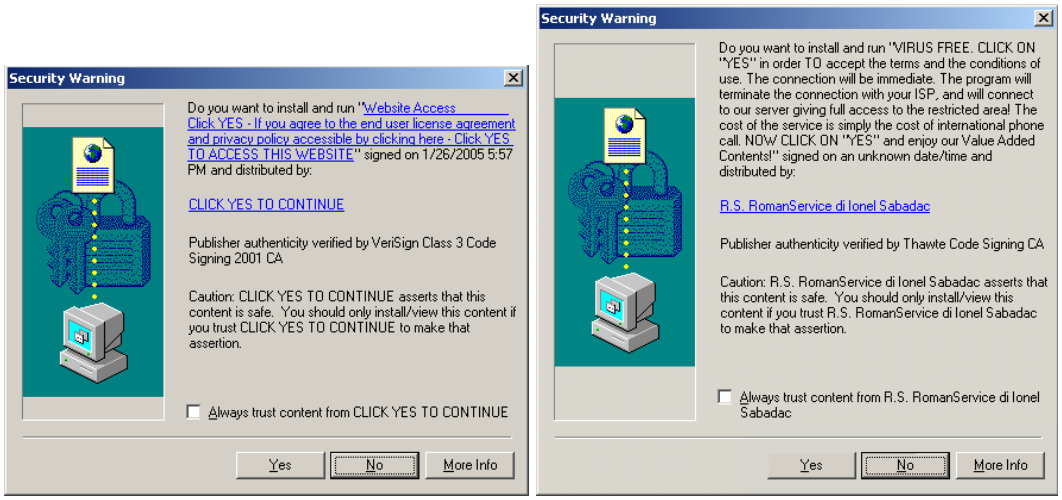
4.4. Kaçak indirme (drive-by download)

Gator firması, 2002 yılında İnternet üzerinde “kaçak indirme ActiveX” denetimini tanıttı. Normal yazılım kurulumu yanında kaçak indirme, alakası bulunmayan bir İnternet sitesinde gezinirken, istenmeyen bir yazılımın kurulması için gösterilen çıkıveren bir pencereden oluşmaktadır. Şekil 4.10’da, bu tür bir pencere görülmektedir.

Şekil 4.10. Lisans anlaşmasını kısa bir paragraf ile belirtmekle yetinen örnek bir kaçak indirme çıkıveren penceresi

Bu pencerede bulunan "Always trust content from X" ("X'den gelen içeriği her zaman güven") seçeneği çok dikkat edilmesi gereken bir kısımdır. Bu seçecek onaylanırsa, bundan sonra o firmanın yayınladığı bütün yazılımlar sisteme kullanıcıdan izin alınmadan kurulabilmektedir.

Şekil 4.11'de görülebileceği gibi bu tür diyalog kutuları şablon halindedir. Şekil 4.11 (a)'da şirket adı yerine "CLICK YES TO CONTINUE" (Devam etmek için Evet'i tıklayın) konularak, kullanıcının fazla düşünmeden istenileni yapması sağlanmaya çalışılmaktadır. Şekil 4.11 (b)'de kurulmak istenen ürünün adı, "VIRUS FREE. CLICK ON "YES"" (Virüssüz. "Evet"i tıkla) olarak belirtilmiş ve kullanıcı yanıltılmaya çalışılmıştır. Bazı sitelerde gösterilen diyaloglarda, Hayır düğmesi bile tıklansa kullanıcıya devam etmesi için Evet'i tıklaması gerektiği belirten bir mesaj, kullanıcı usanıp Evet'i tıklayana kadar sürekli olarak gösterilmektedir. Buradan çıkmanın tek yolu tarayıcıyı Görev Yöneticisini kullanarak İnternet tarayıcısını sonlandırmaktır.



(a) (b)

Şekil 4.11. İndirme ile sürücü diyaloglarının kullanıcıya yanıltmaya yönelik kullanımına iki örnek

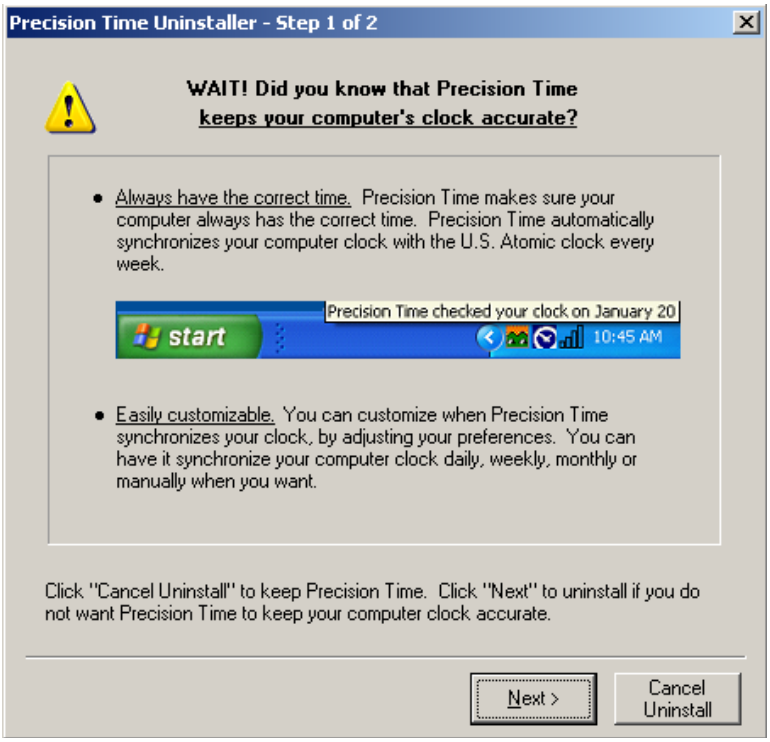
4.5. Program Kaldırma (Uninstall) Mekanizması

Bütün bu aşamalardan geçen bir casus yazılım, bir kere sisteme yerleştikten sonra, kendisini kurulduğu makineden atma ve silme çabalarına karşı da direnç göstermekte ve bunu yapmak isteyen kullanıcılara çeşitli zorluklar çıkarmaktadır. Kurulum sırasında oldukça yardım sever bir anlayış sergileyen casus yazılımlar, sıra programın kaldırılmasına gelince, oldukça "inatçı" bir tavır takınırlar. Yukarıda da bahsedildiği gibi, bu tür casus yazılımlar lisans anlaşmasında otomatik kaldırmayı bile yasaklayabilmektedirler.

Program kaldırmayı önlemek için kullanılan yöntemlerin en basitinden, hemen hemen her program ile beraber gelen standart "program kaldırma" (uninstall) rutinlerine sahip değildirler. Yani denetim masasındaki "Program Ekle/Kaldır" (Add/Remove Programs) bölümünde kurulu bulunan programlar listesinde bulunmazlar. Casus yazılımlar çoğunlukla, Başlat (Start) menüsünde, Şekil 4.12'de gösterildiği gibi, program kaldırma menü seçeneğinin de bulunduğu bir grup olarak değil; sadece çalıştırılabilir dosyayı işaret eden kısayollar halinde bulunur.

Şekil 4.12. Casus yazılımların Başlat menüsünde program kaldırma kısa yolunun da bulunduğu özel bir program grubu oluşturmamasına bir örnek

Şekil 4.13'de görüldüğü gibi Program Ekle/Kaldır bölümünde yazılımın kaldırılması olanağı tanındığı durumda ise program kaldırılmak istendiğinde, kullanıcıyı bir kez daha düşünmeye sevk eden, bir ara adım devreye girmektedir. Yufka yürekli deneyimsiz kullanıcılar buna kanıp programı kaldırmaktan vazgeçebilir.



Şekil 4.13. Casus yazılımın program kaldırma ekranında bir ara adım eklemesi

Casus yazılımların ne şekilde bilgisayara bulaştığını kavrayan bir kullanıcı için, ikinci bir soru "Bu duruma bir daha düşmemek için, casus yazılımların sisteme bulaşmalarına engel olacak ne tür önlemler alınabilir?" olmalıdır. Takip eden kısımda bu soruya cevaplar aranmaya çalışılacaktır.

4.6. Casus Yazılımlara Karşı Alınabilecek Önlemler

Öncelikle, casus yazılımlara karşı tedbirli olmak için, sunulan önlemler bir alışkanlık haline getirilmelidir. Bu konuda sürekli olarak bilgilenmek, bir diğer önemli husustur. Aşağıda oldukça geniş bir yelpazede, alınabilecek önlemlerin en önemlileri listelenmektedir.

- İşletim sistemi korunmasızlıklarını ve güvenlik açıklarını takip etmeye çalışınız.
- İşletim sistemi ve programların hizmet paketlerini, yamalarını ve güncellemelerini düzenli bir şekilde sisteminize kurunuz. Windows işletim sisteminizin otomatik güncellemesi etkin bile olsa; kendiniz Windows Güncelleme sayfasını düzenli olarak ziyaret edip, önerilen güncellemeleri elle yükleyiniz.
- Virüs tanımlama dosyalarınızın güncel olmasını sağlayınız. Önemli virüs uyarılarını dikkate alıp, sadece bu virüsler için çıkan virüs korunma programını indirip, tarama ve temizleme yapınız. Tüm sisteminizi düzenli aralıklarla tam taramadan (full scan) geçiriniz.
- Mümkün oldukça lisanslı yazılım kullanınız. Lisanslı yazılımlar, güvenliği göz ardı etmeyen ve korunmasızlıkların en aza indirilmesine çalışıldığı yazılımlardır. Bu tür yazılımların, kullanıcılara hizmet veren müşteri destek kanalları da bulunmaktadır.
- MP3, warez ve crack gibi, aslında yasal olmayan siteleri ziyaret etmekten kaçınınız. Bu tip sitelerin web yöneticilerinin, iş ahlakını düşündükleri pek söylenemez ve bu sitelere ait çoğu sayfanın HTML kodları arasında, gömülü bir casus yazılım bulunmaktadır.
- BIOS önyükleme (boot) cihaz sıralamasını değiştiriniz. Diskinizde yer alan verilerinize istenmeyen kişilerin erişimini engellemenin önemli bir adımı da, BIOS'ta bulunan sistem başlatımının hangi cihazdan yapılacağını gösteren sıralamadır. Bu sıralamanın başında, disket sürücü, CD, DVD veya USB cihazlarının yerine, "sabit disk" seçilmelidir. Bu ayar BIOS'ta yapıldıktan

sonra, BIOS'a bir şifre koyarak bu ayarın başkaları tarafından değiştirilmesinin önüne geçilebilir.

- Her ne kadar Microsoft, tarayıcısı İnternet Gezgini'ni güvenli yapmaya çalışsa da; bu tarayıcı en çok kullanılan tarayıcı olma özelliği ile korsanların açıklarını yakalamaya çalıştıkları tarayıcıların başında gelmektedir. Bu ihtimali göz önüne alıp başka bir tarayıcı seçmeniz faydalı olabilir.
- Zararlı web sitelerin bilgi toplamada kullandığı bir araç olan çerezlerle (cookie) ilgili İnternet Gezgini izin ayarlarını ve güvenlik bölgelerini aşağıdaki şekilde ayarlayınız:
    - Birinci parti çerezleri sor ("Prompt for first-party cookies")
    - Üçüncü parti çerezleri engelle ("Block third-party cookies")
    - Oturum çerezlerine her zaman izin ver ("Always allow session cookies")
- ActiveX betikleme ve Java betiklemeyi devre dışı bırakmak, bu tür ortamlara saldıran kötücül yazılımları eli boş gönderebilir.
- İnternet kafe'ler, üniversite yerleşkeleri ve oteller gibi umuma açık bilgisayarlarda, şifre, banka hesabı ve kredi kartı numarası gibi önemli verilerinizi kullandığınız işlemleri yapmamaya çalışınız. Bu tür bilgisayarlarda casus yazılım bulunabilir.
- İnternet üzerinde çevrim içi alışveriş yaparken çok titiz ve şüpheci olunuz. Güvenilir ve güvenli protokollerle işlem yapan siteleri tercih ediniz.
- Çevrim içi alışverişlerde kullandığınız kredi kartınızın limitini düşük tutunuz.
- Düzenli aralıklarla kredi kartı dökümlerinizi madde madde inceleyiniz.
- Şifre ve kimlik bilgileri gibi önemli bilgilerin bulunduğu not ve belgeleri olduğu gibi veya yırtarak çöpe ya da başka bir yere atmayınız. Bunun yerine kağıt öğütücü makinelerini kullanınız.
- Posta yolu ile gelen mektup ve belgelerinizi koruyunuz. Posta kutunuzu düzenli bir şekilde boşaltınız ve kilitli tutunuz.
- Dizüstü bilgisayarınızın kasasına isminizi ve şirket adınızı yapıştırınız. Diz üstü bilgisayarınızı standart dizüstü çantaları yerine sıradan çanta veya bavul gibi gözüken modellerde taşıyınız. Dizüstü bilgisayarınızı görünecek şekilde

arabanızın içinde bırakmayınız. Bilgisayarınızı mümkün olduğunca, yanınızdan ayırmayınız. Uçak ve otobüs seyahatlerinde dizüstü bilgisayarınızı kargo bölümüne vermeyip, yanınızda götürünüz. Kaldığınız otel odasında dizüstü bilgisayarınızı bırakmayınız.

- Bilmediğiniz yazılımları indirmeyiniz ve kurmayınız. Programları güvenilir sitelerden indiriniz. Bir çok casus yazılım diğer kurulum programlarının bire bir taklidini oluşturarak, istenilen program yerine kendisini kurabilmektedir.
- Çıkıveren pencerelerdeki bir bağlantıya veya resme tıklamayınız. İşletim sisteminizin veya tarayıcınızın meşru mesajlarını okuyup ne dediği anlaşılmadan, "Evet", "Hayır", "Tamam" ve "İptal" gibi düğmelerine basmayınız.
- Internet üzerinde gezinirken, aniden çıkan pencereleri kapatmak için pencere içindeki düğmeleri değil de; pencerenin sağ üst köşesindeki "X" şeklindeki kapat düğmesini veya Alt + F4 kapatma kısa yol tuşlarını kullanınız. Kötü niyetli kişiler bu tür pencerelerdeki masum görünen düğmeleri, kendi kötü amaçları için üzerlerinde yazandan farklı işlev görecek şekilde tasarlayabilirler.
- Çocuklarınıza bilgisayar güvenliği ile ilgili bilgi veriniz. Onların daha güvenli bir şekilde İnternet'te gezinmelerini sağlayan önleyici programları kullanınız ve güvenli sistem ayarlarını yerine getiriniz. Bu konu ayrıntılı olarak Bölüm 5.7.5 "Ebeveynlerin çocuklarını elektronik ortamda kontrolü" kısmında açıklanmaktadır.
- Şüpheli gözüken e-posta eklentilerini asla açmayınız. Özellikle uzantıları .VBS, .SHS, .SCR, .EXE, .BAT, .COM, .PIF, .LNK, .SHB, .VB, .WSH, .WSF, .WSC, .SCT ve .HTA uzantılı dosyalar için çok dikkatli olunuz (Dosya uzantıları için "Simgeler ve Kısaltmalar" bölümüne bakınız). Tanıdığınız birinden bile gelse, bu tür dosya eklentilerini en azından kaynağından doğrulatınız. Eklentilerin uzantılarının başka bir belge gibi gösterilebileceğini unutmayınız.

- Outlook gibi bazı E-posta araçlarındaki "mesaj ön izleme" (preview) penceresini kapatınız. Bu şekilde gelen mesajlarınız, listeden seçildiği zaman kendiliğinden açılmaz.
- Gönderenin, konusunun ve büyüklüğünün şüpheli olduğu mesajları açmayınız.
- E-posta aracınızın güvenlik ayarlarını sıkı tutunuz. Örneğin Outlook'ta Tools > Options > Security > Secure content > Attachment security kısmındaki eklenti güvenliğini (attachment security), Yüksek (High) yapınız. Bu şekilde eklentiler açılmak istendiğinde bir doğrulama mesajı gösterilerek, size eklenti hakkında düşünmenize ve eklentiyi açmaktan vazgeçmenize bir fırsat verilmiş olacaktır.
- Mümkün oldukça e-postalarınızı "salt-metin" (in text only) olarak açınız.
- Sosyal mühendislik konusunda uyanık olunuz. Bu konuda güvenlik ile ilgili site, dergi ve bilgi kaynaklarını takip ediniz.
- Şifre ve önemli bilgilerinizi kimseye vermeyiniz. Bunları bir kağıda veya bilgisayarınızdaki bir dosyaya yazmayınız; yazdıysanız bunları açıkta bırakmayınız.
- İnternet'te göndereceğiniz eklentilerde, sizi ele verecek gizli bilgilerin olduğunu unutmayınız. Mesela göndermek istediğiniz bir Microsoft Word belgenizde isminiz, şirketiniz ve e-posta adresiniz otomatik olarak ekleniyor olabilir. Siz e-postanızı gönderdikten sonra bu belgenizin başka kimlere daha gönderilebileceğini bilemezsiniz. Bu tür gizli bilgileri elle siliniz veya mesela "Office 2003/XP Add-in: Remove Hidden Data" gibi programları kullanınız.
- Windows işletim sistemde dosya yönetim programı olan Windows gezgini programında "gizli dosyaları göster seçeneğini" etkinleştirerek gizli olan klasör ve dosyaların görebilmesini sağlayınız. Ayrıca yine bu programın varsayılan ayarı olan "bilinen dosya türlerinin uzantılarını gösterme" (Hide file extension for known file types) seçeneğini kaldırınız. Aksi taktirde "zararsiz.txt.exe" isimli aslında çalıştırılabilir bir dosya, "zararsiz.txt" isminde bir metin dosyası olarak gözükeceğinden gözden kaçabilir.

- Bu işleme rağmen uzantısı gösterilmeyen .SHS (Shell Scrap Object) dosyaları için, sistem kütüğünde HKEY_CLASSES_ROOT\ShellScrap anahtarında bulunan "NeverShowExt" değerini; .SHB (Document Shortcut) dosyaları için sistem kütüğünde HKEY_CLASSES_ROOT\DocShortcut anahtarında bulunan "NeverShowExt" değerini siliniz. Bu dosyalar, OLE (Object Linking and Embedding) teknolojisiyle kötücül yazılımların başka dosyalar içinde saklanması için kullanılabilmektedir.
- Düzenli yedeklerinizi alınız.
- Program kurulumlarından önce sistemi daha önceki haline getirmeye yarayan denetim noktaları (check point) oluşturunuz.
- Sistem kütüğünüzü (registry) gereksiz girdilerden temizleyecek ve bütünlüğünü sağlayacak güvenilir programlar kullanınız. Bu şekilde kütük ile ilgili herhangi bir güvenlik açığına meydan vermeyeceğiniz gibi sistem başarımını da artırmış olacaksınız.
- Makinenizin günlük kullanımında, yönetici (Administrator) hesabınızı kullanmayınız. Bir çok casus yazılım, yönetici hesabı sistemde etkinken işlerini daha gizli ve daha ileri seviyede yapabilmektedir. Yönetici seviyesinde bir program çalıştırmak için "Run As" komutunu kullanabilirsiniz.
- Çalışılmayan belli bir süre sonra şifre korumalı ekran koruyucusu çalıştıracak şekilde masaüstü değişikliklerini yapınız. Makinenizi bir süreliğine de olsa terk ederken kilitlemeyi unutmayınız. Windows XP ile birlikte klavyede ⊞ (Microsoft) tuşu ile beraber L (Lock) tuşunu beraber kullanarak, bu işi hızlı bir şekilde yapabilirsiniz. Bu işlemi Windows 2000'de masaüstünde bir kısayol dosyasını "%windir%\System32\rundll32.exe user32.dll,LockWorkStation" şeklinde tanımlayıp. Buna, mesela CTRL + SHIFT + L şeklinde bir kısa yol tanımlayarak da yapabilirsiniz.
- Kişisel bir güvenlik duvarı yazılımı kullanınız.
- Kişisel bir casus savar yazılım kullanınız.

Bir programı satın alırken, kurmadan önce veya kullanırken programın casus yazılım olup olmadığını aşağıdaki soruları cevaplayarak bulmak mümkün olabilmektedir (50). Bu sorular,

- Program kullanıcıya bilgi vermeden sistem faaliyetlerinin kaydını tutuyor mu?
- Uygulama iyi anlaşılmayan veya aşırı hukuki ifadelerin olduğu bir "Uç Kullanıcı Lisans Anlaşması" mı içeriyor?
- Lisans anlaşması son kullanıcı tarafından anlaşılmayan bir mesleki dil (jargon) mu kullanıyor? Örneğin çıkıveren (pop-up) pencereler için "interstitials" veya "daughter consoles" gibi terimler kullanılıyor olabilir.
- Uygulama dağıtım için kaçak indirme (drive-by download) yöntemi mi kullanıyor?
- Uygulama yayılma için bilinen veya bilinmeyen güvenlik boşluklarından yararlanmaya çalışıyor mu?
- Popüler teknik forumlarda uygulama hakkında yoğun şikayetler var mı?
- Uygulama izinsiz başlangıç sayfası veya arama ayarlarını değiştiriyor mu?
- Uygulama ismini, bilinen standart bir Windows işletim sistemi dosyası ismine değiştirme veya program kaldırılmasının önlenmesi gibi gizlenme taktikleri kullanıyor mu?
- Kaba kuvvetle program kaldırıldığında, LSP (Layered Service Provider, Katmanlı Hizmet Sağlayıcı) yığınını kırmak gibi bilgisayarın işlevine ağır yükler bindiriyor mu?
- Kullanıcı tarafından program kaldırıldığında kendini tekrar kurmak için "damlatıcı programı" (trickler program) gibi programlar kullanıyor mu?
- Program üreticileri programın kaldırılması için kullanıcıdan zorla ücret talep ediyor mu?

olarak sıralanabilir. Aşağıda belirtilen önlemler de daha çok sistem veya ağ yöneticilerin alabileceği önlemlerdir:

- Yeni tehditlerden ve saldırı tekniklerinden haberdar olmak için gerekli girişimlerde bulununuz. Örneğin teknik forumlara üye olunuz ve güvenlik ile ilgili bültenlere abone olunuz.
- En son güncellemeleri takip ediniz ve sisteminize vakit geçirmeden uygulayınız.
- E-posta sunucunuzda .exe, .pif, .scr ve .vbs gibi kötücül yazılım dağıtımına müsait dosyalara engel koyunuz.
- Sistemdeki kullanıcılarınızı düzenli aralıklarla eğitiniz. Yeni tehditlere karşı uyarınız.
- Kullanıcılara yetecek kadar haklar veriniz.
- Kullanıcıların önemli verilere erişimlerini kısıtlayınız.
- Bir güvenlik politikası oluşturunuz ve güncelleyiniz. Bu politikaya uyulup uyulmadığını kontrol ediniz.
- Uzaktan erişim ile ilgili riskleri analiz edip önlemler alınız.
- Saldırı ve hasarlara karşı bir yıkım onarımı (disaster recovery) planı hazırlayınız.

4.7. Casus Yazılımların Otomatik Başlatma Yöntemleri

Casus yazılımların bir şekilde bilgisayar sistemine bulaştıktan sonra, sistemin her açılışında kendiliğinden çalışması gerekmektedir. Windows işletim sisteminde, programların sistemin her açılışında çalışmasını sağlamak için çeşitli yöntemler bulunmaktadır. Bu yöntemler bilinirse, bu yöntemleri kullanan casus yazılımların bazı durumlarda silinmesine bile gerek kalmadan, tekrar kendiliğinden çalışıp sisteme zarar vermesi önlenebilir. Aşağıda alt başlıklar halinde, Windows işletim sisteminde bir programın sistem ile beraber otomatik başlatılmasını sağlayacak yapılar incelenmektedir.

4.7.1. AUTOEXEC.BAT

AUTOEXEC.BAT toplu işlem dosyası, Windows'un ilk sürümlerinden beri açılışta yapılacak işleri otomatikleştirmek için kullanılmaktadır. Yeni sürümlerde sistem

tarafından kullanılmasa da; böyle bir dosya oluşturup, genelde C:\ olan açılış diskinin kök dizini altına kopyalamak yeterlidir. Bu dosyanın içinde casus yazılım, yol adresi ile beraber verildiğinde, o program otomatik olarak çalıştırılabilir. Örneğin,

c:\casus.exe

şeklinde bir ifade AUTOEXEC.BAT içine yerleştirilmiş olabilir.

4.7.2. WINSTART.BAT

Windows ile otomatik başlatılan bir toplu işlem dosyası olan WINSTART.BAT dosyasında otomatik çalışması istenen programın adresi yazılabilir.

4.7.3. Başlangıç klasörü (startup folder)

Windows işletim sisteminde, Başlat (Start) menüsü, Programlar bölümü, Başlangıç (Startup) klasöründe yer alan bütün programlar işletim sistemi başladığında çalıştırılırlar. Genelde kullanıcılar tarafından pek göz atılmayan bu klasörde, casus yazılımlar kendilerini kendiliğinden başlatmak için bulunabilirler.

4.7.4. WIN.INI dosyası

Windows'un ilk sürümlerinde sistem kütüğü yerine kullanılan INI (Initialization) ilklendirme dosyaları, casus yazılımların kendiliğinden başlamak için kullanabildikleri dosyalardır. WIN.INI dosyasında [windows] etiketi ile belirtilen bölümün altında yer alan programlar "load=" ve "run=" ile belirtilerek otomatik olarak başlatılır. Örneğin,

[windows]

load=casus.exe

run=casus.exe

4.7.5. SYSTEM.INI

SYSTEM.INI dosyası, [boot] bölümünde, Shell komutu ile programlar açılışta başlatılabilmektedir. Örneğin,

[boot]

Shell=Explorer.exe casus.exe

Burada şuna çok dikkat edilmesi gerekmektedir. Bu dosyada Explorer.exe olması gereken bir ifadedir. Yani yukarıdaki gibi bir dosyada sadece Explorer.exe dışındaki dosyalar silinmelidir. Explorer.exe silinirse sistem açılmaz.

4.7.6. WININIT.INI

Bu dosya Windows yüklendiği zaman çağırılır ve sonra silinir. Casus programlar bu dosyaya kendi girdilerini ekleyebilirler.

4.7.7. Sistem kütüğü (registry) shell open command anahtarı

Sistem kütüğünde bir kaç anahtar altındaki değerler otomatik başlatma için kullanılabilir.

[HKEY_CLASSES_ROOT\exefile\shell\open\command]

[HKEY_CLASSES_ROOT\comfile\shell\open\command]

[HKEY_CLASSES_ROOT\batfile\shell\open\command]

[HKEY_CLASSES_ROOT\htafile\shell\open\command]

[HKEY_CLASSES_ROOT\piffile\shell\open\command]

[HKEY_LOCAL_MACHINE\Software\Classes\exefile\shell\open\command]

[HKEY_LOCAL_MACHINE\Software\Classes\comfile\shell\open\command]

[HKEY_LOCAL_MACHINE\Software\Classes\batfile\shell\open\command]

[HKEY_LOCAL_MACHINE\Software\Classes\htafile\shell\open\command]

[HKEY_LOCAL_MACHINE\Software\Classes\piffile\shell\open\command]

"%1 %*" şeklinde bir anahtar her zaman yürütülecektir.

"casus.exe %1 %*" .

4.7.8. Alternatif sistem kütüğü anahtarları

Aşağıdaki iki anahtar otomatik başlatmak için kullanılabilir:

[HKEY_CLASSES_ROOT\.exe] anahtarında @="casus" şeklinde değer

Aşağıdaki anahtar uzantı değeri .xls gibi bir uzantıda dosya açılmak istendiğinde otomatik olarak çalışacaktır.

[HKEY_LOCAL_MACHINE\Software\CLASSES\.xls\shell\open\command\] anahtarında @="casus.exe %1 %*" şeklinde bir değer.

4.7.9. Ana sistem kütüğü

Aşağıdaki sistem kütüğü anahtarlarında yazılan değerler otomatik olarak başlatılacak programlar için kullanılmaktadır:

[HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\RunServices]

[HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\RunServicesOnce]

[HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Run]

[HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\RunOnce]

[HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run]

[HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\RunOnce
]

[HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\RunServi
ces]

4.8. Bit Sonlandırma ("Kill Bit") Yöntemi ile ActiveX Engelleme

İndirme ile sürücü tekniği ile veya "plug-in" şeklinde kurulmak istenen ActiveX'lerin önüne geçmek, bazen çok zor olabilir. Fakat Microsoft'un açıklamış olduğu bir yönteme göre, sistem kütüğünde engellenmek istenen ActiveX'lerin tanıtıcıları özel bir bayrak değeri ile girilerek o ActiveX'in ileride kurulmasını önlemek mümkündür (51). Normalde kullanılan ActiveX kontrollerinin bilgileri HKEY_CLASSES_ROOT\CLSID anahtarı altında bulunmaktadır. İnternet Gezgininin kullandığı ActiveX kontrolleri ise

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Internet Explorer\ActiveX Compatibility\{ActiveX Kontrolünün CLSID numarası} anahtarı altında tutulmaktadır. Burada "Compatibility Flags" adında bir değer oluşturularak DWORD türündeki değeri de "00000400" yapılırsa ActiveX kontrolünün İnternet Gezgininde çalışması önlenmiş olur.

4.9. İnternet Gezginini Ağ Kullanıcıları İçin Yapılandırma

Bir ağda yer alan tüm İnternet kullanıcılarının, İnternet Gezgini ile ilgili ayarlarının en düşük seviyede tutulması, güvenlik açısından önemlidir. Sistem yöneticileri aşağıdaki adımları uygulayarak bu ayarları en düşük seviyeye çekebilir:

1. Tüm çalışan İnternet Gezgini ve Outlook Express programlarını kapatın (kapatamıyorsanız bir proses izleyici kullanın).
2. Denetim Masası -> İnternet Seçeneklerini (Control Panel > Internet Options) seçin.
3. Güvenlik (Security) sekmesine tıklayın.

4. İnternet simgesini seçin ve Özel Seviyeyi (Custom Level) tıklayın ve aşağıdaki düzenlemeleri yapın:
    a. “İmzalı ActiveX Betiklerini İndir” (“Download Signed ActiveX Scripts") için sor’u (Prompt) seçin
    b. “İmzasız ActiveX Betiklerini İndir” (“Download Unsigned ActiveX Scripts") için Geçersiz (Disable) seçin
    c. “Güvenilir Olarak İşaretlenmemiş ActiveX Betiklerini Başlat” (Initialize and Script ActiveX Not Marked As Safe) için Geçersiz (Disable) seçin
    d. “Masaüstü Öğelerini Kur” "Installation of Desktop Items" için sor’u (Prompt) seçin
    e. “Bir IFRAME’deki Program ve Dosyaları Başlat” "Launching Programs And Files In An IFRAME" için sor’u (Prompt) seçin
5. İçerik (Content) sekmesini tıklayın ve Yayıncılar (Publisher) düğmesini tıklayın.
6. “Bilinmeyen Her Şeyi Kaldır” “Remove Any Unknowns” seçin ve Tamam (OK) düğmesine tıklayın.
7. İleri (Advanced) sekmesini tıklayın ve “İstenince Kur (Diğer)” “Install On Demand (Other)” onayını kaldırın ve Uygula (Apply) veya Tamam (OK)’e tıklayın.

4.10. Casus Yazılım Bulunan Konak Sunucuların Önlenmesi

Sistem yöneticileri için içeriğinde casus yazılım bulunan sunuculara erişimi engellemek aslında çok basittir. Bunun için “hosts” dosyasını oluşturmak ve engellenecek sunucuların isimlerini yazmak yeterlidir:

127.0.0.1 Localhost

127.0.0.1 iads.adroar.com

127.0.0.1 lists.adroar.com

127.0.0.1 advertisingvision.com

İlk satır yerel konağı; son üç satır ise engellenecek konakları belirtmektedir. Böyle bir dosya işletim sisteminin türüne göre aşağıdaki klasörde bulunmalıdır:

Windows XP: C:\WINDOWS\SYSTEM32\DRIVERS\ETC

Windows 2K: C:\WINNT\SYSTEM32\DRIVERS\ETC

Win 98\ME: C:\WINDOWS

İnternet'te elde ettikleri geniş casus yazılım bulunan sunucuları tutan örnek bir hosts dosyası İnternet'ten temin edilebilir (52). Bu dosya kullanılarak bir çok zararlı siteye erişim engellenebilir.

4.11. Casus Savar Yazılımlar

Yukarıda bahsedilen casus yazılım bulaşma tekniklerinin ve bu tür yazılımların önüne geçilmesi için alınacak tedbirlerin, kullanıcılar tarafından takip edilmesi ve uygulanması faydalı ve etkili bir yöntem olarak düşünülse de; onlarca casus yazılım türünden on binlerce casus yazılımın her biri ile baş edebilmek, özellikle sıradan ve acemi kullanıcılar için mümkün değildir. "Güvenlikle ilgilenenler dahil" ileri kullanıcılar bile, tıpkı virüs koruma programlarını kullandıkları gibi; casus yazılımlara karşı etkin mücadeleyi, casus savar yazılımlarla güçlendirmelidir. Konunun yeni olması itibariyle casus savar yazılımlar da oldukça hızlı bir gelişme süreci içine girmektedir.

Piyasada çok sayıda casus savar yazılımı paket halinde sunulmaktadır. McAfee ve Norton gibi daha çok virüs koruma yazılımlarıyla ünlenen büyük şirketler de henüz yeterli seviyeye gelmese de casus savar yazılım ürünleri sunmaya başlamışlardır. Mesaj sağanağı önleme üzerine ürünler geliştiren Giant şirketini satın alan Microsoft'un, casus savar yazılım piyasasına girmesi, piyasayı hareketlendirecek bir gelişme olarak düşünülmektedir. Haziran 2005 itibariyle Beta safhasında olan ve en çok kullanılan işletim sistemlerinden bir olan Windows XP işletim sisteminde ve sonraki sürümlerde sistem ile bütünleşik olarak çalışacak bir casus savar yazılım

modülü, bir çok casus savar yazılımı uzmanı tarafından önemli ve kökten bir gelişme olarak nitelendirilmektedir (53).

Ek-1'de gösterilen 2005 Yılı Casus Savar Yazılım Derecelendirme tablosunda belirtilen ve bir çok derecelendirmede üst sıralarda yer alan, yaygın casus savar yazılımlarla ilgili açıklamalar aşağıda verilmektedir. Bir çok yazılım benzer özelliklere sahip olduğundan diğer yazılımlarda aynı konular tekrar edilmemiştir.

4.11.1. Spyware Eliminator

Aluria Associates firması (54) tarafından üretilen ve deneme sürümü de sağlanan bu casus savar yazılımı, bir çok casus savar yazılım derecelendirmelerinde birinci sırada çıkmaktadır. Spyware Eliminator'ün, hem ev kullanıcılarına hem de AOL gibi büyük şirketlere olmak üzere, 35 milyon kopya satıldığı belirtilmektedir (55). Yazılımın en önemli artılarından biri, hızlı ve sık güncellenmesidir. Bu sayede yazılım, yeni casus yazılımlara karşı daha hazırlıklı olmaktadır. İyi tasarlanmış bir kullanıcı ara birimine sahiptir. Kullanıcı desteği de oldukça gelişmiştir. Sistemin casus yazılımlara karşı taranması oldukça hızlıdır. Casus yazılımları taramada imza tabanlı arama dışında geliştirilen ve kullanılan teknikler bu hızı sağlamaktadır. Bulduğu casus yazılımların zarar derecesini de göstermektedir. Casus yazılım kaldırma sırasında yapılan bir çok işlemi geri alma özelliği bulunmaktadır. Şekil 4.14'de örnek bir ekran görüntüsü verilen Spyware Eliminator'un bir başka iddialı olduğu alan klavye dinleme sistemlerine karşı geliştirdiği seçeneklerdir. Piyasada bulunan bir çok klavye dinleme sistemi yazılım tarafından saptanmaktadır. "Active Defense" olarak adlandırdıkları işlev ile gerçek zamanlı koruma yapabilmektedir.

Şekil 4.14. Spyware Eliminator 4.0

4.11.2. CounterSpy

Sunbelt Software firması tarafından geliştirilen ve deneme sürümü bulunan, renk kodlamalı tehdit göstergesi ve bilgisayarda bulunan casus yazılımların açıklamalarını içeren ucuz, fakat gelişmiş bir casus savar yazılım olan CounterSpy (56), 2005 yılının en iyi casus savar yazılım programları arasında yer almaktadır. "Active Protection" yöntemi ile gerçek zamanlı koruma sağlamakta; otomatik güncellemelerle kendini yeni tehditlere karşı hazır hale getirebilmektedir. Tecrübesiz kullanıcıların bile varsayılan ayarlarla güvenilir bir bilgisayara sahip olmaları, en az müdahaleye ihtiyaç duyacak şekilde gerçekleşebilmektedir.

4.11.3. Spy Sweeper

Webroot Software firması tarafından üretilen ve deneme sürümü de bulunan casus savar yazılım programı Spy Sweeper (57), haftalık tanımlama dosyası güncellemeleri ile casus yazılımlara daha hazırlıklıdır ve casus yazılımların saptanması, kaldırılması ve engellenmesi için oldukça iyi çözümler getirmektedir. Sistem taraması diskteki her dosyayı incelediğinden işlemler uzun sürse de; güvenilir sonuçlar üretmektedir. Kullanıcı arabiriminde yer alan diyalogların büyültülüp küçültülememesi eksi bir yön olarak düşünülebilir. Taranacak sabit diskin seçilmesi, çok büyük dosyaların taranmaması gibi bir çok düzenlemeye olanak vermektedir.

4.11.4. SpySubtract

InterMute firması tarafından geliştirilen ve deneme sürümü de sunulan SpySubtract (58), çok sayıda casus yazılım saptayabilmekte ve yerleşik bir özelliği ile bütün Gator casus yazılım türevlerine karşı koruma sağlayabilmektedir. Casus yazılımın nereden indirildiği bilgisini verebilmektedir. Çalışırken yaptığınız işlerle ilgili iz bırakmamak için, bir çok program ve işletim sistemi kayıtlarını temizleme imkanı sağlamaktadır. Bulunan casus yazılımlarla ilgili çok fazla bilgi vermese de tarama, sağladığı uyarlama imkanları ile rahat bir kullanım imkanı sunabilmektedir.

4.11.5. Spyware Doctor

PC Tools firması tarafından üretilen, deneme sürümü ne yazık ki sunulmayan Spyware Doctor (59), etkileyici kullanıcı arabirimi ile bir çok casus yazılımı "gerçek zamanlı" ve tarama ile bulma yeteneğine sahiptir. İleri kullanıcılar için güçlü araçlar sunmaktadır. Bütün sistemin taranması oldukça hızlı bir şekilde gerçekleşmektedir.

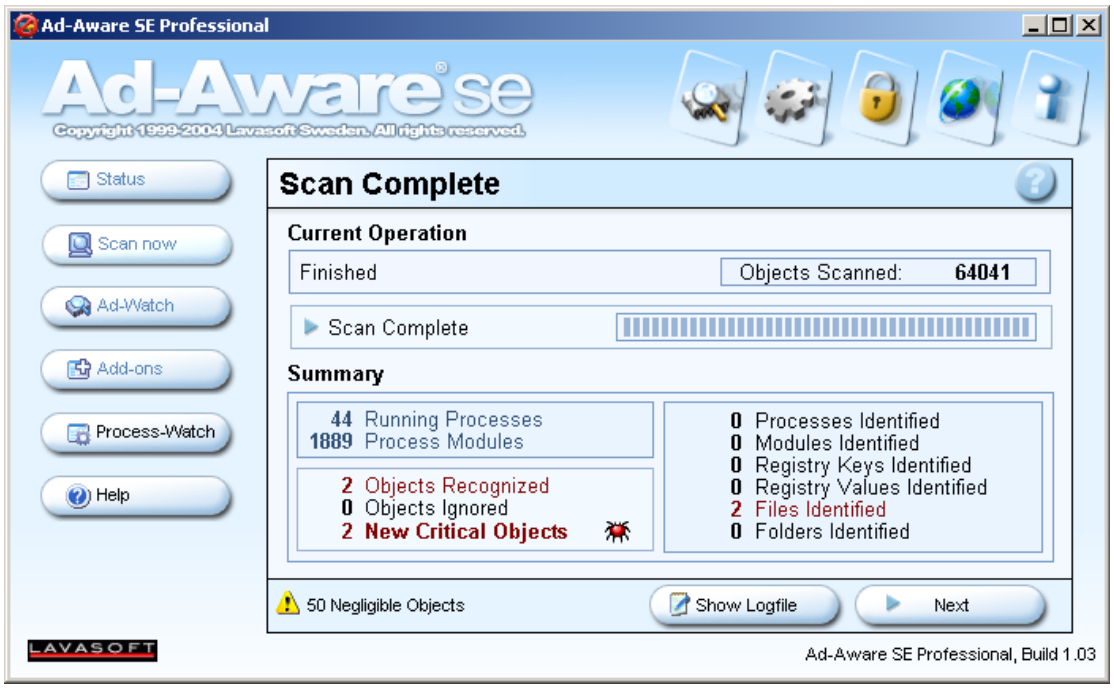
4.11.6. PestPatrol

Computer Associates International firması tarafından üretilen ve bulduğu casus yazılımları temizlemeyen bir deneme sürümünün sunulduğu PestPatrol (60) programı, popüler casus savar yazılımlardan biridir. Gerek program bünyesinde gerekse İnternet sitesinde, casus yazılımlarla ilgili oldukça fazla sayıda bilgi içermektedir. Kullanıcı arabirimi diğer casus savar yazılımlara göre biraz daha karmaşık olan yazılım, geri alma/geri yükleme yeteneği, casus yazılım önem derecesi ve çıkarılabilir ortam tarama özelliklerini içermediğinden tercih edilmeyebilir.

4.11.7. Ad-Aware SE pro

LavaSoft firması tarafından üretilen ve gerçek zamanlı koruma özelliği kaldırılmış bedava sürümü de bulunan Ad-Aware SE Pro (61), belki de en çok bilinen casus savar yazılımdır. Özellikle bedava sürümü bir çok kullanıcı tarafından kullanılmaktadır. Önceki sürümlerine göre daha iyi bir arayüzü sahip olan Ad-Aware

SE Pro'nun, belki de çok tanınmasının verdiği avantajı kullanmak adına, fiyatını da diğer rakiplerine göre yüksek tuttuğu gözlenmiştir. Çok etkin olmasa da gerçek zamanlı koruma sağlayan program, kullanıcının yaptığı güncellemelerle yeni casus yazılımlara daha etkin koruma sağlamaktadır. Şekil 4.15'de örnek bir tarama sonucunun gösterildiği program için, teknik desteğin yetersiz olduğundan bahsedilmekte ve yazılım tarama zaman çizelgesinin olmamasıyla da önerdiği fiyatı karşılamadığı düşünülmektedir. Bedava sürümünde tarama, temizleme ve tanımlama dosyalarının İnternet'ten güncellenmesi mümkün olduğundan bu hali ile kullanılabilir.

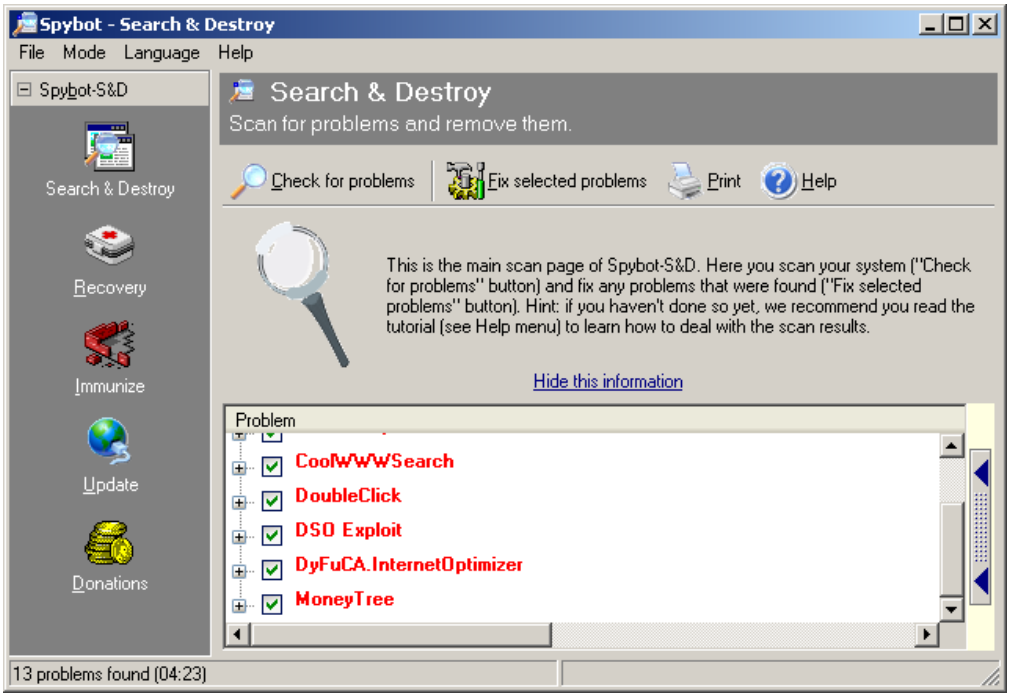


Şekil 4.15. Ad-Aware SE Pro 1.03

4.11.8. SpyBot – Search & Destroy

Patrick M. Kolla adlı bir kişinin inisiyatifi ile üretilen ve bedava olarak kullanıcılara sunulan SpyBot – Search & Destroy programında Türkçe desteği de bulunmaktadır. Program kurulduktan sonra açılışta sistem kütüğünün yedeğini alarak ileride olabilecek zararlar sonucunda tekrar yüklenmesine olanak sağlamaktadır. İlk kullanımda bir sihirbazla başlangıçta yapılacaklar, adım adım kullanıcıya gösterilmektedir. Ad-aware ile taranılan bilgisayarda yapılan 4 dakika süren

taramada 13 736 adet casus yazılım tehdidinden 13 adet bulunmuştur (Şekil 4.16). İleri modu da bulunan programda kullanışlı bir çok araç bulunmaktadır.



Şekil 4.16. SpyBot – Search & Destroy

Yapılan test taramaları ve casus savar yazılımlarla ilgili açıklamalar ışığında daha güvende olmak için "şimdilik" sadece bir casus savar yazılım yerine birden fazla casus yazılımın aynı anda kullanılması gerekebileceği düşünülmektedir.

4.11.9. Microsoft AntiSpyware (beta)

Çalışma aşamasında Beta sürümü sunulan Microsoft AntiSpyware yazılımı, Windows XP işletim sistemi ile beraber kullanılabilmektedir. Şekil 4.17'de örnek bir ekran görüntüsü sunulan Microsoft AntiSpyware, casus yazılımların ve diğer potansiyel olarak istenilmeyecek yazılımların bilgisayarda saptanmasına ve silinmesine yardımcı olmaktadır. Gerçek zamanlı casus yazılım güvenlik ajanları ile sistemde dinamik güvenlik sağlayarak, kötücül yazılımların sisteme girmeden yakalanabilmesi sağlanmaktadır. Tümleşik casus yazılım taraması, elli bin adet bilinen casus yazılım imzasından oluşan ve İnternet üzerinden güncellenebilen bir veritabanını kullanmaktadır. Tarama işlemi elle başlatılacağı gibi zaman çizelgesi ile

çeşitli zamanlarda da otomatik olarak çalışabilir. Tehditlerin daha iyi taranıp tespit edilebilmesi için kullanılan derinlemesine tarama ile bilgisayarın sabit disklerinde, bellekte, çalışan proseslerinde, sistem kütüğünde (registry) ve çerezlerde zararlı yapılar bulunabilmektedir.

Şekil 4.17. Microsoft AntiSpyware (Beta)

Microsoft AntiSpyware casus yazılımlara karşı çeşitli denetleme noktalarında çalışan ve İnternet, sistem ve uygulama ajanları adında üç çeşit ajan çalıştırmaktadır. Bu ajanların kontrol ettiği denetleme noktaları şu şekilde belirlenmiştir:

- İnternet ajanları: telefonla bağlantı, WiFi (kablosuz) bağlantı, İnternet güvenilir siteler, Winsock katmanlı hizmet sağlayıcıları, Windows messenger hizmeti, mesaj sağanağı hayaleti önleme, İnternet vekil sunucu, ad sunucu koruması ve TCP/IP parametreleri
- Sistem ajanları: Windows host dosyası, Windows servisleri, içerik menü işleyici, Windows kabuk yürütme çengelleri, Windows kabuk open komutları, Windows system.ini dosyası, Windows dizin Truva atları, Windows uzantıları, Windows win.ini dosyası, control.ini politikası, ini

dosyası eşlemleme, paylaşılır TaskScheduler, onaylı kabuk uzantıları, kabuk servisi nesne gecikme yükleme, kullanıcı kabuk klasörleri, Winlogon kabuk, Winlogon Userinit, AppInit DLL'leri, gezgin Truva'ları, Windows şifre koruması, Windows güncelleme hizmeti, Windows protokolleri, Windows Anonymous kısıtlama, Windows Logon politikaları ve WOW başlatma kabuğu

- Uygulama ajanları: Proses yürütme, çalışan prosesler, başlangıç dosyaları, başlangıç kütük dosyaları, ActiveX kurulumları, Tarayıcı Yardımcı Nesneleri (BHO), İnternet Gezgini gezgin çubukları, İnternet Gezgini uzantıları, İnternet Gezgini araç çubukları, İnternet Gezgini URL'ler, betik engelleme, İnternet Gezgini güvenlik ayarları, İnternet Gezgini 3. parti çerezler, İnternet Gezgini plug-in'leri, İnternet Gezgini güvenlik bölgeleri, İnternet Gezgini ShellBrowser, İnternet Gezgini güvenilir siteler, İnternet Gezgini WebBrowser, URL arama çengelleri, İnternet Gezgini menü uzantısı, regedit devre dışı bırakma politikası, IE web ayarlarını başa al, İnternet gezgini kısıtlamaları, uygulama kısıtlamaları ve kurulan bileşenler.

Bu denetim noktaları, istenirse pasif hala getirilebilmektedir. Microsoft Antispyware'de ileri seviye araçlar bölümünde, sistem gezginleri ve tarayıcı soyma geri alma sistem araçları; kişisel gizlilik araçları bölümünde, iz silici aracı bulunmaktadır. Sistem gezginleri aracında, indirilen ActiveX'ler, çalışmakta olan prosesler, başlangıç programları, İnternet gezgini BHO'lar, ayarları, araç çubukları, Windows host dosyası, Winsock LSP'leri, Kabuk çalıştırma çengelleri görülebilmektedir. İz silici programı işletim sistemi dışında onlarca programın tarihçelerini silebilmektedir.

4.12. Güvenlik Duvarları (Firewalls)

Bilginin ve bilgi güvenliğinin önemini anlayıp var olan casus yazılımları tanıyıp bunlara karşı gerekli tedbirleri alıp bir de sisteminizi casus savar yazılımlarla destekledikten sonra yine de güvende olunmadığının bilincinde olmak gerekir. Casus savar yazılımlar ve virüs koruma programları bilgi güvenliğinin vazgeçilmez

öğeleridir. Fakat bu güvenlik programlarının korunma sağlayamayacağı durumlar da bulunmaktadır. Eksik parça güvenlik duvarlarıdır.

Özellikle kendi ağınız dışında, kablosuz ağ gibi başka ağlara bağlanıyorsanız; çok önemli ve bir daha yerine koyamayacağınız veri ve belgeler sisteminizde bulunuyorsa; size karşı bilgi casusluğu yapabileceklerinden şüphelendiğiniz kişiler bulunuyorsa ve Truva atları ve virüsler gibi kötücül yazılımlara karşı ilave bir koruma katmanı istiyorsanız, muhakkak bir güvenlik duvarı kullanmanız gerekmektedir.

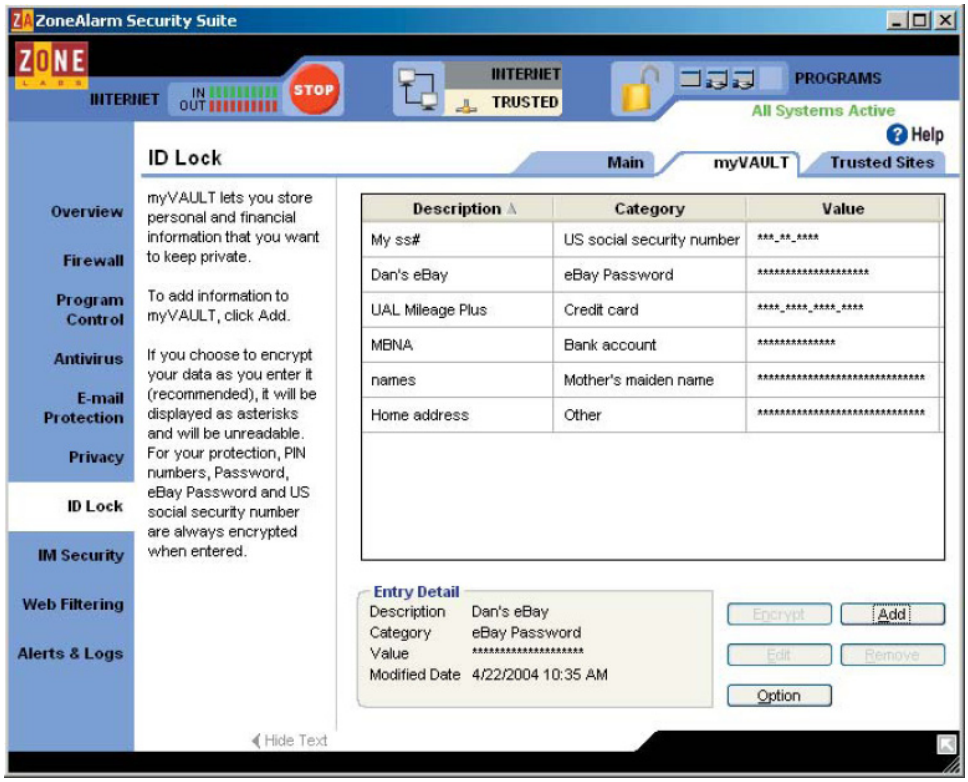
Güvenlik duvarları, en başta dışarıdan bir saldırganın sisteminizi ele geçirmesini önleyecek yapılar içermektedir. Ayrıca bir şekilde kötücül bir yazılım sisteme yerleştikten sonra bu yazılımın dışarı ile haberleşmesinin de önüne geçerek, oluşabilecek zararlar önlenmiş olmaktadır. Yani güvenlik duvarları bilgisayar sisteminiz ile İnternet gibi harici bir sistem arasındaki veri iletişimini kontrol eder ve onaylanmayan veri akışını durdurur. Bu tür bir yapı, casus savar yazılım sistemlerinde "henüz" bulunmamaktadır.

Windows XP Hizmet Paketi 2 ile beraber kişisel bir güvenlik duvarı sisteme ilave edilmiştir. Bu güvenlik duvarı asgari seviyede korunma sağlamaktadır. Dışarıdan gelecek saldırılara duyarlı olan bu sistem, içerden yapılacak saldırılarda etkisiz kalmaktadır. Örneğin sisteme bir şekilde bir klavye dinleme sistemi kurulduğunda ve önemli bilgiler sistem dışına e-posta veya FTP ile aktarılmak istendiğinde, Windows güvenlik duvarı bu konuda etkisiz kalmaktadır. Bunun için işletim sisteminin sağladığı dışında iyi bir güvenlik duvarı yazılımı elde etmekte fayda vardır. İyi bir güvenlik duvarında aşağıdaki özellikler bulunmalıdır:

- Saldırganlara karşı varsayılan şekilde bilgisayarı görünmez yapma
- Sadece güvendiğiniz kişilere dosya ve yazıcı paylaşımı sağlama
- Sadece emin olduğunuz ve onayladığınız uygulamaların İnternet'e erişimini sağlama

- Kötücül yazılımların güvenlik duvarını etkisiz hale getirme çabalarını bertaraf etme
- Güvenlik duvarı engellendiğinde kişisel bilgisayarı kendiliğinden kilitleme

Piyasada bir çok güvenlik duvarı bulunmaktaysa da; bunlar arasında ZoneLabs firması tarafından geliştirilen ve bedava kısıtlı sürümü de bulunan ZoneAlarm Pro (62), Aginitum firmasının ürettiği Outpost Firewall Pro (63), Sygate firmasının ürettiği Sygate Personal Firewall Pro (64) ve Symantec firmasının ürettiği Norton Personal Firewall 2005'i (65) saymak mümkündür.



Şekil 4.18. ZoneAlarm Pro

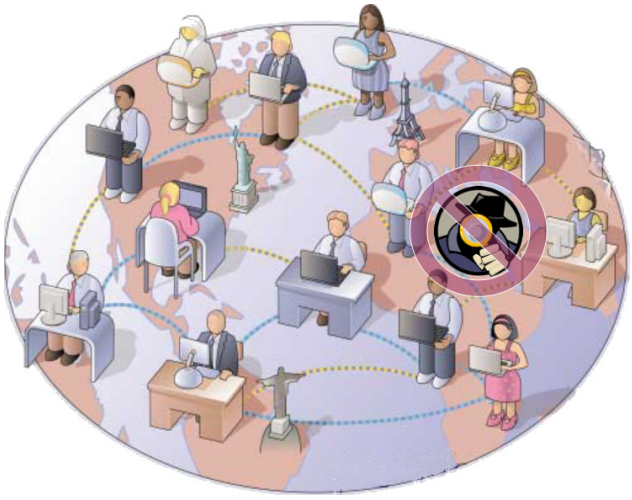
Şekil 4.18'de örnek bir ekran görüntüsü gösterilen ZoneAlarm Pro, dışarıdan gelen yoklama ve saldırıları engellemekte; dışarıya çıkan ağ etkinliklerini göstermekte; kullanıcıya sunulan bir "panik" düğmesi ile saldırı durumunda bütün İnternet haberleşmesini kesebilmekte ve şifre ve kimlik bilgilerini koruyabilmektedir. Çerez kontrolü, reklam engelleme ve program tarihçeleri ve tampon bellek silme gibi özelliklere de sahiptir.

Casus savar yazılımlar konusundaki karmaşayı gidermek; casus yazılımlar ve diğer potansiyel teknolojiler çerçevesinde süre gelen tartışmalarda kullanılan tanımlamalar ve en uygun tatbikatlar konusunda bir uzlaşma temeli sağlamak amacıyla, aralarında Aluria, AOL, Computer Associates, Dell Inc., EarthLink, F-Secure Corporation, HP, Lavasoft, McAfee Inc., Microsoft, Panda Software, PC Tools, Safer-Networking Ltd., Symantec, Tenebril, Trend Micro, Webroot Software, Yahoo! Inc., Center for Democracy & Technology, Samuelson Law, Technology & Public Policy Clinic at Boalt Hall,, UC Berkeley School of Law, The Canadian Internet Policy and Public Interest Clinic ve The Cyber Security Industry Alliance gibi casus savar yazılım firmaları, akademik ve tüketici gruplarından oluşan ASC (Anti-Spyware Coalition, Casus Savar Yazılım Koalisyonu) oluşumu klavye dinleme sistemleri dahil bir çok casus yazılım ile ilgili ilk taslak çalışmalarını yayınlamaya başlamıştır (66).

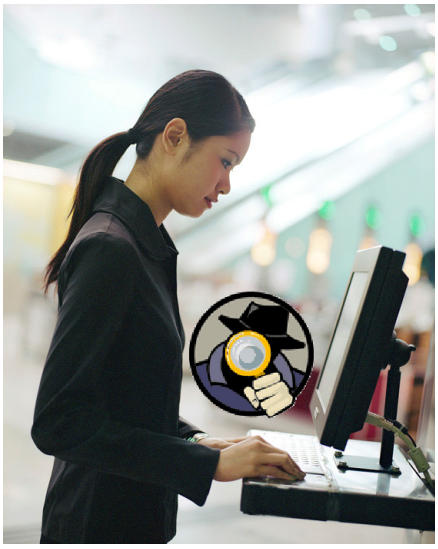
Bu bölüme kadar bilgi ve bilgi güvenliğinin genel unsurlarından ve kötücül yazılım, casus yazılım ve casus savar yazılımlardan bahsedilmiştir. Bölüm 5'de çok tehlikeli sonuçlar doğurabilecek ve genelde göz ardı edilen casus yazılım türlerinden klavye dinleme sistemleri, bütün yönleriyle incelenecektir.

5. KLAVYE DİNLEME SİSTEMLERİ

Bilgi ve bilgisayar güvenliğinde, son zamanlara kadar en dikkat çeken ve üzerinde en çok çalışmanın yapıldığı kısım, makine-makine arayüzü güvenliğinin sağlanmasıdır. Şekil 5.1 (a)'da gösterilmeye çalışıldığı gibi, bir yerel ağ üzerinde, geniş alan ağı üzerinde ve İnternet üzerinde birbirleri ile veri iletişimi içinde bulunan kullanıcılar arasında güvenli bir iletişim sağlanması ve bilgi, kaynak ile hedef arasında gidip gelirken bütün güvenlik unsurlarının sağlanması gerekmektedir. Bu konuda şifreleme ve şifre çözme algoritmaları, açık anahtar altyapısı, e-imza, SSL gibi güvenli protokoller geliştirilmekte ve kullanılmaktadır (6, 67).



(a) Makine-makine



(b) İnsan-makine

Şekil 5.1. Arayüz güvenliği

Şekil 5.1 (b)'de gösterildiği gibi, örneğin bir banka müşterisi güvenli bir protokolle hesabının olduğu bankanın İnternet şubesi ile işlem yaptığında, müşterinin makinesi ile bankanın sunucusu arasında oldukça güvenli bir altyapı sunulmaktadır. Fakat müşteri kendi bilgisayarına şifre ve hesap bilgileri gibi önemli bir bilgi girerken; bu bilginin daha uzağa gitmeden, doğrudan kullanılan makinenin kendisinden elde edilmesi mümkün değil midir? Cevap ne yazık ki evet'tir. Hem de kolaylıkla. İnsan-makine arayüzüne yapılan bir saldırı ile bu verileri elde ettikten sonra; ileri

aşamalarda, makine-makine arayüzünde alınan güvenlik önlemlerinin sadece bu arayüzde gerçekleşebilecek saldırıları önlemenin ötesinde bir değeri yoktur.

Kullanıcı ile bilgisayar sistemi arasında veri iletişimini sağlayan arayüz olarak tanımlanabilecek insan-makine arayüzü, klavye, fare, dokunmatik ekran, ışıklı kalem, iztopu (Trackball), barkod okuyucu, oyun çubuğu, mikrofon, tarayıcı ve sayısal kamera gibi girdi sistemleri; monitör, hoparlör, yazıcı, çizici ve projektör gibi çıktı sistemleri ve disk, disket, CD, DVD, USB bellek, akıllı kart, flash kart, kızılötesi ve bluetooth gibi girdi/çıktı sistemlerinden oluşmaktadır. Bu arayüze karşı yapılan saldırılar, genelde "ortadaki adam" (man-in-the-middle) saldırısı olarak adlandırılmaktadır. Bu tür saldırılar aslında çok yeni değildir. UNIX ve benzeri işletim sistemlerinde sahte kullanıcı giriş (login) ekranları ile kullanıcıların şifrelerini elde etmek mümkündür.

(a) Sahte UNIX/Linux kullanıcı girişi (b) Windows Ctrl+Alt+Del kullanıcı girişi

Şekil 5.2. İşletim sistemleri giriş ekranları

Şekil 5.2 (a)'da gösterildiği gibi, açık bir terminalde standart işletim sistemi kullanıcı girişi sayfasını aynı şekilde ekrana basan ve kullanıcıdan kullanıcı adı ve şifresini isteyen casus program, bu bilgileri aldıktan sonra kendini sonlandırıp, çalıştığı kullanıcı oturumundan çıkıp, standart kullanıcı girişi ekranını göstermektedir. Sahte olan ilk girişimde kullanıcının girdiği şifre, kullanıcıya kasten yanlış olarak sunulmaktadır. Kullanıcılar genelde şifre girerken kendilerine gösterilen bu hatayı doğru zannetmekte ve hatalı şifre girişi yaptığını düşünüp, ikinci deneme için kullanıcı bilgilerini tekrar girmektedir. İşte bu tip saldırıların önüne geçmek için işletim sistemleri, sistem girişini belirli bir tuş kombinasyonu ile çalıştırmaktadırlar.

Windows işletim sistemi Şekil 5.2 (b)'de gösterildiği gibi Ctrl+Alt+Del tuşlarına beraber basıldığında sistem girişi diyalogunu göstermektedir. Linux sistemlerinde de artık buna benzer bir uygulama bulunmaktadır ve bu uygulama "Güvenli Dikkat Tuşu" (SAK, Secure Attention Key) olarak adlandırılmaktadır ve genelde Ctrl+Alt+Pause tuşları bu iş için kullanılır. Windows işletim sistemindeki Ctrl+Alt+Del tuş kombinasyonu hiç bir uygulama tarafından yakalanamamaktadır. Bu yüzden bu tuşları kullanan kullanıcı, karşısına çıkan arayüzün gerçekten işletim sisteminin kendisine ait, güvenilir bir arayüz olduğundan emin olur.

Kullanıcı ile klavye arasında bulunan insan-makine arayüzünde gerçekleştirilen ortadaki adam saldırıları, klavye dinleme sistemi (keylogger) olarak adlandırılmaktadır. Temel işlevi açısından klavye dinleme sistemi, klavye kullanırken basılan tuş bilgilerini çeşitli yöntemlerle gizli bir şekilde yakalayan ve bunları bir yerde depolayıp yine kullanıcının bilgisi dışında başka kişilerin kullanımına sunan casus yazılım olarak tanımlanabilir. Tuş bilgilerini elde eden kişi, kullanıcının bilgisayarını kullanırken şifre ve önemli kişisel bilgiler dahil yazdığı her şeyi ele geçirmiş olacaktır. İngilizce keylogger (tuş kaydedici) veya keycatcher (tuş yakalayıcı, yazı yakalayıcı) olarak adlandırılan bu sistemler, "insanların bilgisayarlarına girdikleri gizli bilgilere erişmek için, parlak bir ajan olmaya hiç gerek yok" sözünü söyletecek kadar önemli etkileri olan casus yazılımlardır (68). Klavye dinleme sistemleri, iz sürme yazılımı (tracking software) ve faaliyet izleme sistemi (activity monitoring) olarak da sınıflandırılmaktadır. Klavye dinleme sistemlerinin son kabiliyetleri arasında "fare dinleme" olarak adlandırılabilecek, fare tıklama bilgilerini çeşitli amaçlarla inceleme yeteneğini de eklemek gerekir. Bunun dışında görsel gözetleme anlamında ekran görüntüsü alan klavye dinleme sistemleri bulunmakta; bu programlar bazı kaynaklarda "screen scraper" (ekran kazıyıcı) olarak da adlandırılmaktadır. Klavye dinleme sistemleri, tuş bilgilerini kullanarak bilgi edinme dışında; fare tıklamaları, ekran görüntüleri, pano değişimleri, İnternet ve bilgisayar kullanımı ile ilgili izleme gibi değişik yöntemleri de kendi içerisine dahil etmektedir. Yine bu bölümde gözler önüne serilebileceği gibi, klavye dinleme sistemlerinin kötü amaçlar dahilinde bir casus yazılım olarak kullanılmasının dışında;

faydalı amaçlara yönelik kullanım imkanlarının da bulunduğunu hemen başta ifade etmekte fayda vardır.

Bu açıdan bakıldığında, en genel anlamıyla klavye dinleme sistemleri, kullanıcının bilgisayar kullanırken sergilediği davranışlarını izlemek veya kişisel anlamda mahremiyet ve önem içeren hassas bilgiler de dahil olmak üzere, kullanıcı hakkında bilgi edinmek amacıyla kullanılan yazılım olarak tanımlanmalıdır.

Klavye dinleme sistemlerinin kullanım amacı ne olursa olsun, kurulduğu bilgisayar sistemlerine belirli bir zararının olmadığının da belirtilmesinde fayda vardır (69). Yani bilgisayar virüsleri, solucanları ve diğer bazı kötücül yazılımlar gibi; klavye dinleme sistemlerinin çalıştıkları sistemi yıkmak gibi bir amaçları bulunmaz. Aksine, işlerini mümkün olduğunca hissettirmeden yapmaya çalışırlar. Klavye dinleme sistemleri sadece çalıştıkları sistemin bellek, MİB (Merkezi İşlem Birimi, CPU) gibi kaynaklarını diğer programlarla paylaşırlar.

Klavye dinleme sistemlerini incelemeye başlamadan önce, klavyenin nasıl bir bilgisayar bileşeni olduğu ve sistem ile ilişkilerinin bilinmesi gereklidir. Takip eden kısımlarda bu temel bilgiler açıklanacaktır.

5.1. Klavye ve Çalışma Prensipleri

Bilgisayar klavyeleri, daktilo makinelerinden esinlenerek geliştirilen, bilgisayar girdi cihazlarıdır. En çok temasta bulunduğumuz bu cihaz, belki de üzerinde en az düşündüğümüz bir bilgisayar parçasıdır. MS-DOS gibi metin tabanlı işletim sistemlerinden, Windows, OS/2, MacOS ve Linux gibi grafik tabanlı işletim sistemlerine geçilmesi ile beraber tanıştığımız fare, klavyenin kullanımını azaltsa da yine de onun yerini tutabilecek bir bilgi girişi mekanizması henüz bulunmamaktadır.

(a) Standart

(b) Doğal

(c) Çoklu ortam

(d) Bilgisayar Korsanı

Resim 5.1. Klavye modelleri

PS/2 standardında bilgisayar klavyelerinin genel görünümü, ortaya çıktıktan sonra Resim 5.1'de görüldüğü gibi çok az değişmiştir. Yeni modeller genelde klavyeye yeni tuşlar ekleyerek, bazı işlerin daha kolay yerine getirecek ek işlev tuşlarını tanıtmaktadır. Resim 5.1 (d)'de görüldüğü gibi üzerinden yazıları silinmiş ve oldukça küçük boyutlu bir klavye türü, üretici firması tarafından, özellikle ileri kullanıcılar ve korsanlar için önerilmektedir. Böyle bir klavye, kullanımı çoğu kullanıcı için oldukça zor olsa da; girilen şifrenin başkaları tarafından bakarak anlaşılmasının zor olması açısından da güvenli bir model olarak adlandırılabilir (70). Değişik teknolojilerin uygulandığı diğer standartta klavye türleri için 7.2.1 kısmına bakınız.

Kullanılan alfabeye göre değişik düzenlerde olan klavyelerde, daktilo tuşları, nümerik bölüm tuşları, fonksiyon tuşları ve kontrol tuşları olmak üzere dört grup tuş bulunmaktadır.

(a) Tuş matrisi

(b) Lastik bombeli anahtarlar

Resim 5.2. Klavye yapıları

Klavyeler, Resim 5.2 (a)'da görülen tuş matrisi ile hangi tuşa basıldığını anlamakta ve Resim 5.2 (b)'de görülen anahtarlarla tuş basımı algılanmaktadır. Sağ üst tarafta görülen mikroişlemci ve kontrolör, tuş basımı bilgilerini derleyip ana karta iletmekle görevlidirler.

5.1.1. Kesmeler ve Windows tuş basımı mesajları

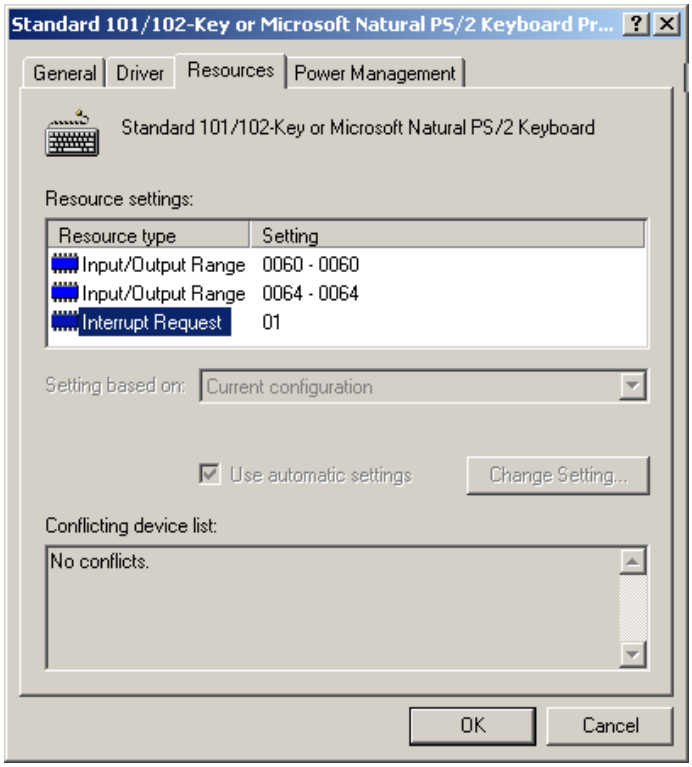
Donanım olarak çalışması bu şekilde özetlenen klavyelerde, tuş basımı bilgilerini işletim sistemine aktaran yazılım altyapısı da işletim sistemlerinin gelişmesi ile çeşitli değişiklikler göstermektedir. Örneğin MS-DOS tabanlı kişisel bilgisayarlarda BIOS kodu, düşük bellek kapasiteli bir makinenin hafızasında, kesme (interrupt) adı verilen hizmetler sunmaktadır.

Bir zamanlar oldukça güncel bir konu olan kesmeler, onaltılık kodları ile adlandırılmaktadır. Çizelge 5.1'de bir listesi verilen kesmelerden 9 numaralı kesme (IRQ1, Interrupt Request 1), klavyeden tuşa basıldığında sistemin ürettiği kesmedir. Bu kesmeyi yakalayan program, basılan tuş bilgilerini elde edebilir. Bu tip kesmeleri dinleyen TSR (Terminate and Stay Resident, Bitince Yerleşik Kalan) türünde programların yazılması ve sistemi etkilemeden çalışması oldukça güçtür.

Çizelge 5.1. Kesmeler (klavye ve fare kesmeleri yatık olarak belirtilmiştir.)

Adres	*Kesme No*	*Açıklama*
0	00	Sıfıra bölme
4	01	Tek adım
8	02	Maskelenemez kesme
C	03	Durma noktası (breakpoint)
10	04	Taşma
14	05	Ekran görüntüsü alma kesmesi
18	06	286 LoadAll işletici
1C	07	Ayrılmış
20	08	IRQ0 – Sistem Zamanlayıcı Kesmesi
24	*09*	*IRQ1 – Klavye Kesmesi*
28	0A	IRQ2 - Ayrılmış
2C	0B	IRQ3 - COM2: Kesme
30	0C	IRQ4 - COM1: Kesme
34	0D	IRQ5 - LPT2: Kesme
38	0E	IRQ6 – Disket Sürücü Kesmesi
3C	0F	IRQ7 - LPT1: Kesme
1C0	70	IRQ8 – Gerçek zamanlı saat kesmesi
1C4	71	IRQ9 - IRQ2 tekrar yönlendirme
1C8	72	IRQ10 - Ayrılmış
1CC	73	IRQ11 – Ayrılmış
1D0	*74*	*IRQ12 - Kullanılır/PS/2 Fare*
1D4	75	IRQ13 - Matematik yardımcı işlemci
1D8	76	IRQ14 – Ana IDE HDD
1DC	77	IRQ15 - Kullanılır/İkincil IDE HDD

Windows işletim sistemi ile beraber bir çok kesmenin yerini, daha yüksek bir soyut katman sağlayan olay (event) mekanizması almıştır. Şekil 5.3'de klavye kesmesi, işletim sisteminde bir kaynak olarak gösterilmekteyse de; sistem, klavye ve fare ile ilgili kesmeleri dinlemeye karşı kilitlenmektedir. Dolayısıyla Windows işletim sisteminde bir tuşa basıldığında elde edilen bir klavye kesmesi değil bir klavye olayıdır.

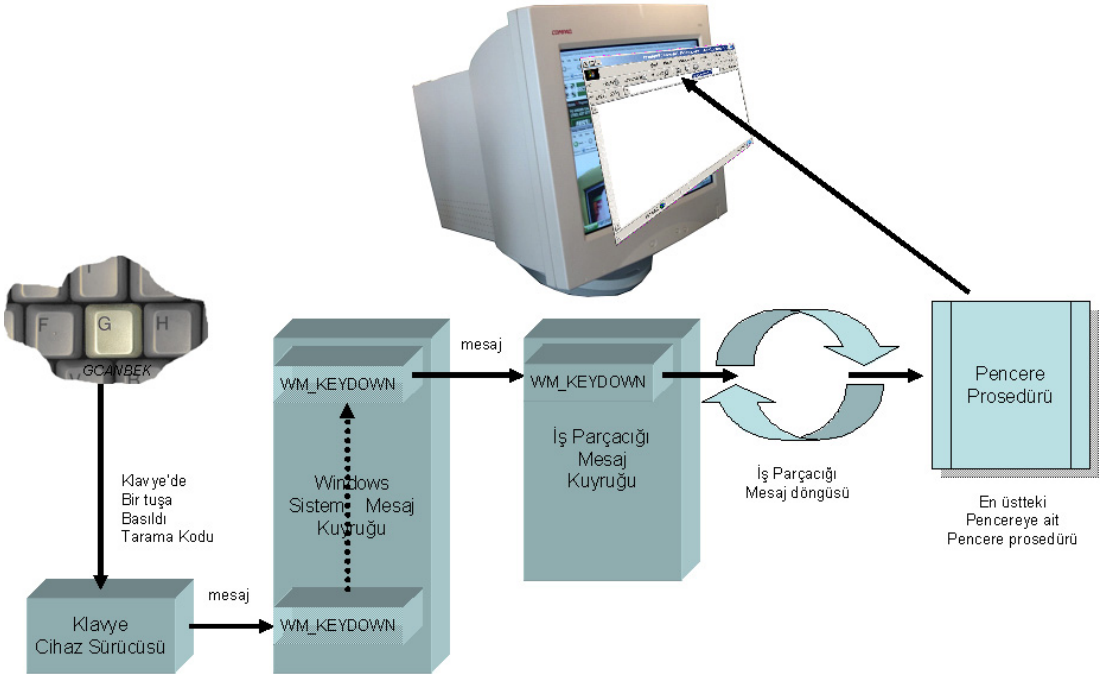


Şekil 5.3. Windows 2000 işletim sisteminde IRQ1 klavye kesmesi

Windows işletim sisteminde klavye çalışma prensibi MS-DOS işletim sistemine göre tamamen farklı bir yapıya dönüştürülmüştür. Windows işletim sisteminde kullanılan bu yapının çalışma prensibi Şekil 5.4'de verilmiştir.

Kullanıcı klavyede herhangi bir tuşa bastığında (keystroke), işletim sisteminin klavye sürücüsü bu tuş basımını WM_KEYDOWN adında bir mesaja paketler. Bu mesaj, sistemin mesaj kuyruğuna atılır. İşletim sistemi, sistem kuyruğundan sırası geldiğinde bu mesajı alır ve o an ekranda en üstte olan odaklanmış pencereye ait uygulamanın iş parçacığı (thread) mesaj kuyruğuna, bu mesajı atar. İş parçacığı mesaj kuyruğunu işleyen, iş parçacığının mesaj döngüsü sürekli olarak bu kuyruktaki mesajları inceler. Mesaj, kuyruktan alınıp, ekranda en üstte duran pencerenin pencere prosedürünü gönderilir.

Bu tür çalışma biçimi fare mesajı gibi bir çok olayda bu yapıya benzer bir şekilde çalışmaktadır.



Şekil 5.4. Windows mesaj kuyruğundan tuş basımı bilgisinin uygulamaya aktarılması

Tuş basımı bilgisi taşıyan Windows mesajları,

- WM_KEYDOWN: Sistem tuşu olmayan bir tuş basılı durumda
- WM_KEYUP: Sistem tuşu olmayan basılı bir tuş bırakıldığında
- WM_SYSKEYDOWN: Menü çubuğunu etkinleştiren F10 tuşuna veya Alt (alternatif) tuşu ile beraber bir başka tuşun basılı olduğu durumda
- WM_SYSKEYUP: Alt (alternatif) tuşu ile beraber basılı olan bir tuşun bırakıldığı durumda

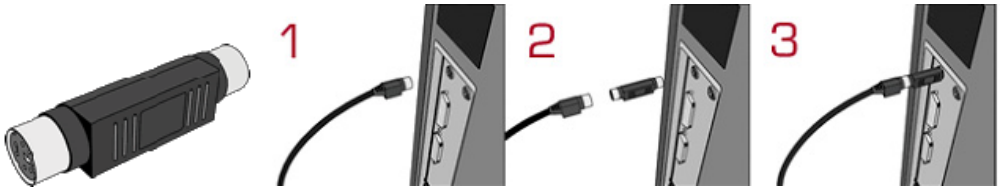
oluşturulmaktadır. Tuş basım bilgileri ile ilgili ayrıntılı bilgi klavye çengelleri bölümünde anlatılacaktır.

5.2. Klavye Dinleme Sistemi Türleri

Klavye dinleme sistemleri, yazılım ve donanım klavye dinleme sistemleri olmak üzere iki grupta toplanmaktadır. Bu iki grup, yeni başlıklar altında takip eden kısımlarda incelenmiştir.

5.3. Donanım Klavye Dinleme Sistemleri

Donanım klavye dinleme sistemleri klavye ile klavye kapısı arasındaki uygun kısımlara takılan cihazlardır. Şekil 5.5 (a) ve Şekil 5.5 (f) ile Resim 5.3 (a) ve (b)'de donanım klavye dinleme sistemleri gösterilmektedir. Şekil 5.5 (a)'da gösterilen donanım klavye dinleme cihazının bir bilgisayara kurulma aşamaları Şekil 5.5 (b), (c) ve (d) 'de verilmiştir. Çoğu donanım klavye dinleme sistemi Şekil 5.5'de gösterildiği gibi klavye kablosunun ucuna takılırken; bazı türleri de bilgisayar kasasının içine, klavye kapısına ve doğrudan klavyenin içine yerleşebilmektedir. Klavye kablosunun ucuna takılan cihazların rengi klavye kablosunun renginde seçilebilmektedir. Zaten bilgisayar kasasının arka kısmı fazla incelenmediği gibi; cihazın da aynı renkte olması, dikkat çekmesini de önleyebilir. Kasa veya klavye içine yerleştirilen türler ise, ancak kasa veya klavye açıldığında fark edilebilir. Bu açıdan bakıldığında donanım klavye dinleme sistemlerinin saptanması oldukça düşüktür. Kalıcı klavye dinleme sisteminin yerleştirildiği ve tamamen normal klavye işlevini gören klavyeler bile satılmaktadır (71).

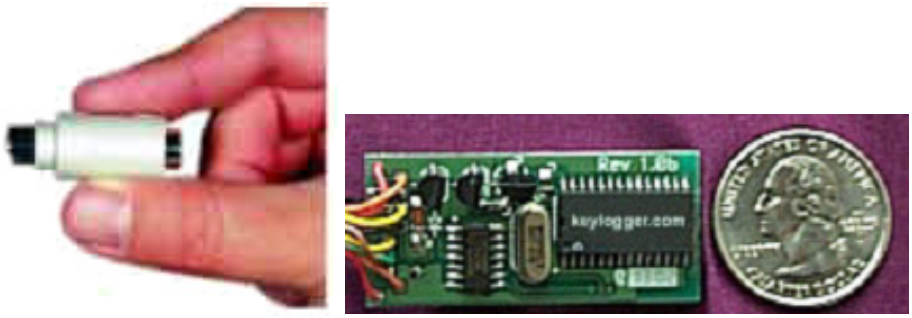


(a) (b) (c) (d)

(e) (f)

Şekil 5.5. Donanım klavye dinleme sistemlerinin bilgisayara kurulması

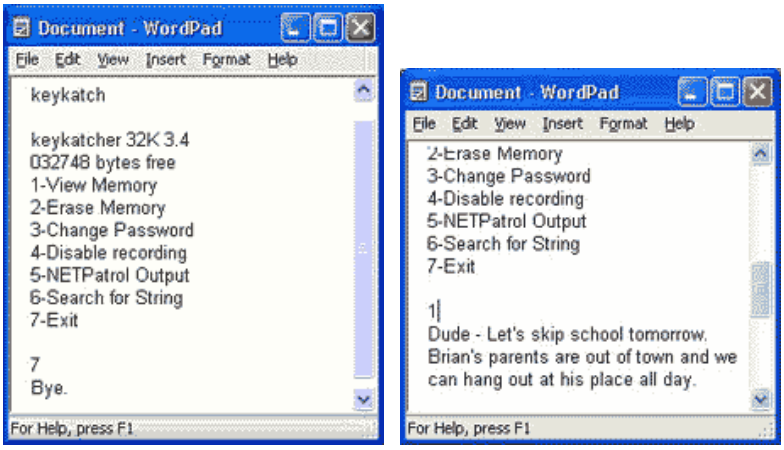
Donanım klavye dinleme cihazlarının boyutları, Resim 5.3'de görüldüğü gibi çok küçüktür. Piyasada bir çok çeşidi bulunan bu cihazlar, içlerinde taşıdıkları bellek kapasitesine göre, çok fazla sayıda tuş basımı bilgisini depolayabilirler. Genelde 32, 64 ve 128 KB kapasiteye sahip donanım klavye dinleme sistemleri, örneğin 128 KB kapasiteli bellek ile, 131 000 adet tuş basımı bilgisini tutabilirler. 1 MB ve 2 MB kapasiteli modeller de bulunmaktadır (72).



(a) (b)

Resim 5.3. Donanım klavye dinleme sistemlerinin küçük boyutları (72, 73)

Piyasada satılan bu cihazların fiyatları ise 50 ile 150$ arasında değişmektedir. Donanım olarak gerçekleştirildiklerinden oldukça hızlı çalışan bu cihazlar, saniyede 450 karakter kadar tuş basım bilgisini yakalayabilmektedirler. PS/2 standardında bütün IBM uyumlu kişisel bilgisayarlarda çalışan bu donanımların kurulumları oldukça kolaydır. Bu sistemlerin en önemli özelliklerinden biri de, hemen hemen bütün işletim sistemlerinde çalışabilmesi ve her hangi bir yazılıma veya sürücüye ihtiyaç duymamalarıdır. Basılan tuş bilgileri, kaynak bilgisayardan cihaz bilgisayara takılıyken alınabileceği gibi; buradan çıkartılarak, başka bir bilgisayarda da aynı işlem yapılabilmektedir. Kayıtlar, dosya olarak bilgisayarda tutulmamaktadır. Sistem kaynaklarını hiç kullanmadıklarından, sistemi yavaşlatmaz veya bozmazlar. Sistem çökmelerinden de etkilenmezler. Donanım seviyesinde çalıştığından, casus savar yazılım ve klavye dinleme önleme sistemleri tarafından saptanmaları ve etkisiz hale getirilmeleri imkansızdır. Bu donanımların bazı modellerinde, saklanan veriler şifrelenebilmektedir. Cihazın başkalarının eline geçmesi durumunda içeriğinin anlaşılamaması, bu tür cihazların kullanımını güvenlik açısından daha da cazip hale getirmektedir.



(a) Örnek menü (b) Örnek kayıt görüntüleme

Şekil 5.6. Donanım klavye dinleme sistemi menü örnekleri (Keycatcher (67))

Donanım klavye dinleme sisteminin kurulduğu, takıldığı veya kullanıldığı sistemlerde genellikle kullanıcının klavyeden tuşladığı bir şifre, Şekil 5.6'da gösterildiği gibi, Notepad veya Wordpad gibi bir metin editöründe girilir. Bunu yakalayan sistem açılan editöre sistem bilgisini ve kullanıcının etkileşim göstereceği menüyü yazar. Kullanıcı menü numaralarını tuşlayarak örneğin cihazın belleğinde yer alan tuş basım bilgilerini görebilir; kayıtları silebilir; şifre değişikliği yapabilir; kayıt almayı durdurabilir ve kayıt içinde özel aramalar yapabilir.

Yukarıda özetlendiği gibi çok tehlikeli güvenlik açıkları oluşturabilecek özelliklere sahip olan donanım klavye dinleme sistemlerine karşı, kişi ve kuruluşların dikkatli olması gerekmektedir. Özellikle düzenli aralıklarla bilgisayar kasasının arkası, içi ve klavyenin içi kontrol edilmelidir. Bu sistemlerden korunmanın yolu bugün için zor gibi görünse de donanım olarak da önleme sistemleri geliştirilinceye kadar alınabilecek tek önlemin bu olacağını hatırlatmakta fayda vardır.

5.4. Yazılım Klavye Dinleme Sistemleri

Yazılım klavye dinleme sistemleri, işletim sistemine klavyeden gelen tuş basım bilgilerini elde edip, bunları diskte veya başka bir ortamda depolayan casus yazılımlardır. Yukarıda belirtildiği gibi tuş basımı bilgileri, MS-DOS tabanlı işletim

sistemlerinde kesme olarak; Windows işletim sisteminde ise mesaj olarak üretilmektedir. Windows işletim sisteminde klavye cihaz sürücüsü, klavyeden gelen tarama kodunu, ilgili tuş basımı mesajına çevirir. İşte bu noktada çeşitli yazılım yöntemleri ile üretilen tuş basımı bilgisini elde etmek mümkündür.

Windows işletim sisteminde, yazılım klavye dinleme sistemi gerçekleştirmek için,

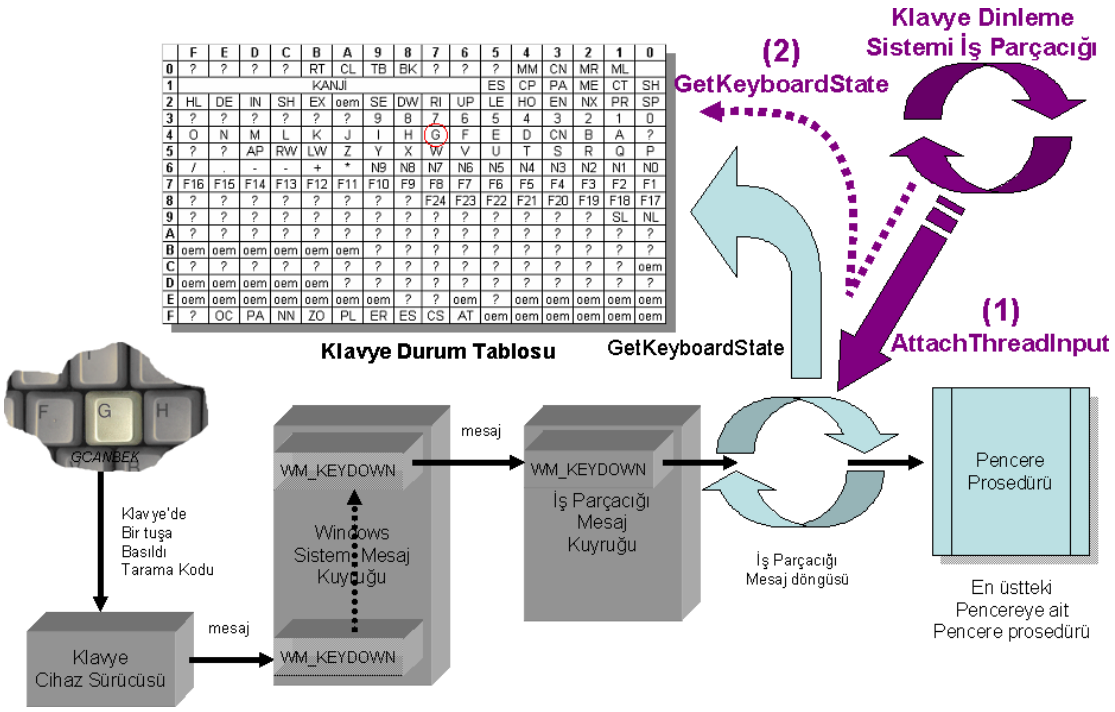
- Klavye durum tablosu yöntemi
- Windows klavye çengeli yöntemi
- Çekirdek tabanlı klavye süzgeç sürücüsü

gibi bilinen üç yöntem kullanılmaktadır. Bu yöntemlerin özellikleri aşağıdaki kısımda incelenmektedir.

5.4.1. Klavye durum tablosu yöntemi

Bazı durumlarda geliştirilen bir uygulama, klavyeden gelen bir tuş basımı mesajını işlerken, o mesajı üreten tuş dışında diğer tuşların durumunu da öğrenmeye ihtiyaç duyabilir. Örneğin, bir metin düzenleme uygulamasında, kullanıcı imlecin bulunduğu noktadan bütün metnin sonuna kadar var olan içeriği seçmek için, Ctrl ve Shift tuşlarına basılı iken End (sona) tuşuna basması isteniyorsa; End tuşuna basılma mesajı geldiğinde, Ctrl ve Shift tuşlarına basılı olup olunmadığının bilinmesi gerekmektedir. Windows işletim sisteminde, her tuş basımı mesajı üretildiğinde, 256 adet olan bütün sanal tuşların basım bilgisi bir klavye durum tablosunda tutulmaktadır. Bu tablonun tamamının içeriği GetKeyboardState ile; sadece merak edilen bir tuşun içeriği ise GetAsyncKeyState fonksiyonu ile elde edilmektedir. Uygulamalar her hangi bir tuşun ismini, klavye cihaz sürücüsünden GetKeyNameText fonksiyonu ile elde edebilirler.

Bir klavye dinleme sistemi, Şekil 5.7’de gösterildiği gibi klavye durum tablosunu inceleyerek tuş basım bilgilerini elde edebilir.



Şekil 5.7. Klavye durum tablosu kullanılarak klavye dinleme

GetKeyboardState fonksiyonunun imzası (function signature),

```
BOOL GetKeyboardState(
        PBYTE lpKeyState   // durum verilerini almaya yarayan diziye işaretçi
);
```

şeklinde tanımlanmaktadır.

Farklı iş parçacıklarında oluşturulan pencereler, klavye ve fare gibi girdileri, normal olarak birbirlerinden bağımsız işlemektedirler. Yani, her bir pencere kendi girdi durumlarına sahiptir. Bu girdi durumları, odaklanan, etkin ve yakalama pencereleri, kuyruk durumu ve tuş durumu gibi bilgilerdir. Bu bilgiler, diğer iş parçacıklarıyla eş zamanlı değildirler. Bu yüzden, tuş durum tablosu yöntemiyle sistemde girilen tuş bilgilerini almak için klavye dinleme sisteminin dahilindeki bir iş parçacığı, o an en üstte olan ve bundan dolayı klavyeden girilen mesajları işleyen iş parçacığının girdi sistemine kendini dahil etmelidir. Bunun için Şekil 5.7'de görüldüğü gibi klavye dinleme sistemi iş parçacığı, o an klavye bilgilerini alan iş parçacığını bulup, onun

girdi sistemine AttachThreadInput fonksiyonu ile dahil olur. Bu durumda artık GetKeyboardState fonksiyonu ile etkin pencereye ait iş parçacığının işlediği klavye tablosu okunarak, o an basılı olan tuş bilgisine erişilir. Bu fonksiyonunun imzası,

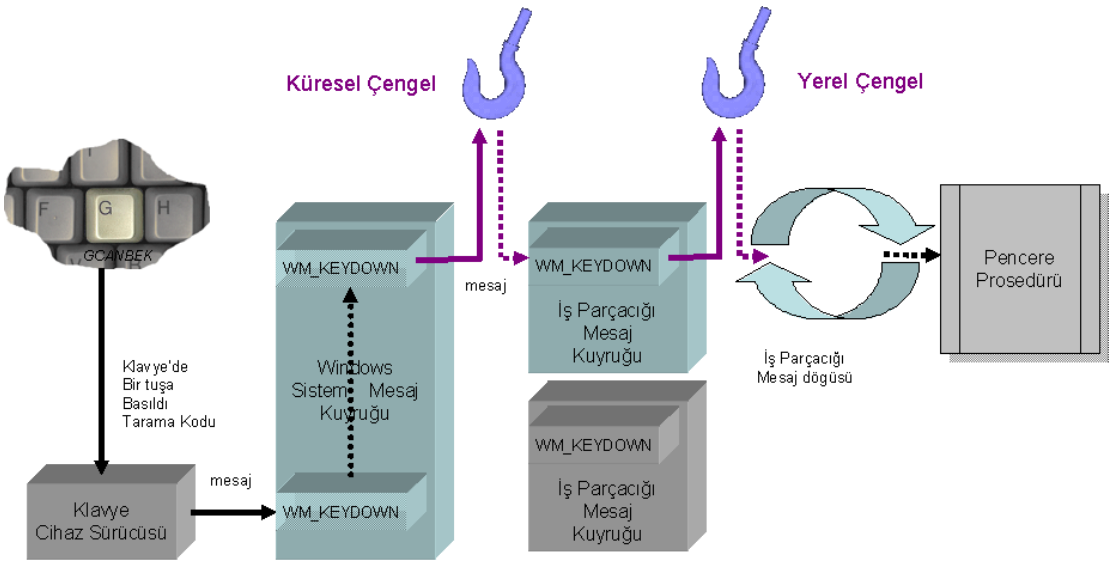
```
BOOL AttachThreadInput(
        DWORD idAttach,         // dahil olacak iş parçacığı
        DWORD idAttachTo,       // dahil olunacak iş parçacığı
        BOOL fAttach            // dahil ol (TRUE) veya ayrıl (FALSE)
);
```

şeklinde tanımlanmaktadır.

5.4.2. Windows klavye çengeli yöntemi

Microsoft İşletim sisteminde bir çok işlem, mesaj trafiği ile halledilmektedir. Bir pencere açılırken, açık bir pencere simge durumuna küçültülürken, bir düğmeye tıklandığında, fare ekranda hareket ederken ve klavyede her hangi bir tuşa basıldığında, basılı tutulduğunda ve bırakıldığında, sistem, gerçekleştirilen işleme özgü bir mesaj üretir. Bu mesajı alan proses onu işler. Şekil 5.8'de gösterildiği gibi, örneğin WM_LBUTTONDOWN mesajı alan bir pencere, buradan pencere üzerinde farenin sol tuşuna basıldığını anlar. Bu mesajı alan etkin uygulama, programın işlevine göre gereken işlemleri yapar. Sistemde tanımlı onlarca mesaj bulunmaktadır. Bunun yanında kullanıcı tanımlı mesajlar da üretebilmek mümkündür.

Kullanıcı ile etkileşimi sağlayan; klavyede bir tuşa basma ve fare kullanımı ile ilgili işlemlere ait mesajlar o an etkin olan ya da, bir fare tıklamasında olduğu gibi, farenin tıklandığında etkin olacak olan, kullanıcı proseslerine iletir. Bu mesaj başka bir pencereye veya prosese normalde aktarılmaz.



Şekil 5.8. Windows klavye çengeli yöntemi

Bu mesajlaşma trafiğinde araya girmek isteyen prosesler için, işletim sistemi tarafından sunulan mekanizmaların en başında geleni çengellerdir (hook). Çengel, sistem mesaj işleme mekanizmasında özel bir nokta olarak tanımlanmaktadır. Herhangi bir Windows uygulaması bu noktaya bir altyordam kurarak ("çengel atarak"), bütün sistem çapında gerçekleşen mesaj trafiğini izleyebilir veya belirli türlerdeki mesajları, normalde mesajın gideceği hedefte bulunan pencereye ulaşmadan önce işleyebilir. İşte bu bölümde, klavye dinleme sistemlerinde etkin bir şekilde Windows işletim sisteminde kullanılan çengeller tanıtılacak ve Win32 tabanlı uygulamalarda çengel kullanımının nasıl olacağından bahsedilecektir.

Çengeller, mesaj trafiğinde bir nöbetçi gibi çalışmaktadırlar. Getirdiği avantajlarının yanında sistemin her bir mesajı işlemek için gerekli olan süreyi ve işlem yükünü arttırdığından sistemde yavaşlamaya sebep olmaktadır. Bu düz yolda taşıtların bir yerden bir yere giderken, yapılan bir değişiklikle yol üzerine kurulan bir denetleme noktasında, gelen her taşıtın tek bir şerit üzerinde incelenmesine benzetilebilir. Böyle bir durumda taşıtların hızı azalacak ve denetleme için de ek bir düzenlemeye ihtiyaç duyulacaktır. Bu açıdan bakıldığında Windows çengelleri, sadece gerekli durumlarda kullanılmalı ve eğer kullanıma devam etmeye gerek yoksa kurulan çengel sistemden çıkarılmalıdır. Takip eden kısımlarda çengellerle ilgili çengel zincirleri ve

prosedürleri ayrıntılı olarak açıklanacaktır. Bu kısımda anlatılan bilgiler için Microsoft'un Windows işletim sistemine ve bu sistemde çalışan uygulamalara yönelik resmi kaynağı MSDN (Microsoft Developer Network) kütüphanesinden yararlanılmıştır (74). Çengel zincirlerinin ve prosedürlerinin kullanımı ve en temel çengel fonksiyonlarından, çengeli kuran SetWindowsHookEx fonksiyonu; çengel zincirinde bir sonraki çengeli çağıran CallNextHookEx fonksiyonu ve çengeli sistemden koparan UnhookWindowsHookEx fonksiyonu aşağıda ayrıntılı olarak açıklanmıştır.

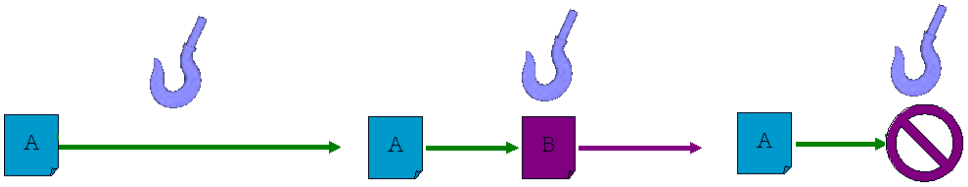
Çengel Zincirleri

Windows işletim sistemi, değişik türlerde bir çok çengeli destekleyecek şekilde tasarlanmıştır. Bu çengellerin her biri, farklı mesaj işleme mekanizmalarına erişime olanak tanımaktadır. Örneğin WH_MOUSE olarak (WH: Windows Hook) adlandırılan bir çengel, sadece fare mesajlarının oluşturduğu trafiği izlemek için kullanılabilir.

Sistem her bir türde çengel için ayrı birer çengel zinciri sunar. Çengel zinciri basit olarak bir işaretçi (pointer) listesinden oluşmaktadır. Bu listede yer alan işaretçiler, özel "uygulama tanımlı" geri çağırma (callback) fonksiyonlarının adreslerini işaret etmektedirler. Çengel zincirine kaydedilen geri çağırma fonksiyonları, çengel prosedürleri olarak adlandırılmaktadır. Belirli bir türde mesajla ilgilenen uygulama, kendisini o türe ait çengel zincirine ekler ve çengel zincirinde yer alan ve kendisi için belirlenmiş çengel prosedürünün adresini, kendi geri çağırma fonksiyonunun adresi olarak atar. Bu şekilde bu türde bir mesaj oluştuğunda, sistem bu mesajı çengel zincirinde yer alan her bir çengel prosedürüne sırası ile iletir. Mesajı alan her bir çengel prosedürü, bu durumda Şekil 5.9'da gösterildiği gibi üç şey yapabilir:

- Dinleme: Sadece gelen mesajı okur ve mesajı çengel zincirinde bir sonraki çengele iletir. Şekil 5.9 (a)'da bu durum gösterilmektedir.
- Değiştirme: Gelen mesajı okur ve üzerinde değişiklik yapıp çengel zincirinde bir sonraki çengele iletir. Şekil 5.9 (b)'de bu durum gösterilmektedir.

- Kesme: Gelen mesajı okur ve çengel zincirinde sıradaki çengele mesajı aktarmayarak mesajı engeller. Şekil 5.9 (c)'de bu durum gösterilmektedir.



(a) dinleme (b) değiştirme (c) kesme

Şekil 5.9. Çengel zincirinde mesajların çengel prosedürü ile işlenmesi

Çengel Prosedürleri

Belirli bir türde mesajlarla ilgilenen bir çengel geliştirmek isteyen kişilerin yapması gereken işlerin başında, çengel zincirine dahil edilecek bir çengel prosedürü sağlamak gelmektedir. Geri çağırma fonksiyonu (CALLBACK) şeklinde tanımlanan fonksiyonun imzası aşağıdaki şekilde olmak zorundadır:

```
LRESULT CALLBACK HookProc(
        int nCode,          // Çengel kodu
        WPARAM wParam,      // Çengel türüne bağlı 1. parametre
        LPARAM lParam       // Çengel türüne bağlı 2. parametre
);
```

Bu fonksiyonda; HookProc, çengel prosedürünün kullanıcı tarafından belirlenen ismini ifade etmektedir. nCode, hook prosedürün ne gibi bir işlem icra edeceğini belirleyen bir koddur. Her bir çengel türüne göre nCode değişik anlam ifade eder. wParam ve lParam parametrelerin anlamı da nCode'a göre belirlenmektedir.

Hazırlanan bu prosedür, SetWindowsHookEx adında bir API fonksiyonu ile çengel zincirine dahil edilir. SetWindowsHookEx fonksiyonu belirtilen her bir çengeli, çengel zincirinin en başına kurmaktadır. Belirli bir çengel türünde izlenen bir olay (event) meydana geldiğinde, sistem o çengel türü ile ilişkili çengel zincirinde bulunan ilk çengelin prosedürünü çağırır. Zincirde bulunan her bir çengel prosedürü

olayı bir sonraki prosedüre iletip iletmemeye kendisi karar verir. Herhangi bir çengel prosedürü kendisine gelen bir olayı sıradaki bir sonraki prosedüre CallNextHookEx adında bir fonksiyonu çağırarak iletir.

Bu arada, bazı çengel türleri için çengeller sadece mesajları izleyebilmektedir. Sistem, mesajı zincirindeki her bir çengel prosedürüne, CallNextHookEx çağrımı yapılsın ya da yapılmasın iletmektedir. Bir çengel prosedürü, faaliyet alanları,

- Küresel (Sistem) çengel prosedürü
- Yerel (İş Parçacığı (Thread)) çengel prosedürü

olmak üzere iki şekilde gerçekleşmektedir.

Küresel çengel prosedürleri, sistemde çalışan bütün iş parçacıkları için geçerli olan mesajları izleyebilir. Yerel çengel prosedürü ise sadece belirli bir iş parçacığı için geçerli olan mesajlarla ilgilenmektedir. Küresel çengel prosedürü herhangi bir uygulama bağlamında çağrılabileceğinden; bu prosedürler ayrı birer dinamik bağlantı kütüphanesi (DLL, Dynamic Link Library) modülünde tanımlanmalıdır. Yerel çengel prosedürleri, ilgilenilen iş parçacığı, uygulama ile aynı iş parçacığı ise yine ayrı bir DLL'de tanımlanacağı gibi uygulamayla aynı modülde de belirtilebilir. Bunun dışındaki iş parçacıklarına özgü yerel çengel prosedürleri, yine ayrı bir DLL'de tanımlanmalıdır. Küresel çengel kullanımı, gerekmedikçe kullanılmamalıdır. Kullanılması şartsa, aynı türde çalışan diğer çengel prosedürleri ile bir sorun yaşamayacak şekilde tasarım yapılmalıdır.

Klavye dinleme sistemlerinde kullanılan çengel prosedürleri genelde küresel olarak tanımlanmaktadır.

Çengel mekanizmasının işleyişini sağlayan üç ana fonksiyon olan, SetWindowsHookEx, CallNextHookEx ve UnhookWindowsHookEx fonksiyonları aşağıda sırası ile açıklanmaktadır.

SetWindowsHookEx

Belirli bir çengel türü için tanımlanan bir çengel prosedürü küresel veya yerel olarak SetWindowsHookEx API fonksiyonu ile çengel zincirine dahil edilir. Bu fonksiyon,

```
HHOOK SetWindowsHookEx(
        int idHook,             // kurulacak çengelin türü
        HOOKPROC lpfn,          // çengel prosedürünün adresi
        HINSTANCE hMod,         // uygulama kopyasının tanıtıcısı (handle)
        DWORD dwThreadId        // çengellenecek iş parçacığının numarası
);
```

şeklinde tanımlanmaktadır. Bu fonksiyonda;

idHook parametresi kurulan çengelin türünü belirtmektedir. Bu parametre aşağıda tanımlı değerlerden biri olabilir:

- WH_CALLWNDPROC (Pencere Prosedürü Çağrısı) (Yerel veya Küresel)
- WH_CALLWNDPROCRET (Pencere Prosedürü Çağrı Dönüşü) (Yerel veya Küresel)
- WH_CBT (Bilgisayar Tabanlı Eğitim) (Yerel veya Küresel)
- WH_DEBUG (Hata Ayıklama) (Yerel veya Küresel)
- WH_FOREGROUNDIDLE (Uygulama Ön Plan İş Parçacığı Boşta) (Yerel veya Küresel)
- WH_GETMESSAGE (Kuyruk Mesaj Alması) (Yerel veya Küresel)
- WH_JOURNALPLAYBACK (Günlük Tekrar Oynatma) (Sadece Küresel)
- WH_JOURNALRECORD (Günlük Kaydı) (Sadece Küresel)
- WH_KEYBOARD (Klavye) (Yerel veya Küresel)
- WH_KEYBOARD_LL (Alt Seviye Klavye) (Yerel veya Küresel)
- WH_MOUSE (Fare) (Yerel veya Küresel)
- WH_MOUSE_LL (Alt Seviye Fare) (Yerel veya Küresel)
- WH_MSGFILTER (Girdi Mesaj Filtresi) (Yerel veya Küresel)

- WH_SYSMSGFILTER (Sistem Girdi Mesaj Filtresi) (Sadece Küresel)
- WH_SHELL (Kabuk) (Yerel veya Küresel)

lpfn, çengel prosedürünün adresini belirten bir işaretçidir. Eğer dwThreadId parametresi sıfır ise veya farklı bir proses tarafından üretilen bir iş parçacığının kimlik numarasını belirtiyorsa; lpfn parametresi, bir DLL'de tanımlanan çengel prosedürünü işaret etmelidir. Diğer durumda geçerli proses ile ilişkilendirilmiş kaynak kod içinde ki bir çengel prosedürü işaret edilebilir. hMod parametresi, lpfn parametresi ile işaretlenen çengel zincirini içeren DLL modülü için tanımlı modül tanıtıcısıdır. Geçerli proses için tanımlanan çengeller için bu parametre NULL olmalıdır. dwThreadId, çengel prosedürün ilişkilendirildiği iş parçacığının kimlik numarasını belirler. Bu parametre sıfır olduğunda çengel prosedürü var olan bütün iş parçacıkları ile ilişkilendirilmiştir.

SetWindowsHookEx fonksiyonu başarı ile sonuçlanırsa çengel prosedürü tanıtıcısını döndürür; eğer başarısızlık olursa dönen değer NULL'dır. Hatanın neden kaynaklandığı GetLastError fonksiyonu ile belirlenebilir.

CallNextHookEx

Çengel prosedürünün içinde kullanılan bu API fonksiyonu, işlenen çengel türüne ilişkin kendisine iletilen çengel bilgisini, çengel zincirinde sırada bulunan bir sonraki çengele aktarır. Bir çengel prosedürü bu fonksiyonu, çengel bilgisini işlemeden önce veya işledikten sonra çağırabilir. Bu fonksiyonun imzası,

```
LRESULT CallNextHookEx(
        HHOOK hhk,          // geçerli çengelin tanıtıcısı
        int nCode,          // çengel prosedürüne iletilen çengel kodu
        WPARAM wParam,      // çengel prosedürüne iletilen 1. parametre
        LPARAM lParam       // çengel prosedürüne iletilen 2. parametre
);
```

şeklinde tanımlanmaktadır. Bu fonksiyonda; hhk, birinci parametre, çengel prosedürü SetWindowsHookEx ile kurulurken fonksiyondan dönen geçerli çengelin tanıtıcısını belirtir. Diğer bilgiler yine çengel prosedüründe tanımlanan parametrelerle aynıdır. Yukarıda belirtildiği gibi CallNextHookEx ile zincirde bir sonraki çengel prosedürüne mesajın iletilmesi isteğe bağlıdır. Fakat özellikle küresel çengel prosedürleri için doğabilecek bazı yan etkilerin önüne geçmek ve sistemin işleyişindeki bütünlüğü bozmamak için, bu fonksiyon tanımlanan çengel prosedüründe mutlaka bulunmalıdır.

UnhookWindowsHookEx

Çengel zincirini düzenlemede kullanılan üçüncü ve son fonksiyon UnhookWindowsHookEx API fonksiyonudur. Bu fonksiyon SetWindowsHookEx ile kurulan bir çengeli, çengel zincirinden çıkartır.

Bu fonksiyonun imzası ise,

```
BOOL UnhookWindowsHookEx(
        HHOOK hhk   // çıkartılacak çengel prosedürünün tanıtıcısı
);
```

şeklinde tanımlanmaktadır. Bu fonksiyonda; hhk, birinci parametre, çengel prosedürü SetWindowsHookEx ile kurulurken fonksiyondan dönen geçerli çengelin tanıtıcısını belirtir.

5.4.3. Çengel türleri

Windows işletim sisteminde tanımlı 15 çeşit çengel türü bulunmaktadır. Bu çengeller belirli amaçlarla ve belirli türde sistem mesajları ile ilgilenmek için tanımlanmaktadır. Aşağıda bu 15 çengel türü, bunlarla ilişkili yapılar (“struct”) ve çengel prosedürleri sırasıyla açıklanmaktadır.

1. Pencere prosedürü çağrısı ve çağrı dönüşü çengeli (WH_CALLWNDPROC, WH_CALLWNDPROCRET)

WH_CALLWNDPROC ve WH_CALLWNDPROCRET türünde çengeller, SendMessage fonksiyonu ile bir pencere prosedürüne gönderilen mesajları izlemeye olanak vermektedir. WH_CALLWNDPROC çengel prosedürleri, mesajı alacak pencere prosedüründen "önce" mesajı alırken; WH_CALLWNDPROCRET çengel prosedürleri, mesajı alan pencere prosedürü mesajı işledikten sonra devreye girmektedir. Bu çengel türüne ait çengel prosedürleri,

```
LRESULT CALLBACK CallWndProc(
        int nCode,          // çengel kodu
        WPARAM wParam,      // geçerli proses bayrağı
        LPARAM lParam       // mesaj verilerini içeren yapının adresi
);
```

şeklinde tanımlanmaktadır. Bu fonksiyonda; nCode, çengel kodu parametresi mesajı alan çengel prosedürünün mesajı işlemesi gerekip gerekmediğini belirlemektedir. Eğer bu parametre HC_ACTION ise çengel prosedürü mesajı işlemelidir. Eğer bu kod sıfırdan küçükse çengel prosedürü daha fazla işlem yapmadan mesajı CallNextHookEx fonksiyonu ile sıradaki çengel prosedürüne aktarıp; bu fonksiyondan dönen değeri geri döndürmelidir. wParam parametresi, mesajın geçerli iş parçacığından gelip gelmediğini belirlemektedir. Eğer mesaj geçerli iş parçacığından geliyorsa, bu değer sıfırdan farklıdır; değilse sıfırdır. lParam parametresi ise mesaj hakkında bilgi içeren CWPSTRUCT yapısına bir işaretçidir. Bu yapı aşağıdaki şekilde tanımlanmaktadır:

```
typedef struct tagCWPSTRUCT {    // cwps
        LPARAM lParam;           // Mesaj değerine bağlı ilave 1. bilgi
        WPARAM wParam;           // Mesaj değerine bağlı ilave 2. bilgi
        UINT message;            // Mesaj
        HWND hwnd;               // Mesajı alan pencerenin tanıtıcısı
} CWPSTRUCT;
```

Aynı şekilde pencere prosedürü kendisine gelen bir mesajı işledikten sonra çağırılan WH_CALLWNDPROCRET türünde çengel için tanımlı çengel prosedürü CallWndRetProc olarak belirtilir ve imzası CallWndProc ile aynıdır. İşlenen mesaj bilgisine dair yapı ise CWPRETSTRUCT olarak adlandırılır ve içeriği CWPSTRUCT ile aynıdır.

2. Bilgisayar tabanlı eğitim çengeli (WH_CBT)

WH_CBT çengelinin asıl amacı bilgisayar tabanlı eğitim (CBT, Computer-Based Training) uygulamalarıdır. Bu çengel için sistem, bir WH_CBT çengel prosedürünü,

- Bir pencere oluşturulmadan, etkinleşmeden, simge durumuna küçültülmeden, ekranı kaplar hale getirilmeden, genişliği değiştirilmeden ve yok edilmeden önce
- Bir sistem komutu bitirilmeden önce
- Sistem mesaj kuyruğundan bir fare veya klavye olayı çıkarılmadan önce
- Girdi odağını atamadan önce
- Sistem mesaj kuyruğu ile eş zamanlaştırmadan önce

çağırmaktadır.

Bu çengel prosedüründen dönen değer, yukarıda bahsedilen işlemlere izin verilip verilmediğini belirlemektedir.

Bu çengel türü için kullanılan CBTProc çengel prosedürü, aşağıdaki gibi tanımlanmaktadır:

```
LRESULT CALLBACK CBTProc(
        int nCode,              // çengel kodu
        WPARAM wParam,  // çengel koduna göre değişen 1. parametre
        LPARAM lParam       // çengel koduna göre değişen 2. parametre
);
```

Bu fonksiyona ilişkin çengel kodunun değerine göre, wParam ve lParam parametrelerinin ne tür değerler taşıdığı Çizelge 5.2'de gösterilmektedir.

Çizelge 5.2. CBTProc'a ait parametrelerin anlamları

Çengel Kodu	*Anlamı*	*wParam*	*lParam*
HCBT_ACTIVATE	Bir pencere etkinleşmek üzere	Pencerenin tanıtıcısı	CBTACTIVATESTRUCT yapısına bir işaretçi.
HCBT_CLICKSKIPPED	Sistem mesaj kuyruğundan bir fare mesajı çıkarılmak üzere	Fare mesajını tanımlar	MOUSEHOOKSTRUCT yapısına bir işaretçi
HCBT_CREATEWND	Bir pencere oluşturulmak üzere. Çengel prosedürü sıfırdan farklı bir değer döndürürse sistem pencereyi oluşturulmadan yok eder ve pencereyi oluşturan CreateWindow fonksiyonu NULL değer döndürür.	Yeni pencerenin tanıtıcısı	Pencerenin koordinatlarını ve büyüklüğünü de içeren CBT_CREATEWND yapısına bir işaretçi
HCBT_DESTROYWND	Bir pencere yok olmak üzere	Pencerenin tanıtıcısı	Tanımlı değil ve sıfır olarak atanmalı
HCBT_KEYSKIPPED	Sistem mesaj kuyruğundan bir klavye mesajı çıkarılmak üzere	Sanal tuş kodu	Tekrarlama sayısı, tarama kodu, tuş geçiş kodu, önceki tuş durumu ve bağlam kodunu içerir
HCBT_MINMAX	Bir pencere simge durumuna küçültülmek veya ekranı kaplar hale getirilmek üzere	Pencerenin tanıtıcısı	Düşük anlamlı kelimesinde yapılan işlemi belirleyen SW_ kodu bulunmaktadır.
HCBT_MOVESIZE	Bir pencere yer değiştirmek veya büyüklüğü değiştirilmek üzere	Pencerenin tanıtıcısı	Pencerenin koordinatlarını ve büyüklüğünü belirleyen RECT yapısına bir işaretçi
HCBT_QS	Sistem mesaj kuyruğundan WM_QUEUESYNC mesajı alındı	Tanımlı değil ve sıfır olarak atanmalı	Tanımlı değil ve sıfır olarak atanmalı
HCBT_SETFOCUS	Bir pencere klavye odağı almak üzere	Odağı alan pencerenin tanıtıcısı	Odağı kaybeden pencerenin tanıtıcısı
HCBT_SYSCOMMAND	Sistem komutu icra edilmek üzere	SC_ Sistem komutunu belirler	WM_SYSCOMMAND mesajının lParam değeri ile aynı veriyi içerir. Menü komutunda düşük anlamlı kelime imlecin x koordinatını; yüksek anlamlı kelime ise imlecin y koordinatını belirtir.

3. Hata ayıklama çengeli (WH_DEBUG)

İşletim sistemi, sistemde tanımlanan diğer türde her çengele ait çengel prosedürleri çağırılmadan, WH_DEBUG hata ayıklama çengel prosedürlerini çağırır. Bu çengeli diğer türde çengellerle ilişkilendirilmiş çengel prosedürlerinin sistem tarafından çağırılmasına izin verip vermemek için kullanmak mümkündür. Ayrıca çengellerle ilişkili hataları da tespit için kullanılabilir.

DebugProc olarak isimlendirilen hata ayıklama çengel prosedürünün imzası,

```
LRESULT CALLBACK DebugProc(
        int nCode,              // çengel kodu
        WPARAM wParam,  // çağırılacak çengelin türü
        LPARAM lParam       // hata ayıklama bilgisi içeren yapının adresi
);
```

şeklindedir. Bu fonksiyonda;

wParam parametresi, WH_CALLWNDPROC, WH_CALLWNDPROCRET, WH_CBT, WH_DEBUG, WH_FOREGROUNDIDLE, WH_GETMESSAGE, WH_JOURNALPLAYBACK, WH_JOURNALRECORD, WH_KEYBOARD, WH_KEYBOARD_LL, WH_MOUSE, WH_MOUSE_LL, WH_MSGFILTER, WH_SYSMSGFILTER ve WH_SHELL değerleri ile hata ayıklama yapılan çengelin türünü belirtir. lParam ile elde edilen yapı DEBUGHOOKINFO türündedir. Bu yapının elemanları,

```
typedef struct tagDEBUGHOOKINFO { // dh
        DWORD  idThread;   // Filtre fonksiyonunu içeren iş parçacığının tanıtıcısı
        DWORD  idThreadInstaller; // Filtre fonk. kuran iş parçacığının tanıtıcısı
        LPARAM lParam;              // DebugProc fonksiyonunun lParam değeri
        WPARAM wParam;          // DebugProc fonksiyonunun wParam değeri
        int    code;                    // DebugProc fonksiyonunun nCode değeri
} DEBUGHOOKINFO;
```

şeklinde tanımlanmaktadır.

4. Uygulama ön plan iş parçacığı boşta çengeli (WH_FOREGROUNDIDLE)

WH_FOREGROUNDIDLE çengeli ilişkilendirilen ön plan iş parçacığı boşta kaldığı (idle) zamanlarda düşük öncelikli görevler icra etmek amacıyla kullanılmaktadır. Çengel prosedürü ForegroundIdleProc olarak adlandırılmaktadır ve imzası aşağıdaki şekildedir:

```
DWORD CALLBACK ForegroundIdleProc (
        int code,               // çengel kodu
        DWORD wParam,     // kullanılmıyor
        LONG lParam         // kullanılmıyor
);
```

5. Kuyruk mesaj alması çengeli (WH_GETMESSAGE)

WH_GETMESSAGE çengeli GetMessage veya PeekMessage fonksiyonları tarafından döndürülmek üzere olan mesajları izlemek için kullanılabilir. Bu çengel ile mesaj kuyruğunu gönderilen klavye, fare ve diğer türdeki mesajlar izlenebilir. GetMsgProc olarak adlandırılan çember prosedürünün imzası aşağıdaki şekildedir:

```
LRESULT CALLBACK GetMsgProc(
        int code,               // çengel kodu
        WPARAM wParam,  // çıkarma bayrağı
        LPARAM lParam       // mesajla ilgili yapının adresi
);
```

wParam parametresi mesajın kuyruktan çıkarılıp çıkarılmadığını belirler. Bu parametre PM_NOREMOVE ise bir uygulamanın PeekMessage fonksiyonunu PM_NOREMOVE kullanarak kuyruktan mesajı çıkarmadığını belirtir. PM_REMOVE ise mesajın kuyruktan çıkarıldığını belirtir. lParam parametresi ise mesaj hakkında ayrıntılı bilgi içeren MSG yapısına bir işaretçidir. MSG yapısı,

```
typedef struct tagMSG {       // msg
        HWND hwnd;          // pencere prosedürü mesajı alan pencerenin tanıtıcısı
        UINT message;       // mesaj numarası
        WPARAM wParam;  // message değerine göre mesaj hakkında diğer bilgi
        LPARAM lParam;     // message değerine göre mesaj hakkında diğer bilgi
        DWORD time;         // mesajın postalandığı zaman
        POINT pt;       // mesaj postalandığında fare işaretçisinin ekran koordinatı
} MSG;
```

şeklinde tanımlanmaktadır.

6. Günlük tekrar oynatma çengeli (WH_JOURNALPLAYBACK)

WH_JOURNALPLAYBACK çengeli, sistem mesaj kuyruğuna mesaj eklemeye olanak verir. Bu çengel daha önce WH_JOURNALRECORD çengeli ile kaydedilmiş olan bir dizi fare ve klavye olaylarını tekrar oynatabilir. Her zamanki fare ve klavye girdileri bu çengel kurulu olduğu süreci etkin değildir. Bu çengel küresel bir çengeldir ve bir zaman aşımı değerini geri döndürür. Bu değer sisteme, tekrar oynatma çengelinden geçerli mesajı işlemeden önce ne kadar milisaniye beklemesi gerektiğini belirtir. Bu şekilde tekrar oynatma sırasında, olayların zamanlamasını ayarlamak mümkün olabilmektedir. Çengel prosedürü JournalPlaybackProc olarak adlandırılmaktadır. Bu prosedürün imzası aşağıdaki gibidir:

```
LRESULT CALLBACK JournalPlaybackProc(
        int code,           // çengel kodu
        WPARAM wParam,      // tanımlı değil
        LPARAM lParam       // işlenen mesajın adresi
);
```

nCode, çengel prosedürünün mesajı nasıl işleyeceğini belirlemek için kullanılmaktadır. Bu parametre aşağıdaki değerleri içerebilir:

- HC_GETNEXT: Çengel prosedürünün geçerli fare ve klavye mesajını lParam parametresi ile işaret edilen EVENTMSG yapısına kopyalaması gereklidir.
- HC_NOREMOVE: Bir uygulamanın PM_NOREMOVE ile PeekMessage fonksiyonunu çağırdığını gösterir.
- HC_SKIP: Çengel prosedürü, bir sonraki fare veya klavye mesajını lParam parametresi ile işaret edilen EVENTMSG yapısına kopyalamaya hazırlanmalıdır. HC_GETNEXT kodu alır almaz mesaj yapıya kopyalanmalıdır.

- HC_SYSMODALOFF: Sistem kipi (system modal) türünde bir diyalog kutusu yok edildi. Çengel prosedürü mesajları tekrar oynatmaya kaldığı yerden devam etmelidir.
- HC_SYSMODALON: Sistem kipi türünde bir diyalog kutusu gösteriliyor. Diyalog kutusu yok edilene kadar çengel prosedürü mesajları tekrar oynatmayı durdurmalıdır.

lParam parametresi, çengel prosedürü tarafından işlenmekte olan mesajı temsil eden bir EVENTMSG yapısına işaret etmektedir. Bu yapı aşağıda tanımlanmaktadır:

```
typedef struct tagEVENTMSG {      // em
        UINT  message;            // mesaj
        UINT  paramL;             // mesaja göre tanımlanan 1. ek bilgi
        UINT  paramH;             // mesaja göre tanımlanan 2. ek bilgi
        DWORD time;               // mesajın postalandığı zaman
        HWND  hwnd;               // mesajın postalandığı pencerenin tanıtıcısı
} EVENTMSG;
```

7. Günlük kaydı çengeli (WH_JOURNALRECORD)

WH_JOURNALRECORD çengeli girdi olaylarını izleme ve kaydetme imkanı vermektedir. Kaydedilen fare ve klavye olayları, yukarıda bahsedilen WH_JOURNALPLAYBACK çengeli ile yeniden oynatılabilir. Bu çengel küresel olarak tanımlanabilmektedir. JournalRecordProc olarak adlandırılan çengel yordamının imzası,

```
LRESULT CALLBACK JournalPlaybackProc(
        int code,              // çengel kodu
        WPARAM wParam,         // tanımlı değil
        LPARAM lParam          // işlenen mesajın adresi
);
```

şeklinde tanımlanmaktadır. Burada, code parametresi aşağıdaki değerlerden birini içerir:

- HC_ACTION: lParam parametresi sistem kuyruğundan çıkarılan bir mesaj hakkında bilgi içeren EVENTMSG yapısına işaret etmektedir. Çengel prosedürü yapının içeriğini bir tampon alana veya dosyaya kaydetmelidir.
- HC_SYSMODALOFF: Sistem kipi türünde bir diyalog kutusu yok edildiği anlamına gelmektedir. Çengel prosedürü kayıt işlemine kaldığı yerden devam etmelidir.
- HC_SYSMODALON: Sistem kipi türünde bir diyalog kutusunun gösterildiği anlamına gelmektedir. Diyalog kutusu yok edilene kadar çengel prosedürü kayıt işlemini durdurmalıdır.

8. Klavye çengeli (WH_KEYBOARD)

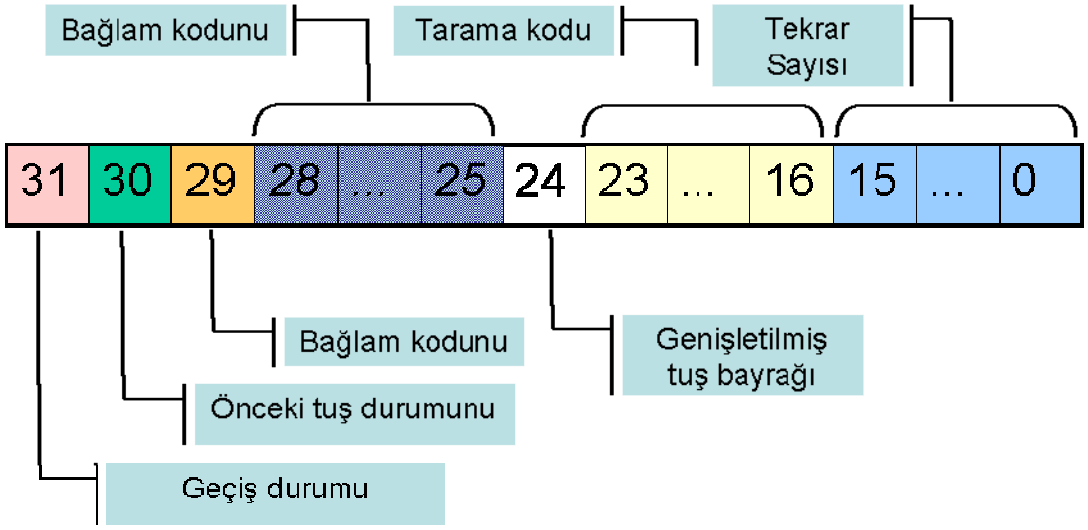
Klavye dinleme sistemlerinin en çok kullandığı çengel türlerinin başında gelen WH_KEYBOARD çengeli, GetMessage veya PeekMessage fonksiyonlarından döndürülmekte olan WM_KEYDOWN (Tuş Basıldı) ve WM_KEYUP (Tuş Bırakıldı) mesajlarının trafiğini izlemeye olanak vermektedir. Bu çengelin kullandığı çengel prosedürü KeyboardProc olarak adlandırılmaktadır. Bu prosedürün imzası,

```
LRESULT CALLBACK KeyboardProc(
        int code,           // çengel kodu
        WPARAM wParam,      // sanal tuş kodu
        LPARAM lParam       // tuş basımı mesaj bilgisi
);
```

şeklinde tanımlanmaktadır. Burada;

code parametresi, HC_ACTION değerine sahipse wParam ve lParam parametreleri bir tuş basımı mesajı hakkında bilgiler içermektedir. Bu parametre HC_NOREMOVE ise yine böyle bir durum mevcuttur; ama tuş basım mesajı mesaj kuyruğundan çıkarılmamıştır. Bu değer sıfırdan küçükse, çengel prosedürü mesajı

daha fazla işlemeden CallNextHookEx fonksiyonu ile bir sonraki çengel prosedürüne iletmelidir. wParam parametresi, tuş basım mesajını üreten tuşun sanal tuş kodunu belirtmektedir. Bütün sanal tuş kodları Ek-2'de verilmiştir. lParam parametresi ise tekrar sayısı, tarama kodu, genişletilmiş tuş bayrağı, bağlam kodu, önceki tuş durum bayrağı ve geçiş durumu bayrağını belirtmektedir. Şekil 5.10'da şematik olarak gösterilen bu parametre, aşağıdaki değerlerin birleşiminden oluşmaktadır. Rakamlar bit sırasını göstermektedir.



Şekil 5.10. Windows tuş basımı bilgisinin bit dizilimi

Bu bit dizilimlerin ne anlam ifade ettiği aşağıda açıklanmaktadır:

- 0-15 : Tekrar sayısı belirtilmektedir. Değeri, kullanıcının bir tuşu basılı tutması sonucunda tuş basımının kaç kere tekrar edildiğini göstermektedir.
- 16-23 : Tarama kodunu belirtmektedir. Değer orijinal malzeme üreticisine (OEM) göre değişmektedir.
- 24 : Fonksiyon tuşu veya nümerik alandaki bir tuş gibi tuşun genişletilmiş bir tuş olup olmadığını gösterir. Değer 1 ise tuş genişletilmiş tuştur.
- 25-28 : İlerisi için ayrılmış
- 29 : Bağlam kodunu belirtir. Değer 1 ise alternatif tuşu basılıdır; 0 ise değildir.

- 30 : Önceki tuş durumunu belirtir. Değer 1 ise mesaj gönderilmeden önce tuşun basılı olduğunu gösterir. Değer 0 ise tuş basılı değildir.
- 31 : Geçiş durumunu belirtir. Tuş basılıyorsa değer 0'dır; tuş bırakılıyorsa değer 1'dir.

Bir uygulama için kaynak kodda aşağıdaki sistem tanımlı sabit ifadeler kullanılarak, tuş basım bayraklarını daha kolay elde etmek mümkündür:

- KF_ALTDOWN: Alternatif tuşunun basılı olma bilgisi
- KF_DLGMODE: Bir diyalog kutusunun etkin olup olmadığını gösteren diyalog modu bayrağı
- KF_EXTENDED: Genişletilmiş tuş bayrağı
- KF_MENUMODE: Bir menünün etkin olup olmadığını gösteren menü modu bayrağı
- KF_REPEAT: Tekrar sayısı
- KF_UP: Geçiş durumu bayrağı

Yukarıdaki terimlerden tekrar sayısı, tarama kodu, genişletilmiş tuş bayrağı, bağlam kodu, önceki tuş durumu bayrağı ve geçiş durumu bayrağının ayrıntıları aşağıdaki paragraflarda açıklanmaktadır.

Tekrar sayısı: Bu değer, bir tuş basım mesajının birden fazla tuş basımını gösterip göstermediğini anlamak amacıyla kullanılır. İşletim sistemi, klavye bir uygulamanın kendisini işleyebilecek hızdan daha hızlı WM_KEYDOWN veya WM_SYSKEYDOWN mesajı ürettiğinde bu sayıyı artırmaktadır. Bu durum, çoğunlukla kullanıcının bir tuşu klavyenin otomatik tekrar etme özelliğini başlatmaya yetecek sürede basılı tutmasıyla oluşmaktadır. Sistem aynı tuş basım bilgisinin mesaj kuyruğuna her defasında atmak yerine, bu mesajlar tek bir mesaj olarak birleştirilir ve tekrar sayısı gerektiği kadar artırır. Bir tuş bırakıldığında otomatik tekrar etme özelliği başlamadığından WM_KEYUP ve WM_SYSKEYUP mesajları için tekrar sayısı her zaman 1'dir.

Tarama kodu: Donanım ile bağlantılı olan bu kod, var olan klavye donanımına göre kullanıcı bir tuşa bastığında üretilen koddur. Genelde bu kod uygulamalar tarafından ele alınmaz. Basılan tuş bilgisi için donanımdan bağımsız sanal tuş kodları kullanılır.

Genişletilmiş tuş bayrağı: Bu bayrak bir tuş basım bilgisinin, genişletilmiş klavyedeki ilave tuşların birinden kaynaklanıp kaynaklanmadığını belirtmektedir. Genişletilmiş tuşlar, klavyenin sağ tarafındaki Alt ve Ctrl tuşları; nümerik tuş bölümünün solunda yer alan Ins (araya ekleme), Del (silme), Home (başa), End (sona), Page Up (sayfa yukarı), Page Down (sayfa aşağı) ve ok tuşları; Num Lock (rakam kilidi), Break (Ctrl+Pause) (duraklatma), Print Scrn (ekran görüntüsü) tuşları; nümerik tuş bölümünde yer alan bölme (/) ve giriş (Enter) tuşlarıdır.

Bağlam kodu: Bu kod, tuş basımı mesajı üretildiğinde alternatif (Alt) tuşuna basılı olup olunmadığını göstermektedir. Kod 1 ise Alt tuşuna basılıdır.

Önceki tuş durumu bayrağı: Tuş basımı mesajını üreten tuşun, daha önce basılı olup olmadığı bu bayrak ile belirtilmektedir. Eğer bu tuş 1 ise tuş daha önce basılı durumdadır; 0 ise basılı değildir. Bu bayrak otomatik tekrar etme özelliği ile üretilen WM_KEYDOWN ve WM_SYSKEYDOWN tuş basımı mesajları için 1; WM_KEYUP ve WM_SYSKEYUP mesajları için 0'dır.

Geçiş durumu bayrağı: Tuş basımı mesajını üreten tuşun, basılır durumda mı olduğu yoksa bırakılır durumda mı olduğunu gösteren bir bayraktır. WM_KEYDOWN ve WM_SYSKEYDOWN mesajları için bu bayrak 0; WM_KEYUP ve WM_SYSKEYUP mesajları için 1'dir.

9. Alt seviye klavye çengeli (WH_KEYBOARD_LL)

Windows NT 4.0 Hizmet Paketi 3.0 ile beraber gelen WH_KEYBOARD_LL çengeli, bir iş parçacığının girdi kuyruğuna postalanan klavye girdi olaylarını izlemek amacıyla kullanılmaktadır. Çengel prosedürü LowLevelKeyboardProc olarak adlandırılmaktadır.

Sistem, bir iş parçacığının girdi kuyruğuna yeni bir klavye girdi olayı postalanmak üzere olduğunda LowLevelKeyboardProc fonksiyonu çağırmaktadır. Klavye girdisi yerel klavye sürücüsünden veya keybd_event fonksiyonundan gelebilir. Eğer girdi bir keybd_event çağrısından geliyorsa girdi "enjekte" edilmiştir. keybd_event fonksiyonu ile bir tuş basımını sentezlemek mümkündür. Bu şekilde sistem sentezlenmiş tuş basımı ile WM_KEYUP veya WM_KEYDOWM mesajları üretebilir. Klavye sürücüsünün kesme işleyicisi keybd_event fonksiyonunu çağırmaktadır. Bu fonksiyonun imzası,

```
VOID keybd_event(
        BYTE bVk,               // sanal tuş kodu
        BYTE bScan,             // donanım tarama kodu
        DWORD dwFlags,          // değişik fonksiyon seçenekleri için bayraklar
        DWORD dwExtraInfo       // tuş basımı ile ilişkili ilave veriler
);
```

şeklindedir. Burada;

dwFlags için KEYEVENTF_EXTENDEDKEY değeri tarama kodunun önünde 0xE0 (224) değerinde ön ek baytının olduğu belirtilir; KEYEVENTF_KEYUP değeri tuşun bırakıldığını gösterir. Bu fonksiyon kullanan bir uygulama, ekran görüntüsü alma tuşunun benzetimini ekran görüntüsünü alıp; panoya kaydetmek için kullanılabilir. Bunun için bVk parametresi VK_SNAPSHOT ve bScan parametresi bütün ekran görüntüsü için 0; etkin pencere için 1 olarak alınır.

LowLevelKeyboardProc çengel prosedürün imzası ise,

```
LRESULT CALLBACK LowLevelKeyboardProc(
        int nCode,              // çengel kodu
        WPARAM wParam,  // mesaj tanımlayıcı
        LPARAM lParam       // mesaj verileri yapısına işaretçi
);
```

şeklinde verilmektedir.

Burada nCode değeri HC_ACTION ise wParam ve lParam parametreleri bir klavye mesajı ile ilgili bilgiler içermektedir. wParam klavye mesajının türünü gösterir. Bu parametre WM_KEYDOWN, WM_KEYUP, WM_SYSKEYDOWN veya WM_SYSKEYUP değerlerini içerir. lParam ise KBDLLHOOKSTRUCT türünde bir yapıya işaretçidir. Bu yapı aşağıdaki şekilde tanımlanmaktadır:

```
typedef struct tagKBDLLHOOKSTRUCT {
        DWORD vkCode;           // sanal tuş kodu
        DWORD scanCode;         // tarama kodu
        DWORD flags;            // bayraklar
        DWORD time;             // bu mesaj için zaman damgası
        DWORD dwExtraInfo;      // sürücüden veya keybd_event'ten ilave bilgi
} KBDLLHOOKSTRUCT, FAR *LPKBDLLHOOKSTRUCT,
*PKBDLLHOOKSTRUCT;
```

Burada; flags değeri için 0. bit genişletilmiş tuşu (1: genişletilmiş; 0: değil); 1-3. bitler ayrılmış; 4. bit olayın enjekte olup olmadığı (1: enjekte); 5. bit bağlam kodunu (1: Alt tuşu basılı); 6. bit ayrılmış; 7. bit geçiş durumunu (0: tuş basıldı; 1: bırakıldı) anlamına gelmektedir. Bu değerleri elde etmek için LLKHF_EXTENDED, LLKHF_INJECTED, LLKHF_ALTDOWN ve LLKHF_UP değerleri kullanılabilir.

10. Fare çengeli (WH_MOUSE)

WH_MOUSE çengeli, GetMessage veya PeekMessage fonksiyonlarından döndürülmek üzere olan fare mesajlarını izlemek için kullanılmaktadır. Bu şekilde bir mesaj kuyruğuna postalanan fare girdileri izlenebilmektedir.

Bu çengelin çengel prosedürü MouseProc olarak adlandırılmaktadır ve böyle bir fonksiyonun imzası aşağıdaki gibidir:

```
LRESULT CALLBACK MouseProc(
        int nCode,              // çengel kodu
        WPARAM wParam,  // mesaj tanımlayıcı
        LPARAM lParam       // fare koordinatları
);
```

Burada;

nCode, çengel kodu mesajın nasıl işlenmesi gerektiğini belirtmektedir. Bu kod HC_ACTION ise wParam ve lParam parametreleri fare mesajı hakkında bilgiler içermektedir. HC_NOREMOVE ise yine bu parametreler geçerlidir ve fare mesajı mesaj kuyruğundan çıkartılmamıştır. Bunun dışındaki kod değerleri için, mesaj daha fazla işlenmeden bir sonraki çengel prosedürüne geçiş yapılır. lParam, MOUSEHOOKSTRUCT cinsinden bir yapıya işaretçidir.

Bu yapı aşağıdaki gibi tanımlanmaktadır:

```
typedef struct tagMOUSEHOOKSTRUCT { // ms
        POINT pt;
        HWND  hwnd;
        UINT  wHitTestCode;
        DWORD dwExtraInfo;
} MOUSEHOOKSTRUCT;
```

Burada kullanılan parametrelerden;

pt, POINT yapısı cinsinden ekran koordinatlarında fare işaretçisinin x ve y koordinatlarını içermektedir. hwnd, fare olayına cevap veren fare mesajını alan pencerenin tanıtıcısıdır. wHitTestCode, isabet test değerini içerir. Bu değerler Çizelge 5.3'de listelenmektedir:

Çizelge 5.3. İsabet test (hit test) değerleri

Değer	*Dokunma Noktasının Yeri*
HTBORDER	Boyutunu değiştirme sınırı olmayan bir pencerenin sınırında
HTBOTTOM	Boyutu değiştirilebilir bir pencerenin alt yatay sınırında
HTBOTTOMLEFT	Boyutu değiştirilebilir bir pencerenin sol alt köşesinde
HTBOTTOMRIGHT	Boyutu değiştirilebilir bir pencerenin sağ alt köşesinde
HTCAPTION	Başlık çubuğunda
HTCLIENT	İstemci (client) alanında
HTCLOSE	Kapat düğmesinde
HTERROR	Ekran arka planında veya pencereler arasındaki bölme hattında
HTGROWBOX	Büyüklük kutusunda (HTSIZE ile aynı)
HTHELP	Yardım düğmesinde
HTHSCROLL	Yatay kaydırma çubuğunda
HTLEFT	Boyutu değiştirilebilir bir pencerenin sol sınırında
HTMENU	Bir menüde
HTMAXBUTTON	Ekranı kapla düğmesinde
HTMINBUTTON	Simge durumuna küçült düğmesinde
HTNOWHERE	Ekran arka planında veya pencereler arasındaki bölme hattında
HTREDUCE	Simge durumuna küçült düğmesinde
HTRIGHT	Boyutu değiştirilebilir bir pencerenin sağ sınırında
HTSIZE	Büyüklük kutusunda (HTGROWBOX ile aynı)
HTSYSMENU	Sistem menüsünde veya yavru pencerenin Kapat düğmesinde
HTTOP	Bir pencerenin üst yatay sınırında
HTTOPLEFT	Bir pencerenin sol üst köşesinde
HTTOPRIGHT	Bir pencerenin sağ üst köşesinde
HTTRANSPARENT	Aynı iş parçacığında bir başka pencere tarafından kaplanan bir pencerede (mesaj aynı iş parçacığında alttaki bütün pencerelere biri HTTRANSPARENT kodu gönderene kadar gönderilir)
HTVSCROLL	Dikey kaydırma çubuğunda
HTZOOM	Ekranı kapla düğmesinde

11. Alt seviye fare çengeli (WH_MOUSE_LL)

Windows NT 4.0 Hizmet Paketi 3.0 ile beraber gelen WH_MOUSE_LL çengeli bir iş parçacığı girdi kuyruğuna postalanan fare girdi olaylarını izlemek amacıyla kullanılmaktadır. Çengel prosedürü LowLevelMouseProc olarak adlandırılmaktadır.

Sistem, bir iş parçacığının girdi kuyruğuna yeni bir klavye girdi olayı postalanmak üzere olduğunda LowLevelMouseProc fonksiyonu çağırmaktadır. Fare girdisi yerel fare sürücüsünden veya mouse_event fonksiyonundan gelebilir. Eğer girdi bir mouse_event çağrısından geliyorsa girdi "enjekte" edilmiştir. mouse_event

fonksiyonu ile bir fare hareketi ve fare tuş basımını sentezlemek mümkündür. Bu fonksiyonun imzası,

```
VOID mouse_event(
        DWORD dwFlags,      // hareket ve tıklama şekillerini belirleyen bayraklar
        DWORD dx,           // yatay fare konumu veya konum değişimi
        DWORD dy,           // dikey fare konumu veya konum değişimi
        DWORD dwData,       // teker hareket miktarı
        DWORD dwExtraInfo // 32 bit uygulama tanımlı bilgi
);
```

şeklinde tanımlanmaktadır. Bu fonksiyonda;

dwFlags parametresi MOUSEEVENTF_ABSOLUTE, MOUSEEVENTF_MOVE, MOUSEEVENTF_LEFTDOWN, MOUSEEVENTF_LEFTUP, MOUSEEVENTF_RIGHTDOWN, MOUSEEVENTF_RIGHTUP, MOUSEEVENTF_MIDDLEDOWN, MOUSEEVENTF_MIDDLEUP ve MOUSEEVENTF_WHEEL değerleri ile fare tuşu basma ve bırakmalarını, teker hareketlerini ve fare hareketlerini belirler.

WH_MOUSE_LL çengeli için kullanılan çengel yordamı LowLevelMouseProc'un imzası aşağıdaki gibidir:

```
LRESULT CALLBACK LowLevelMouseProc(
        int nCode,          // çengel kodu
        WPARAM wParam,  // mesaj tanımlayıcı
        LPARAM lParam       // mesaj verileri yapısına işaretçi
);
```

Eğer nCode değeri HC_ACTION ise wParam ve lParam parametreleri fare mesajı ile ilgili bilgiler içermektedir. wParam mesaj türünü belirlemektedir. Bu türler WM_LBUTTONDOWN, WM_LBUTTONUP, WM_MOUSEMOVE, WM_MOUSEWHEEL, WM_RBUTTONDOWN veya WM_RBUTTONUP olabilir.

lParam ise MSLLHOOKSTRUCT adında bir yapıya işaretçidir. Bu yapı aşağıdaki şekilde tanımlanmaktadır:

```
typedef struct tagMSLLHOOKSTRUCT {
        DWORD pt;
        DWORD mouseData;
        DWORD flags;
        DWORD time;
        DWORD dwExtraInfo;
} MSLLHOOKSTRUCT, FAR *LPMSLLHOOKSTRUCT, *PMSLLHOOKSTRUCT;
```

Bu fonksiyonda; pt, farenin ekran koordinatları cinsinden x ve y koordinatlarını vermektedir. mouseData parametresi, WM_MOUSEWHEEL mesajı tarafından kullanılmaktadır. flags parametresinin 0. biti olayın enjekte olup olmadığını belirtir. Bu bit 1 ise olay enjektedir. Bu değer LLMHF_INJECTED sabiti ile test edilebilir. time parametresi, mesajın oluşma zamanıdır. dwExtraInfo, mesaj ile ilgili ilave veridir.

12. Girdi mesaj filtresi çengeli (WH_MSGFILTER)

WH_MSGFILTER ve WH_SYSMSGFILTER çengelleri bir menü, kaydırma çubuğu, mesaj kutusu veya diyalog kutusu tarafından işlenmek üzere olan mesajları izlemeye ve farklı bir pencerenin kullanıcı tarafından Alt+Tab veya Atl+Esc tuş kombinasyonu basarak etkinleşmesinin saptanmasına olanak vermektedir. WH_MSGFILTER, sadece çengel prosedürünü kuran uygulama tarafından oluşturulmuş olan menü, kaydırma çubuğu, mesaj kutusu veya diyalog kutusuna iletilen mesajları izleyebilmektedir. WH_SYSMSGFILTER çengeli ise bu tür mesajları bütün uygulamalar için izleyebilmektedir.

Bu iki çengel için kullanılan çengel prosedürleri MessageProc ve SysMsgProc olarak adlandırılmaktadır. Bu prosedürlerin imzası, her ikisi de aynı olmak üzere, aşağıdaki gibidir:

```
LRESULT CALLBACK MessageProc(       // SysMsgProc aynı
        int code,                   // çengel kodu
        WPARAM wParam,  // tanımsız
        LPARAM lParam       // mesaj verileri yapısının adresi
);
```

code parametresi mesajı üreten girdi olayının türünü belirlemektedir. Bu parametre:

- MSGF_DDEMGR: Girdi olayı Dinamik Veri Değişimi Yönetim Kütüphanesi (DDEML, Dynamic Data Exchange Management Library) eşzamanlı bir işlemin bitmesini beklerken oluşmuştur.
- MSGF_DIALOGBOX: Girdi olayı bir mesaj kutusunda veya diyalog kutusunda oluşmuştur.
- MSGF_MENU: Girdi olayı bir menüde oluşmuştur.
- MSGF_NEXTWINDOW: Girdi olayı kullanıcı farklı bir pencereyi etkinleştirmek üzere olduğunda oluşmuştur.
- MSGF_SCROLLBAR: Girdi olayı bir kaydırma çubuğunda oluşmuştur.

wParam değeri NULL olarak dikkate alınmaz. lParam MSG yapısına bir işaretçidir. MSG yapısı WH_GETMESSAGE çengeli kısmında açıklanmaktadır.

13. Kabuk çengeli (WH_SHELL)

Bir kabuk uygulaması, önemli haber vermeleri alabilmek için WH_SHELL çengelini kullanabilir. Sistem WH_SHELL çengeli prosedürünü bir kabuk uygulaması etkinleşmek üzereyken ve üst seviye penceresi oluşturulduğunda veya yok edildiğinde çağırır.

Çengel prosedürü ShellProc olarak adlandırılmaktadır ve bu prosedürün imzası aşağıdaki gibidir:

```
LRESULT CALLBACK ShellProc(
        int nCode,              // çengel kodu
        WPARAM wParam,  // olaya göre belirli bilgi
        LPARAM lParam       // olaya göre belirli bilgi
);
```

Çengel kodunu belirleyen nCode parametresi, aşağıdaki değerleri alabilir:

- HSHELL_ACCESSIBILITYSTATE: (Windows NT 5.0 veya daha sonra) Erişilebilirlik durumu değişti
- HSHELL_ACTIVATESHELLWINDOW: Kabuk ana penceresini etkinleştirmeli
- HSHELL_GETMINRECT: Bir pencere simge durumuna küçültülüyor veya ekranı kaplar hale getiriliyor. Sistem pencere için simge durumu dikdörtgeninin koordinatlarına ihtiyaç duyar.
- HSHELL_LANGUAGE: Klavye dili değişti veya yeni bir klavye düzeni yüklendi.
- HSHELL_REDRAW: Görev çubuğundaki bir pencerenin başlığı tekrar çizildi.
- HSHELL_TASKMAN: Kullanıcı görev listesini seçti. Bir görev listesi sağlayan bir kabuk uygulaması Windows'un onun görev listesini başlatmasını önlemek için TRUE değer döndürmelidir.
- HSHELL_WINDOWACTIVATED: Etkinleşme sahipsiz farklı bir üst seviye pencereye değişti.
- HSHELL_WINDOWCREATED: Pencere sahibi bulunmayan bir üst seviye penceresi oluşturuldu. Pencere sistem ShellProc fonksiyonunu çağırdığında çıkacaktır.

- HSHELL_WINDOWDESTROYED: Pencere sahibi bulunmayan bir üst seviye penceresi yok edildi. Pencere sistem ShellProc fonksiyonunu çağırdığında hala var olacaktır.

wParam parametresi, nCode parametresine göre aşağıdaki değerleri alabilir:

- HSHELL_ACCESSIBILITYSTATE: Hangi erişilebilirlik özelliğinin durumunu değiştirdiğini gösterir. Bu değerler ACCESS_FILTERKEYS, ACCESS_MOUSEKEYS veya ACCESS_STICKYKEYS olabilir.
- HSHELL_GETMINRECT: Simge durumuna küçültülen veya ekranı kaplar hale getirilen pencerenin tanıtıcısı.
- HSHELL_LANGUAGE: Pencerenin tanıtıcısı
- HSHELL_REDRAW: Yeniden çizilen pencerenin tanıtıcısı
- HSHELL_WINDOWACTIVATED: Etkinleşen pencerenin tanıtıcısı
- HSHELL_WINDOWCREATED: Oluşturulan pencerenin tanıtıcısı
- HSHELL_WINDOWDESTROYED: Yok edilen pencerenin tanıtıcısı

lParam parametresi, nCode parametresine göre aşağıdaki değerleri alabilir:

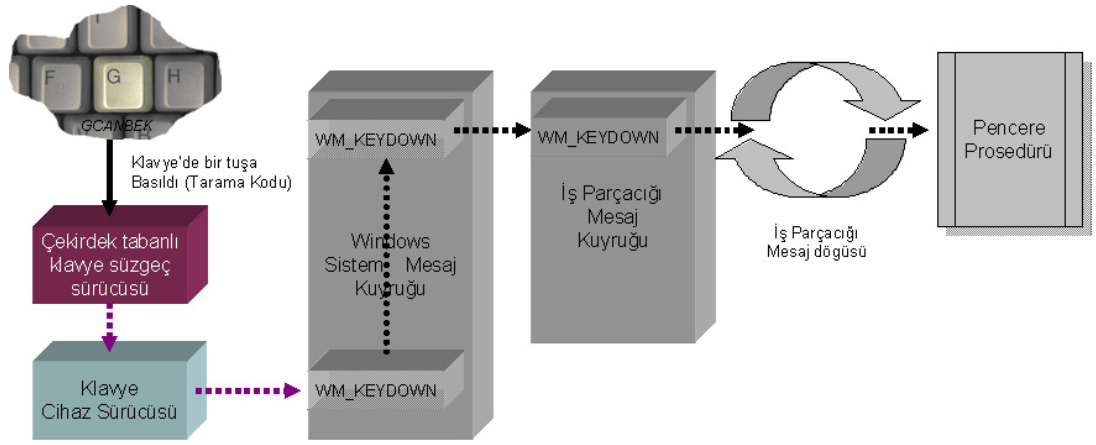
- HSHELL_GETMINRECT: Bir RECT yapısına işaretçi
- HSHELL_LANGUAGE: Bir klavye düzenine tanıtıcısı
- HSHELL_REDRAW: Pencere yanıp sönüyorsa TRUE değilse FALSE değerini alır
- HSHELL_WINDOWACTIVATED: Pencere tüm ekran ise TRUE değilse FALSE değerini alır

5.4.4. Çekirdek tabanlı klavye süzgeç sürücüsü

Klavye dinleme sistemlerinin kullandığı yöntemlerin sonuncusu, çekirdek tabanlı klavye süzgeç sürücüsü (kernel level keyboard fitler driver) kullanımıdır. Sürücü tasarımı gerektiğinden ileri derecede programlama istemektedir.

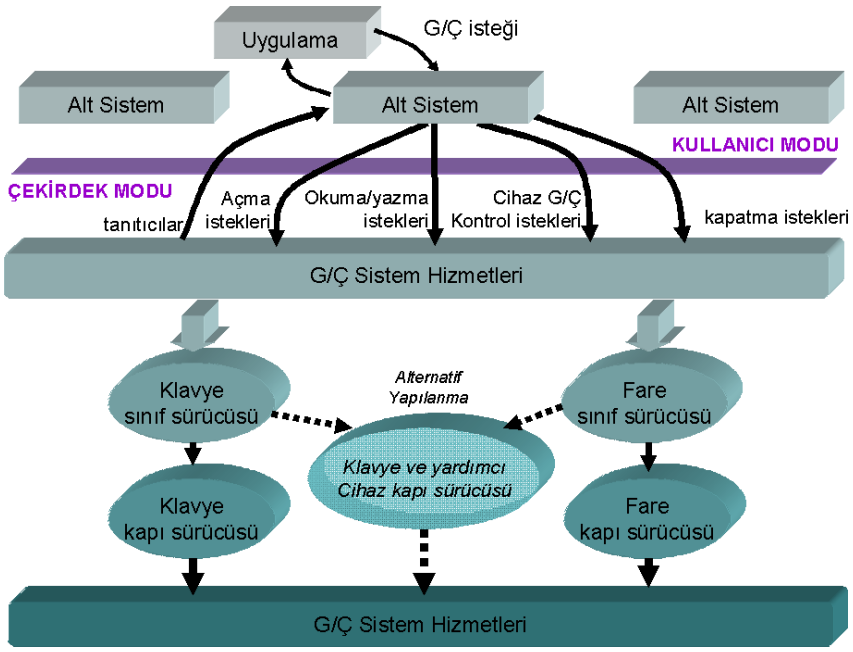
Şekil 5.11'de görüldüğü gibi, çekirdek tabanlı klavye süzgeç sürücüsü yöntemi ile gerçekleştirilen ortadaki adam saldırısı, bu kez Windows işletim sisteminin klavye cihaz sürücüsü ile klavyenin kendisi arasında gerçekleşmektedir. Hazırlanan sürücü, klavye cihaz sürücüsünün üstündedir. Bu yüzden işletim sisteminin bile basılan tuş bilgisini algılamasından önce devreye girdiğinden bu tür klavye dinlemenin saptanması daha güçtür.

Çekirdek tabanlı klavye süzgeç sürücüsü bu şekilde klavye cihaz sürücüsüne gönderilen bütün G/Ç (Girdi/Çıktı) istek paketlerini (IRP, I/O Request Packet) alacaktır. Bu sayede bütün okuma istekleri izlenebilir ve her bir istek için bir G/Ç tamamlama rutini kurulabilir. Bir kaç tuşa basılınca okuma isteği tamamlanınca G/Ç tamamlama rutini başlatılır ve basılan gerçek tuş bu sayede elde edilebilir.



Şekil 5.11. Çekirdek tabanlı klavye süzgeç sürücüsü

Şekil 5.12'de görüldüğü gibi Windows NT teknolojisinde NT sürücüleri, uç kullanıcı modundan gizlidir. Uç kullanıcılar, korumalı alt sistemler aracılığıyla cihazlara erişebilmektedirler. Win32 alt sistemi, G/Ç isteklerini G/Ç sistem hizmetleri aracılığıyla uygun çekirdek modu sürücüsüne iletir. Sistem tarafından sağlanan klavye ve fare cihaz sürücüleri, bir veya birden fazla kapı sürücüsü sınıfı üzerinde, katmanlı sınıf sürücüleri şeklinde gerçekleştirilirler ya da klavye ve cihaz sürücüleri hep beraber, tek parça sürücü olarak da tasarlanabilir.



Şekil 5.12. Klavye ve fare sürücü katmanları

Çengel veya klavye durum tablosu yönteminde elde edilen tuş basımı bilgileri, bellekte veya diskte bir dosya olarak saklanırken; çekirdek tabanlı klavye süzgeç sürücüsü tasarımında elde edilen tuş basımı bilgileri, bir dosyaya doğrudan kaydedilebileceği gibi bu bilgiler önce bir çekirdek alanı tamponuna da kaydedilebilir. Bu durumda yakalanan tuş basımı bilgilerini elde edebilmek için kullanıcı tarafında hazırlanan bir uygulamanın, belirli aralıklarla süzgeç sürücüsünü yoklaması sağlanabilir. Aşağıdaki verilen kaynak kod parçası her bir okuma isteği için gerçekleştirilen G/Ç tamamlama rutininin kurulumunu göstermektedir:

```
PDEVICE_OBJECT gKbdTopOfStack;
PDRIVER_OBJECT irpStack;
PIO_COMPLETION_ROUTINE  OnKbdReadComplete;
PDEVICE_OBJECT DeviceObject;
/* .... */
if (irpStack->MajorFunction == IRP_MJ_READ)
{
        PIO_STACK_LOCATION nextIrpStack;
        nextIrpStack = IoGetNextIrpStackLocation(Irp);
```

```
        *nextIrpStack = *irpStack;
        // Tuş basım bilgilerini elde edebilmek için tamamlama rutinini ata
        IoSetCompletionRoutine(
                Irp, OnKbdReadComplete, DeviceObject, TRUE, TRUE, TRUE);
        // Çağrının sonuçlarını düşük seviye klavye sürücüsüne döndür
        return IoCallDriver(gKbdTopOfStack, Irp);
}
else
{
        Irp->CurrentLocation++;
        Irp->Tail->Overlay.CurrentStackLocation++;
        // İsteği düşük seviye klavye sürücüsüne ilet
        return IoCallDriver(gKbdTopOfStack, Irp);
}
```

Bu teknik, "kök kullanıcı araç takımını" (NTRootkit) kullanmaktadır. Çekirdek alanında çalışacak böyle bir klavye dinleme sisteminin gerçekleştirilebilmesi için Windows DDK (Driver Developer Kit, Sürücü Geliştirici Takımı) gereklidir. Hazırlanan sistem bir SYS sürücü dosyası halinde hedef sisteme yerleştirilir. İstenirse bu sürücü dosyası çalıştırılabilir bir dosyanın kaynak (resource) bölümünün içinde de saklanabilir. Saklanan bu dosya belgelendirilmemiş NtLoadDriver doğal API'si ile dinamik olarak yüklenebilir. Hazırlanan sürücü dosyaları yine belgelendirilmemiş ZwSetSystemInformation doğal API'sini SystemLoadAndCallImage seçeneği kullanılarak da yüklenebilir.

5.4.5. POSIX (Linux/BSD/UNIX benzeri işletim sistemleri) ve Linux'ta yazılım klavye dinleme sistemleri

UNIX benzeri ve Linux işletim sistemlerinde de yazılım ile klavye dinleme sistemi oluşturmak mümkündür. Bir Linux konsol klavyesinden herhangi bir tuşa basıldığında, sistem donanımdan gelen tarama kodunu alır ve çekirdek, bu kodu tuş koduna çevirir. Hazırlanan bir klavye dinleme sistemi 0x64 klavye kontrol kapısını

ve 0x60 klavye kapısını dinleyerek, klavyeden girilen bilgileri elde edebilirler. Bu şekilde çalışan bir klavye dinleme sistemini aşağıdaki gibi bir C kodu ile basit bir şekilde hazırlamak mümkündür:

```
int nDurum;
unsigned char cTus;

while (1)
{
        nDurum = inb(0x64);
        cTus = inb(0x60);
        if (20 == nDurum) && (cTus < 128)
                printf("Karakter = %s\n", cTus);
        usleep(1); // Biraz bekle
} // while sonu
```

5.5. Yazılım Klavye Dinleme Sistemlerinin İşleyiş Esasları

Yazılım klavye dinleme sistemlerinin işleyişini beş aşamada belirtmek mümkündür:

1) Sisteme kurulum ve sistem açılışı ile otomatik başlama
2) Sistem faaliyetlerinin gizlice izlenmesi
3) Bu faaliyetlere ilişkin bilgilerin gizli bir dosyada tutulması
4) Bu bilgilerin çeşitli yollarla sistemi kuran şahısa aktarılması ve
5) Gerekli durumlarda kurulan sistemin kaldırılması

Bu aşamalarda klavye dinleme sistemlerinde yapılan işlemlerin ayrıntıları, takip eden alt başlıklarda sunulmuştur.

5.5.1. Kurulum ve otomatik başlatma

Klavye dinleme sistemlerinin çalışacağı hedef bilgisayara çeşitli yöntemlerle kurulması (install) veya kopyalanması gerekmektedir. Bunun için bir e-posta ekinde

var olan bir Truva programının kullanılması gibi, bir çok casus yazılımının sistemlere bulaşmak için yararlandıkları teknikler kullanılabileceği gibi; sisteme gerekli olan dosyaların bir şekilde doğrudan kopyalanmasıyla da klavye dinleme sisteminin faal hale getirilmesi mümkündür. Bazı klavye dinleme sistemleri kendi dosyalarını çeşitli şekillerde gizlemektedirler. Sisteme kurulduktan sonra bu tür programların, otomatik bir şekilde sistem ile birlikte kendilerini başlatmaları gerekmektedir. Bunun için casus yazılım otomatik başlatma yöntemlerinden biri kullanılabilir.

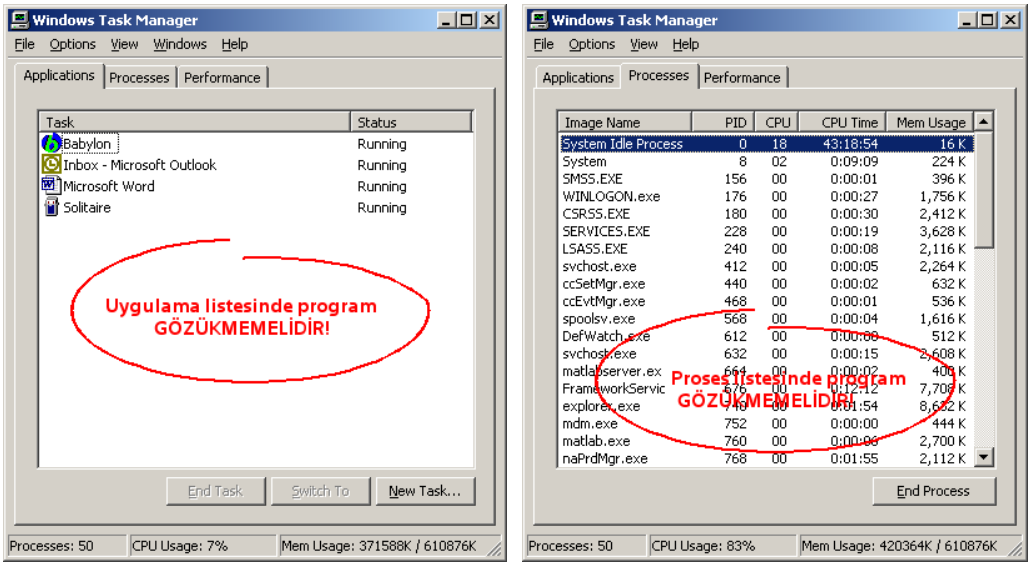
5.5.2. Faaliyetlerin gizlice izlenmesi

Klavye dinleme sistemleri istenilen bilgileri çengel, klavye durum tablosu v.s. gibi yukarıda anlatılan yöntemlerle gizlice izlerler. Bunun için çoğu zaman oldukça ileri seviyede programlama ve işletim sistemine hakimiyet gerekir. Örneğin, kullanıcının normal yollarla sistemde böyle bir programın çalışıp çalışmadığını saptaması önlenmelidir. Kullanıcının çalıştığı sistem üzerinde o an etkin olan uygulama ve prosesleri incelerken kullandığı temel araçlar bünyesinde klavye dinleme sisteminin,

- Windows görev çubuğunda ve sistem tepsisinde görülmemesi
- Windows görev yöneticisinde uygulamalar listesinde gözükmemesi
- Windows görev yöneticisinde prosesler listesinde gözükmemesi

sağlanmalıdır.

Şekil 5.13'de gösterildiği gibi özellikle klavye dinleme sistemlerinin kendilerini Windows işletim sisteminin görev yöneticisi aracından gizlemeleri oldukça zordur fakat bunu gerçekleştiren sistemler mevcuttur. Klavye dinleme sistemleri çalıştıkları sistemin kaynaklarını aşırı kullanmamalıdırlar. Böyle bir durum sistemi kullanan kişiyi şüphelendirebilir. Bu yüzden işlerin hızlı ve zaman paylaşımlı olarak gerçekleştirilmesi bir klavye dinleme sisteminin çalışmakta olduğu platformda gizli kalabilmesi için şarttır. Dolayısıyla, bu tür programları tasarlamak, geliştirmek ve optimize etmek uzun, zahmetli ve zor bir iştir.



(a) Uygulamalar (b) Prosesler

Şekil 5.13. Windows görev yöneticisinden klavye dinleme sisteminin gizlenmesi

Klavye dinleme sistemleri bu gizliliğe, istenilen bilgilerin kayıtlarının sessizce tutulması, tutulan bu bilgilerin aktarılması ve işi biten kayıtların ve gerekli durumlarda, klavye dinleme sisteminin kendisinin sistemden iz bırakılmadan silinmesi için ihtiyaç duymaktadır. Bu süreçler takip eden kısımlarda açıklanmıştır.

5.5.3. Bilgilerin kaydının tutulması

Gizlice elde edilen bilgiler, belirlenen bir formatta disk veya ağ adresi gibi bir ortamda saklanır. Bazı klavye dinleme sistemlerinde bu veriler şifrelenerek, herhangi bir şekilde ele geçtiğinde içindeki verilerin anlaşılmaması sağlanmaktadır.

5.5.4. Kayıt bilgilerinin transferi

Kayıt bilgilerinin hedef bilgisayarda kalması hiç bir anlam ifade etmemektedir. Sistemi kuran kişinin, hedef kullanıcının haberi olmadan bu bilgileri elde etmesi gerekmektedir. Bunun için uygulanan yöntemlerin başında e-posta ve FTP ile kayıt dosyalarının transferi sayılabilir. Böyle bir sistemin olmadığı durumlarda klavye dinleme sistemini kuran kişinin, bir kez daha hedef bilgisayara doğrudan veya

uzaktan erişip; kaydedilen bilgileri elde etmesi gerekecektir. Bu konu ile ilgili bir başka husus da tutulan kayıt bilgisinin eriştiği büyüklüğün kontrolüdür. İleri klavye dinleme sistemleri, bilgilerin tutulduğu dosya belli bir büyüklüğe gelince, otomatik transfer ile ya da son çare olarak, kayıtların otomatik silinmesi ile bu tür durumlarla karşılaşmamaya çalışırlar. Kimi klavye dinleme sistemleri belirli aralıklarla ya da bir zaman çizelgesi çevresinde kayıt dosyasının transferinin zamanlamasını da yapabilmektedir.

5.5.5. Sistemden kaldırılması

Gerekli görülen durumlarda klavye dinleme sisteminin kurulduğu sistemden kaldırılması ya da daha fazla faaliyet göstermesinin engellenmesi gerekebilir. Bunu otomatikleştiren çeşitli yaklaşımlar geliştirilebilir.

5.6. Yazılım Klavye Dinleme Sistemlerinin Yetenekleri

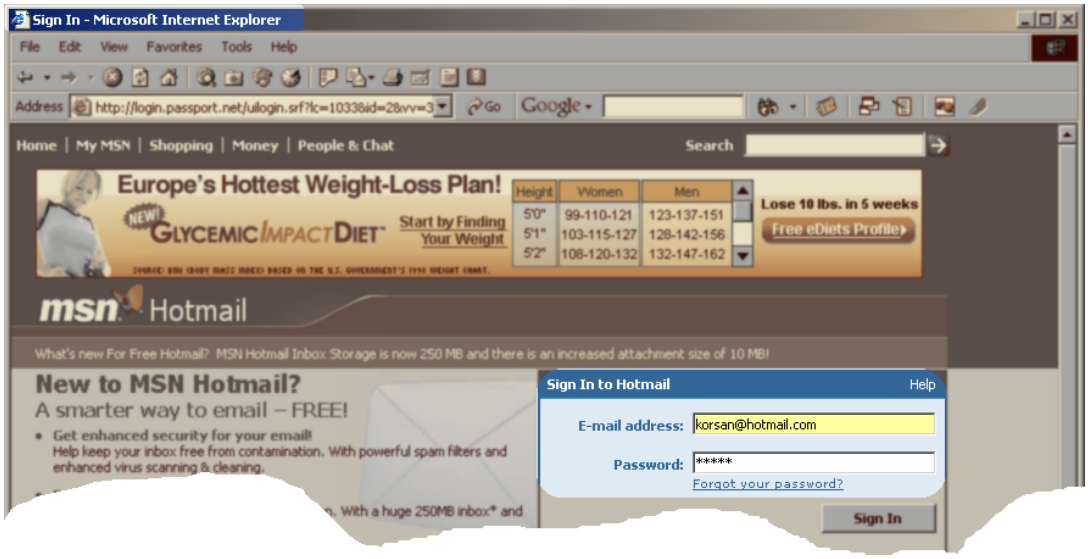
Yazılım klavye dinleme sistemleri olarak adlandırılan casus yazılımların yetenekleri, artık sadece klavyeden girilen bilgileri gizlice tutmaktan ibaret değildir. Bunun çok ötesinde işlevlere sahip bir çok klavye dinleme sistemi vardır ki, klavye dinleme sistemi (keylogger) tanımlaması yanıltıcı olabilmektedir. Bu tür sistemler faaliyet izleme (activity monitoring) olarak da adlandırılmalarına rağmen; klavye dinleme sistemi (keylogger) tanımı hala kullanılmaya devam etmektedir.

Klavye dinleme sistemlerinin sergileyebileceği yetenekler aşağıda kısaca listelenmiştir:

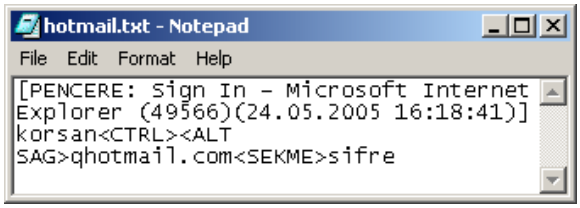
5.6.1. Klavye giriş bilgileri

Fonksiyon ve kontrol tuşları dahil, bir kullanıcının klavyeyi kullanarak girdiği bilgiler, girişin yapıldığı zaman ve pencere (program) bilgileri ile beraber bu tür sistemler tarafından tutulabilir. Bu, özellikle Şekil 5.14'de gösterildiği gibi çeşitli şifre bilgilerini ele geçirmek için kullanılabilir. Şekilde verilen örnekte, klavye dinleme sistemi ile elde edilen kayıtta bilgi girişinin yapıldığı pencerenin adı

"[PENCERE: Sign In - Microsoft Internet Explorer..." şeklinde; pencerenin etkin duruma geldiği tarih ve zaman "(24.05.2005 16:18:41)" şeklinde; E-posta adresi "korsan<CTRL><ALT SAG>qhotmail.com" (<CTRL><ALT SAG>q @ işaretini gösterir: korsan@hotmail.com) şeklinde; normalde ekranda "*" karakteri ile gizlenen şifre bilgisi ise "sifre" şeklinde gösterilmektedir. Bu sayede kullanıcı şifreleri, hesap şifreleri, belgelere ait şifrelerin elde edilmesi mümkündür.



(a) Klavye kullanılarak girilen e-posta adresi ve görünmez şifre



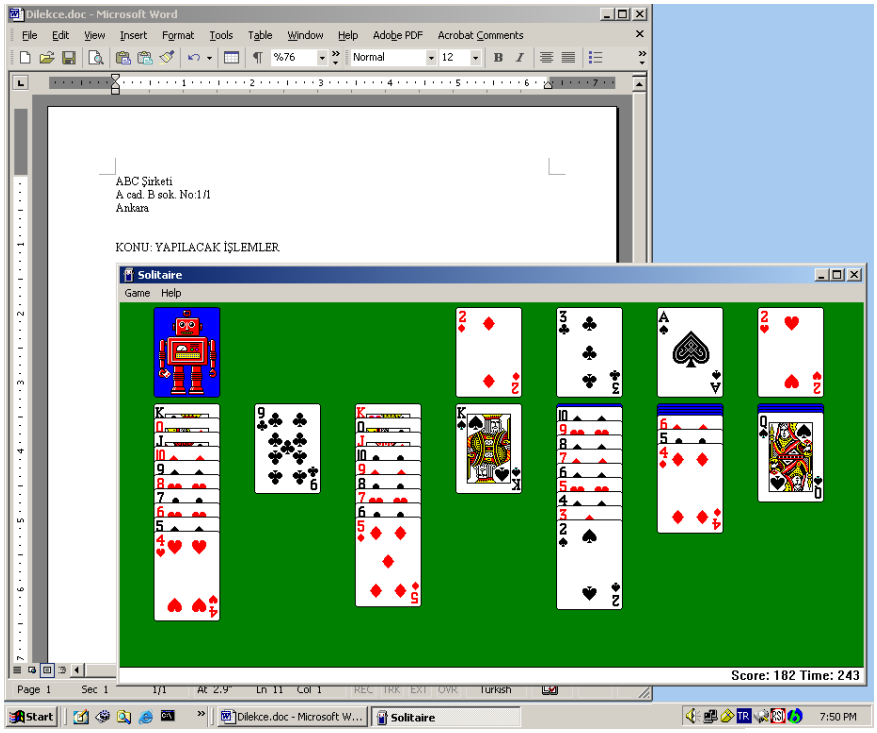
(b) Girilen bilgilerin kayıtlardan elde edilişi

Şekil 5.14. Bir İnternet sayfasından girilen bilgilerin klavye dinleme sistemi (TürkSpyware) ile elde edilmesi

5.6.2. Periyodik ekran görüntüleri (görsel gözetim)

Bu özellik klavye dinleme sistemlerinin en ilginç özelliklerinden biridir. Şekil 5.15'de de görülebileceği gibi, belirli aralıklarla ya da belli şartlar altında ekranın tamamının veya o an etkin olan pencerenin görüntüsünün bir resim olarak gizlice

elde edilip saklanması mümkündür. Görüntünün alınma zamanı gibi bilgiler resim ile beraber elde edilebilir. Bazı klavye dinleme sistemleri "jpg" gibi değişik resim formatlarını da desteklemektedir. Resim sıkıştırma parametreleri ayarlanarak bu dosyaların sistemde az yer kaplaması sağlanabilir.



Şekil 5.15. Periyodik ekran görüntüsü alınarak görsel gözetim yapma

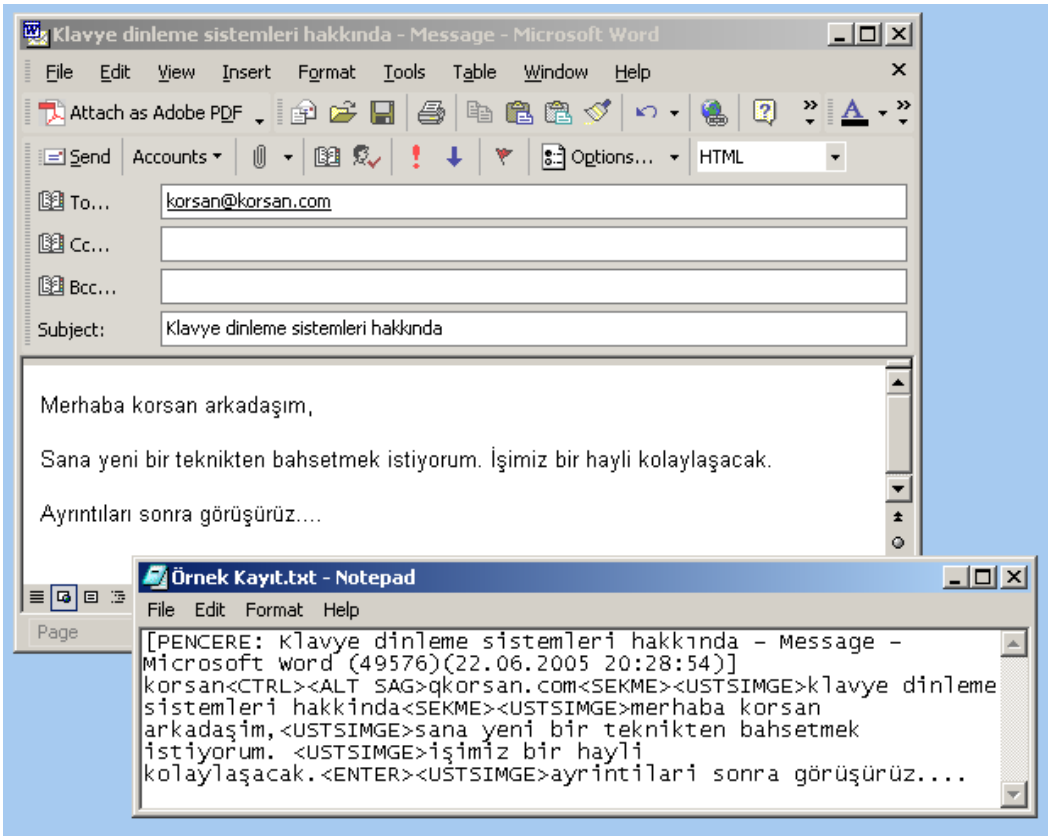
5.6.3. Fare hareketleri

Klavye dinleme sistemlerinde fare ile yapılan etkinliklerin izlenmesi de mümkündür. Kullanıcının tıkladığı ekran koordinatları, tıklanılan pencerenin ismi v.b. gibi çeşitli bilgiler bu tür izleme ile elde edilebilir. Bu özellik sanal klavyelerle bilgi girişinde sistemden bilgi çekmek için kullanılabilir.

5.6.4. Gönderilen ve alınan e-posta mesajları

Şekil 5.16'da hayali bir örneğinin gösterildiği gibi, klavye kullanılarak gönderilen e-posta mesajları da klavye dinleme sistemleri ile elde edilebilir. Bunun dışında

kullanılan e-posta işleyiciye özgü bazı teknikler kullanılarak “gelen” (okunan) e-posta mesajlarının da elde edilmesi mümkündür.



Şekil 5.16. Gönderilen e-posta mesajlarının yakalanması

5.6.5. Sohbet programları mesajları

ICQ, Messenger, IRC gibi popüler sohbet programlarından gönderilen mesajların gizlice izlenmesi mümkündür. Bu tür sohbet programlardan yararlanan kullanıcının ne türde bir sohbet yaptığı, klavye dinleme sisteminin tuttuğu kayıtlar okunarak anlaşılabilir.

5.6.6. İnternet’te ziyaret edilen sitelerin adresleri

Klavye dinleme ve diğer tekniklerle İnternet tarayıcısı kullanılarak, gezilen sitelerin adreslerini elde etmek mümkündür. Bu tip işlem kabiliyetine sahip klavye dinleme sistemleri, Microsoft İnternet Gezgini, Netscape Navigator, Mozilla FireFox gibi

farklı tarayıcı modelleri için farklı teknikler kullanmaktadırlar. Böyle bir işlev sergilemek isteyen klavye dinleme sisteminin, en azından en çok kullanılan Microsoft İnternet Gezgini tarayıcısını desteklemesi gerekmektedir.

5.6.7. Çalıştırılan programlar

Kullanıcının veya sistemin .exe, .bat, .com, *.cpl gibi uzantılarda çalıştırdığı programların neler olduğu ve ne zaman çalıştığı saptanabilir.

5.6.8. Üzerinde işlem yapılan dosya ve belgeler

Kullanıcının veya sistemin hangi dosyaları açtığı, değiştirdiği veya sildiği disk işlemleri izlenerek elde edilebilir.

5.6.9. Sistem kütüğünde (registry) yapılan değişiklikler

İşletim sistemine ait olan sistem kütüğünde yer alan çeşitli anahtar ve değerlerde yapılan değişiklikler izlenebilir.

5.6.10. Pano (clipboard) faaliyetleri

Kullanıcının daha sonra yapıştırmak üzere kopyaladığı yazı ve grafiği yakalamak mümkündür.

5.6.11. Kurulan ve kaldırılan programlar

Çeşitli yöntemlerle sisteme kurulan ve sistemden kaldırılan programların takip edilmesi mümkündür.

5.6.12. Yazıcıdan çıktısı alınan belgeler

Kullanıcının yazıcıdan çıktısını aldığı belgelerin ismi, sayfa sayısı ve çıktı alma zamanı elde edilebilir.

5.6.13. Diğer yetenekler

Klavye dinleme sistemleri aslında bilgisayar ortamında bir çok elektronik izleme işini yapabilir. Örneğin, her hangi bir ağ kapısına gönderilen ya da alınan paketler izlenebilir; İnternet'ten indirilen dosyalar izlenebilir; her hangi bir program veya belge üzerinde çalışma zamanı ve süresi belirlenebilir; sistem açılış ve kapanış zamanları belirlenebilir ve bilgisayara bağlı mikrofondan ses kaydı; "webcam" türü kameralardan video kaydı alınabilir. Bu tip izlenecek alanları daha da artırmak mümkündür.

5.7. Klavye Dinleme Sistemlerinin Kullanım Alanları

Bir çok yeteneğinin açıklandığı klavye dinleme sistemleri, çok çeşitli amaçlar için kullanılabilir. Bunlardan bazıları kötü niyetli sonuçlar doğururken; bazıları da oldukça faydalı olabilecek amaçlara hizmet etmektedir.

Klavye dinleme sistemlerinin en öne çıkan kullanım alanları arasında,

- Casusluk ve gizli bilgilere erişme
- Çevrimiçi banka hesap bilgilerinin ele geçirilmesi
- Karı-kocanın haber vermeden birbirlerinin İnternet ve bilgisayar kullanımını takip etmesi
- Öğrenci bilgisayar laboratuarındaki bilgisayarların kullanımının takip edilmesi
- Ebeveynlerin çocuklarının İnternet ve bilgisayar kullanımını kontrol altında tutması
- İşyeri gözetleme ve
- Kişilerin kendi kendilerini izlemesi

sayılabilir. Bu alanlarda klavye dinleme sistemlerinin nasıl kullanıldığı takip eden kısımlarda sırasıyla alt başlıklar altında anlatılmaktadır.

5.7.1. Casusluk ve gizli bilgilere erişme

Casusluk ve gizli bilgilere erişme bir klavye dinleme sisteminin en çok ilgi çeken yönüdür. Bu gibi kullanımlar, bir kişi veya grubun bir bilgisayarda ne yaptığını gizlice izleyip, elde etmesine yönelik faaliyetlerdir. Bu konuda sıradan kullanıcıların yanı sıra; sistem yöneticilerin, işverenlerin, güvenlik birimlerinin ve devletin bilgilendirilmesi gerekmektedir. Bir kullanıcının gizli bilgilerine erişmek; bir kişinin bilgisayar faaliyetlerini ve bilgisayar ve İnternet kullanarak yapmış olduğu bütün haberleşme bilgilerine erişmek; bir şirketin ticari sırlarına erişmek; suçluların elektronik ortamda takibini yapmak gibi bir çok işlem, gizli bir şekilde klavye dinleme sistemleri tarafından gerçekleştirilebilir.

Kimlik hırsızlığı (identity theft) olarak adlandırılan, özellikle kredi kartı bilgileri gibi önemli bilgileri almak amacıyla kullanılan casus yazılımların başında, klavye dinleme sistemleri gelmektedir. Kimlik hırsızlığı geliştirmek amacıyla özellikle ülkemizde kullanılan yöntemlerden sazan avlama (phishing), son günlerde popüler olsa da klavye dinleme sistemlerinin bu konudaki etkilerinin çok kısa sürede çeşitli örnekleri ile ortaya çıkacağı düşünülmektedir.

5.7.2. Çevrimiçi bankacılık ve Türkiye'de durum

Bankacılık, teknoloji kullanımı ve gelişiminde baş rollerden birini oynayan önemli bir sektör olarak karşımıza çıkmaktadır. Teknolojinin getirdiği imkanları kullanan bankalar, geleneksel bankacılığın yanı sıra telefon, cep telefonu, WAP ve İnternet ortamlarını kullanarak verdikleri hizmetleri geliştirmede birbirleriyle yarışmaktadır. Bu sayede sistemler çevrimiçi olarak müşterilerine 7 gün 24 saat dünyanın herhangi bir yerinden hizmet verebilmektedirler.

İnternet'in Amerikalılar üzerine sosyal etkilerini inceleyen bir araştırma merkezinin (Pew Internet & American Life) yaptığı ankete göre, son beş yıl içinde çevrimiçi bankacılık, İnternet etkinliklerinin en hızlı artan kısmı olmuştur. 2002'ye göre

İnternet bankacılığı kullanımı, 2005'e gelindiğinde %47'i artış göstermiştir. 53 milyon Amerikalı bankacılık işlemlerini İnternet üzerinden yapmaktadır (75).

Hal böyle olunca, bu sitelerin güvenliği çok önemli bir konu olarak ortaya çıkmaktadır. Kullanıcıların ilk zamanlarda İnternet üzerinde yapılan bankacılığa olan tedirginliklerini kısmen üzerlerinden atmaları, kullanımın artmasına ve yapılan yatırımların geri alınmasını sağlasa da bilgi güvenliğine yönelik konuların hafife alınması ve güncelliğinin takip edilmemesi ile ortaya çıkabilecek nahoş hadiseler bu güveni, ileride daha da zor olarak tekrar inşa edilebilecek şekilde kökten sarsabilir.

Ülkemizde çevrimiçi İnternet bankacılığı özellikle klavye dinleme sistemlerinin doğrudan uygulama alanı olduğundan üzerinde durulması gereken bir noktadır. Bu çalışmada bu konu bütün ayrıntıları ile incelenmiştir. Bankaların sunduğu sistemlerde müşterilerini mağdur edecek açıklar ve yanlış uygulamalar gözler önüne serilmeye çalışılmıştır.

Türkiye'de yerli/yabancı sermayeli 48 adet banka faaliyet göstermektedir. Bunların 40'ının İnternet üzerinde adresi bulunmaktadır. Bu gruptan sadece 24 banka, İnternet bankacılığı yapmaktadır (76). İnternet üzerinden yapılan bankacılık işlemleri gün geçtikçe artmakta ve bankalar işlemlerde İnternet'in kullanılmasını teşvik etmektedir. Çizelge 5.4'de Türkiye'de İnternet üzerinden çevrimiçi bankacılık yapan bankaların İnternet adresleri, klavye dinleme sistemlerine karşı kullandıkları sanal klavye ve diğer türde güvenlik önlemleri listelenmektedir. Bu çizelgeden de görülebileceği gibi bankaların güvenlik ile ilgili uygulama yöntemleri birbirlerinden farklı düzeylerdedir.

Türkiye'de İnternet bankacılığı incelendiğinde öncelikle bankalar, İnternet üzerinden güvenli veri iletimi için 128 bit SSL (Secure Sockets Layer) teknolojisini ve açılan oturum için güvenli HTTPS (Secure Hypertext Protocol) protokolünü kullanmaktadırlar. Bağlanılan bankanın kaynağını doğrulatmak için VeriSign, GlobalSign gibi kuruluşlarından alınan güvenlik sertifikaları kullanılmaktadır.

Çizelge 5.4. Türkiye'de İnternet bankacılığı yapan bankalar ve güvenlik hususları (Nisan 2005 tarihi itibariyle, Kaynak: Türkiye Bankalar Birliği)

Sıra No	*Banka*	*Banka Internet Adresi*	*Sanal Klavye*	*Diğer Türde Önlemler*
1	Akbank T.A.Ş.	http://www.akbank.com.tr/	Evet (Tıklamasız)	
2	Alternatif Bank A.Ş.	http://www.abank.com.tr/	Hayır	
3	Anadolubank A.Ş.	http://www.anadolubank.com.tr/	Evet	
4	BankEuropa Bankası A.Ş.	http://www.bankeuropa.com/	Evet	
5	C Kredi ve Kalkınma Bankası A.Ş.	http://www.cbank.com.tr/	Evet	
6	Citibank A.Ş.	http://www.citibank.com.tr/	Hayır	
7	Çalık Yatırım Bankası A.Ş.	http://www.calikbank.com.tr/	Hayır	
8	Denizbank A.Ş.	http://www.denizbank.com/	Evet	
9	Finans Bank A.Ş.	http://www.finansbank.com.tr/	Evet	
10	HSBC Bank A.Ş.	http://www.hsbc.com.tr/	Evet (Tıklamasız)	
11	Koçbank A.Ş.	http://www.kocbank.com.tr/	Evet (Tıklamasız ve hareketli)	Tek Kullanımlık Şifre (http://www.kocbank.com.tr/kocbank/adk/01/05/akillianahtar.asp)
12	MNG Bank A.Ş.	http://www.mngbank.com.tr/	Hayır	
13	Oyak Bank A.Ş.	http://www.oyakbank.com.tr/	Evet	
14	Şekerbank T.A.Ş.	http://www.sekerbank.com.tr/	Evet (Tıklamasız)	
15	Tekfenbank A.Ş.	http://www.tekfenbank.com/	Evet	
16	Tekstil Bankası A.Ş.	http://www.tekstilbank.com.tr/	Evet	
17	Türk Dış Ticaret Bankası A.Ş.	http://www.disbank.com.tr/	Evet	
18	Türk Ekonomi Bankası A.Ş.	http://www.teb.com.tr/	Evet	GüvenliGiriş programı. TebEdit adında bir Internet Gezgini nesnesi kurmakta
19	Türkiye Garanti Bankası A.Ş.	http://www.garanti.com.tr/	Evet	Garanti Güvenlik Kalkanı (http://www.garanti.com.tr/subesiz/internet_bankaciligi/kalkan1.html) SubClassEditCtrlContainer isminde bir Internet Gezgini nesnesi kurmakta Şifrematik.
20	Türkiye Halk Bankası A.Ş.	http://www.halkbank.com.tr/	Evet	İnternet Şubesi Sertifika (https://hercules.halkbank.com.tr/Turkce/CertRequest/IEMusSert.asp)
21	Türkiye İş Bankası A.Ş.	http://www.isbank.com.tr/	Evet	Güvenlik Çemberi programı (http://www.isbank.com.tr/interaktif/i-interaktif-guvcem.html) JaguarEditControl-ISBANK adında bir nesne kurmakta
22	Türkiye Sınai Kalkınma Bankası A.Ş.	http://www.tskb.com.tr/	Evet	
23	Türkiye Vakıflar Bankası T.A.O.	http://www.vakifbank.com.tr/	Hayır	
24	Yapı ve Kredi Bankası A.Ş.	http://www.ykb.com.tr/tr/	Evet	

Bu sertifikaya sahip güvenli bir web sayfası, genellikle tarayıcının durum çubuğunda Şekil 5.17'de gösterildiği gibi bir kilit resmi ile belirtilir. Bu kilidin var olması yine

de o sayfanın bağlanılmak istenen kuruma ait olduğunu göstermez. Kullanıcının o kilit resmini çift tıklayarak var olan sertifika bilgilerini kendisinin doğrulatması gerekir. Infosurv araştırma şirketinin yaptığı bir ankette, banka müşterilerinin %79'unun bu simgenin var olup olmadığını kontrol ettiği ama sadece %40'ının bu simgeyi tıklayarak sertifikayı incelediği belirtilmiştir (77).

Şekil 5.17. SSL güvenliğini gösteren simgenin İnternet tarayıcılarında görünümü

Bankalarımız genelde; müşteri adı, hesap veya müşteri numarası, şifre, nüfus bilgileri (doğum yeri, tarihi, ana, baba adı), telefon numaraları gibi bilgilerin bir kısmını, İnternet bankacılığına girişte istemektedirler. Burada en kritik bilgi genelde giriş şifresidir. Bu şifre ile ilgili, sonuçları iletilen ankette belirtilen hususlar, "doğru" şifre kullanımının önemini göstermektedir (77). Bu ankete göre müşterilerin %44'ü bir bankadaki şifresini başka diğer bankalar için de kullanmaktadır. Daha da vahimi, %37'lik bir banka müşterisi, banka için kullandığı şifreyi başka tam güvenilir olmayan sitelerde de kullanmaktadırlar. Bu şifrelerin kötü niyetli kişiler tarafından elde edilmesinde bir diğer yöntem sazan avlama (phishing)'dır. Bu yöntemde, kişilerin şifreleri dahil özel bilgilerini, sanki talep bir bankadan resmi olarak gönderiliyormuş gibi bir e-posta iletisi ile istenmektedir. Amerika'da yapılan bu ankette bu tip e-postalara cevap vermeme oranı, %70 gibi bir rakam iken ülkemizde

bununla ilgili bir bilgi mevcut değildir. Sazan avlama yöntemine başvuran kötü niyetli kişiler artık ilk örneklerinde olduğu gibi dilbilgisi bozuk, içerik tarzı açısından daha kolay şüphe duyulabilecek mesajlar yerine; son derece profesyonel ve resmi makamdan gönderilmiş gibi gözüken e-postalarla kişisel bilgileri ele geçirmeye başlamışlardır. Bu konuda, bilgisayar kullanıcılarının bilinçlendirilmesi çok önemlidir. Genelde bankaların "bankanın hiç bir şekilde e-posta ile müşteriden bilgi istemediğini" vurgulaması etkili bir yöntem olarak değerlendirilmektedir.

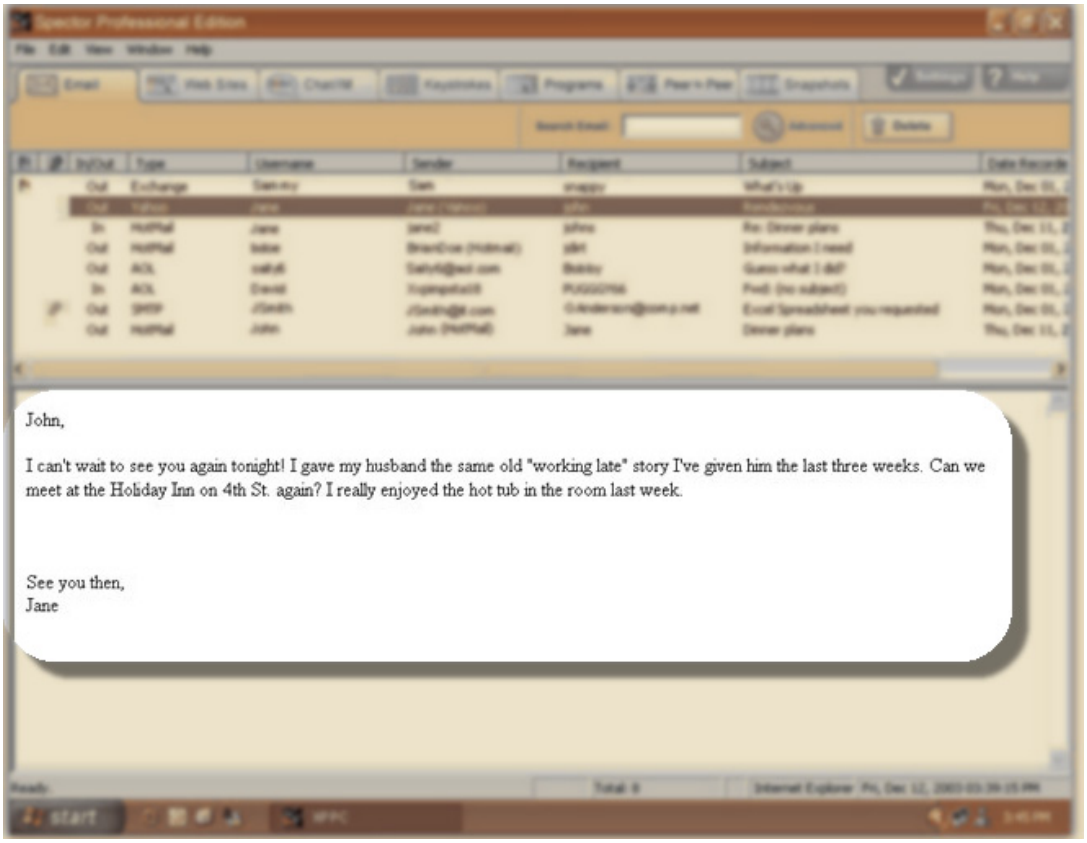
Kimi bankalar, yetkisiz kişilerin sahteciliğine karşı müşterinin İnternet bankacılığına erişeceği bilgisayarın IP'sini, İnternet servis sağlayıcısını, erişim zamanını kısıtlamasına olanak vermektedir. Ayrıca belli bir meblağı aşan işlemler için artı güvenlik önlemleri alınmaktadır. Yanlış şifre girilmişse bu durum ve bir önceki erişim tarih ve zamanı, yeni oturum açıldığında kullanıcıya gösterilmektedir.

Bütün bu önlemler dışında, bilgisayarda var olabilecek klavye dinleme sistemlerinin yol açabileceği zararların önüne geçmek için sanal klavye, klavye dinleme önleme sistemi desteği ve son olarak tek kullanımlık şifre üretme cihazları, daha fazla güvenlik isteyen hesap sahiplerinin kullanımına sunulmaktadır. Türkiye'deki bankaların klavye dinleme sistemine karşı aldıkları yöntemlerin bu çalışma için hazırlanan klavye dinleme sistemine göre testlerinin sonuçları ve değerlendirmeleri Bölüm **Hata! Başvuru kaynağı bulunamadı.**'de ayrıntıları ile bahsedilmektedir.

Klavye dinleme sistemleri ile elde edilen giriş bilgileri ve şifreler kötü niyetli kişiler tarafından kullanılabilir. Bu durumda mesela, banka hesabınıza ait bütün yetki bu kişilerin eline geçmiş olacaktır. Size hissettirmeden hesabınızdan az miktarda para kaçırabilecekleri gibi hesabınızla elde edilebilecek bütün paraya da göz dikebilirler. Bazı kişiler için para kaybından daha önemli konular da söz konusu olabilir. Giriş bilgilerinizi ve şifrelerinizi klavye dinleme sistemi ile ele geçiren kişi hesabınızda hiç bir işlem yapmaz sadece hesap durumunuzu ve yatırdığınız, çektiğiniz parayı, yatırım işlemlerinizi ve kimlerle para transferi yaptığınızı öğrenebilir. İş adamları, politikacılar gibi kişiler için belki bu para kaybından daha önemli olarak düşünülebilir.

5.7.3. Bir kişinin kendi eşini elektronik takip etmesi

Özellikle yurtdışında piyasaya sürülen bir çok klavye dinleme sisteminin reklamlarında Şekil 5.18'de gösterildiği gibi en çok vurgulanan bu konu, klavye dinleme sistemlerin ilginç kullanım alanlarından biri olarak karşımıza çıkmaktadır.



Şekil 5.18. Bir klavye dinleme sisteminde yakalanabilecek örnek bir e-posta metni

5.7.4. Bilgisayar laboratuarındaki öğrencilerin takibi

Üniversite yerleşkelerinde bulunan ve öğrencilerin hizmetine sunulan bilgisayar laboratuarında, öğrencilerin bilgisayarları uygun amaçlar için kullanıp kullanmadığı klavye dinleme sistemleri ile gerçekleştirilebilir. Hatta bazı klavye dinleme sistemlerinde olduğu gibi, öğrenci bilgisayarını açtığında sistemde böyle bir izlemenin yapıldığı öğrenciye bildirilerek daha doğru bir kullanım bile sağlanabilir. Bu mesajı okuyan öğrenci faaliyetlerinin izlendiğini düşüneceğinden bilgisayarını faydalı olabilecek amaçlar için kullanacaktır.

5.7.5. Ebeveynlerin çocuklarını elektronik ortamda kontrolü

Belki de klavye dinleme sistemlerinin en faydalı gözüken kullanımı bu sistemlerin ebeveynler tarafından kendi çocuklarının evdeki bilgisayarları kullanırken neler yaptığı, İnternet üzerinde ne tür sitelere girdiği ve kimlerle ve nasıl mesajlaştığını çocuğunun farkında olmadan ve onu rahatsız etmeden denetlemek ve bu tür faaliyetlerden zararlı olabileceklerin önüne geçmek amacıyla kullanılmasıdır.

Bilgisayar ve İnternet, sadece erişkinler için değil aynı zamanda çocuklar için de oldukça faydalı bir ortamdır. Bir çok anne baba, çocuğunun kendisini geliştirmesi, çağa ayak uydurması ve bilgiye daha çabuk ve etkin bir şekilde erişebilmesi için çocuklarına bu imkanı sunmak istemektedirler. Çocukların, bir eğitim, eğlence ve iletişim aracı olarak bilgisayarlardan faydalanması özendirilmelidir. Fakat nasıl normal olarak bir ebeveynin, kendi çocuğunun kendisi olmadan evin dışında, nerede, kiminle olduğunu bilmesi gerekiyorsa; başı boş ve uçsuz bucaksız bir ortam olarak nitelendirilebilecek İnternet'te çocukları kontrolsüz bırakmak oldukça tehlikeli sonuçlar doğurabilir.

Çocukların karşılaşabileceği risklerle, ebeveynlerin en çok düşündükleri konuların başında İnternet'te bulunan zararlı içerikli sitelere çocuklarının kazara da olsa erişme olasılıklarıdır. Bunun için Cyber Patrol (78) gibi İnternet'te bulunan siteleri türlerine göre sınırlayan filtre programları kullanılabilir. Bu tür programlar düzenli aralıklarla İnternet'te bulunan siteleri takip edilip oluşturulmuş bir veritabanından yararlanarak gezilen sitelere kullanıcının belirlediği kurallar çerçevesinde sınır koymaktadır. Bu veritabanında olmayan İnternet sayfalarını, göstermeden önce sayfa bulunan pornografik resimleri bilişsel ve/veya zeki algoritmalarla tespit edip bu sayfalara erişimi kısıtlayan programlar da bulunmaktadır.

Bu tür filtreleme programları önemli bir işlev gösterse de çocuklara yönelik bir çok risk yine de mevcudiyetine korumaktadır. Çocuklar,

- Pornografik öğe, öfke ve şiddet içeren ve yasa dışı içeriğe İnternet üzerinde maruz kalabilir,
- Çevrimiçi ortamlarda, kendilerini veya ailelerini tehlikeye atacak adres, kredi kartı numarası, evde o an kaç kişinin bulunduğu bilgisi gibi bilgileri üçüncü şahıslara, e-posta veya sohbet programları vasıtasıyla iletebilirler,
- İnternet üzerinden ebeveynlerinin kredi kartı ile haber vermeden alışveriş yapabilirler ve
- Kendisinden yaşça büyük ve kötü niyetli kişilerle ve suç örgütleri ile haberleşme

gibi bir çok risk ile karşı karşıyadır. Bütün bu riskler, konunun önemini gözler önüne sermektedir. Amerika'da küçük yaşta çocukların İnternet ortamında sohbet programları ile karşılaştıkları kişiler tarafından kaçırılıp, öldürüldüğü vakalar bile bulunmaktadır (79).

Ülkemizde ebeveynlerin çocuklarının İnternet ve bilgisayar kullanımıyla karşılaşabileceği riskler konusunda yeterli bir bilgiye sahip olmadıkları düşünülmektedir. Ebeveynler, çocuklarına bu konuda yol göstermelidir. Özellikle ilk bilgiler, bizzat bilgisayar başında gösterilerek ve çocuğun kendisinin denemeleri izlenerek verilmelidir. Ebeveynler, çocukların çevrimiçi bilgisayar kullanımı ile ilgili çeşitli konuları dikkate almalıdır (80). Bu konular aşağıda sunulmuştur:

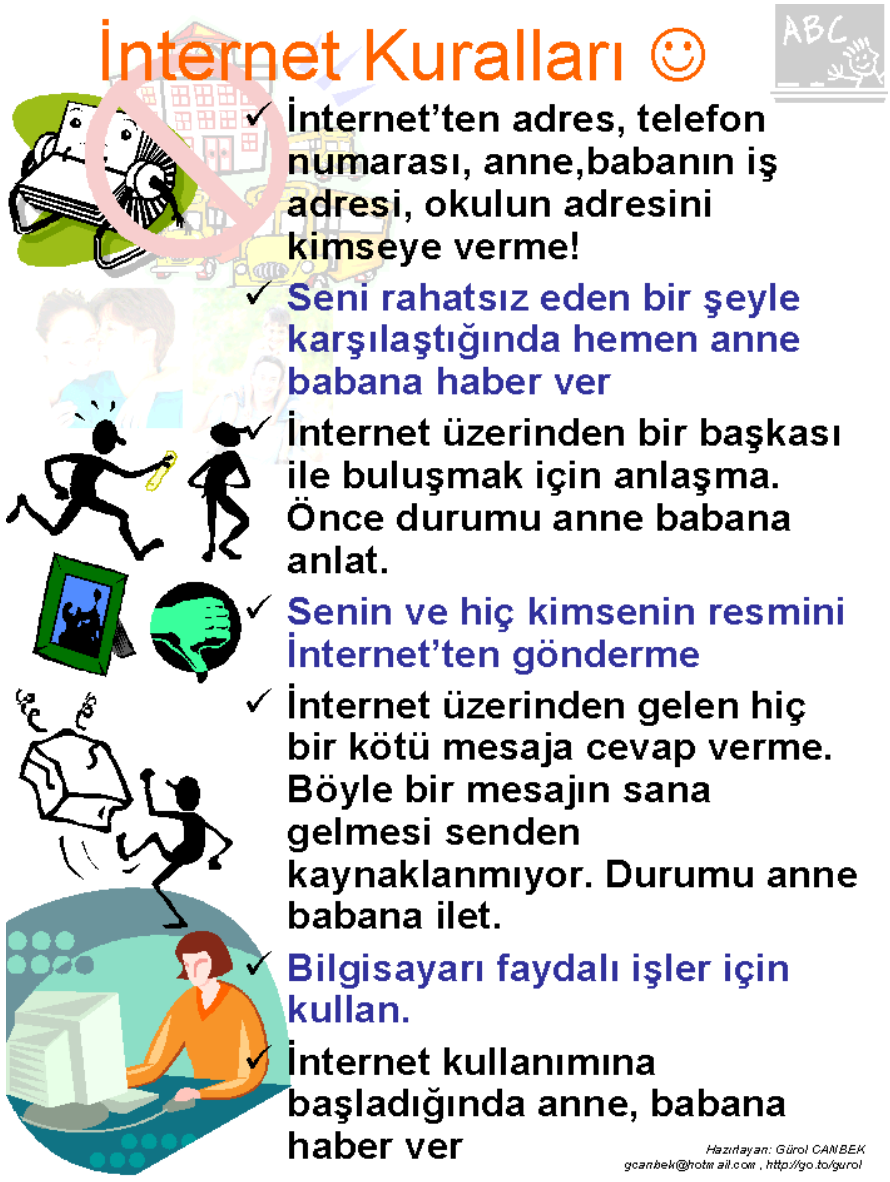
- Ev adresi, okul adı, telefon numarası gibi kimin olduğunu belirtici bilgileri e-posta, sohbet programları v.s. ile hiç kimseye vermeyiniz.
- Çocuğunuzun fotoğrafını hiç bir İnternet sitesine veya haber grubuna göndermeyiniz.
- Çocuğun kullanacağı İnternet ortamı ve İnternet servisleri hakkında bilgi edininiz.
- İzin alınmadan İnternet üzerinde tanışılan bir kişi ile yüz yüze görüşme yapılmayacağını çocuğunuza anlatınız. Böyle bir durumda oldukça tedbirli olun ve çocuğunuzun görüşmesinde bir sakınca görmeseniz bile en azından

ilk görüşmede çocuğunuzun yanında gidiniz ve görüşmenin halka açık alanda olmasını sağlayınız.

- Müstehcen, kavgacı, tehditkar veya sizi rahatsız eden hiç bir mesaja cevap vermeyiniz. Çocuğunuzu, böyle bir durumla karşılaştığında kendinize haber vermesine teşvik ediniz.
- Siz veya çocuğunuz bu tür bir mesaj aldığınızda, bu mesajı İnternet Servis Sağlayıcınıza iletiniz ve yardımlarını isteyiniz.
- Çocuğunuza bilmediği kişilerden aldığı e-postaların içinde yer alan bağlantıları tıklamaması gerektiğini anlatınız. Bu tür bağlantılar çocuğunuzun uygunsuz sitelere ulaşmasına neden olabilir.
- Çok kaba ve tehditkar mesajları emniyet birimlerine haber veriniz.
- Çevrimiçi ortamda insanların belirttikleri gibi olmayacaklarını unutmayınız ve bu konuda çocuğunuzu bilinçlendiriniz. Örneğin kendini 12 yaşında bir kız çocuğu gibi gösteren bir kişinin 40 yaşında bir adam olabileceği çocuğa anlatılmalıdır.
- Çevrimiçi ortamlarda okunulan veya karşılaşılan şeylerin doğru olamayabileceğini unutmayınız. Kulağa ve akla çok iyi gelebilen bilgi ve öneriler hatalı ve yanıltıcı olabilir. Çocuğunuza, kendisi ile buluşmak isteyen ve kendini ünlü biri olarak tanıtan kişilere, kendi evine davet eden kişilere ve kendisine para, kredi kartı ve diğer türde hediyeler göndermek isteyen kişilere karşı uyanık olması gerektiğini anlatınız.
- Çocuğunuzla beraber, bilgisayar ve İnternet kullanımı ile ilgili makul kuralların olduğu bir liste hazırlayınız. Bu listeyi bilgisayarın yakınında her zaman görülebilecek bir yere asınız.
- Çocuğunuzun bu kurallara uyup uymadığını kontrol etmeye çalışınız.
- Bakıcıların evdeki bilgisayarı kullanmasına ve İnternet'te gezinmesine müsaade etmeyiniz.
- Mümkünse çocuğunuzun kullandığı bilgisayarı çocuk odası yerine salon veya oturma odasına koyunuz.
- Çocuğunuzun "çevrimiçi arkadaşlarını" normal arkadaşlarında yaptığınız gibi biliniz ve takip ediniz.

- Eğer bunların bir çoğunu yapmada zorluklar yaşıyorsanız daha önceki bölümlerde anlatılan casus savar yazılımların bazılarını veya bu çalışmada geliştirilen TürkSpyware yazılımını kullanarak çocuğunuzun bilgisayar ve İnternet kullanımından emin olabilirsiniz.

Şekil 5.19'da çocukların uyması gereken kuralları çocukların ilgisini çekecek şekilde listelemek amacıyla bu çalışma için hazırlanmış bir sayfa gözükmektedir. Bu sayfa çocuğun bilgisayarının yakınında bir yere asılabilir.



Şekil 5.19. Çocuklar için hazırlanan örnek bir İnternet kullanım kuralı listesi

Bu risklerle baş edebilmek için çocukların bilgisayar kullanımını engellemeye gidilmemelidir. Ebeveynlerin belirtilen kurallara uyulup uyulmadığını sürekli takip etmeleri imkansızdır. Bu yüzden her ne kadar çocukların da kişisel gizliliğe ihtiyaçları olsa da; bu işi etkin bir şekilde yapan ve çocuğun bilgisayarda yapmış olduğu bütün faaliyetleri izleyebilen klavye dinleme sistemlerinin, ebeveynler tarafından kullanılması şarttır. Klavye dinleme sistemleri çocuğunuzun bütün bilgisayar faaliyetlerini gizli (veya çocuğun bilgisi dahilinde) disk üzerinde bir yerde tutar ve bu bilgileri kendiniz akşamları kontrol edebileceğiniz gibi; bu bilgiler çocuğunuz evde bilgisayarda iken siz işte olsanız bile size belli aralıklarla veya çeşitli durumlarda e-posta ile ulaştırılabilir. Böylelikle çocuğun tehlikeli ve zararlı bir yola girmesinin önüne geçilebilir.

5.7.6. İşyeri gözetleme

Bilgi ve bilgisayar güvenliği ve çalışanların kişisel gizliliği ile ilgili konular bir çok kurum ve kuruluş için ele alınması gereken en önemli konular arasındadır. 2003 yılında Amerikan CSI/FBI Bilgi Suçları ve Güvenlik İncelemesinde şirkete özel bilgilerin çalınmasından kaynaklanan kaybın 70 milyon ABD $ tuttuğu, rapor edilen ortalama kaybın ise yaklaşık 2,7 milyon ABD $ olduğu belirtilmektedir (81). Bu tür kayıpların bir çoğunun şirket içinde çalışan kişiler tarafından dışarıya sızdırıldığı düşünülürse konunun önemi daha da açığa çıkmaktadır. Firmalar çalışanlarının etkinliklerini göz ardı etmemeli; kurum içinde yapılan faaliyetler, kontrol altında tutulmalıdır. Bu konuda kurum ve kuruluşlara destek sağlayacak güvenlik çalışmaları hızla artmaktadır. İçerik ve bilgi güvenliği hizmet pazarı, IDC'nin tahminine göre yıllık %20,9 büyüme ile 2007 yılında 23,5 milyar $'ı geçecektir (82).

İçerik güvenliği, şirket dahilinde verilerin depolanması ve iletiminin elektronik yollarla takip edilmesiyle sağlanmaktadır. İçerik filtreleme, e-postaları tarayarak mesaj sağanağının önüne geçebilir; zararlı e-posta eklentilerine engel koyabilir; uygunsuz içerikteki mesajları karantina altına alabilir ve içerik güvenliği çerçevesinde hazırlanan politikalara uygun düşmeyen durumları sistem yöneticilerine haber verebilir. E-posta izleme yazılımları, içerik güvenliğini sağlayan araçlar

arasında işyerlerinde kullanılmaktadır. Bu tür yazılım satışlarının, 2001 yılında 139 milyon $'dan 2006 yılında 662 milyon $'a artış göstereceği tahmin edilmektedir (82). E-posta izleme yazılımları gelen ve giden mesajları virüs ve casus yazılımlara karşı tarama yapıp bu tür zararlı öğelerden temizleyebilir. Şirket e-posta hesaplarından gönderilen mesajların uygunsuz içerik ve eklentilere karşı elektronik yolla gözden geçirilmesi, mesajı alan kişilerde meydana gelebilecek zararların önüne geçerek şirketin imajının zedelenmesini önleyebileceği gibi yasalara ve genel ahlak kurallarına aykırı uygunsuz mesajların gönderilmesi engellenerek yasalar ve insanların gözünde şirketin zor duruma düşmesine veya itibarının zedelenmesine engel olunmaktadır.

İş yerlerinde çalışan kişilerin bilgisayarlarını işle ilgili olarak kullanıp kullanmadıklarını saptamak, bir çok işveren için oldukça ilgi çekici bir konu olabilir. Bu belki de verimliliği yükseltmek için bir yol da olabilir. Aslında herkesin de bildiği gibi çalışanlar, zaman zaman işle alakası olmayan şekilde bilgisayarlarını kullanmaktadırlar. Bu İnternet'e bağlı bir sistemde işle ilgili olmayan İnternet sitelerini gezmek; borsada hisse senedi fiyatlarını çevrimiçi takip etmek; çevrimiçi alışveriş yapmak, kişisel e-postalar alıp, göndermek; sohbet programlarında laflamak ve en basitinden bilgisayarda oyun oynamak şeklinde olabilmektedir. Genelde belli bir ölçüde bu şekilde kullanım, insanların işlerine daha şevkle eğilmeleri için maruz görülse de; bir çok işyeri bu tür kullanımları kontrol altında tutmak istemektedirler. Çünkü bazen bu faaliyetler, işten kaytarmaya ve yapılması gereken görevlerin zamanında ve gereken ölçüde yerine getirilmemesine sebep olabilmektedir. Ayrıca bu tür faaliyetler gereksiz ağ trafiğine neden olarak, iş için kullanılan ağ bant genişliğini daraltmaktadır.

Bu konu ile ilgili 15 Haziran 2005'de sunulan yeni bir araştırma, ülkemiz açısından da oldukça çarpıcı sonuçlar sunmaktadır. Amerika ve Avrupalı gözde araştırma firmalarından oluşan, NOP World piyasa araştırma şirketi tarafından, 30 ülkede, 13 yaşından büyük 30 000 kişi arasında, Aralık 2004 ve Şubat 2005 tarihleri arasında yapılan kapsamlı görüşmeler neticesinde, Kültür Puanı (Culture Score) adında tescil ettikleri medya alışkanlıkları incelemesi sunulmuştur (83).

Çizelge 5.5. Dünya Kültür Puanı

Televizyon İzleme		*Radyo Dinleme*		*Okuma*		*İşle İlgisiz Bilgisayar ve İnternet Kullanımı*	
Ülke	*Ortalama Saat*	*Ülke*	*Ortalama Saat*	*Ülke*	*Ortalama Saat*	*Ülke*	*Ortalama Saat*
Tayland	22,4	Arjantin	20,8	Hindistan	10,7	Tayvan	12,6
Filipinler	21	Brezilya	17,2	Tayland	9,4	Tayland	11,7
Mısır	20,9	Güney Afrika	15	Çin	8	İspanya	11,5
Türkiye	**20,2**	Çek Cumhuriyeti	13,5	Filipinler	7,6	Macaristan	10,9
Endonezya	19,7	Tayland	13,3	Mısır	7,5	Çin	10,8
ABD	19	**Türkiye**	**13,3**	Çek Cumhuriyeti	7,4	Hong Kong	10,7
Tayvan	18,9	Polonya	12,5	Rusya	7,1	Polonya	10,6
Brezilya	18,4	Macaristan	12,1	İsveç	6,9	**Türkiye**	**10,6**
İngiltere	18	Almanya	11,5	Fransa	6,9	Brezilya	10,5
Japonya	17,9	Avustralya	11,3	Macaristan	6,8	Mısır	10,3
Suudi Arabistan	17,7	Meksika	11,1	Suudi Arabistan	6,8	Filipinler	9,8
Fransa	17,3	İsveç	10,9	Hong Kong	6,7	Kore	9,6
Hong Kong	16,7	İngiltere	10,5	Polonya	6,5	Suudi Arabistan	9,3
KÜRESEL	16,6	ABD	10,2	KÜRESEL	6,5	Güney Afrika	9
Çek Cumhuriyeti	16,2	İspanya	9,9	Venezuela	6,4	KÜRESEL	8,9
Polonya	15,9	Filipinler	9,5	Güney Afrika	6,3	Arjantin	8,9
İspanya	15,9	Kanada	9,1	Avustralya	6,3	Rusya	8,9
Çin	15,7	Mısır	9	Endonezya	6	Fransa	8,8
Kore	15,4	Fransa	9	Arjantin	5,9	İngiltere	8,8
Almanya	15,2	KÜRESEL	8	**Türkiye**	**5,9**	ABD	8,8
Macaristan	15,1	Venezuela	7,6	İspanya	5,8	Kanada	8,3
Rusya	15	İtalya	7,2	Kanada	5,8	İsveç	8
İtalya	14,9	Rusya	6,6	Almanya	5,7	Hindistan	7,9
Güney Afrika	14,8	Endonezya	5,8	ABD	5,7	Endonezya	7,7
Kanada	14,7	Hong Kong	5,1	İtalya	5,6	Venezuela	7,5
Arjantin	14	Tayvan	4,7	Meksika	5,5	Avustralya	7
Avustralya	13,3	Japonya	4,1	İngiltere	5,3	Çek Cumhuriyeti	7
Hindistan	13,3	Hindistan	4,1	Brezilya	5,2	Japonya	6,9
İsveç	12,3	Suudi Arabistan	3,9	Tayvan	5	Almanya	6,4
Venezuela	11,9	Kore	3	Japonya	4,1	İtalya	6,3
Meksika	11,6	Çin	2,1	Kore	3,1	Meksika	6

Çizelge 5.5'de sonuçları aktarılan bu araştırmaya göre 30 ülke arasında Türkiye, okumaya ayrılan saat bakımından haftada 5,9 saat ile Suudi Arabistan ve dünya

ortalamasının da gerisinde 19. sırada iken televizyon izlemede haftada 20,2 saat ile 4. sırada ve radyo dinlemede haftada 13,3 saat ile 6. sırada bulunmaktadır. Bu araştırmanın konumuz açısından en can alıcı sonucu ise iş ile ilgisi olmayan bilgisayar ve İnternet kullanımıdır. Türkiye, haftada 10,6 saat ile işyerinde bu tür bilgisayar ve İnternet kullanımında 8. sıradadır. Bu durum işyeri gözetleme konusuna ülkemiz kurum ve kuruluşlarının ciddi bir şekilde eğilmesi gerektiğini ve bu konuda klavye dinleme sistemlerine olan ihtiyacı vurgulaması açısından kayda değer bulunmaktadır.

İşyerinde gezilen sitelerle ilgili, mesai saatlerinde çalışanların erişebileceği İnternet sitelerini sınırlayan WebSense, SurfControl ve Secure Computing gibi İnternet izleme araçları artık bir çok şirkette kullanılmaktadır. Bu tür araçlar, çalışanların İnternet kullanımlarını izleyip, raporlar sunabilmekte, engelledikleri bazı sitelere öğle arası, mesai sonrası veya belirli bir süre için izin verebilmektedir. WebSense yazılımından, 2004 yılında 26.6 milyon $'lık satış yapıldığı ve şirketin sonraki üç yılda yüzde 25'lik bir büyümeye sahip olacağı belirtilmektedir (84). Bu tür araçlar İnternet üzerindeki gezilen sitelere, alışveriş (İnternet müzayedesi, emlak), bilgi teknolojileri (bilgisayar güvenliği, bilgisayar korsanlığı, vekil önleme, arama motorları ve portal'ları), URL çevirim siteleri, web konakçılığı), cemiyet ve yaşam biçimleri (alkol, tütün, hobiler, kişisel web siteleri, ilişkiler ve çöpçatanlık, lokanta ve yemek), diğer (içerik teslim ağları, dinamik içerik, dosya indirme sunucuları, resim sunucuları, özel IP adresleri v.s.), dini, eğitim, eğlence, erişkin materyali, haberler ve medya, hükümet, İnternet haberleşmesi (web sohbeti, web tabanlı e-posta), ırkçılık ve nefret, iş arama, iş ve ekonomi (mali veri ve hizmetler), kumar, kürtaj, oyunlar, özel olaylar, sağlık, saldırgan ve aşırı, seyahat, şiddet, silahlar, spor, taraftar grupları, taşıtlar, toplumsal teşkilatlar, uygunsuz, uyuşturucu, yasal veya tartışmalı siteler gibi kategorilere göre önceden atanan kurallar çerçevesinde izin vermektedir (85). Şekil 5.20'de WebSense ile filtrelenmiş bir ağ üzerinde yasaklanan kategoride bir sayfaya gidilmek istendiğinde kullanıcının İnternet tarayıcısında çıkan örnek sayfa görülmektedir.

Şekil 5.20. WebSense ile filtrelenmiş örnek sayfa

20 çalışanı bulunan bir firmada, ek yükler dahil çalışan başına düşen bir saatlik maliyet 20 YTL ve İnternet üzerinde sörf edilirken geçen sürenin haftalık ortalaması da 8 saat ise, İnternet erişimini kısıtlamayan bir firmada bunun maliyeti, günlük 640 YTL; haftalık 3 200 YTL ve yıllık 150 400 YTL olarak hesaplanmaktadır (86).

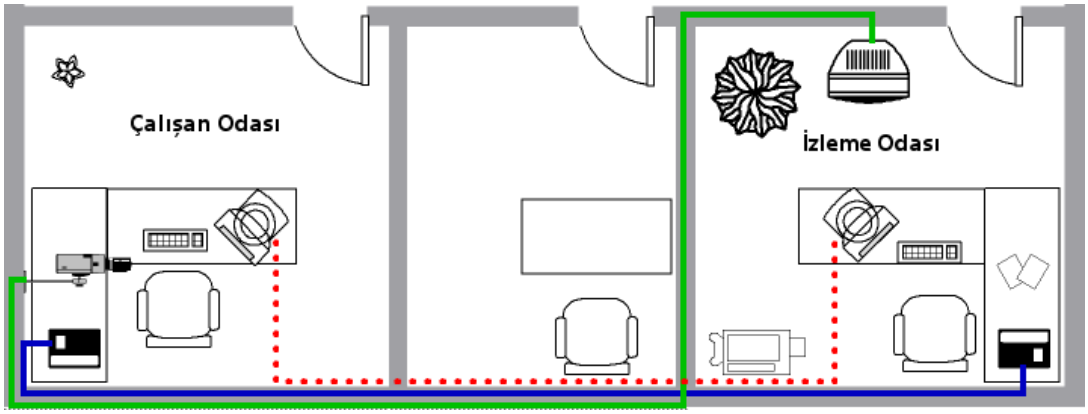
İşyeri gözetleme, bu tür filtreleme uygulamalarından daha farklıdır. İşverenlerin veya yöneticilerin, çalışanların işyerindeki faaliyetlerini, bilgileri dahilinde veya daha çok bilgileri olmadan gizlice izlemeleri, işyeri gözetleme (workspace surveillance) olarak adlandırılmaktadır.

İşyerinde iş ile ilgisi olmayan bilgisayar ve İnternet kullanımı dışında, çalışanların birbirlerine gönderebilecekleri kaba veya uygunsuz mesajların saptanması veya bu tür mesajların önüne geçilmesi de gerekmektedir. İşyeri gözetlemenin bir başka önemli amacı da şirket dahilinde hassas ve önemli bilgilerin üçüncü şahıslara aktarılmasını saptamak veya mümkünse engel olmaktır. Ticari sırlar ve iş stratejileri, bir çok firmanın en önemli varlıkları olduğundan; işyerinde kullanılan bilginin korunması gerekmektedir. Bunun sağlanmasında işyeri gözetleme, önemli bir bileşen olarak karşımıza çıkmaktadır.

İşyeri gözetleme şirketin yasal güvenilirliliğini temin etmek için ve çalışanların performansını ölçmek için kullanılabilir. İşyerinde yapılan gözetlemelerden biri de,

çalışanların çeşitli ulaşım araçları ile seyahat ettiği taşımacılık, kargo, taksicilik ve acil servisler gibi alanlarda yapılan gözetlemedir. Son günlerde ülkemizde de yaygınlaşan sistemde, uydu sistemleri ve cep telefonu şebekelerinin koordineli bir şekilde çalışması ile hazırlanan elektronik sistemlerle, taşıt içinde bulunan çalışanın nereye, ne zaman ve nasıl gittiği çevrimiçi olarak izlenebilmektedir.

Şekil 5.21'de gösterilmeye çalışıldığı gibi bir bina içinde yapılan işyeri gözetleme yönteminde bir çok elektronik yöntem kullanılmaktadır. Telefon görüşmelerinin dinlenmesi veya kaydedilmesi ve kamera ile gözetleme bu tür yöntemlerden birkaçıdır. Bilgisayar faaliyetlerinin elektronik olarak elde edilmesi için ise genelde faaliyet izleme (activity monitoring), uzaktan erişim ve klavye dinleme sistemleri kullanılmaktadır. Ayrıca bilgisayar loglarının incelenmesi ve paket koklayıcılarla ağ trafiğin gözetlenmesi de mümkündür.



Şekil 5.21. Telefon, video ve bilgisayar ile etkin işyeri gözetlemesi

Örneğin bunlardan paket koklama tekniği, aslında çoğu kullanıcının evinden İnternet'e bağlanırken bile farkında olmadan maruz kaldığı bir durumdur. Bir İnternet Servis Sağlayıcıdan (ISP, Internet Service Provider) İnternet'e erişen bir kişinin, hangi siteleri ne kadar sürede gezdiği; tıkladığı bağlantılar incelenerek sitede nelere ilgi duyduğu; kimlere e-posta attığı; aldığı veya gönderdiği e-postaların içeriği ve İnternet üzerinden ne gibi dosyalar indirdiği gibi bilgilerin elde edilmesi mümkündür. Çünkü ISP, kullanıcının İnternet üzerinden alıp gönderdiği tüm paketleri kendi bünyesinden aktarmaktadır. İşte, işyerlerinin ağ sisteminde teşkil edilecek bir paket koklayıcının ağ arayüzü ayrımsız kipte (promiscuous mode)

tutularak her türlü paket bilgisinin elde edilmesi mümkündür (87). Bu paketler, sistem performansının ve ağ hatalarının belirlenmesi için kullanıldığı gibi; kimin ne tür ağ haberleşmesi yaptığını da saptamak mümkündür. Özel filtreleme kurallarına göre iletilen paketleri inceleyen sistemler, bu paketlerde yer alan yasaklanan veya tehlikeli kelime veya ifadelere rastladığında bunu yetkili kişilere aktarabilir.

Uzaktan erişim, çalışanların bilgisayarlarına kurulan özel yazılımlarla başka bir bilgisayardan erişmeye, yönetmeye veya izlemeye yaramaktadır. Bu tür programlar rasgele zamanlarda çeşitli kişilerin bilgisayarlarının ekranlarını sistem yöneticisinin bilgisayarına da aktarabilir, bu ekran bilgilerini saklayabilirler veya ekranı bire bir görerek erişilen bilgisayarda her türlü işlemi yapabilirler.

Bilgisayarlar aslında yapılan bir çok işin izlerini kendi bünyelerinde tutmaktadırlar. İşletim sistemi ve uygulamaların tuttuğu log'lar, çeşitli programlar tarafından erişilen belgeler, İnternet tarayıcıların önbelleğinde ve tarihçelerinde tuttuğu dosya ve kayıtlar, e-posta yerel kopyaları bilgisayarın sabit diskinde yer almaktadır. Bunlara sistem yöneticileri, gün sonunda bizzat bilgisayara giriş yaparak veya uzaktan erişimle inceleyebilirler. Bilinçli kullanıcılar, çalıştıkları bilgisayarda iz bıraktıklarının farkında olmalı ve gerekli durumlarda bu izleri silebilmeli veya bu tür izleri silen ve bir çok casus savar yazılım programlarında tümleşik olarak bünyesinde bulunduran araçlardan faydalanmalıdır.

Çalışanların iş yerlerinde kullandıkları bilgisayarlarda yaptıkları işleri izleyen yazılımlar, klavye dinleme sistemleri veya faaliyet izleme programları olarak adlandırılmaktadır. Çalışanın bilgisayarına, bilgisi dahilinde veya haber vermeden kurulan ve sistem her çalıştığında kendiliğinden yürütülen böyle bir program, sahip olduğu yeteneklere göre kullanıcının klavyesini kullanarak yazdıklarını, açtığı, değiştirdiği ve sildiği dosyaların isimlerini, çalıştırdığı programları, İnternet üzerinde bağlandığı siteler ve görüntülenen sayfaların adreslerini, kendisine gelen veya kendisinin gönderdiği e-posta ve mesajları, yazıcıdan aldığı çıktılara ait belge bilgilerini v.s. gizlice elde edebilir; bu bilgileri şifreli olarak tutabilir ve e-posta, FTP gibi çeşitli yollarla yöneticilerine aktarabilir. Bu programlarda kullanılan görsel

gözetleme ile çalışma sırasında çeşitli zamanlarda ekran görüntüleri alınarak bunlarda yöneticilerin denetimine sunulabilir. Klavye dinleme sistemlerinin işyerinde bir başka kullanımı da çalışanın bir günde klavyeyi ne kadar kullandığının tutulmasıdır. Bu bilgiler hesaplanan normal değerlerin altında veya üstünde olduğu saptanarak çalışanın performansı ölçülebilmektedir.

İşyeri gözetleme, telefon dinleme ve kamera ile gözetim gibi tekniklerin daha önce de kullanılması ile yeni bir konu olmasa da klavye dinleme sistemleri gibi elektronik tekniklerle gözetim, işverene çalışanları üzerinde kullanabileceği geniş imkanlar sunmaktadır. Firmalar, bu imkanları çeşitli şekillerde değerlendirmektedir. Örneğin, 2001 yılında Amerika'da yapılan bir araştırmaya göre, ülkedeki firmaların %82'sinin işyerinde etkin izleme yaptığı belirtilmektedir (88). Çizelge 5.6'da gösterilen söz konusu araştırmanın sonuçlarına göre işyeri gözetlemesinin oldukça yaygın olduğu ortaya çıkmaktadır. 2005 yılında yinelenen araştırmanın ilginç sonuçlarından biri de şirketlerin %26'sı İnternet'in, %25'i e-postaların ve %6'sının telefonun kötüye kullanımını sebep göstererek çalışanların işlerine son vermesidir (89).

Çizelge 5.6. AMA (American Management Association) tarafından yapılan "Elektronik İzleme ve Gözetleme Araştırması" sonuçları

İşyeri Gözetleme	*2000*	*2001*	*2005*
Telefon konuşmalarının kaydı ve incelenmesi	%11,5	%11,9	%19
Sesli mesajların saklanması ve incelenmesi	%6,8	%7,8	%15
Bilgisayar dosyalarının saklanması ve incelenmesi	%30,8	%36,1	%50
E-posta iletilerinin saklanması ve incelenmesi	%38,1	%46,5	%55
İnternet bağlantılarının izlenmesi	%54,1	%62,8	%76
Çalışanların iş çalışmalarının video ile kaydı	%14,6	%15,2	%20
Telefon kullanımı (harcanan süre, aranan numara)	%44,0	%43,3	%51
Bilgisayar kullanımı (bilgisayara giriş zamanı, klavyede basılan tuşların sayıları, v.s.)	%19,4	%18,9	%21
Güvenlik amaçlı video gözlemi	%35,3	%37,7	%51
Toplam bütün çeşitlerde elektronik izleme ve/veya gözetim	%78,4	%82,2	Belirtilmemiş

İşyeri gözetlemede bilgisayar kullanımı konusunun, insan hakları, kişisel gizlilik ve iş ahlakı gibi alanlarda hukuki alt yapısında, Avrupa (90, 91) ve Amerika'da (92) çeşitli düzenlemeler getirilmektedir. Avrupa Birliği ülkelerinde, işyeri gözetlemede çalışanların e-posta trafiğini ve İnternet kullanımının izlenmesini yasaklayan ülkeler bulunduğu gibi bazı ülkeler iş yasası veya suç yasaları bağlamında işverenlere çeşitli

önlemlere olanak tanımaktadır (93). Haziran 2002 yılında Avrupa Birliği Konseyi yeni "Kişisel Gizlilik ve Elektronik Haberleşme Direktifi"ni parlamentoda oylayarak, üye ülkelerin cep telefonları, SMS, telefon, faks, e-posta, sohbet odaları, İnternet ve diğer elektronik haberleşme cihazları üzerinden gerçekleşen bütün haberleşmelere ait trafik ve konum verilerini elde etme hakkını tanımıştır (25). Ülkemizde bu konu yeni olduğundan, üzerinde yapılan bir çalışmaya rastlanmamıştır.

Çalışanların işyerinde gözetlenmesine dair, gerek işveren gerekse çalışan yönünden gerçekleşen çeşitli tartışmalar bulunsa da; işverenlerin belirli oranlarda çalışanının kontrol etmesi gerektiği genel olarak kabul görmektedir. Burada altı çizilmesi gereken husus, işyeri gözetlemede ne gibi ilkelere uyulması gerektiğinin doğru ve adil bir şekilde belirlenmesidir. Örneğin, işyerinde gözetleme yapıldığı ve bu gözetlemenin ne şekilde yerine getirildiği çalışanlara önceden haber verilmelidir. Bu konuda özellikle yeni katılan personel dahil, bütün çalışanlara belirli aralıklarla eğitim verilmelidir. Gözetleme yapılırken tutulan kayıtlar, özellikle çalışanların kişisel ve önemli bilgileri, güvenli bir şekilde saklanmalı; bu bilgiler sadece amaç kapsamında kullanılmalı ve üçüncü şahıslara iletilmemelidir. Böyle bir gereksinim doğrultusunda, bu tez çalışması için gerçekleştirilen klavye dinleme sisteminde, sistem açıldığında kullanıcıya "izlendiğine" dair bir mesaj alma imkanı da sunulmaktadır.

5.7.7. Kişilerin kendi kendilerini izlemesi

Klavye dinleme sistemleri, kişilerin kendi klavyelerini dinlemeleri için bilinçli olarak bizzat kendi sistemlerinde kullanılabilir. Bunun bir çok faydalı yönü söz konusu olabilir. Bu şekilde çalışan klavye dinleme sistemine, bir nevi günlük gözüyle bakılabilir. Sizin adınıza ve size hiç bir yük yüklemeden çalışmalarınızı çeşitli kategorilerde saklayabilir. Herhangi bir şekilde belli bir tarih ve zamanda yaptığınız bir şeyi görmek istediğinizde, bu tür programların getirdiği görüntüleme ve raporlama teknikleri ile hızlı bir şekilde bu bilgi karşınıza çıkacaktır. Görsel gözetleme yapan bir sistemde yapılan işlere ait ekran görüntülerini de beraberinde elde etmek mümkündür.

Klavye dinleme sisteminin kendi bilgisayarınızda bulunması, bazen hayat kurtaracak derecede fayda görebileceğiniz imkanlar sunabilir. Çoğu kullanıcı, Microsoft Word, Excel gibi bir çok paket program ile yoğun bir çalışma içindeyken, yaptıklarını kaydetmeyi unutabilmektedir. Program hatası sebebi ile programın sonlanması, işletim sistemi hatası sonucu sistemin çökmesi ve elektrik kesintisi gibi sebeplerle yapılan çalışmanın tamamını veya önemli bir kısmını kaybetmek mümkündür. Bu durum sizin veya çevrenizdeki kişilerin başına gelmiştir ve "bütün yazdıklarımı kaybettim" şeklinde şikayetlere rastlamışsınızdır. İşte klavye dinleme sistemini kendi bilgisayarında kullanan bir kişi, yazdığı her bilgiye o bilginin yazıldığı dosya kasten silinse bile erişebilir. Bu klavye dinleme sistemlerinin sağladığı gerçekten çok önemli bir kazanımdır.

Bunun dışında böyle bir sistemde, daha önce girdiğiniz ve sonra unuttuğunuz bir bilgiye erişmeniz de mümkündür. Kısa bir süre önce kayıt olduğunuz bir İnternet sitesine, kayıt olurken vermiş olduğunuz kullanıcı adı ve şifresini unuttuğunuzda; bir kaç gün önce gezdiğiniz fakat sık kullanılanlara eklemediğiniz ve tarayıcınızın tarihçesinde de bulunmayan bir adresi bulmak istediğinizde, klavye dinleme sisteminin tuttuğu kayıtlar işe yarayabilir.

Klavye dinleme sistemlerinin bu şekilde bir başka kullanım alanı, iş yerinde veya başka bir yerde açık tuttuğunuz veya bir süreliğine paylaştığınız bilgisayarınızda, yetkisiz ve izinsiz bir kullanım olup olmadığını saptayabilme imkanıdır. Bu durum ile bizzat bu çalışma sırasında karşılaşılmıştır. İşyerinde zaman zaman açık bırakılan bir bilgisayarda kurulu olan TürkSpyware klavye dinleme sisteminin görsel kayıtları arasında, bir kaç kez oyun oynandığı tespit edilmiştir. Klavye dinleme sisteminin olmadığı bir makinede bu tür geçmişe yönelik bilgileri alabilmek mümkün değildir.

Kendi bilgisayarında, kendisinin kontrol ettiği ve kurduğu bir klavye dinleme sisteminin bulunması, belki kendi kendimize casusluk yapmak veya başkalarının bilgisayarımıza bir şekilde eriştiğinde elde etmek isteyeceği bilgileri kendi elimizle sunmak gibi görülebilirse de klavye dinleme sisteminin yakaladığı bilgiler şifreli

olarak tutulduğundan, çözülmesi oldukça güç olan bu kayıtların başkasının eline geçmesi hiç bir anlam ifade etmeyecektir.

Sonuç olarak, klavye dinleme sistemleri zararlı olabilecek yönlerinin yanı sıra çok önemli faydalar sağlayabilecek sistemlerdir. Bu faydalarından bilgisayar kullanıcılarının, ebeveynlerin ve işverenlerin haberdar olması ve bu sistemleri faydalı ve verimli bir şekilde kullanma yollarının araştırılması ve tatbik edilmesi gerekmektedir. Takip eden kısımda, piyasada varolan klavye dinleme sistemleri incelenmiş ve bu sistemlerin sahip oldukları özellikler değerlendirilmiştir.

5.8. Mevcut Klavye Dinleme Sistemleri

Piyasada özellikle İnternet ortamında yayınlanan bir çok klavye dinleme sistemi bulunmaktadır. "Casus yazılımlara adanmış" projesini yöneten JSC adında bir Litvanya firmasının veritabanında, 474 adet klavye dinleme sistemi ve türevi bulunmaktadır (94). Bunların arasında Çizelge 5.7'de özellikleri ve bulaştığı sistemden elle nasıl temizleneceği belirtilen ve kim tarafından yazıldığı bilinmeyen bir Türk klavye dinleme sistemi türevi de bulunmaktadır.

Çizelge 5.7. Türkler tarafından yazıldığı belirtilen klavye dinleme sistemi türevi (TrojanSpy.Win32.ProAgent)

Tam adı:		TrojanSpy.Win32.ProAgent
İlgili dosyalar:		project1.exe, server.exe, trojanspy.win32.proagent.122.exe, 2027171645.dll, trojanspy.win32.proagent.122.scr
Tehlike seviyesi (/100):		50
Açıklama:		"Bu Türk klavye dinleme sistemi C++ programlama dili ile yazılmıştır. Tuş basımlarını kaydederek ve kayıt dosyasını korsanın e-postasına göndererek kullanıcıdan şifre kaçırmak için kullanılır."
Özellikleri:		Tuş basımlarını FTP veya E-posta ile kayıtları gönderir Kullanıcıdan saklanır. Arka planda kalıcı durur
Elle temizleme	*Prosesleri sonlandır:*	project1.exe, server.exe, trojanspy.win32.proagent.122.exe
	DLL'leri unregister ile kaldır:	2027171645.dll
	Dosyaları sil:	trojanspy.win32.proagent.122.scr, project1.exe, server.exe, trojanspy.win32.proagent.122.exe, 2027171645.dll, trojanspy.win32.proagent.122.scr

Mevcut klavye dinleme sistemlerini çeşitli ölçütlere göre değerlendiren Security Technology firması, en iyi klavye dinleme sistemlerini Haziran 2005 tarihi için Çizelge 5.8'deki gibi sıralamaktadır (95).

Çizelge 5.8. En iyi klavye dinleme sistemleri derecelendirmesi

Sıra	*Ürün Adı*	*İşletim Sistemi Desteği*	*Demo Sürümü*	*Bilgi Ele geçirme*	*Kayıt Gösterimi*	*Güvenlik*	*Ağ Seçenekleri*	*Toplam Puan*
1	PC Activity Monitor Pro (PC Acme Pro) 6.3	7.6	3	6.3	6.4	7.2	2.8	33.3
2	Keyboard Spectator Pro (KGB Spy) 3.30	7.6	8	2.6	4.8	3.8	2.7	29.5
3	Powered Keylogger 1.20	4.8	8	4.3	4	6.5	1.9	29.5
4	Handy Keylogger 3.24	10	8	3.6	2.8	2.3	1.2	27.9
5	WinSession Logger 1.5.0.3	9.3	8	3.9	2	1.5	2.7	27.4
6	Stealth Keylogger 3.1	9.8	8	3.6	2.8	1.5	1.2	26.9
7	Spytech SpyAgent Professional 4.4	7.6	3	5.4	3.5	4.4	1.9	25.8
8	All In One Keylogger 1.5	6.9	8	3.9	1.9	3	1.9	25.6
9	Stealth Keylogger 2.1	9.8	8	2.8	2.2	1.5	1.2	25.5
10	Perfect Keylogger 1.47	7.6	3	3.2	1.9	5.5	3.4	24.6
11	Golden Eye 3.11	7.6	8	4.1	2.8	1.4	0	23.9
12	Boss Everyware 2.6	7.6	5	2	3.1	2.1	3.3	23.1
13	Elite Keylogger 2.0	4.8	3	5.4	3	3.1	2.8	22.1
14	SpyBuddy 2.4	7.6	5	3.4	1.7	1.9	1.9	21.5
15	iOpus STARR PC & Internet Monitor 3.27	7.6	3	3.3	2	3.4	1.9	21.2
16	KeyKey 2002 Professional 1.22	7.6	5	3	1.2	2.2	1.2	20.2
17	KeySpy 7.51	7.6	5	1.2	0.2	2.4	1.9	18.3

Bu değerlendirmede her bir ana özelliğe ait verilen puanın, aşağıda belirtilen ölçütlere göre saptandığı, testi yapan firma tarafından belirtilmektedir:

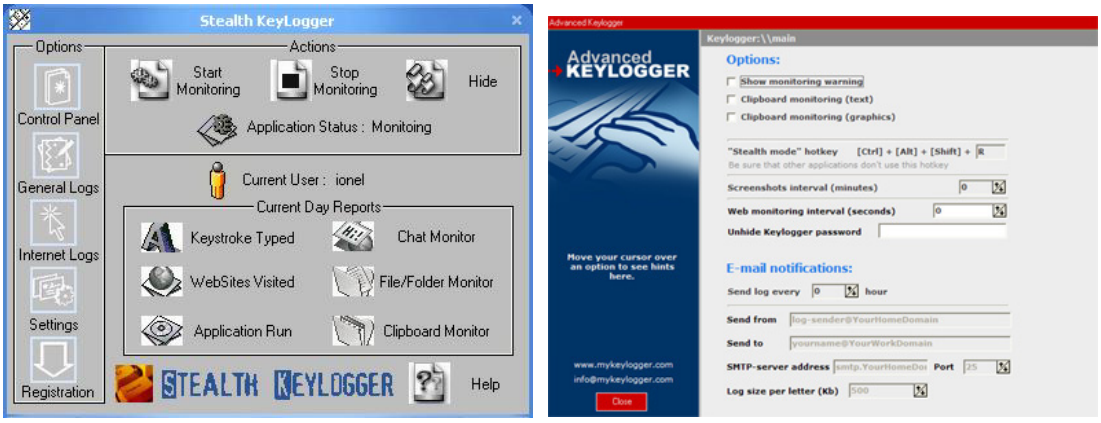
- İşletim sistemi desteği: Windows 2000 Professional, XP Home / Professional, Server 2003, ME, 98, NT Workstation, 95 işletim sistemlerini destekleyip desteklemedikleri
- Demo sürümü: Bedava yazılım, özelliklerin sınırlanmadığı deneme sürümü, özellik sınırlamalı deneme sürümü ve demo veya deneme sürümünün bulunmaması
- Bilgi Ele geçirme: Evrensel kod (Unicode) dillere ait tuş karakterlerini, uluslararası evrensel olmayan dillere ait tuş karakterlerini, MS-DOS konsolundaki tuş basımlarını, sistem giriş şifrelerini, dosya sistemi

faaliyetlerini, sistem kullanıcı çıkışlarını (log off), kapatmalarını ve kış uykusu modunu (hibernate), fare tıklamalarını, ICQ, MSN, YIM ve AIM gibi sohbet programlarında sohbet eden her iki tarafın konuşmalarını, sistem girişi tarih, zaman ve kullanıcı bilgilerini, yazıcı kuyruğunu, olayların zaman damgalarını, mikrofon sesini, pano kopyalama ve yapıştırmalarını, açılan pencerelerin statik ve düzenleme kutularının içeriklerini, web kamerasından video, zaman çizelgesi ile izlemeye, izlenecek veya izlenmeyecek programları filtreleme, ziyaret edilen İnternet adresleri, ekran görüntüleri, seçimli şifre ve güvenli web formu yakalaması, açılan pencerelerin başlıkları gibi yetenekler

- Kayıt gösterimi: Çoklu dilde arayüz, rapor biriminde SQL benzeri sorgulamalar oluşturabilme, çeşitli günleri seçerek raporlama, gösterimden sonra şifresi çözülen kayıtların otomatik silinmesi, anahtar sözcük ile arama yapabilme, ölçütlere göre bilgi seçimi, kayıt dosyalarının yedeğinin alınması, takvim tabanlı sorgulama, HTML raporu, Excel CSV raporu, DOC/RTF raporu, kayıt görüntüleme için ayrı program, kayıt dosyasının sıkıştırılması, salt metin raporu
- Güvenlik: Görünmez çalıştırılabilir modüller, görünmez kayıt dosyaları, görünmez sistem kütüğü girişleri, çalıştırılabilir modüllerin bütünlüğünün kontrolü, Görev Yöneticisi'nden gizlenme, anormal kapanmalarda bilgi kaybının önlenmesi, çalıştırılabilir modülleri rasgele isimlendirmek, kurulum paketi tek bir diskete sığabilmesi, belirlenen tarih ve zamanda otomatik kaldırma, dosyaların elle yeniden adlandırılması, kayıt dosyalarının şifrelenmesi, kayıt dosyalarını gönderebilmek için birden fazla e-posta hesabı tanıtabilme, korumalı program kaldırılması, program yapılandırılmasında gizli kelime kullanımı, kısayol tuşları ile program yapılandırma, yapılandırmayı değiştirebilmek için yönetici hakkının gerekli olması, kurulum ve kaldırma için yönetici hakkının gerekli olması, izleme yapıldığına dair uyarı ekranı seçenekleri
- Ağ seçenekleri: İstemci/sunucu mimarisi, izlenen bütün sistemlerinin durumlarını görmeye olanak veren Ağ Yöneticisi, büyük ağlar için kolay

otomatik kurulum, kayıt dosyalarının e-posta ile gönderilimi, paylaşılan ağ sürücülerine kayıt dosyalarının kaydedilmesi, anahtar sözcük girildi uyarısı, kayıt dosyalarını gönderiminin test edilebilmesi, kayıt dosyalarının FTP ve HTTP ile gönderilmesi, pencere başlıklarında anahtar sözcük bulundu uyarısı, otomatik telefon arama, haberleşme için açık kapıların kullanımı

Şekil 5.22'de görüldüğü gibi klavye dinleme sistemlerinin bir çoğu, kuruldukları sistemde çalışma özelliklerinin ayarlanmasını sağlayan bir arayüz sunarlar. Bu arayüz, genelde gizli bir tuş kombinasyonu ile ortaya çıkar. Yapılandırma bir defa yapılınca gerek görülmediği takdirde bir daha değiştirilmez.



Şekil 5.22. Değişik klavye dinleme sistemlerinin örnek yapılandırma ekran görüntüleri

Mevcut klavye dinleme sistemleri ile bu tez çalışmasında geliştirilen ve Bölüm 7'de ayrıntılı olarak tanıtılacak olan, TürkSpyware klavye dinleme sisteminin karşılaştırmalı özellikleri Çizelge 5.9'da ayrıntıları ile listelenmektedir.

Çizelge 5.9. TürkSpyware ve mevcut klavye dinleme sistemlerinin özellikleri (X: özellik mevcut, -: özellik mevcut değil, P: planlanıyor)

	TürkSpyware	*007 Spy Software*	*Advanced KEYLOGGER*	*All In One Keylogger 1.5*	*Golden Eye*	*ELITE Keylogger 2.1*	*PC Activity Monitor*	*Perfect Keylogger*	*Powered Keylogger*	*Real Spy Monitor*	*SpyBuddy*	*Stealth Keylogger*	*WinSession Logger*	*Ghost keylogger*	*Boss Everyware*
Sürüm no	2.1	3.6	1.7	1.57	4.01	2.1	6.3	1.47	1.3	2.33	3.5	2.1	2.0.2	3.8	2.84
Sürüm tarihi (ay.yıl)	6/05	11/04	7/04	12/04	-	6/05	12/03	-	10.04	6/05	-	-	-	-	4/05
Dosya büyüklüğü	600 KB	2.4 MB	1.2 MB	2.8 MB	1.6 MB	4.35 MB	-	472 KB	2.6 MB		1.7 MB	-	-	611 KB	-
Fiyat	-	40$	40$	40$	30$	70$	150 $	35$	70$	40$	50$	20$	25$	50$	50$
Tuş İzleme	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X
Sistem Tuşları İzleme	X	X	X	X	-	X	-	X	X	-	X	-	-	-	X
Fare İzleme	X	-	-	-	-	-	-	X	X	-	-	-	X	-	-
Gezilen Pencerelerin Tutulması	X	X	-	X	X	X	X	X	-	X	X	-	X	X	X
Windows ile Başlangıç	X	X	-	-	X	X	X	X	X	X	X	-	-	X	X
Kullanıcı Tabanlı Başlangıç	P	X	-	-	-	X	-	-	X	X	X	-	-	-	X
Otomatik Etkin Başlangıç	X	X	X	X	X	X	-	-	X	X	X	-	-	X	-
Değiştirilebilir Ortaya Çıkarma Kısa yol Tuşları	X	X	X	-	X	-	-	X	X	X	X	X	-	X	-
Windows Görev Yöneticisinden Gizlenme	X	X	X	X	X	X	X	X	-	X	X	X	X	X	-
Başlangıçta İzleme Yapıldığına Dair Mesaj	X	-	X	-	-	-	-	-	-	-	X	-	-	-	X
Zaman Tablosu Belirterek Çalışma	P	X	-	-	-	-	-	X	X	-	X	-	-	-	X
E-posta ile log teslimi	X	X	X	X	-	X	-	X	X	X	X	X	X	X	X
FTP ile log teslimi	X	X	-	-	-	-	-	X	-	-	-	-	X	-	-
HTML Log aktarımı	P	X	-	X	X	-	X	X	-	X	X	-	-	-	X
Değiştirilebilir Log dosyası konumu	X	-	-	-	X	-	X	X	-		X	-	-	X	-
Disk Kotasında Log Silme	P	X	X	-	-	-	-	X	-	-	-	-	-	-	-
Log Sınırı Aşıldığında Log Silme	P	X	-	X	X	X	-	X	-	X	X	X	-	-	X
Log Şifreleme	X	-	-	X	-	X	X	-	-	-	-	-	-	X	-
Log Görüntüleyici ve Arama Motoru	X	X	-	X	X	X	X	X	X	X	X	-	X	-	X
Ziyaret Edilen Web Site Adreslerini Kaydetme	X	X	X	X	-	X	X	X	X	X	X	X	X	X	X
Netscape Desteği	P	X	-	-	-	-	-	-	-	-	X	-	X	X	X
Opera Desteği	-	X	-	-	-	-	-	-	-	-	X	-	-	-	X
Mozilla FireFox	-	-	-	-	-	-	-	-	-	-	X	-	-	-	X
Periyodik Ekran Görüntüsü Alma	X	X	X	X	X	X	-	X	X	X	X	-	X	-	-
JPG Formatta Ekran Görüntüsü	X	X	-	X	X	-	-	X	-	-	-	-	-	-	-
Ekran Görüntülerinin Slayt Gösterisi	P	X	-	-	-	-	-	-	-	-	-	-	-	-	-
Ekran Görüntüsüne Bilgi Ekleme	-	X	-	-	-	-	-	-	-	-	-	-	-	-	-
Aktif Pencere/Tüm Ekran	X	X	-	-	X	-	-	-	-	X	X	-	X	-	-
Fare Tıklamalarının Görüntüsü	X	-	-	X		-	-	-	-	-	-	-	X	-	-

Çizelge 5.9. (Devam) TürkSpyware ve mevcut klavye dinleme sistemlerinin özellikleri (X: özellik mevcut, -: özellik mevcut değil, P: planlanıyor)

	TürkSpyware	*007 Spy Software*	*Advanced KEYLOGGER*	*All In One Keylogger 1.5*	*Golden Eye*	*ELITE Keylogger 2.1*	*PC Activity Monitor*	*Perfect Keylogger*	*Powered Keylogger*	*Real Spy Monitor*	*SpyBuddy*	*Stealth Keylogger*	*WinSession Logger*	*Ghost keylogger*	*Boss Everyware*
Mikrofon ile ses kaydı	-	-	-	X	-	-	-	-	-	-	-	-	-	-	-
Anahtar sözcük saptama	X	-	-	-	-	X	-	-	-	-	-	-	-	-	-
Windows logon şifresi	-	-	-	-	-	X	X	-	X	-	-	-	X	-	-
Çekirdek modu	-	-	-	-	-	X	-	-	X	-	-	-	-	-	-
Açık kapılar	P	-	-	-	-	X	-	-	-	-	-	-	-	-	-
Uzaktan Erişim	-	-	-	-	-	X	X	X	-	-	-	-	-	-	-
Güvenlik Duvarlarına Koruma	-	-	-	-	-	-	X	X	X	-	-	-	-	-	-
Kullanım Olmadığında Geçici Olarak Duraklatma	X	X	-	-	X	X	-	-	X	-	X	-	X	-	-
İş parçacığı önceliği ayarı	-	-	-	-	-	-	X	-	-	-	X	-	-	-	-
E-posta izleme	-	-	-	-	-	X	-	-	-	-	-	-	-	-	-
Çalıştırılan Programların Tutulması	X	X	-	X	X	-	X	-	X	X	X	X	X	X	-
Yazıcı Çıktısı Alınan Belgelerin Bilgilerinin Tutulması	X	-	-	-	-	-	-	-	-	-	X	-	-	-	-
Windows Explorer'dan Açılan Belge Bilgilerinin Tutulması	X	X	-	-	-	-	-	-	-	X	-	-	-	-	-
Disk Aktivitesi	X	X	X	-	X	X	-	-	-	-	X	X	X	-	-
Pano Metin Değişimlerini Tutma	X	-	X	X	X	X	X	X	-	-	-	X	X	-	-
Pano Grafik Değişimlerini Tutma	P	-	X	-	-	X	-	-	-	-	-	-	X	-	-
Uygulama Filtreleme	P	-	-	-	-	X	-	-	-	X	X	-	X	-	X
İnternet sitesi Filtreleme	P	-	-	-	-	-	-	-	-	X	X	-	X	-	X
Parola Koruması	X	X	X	X	X	X	-	-	-	X	X	X	-	-	X
Casus Yazılım Koruma Programlarına Karşı Önlem	P	X	-	-	-	-	-	X	X	-	X	-	-	-	-
Log Dosyasının Tarihini Geriye Alma	P	-	-	-	-	-	-	-	-	-	X	-	X	-	-
Win95	-	-	X	-	X	-	-	X	-	-	X	-	-	X	-
Win98	-	X	X	X	X	-	-	X	-	-	X	-	-	X	-
WinMe	-	X	X	X	X	-	-	X	-	-	X	-	-	X	-
WinNT	X	X	X	-	-	-	-	X	-	-	X	-	-	X	-
Win2000	X	X	X	X	X	X	-	X	X	-	X	-	-	X	-
WinXP	X	X	X	X	X	X	-	X	X	-	X	-	-	X	-
Demo sürümü	P	X	X	X	X	X	X	X	X	-	-	-	X	X	X
CD/USB kullanımı	X	-	-	-	-	-	-	-	-	-	-	-	-	-	-
MAC ve IP adresleri	X	-	-	-	-	-	-	-	-	-	-	-	-	-	-
Fare tıklama görüntüsü boyut ve kalitesi	X	-	-	-	-	-	-	-	-	-	-	-	-	-	-
İlgilenen uzantıda dosyalardaki değişimlerin izlenmesi	X	-	-	-	-	-	-	-	-	-	-	-	-	-	-
Türkçe	X	-	-	-	-	-	-	-	-	-	-	-	-	-	-
Maxthon	X	-	-	-	-	-	-	-	-	-	-	-	-	-	-

Sonuçta, piyasada mevcut bulunan yazılımlar ile bu tez çalışmasında geliştirilen yazılım karşılaştırıldığında, yaklaşık 500 kadar klavye dinleme sistemi arasında gerçekleştirilen yazılımın, ülkemizde ileri seviyede özellikleri olan bir klavye

dinleme sistemi olması, bu çalışmanın en önemli güdü kaynaklarından birisidir. Bölüm 7'de bu çalışma için hazırlanan klavye dinleme sistemi TürkSpyware yazılımı ayrıntılı olarak tanıtılacaktır.

Klavye dinleme sistemlerinin, geniş bir alanda kullanım alanlarının olmasına ve piyasada mevcut yüzlerce yazılım klavye dinleme sistemi ile çok sayıda donanım klavye dinleme sisteminin bulunmasına rağmen, klavye dinleme sistemleri konusunda çoğu kullanıcının hatta bilgi ve bilgisayar güvenliği konusunda çalışan uzmanların bile bu konuda yeterli bilgiye sahip olmadığı değerlendirilmektedir. Klavye dinleme sistemlerinin kötü niyetli kullanım yollarının yanı sıra, çok faydalı kullanım alanlarının bulunduğu göz ardı edilmemelidir. Bunlardan özellikle çevrimiçi bankacılık, işyeri gözetleme ve çocukların bilgisayar ve İnternet kullanım güvenliğinin sağlanması gibi hususlar, üzerinde çalışılması ve klavye dinleme sistemlerinin bu konularda değerlendirilebilecek şekilde düzenlenmesinin sağlanması gerekmektedir. Yine de klavye dinleme sistemlerinin kötü niyetli kullanımlarına karşı gerekli tedbirlerin alınması ve uygulanması, bilgi ve bilgisayar güvenliği konusunda göz ardı edilemeyecek kadar önemli bir konudur. Klavye dinleme önleme sistemleri hakkında ayrıntılı bilgi Bölüm 6'da sunulmaktadır.

6. KLAVYE DİNLEME ÖNLEME SİSTEMLERİ

Bu bölümde, hem donanım hem de yazılım klavye dinleme sistemlerine karşı ne tür önlemler alınabileceği; mevcut klavye dinleme önleme sistemlerinin ne tür bir koruma sağladığı veya sağlayabileceği ve yazılım klavye dinleme önleme sistemlerinin kullanabileceği yaklaşımlar incelenmiştir. Son yıllarda artık klavye dinleme sistemleri, kötü niyetli kişiler tarafından büyük çapta vurgunlar yapmak amacıyla bile kullanılmaktadır. Bunlar arasında, 2005 Mart ayında klavye dinleme sistemlerini kullanarak gerçekleştirilmek istenen 420 milyon $'lık bir soygun yapma girişimi, bunlardan en dikkat çekici olanıdır (96).

Bu yüzden, klavye dinleme yapan casus yazılımların ciddiye alınması ve gereken önlemlerin dikkatli bir şekilde yerine getirilmesi gerekmektedir. Aslında casus yazılımlara karşı alınacak bir çok tedbir klavye dinleme sistemlerinin, bilgisayar sistemlerine bulaşmasını da önleyecektir. Bunun için 3. ve 4. bölümde anlatılan casus yazılımlara yönelik tedbirler klavye dinleme sistemlerine karşı da geçerli olabilmektedir.

Mevcut casus savar yazılımların etkin bir şekilde klavye dinleme sistemlerine karşı güvenlik sağlandığını kabul etmek, şu an için mümkün gözükmemektedir. Casus savar yazılımların, en tehlikeli casus yazılımlardan biri olan klavye dinleme sistemlerini de korunma şemsiyesine alması gerekmektedir. Böylelikle tümleşik bir casus yazılım koruması sağlanmış olacaktır.

6.1. Klavye Dinleme Sisteminin Varlığını İşaret Eden Bulgular

Bölüm 4.1'de "Bir Bilgisayarda Casus Yazılımın Olduğuna İşaret Eden Bulgular" başlığı altında anlatılanlar, klavye dinleme sistemlerinin varlığına da işaret edebilir. Bunun dışında klavye dinleme sisteminin, çalışılan sisteme bulaştığını gösteren diğer özel bulgulardan burada belirtmekte fayda vardır. Bunlar:

- Klavyede bastığınız bazı tuşlar çalışmıyorsa
- Klavyeye bastığınız tuşa ait karakterin ekranda görünmesi uzun sürüyorsa
- Klavyede hızlı veri girerken ekrandaki yansıması daha yavaşsa
- Fare tıklamalarında bazen beklediğiniz tepkiyi almıyorsanız
- Fare çift tıklamaları veya sürükle bırak işlemi çalışmıyorsa,

sistemde bir klavye dinleme sisteminin varlığından şüphelenebilir. Bu bulguların başka sebeplerden de kaynaklanacağı da unutulmamalıdır. Ama şüpheci olup sisteminizi gözden geçirmek, ileride olabilecek zararlara karşı erken tedbir alınmasını sağlayacaktır.

6.2. Donanım Klavye Dinleme Sistemlerine Yönelik Tedbirler

Donanım klavye dinleme sistemleri, Bölüm 5'de anlatıldığı gibi, oldukça tehlikeli ve fark edilmesi bir o kadar zordur. Normal PS/2 klavyeler için bu tehdit olasılığı çok daha yüksektir. Bunun için bilgisayarınızı açmadan önce ve öğle mesaisine başladığınızda, bilgisayar kasanızın arkasını kontrol etmekte fayda olabilir. Uygulaması biraz zor gibi gözükse de, klavyenin içine ve kasanın içine belli aralıklarda bakmak da gerekebilir. Takip eden alt başlıklarda, donanım klavye dinleme sistemlerine karşı kullanılabilecek farklı klavye sistemleri gözden geçirilmiştir. Ayrıca, önemli bilgiler girerken klavye dinleme sistemlerini tamamen sağır edecek sanal klavyeler de incelenecektir.

6.2.1. Kablosuz, kızıl ötesi, bluetooth ve lazer klavyeler

Bölüm 5.1'de "Klavye ve Çalışma Prensipleri" kısmında belirtildiği gibi, pek çok kullanıcı geleneksel türde PS/2 klavye kullanmaktadır. Fakat son senelerde kablo ile bilgisayara bağlanmayan klavye modelleri piyasalarda bulunmaktadır. Bu modeller donanım klavye dinleme sistemlerine karşı bir tedbir olarak kullanılabilir. Bu tür klavyeler ayrıca bilgisayar masanızda kablo karmaşasının önüne de geçeceğinden ayrıca tercih edilebilir.

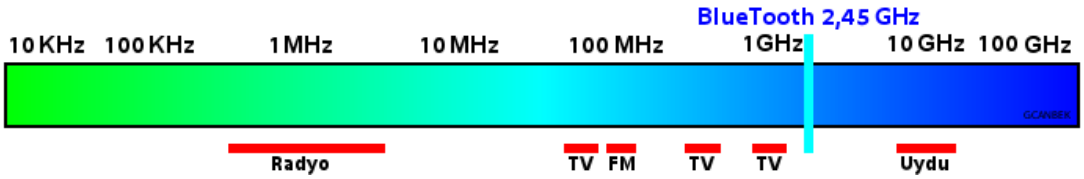
Resim 6.1'de bir örneği verilen kablosuz klavyelerin ilk modelleri radyo frekansı ile çalışmaktadır. Klavyenin belli bir frekansta yaptığı yayın, bilgisayar kartı tarafından algılanır ve yayınlanan dalgada yer alan klavyede basılan tuş bilgisinin kodlarına göre tuş bilgisi sisteme iletilir.

Resim 6.1. Kablosuz klavye ve fare

Bu tür klavyeler, donanım klavye dinleme sistemlerinin önüne geçebilir. Fakat bu tür klavyelerin yaptıkları yayınların yakınlarda bulunan başka bilgisayarlardan da yakalanabildiğine dair çeşitli haberler çıkmıştır. Bu haberlerden birine göre, Norveç'te ayrı apartmanlarda oturan ve aynı marka ve model kablosuz klavyeye sahip iki kişi, aynı anda bilgisayarlarını kullandıklarında birbirlerinin klavyeden girdiği bilgileri kendi ekranlarında görmüşlerdir (97). Teorik olarak 20 m çapında etkili olan bu yayının, böyle uzak mesafelerden algılanabilmesi, radyo konusunda uzman kişilerin "yerel hava koşullarının ya da ekranlanmamış güç kabloların radyo sinyallerinin menzilini artırmaya sebep olduğu" görüşü ile açıklanabilir. Bu tür klavyeler, belirli sayıda radyo kanalı seçeneği ile, örneğin bir ofis içinde sistemlerin karışmasını önlemeye çalışmaktadırlar. Fakat radyo sinyalleri, duvarları bile geçtiğinden; klavye dinleme sistemine önlem olarak düşünülen RF kablosuz klavyeler bizzat klavye dinlemeye olanak tanımaktadır.

Bir diğer kablosuz klavye türü de kızılötesi ışınlarla çalışan klavyelerdir. Televizyon uzaktan kumandasından yayılan ışının duvarlardan geçmediği ve bu ışın hedefe (televizyona) doğru yöneltilmediğinde sistemin çalışmadığını herkes tecrübe etmiştir. Bu yüzden kızılötesi kablosuz klavyeler, klavye dinleme açısından daha güvenilir donanımlardır.

Son günlerde kablosuz iletişim ile ilgili en yaygın yeni uygulamalardan biri de bluetooth teknolojisidir. Şekil 6.1'de gösterildiği gibi 2,45 GHz frekansta çalışan bu radyo frekansı teknolojisi, cep telefonları, dizüstü ve avuçiçi bilgisayarlar, müzik sistemleri ve klavyelerin kablosuz iletişim kurabilmesi için kullanılmaktadır. 2,45 GHz frekansı ISM (Industrial, Scientific and Medical) olarak adlandırılan endüstriyel, bilimsel ve tıbbi cihazların kullanımı için daha önce ayrılmış bir frekanstır.



Şekil 6.1. Uluslararası radyo frekans tahsisi

Kablosuz ve kızılötesi iletişimde, iletişim cihazlarında yaşanan senkronizasyon sorununu gideren bluetooth, aynı zamanda gerçekleştirme maliyeti düşük bir radyo standardıdır. Bluetooth, diğer yayın yapan kaynaklarla karışımı önlemek için iki yaklaşım sunmaktadır:

- Güç seviyesi 1 mili vat düzeylerinde zayıf sinyal içeren bluetooth araçları daha yüksek güçte yayın yapan sinyallerle karışıma girmeyecektir. Bu sayede bilgisayar veya cep telefonu gibi vat seviyelerinde yayın yapan diğer ISM cihazları ile karışma şansı oldukça düşük olacaktır. Düşük güç seviyesinin tek olumsuz yanı yayın çapının 10 metreye düşmesidir.
- Bluetooth cihazlarının bir birleri ile karışımını önlemek için kullanılan teknik yayılı izge frekans atlamasıdır (spread-spectrum frequency hopping). Bu teknik ile saniyede 1600 kez rasgele frekans atlaması yapılmaktadır. Bu sayede bluetooth cihazları birbirleriyle karışım olmadan rahatlıkla iletişim kurabilmektedir.

Donanım klavye dinleme sistemlerine karşı, Resim 6.2'de bir örneği gösterilen, bluetooth teknolojisine sahip klavyeler iyi bir çözüm olarak kullanılabilir. Klavye ile

ilgili son gelişmelerden birinden de bu kısımda bahsetmede fayda görülmektedir. Klavye alanında ileri gelişmelerden biri de sanal lazer klavyelerdir.

Resim 6.2. Bluetooth klavye ve fare (solda), USB alıcı/verici (sağda) (98)

Masaüstü, dizüstü ve avuç içi bilgisayarların yanında; uyumlu cep telefonları, akıllı telefonlar ve PDA'lar (Kişisel Sayısal Asistan - Personal Digital Assistant) ile beraber de kullanılabilen sanal lazer klavyeler mevcuttur. Resim 6.3'de buna bir örnek verilmiştir. Bu klavyelerde, lazer ışınları ile yansıtılan bir yüzeyde tuşlara basılma, optik algılama ile çözümlenmekte ve bu sayede girilen bilgi istenen bilgisayara iletilmektedir.

(a) Çalıştırılmadan önce (b) Çalıştırılınca

Resim 6.3. Sanal lazer klavye cihazı

Bu cihazlar kullanıcıya tuşlama hissini verebilmek için kullanıcının yüzeye dokunmasını algıladığında sanki bir klavyeye basılıyormuş gibi ses bile üretebilmektedirler (99).

Klavyeler ve donanım klavye dinleme sistemleri ile ilgili bir hususu belirtmekte fayda vardır. Her ne kadar yukarıda bahsedilen yeni teknolojide, klavyeler PS/2 türünde klavyeler için geliştirilen donanım klavye dinleme sistemleri için bir çözüm olarak düşünülse de ileride bu klavyeyi dinleyen donanım klavye dinleme sistemlerinin çıkmayacağını kimse garanti edemez.

6.3. Sanal Klavyeler

Bu kısımda, bir çok donanım ve yazılım klavye dinleme sistemlerinin önemli bilgileri almasını önleyebilmek amacıyla kullanılabilecek bir girdi modülü olan sanal klavyeler gözden geçirilecektir. Sanal klavyeler, bir klavyede yer alan bütün tuşların genelde, klavyedeki yerlerine göre dizildiği bir penceredir. Kullanıcılar, bilgi girmek için normal bilgisayar klavyelerini kullanmak yerine; yazılarını yazmak istedikleri alana tıkladıktan sonra sanal klavye üzerinde fare ile tıkladıkları tuşlara ait karakterleri o alana bastırırlar. Microsoft, işletim sisteminde Madentec Limited (100) şirketinden lisansını satın aldığı bir sanal klavyeyi (On-Screen Keyboard) Start | Accessories | Accessibility | On-Screen Keyboard menüsünde kullanıcıların hizmetine sunmaktadır. Genelde engellilerin kullanımı için düşünülen Şekil 6.2'de ekran görüntüsü gösterilen bu program, önemli bilgi girişleri sırasında rahatlıkla kullanılabilir.

Şekil 6.2. Microsoft işletim sisteminde yerleşik sanal klavye (On-Screen Keyboard)

Bu program bir sanal klavyenin yapabileceği bir çok işi yerine getirebilmektedir. "Enhanced Keyboard" seçeneğinde nümerik alan bölümü yer alırken; "Standard Keyboard" modunda bu bölüm yoktur. Klavyedeki tuşların yerleşimi iki şekilde

olabilmektedir. “Regular Layout”da tuşlar normal klavyedeki gibi dizilirken “Block Layout”da en sık kullanılan karakterler birbirlerine yakın olarak dizilmektedir. Ayrıca, sanal klavyede var olan tuş sayıları da klavye türlerine göre belirlenmektedir. ABD standart klavye için 101 tuşluyu; evrensel klavye için 102 tuşluyu; ilave Japon karakterleri için 106 tuşlu düzeni seçmek yeterlidir. Türkçe klavye modu için Settings | Font menüsünden Script seçeneği olarak Turkish seçilmelidir.

Bu sanal klavyenin bir özelliği de tuşlara fare ile tıklamak yerine, belirlenen bir sürede o tuşun olduğu yerin üzerinde fare işaretçisini tutarak karakter gönderimi yapabilmektir. Bunun için Settings | Typing Mode menü seçeneği ile çıkan diyalogda “Hover to select” seçeneği seçilmelidir. Burada tuş üzerinde bekleme süresini de değiştirmek mümkündür.

6.4. Güvenli Bilgi Girişi Nasıl Sağlanır?

Önemli bir bilgiyi veya şifreyi özellikle İnternet kafe, üniversite bilgisayar laboratuarı gibi umuma açık bir bilgisayarı veya bir başkasının bilgisayarını kullanarak yaptığınızda klavye dinleme sistemlerine karşı biraz daha dikkat etmeniz gerekmektedir. Öncelikle böyle bir durumda salık verilebilecek birinci şey “mümkünse bu tür bilgisayarlardan böyle önemli verilerin girilmemesidir”. Bu konuda çözüm olarak sunulan önerilerin neler sağladığı ve ne gibi açıklarının olabileceği Çizelge 6.1’de sıralanmaya çalışılmıştır.

Çözüm önerileri ve bunlara karşı yürütülebilecek faaliyetler aslında saymakla bitmez. Bütün bunlar değil ileri seviyede kullanıcının; sıradan kullanıcının bile kafasını karıştıran şeylerdir. Casus yazılımlara karşı mücadelede önerildiği gibi, klavye dinleme sistemlerine karşı mücadele de önemli sorumluluğu profesyonel klavye dinleme önleme sistemlerine bırakmak akla en yatkın çözüm olarak karşımıza çıkmaktadır.

Çizelge 6.1. Güvenli bilgi girişi ile ilgili çözüm önerileri ve olumlu/olumsuz yanları

Çözüm Önerisi	*Olumlu Yanları*	*Olumsuz Yanları*
Bilgisayarı temiz bir CD ile başlatılarak bilgi girişi yapmak	Bu durumda bir çok casus yazılım devre dışı kalabilir.	Uygulanması zor. Makinede donanım klavye dinleme sistemi olabilir.
Notepad'te yazılacak şifre aralarına rasgele karakterler girilerek yazılır ve bunların arasından şifre karakterleri seçilip kopyalanıp bilgi girişi yapılacak yere yapıştırılır	Klavye dinleme ile elde edilen bilgi anlamsız olduğundan şifrenin anlaşılması zordur.	Pano faaliyetlerini izleyen klavye dinleme sistemleri her yapıştırmayı saptayacaktır.
Sanal klavye kullanmak	Yazılım ve donanım ile klavye dinlemeye karşı iyi bir çözüm	Fare hareketlerini algılayan klavye dinleme sistemleri bu tür bilgi girişlerini yakalayabilir. Sanal klavye kullanımında bulunulan ortamdaki başka kişi yazdıklarınızı görebilir.
USB bellek kartında daha önceden var olan şifre bilgilerini fare hareketleriyle İnternet formlarına dolduran programlar kullanmak	Klavye dinleme ile bilgi edinmeyi önler	İnternet formlarında girilen bilgileri şifreleyip göndermeden önce yakalayabilen form yoklayıcılar (form sniffer) bilgi nasıl girilirse girilsin bu bilgileri elde edebilir.
USB sürücüden taşınabilir İnternet tarayıcı (Portable Firefox gibi) kullanılması	Casus yazılımlara karşı daha fazla korunma sağlayabilir	Yine de aşılması imkansız değildir
İnternet kafe gibi yerlerde kendi dizüstü bilgisayarınızı kullanmak	Başka bilgisayarlarda yer alacak casus yazılımlar bertaraf edilir.	Bağlanılan ağ üzerinde bulanabilecek diğer donanım yoklama araçları ile bilgisayarınıza erişilebilir; gerçekleştirdiğiniz trafik ağ üzerinde her hangi bir noktadan izlenebilir.
WWW için hazırlanan İnternet üzerinden bilginin şifrelenip tekrar şifre çözülmesi ile güvenli veri iletimi sağlayan HTTPS protokolünün kullanımı	Ağ üzerinde taşınan bilginin daha güvenli iletilmesini sağlar.	Bu protokolün kullandığı SSL, Secure Sockets Layer, Güvenli Soket Katmanı algoritmasının kırılabildiğini bilmek gerekir.
Tek kullanımlık şifre	Şifre her hangi bir yolla başkalarının eline geçse bile hesabınıza daha sonra bu şifre ile kimse giriş yapamaz	Kötü niyetli kişilerin tek amacı sizin hesabınızı kontrolünü tamamen elinize geçirmek değil de girdiğiniz sayfaları izlemek veya hesap durumunuzu görmek olabilir. Bu bazı kişiler için sisteme giriş bilgilerinin çalınmasından çok daha önemli olabilir.
Kendi güvendiğiniz bilgisayarınızın dışında başka bir bilgisayarda banka işlemleri gibi önemli işlerinizi yapmayın. Bizzat en yakınınızdaki banka şubesine gidin.	Bir çok (sanal) problemin önüne geçecek bu yöntem yapılan yürüyüşle de sağlığınıza faydalı olabilir.	Zaman?

6.5. Mevcut Klavye Dinleme Önleme Sistemleri

Yüzlerce klavye dinleme sisteminin bulunduğu piyasada, tamamıyla klavye dinleme sistemlerine odaklanan sadece üç tane ticari klavye dinleme önleme sistemi (antikeylogger) bulunmaktadır. Çoğu casus savar yazılımların kullandığı imza tabanlı korumayı kullanmayı haklı olarak kullanmayan bu sistemler Türkçe arayüze ne yazık ki sahip değildirler.

Bu çalışmada incelenen klavye dinleme önleme sistemleri aşağıda listelenmiştir:

- Advanced Anti Keylogger (101)
- Anti-keylogger (102)
- Keylogger Hunter (103)

Advanced Anti Keylogger, diğer klavye dinleme sistemlerinde en gelişmiş olanıdır. İleri kullanıcıya çeşitli ayarlamalar yapma imkanı veren program tecrübesiz kullanıcılar için de kullanışlı bir yapı sergilemektedir. Programın diğer programlardan farklı bir özelliği de şifre korumalı olmasıdır. Bu sayede, başka kişilerin klavye dinleme sistemine müdahale etmesi önlenerek program ayarlarının korunması sağlanmaktadır. Program kurulduğunda, sistem tepsisinin üstünde bilgilendirme mesajı ile yakalanan modüller kullanıcıya iletilmektedir. Programın, Keylogger Hunter programını, Şekil 6.3'den de görülebileceği gibi bir klavye dinleme izleme programı olarak nitelemesi ilginç bir durum olarak not edilmiştir. Programda, gizli bilgileri girerken ileri derecede güvenlik sağlayan "High Security Mode" adı verilen bir mod bulunmaktadır.

Şekil 6.3. Klavye dinleme önleme sisteminin izleme programı olarak nitelendirilmesi

Anti-keylogger sistemi, klavye dinleme sistemlerini yakaladığında kullanıcıya uyarı vererek bunları ihraç listesine atmaktadır. Kullanıcı gerekli görürse listede bulunan bir modülün engellenmesini bilerek devre dışı bırakabilir. Bu açıdan programda, program seçenek ve ayarların parola ile korumasının bulunmaması sakıncalı bir durum olarak değerlendirilmektedir.

Diğer iki klavye dinleme önleme sisteminden daha ucuz olan Keylogger Hunter klavye dinleme önleme sistemi, özellik açısından bu sistemlerden oldukça zayıftır.

Sadece Windows klavye çengelini engelleyerek klavyeye çengel atan klavye dinleme sistemlerinin kullanıcının girdiği tuş bilgilerini ele geçirmesi önlenmektedir.

Çizelge 6.2'de Advanced Anti Keylogger, Anti-keylogger ve Keylogger Hunter klavye dinleme önleme sistemlerinin özellikleri gösterilmektedir. Çizelgeden de görülebileceği gibi Advanced Anti Keylogger programı diğer iki programa göre daha ileri seviyede güvenlik sağlamaktadır.

Çizelge 6.2. Mevcut klavye dinleme önleme sistemlerinin özellikleri

Ürün:	*Advanced Anti Keylogger*	*Anti-keylogger*	*Keylogger Hunter*
Üretici	Spydex, Inc.	Raytown Corporation LLC.	Alexander G. Styopkin
Sürüm	3.4.2	6.0.1	2
Platformlar	XP/2000/NT	2000/XP	XP/2000/NT
Fiyat	59.95$	59.95$	19.95$
Windows klavye çengeli yöntemi	X	X	X
Çekirdek tabanlı klavye süzgeç sürücüsü	X	X	-
Güvenli bilgi girişi sağlama	X	-	-
Klavye dinleme yapmak isteyen programlara ilişkin kural belirleyebilme	X	X	-
Değiştirilebilir güvenlik seviyesi	X	-	-
Program parola koruması	X	-	-
Dinamik koruma	X	X	Sadece klavye dinleme sisteminin yakalayacağı tuş basımı bilgisini araya girip siliyor.
İmza tabanlı	-	-	-
Pano yakalama önleme	-	X	-
Pencerelere ait metinlerin alınmasını önleme	X	X	-

Bu klavye dinleme önleme sistemlerinin, bu çalışma için gerçekleştirilen klavye dinleme sistemi TürkSpyware ile yapılan testlerin sonuçları yazılımın ayrıntıları ile anlatıldığı Bölüm 7.7.3'de sunulmaktadır.

Sonuç olarak klavye dinleme sistemleri, asla göz ardı edilemeyecek derecede ciddi zararlar verebilecek casus yazılımlardır. Onun içindir ki piyasada 500 kadar klavye

dinleme sistemi ve türevi bulunmaktadır. Ne yazık ki casus yazılımlara karşı az da olsa var olan duyarlılık klavye dinleme sistemlerinde yok denecek kadar azdır. Klavye dinleme sistemlerine karşı genelde imza tabanlı bir yöntem izleyen casus savar yazılımların tek başına kullanılmasının yeterli olmayacağı düşünülmektedir. Sadece bu tür yazılımlara karşı kullanılan, az sayıda klavye dinleme önleme sistemi temel klavye dinleme tekniklerine karşı önlem alabilmektedir. Fakat bunları bile aşabilen teknikler, bu çalışmada gösterildiği gibi geliştirilebilir. Ayrıca günümüz klavye dinleme sistemleri Bölüm 5 ve Bölüm 7'de incelendiği, tanıtıldığı ve tartışıldığı gibi sadece tuş basımı bilgisinin izini sürmemektedir. Bunlara karşı incelenen klavye dinleme önleme sistemlerinin hiç bir tedbiri yoktur. Dolayısıyla bu tür yazılımların daha geniş bir korunma sağlayacak şekilde düzenlenmesi gerekmektedir. Casus savar yazılımların da bu konuya ciddi bir şekilde eğilmesi ve bütünleşik bir şekilde korunma sağlanması gerekmektedir.

6.6. Yazılım Klavye Dinleme Önleme Teknikleri

Bölüm 5'de aktarılan tekniklerden Windows çengeli, klavye dinleme sistemlerinin klavyeden girilen tuş bilgilerini ele geçirmek için en çok kullanılan tekniktir. Bu yöntemi kullanan klavye dinleme sistemleri ve türevlerini önlemek için geliştirilebilecek bir yöntem sistemde çalışmakta olan prosesleri inceleyip bunlardan Windows çengelini kullanan modüllere sahip olanın saptanmasıdır (104). Bu yöntem, bilinçli kullanıcı etkileşimine ihtiyaç duyması, yavaş çalışması ve zararsız yazılımların çengel kullanımını engelleyebilme olasılığı açısından sakıncalı olabilir.

Çengel tekniği kullanan klavye dinleme sistemlerini önlemede kullanılabilecek ikinci bir teknik, klavye dinleme sistemlerinin kullandığı API fonksiyonlarını dinamik olarak izleyecek yapılar geliştirmektir (105). Bu şekilde herhangi bir uygulama ya da modül klavye çengelini kullandığında, bunun yakalanması ve buna karşı alınabilecek tedbirlerin uygulanması mümkün olabilir. API çengeli (API hooking) olarak da adlandırılan bu yöntemin nasıl gerçekleştirilebileceği takip eden kısımda anlatılmaktadır.

6.6.1. API izleme teknikleri

Kullanıcı ve sistem programları tarafından kullanılan API çağrılarının izlenmesi, uygulamalar ve işletim sisteminin iç yapısı hakkında önemli bilgiler sunabilmektedir. Klavye dinleme sistemleri gibi bir çok casus yazılımda bazı API fonksiyonları ana öğe olarak kullanılmaktadır. Eğer bu çağrılar yapıldığı anda tespit edilebilirse bu tür casus yazılımların saptanması da kolay olacaktır. Bölüm 5.4'de, klavye dinleme sistemlerinin kullandıkları teknikler anlatılırken SetWindowsHookEx gibi çeşitli API fonksiyonlarının klavye dinleme yapmak için kullanıldığını burada tekrar etmekte fayda vardır. İşte bu API fonksiyonunu izleyen bir sistem kurulabilirse bu fonksiyon kullanıldığında araya girilebilir. Hatta bu fonksiyonun işletilmesi bile engellenebilir. Burada ince bir noktadan bahsetmekte fayda vardır. SetWindowsHookEx dahil çoğu API fonksiyonu, kötücül yazılım olmayan bir çok yazılım tarafından da kullanılmaktadır. Bunun için önlenmesi veya izlenmesi düşünülen her API fonksiyonunun tamamen engellenmesi doğru olmaz ve ayrıca sistemin düzgün çalışmamasına hatta çökmesine sebep olabilir. Bunun için bu tür çağrılar yakalandığında kullanıcıya bu durum iletilir. Kullanıcı, eğer API'yi kullanan programın güvenilir olduğundan emin ise bu programın daha sonraki API çağrısı girişimlerine, kullanıcıya bir daha sorulmadan izin verilebilir. Tersi durumda, eğer kullanıcı programdan şüphelenir ve yaptığı API çağrısının engellenmesini isterse bu programın bundan sonra kullandığı her izlenen API çağrısı sürekli olarak kullanıcıya bilgi sormadan engellenebilir.

API izleme, teorik olarak ortaya konulan bir kavram olsa da ne yazık ki Microsoft'un SDK (Yazılım Geliştirme Takımı, Software Developer Kit) ve DDK (Sürücü Geliştirme Takımı, Driver Developer Kit) belgelerinde bu konuya ilişkin hiç bir bilgi ve örnek bulunmamaktadır. Bu kısımda Windows uygulamalarının yaptığı API çağrılarına çengel atma ile ilgili keşfedilen tekniklerden bahsedilecektir (106).

Bu teknikler,

- Vekil DLL
- İzlenecek uygulamanın API çağrılarını yamalamak
- İçeri Aktarma Adres Tablosunu (IAT) yamalamak
- API'yi yamalamak

olarak sıralanmaktadır. Bu tekniklerin ayrıntıları aşağıdaki kısımlarda sunulacaktır.

1. Vekil DLL

Diğer tekniklere göre, gerçekleştirilmesi daha kolay gözüken bu teknik, API fonksiyonunun bulunduğu DLL'in ihraç ettiği bütün fonksiyonları aynı imzayla ihraç ederler. Orijinal DLL normalde yüklenmeyecek bir dizinde olmalıdır. Sadece bir uygulama için böyle bir şey yapılıyorsa, vekil DDL'i uygulamanın bulunduğu dizine atmak gerekir. Herhangi bir uygulama, izlenmek istenen API'ye çağrı yaparsa orijinal DLL yerine vekil DLL yüklenir ve bu sırada, istenilen işlemler yapıldıktan sonra çağrı orijinal DLL'e yönlendirilir. İzlenmek istenmeyen API'ler için ise, sadece orijinal DLL'deki karşılığına yönlendirme yeterli olacaktır. Bu yöntem teorik olarak basit bir uygulama olarak gözükse de, yüzlerce fonksiyon ihraç eden bir DLL için vekil DLL hazırlamak oldukça zahmetli olabilir. Orijinal DLL'in yerini değiştirmek de pek doğru bir yaklaşım değildir.

2. İzlenecek uygulamanın API çağrılarını yamalamak

Eğer API izleme tek bir uygulama için yapılacaksa, bu uygulamanın kodunda bulunan API çağrımları, diskte bulunan uygulamanın çalıştırılabilir dosyasının içinde veya hafızaya yüklenen çalıştırılabilir kısmında değişiklik yaparak gerçekleştirilebilir. Burada API çağrımının yapıldığı konumun tam yerinin bulunması gerekmektedir. Bunun için de, yürütülür koddan "assembly" kodunu üretecek "disassembler" araçlarına gerek vardır. Yani tersine mühendislik yapılması gerekmektedir ki buna çoğu uygulama üreticileri tarafından izin verilmemektedir.

3. İçeri Aktarma Adres Tablosunu (IAT) yamalamak

Windows işletim sisteminde API izlemek için kullanılan en yaygın ve en makul olan yöntemdir. 32 bit Windows işletim sisteminde çalıştırılabilir dosyalar ve DLL'ler Taşınabilir Çalıştırılabilir (PE, Portable Executable) dosya formatında inşa edilmektedirler. Belirli bir mimariye bağlı olmadığı için bu şekilde adlandırılan bu formatta dosyalar kısım (section) olarak bilinen çeşitli mantıksal külçelerden (chunk) oluşmaktadır. Her bir kısım belirli bir türde içeriğe sahiptir. Kısımlardan, ".text" kısmı, uygulamanın derlenmiş kodunu içerirken; ".rsrc" kısmı, uygulamada yer alan diyalog kutuları, resimler ve araç çubukları gibi kaynaklar için bir havuz gibi görev yapar.

Bu kısımlardan biri de ".idata" kısmıdır. Bu kısımda İçeri Aktarma Adres Tablosu (IAT, Import Address Table) olarak adlandırılan özel bir tablo bulunmaktadır. Bu tablo çalıştırılabilir kod tarafından başvurulan, içeri aktarılmış fonksiyonların adlarına, dosyaya bağımlı olan göreli konum (offset) değerlerini tutmaktadır. Windows işletim sistemi herhangi bir çalıştırılabilir dosyayı hafızaya yüklediği zaman, bu göreli konum değerlerini, içeri aktarılan fonksiyonların doğru adresleri ile yamalamaktadır. Bütün prosesler ve DLL'lerin ilklendirilmesi yapılırken, sistem hummalı bir şekilde bu adresleri doğru değerleri ile günceller. İşte bu yüzden programlar çalışmaya başladıklarında işletim sistemine büyük bir yük bindirirler.

İşte böyle bir tabloda izlenmek istenen API fonksiyonuna çağrının adresi, hazırlanan izleme fonksiyonu ile değiştirilirse uygulamanın her API çağrısında, bu izleme fonksiyonu çağrılacaktır. İstenirse izleme fonksiyonu, istenilen işlevi yerine getirdikten sonra asıl API fonksiyonuna yönlendirme yapabilir.

Bu teknik gerçekten etkili bir çözüm üretse de değiştirilen bu tabloların onarılıp tekrar yerine konulmasının da mümkün olduğu unutulmamalıdır (107).

4. API'yi yamalamak

API izleme için kullanılabilecek bir başka yöntem de, kaynağın, yani API fonksiyonunun kendisinin yamalanmasıdır. Bir çok yan etkisi bulunsa da böyle bir şeyi en azından araştırma amaçlı olarak, izlenmek istenen API'nin ilk baytını duraklama noktası (breakpoint) komutu (Int 3) ile yer değiştirmektir. Böylece bu API fonksiyonunu kullanan her çağrı, bir kural dışı durum (exception) üretecektir. Hazırlanan API izleme programı bu kural dışı durumu işleyip gerekli bilgileri alacak şekilde düzenlenebilir. Bu teknik de API makine kodunun değiştirilmesini gerektirir ki bu işlemin çok dikkatli bir şekilde gerçekleştirilmesi gerekmektedir.

6.6.2. Çekirdek tabanlı klavye süzgeç sürücülerini önleme

Belirlenmesi en zor klavye dinleme sistemleri çekirdek tabanlı klavye süzgeç sürücüleri kullanan sistemlerdir. Bu sistemlerin en kritik noktası sürücünün kurulması için yönetici hakkının gerekli olmasıdır. Bu yüzden, normal bilgisayar kullanımı sırasında yönetici hakkı olmayan bir hesaptan çalışmanın ve yönetici şifresinin güvenli bir şekilde saklanıp, belli aralıklarla değiştirmenin ne kadar önemli olduğu ortaya çıkmaktadır.

Çekirdek tabanlı sürücü işlemleri yapmak için geliştirilen kök kullanıcı takımları (rootkit), modül yüklemek için resmi olarak kullanılan SCM (Hizmet Kontrol Yöneticisi, Service Control Manager, İngilizce "scum" olarak telaffuz edilir) API'leri (108), ZwLoadDriver ve ZwSetSystemInformation API'lerini kullanmaktadırlar. Bunun dışında başka teknikler de geliştirilebilir. Bu ve bunun gibi tekniklere karşı çekirdeğin korunmasına yönelik kullanılabilecek seçenekler,

- Sürücü imzalama
- Bütünlük koruma sürücüsü ve çengelleri
- ServerLock programı

şeklinde özetlenebilir (109). Bu önlemlerin ayrıntıları takip eden kısımda alt başlıklar halinde sunulmaktadır.

1. Sürücü imzalama

Kök kullanıcı takımlarını gerçek anlamda önlemese de, en azından sürücüler incelenirken şüpheli sürücülerin ileri kullanıcılar için saptanmasını sağlayabilir. Hazırlanan sürücülerin kalitesini kontrol altına almak amacıyla Microsoft, sürücü inceleme ve imzalama programı geliştirmiştir (110). Hazırlanan sürücüler Windows Donanım Kalite Laboratuarlarına (WHQL, Windows Hardware Quality Lab) gönderilmektedir. Yapılan testlerden başarı ile geçenlerin sürücüleri imzalanır. Bu sürücüleri tarayan bir program imzası bulunmayan sürücüleri uyarabilir.

2. Bütünlük koruma sürücüsü ve çengelleri

Pedestal Software firması tarafından geliştirilen ve açık kaynak kodlu bütünlük koruma sürücüsünün (IPD, Integrity Protection Driver) kendisi bir çekirdek sürücüsüdür. Bu sürücü herhangi bir yeni modülün yüklenmesini önlemek amacıyla bazı sistem servislerine çengel atar. System32\Drivers dizininde bulunan standart sürücülerin yüklenmesine izin verir. Yeni modüllerin yüklenmesini engellemek için,

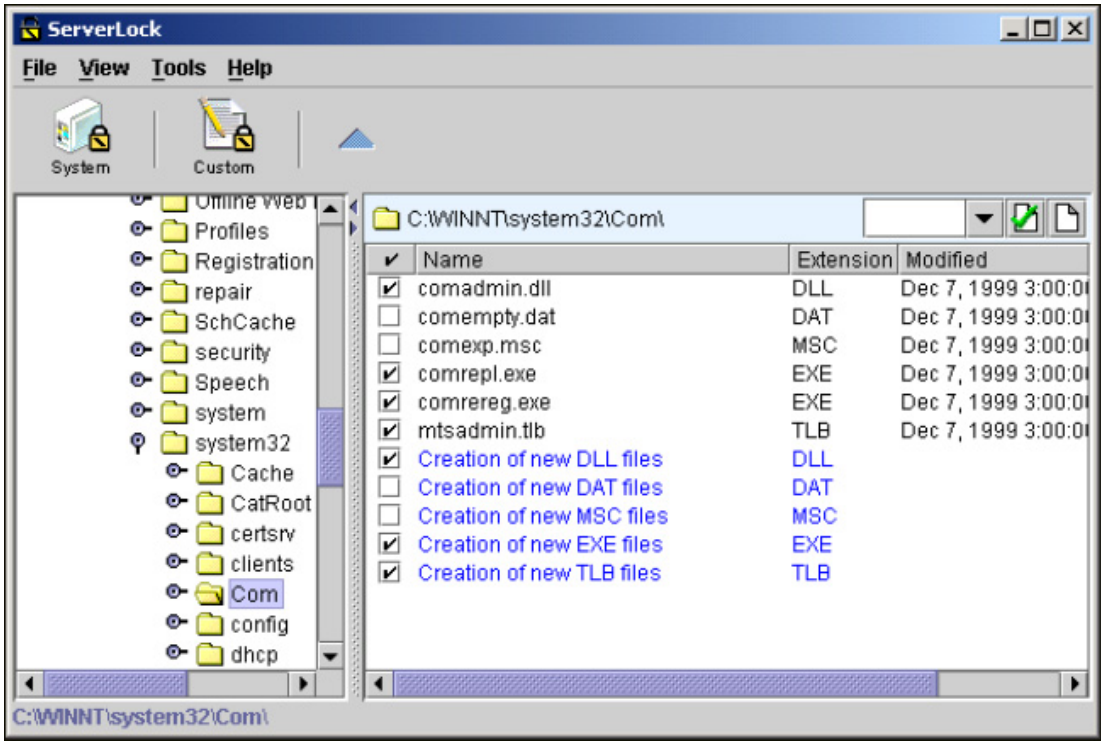
- \HKLM\System\CurrentControlSet\Services kütük anahtarını korumak için ZwOpenKey, ZwCreateKey ve ZwSetValueKey fonksiyonlarına;
- \device\PhysicalMemory anahtarını engellemek için ZwOpenSection fonksiyonuna;
- \Device\Harddisk*, v.b. anahtarları engellemek için ZwCreateFile ve ZwOpenFile fonksiyonuna,
- ZwOpenSection, ZwCreateFile ve ZwOpenFile fonksiyonlarının kandırılmasının önlenmesi için ZwCreateLinkObject fonksiyonuna;
- SystemLoadAndCallImage ve SystemLoadImage fonksiyonları için ZwSetSystemInformation fonksiyonuna;

- Çalışma zamanında proses enjeksiyonunu önlemek için ZwOpenProcess fonksiyonuna;

çengel atılır. Bu sürücü de son bir kaç yıldır saptanan hatalar işletim sisteminin doğrudan gerçekleştirmediği koruma programlarının istenilen başarımı tam olarak sağlamadığını göstermektedir.

3. ServerLock programı

WatchGuard (111) firması tarafından Windows NT ve Windows 2000 Servers işletim sistemleri için geliştirilen ServerLock programı, IPD gibi yeni modüllerin yüklenmesine izin vermemektedir. Şekil 6.4'de örneği gösterilen kullanıcı arabirimi ile yapılandırmanın kolay bir şekilde gerçekleştirilmesi mümkündür. Ayrıca bazı dosyaların virüs ve benzeri kötücül yazılımlarla değiştirilmesine karşı koruma da sağlayabilmektedir.



Şekil 6.4. ServerLock programı grafik kullanıcı arabirimi

Görüldüğü gibi çekirdek tabanlı klavye dinleme sistemlerinin engellenmesi oldukça güçtür. Fakat şunun da belirtilmesi gerekir ki bu tür klavye dinleme sistemlerinin gerçekleştirilmesi de oldukça zordur. Bu çalışmada, piyasada sunulan çekirdek tabanlı klavye dinleme sistemlerinin testinde, klavye dinleme sistemi bilgisayara kurulduktan sonra bunlardan bir kaçının sistemi çökerttiği; bir kaçının da Windows'un ancak güvenli kipte açılabilmesine neden olduğu gözlenmiştir.

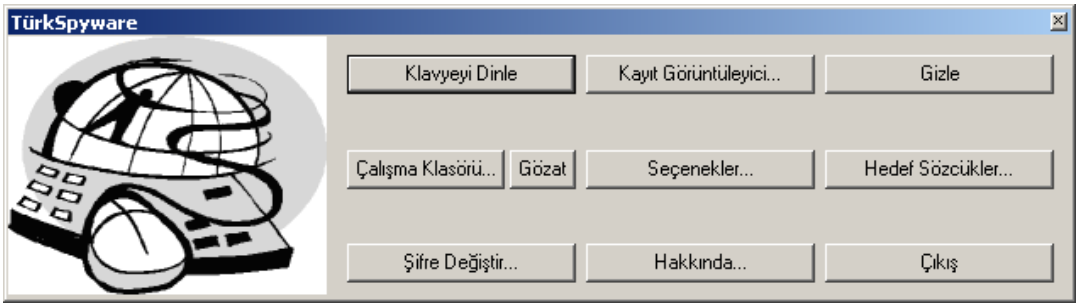
Bundan sonraki iki bölümde, bu kısma kadar elde edilen klavye dinleme ve önleme sistemlerine yönelik kuramsal bilgilerin, uygulamaya yönelik kullanımına ilişkin gerçekleştirilen çalışmalar anlatılacaktır. Bölüm 7'de, TürkSpyware klavye dinleme sistemi yazılımından; Bölüm 8'de, bu bölümde aktarılan bilgilerden hareket ederek çeşitli tekniklerle casus yazılım ve yazılım klavye dinleme sistemlerini önleyebilecek bir çalışma olarak tasarlanıp, gerçekleştirilen TürkAntiSpyware yazılımından bahsedilecektir.

7. GELİŞTİRİLEN KLAVYE DİNLEME SİSTEMİ: TürkSpyware

Daha önceki bölümlerde klavye dinleme sistemleri ayrıntılı bir şekilde incelenmiş; mevcut klavye dinleme sistemlerinin çalışma mekanizmaları, üstünlükleri, oluşturduğu tehditler özetlenmiştir. Daha önceki bölümlerden çıkan sonuçlara göre bu tez çalışmasında TürkSpyware olarak isimlendirilen bir klavye dinleme sistemi yazılımı geliştirilmiştir. Geliştirilen bu yazılımın özellikleri, tasarım ve gerçekleştirme aşamaları ile ilgili genel bilgiler, kullanım durumları, yazılım modülleri, kullanıcı arabirimi ve kullanıma yönelik açıklayıcı bilgilerle yazılımın gerçek hayatta kullanım alanlarına örnekler takip eden bölümlerde açıklanmaktadır.

TürkSpyware ülkemizde gerçek manada hazırlanmış, ilk klavye dinleme sistemidir. Her ne kadar akademik amaçlarla hazırlanmış olsa da; piyasada bulunan ve 5. bölümde aktarılan bir çok başarılı klavye dinleme sistemi ile aynı işlevi yerine getirmekte; dahası onlarda bulunmayan bir kısım ek ve kullanışlı özellikleri de bünyesinde barındırmaktadır. Bilimsel olarak bir çok güvenlik çalışmasında ve sistemlerin güvenlik seviyesinin belirlenmesinde kullanılabileceği düşünülen bu yazılımın, kullanıcı arabiriminin tamamıyla Türkçe olması ile de tamamıyla ülkemize yönelik bir ürün olarak tasarlanmıştır. TürkSpyware ifadesi böyle bir klavye dinleme sisteminin ülkemizde de geliştirilebileceğine işaret etmek amacıyla geliştirilen klavye dinleme sisteminin ismi olarak seçilmiştir.

TürkSpyware ürünü yazılım yolu ile çalışan bir klavye dinleme sistemidir. Çeşitli yöntemlerle klavye dinleme, fare hareket ve tıklamalarının izlenmesi, görsel gözetleme, kayıt dosyası işlemleri ve transferi, gizlenme özellikleri ile bir klavye sisteminden beklenen temel özellikleri yerine getirmenin yanında bir çok ileri izleme ve gözetleme işlemini de yerine getirmektedir. Şekil 7.1'de ana ekran görüntüsü verilen programın genel özellikleri Çizelge 7.1'de verilmiştir.



Şekil 7.1. TürkSpyware, sürüm: 2.1 ana ekran görüntüsü

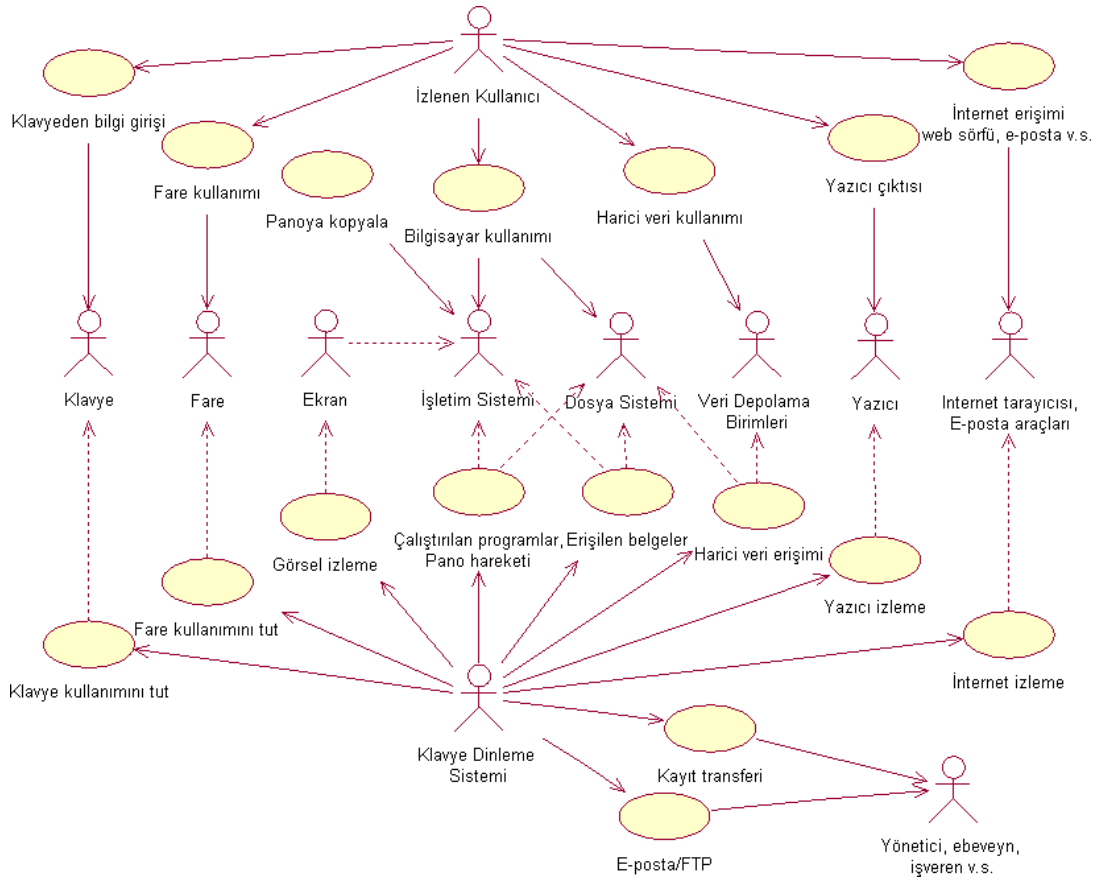
Çizelge 7.1. TürkSpyware genel özellikleri

Program Adı	TürkSpyware
Sürüm	2.1.
Sürüm Tarihi	15.06.2005
Çalıştığı Platformlar	Microsoft NT/2000/XP
Geliştirme Dili	Microsoft Visual C++, Platform Software Developer Kit
Kaynak Kod Satır Sayısı	~20000 satır
Çalıştırılabilir Modül Boyutu	912 KB
Modül Sayısı	30

Bu tez çalışmasında, geliştirilen TürkSpyware yazılımının tasarımı ile ilgili kullanım durumları, yazılımı oluşturan modüller, grafik kullanıcı arabirimleri, kullanım açıklamaları, kayıt dosyasının yapısı ve TürkSpyware'in web tabanlı e-posta sağlayıcılar ve çevrimiçi bankaların İnternet şubeleri gibi şifreli bilgi isteyen alanlar başta olmak üzere çeşitli kullanım örnekleri takip eden kısımlarda farklı başlıklarda açıklanmıştır.

7.1. Kullanım Durumları

Programın tasarımı ile ilgili kullanım durumu (use case) diyagramı Şekil 7.2'de verilmiştir. Yönetici, ebeveyn, işveren v.s. gibi bir kullanıcı, klavye dinleme sistemi, izlenen kullanıcı ana aktörlerinden oluşan sistemde klavye, fare, ekran, işletim sistemi, dosya sistemi, veri depolama birimleri, yazıcı, İnternet tarayıcısı ve e-posta araçları yardımcı aktörler arasında bulunmaktadır.



Şekil 7.2. TürkSpyware 2.1 kullanım durumu (use case) diyagramı

Sistem tarafından gerçekleştirilen kullanım durumları aşağıda listelendiği gibidir:

- İzlenen kullanıcının klavye bilgi girişleri, klavye dinleme sistemi tarafından takip edilir. Klavyeden girilen bilgiler elde edilir ve klavye kullanım bilgileri tutulur.
- İzlenen kullanıcının fare işlemleri klavye dinleme sistemi tarafından tutulur.
- Klavye dinleme sistemi ekrandan görüntü alarak görsel izleme yapar.
- İzlenen kullanıcının bilgisayar kullanımı ve panoya kopyalama işlemleri işletim sistemi aracılığıyla, klavye dinleme sistemi tarafından çalıştırılan programlar ve pano hareket bilgileri tutulur.
- İzlenen kullanıcının bilgisayar kullanımı sırasında dosya sistemi üzerinde yaptığı işlemler, erişilen belgeler olarak klavye dinleme sistemi tarafından tutulur.

- İzlenen kullanıcının veri depolama birimleri kullanarak yaptığı harici veri kullanımı klavye dinleme sistemi tarafından harici veri erişimleri olarak tutulur.
- İzlenen kullanıcının yazıcıdan aldığı çıktılar klavye dinleme sistemi tarafından izlenir.
- İzlenen kullanıcının İnternet tarayıcısı ve e-posta araçları kullanarak İnternet üzerinde yaptığı işlemler klavye dinleme sistemi tarafından izlenir.
- Bütün bu işlemlerden sonra, klavye dinleme sistemine sahip bir kullanıcı, klavye dinleme sisteminden kayıt bilgilerini, kayıt transferi, e-posta veya FTP aracılığıyla elde edebilir.

7.2. Yazılım Modülleri

TürkSpyware klavye dinleme sistemi yazılımına ait tasarlanan ve gerçekleştirilen modüller aşağıda sıralanmış; takip eden alt başlıklarda ayrıntıları aktarılmıştır.

- Klavye dinleme modülü
- Fare izleme modülü
- Pencere izleme modülü
- Görsel gözetleme modülü
- Bitmap dosya modülü
- JPG kütüphanesi
- İnternet izleme modülü
- Harici veri izleme modülü
- Program izleme modülü
- Dizin değişiklik izleme modülü
- Yazıcı belirleme modülü
- Yazıcı kuyruğu izleme modülü
- Pano izleme modülü
- Program gizleme modülü
- Şifre özetleme modülü

- Şifreleme ve şifre çözme modülü
- Sistem kütüğü modülü
- Elektronik posta modülü
- Dosya transferi modülü
- Ana kullanıcı grafik arabirimi modülü
- Program yapılandırma arabirimi modülü
- Kayıt dosyası yazma modülü
- Kayıt transferi zamanlama modülü
- Kayıt görüntüleme modülü
- Kullanıcı şifre değiştirme modülü
- Ağ bilgileri modülü
- Windows oturum modülü
- Hedef sözcük modülü
- Çalışma klasörü modülü
- Uyarı ekranı modülü
- Veri sıkıştırma modülü

7.2.1. Klavye dinleme modülü

Klavye dinleme sisteminin ana işlevinin gerçekleştirildiği bu modülde çeşitli yöntemlerle tuş basımı bilgileri Türkçe karakter koduna göre ve sistem tuşlarının özel olarak belirtilmesi ile yakalanıp kaydedilebilmektedir.

7.2.2. Fare izleme modülü

Fare izleme modülü kullanıcının fare ile yaptığı işlemleri izleyen bir modüldür. Fare tıklamalarını, tıklanılan fare tuşunu ve tıklanılan noktanın ekran koordinatlarını alabilen bu modül bu bilgiyi çeşitli amaçlarla kullanmaktadır.

7.2.3. Pencere izleme modülü

Pencere izleme modülü, kullanıcı bilgisayarı kullanırken açtığı, etkinleştirdiği ve kapattığı pencerelere ait bilgileri yakalayan bir modüldür. Bu modül kullanıcının her hangi bir zamanda etkin olarak kullandığı pencereye ait çeşitli bilgileri elde edebilmek için tasarlanmıştır.

7.2.4. Görsel gözetleme modülü

Görsel gözetleme modülü, fare tıklamalarının ve belirli aralıklarla, o anki ekranın görsel kaydının alınması amacıyla hazırlanmış bir modüldür. Kullanıcının isteğine göre, ekranın tamamının ekran görüntüsünün alınabilmesinin yanında sadece o an etkin olan pencerenin ekran görüntüsü de tasarlanan bu modül ile kolaylıkla alınabilmektedir.

7.2.5. Bitmap dosya modülü

Görsel gözetleme modülünün kullandığı Bitmap dosya modülü alınan ekran görüntülerinin BMP formatında dosya olarak saklanabilmesini sağlamaktadır.

7.2.6. JPG kütüphanesi

Görsel gözetleme modülünün kullandığı bir diğer modül olan JPG kütüphanesi alınan ekran görüntülerinin JPG formatında dosya olarak saklanabilmesini sağlamaktadır. Bu kütüphane kullanılarak elde edilen görüntüler kullanıcının belirlediği oranda sıkıştırılarak daha küçük dosya boyutlarında görsel gözetleme yapılarak klavye dinleme sisteminin kullandığı sistem kaynaklarının, düşük seviyede tutulması sağlanmaktadır.

7.2.7. İnternet izleme modülü

İnternet izleme modülü İnternet Gezgini ve Maxthon İnternet tarayıcıları ile kullanıcının İnternet üzerinde gezdiği sitelerin adreslerini yakalayan bir modüldür.

Kullanıcının bulunduğu sitenin URL adresini elde eden bu modül, bunu kayıt sistemine aktararak bu bilginin tutulabilmesini sağlamaktadır.

7.2.8. Harici veri izleme modülü

CD, DVD, USB bellek kartları gibi harici veri ortamlarının sistemle olan irtibatlarında, bu ortamlara ait temel bilgileri elde eden bir modüldür. Ortamın türü, seri numarası, sisteme ulaştığı veya sistemden çıkartıldığı tarih gibi bilgiler, bu modül de tasarlanan yapı ile elde edilebilmektedir.

7.2.9. Program izleme modülü

Program izleme modülü bir disk yönetim sisteminde çalıştırılan *.exe, *.bat, *.com ve *.cpl uzantılı çalıştırılabilir dosyaları izlemektedir. Bu tür programlar sistem veya kullanıcı tarafından çalıştırılınca, bu tür programlara ilişkin bilgiler bu modül desteğiyle kolaylıkla elde edilmektedir.

7.2.10. Dizin değişiklik izleme modülü

Dizin değişiklik izleme modülü kullanıcının belirlediği uzantılarda dosyalarda yapılan değişiklikleri (yeni dosya ekleme, dosya değiştirme, isim değiştirme ve silme) izlemektedir. TürkSpyware'in diğer klavye dinleme sistemlerine göre farklı yönü sadece bir adet disk sürücüsünü değil sistemde varsa iki adet disk sürücüsünde (C:\ ve D:\) yapılan değişiklikleri takip edebilmesidir.

7.2.11. Yazıcı belirleme modülü

Yazıcı belirleme modülü, kullanıcının sisteminde tanımlı olan yazıcı sürücülerini ve varsayılan yazıcıyı belirleyen modüldür.

7.2.12. Yazıcı kuyruğu izleme modülü

TürkSpyware'in ileri özelliklerinden biri de kullanıcının varsayılan yazıcıdan almış olduğu çıktılara ait bilgileri elde edebilmesidir. Yazıcı kuyruğu izleme modülü ile böyle bir iş yazıcının kuyruğuna ulaştığında bu bilgi modül tarafından değerlendirilir ve çıktı alınma zamanı, çıktısı alınan dosyanın adı ve sayfa sayısı gibi bilgiler kayıt sistemine iletilir.

7.2.13. Pano izleme modülü

Pano izleme modülü, kopyalama yapıştırma işlemi sırasında işletim sistemi ve uygulamalar arasında veri aktarımını sağlayan panoda (clipboard) yapılan hareketleri takip eder. Kullanıcı herhangi bir metni panoya kopyalayarak aktardığında klavye dinleme sistemi bu yapıya zarar vermeden panoya aktarılan verinin bir kopyasını kayıt sistemine ulaştırır.

7.2.14. Program gizleme modülü

Program gizleme modülü, klavye dinleme sisteminin çalışırken kullanıcıdan saklanmasını sağlayan modüldür. Görev yöneticisinin uygulama ve proses listesinden saklama ve görev çubuğundan saklanma bu modül desteğiyle sağlanmaktadır.

7.2.15. Şifre özetleme modülü

Klavye dinleme sistemine sahip bir kullanıcının belirlediği ve daha sonra gerek program kayıtlarına ulaşmak gerekse sistem yapılanmasını değiştirmek istediğinde programı kullanabilmesi için sorulan şifrenin özetleme algoritması ile güvenli olarak saklanmasını sağlayan bu modül, ayrıca girilen şifrenin doğruluğunun kontrolünü ve şifre değiştirme işlemlerini de yerine getirmektedir. Bu özellik, bir çok klavye dinleme yazılımında bulunmayan bir özelliktir.

7.2.16. Şifreleme ve şifre çözme modülü

Klavye dinleme sisteminin tuttuğu bütün kayıtları şifreleyen ve şifrelenen kayıtların şifresini çözerek kullanıcı tarafından okunabilmesini sağlayan modüldür. İleri seviye şifreleme algoritması olan Blowfish algoritması bu modülde kullanılmaktadır.

7.2.17. Sistem kütüğü modülü

Sistem kütüğü modülü, sistemin işletim sistemi kütüğü (registry) ile ilgili işlemleri yerine getiren modüldür.

7.2.18. Elektronik posta modülü

Elektronik posta modülü klavye dinleme sisteminin tuttuğu kayıtların e-posta ile gönderilebilmesini sağlamak amacıyla kullanılacak e-posta sistemine ait SMTP sunu adresi ve kullanılan hesap ve e-postanın ulaşması istenilen hesaba ait bilgilerin atanması, test edilmesi ve eklenti imkanı ile kayıt bilgilerinin ayarlanan şekilde ulaştırılabilmesini sağlamaktadır.

7.2.19. Dosya transferi modülü

Dosya transferi modülü FTP protokolü kullanarak kayıt bilgilerinin bir FTP sunucusuna aktarılabilmesini sağlamaktadır.

7.2.20. Ana kullanıcı grafik arabirimi modülü

Programın kullanıcı ile etkileşim kurduğu ana kullanıcı grafik arabirimine ilişkin işleri düzenleyen modüldür.

7.2.21. Program yapılandırma arabirimi modülü

Kullanıcının TürkSpyware programının çalışma şeklini belirleyen bir arabirim modülü mevcuttur. Bu arabirim yapılacak iş ve işlemleri aynı zamanda düzenleyen bir modüldür.

7.2.22. Kayıt dosyası yazma modülü

Elde edilen her tür bilginin farklı şekilde kayıtlarının tutulmasını sağlayan modül, İleri düzeyde koruma için şifreli kayıt tutma seçenekleri sunmaktadır.

7.2.23. Kayıt transferi zamanlama modülü

Kayıt transferi zamanlama modülü, tutulan kayıt bilgilerinin ne zaman ve ne şekilde aktarılacağını belirlemek için kullanılır. Burada e-posta ve FTP ile aktarım seçenekleri bu modülde sunulmaktadır.

7.2.24. Kayıt görüntüleme modülü

Şifrelenmiş olan kayıt bilgileri ancak bu modül kullanılarak deşifre edilebilir. Bu modül şifreli kayıtların şifresini çözerek bu bilgileri kullanıcıya sunar; istenirse bu modül kullanılarak ana kayıt dosyası dışında diğer dosyalar da görüntülenebilir. Bu modül ayrıca metin tabanlı kayıt bilgilerinden HTML tabanlı bir rapor üretilebilmesine imkan sunmaktadır.

7.2.25. Kullanıcı şifre değiştirme modülü

Kullanıcının programı kullanırken girdiği şifreyi yenilemek istediğinde bu modül devreye girer. Şifrenin eski şifre ile aynı olmaması ve kullanıcının yeni şifreye iki kez girmesini bu modül yürütmektedir.

7.2.26. Ağ bilgileri modülü

IP adresi, kullanıcı adı, bölge adı ve MAC adresi gibi kullanılan ağa ait bilgiler bu modül yardımıyla sistemden elde edilmektedir.

7.2.27. Windows oturum modülü

Oturum başlatma ve sistem kapatma, kullanıcı değiştirme ve yeniden başlatma ile kapatılan oturumlar bu modül ile izlenir.

7.2.28. Hedef sözcük modülü

Kullanıcının daha dar kapsamda belirli bir hedefe yönelik izlenmesini sağlamak için bu modül tasarlanmıştır. Bu çerçevede, kullanıcıların izlenmesi istenen hedef anahtar sözcüklerin girilmesi ve bunların klavyeden girilip girilmediğini izlenmesi bu modül ile gerçekleştirilir.

7.2.29. Çalışma klasörü modülü

Kayıt dosyası ve bazı modüllerin bulunduğu klasörü düzenlemek için tasarlanmış bir modüldür.

7.2.30. Uyarı ekranı modülü

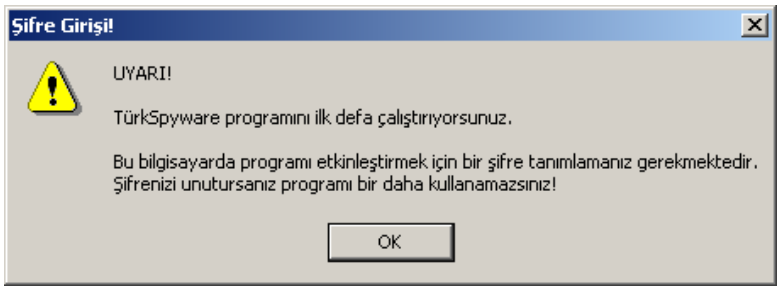
Kullanıcılara, izlendiklerine ilişkin bir mesajın belirlenmesini ve bu mesajın her açılışta gösterilmesini sağlayan modüldür. Seçenekler bölümünde girilen metin, sistemin her açılışında otomatik olarak gösterilmektedir. Uyarı ekranı istenilmediğinde ekranı görünmez hale gelir.

7.2.31. Veri sıkıştırma modülü

Kayıt bilgilerinin çok fazla yer kaplamaması için ZIP formatında sıkıştırılmasını sağlayan modüldür.

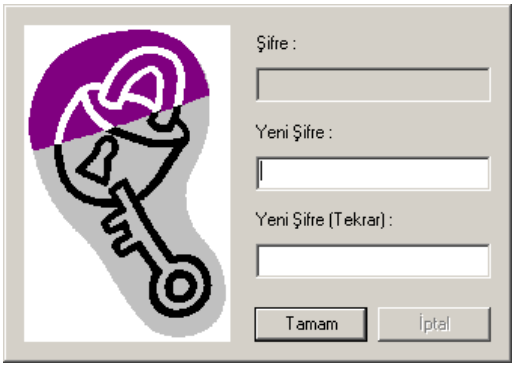
7.3. TürkSpyware Kullanıcı Arabirimi ve Kullanım Açıklamaları

TürkSpyware Windows NT/2000/XP işletim sistemlerinde çalışacak şekilde tasarlanmış ve gerçekleştirilmiştir. Bir Windows uygulamasının taşıdığı bir çok özelliği bünyesinde toplamaktadır. Kullanıcı dostu arabirim tasarımı ile ve kullanıcıya sunulan Türkçe iletilerle rahat bir kullanım ortamı sağlanmaya çalışılmıştır. Program modülleri hedef bilgisayara kopyalandıktan sonra, ana modül çalıştırılır. Bu ilk çalıştırmada, Şekil 7.3'de görüldüğü gibi önemli bir mesaj kullanıcıya iletilir:



Şekil 7.3. TürkSpyware ilk çalıştırma uyarı mesajı

Bu mesajda belirtildiği gibi programı daha sonraları etkinleştirerek, çeşitli işler yapmanız gerektiğinde, kullanmak üzere gerekecek bir şifrenin belirlenmesi gerekmektedir. Bu şifre daha sonra unutulursa, programın kullanılması mümkün olmayacaktır. Bundan sonra kullanıcıya Şekil 7.4'de verildiği gibi yeni şifrenin tanımlanacağı diyalog gösterilir.



Şekil 7.4. İlk şifrenin belirlenmesi

Tanımlanan şifrenin en az beş karakter olması gerekmektedir. Bu şifre de tanımlandıktan sonra Şekil 7.1'de gösterilen TürkSpyware ana penceresi ekranda görünmektedir. Bu pencerede sunulan seçenekler ve geliştirilen yazılım ile ilgili ayrıntılar takip eden kısımlarda açıklanmaktadır.

7.3.1. Ana pencere

Ana pencerede kullanıcının yapacağı en genel işlevler yerine getirilmektedir. Bu pencerede yer alan düğmelerin ne gibi bir işlev üstlendiğine dair bilgiler aşağıda Çizelge 7.2'de verilmiştir.

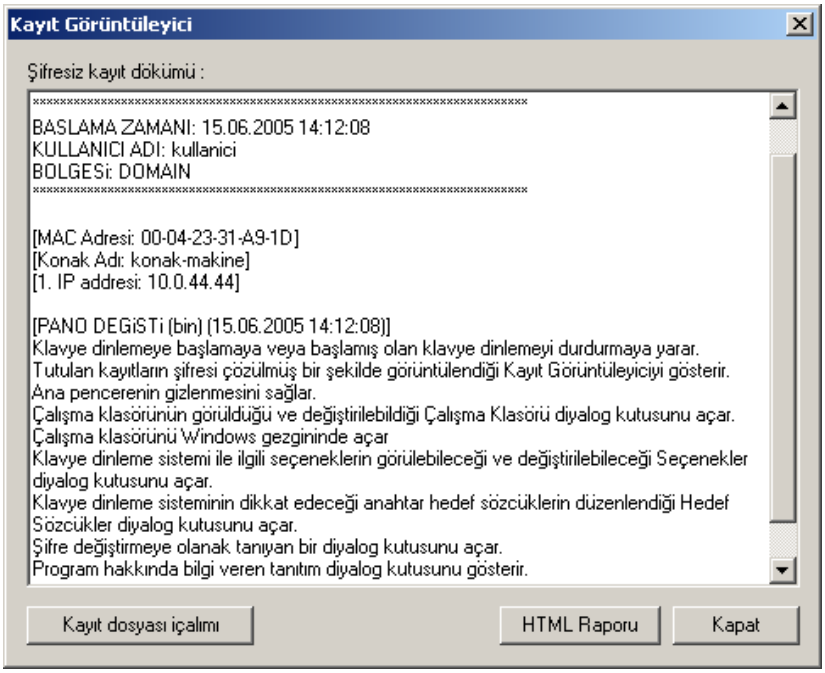
Çizelge 7.2. Ana pencerede yer alan düğmeler ve açıklamaları

Düğme	*Açıklama*
Klavyeyi Dinle / Klavyeyi Dinleme!	Klavye dinlemeye başlama veya başlamış olan klavye dinlemeyi durdurmaya yarar.
Kayıt Görüntüleyici...	Tutulan kayıtların şifresi çözülmüş bir şekilde görüntülendiği Kayıt Görüntüleyiciyi gösterir.
Gizle	Ana pencerenin gizlenmesini sağlar.
Çalışma Klasörü...	Çalışma klasörünün görüldüğü ve değiştirilebildiği Çalışma Klasörü diyalog kutusunu açar.
Gözat	Çalışma klasörünü Windows gezgininde açar.
Seçenekler...	Klavye dinleme sistemi ile ilgili seçeneklerin görülebileceği ve değiştirilebileceği Seçenekler diyalog kutusunu açar.
Hedef Sözcükler...	Klavye dinleme sisteminin dikkat edeceği anahtar hedef sözcüklerin düzenlendiği Hedef Sözcükler diyalog kutusunu açar.
Şifre Değiştir...	Şifre değiştirmeye olanak tanıyan bir diyalog kutusunu açar.
Hakkında...	Program hakkında bilgi veren tanıtım diyalog kutusunu gösterir.
Çıkış	Programın sonlandırılmasını sağlar.

Bu düğmelerin bazılarının ne şekilde çalıştığı takip eden kısımlarda açıklanmaktadır.

7.3.2. Kayıt görüntüleyici

Kayıt görüntüleyici tutulan kayıtları görüntüleyebileceğiniz tek ortamdır. Çünkü TürkSpyware'in tuttuğu tüm kayıtlar güçlü bir şifreleme algoritması ile şifrelenmektedir. Ana pencereden Kayıt Görüntüleyici düğmesine tıklandığında açılan görüntüleyici Şekil 7.5'de gösterildiği gibi ilk olarak o ana kadar tutulmuş kayıtları şifresiz olarak göstermektedir.

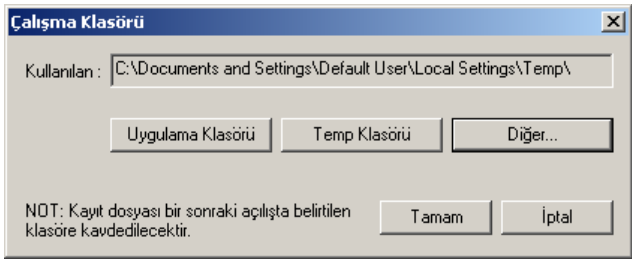


Şekil 7.5. Kayıt görüntüleyici

Bunun dışında başka kayıt dosyaları “Kayıt dosyası içeri aktarımı” düğmesi ile seçilerek görüntüleyicide şifresi çözülerek görüntülenebilir. Kayıtların HTML formatında raporunu almak için HTML Raporu düğmesine basmak yeterlidir.

7.3.3. Çalışma klasörü

Çalışma klasörü diyalog kutusu Şekil 7.6’da verilmiştir. Burada kullanılan çalışma klasörü görülebilmekte ve istenirse bu klasör uygulamanın bulunduğu klasör, geçici dosyaların tutulduğu işletim sistemi “Temp” özel klasörü veya herhangi bir klasör seçilerek, kayıt bilgilerinin ve diğer kayıt dosyalarının belirtilen klasörde saklanması sağlanabilmektedir.

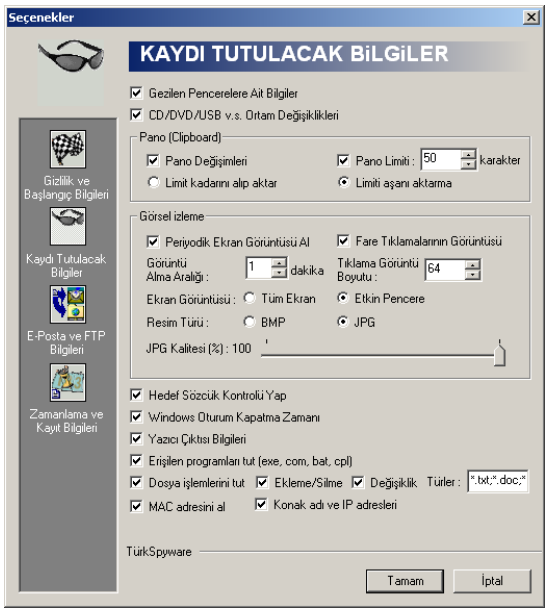


Şekil 7.6. Çalışma klasörü

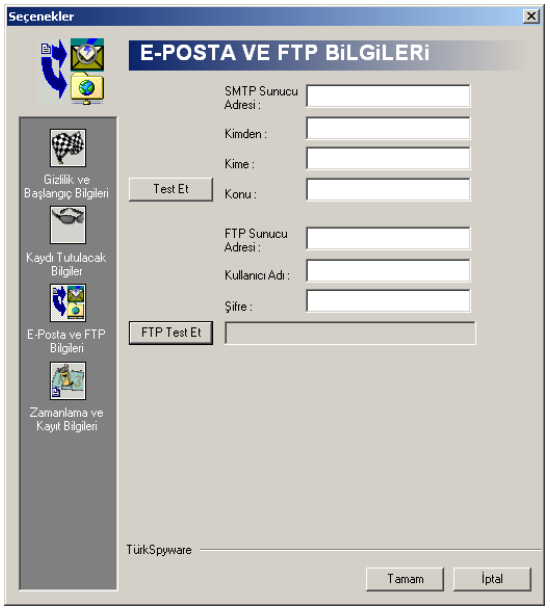
7.3.4. Seçenekler

Klavye dinleme sisteminin çalışmasını belirleyen Seçenekler diyalog kutusu Şekil 7.7'de gösterildiği gibi dört sayfadan oluşmaktadır.

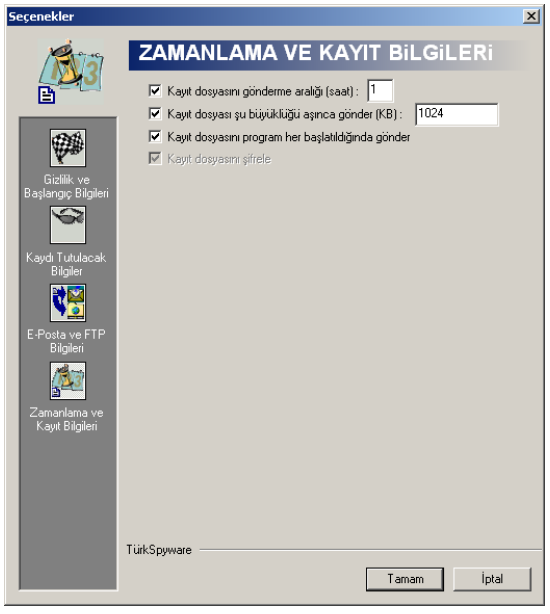
(a) Gizlilik



(b) Kaydı Tutulacak Bilgiler



(c) E-posta ve FTP Bilgileri



(d) Zamanlama ve Kayıt Bilgileri

Şekil 7.7. Seçenekler

Şekil 7.7'de görülen bu seçenek grupları aşağıdaki kısımlarda sırasıyla açıklanmaktadır.

Seçenekler: Gizlilik ve Başlangıç Bilgileri

Şekil 7.7 (a)'da gösterilen bu sayfada TürkSpyware'in gizli kalması ve başlangıç ile ilişkili seçenekler değiştirilmektedir. Seçeneklerin ayrıntıları aşağıda sunulmaktadır.

- İlk çalıştığında gizli başla: Program çalıştığında gizli modda açılır. Bu esnada ana pencere görüntülenmez.
- Windows ile otomatik başlat: Program her oturum açılışında otomatik olarak başlatılır.
- Windows Görev Yöneticisi (Task Manager) Proses Listesinden Gizle: Program Windows işletim sisteminin proses ve uygulama listelerinde yer almaz.
- Program Açığa Çıkartma Kısayol Tuşları : CTRL + SHIF + ALT + ?: Gizli çalışan programı ortaya çıkarmak için kullanıcı tarafından belirlenen tuş kombinasyonudur.
- Gizli Başladığında Uyarı Mesajı Göster: Bu seçenekle program gizli olarak başlatıldığında kullanıcıya Şekil 7.8'de gösterildiği gibi bir uyarı mesajı belli bir süre gösterilir. TürkSpyware için gösterilecek bu mesajın içeriği ihtiyaca göre kolaylıkla değiştirilebilmektedir.

Şekil 7.8. Klavye dinlemesi yapıldığına dair bir uyarı mesajı

Seçenekler: Kaydı Tutulacak Bilgiler

Şekil 7.7 (b)'de ekran görüntüsü verilen bu sayfada TürkSpyware'in ne tür bilgilerin izlenip kaydının tutulacağı ile ilişkili seçenekler verilmektedir.

- Gezilen Pencerelere Ait Bilgiler: Kullanıcı hangi pencerede işlem yapıyorsa o pencereye ait bilgiler kayıt bilgilerinin arasına eklenir.
- CD/DVD/USB v.s. Ortam Değişiklikleri: Kullanıcı bu ortamlardan birini bilgisayarına taktığında ve çıkardığında bu işleme ilişkin zaman ve ortama ilişkin seri numarası, etiket v.s. gibi bilgiler kayda eklenir.
- Pano Değişimleri: Panoya kopyalanan metin bilgilerin kaydı ve bu işlemin zamanı tutulur.
- Pano Limiti: Pano değişiminden kayda eklenecek metnin büyüklüğüne bir sınır koyar.
- Limit Kadarını Alıp Aktar: Bu sınır belirlenmişse eğer panoya kopyalanan metin bu sınırı aşarsa bu işlemde sadece sınır kadar olanı alınıp kayıt bilgilerine eklenir.
- Limiti Aşanı Aktarma: Bu durumda panoya kopyalanan metin sınırı aşıyorsa metin kayıt bilgilerinin arasına aktarılmaz fakat işleme ait bilgi kayıtta yer alır.
- Periyodik Ekran Görüntüsü Al: Periyodik olarak ekranın görüntüsünü alır.
- Görüntü Alma Aralığı: Dakika cinsinden periyodik ekran görüntüsü alma aralığı.
- Tüm Ekran: Ekran görüntüsü tüm ekranı gösterir.
- Etkin Pencere: Ekran görüntüsü sadece kullanıcının o an çalıştığı pencereyi gösterir.
- Fare Tıklamalarının Görüntüsü: Fare ile tıklanan bölgenin ekran görüntüsü alınır.
- Tıklama Görüntü Boyutu: Fare tıklama görüntülerinin boyutu.
- BMP: Görüntülerde BMP formatını kullan. Bu durumda dosya büyüklüğü çok fazla olacaktır.

- JPG: Görüntülerde JPG formatını kullan.
- JPG Kalitesi (%): JPG kalitesi. Düşük kalite az dosya büyüklüğünü ifade etmektedir.
- Hedef Sözcük Kontrolü Yap: Hedef anahtar sözcüklerin klavyeden girilip girilmediğinin kontrolü yapılır.
- Windows Oturum Kapatma Zamanı: Windows işletim sistemi kapandığında bu işlemin yapıldığı tarih ve zaman kayıtlar arasına alınır.
- Yazıcı Çıktısı Bilgileri: Varsayılan yazıcıdan alınan yazıcı çıktılarına ilişkin bilgiler tutulur.
- Erişilen Programları Tut (Exe, Com, Bat, Cpl): Sistemin veya kullanıcının çalıştırdığı programlar çalışma zamanları ile beraber tutulur.
- Dosya İşlemlerini Tut: En fazla iki sabit disk sürücüde dosyalarda ekleme/silme ve değişikliklerin kaydı tutulur.
- Ekleme/Silme: Yeni dosya eklendiğinde ve silindiğinde kayıt tutar.
- Değişiklik: Dosyalar üzerinde değişiklik yapıldığında ve dosya ismi değiştirildiğinde kayıt tut.
- Türler: Diskte değişiklikleri takip edilecek dosyaların uzantılarını barındırır.
- MAC Adresini Al: Her açılışta bilgisayarın MAC adresini alır.
- Konak Adı Ve IP Adresleri: Her açılışta bilgisayarın konak adını ve IP adreslerini alır.

Seçenekler: E-Posta ve FTP Bilgileri

Şekil 7.7 (c)'de ekran görüntüsü verilen bu sayfada TürkSpyware'in kayıt dosyasını e-posta ve FTP ile aktarabilmesi ile ilişkili seçenekler sunulmuştur. Bu seçenekler aşağıda açıklanmıştır.

- SMTP Sunucu Adresi: SMTP protokolü ile çalışan sunucunun IP adresi veya URL adresidir.
- Kimden: Seçimlik mesajın kimden geldiği bilgisidir.
- Kime: Kayıt dosyalarının E-posta ile gönderileceği adrestir.
- Konu: Bu bilgisayardan gönderilen mesajlarda konuya eklenecek etikettir.

- Test Et: Ayarların doğru çalışıp çalışmadığının sınanmasıdır.
- FTP Sunucu Adresi: Kayıtların gönderileceği FTP sunucusunun IP adresi veya URL adresidir.
- Kullanıcı Adı: FTP hesabının kullanıcı adıdır.
- Şifre: FTP hesabının şifresidir.
- FTP Test Et: Ayarların doğru çalışıp çalışmadığının sınanmasıdır.

Seçenekler: Zamanlama ve Kayıt Bilgileri

Şekil 7.7 (d)'de ekran görüntüsü verilen bu sayfada TürkSpyware'in kayıt dosyasını e-posta ve FTP ile aktarırken yerine getirmesi istenen zamanlama ile ilişkili bilgiler görülebilmekte ve değiştirilebilmektedir. Sunulan seçenekler aşağıda açıklanmaktadır.

- Kayıt dosyasını gönderme aralığı (saat): Belirtilen saat her geçildiğinde kayıt bilgileri otomatik olarak E-posta ile gönderilir.
- Kayıt dosyası şu büyüklüğü aşınca gönder (KB): Kayıt dosyası belirtilen büyüklüğü her geçtiğinde otomatik olarak e-posta ile gönderilir.
- Kayıt dosyasını program her başlatıldığında gönder: Program her başlatıldığında kayıt bilgileri gönderilir.
- Kayıt dosyasını şifrele: Kayıt dosyasını şifrele.

7.4. Kayıt Dosyası Yapısı

Kayıt dosyası tutulan bilgilere göre değişik yapılarda kayıtlar içermektedir. Bu yapılar takip eden kısımda örneklerle açıklanmıştır.

7.4.1. Kayıt dosyası başlık bilgileri

Her program açılışında programın açılış zamanı, sistemi kullanan kullanıcının adı ve bağlandığı bölgenin adı bu kısımda aşağıdaki örnekte verildiği gibidir.

****

BASLAMA ZAMANI: 15.06.2005 15:48:52

KULLANICI ADI: kullanıcı

BÖLGESİ: DOMAIN

****

7.4.2. Gezilen pencerelere ait bilgiler

Kullanıcının üzerinde çalıştığı pencere her değiştiğinde aşağıda verilen biçemde bilgi kaydedilmektedir:

[PENCERE: PENCERE BAŞLIĞI (PENCERE SINIF NUMARASI) (TARİH ZAMAN)]

Buna bir örnek aşağıda verilmiştir.

[PENCERE: Tez - TurkSpyware Klavye Dinleme Sistemi.doc - Microsoft Word (49539)(15.06.2005 15:50:41)]

7.4.3. CD/DVD/USB v.b. ortam araçları değişiklikleri

Böyle bir ortam bilgisayara takıldığında veya çıkarıldığında aşağıda verilen biçemde bilgi, kayıt dosyasına yazılmaktadır.

[(SÜRÜCÜ KÖK DİZİNİ) SÜRÜCÜ TİPİ Ortamı ULASTI/CIKARILDI (TARİH ZAMAN)]

ETİKET: ETİKET BİLGİSİ (Seri No: SERİ NUMARASI)

Böyle bir kayıta örnek takip eden satırda verilmiştir.

[(E:\) CD-ROM Ortamı ULASTI (15.06.2005 15:53:24)]

ETİKET: OYUNLAR (Seri No: 433365628)

7.4.4. Pano değişimleri

Kullanıcı herhangi bir metni kopyaladığında kayıt yapısı sınır seçeneklerine göre değişmektedir.

Sınır konulmadığında kayıt dosyasına takip eden satırlarda verilen biçem ve örnekte olduğu gibi bir kayıt eklenir:

[PANO DEĞİŞTİ (KOPYALAMA İŞLEMİNİN YAPILDIĞI PENCERE ADI) (TARİH ZAMAN)]

KOPYALANAN METNİN TAMAMI

[PANO DEĞİŞTİ (Tez - TurkSpyware Klavye Dinleme Sistemi.doc - Microsoft Word) (15.06.2005 15:57:01)]

v.s. v.s. v.s. v.s. v.s. ... v.s.

Belirlenen limit kadarını alıp aktar seçeneği ile aşağıdaki örnekteki gibi bir kayıt oluşabilir:

[PANO DEĞİŞTİ (Tez - TurkSpyware Klavye Dinleme Sistemi.doc - Microsoft Word) (15.06.2005 15:58:51)]

[15 karakterlik bolümü:]

v.s. v.s. v.s. ...

Limiti aşanı aktarma seçeneği seçilmişse belirlenen limiti geçen bilgilerin hiç biri kayıt dosyasına alınmaz sadece aşağıda verilen örnekteki gibi bir pano değişimi yaşandığına dair bir not düşülür:

[PANO DEĞİŞTİ (Tez - TurkSpyware Klavye Dinleme Sistemi.doc - Microsoft Word) (15.06.2005 16:00:19)]

[50 karakterlik limiti astığından tutulmamıştır]

7.4.5. Windows oturum kapatma zamanı

Kullanıcı herhangi bir şekilde bilgisayarını kapattığında sistem bu bilgiyi aşağıdaki örnekteki gibi kaydeder:

****

WINDOWS OTURUMU KAPATILIYOR...

15.06.2005 16:44:44

****

7.4.6. Yazıcı çıktısı bilgileri

Varsayılan yazıcıdan çıktı alındığında bu işe ait bilgiler aşağıdaki örnekte olduğu gibi kaydedilir:

[YAZICI KUYRUK DÖKÜMÜ]

İŞ NO: 9

İŞ DURUMU: BASKI ALINIYOR

YAZICI ADI: HP LaserJet 1220 Series PCL

MAKİNE ADI: \\10.44.44.44

KULLANICI ADI: kullanici

BELGE ADI: Klavye Dinleme Sistemleri - Notepad

SAYFA SAYISI: 1

BELGE BOYUTU: 96 Byte

ZAMAN: 15.06.2005 16:38:56

7.4.7. Erişilen programları tut (exe, com, bat, cpl)

C:\ ve D:\ gibi en fazla iki adet sabit disk sürücü üzerinde sistem ve kullanıcı tarafından çalıştırılan programlara ait bilgiler aşağıdaki örnekte olduğu gibi gösterilmektedir.

[PROGRAM ERİŞİM: C:\WINNT\system32\notepad.exe (15.06.2005 16:39:15)]

7.4.8. Dosya işlemlerini tut

C:\ ve D:\ gibi en fazla iki adet sabit disk sürücü üzerinde önceden belirlenen uzantıdaki dosyalarda yapılan işlemler aşağıdaki gibi tutulmaktadır.

Yeni bir dosya eklendiğinde:

[DOSYA SİSTEMİNDE DEĞİŞİKLİK: DOSYA EKLENDİ: C:\New Text Document.txt (15.06.2005 16:41:42)]

Dosya ismi değiştirildiğinde:

[DOSYA SİSTEMİNDE DEĞİŞİKLİK: DOSYA ADI C:\New Text Document.txt'dan C:\Deneme.txt'e DEĞİŞTİRİLDİ (15.06.2005 16:41:55)]

Dosyanın içeriği değiştiğinde:

[DOSYA SİSTEMİNDE DEĞİŞİKLİK: DOSYA DEĞİŞTİRİLDİ: C:\Deneme.txt (15.06.2005 16:42:02)]

Dosya silindiğinde:

[DOSYA SİSTEMİNDE DEĞİŞİKLİK: DOSYA SİLİNDİ: C:\Deneme.txt (15.06.2005 16:42:06)]

7.4.9. MAC adresini al

Sistemin çalıştığı bilgisayarın MAC adresi alınması istenildiğinde her çalışmada bu bilgi aşağıdaki gibi kaydedilir:

[MAC Adresi: 00-04-44-44-A4-4D]

7.4.10. Konak adı ve IP adresleri

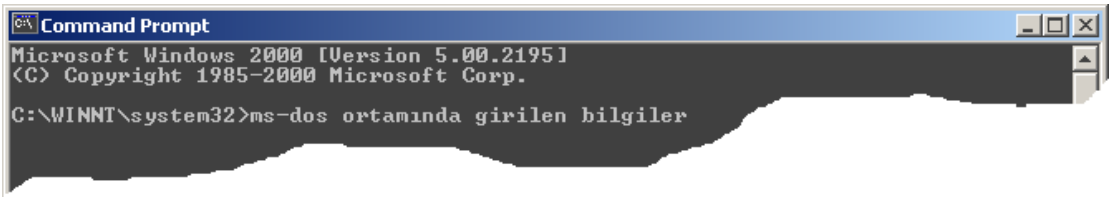
Konak adı ve IP adresleri tutulmak istenirse program her açılışta bu bilgileri aşağıdaki gibi kaydeder:

[Konak Adı: konak-makine]

[1. IP adresi: 10.0.44.44]

7.5. Program Çalışma Örnekleri

Geliştirilen TürkSpyware yazılımının problemsiz çalıştığını tespit etmek için, yazılım bir çok durumda test edilmiştir. Elde edilen sonuçlar programın başarımı açısından oldukça iyidir. Notepad, Wordpad ve tüm Microsoft Office ürünlerinde kısacası bütün programlarda program tuş basımı bilgilerini başarı ile elde etmiştir. Klavyeden girilen şifre bilgileri dahil bütün bilgiler kayıt dosyasında bulunmaktadır.



Şekil 7.9. MS-DOS komut istemi kutusu

Örneğin farklı bir yapı sergileyen MS-DOS komut istemi kutusundan girilen Şekil 7.9'daki bilgi aşağıdaki gibi elde edilmiştir:

[PENCERE: (49867)(15.06.2005 18:11:46)]

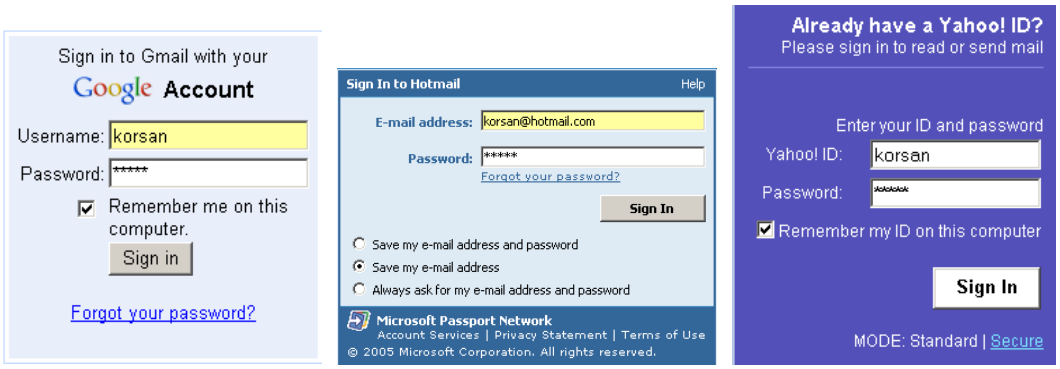
ms-dos ortamında girilen bilgiler

Programın çalışmasına ilişkin örnek seçerken, çok sayıda kişinin kullandığı iki ortam seçilmiştir. Web tabanlı e-posta hizmeti sağlayan İnternet siteleri ve Türkiye'de çevrimiçi bankacılık yapan bankaların İnternet şubelerinin giriş sayfaları üzerinde yazılım etkin bir şekilde test edilmiştir. Her iki örnek çalışma oldukça sarsıcı

sonuçları ortaya çıkarmaktadır. Bu alanların seçilmesi bilgi ve bilgisayar güvenliği konusunda hem dünya'da hem de Türkiye'de durumun ne olduğunu ve klavye dinleme sistemlerinin bu durumlarda ne kadar tehlikeli olacağını göstermek için özellikle seçilmiştir. Örneklerle ilgili ayrıntılı bilgi Bölüm 7.6 ve 7.7'de sunulmuştur.

7.6. Web Tabanlı E-Posta Sağlayıcıların Giriş Sayfaları

Programın çalışmasına ilişkin örnek olarak çok sayıda kişiye e-posta hizmeti sağlayan Google'ın Gmail'i, Microsoft'un Hotmail'i ve Yahoo'nun Yahoo e-posta giriş sayfaları verilebilir. Şekil 7.10'de test sırasında alınan görüntüler gösterilmektedir.



(a) Google Gmail (b) Microsoft Hotmail (c) Yahoo mail

Şekil 7.10. Popüler e-posta hizmeti veren sitelerin giriş sayfasının TürkSpyware ile test görüntüsü

Gmail giriş sayfasında girilen, "korsan" ve "sifre" bilgisinin klavye dinleme sistemindeki kaydı aşağıdadır:

[PENCERE: Welcome to Gmail - Microsoft Internet Explorer (49566)(24.05.2005 16:28:26)]

[INTERNET EXPLORER URL: https://www.google.com/accounts/ServiceLogin?service=mail&passive=true&rm=false&continue=http%3A%2F%2Fgmail.google.com%2Fgmail%3Fui%3Dhtml%26zy%3Dl]

korsan<SEKME>sifre

Hotmail giriş sayfasında girilen “korsan@hotmail.com” ve “sifre” bilgisinin klavye dinleme sistemindeki kaydı aşağıdadır:

[PENCERE: Sign In - Microsoft Internet Explorer (49566)(24.05.2005 16:18:41)]

[INTERNET EXPLORER URL: http://login.passport.net/uilogin.srf?lc=1033&id=2&vv=30]

korsan<CTRL><ALT SAG>qhotmail.com<SEKME>sifre

Yahoo mail giriş sayfasında girilen “korsan” ve “sifre” bilgisinin klavye dinleme sistemindeki kaydı aşağıdadır:

[PENCERE: Yahoo! Mail - The best web-based email! - Microsoft Internet Explorer (49566)(24.05.2005 16:23:38)]

[INTERNET EXPLORER URL: http://mail.yahoo.com]

korsan<SEKME>sifre

Yukarıdaki örneklerden görüleceği gibi kayıtlarda giriş sayfalarının URL adreslerini de elde etmek mümkündür. Bu örneklerden elde edilen sonuç TürkSpyware gibi klavye dinleme sisteminin yüklenmiş olduğu bir bilgisayardan bu tür şifre bilgilerini elde etmenin çok kolay olduğudur. Bu tür e-posta hizmeti sağlayan şirketler, her kadar bedava olarak hizmet verse de bu konuya yönelik bir tedbir sunmamaları da ilginç bir durumdur. Yapılan bu tip testlerden çıkarılan sonuç, ücretsiz olarak sunulan hizmetlerin çoğunda bir güvenlik açığının olabileceğinin her zaman hatırda tutulmasıdır.

7.7. Türkiye’de Çevrimiçi Faaliyet Gösteren Bankaların Klavye Dinleme Sistemlerine Karşı Korunma Durumu

Bölüm 5.7.2’de “Çevrimiçi bankacılık ve Türkiye’de durum” konusu ele alınmış ve konunun ileride mercek altına alınacağı belirtilmişti. Dünya çapında yaygın ücretsiz hizmet veren web tabanlı e-posta sitelerine giriş sırasında başarı ile bütün bilgileri ele geçiren TürkSpyware yazılımının son derece güvenli olduğu iddia edilen bankaların İnternet şubelerinde ne yaptığı ile ilgili ayrıntılar aşağıda verilmektedir. İnternet

bankacılığının klavye dinleme sistemleri açısından güvenlik seviyesini gözler önüne serecek bilgiler bu kısımda anlatılmaktadır. TürkSpyware ile yapılan test sonuçlarına geçmeden önce bir kaç hususun belirtilmesinde fayda görülmektedir.

İnternet üzerinde çalışan bankaların çoğunluğu klavye dinleme sistemlerinden haberdar olduğu ve sistemlerini bunları önleyecek şekilde tasarlamaya çalıştıkları görülmüştür. Kullanıcı adının normal, şifrenin şifreli (girilen şifre karakterlerinin görülmemesi için maskeli olarak * basan) metin kutuları ile alındığı ve sadece bu tür bilgi girişini güvenlik açısından yeterli gören bir kaç bankanın var olduğunu görmek, hayret verici bir durum olarak tanımlanmaktadır. Bankanın müşterisinden giriş sırasında istediği bilgilerin türü ve sayısı ne olursa olsun; sadece klavyeden girilen bu tür bilgilere dayanan bir çevrimiçi banka şubesi, klavye dinleme sistemleri için çok kolay bir avdır. Bunun farkında olan çoğu bankanın bir kısmı, şifre, parola gibi bir bilginin kullanıcı tarafından klavyeden değil de sanal klavye ile girilmesini sağlamaktadır. Çok az sayıda banka ise güvenli bilgi girişini sağlamak için daha farklı yaklaşımlar kullanmaktadır. Bu yaklaşımlarla, klavye dinleme sistemleri arasında ilişkinin doğru bir şekilde belirlenmesi gerekmektedir. Çalışmanın bu kısmında öncelikle bankaların klavye dinleme sistemlerine karşı aldığı önlemler belirtilmiştir. Sonraki kısımda ise bütün bu önlemlere rağmen hazırlanan TürkSpyware klavye dinleme sistemi ile ne tür sonuçlar elde edildiği ayrıntılarla gösterilecektir. Son kısımda bütün bu veriler ışığında Türkiye'de çevrimiçi faaliyet gösteren bankaların "hali hazırda" güvenlik yeterlilik seviyeleri incelemesine dayanan sonuçlar değerlendirilecektir. Konu farklı başlıklar altında incelenmiş olup takip eden kısımlarda sunulmaktadır.

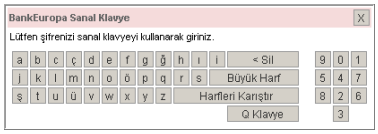
7.7.1. Sanal klavyeler

Yukarıda bahsedildiği gibi bankaların klavye dinleme sistemlerine karşı buldukları çarelerin en başında özellikle şifre gibi bilgilerin klavyeden değil de fare kullanarak girilmesini sağlayan sanal klavyeler gelmektedir. İşletim sistemi ile bütünleşik gelen veya üçüncü parti sanal klavyelerin kullanımı ve farklı klavye donanımları ile ilgili ayrıntılı diğer bilgiler Bölüm 7'de ayrıca sunulmaktadır. Bu kısımda bankaların

İnternet sayfalarında kullanmış oldukları sanal klavye yaklaşımları incelenmektedir. Şekil 7.11'de Türkiye'de çevrimiçi faaliyet gösteren bankaların kullanmış oldukları sanal klavye yaklaşımları sunulmuştur. Bu yapılarda, kullanıcı şifre ve önemli bilgi girişlerini, klavye yerine ekranda gösterilen tuşlardan oluşan tuş resimlerini fare ile tıklayarak ya da üzerinde bir süre bekleyerek yapmaktadır.

Şekil 7.11'de görülebileceği gibi çok çeşitli sanal klavyeler bankalar tarafından kullanılmaktadır. Sadece sayısal bilgi içeren sanal klavyeler olduğu gibi alfa sayısal bilgi girişine de izin veren sanal klavyeler bulunmaktadır. Sanal klavyedeki bir diğer önemli hususta sanal klavyedeki kullanılmak istenen tuşa fare ile tıklamaya gerek kalmadan belli bir süre o tuşun üzerinde beklenmesiyle o tuş bilgisini ana sayfaya gönderen sanal klavye seçeneklerinin bulunmasıdır. "Tıksız sanal klavye" olarak adlandırılabilecek bu tip sanal klavyeler fare tıklamalarının ekran çıktısını alan casus programlara karşı bir önlem olarak kullanılmaktadır. Sanal klavyelerin kullanımında ortaya çıkabilecek bir diğer husus gizli bilgi girişi sırasında kullanıcının her hangi bir kişi tarafından fark edilmeden izlenip tıkladığı tuşların gözlemlenmesidir. Bu durumu zorlaştırmak için bazı sanal klavyeler üzerindeki her tuşun yerini bir kullanımdan sonra rasgele olarak karıştırmaktadır. Bu sayede, davetsiz gözlerin sanal klavye kullanıcılarını işlem yaparken fark edebilmeleri veya tıklanan tuşu tahmin edebilmeleri güçleştirilmiş olmaktadır.

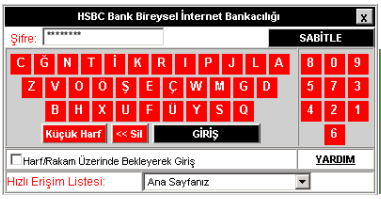
Anadolubank A.Ş.



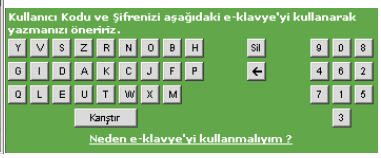
BankEuropa Bankası A.Ş.

Denizbank A.Ş.

Finans Bank A.Ş.

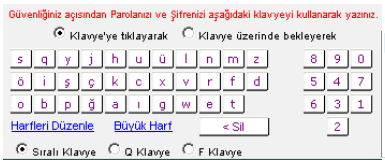


HSBC Bank A.Ş.

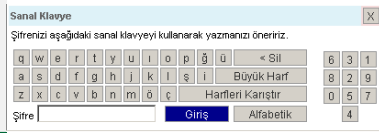


Koçbank A.Ş.

Oyak Bank A.Ş.



Şekerbank T.A.Ş.



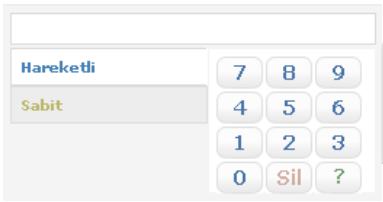
Tekfenbank A.Ş.

Tekstil Bankası A.Ş.

Türk Dış Ticaret Bankası A.Ş.

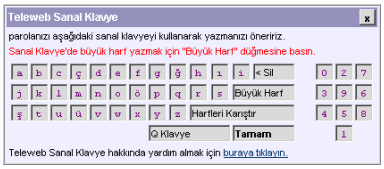
Türk Ekonomi Bankası A.Ş.

Türkiye Garanti Bankası A.Ş.



Türkiye İş Bankası A.Ş.

Türkiye Sınai Kalkınma Bankası A.Ş.



Yapı ve Kredi Bankası A.Ş.

Şekil 7.11. Bankaların kullandıkları sanal klavyeler (Haziran 2005 itibariyle)

7.7.2. Diğer önlemler

Gizli bilgilerin alınmasını önlemek için bankaların son günlerde kullandığı yöntemlerden biri de klavye dinleme önleme sistemi yazılım modüllerinin banka tarafından kullanıcının bilgisayarına (bir defaya mahsus) kurdurulup; sadece o bankaya giriş yapıldığında otomatik olarak çalıştırılmasıdır. Bu sayede her hangi bir şekilde o bilgisayarda bir klavye dinleme sistemi yazılımı varsa o program bloke edilebilmektedir. Genelde ücretsiz olarak dağıtılan bu programların fare tıklamaları ile bilgi kaçırılmasını önleyen türleri de bulunmaktadır.

Bunun dışında daha ileri bir koruma sağlayan tek kullanımlık şifre üreten küçük cihazlar bankaların İnternet siteleri ile eş zamanlı çalışarak; belirli bir zaman için geçerli olacak şekilde üretilen şifre bir şekilde ele geçirilmiş olsa bile geçerlilik süresi dolduğundan tekrar kullanılamayacaktır. Bu cihazlarla üretilen şifreler kullanıcı tarafından kullanılmazlarsa belli bir süre sonra (40 sn gibi) geçersiz kılınır. Ülkemizde bu tür yaklaşımı kullanan iki bankanın verdikleri cihazların görüntüleri Resim 7.1'de verilmektedir.

(a) Akıllı Anahtar, Koçbank A.Ş. (b) Şifrematik, Türkiye Garanti Bankası A.Ş.

Resim 7.1. Tek kullanımlık şifre üretme cihazları

7.7.3. Mevcut klavye dinleme önleme sistemleri ile TürkSpyware'in testi

Çizelge 7.3'de, Bölüm 6.5'de ayrıntıları ile açıklanmış olan piyasada mevcut klavye dinleme önleme sistemlerinden Advanced Anti Keylogger, Anti-keylogger ve

Keylogger Hunter paket yazılımlarının, TürkSpyware ile yapılan test sonuçları gösterilmektedir. X, o özelliğin var olduğunu; - ise belirtilen özelliğin bulunmadığını göstermektedir. Testler Windows XP Hizmet Paketi yüklü bir bilgisayarda yapılmıştır. Test sonuçları klavye dinleme önleme sistemleri için çok iç açıcı değildir. Tuş basımı bilgilerini önlemede başarılı olan sistemler fare tıklamaları, gezilen pencereler, pano hareketleri gibi bir çok klavye sisteminde bulunan özelliklerin önüne geçememektedirler. TürkSpyware için bu test sonuçları başarılı sayılabilir. Klavye dinlemenin önlenmesi oldukça önemli bir durum olsa da TürkSpyware'in sağladığı diğer tüm izlemelerin önlenememesi geliştirilen yazılımın oldukça yetenekli olduğunu göstermektedir.

Çizelge 7.3. Mevcut klavye dinleme önleme sistemlerinin TürkSpyware ile test sonuçları

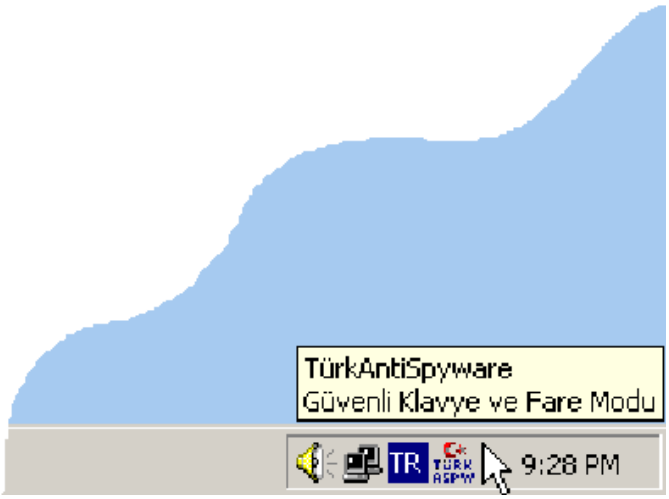
Ürün:  *TürkSpyware 2.1. ile test*	*Advanced Anti Keylogger* 	*Anti-keylogger* 	*Keylogger Hunter* 
Tuş bilgilerinin yakalanmasının önlenmesi	X	X	X
Kontrol ve sistem tuşlarının yakalanmasının önlenmesi	X	-	-
Pano değişiminin izlenmesinin önlenmesi	-	- (önlendiği söyleniyor)	-
Fare tıklama görüntülerinin alınmasının önlenmesi	-	-	-
Gezilen pencerelerin yakalanmasının önlenmesi	-	-	-
Diğer seçeneklerin önlenmesi	-	-	-

Sonuç olarak TürkSpyware yazılımı, amaçladığı hedefler açısından oldukça başarılı sayılabilir. Bu yazılımın Bölüm 5.7'de anlatıldığı gibi faydalı kullanımlara yönelik düzenlemelerle bir çok yerde kullanılabileceği düşünülmektedir. Ama bu bölümde gösterildiği gibi klavye dinleme sistemleri oldukça tehlikeli sonuçlar üretebilecek casus yazılımlardır. Bunlara karşı ne gibi önlemler alınacağı Bölüm 6'da

incelenmiştir. Bu bölümden yola çıkarak geliştirilen klavye dinleme önleme sistemi, TürkAntiSpyware yazılımı hakkında ayrıntılı bilgi Bölüm 8'de verilmektedir.

8. GELİŞTİRİLEN KLAVYE DİNLEME ÖNLEME SİSTEMİ: TürkAntiSpyware

Günlük hayatta karşılaşılan örneklerle klavye dinleme sistemlerinin bilgi güvenliğine yönelik ne kadar ciddi tehditler içerebileceğinin Bölüm 5'de açıklandığını ve bu tür kötü niyetli kullanımlara karşı etkin çözüm alması gereken yazılımların, hem sayı hem de koruma anlamındaki yetersizliklerinin gözden geçirildiği Bölüm 6'da, klavye dinleme sistemlerine yönelik tedbirlerden ve bunların önlenmesi için alınması gereken tüm tedbirlerin neler olduğunun incelendiğini bir kez daha hatırlatmakta fayda vardır. Bu bölümde, daha önceki iki bölümde üzerinde durulmuş olan tehditlerin ortadan kaldırılmasında kullanılabilecek ve klavye dinleme sistemlerini etkisiz hale getirebilen bir sistem olarak tasarlanmış ve gerçekleştirilmiş olan bir klavye dinleme önleme sistemi olan TürkAntiSpyware yazılımı ayrıntılı olarak tanıtılmıştır.



Şekil 8.1. TürkAntiSpyware sistem tepsisi simgesi

Geliştirilen TürkAntiSpyware yazılımının sistem tepsisinde tek bir simge ile ekranda çok küçük yer işgal edecek şekilde tasarlanan bir yazılım olduğu Şekil 8.1'de gösterilmektedir. Bu yazılım, klavye dinleme yöntemlerinden özellikle virüs ve Truva atı casus yazılımları ve çoğu klavye dinleme sistemi tarafından en çok kullanılan yöntem olarak bilinen Windows klavye çengeli yöntemine karşı, diğer mevcut klavye dinleme önleme sistemlerinde bulunmayan yeteneklere sahip bir

casus savar yazılımdır. Bu yetenekler arasında en önemlisi, hiç bir klavye dinleme önleme sisteminde bulunmayan görsel izleme ile fare tıklama görüntülerinin alınarak; sanal klavyelerin kullanımını faydasız hale getiren klavye dinleme sistemlerine karşı etkin koruma sağlamasıdır. Bu özelliği ile TürkAntiSpyware yazılımı, mevcut klavye dinleme sistemleri arasında ayrıcalıklı bir konuma sahiptir.

Yazılımın bir diğer kullanım alanı ise casus yazılımlara karşı korunmadır. Bilgisayar sistemine bulaşmış olabilecek casus yazılımları tespit etmek için Bölüm 3 ve 4'de aktarılan bilgiler ışığında gerçekleştirilen bazı kullanışlı araçlar TürkAntiSpyware yazılımıyla bütünleştirilmiştir. Bu araçlar yardımıyla herhangi bir kullanıcı, çok kolay bir şekilde sistemini denetleyebilmekte; şüpheli görülebilecek öğeler hakkında ayrıntılı bilgileri anında alabilmekte ve kötücül yazılımların sistemde varlığını sürdürmesi için ihtiyaç duyduğu bazı kritik noktalarda gerçek zamanlı korunma elde edebilmektedir. Yazılımın bir diğer faydalı işlevi ise, bilgisayar kullanırken otomatik olarak tutulan bilgilerin kişisel gizliliği sağlamak amacıyla görülebilmesi ve silinebilmesidir.

Yazılımın genel özellikleri Çizelge 8.1'de verilmektedir:

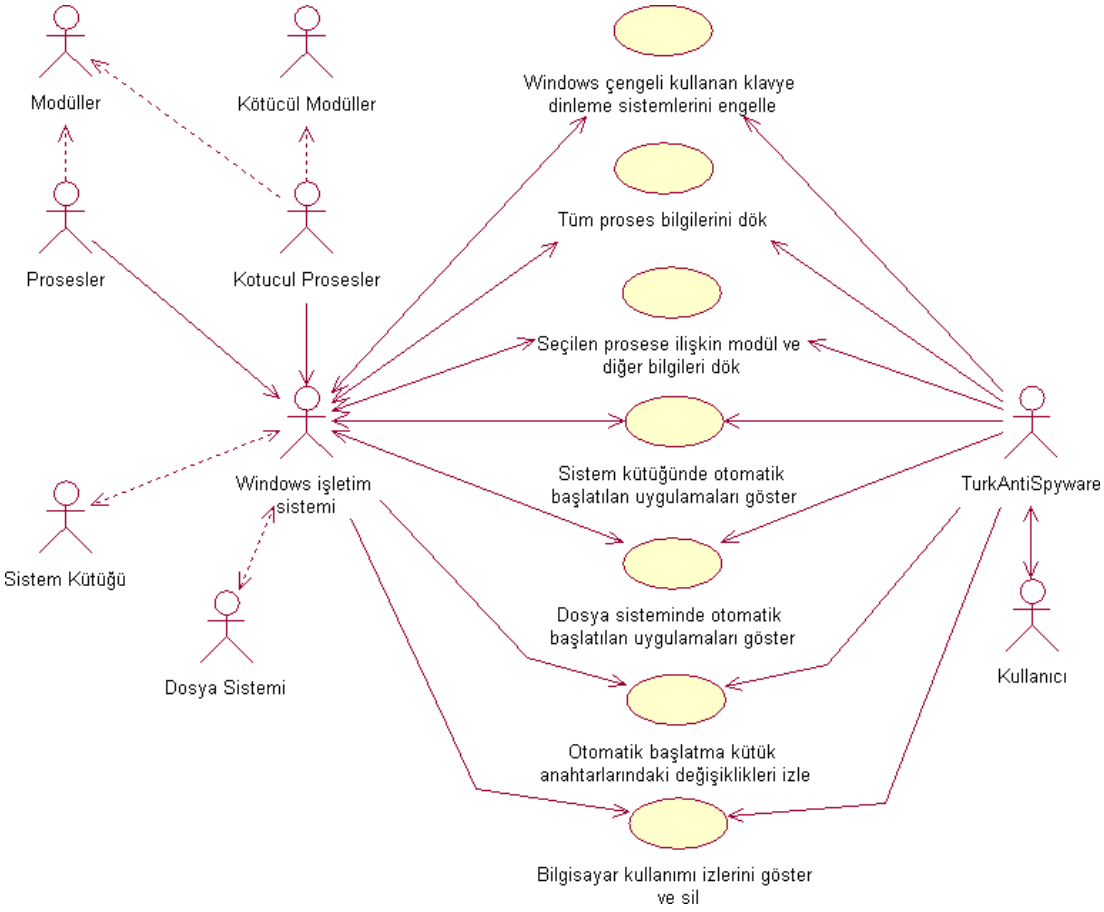
Çizelge 8.1. TürkAntiSpyware genel özellikleri

Program Adı	TürkAntiSpyware
Sürüm	1.1.
Sürüm Tarihi	15.06.2005
Çalıştığı Platformlar	Microsoft NT/2000/XP
Geliştirme Dili	Microsoft Visual C++, Platform Software Developer Kit
Kaynak Kod Satır Sayısı	~5000 satır
Çalıştırılabilir Modül Boyutu	332 KB
Modül Sayısı	9

Geliştirilen TürkAntiSpyware klavye dinleme önleme sisteminin kullanım durumları, yazılım modülleri, kullanıcı arabirimi yapıları ve sahip olduğu işlevler hakkında ayrıntılı bilgiler takip eden kısımlarda ayrıntılı olarak verilmektedir.

8.1. Kullanım Durumları

TürkAntiSpyware yazılımın tasarımı ile ilgili hazırlanan kullanım durumu diyagramı Şekil 8.2'de gösterilmektedir.



Şekil 8.2. TürkAntiSpyware kullanım durumu (use case) diyagramı

Windows işletim sisteminde normal proseslerin yanında kötücül proses ve bunlara ait modüller işletim sisteminin sistem kütüğünü ve dosya sistemlerini kullanmaktadır. Şekil 8.2'deki kullanım durumu diyagramında gösterildiği gibi, TürkAntiSpyware yazılımı bir klavye dinleme önleme sistemi olarak, Windows çengeli kullanan klavye dinleme sistemlerini engellemekte; sistemde o an çalışmakta olan bütün proses bilgilerini ve bu proseslere ilişkin modül ve diğer bilgileri dökümünü sunabilmekte; sistem kütüğü ve dosya sistemi aracılığıyla otomatik başlatılan uygulamaları göstermekte; kendini otomatik başlatmak isteyen uygulamaların kütükte yaptıkları değişiklikler gerçek zamanlı olarak takip edilmekte ve kişisel gizlilik sağlamak

amacıyla bilgisayar kullanırken gerek işletim sistemi gerekse çok sık kullanılan farklı üçüncü parti uygulamalar tarafından toplanan hemen hemen bütün bilgiler silinebilmektedir.

8.2. Yazılım Modülleri

Bu özellikleri sağlamak amacıyla tasarlanan ve gerçekleştirilen yazılıma ait modüller aşağıda sıralanmaktadır:

- Klavye Dinleme Önleme Modülü
- Fare Dinleme Önleme Modülü
- Proses ve Modül Bilgileri Modülü
- Dosya Sistemi Otomatik Başlatma Raporlama Modülü
- Sistem Kütüğü Otomatik Başlatma Raporlama Modülü
- Sistem Kütüğü Otomatik Başlatma Gerçek Zamanlı Koruma Modülü
- Bilgisayar Kullanımı İzleri Listeleme ve Silme Modülü
- Güvenli Klavye Modülü
- Diğer Araçlar Modülü

Bu modüllerin açıklamaları takip eden kısımda alt başlıklar halinde sunulmaktadır.

8.2.1. Klavye dinleme önleme modülü

TürkAntiSpyware klavye dinleme önleme sisteminin en önemli modüllerinden biri olan bu modülde, Windows çengeli yöntemi ile çalışan klavye dinleme sistemlerinin klavye kullanılarak girilen bilgileri elde edebilmesinin önüne geçecek yazılım yapıları bulunmaktadır.

8.2.2. Fare dinleme önleme modülü

Fare dinleme önleme modülünde fare hareket ve tıklamalarını takip eden klavye dinleme sistemlerinin bilgi toplamasını önleyecek yazılım yapıları bulunmaktadır.

8.2.3. Proses ve modül bilgileri modülü

Bu modül sistemde o an çalışmakta olan prosesler ve modüller hakkında ayrıntılı bilgi vermek amacıyla hazırlanmıştır. Windows işletim sisteminde kullanılan görev yöneticisinde (Task Manager) bile bulunmayan ve çalışan prosesler hakkında oldukça kullanışlı bilgilerin alınabilmesi bu modül aracılığıyla gerçekleştirilmiştir.

8.2.4. Dosya sistemi otomatik başlatma raporlama modülü

Windows işletim sisteminde kullanılan özel dosyalara kendilerini Windows işletim sistemi ile otomatik olarak başlatan yapılar bu modülde listelenmektedir.

8.2.5. Sistem kütüğü otomatik başlatma raporlama modülü

Windows işletim sistemi kütüğünde otomatik başlatma anahtarlarının içeriklerinin tamamı bu modül ile listelenmektedir. Modül, bu yapılardan istenilenlerin silinmesine de olanak sağlamaktadır.

8.2.6. Sistem kütüğü otomatik başlatma gerçek zamanlı koruma modülü

Kullanıcıların her zaman sistem kütüğünde yer alan otomatik başlatma girdilerini takip etmesinin zor olabileceği düşünülerek geliştirilen bu modül, sistem kütüğünün bu anahtarlarını gerçek zamanlı olarak izlemekte; bu alanlarda yapılan değişiklikler anında kullanıcıya aktarılmakta ve istenirse yapılan değişiklik geri alınabilmektedir. Bu sayede sisteme bulaşmak isteyen yazılımları saptamak ve gerekli tedbirleri gecikmeden almak mümkün olabilmektedir.

8.2.7. Bilgisayar kullanımı izleri listeleme ve silme modülü

Bu modül geçici dosyalar, İnternet Gezgini'nden girilen adresler ve çeşitli programlar ile en son erişilen dosyalar gibi bir çok bilgisayar kullanımı izini göstermekte ve kullanıcının seçtiği izleri silebilmektedir.

8.2.8. Güvenli klavye modülü

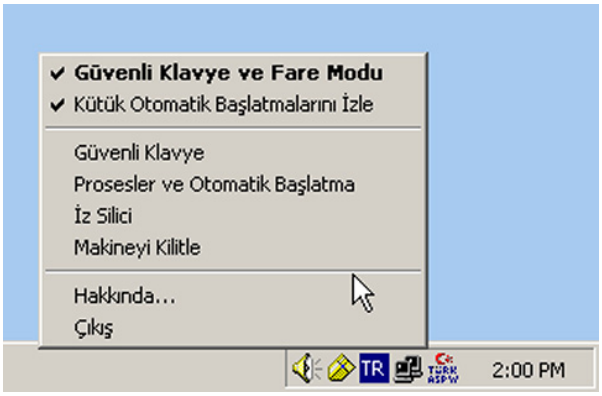
Klavye dinleme sistemlerine karşı özellikle şifre gibi önemli bilgiler girerken kullanılması amacıyla geliştirilen Türkçe sanal klavyeye ilişkin yazılım birimi, bu modül içinde gerçekleştirilmiştir. Modülün sağladığı önemli ayrıcalıklarla ilgili ayrıntılar 8.3.3 kısmında açıklanmaktadır.

8.2.9. Diğer araçlar modülü

İleride daha farklı araçların dahil edilmesinin planlandığı bu modülde şimdilik tek bir tıklama ile çalışılmakta olan bilgisayarın kilitlenmesini sağlayan yapı ve bütün işlevlerin sistem tepsisindeki simge aracılığıyla yerine getirilmesini sağlayan yapı gerçekleştirilmiştir.

8.3. TürkAntiSpyware Kullanıcı Arabirimi ve Kullanım Açıklamaları

TürkAntiSpyware yazılımının sürekli olarak sistemde çalışacak bir program olarak tasarlandığından Şekil 8.3'de örnek bir ekran görüntüsü verilen ana kullanıcı arabiriminin de buna uygun olarak oluşturulmuştur. Bu program, Windows işletim sistemi tepsisinde (system tray) bir simge olarak gözükmektedir. Bu şekilde programın görev çubuğunda yer işgal etmemesi sağlanmaktadır. Kullanıcı bu simge üzerine farenin sağ tuşu ile tıklayınca çıkan menü üzerinden sunulan işlemleri yapabilmektedir.



Şekil 8.3. TürkAntiSpyware program menüsü

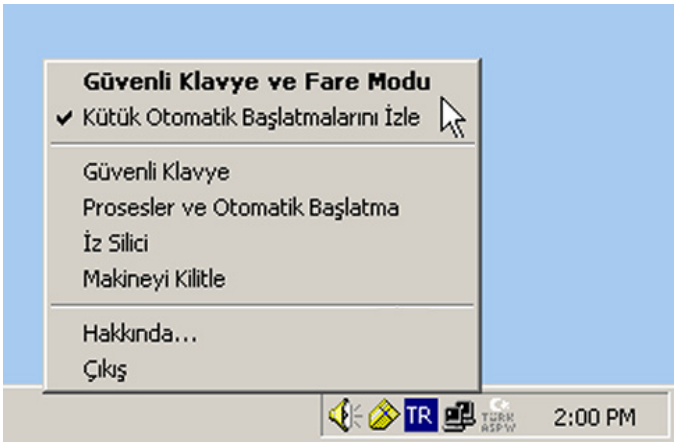
Şekil 8.3'de görülebileceği gibi bu menü,

- Güvenli Klavye ve Fare Modu
- Kütük Otomatik Başlatmalarını İzle
- Güvenli Klavye
- Prosesler ve Otomatik Başlatma
- İz Silici
- Makineyi Kilitle
- Hakkında ve
- Çıkış

öğelerinden oluşmaktadır. Bu menü öğelerin sunduğu işlevler aşağıdaki kısımlarda açıklanmaktadır.

8.3.1. Güvenli klavye ve fare modu

Bu öğe seçili durumda iken kullanılan sistem Windows çengeli ile klavye dinlemeye ve fare tıklama görüntülerine almaya karşı korunma altındadır. İstenildiği durumda bu koruma menü öğesi tıklanarak kaldırılabilir. Tekrar seçildiğinde ise güvenli mod tekrar devreye girer. Bu işlem aynı zamanda sistem tepsisindeki program simgesi çift tıklanarak da gerçekleştirilebilir.

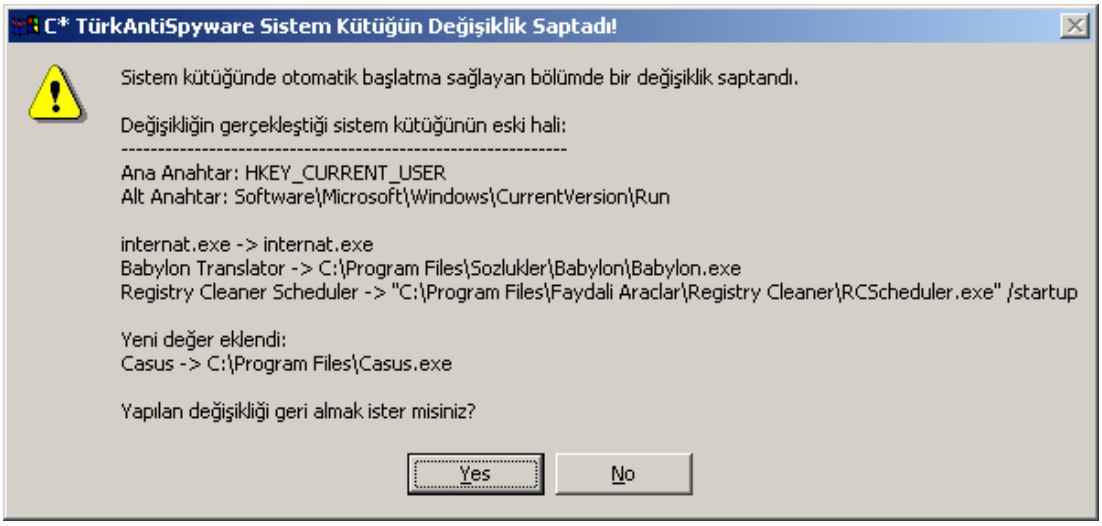


Şekil 8.4. Güvenli klavye ve dinleme modunun devre dışı bırakılması

Güvenli klavye ve fare modu devre dışı bırakıldığında sistem tepsisindeki program simgesi, Şekil 8.4'de görüldüğü gibi program simgesi, renkli görünümden gri tonlu görünüme dönüşür.

8.3.2. Kütük otomatik başlatmalarını izle

Bu menü öğesi seçili olduğu zaman Bölüm 4.7'de "Casus Yazılımların Otomatik Başlatma Yöntemleri" başlığında bahsedilen programların, işletim sistemi açılırken otomatik olarak başlatmak amacıyla kendilerini yazdığı özel alanları gerçek zamanlı olarak takip etmektedir. Bu alanlarda ekleme, çıkarma ve değişiklikler oluşur oluşmaz Şekil 8.5'de gösterildiği gibi kullanıcı bilgilendirilmektedir. Yapılan bu değişiklikler istenirse tekrar değişiklikten önceki duruma döndürülebilmektedir.

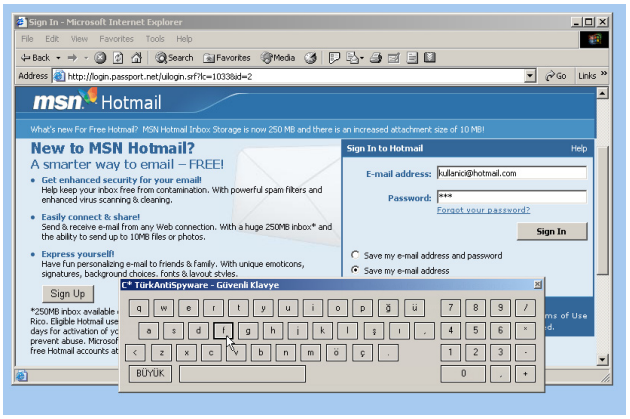


Şekil 8.5. Sistem kütüğü ile otomatik başlatma öğelerinin gerçek zamanlı izlenmesi

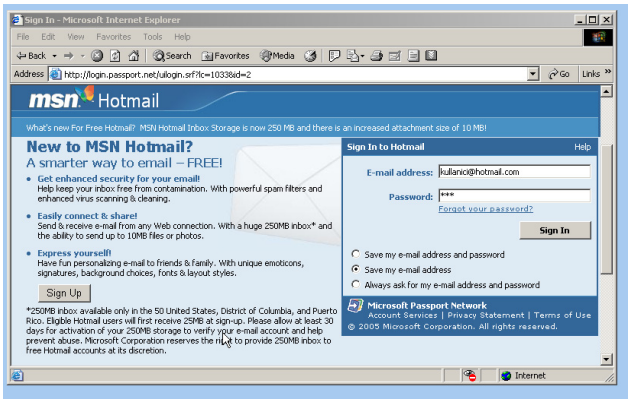
8.3.3. Güvenli klavye

TürkAntiSpyware klavye dinleme önleme sisteminin getirmiş olduğu yeniliklerden biri de güvenli klavyedir. Bu tez çalışması için incelenen tüm sanal klavyelerden farklı bir işleve sahip olan bir sistem geliştirilmiştir. Bu sistemde, donanım klavye dinleme dahil klavye dinleyen "tüm" sistemler atlatıldığı gibi; görsel izleme ile fare tıklama görüntülerini veya periyodik ekran görüntülerini alan klavye dinleme sistemlerinin de bilgi elde etmesi önlenebilmektedir. Şekil 8.6 (a)'da örnek bir

kullanıma ait gösterilen görüntü, kullanıcının kendi ekranında gördüğü görüntüdür. Şekil 8.6 (b)'de gösterilen görüntü ise programların ekran görüntüsünü alırken elde edilen resimdir. Çoğu görsel izleme yapan klavye dinleme sistemleri fare işaretçisini çektikleri görüntü de bulundurmadıklarından Şekil 8.6 (b)'de bulunan fare işaretçisi görüntüsü bile gözükmemektedir. Bu resmi elde eden kişi, kullanıcının güvenli klavyeden girdiği tuşu asla öğrenemeyecektir. Hatta bir sanal klavyenin kullanıldığını bile anlamayacaktır. Bu özellik ile TürkAntiSpyware'in klavye dinleme sistemlerine karşı sağladığı koruma en yukarı seviyeye getirilmiştir. Türkçe karakter desteğinin de bulunduğu TürkAntiSpyware Güvenli Klavye'si, özellikle Bölüm 5.7.2'de aktarılan İnternet bankacılığı giriş sayfalarında var olan güvenlik açıklarını en düşük seviyeye indirebileceği düşünülmektedir.



(a) Kullanıcının gördüğü ekran

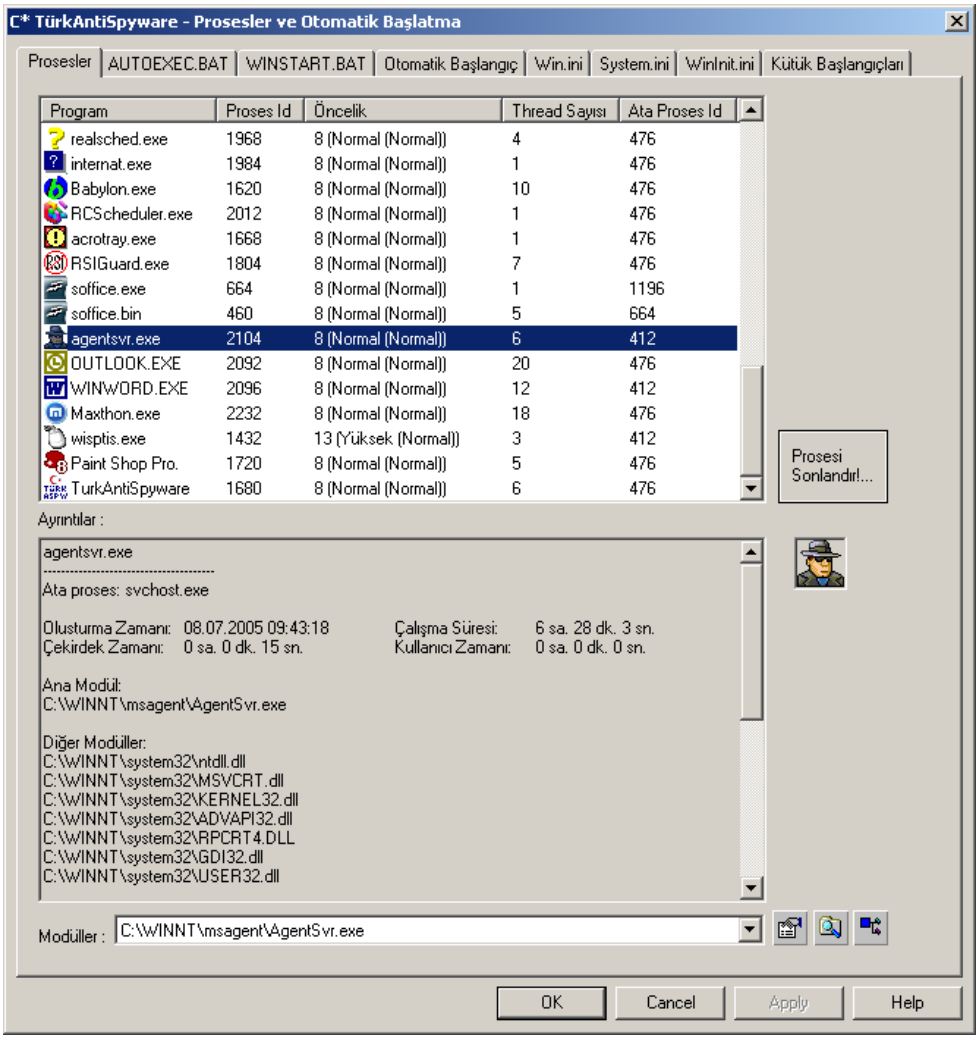


(b) Casus programların aldıkları görüntü

Şekil 8.6. TürkAntiSpyware Güvenli Klavye kullanımı

8.3.4. Prosesler ve otomatik başlatma

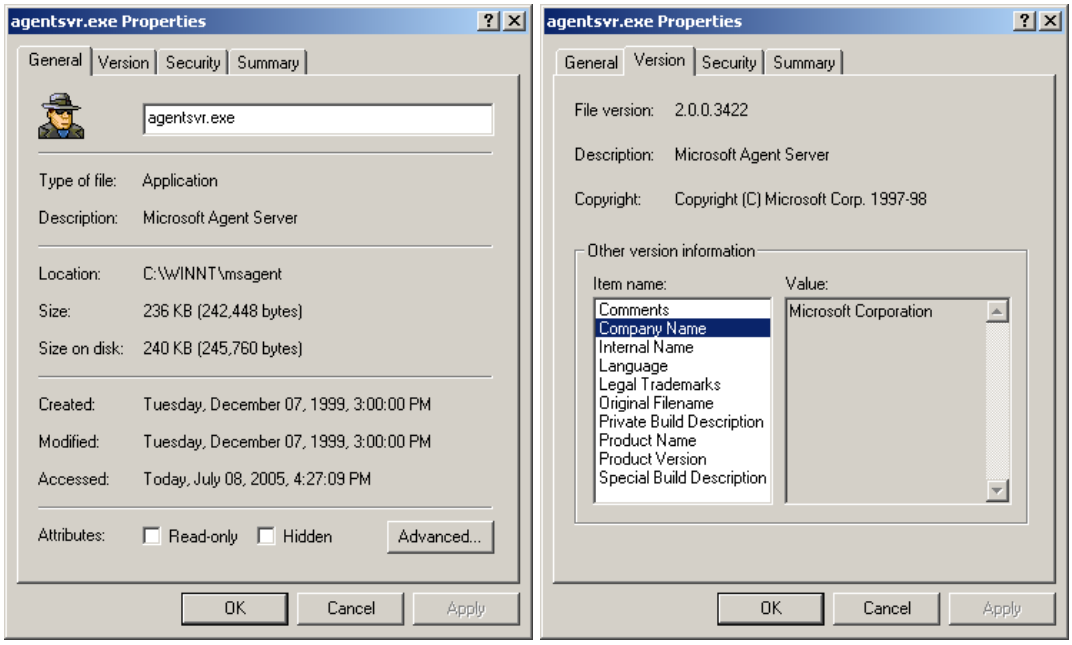
Prosesler ve Otomatik başlatma menüsü ile gösterilen diyalog kutusu, Şekil 8.7'de bir örneği gösterildiği gibi sistemde o an çalışmakta olan prosesler hakkında ayrıntılı bilgi almayı sağlar ve casus yazılımlarla beraber klavye dinleme sistemlerinin de kendilerini otomatik bir şekilde işletim sisteminin açılışıyla başlatmak amacıyla kullanabilecekleri sistem kütüğü alanlarını ve içerdikleri değerleri göstermektedir.



Şekil 8.7. Prosesler ve Otomatik Başlatma – Prosesler sekmesi

Şekil 8.7'de örnek ekran görüntüsü verilen Prosesler sekmesinde, çalışan programların, adları, proses numaraları, öncelik değerleri, sahip oldukları iş parçacığı sayıları ve prosesi oluşturan ata prosesin proses numaraları listelenmektedir.

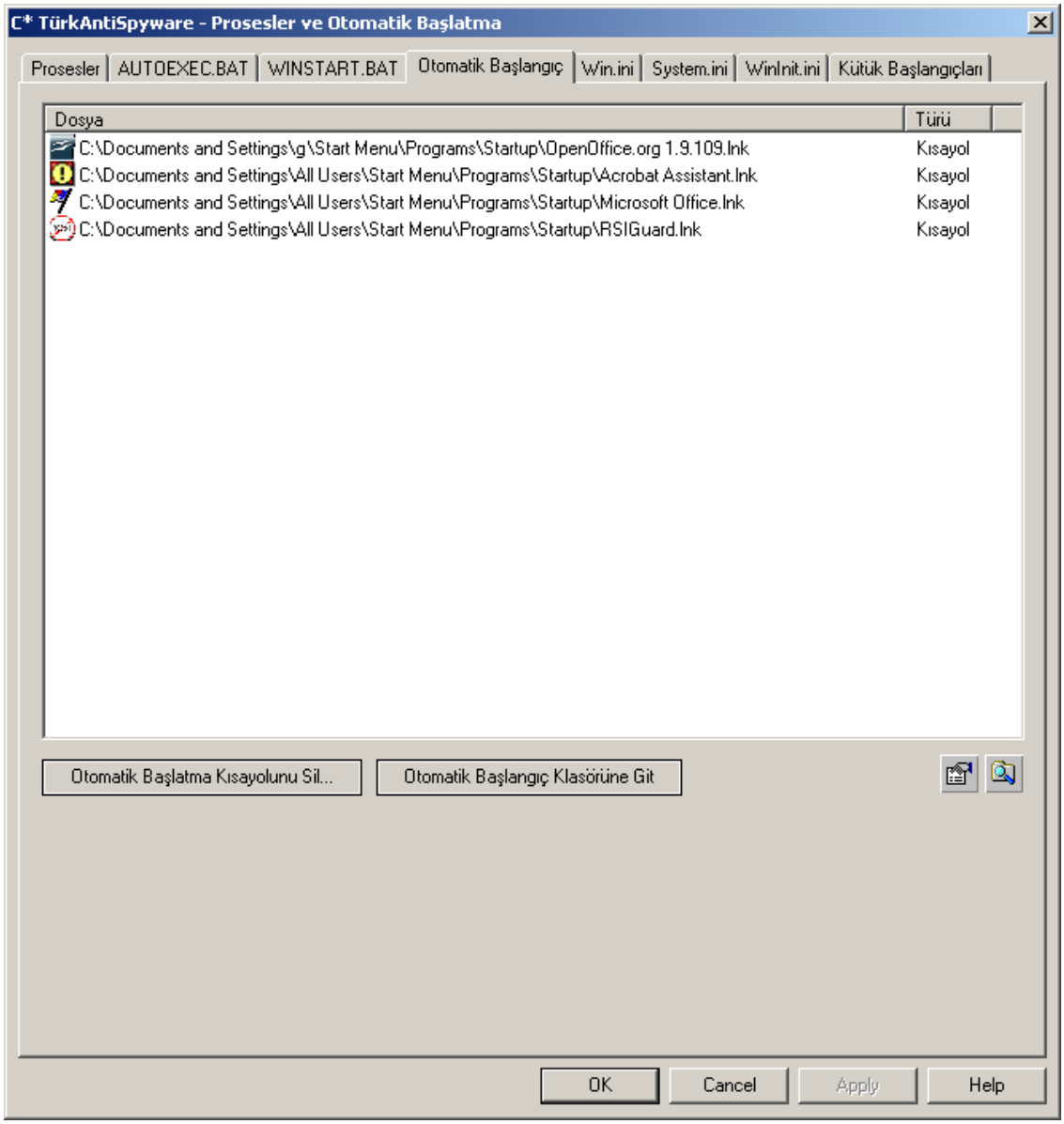
Windows Görev Yöneticisi'nden farklı olarak bu listede programların varsa simgeleri de gösterilmektedir. Bu listenin bir başka özelliği ise kendini Windows Görev Yöneticisi'nden saklamaya çalışan proseslerin burada görülebilmesidir. Listede seçilen prosese ait ayrıntılı bilgiler görülebilmektedir. Gerek ana program gerekse programın kullandığı modüllerin özellikleri, Şekil 8.8'de örnek ekran görüntülerinin verildiği gibi, Windows işletim sistemi dosya özellikleri (File | Properties) olarak gösterilebilmekte; ilgili modülün bulunduğu klasör Windows Gezgini ile açılabilmekte ve modülün bağlılıkları gösterilmektedir.



(a) Genel sekmesi (b) Sürüm sekmesi

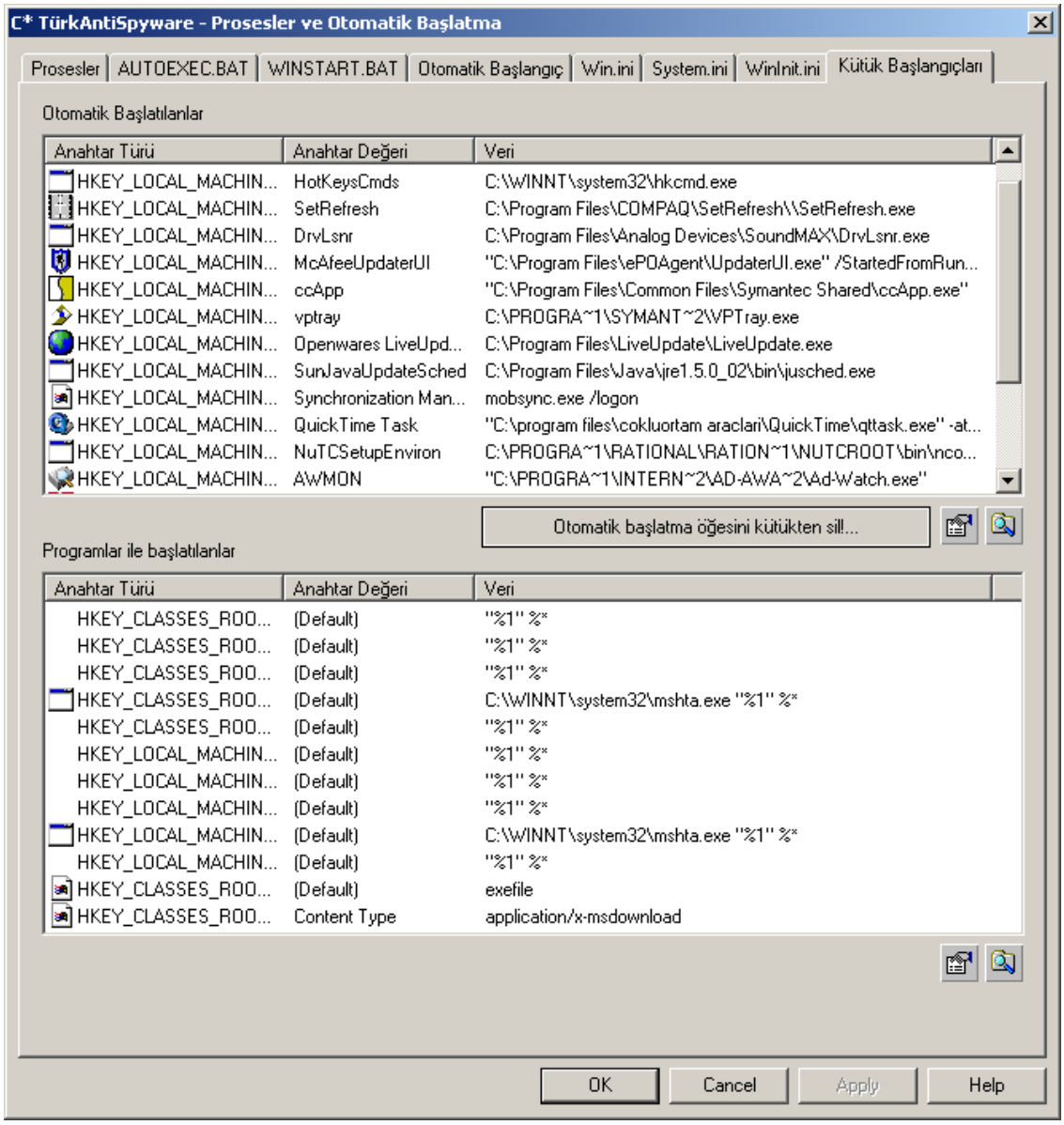
Şekil 8.8. Program özellikleri

Şekil 8.9'da bir örneği gösterilen Otomatik Başlangıç sekmesinde Windows otomatik başlangıç klasöründe hem geçerli kullanıcı hem de bütün kullanıcılar için Windows otomatik klasöründe yer alan kısayollar listelenmektedir. Seçilen kısayolu silerek bir daha otomatik başlaması engellenebilmektedir.



Şekil 8.9. Prosesler ve Otomatik Başlatma – Otomatik Başlangıç sekmesi

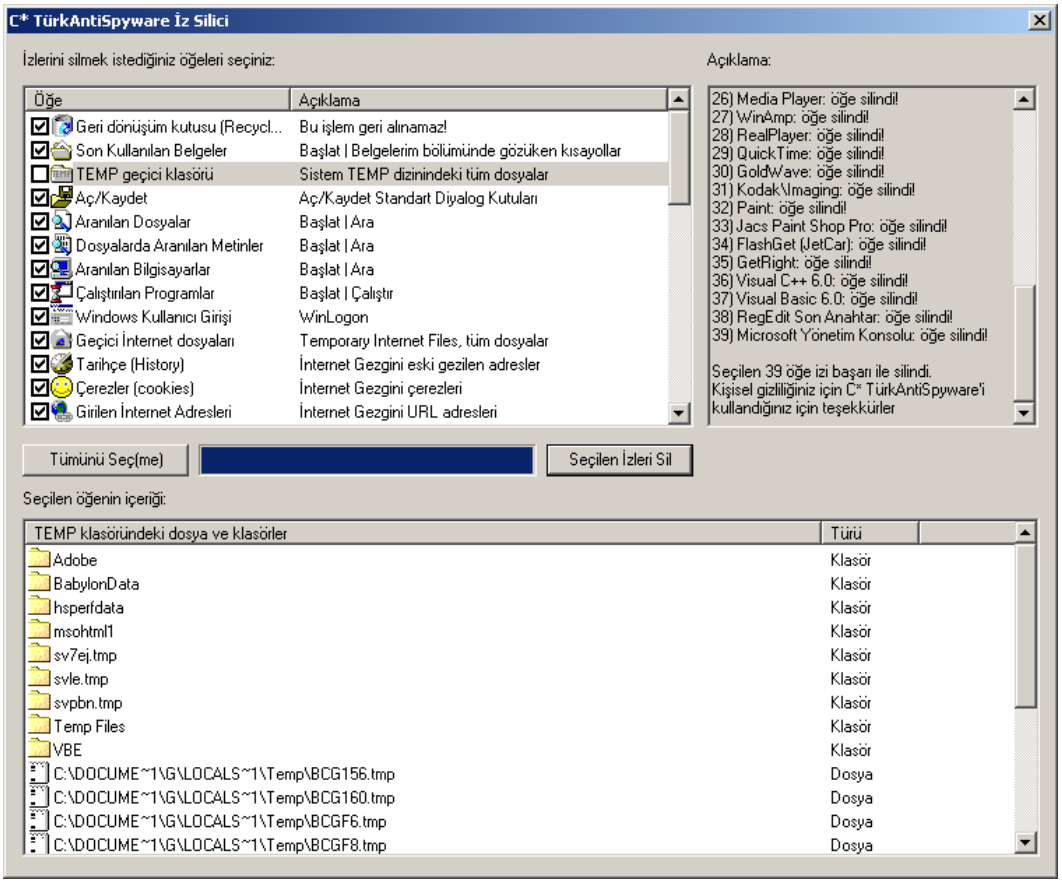
Şekil 8.10'da örnek ekran görüntüsü verilen Kütük Başlangıçları sekmesinde, Windows sistem kütüğünde otomatik program başlatmak için kullanılan anahtarların hepsini toplu olarak görmek ve listede yer alan programlara ait bilgi alabilmek mümkündür. Yine seçilen öğe bu listeden silinerek programın otomatik başlatılması önlenebilmektedir.



Şekil 8.10. Prosesler ve Otomatik Başlatma – Kütük Başlangıçları sekmesi

8.3.5. İz silici

Şekil 8.11'de gösterilen İz Silici sekmesinde, bilgisayar kullanımı sırasında tutulan ve daha sonra kişinin bilgisayarda yaptığı çalışmalar, çeşitli programlar ile eriştiği son dosyalar ve İnternet kullanımı ile ilgili bilgileri açığa çıkartabilecek öğelerin görünmesi ve silinmesi sağlanabilmektedir.



Şekil 8.11. İz Silici ekranı

TürkAntiSpyware programı ile,

- Geri dönüşüm kutusu (recycle-bin)
- Son kullanılan belgeler (Start | Documents, Başlat | Belgeler)
- TEMP geçici klasörü
- Aç/Kaydet standart diyalog kutularında dosya ismi bölümünde gözüken öğeler
- Bilgisayarda aranılan dosyalar (Start | Search | For Files and Folders, Başlat | Ara | Dosya ve Klasörler)
- Aranılan dosyalarda geçen metinler
- Aranılan bilgisayarlar
- Çalıştırılan programlar (Start | Run, Başlat | Çalıştır)
- Windows kullanıcı girişinde gözükecek kullanıcı adı

- Geçici İnternet dosyaları (İnternet Gezgini için)
- İnternet tarihçesi (history) (İnternet Gezgini için)
- Çerezler (cookies) (İnternet Gezgini için)
- Girilen İnternet adresleri (İnternet Gezgini için)
- Otomatik tamamlama (Auto-complete) (İnternet Gezgini için)
- IntelliForm girişleri (İnternet Gezgini için)
- Ağ komşulukları
- WordPad, Microsoft Office, Word, Excel, PowerPoint, Access, Microsoft Reader, Adobe Acrobat ofis programları
- WinZip, WinRar sıkıştırma programları
- Media Player, WinAmp, RealPlayer, QuickTime, GoldWave ses ve video programları
- Kodak\Imaging, Paint, Jacs Paint Shop Pro grafik düzenleme programları
- FlashGet, GetRight dosya indirme programları
- Microsoft Visual C++ 6.0 ve Visual Basic 6.0 programlama yazılımlarının son kullandığı dosyalar
- RegEdit ile erişilen son anahtar
- Microsoft Yönetim Konsolunda erişilen son araçlar

görülebilmekte ve silinebilmektedir. Bu özellik ile yazılım bir kişisel gizlilik aracı olarak da kullanılabilmektedir. Bu aracın, diğer kişisel gizlilik ve iz silme araçlarına göre oldukça ayrıntılı bir şekilde tasarlanıp, gerçekleştirildiği; izleri silinmek istenen öğeler hakkında daha ayrıntılı bilgi verdiğini vurgulamakta fayda vardır.

8.3.6. Makineyi kilitle

Tek bir diskete sığabilen klavye dinleme sistemlerinin bir bilgisayara kurulması, bilgisayar bir süreliğine terk edildiğinde rahatlıkla gerçekleştirilebilmektedir. Çoğu kullanıcı bunun için kullanılabilecek tedbirleri ya bilmemektedir ya da bu tedbirleri almakta üşengeçlik göstermektedir. Bu sebepten dolayı TürkAntiSpyware yazılımına tek tıklama ile bir makinenin kilitlenmesini sağlayan bir menü eklenmiştir. Bu menü

kullanıldığında makine anında kilitlenmekte ve sonra, makine sadece şifre girilince tekrar kullanılabilmektedir.

Bütün bu özellikleri ile TürkAntiSpyware yazılımı klavye dinleme sistemlerine karşı etkili olmak için geliştirilen ileri önlemlerle ve bilgi ve bilgisayar güvenliğine ve kişisel gizliliğe yönelik sağladığı kullanıcı dostu araçları ile örnek bir klavye dinleme önleme sistemidir. Gerçekleştirilen bu yazılımın gelecekte yapılabilecek bir çok çalışmaya temel teşkil edebileceği; gelişen teknolojiye uygun olarak yeni yaklaşımların ve özelliklerin sisteme eklenebileceğini belirtmekte fayda vardır. Bu yazılımın ülkemizde var olan klavye dinleme sistemlerine yönelik açıkları kapatabileceği değerlendirilmektedir.

9. SONUÇ VE ÖNERİLER

Bilginin bir varlık olarak değerini özümseyen ve bilgi ve bilgisayar teknolojileri üretimine ve bu teknolojilerin güvenliğine önem veren toplum ve devletlerin, kendi geleceklerini şekillendireceği; geride kalanların ise oldukça önemli ve hayati sorunlar yaşayacağı çok açıktır. Bu açıdan bilginin kapsamı ve önemi herkes tarafından bilinmelidir. Bu kadar önemli olan bir varlığın korunmasına yönelik olarak yapılacak araştırmalar ve geliştirilecek olan yeni yaklaşımlar büyük önem arz etmektedir.

Bilgisayar sistemlerindeki gelişmeler ve özellikle İnternet'in her alanda yoğun bir şekilde kullanılması ile son yıllarda bilgi ve bilgisayar güvenliğini zaafa uğratmaya hatta yıkmaya çalışan, kişisel gizliliği zedeleyip kişi, kurum ve kuruluşların maddi ve manevi zararlara uğramasına sebep olan kötücül ve casus yazılımlar gözden geçirildiğinde, bu yazılımların sanılanın aksine çok yaygın olduğu ve bir çok çeşidinin olduğu saptanmıştır.

Kötücül ve casus yazılımların ve verebilecekleri zararların boyutlarının iyi anlaşılmamış olması ve bu konuda yasal çerçevenin de özellikle ülkemizde oturmamış olmasının bilgi ve bilgisayar güvenliğinde önemli bir tehdidin varlığını sürdürmesine neden olmaktadır.

Bilgi ve bilgisayar güvenliği konusunda, literatürdeki bilgisayar sistem saldırıları incelendiğinde; saldırıların oldukça geniş bir yelpazede gerçekleştirildiği görülmüştür. Saldırı türlerinin sıkı bir şekilde takip edilmesi, kullandıkları yöntemlerin saptanması, saldırılar hakkında bilgi kaynaklarının ve bu konuda yapılan araştırmaların takip edilmesi, her bir saldırıya karşı alınabilecek etkin önlemlerin kısa sürede belirlenmesi ve belirlenen tedbirlerin uygulamasının sürekli bir şekilde gözetlenip uygulama neticelerinin değerlendirilmesi ve değerlendirme sonuçları ve saldırı türünün takip edilen değişim ve gelişimine göre gerekli düzenleme ve güncellemelerin yapılması gereklidir.

Casus yazılımların sistemlere bulaşmak için bir çok yöntem kullandığı ve bu yöntemlerin çoğunun, dikkatsiz ve bilinçsiz kullanıcıları hedeflediği belirlenmiştir. Bu çalışmada araştırılıp sunulan, klavye dinleme sistemleri dahil iyi bilinen kırk altı adet kötücül yazılımın, her birinde kullanılan yöntemler genel hatları ile incelenmiştir. Casus yazılımlara karşı kullanıcının alabileceği tedbirlerin neler olabileceği araştırılmış ve bu yazılımlara karşı daha etkin korumayı sağlamak amacıyla geliştirilen casus savar yazılımlar değerlendirilmiştir. Çok boyutlu olarak, casus yazılımların en tehlikeli türlerinden biri olan klavye dinleme ve önleme sistemlerinin incelenmesi, analizi, tasarımı ve gerçekleştirilmesi üzerine ülkemizde ilk defa kapsamlı bir tez çalışması başarıyla sunulmuştur.

Bu sistemlerin incelenmesi sırasında saptanan en önemli bulgulardan biri, klavye dinleme sistemleri hakkında her düzeyde kullanıcının, bilgisayar sistemi yöneticilerinin ve kurum ve kuruluş çalışanlarının çoğunluğunun, yeterli derecede bir bilgiye sahip olmadıklarıdır. Bu konuda kulaktan dolma bilgiye sahip olan kişilerin çoğunluğu, klavye dinleme sistemlerini (keylogger), isminin yanlış çağrışım yapması nedeniyle, sadece klavyeden girilen bilgilerin gizlice elde edildiği yazılım şeklinde değerlendirmektedir. Fakat günümüz klavye dinleme sistemleri bir bilgisayarda gerçekleştirilen hemen hemen bütün faaliyetleri gizlice izleyip bunları başka kişilere iletebilen, son derece tehlikeli casus yazılımlardır. Bu sebepten dolayı, bazı kaynaklarda daha doğru bir şekilde, faaliyet izleme araçları (activity monitoring tool) olarak adlandırılmaktadır. Klavye dinleme sistemleri konusunda yapılan literatür araştırmalarında yurt dışında bu konuda sunulmuş olan yayınların da çok az olduğu tespit edilmiştir. Klavye dinleme sistemleri, çoğu çalışmada bir iki cümle ile geçiştirilmektedir. Bu açıdan, akademik çalışmalardan ziyade bilgi güvenliği konusunda çalışan güvenlik firmalarının İnternet sayfalarında sunulan en güncel bilgi ve makalelerden faydalanmak zorunda kalınmıştır.

Türkiye'de bulunan üniversitelerde, bilgi ve bilgisayar güvenliği, casus yazılımlar ve casus savar yazılımlar konusunda yapılan araştırma ve çalışmaların yok denecek kadar az olduğu görülmüştür. Klavye dinleme ve önleme sistemleri hakkında ise, şu an için bir çalışmaya rastlanmamıştır. Bu çalışmanın bu konuda yapılan ilk yüksek

lisans tez çalışması olduğu ve bu çalışmanın ileride yapılacak çalışmalara temel teşkil edebileceği değerlendirilmektedir.

Donanım ve yazılım klavye dinleme sistemlerinin kullandıkları yöntemlerin geniş bir şekilde incelendiği bu çalışmada, yazılım klavye dinleme sistemlerinin en çok kullandıkları tekniğin Windows işletim sisteminin sağladığı çengeller olduğu saptanmıştır. Diğer yöntemlerden çekirdek tabanlı klavye süzgeç sürücüsü yönteminin hem gerçekleştirilmesinin hem de saptanmasının oldukça zor olduğu görülmüştür. Mevcut klavye dinleme sistemleri, her ne kadar Windows işletim sistemlerinde yoğunlaşsa da; UNIX işletim sistemi ve türevlerinde ve MacOS işletim sisteminde de yazılım klavye dinleme sistemleri çok rahat bir şekilde tasarlanabilmektedir. Bu sistemleri tercih eden kesimlerin, mesela reklam ve güzel sanatlar ile uğraşan ve MacOS işletim sistemini tercih eden profesyonellerin, bu konuda yeterli seviyede bir duyarlılığa sahip olduğu da düşünülmemektedir.

Klavye dinleme sistemlerinin yetenekleri arasında fare tıklamalarının dinlenmesi, ekran görüntülerinin alınmasıyla görsel gözetleme yapma, İnternet'te gezilen adreslerin tutulması, yapılan her türlü mesajlaşmanın elde edilmesi, bilgisayarda çalıştırılan programların ve erişilen ve yazıcı çıktısı alınan belgelerin belirlenmesi gibi sayısız yetenekler sayılabilir. Bu bilgiler son derece kritik bilgilerdir. Bu tür bilgileri elde eden kötü niyetli kişilerin, bilgisayar kullanıcılarını oldukça büyük zararlara uğratabileceği değerlendirilmektedir.

Klavye dinleme sistemlerinin casusluk ve gizli bilgilere erişmeye neden olması dışında başka önemli kullanım alanları da bu çalışma ile gözler önüne serilmiştir. İnternet üzerinde çevrimiçi faaliyet gösteren bankaların İnternet şubelerinin giriş sayfalarında, müşterilerini doğrulatmak amacıyla sorulan kullanıcı adı, hesap numarası ve şifre gibi bilgiler, bankanın sağladığı güvenlik altyapısı ne durumda olursa olsun klavye dinleme sistemleri tarafından elde edilebilmektedir. Bu tez çalışması için özel olarak tasarlanan ve gerçekleştirilen klavye dinleme sistemi TürkSpyware ile bizzat bütün bankaların giriş sayfaları tek tek test edilmiş ve bir kaç banka hariç bankaların tamamında gizli giriş bilgilerin rahatlıkla elde edildiği

saptanmıştır. Klavye dinleme sistemlerinden haberdar olan ve bunları atlatmak için sanal klavye imkanı sunan bankaların bile, ne yazık ki TürkSpyware gibi görsel gözetleme yapan klavye dinleme sistemlerinin bu bilgileri almasını engelleyemediği görülmüştür. Bankaların müşterilerini zarara uğratmadan, bu konuda gereken önlemleri almaları gerektiği; alınması gereken önlemler konusunda ise bu tez çalışmasının rehberlik edebileceği değerlendirilmektedir.

Klavye dinleme sistemlerinin zararlı kullanım alanları dışında son derece faydalı olabilecek kullanım alanları da bu çalışmada sunulmuştur. Bunlar arasında işyeri gözetleme ve çocukların ve öğrencilerin bilgisayar ve İnternet kullanırken güvenliklerinin temini, en önemli ve faydalı kullanım alanlarının başında gelmektedir.

İşyerinde bilgisayar ve İnternet kullanımının verimsizliği, bu tez çalışmasında istatistiklerle gözler önüne serilmiş ve işverenlerin ve yöneticilerin, çalışanların İnternet ve bilgisayar kullanımlarını yeterli seviyede değerlendiremediği belirlenmiştir. Bu çalışmada sunulan TürkSpyware klavye dinleme sistemi, çalışanların makinelerine, bilgileri dahilinde veya bilgileri olmadan kurulabilir ve çalışanın işyerinde bilgisayar kullanırken gerçekleştirdiği faaliyetler izlenip, bu bilgiler değerlendirilebilir. Bu şekilde işyeri verimliliği artabilecek ve iş ile alakası olmayan kullanım sebebi ile oluşan büyük maliyetlerin önüne geçilebilecektir. Klavye dinleme sistemlerinin bu şekilde kullanımından bir çok işverenin haberdar olmadığı ve kamuda bu tür yazılımların kullanımının büyük bir verimlilik artışı sağlayabileceği değerlendirilmektedir.

Bu çalışmada elde edilen bir başka önemli sonuç, klavye dinleme sistemlerinin çocukların bilgisayar ve İnternet kullanım güvenliklerinin sağlanmasında en önemli araç alarak kullanılabileceğidir. Ebeveynlerin, çocuklarının bilgisayar kullanımlarını sürekli ve etkin bir şekilde kendi başlarına takip etmesi nerdeyse imkansızdır. Bu çalışmada sunulan klavye dinleme sistemi, bu etkin izlemeyi ebeveynler yerine rahatlıkla yapabilir. Bu sayede oluşabilecek bir çok kötü olay önlenmiş; çocukların bilgisayar ve İnternet'ten olumlu bir şekilde yararlanması sağlanmış olacaktır. Yine

ebeveynlerin de klavye dinleme sistemlerinin böyle hayati bir kullanımından haberdar olmadığı düşünülmektedir.

Bu tür önemli kullanım alanları dışında, öğrenci bilgisayar laboratuarlarının izlenmesi ve kişilerin kendi kendilerinin bilgisayar faaliyetlerini kaydetmesi gibi, kullanım alanları da bulunmaktadır. Öğrenci laboratuarlarında yapılan gözetleme ile öğrencilerin bilgisayar kullanımındaki eksiklikler tespit edilerek, daha etkin bir eğitimin verilmesi gibi katkılar sağlanabilir.

Bu çalışmanın somut getirilerinden bir diğeri ise, klavye dinleme sistemi olarak tasarlanan ve gerçekleştirilen TürkSpyware yazılımıdır. Klavye dinleme sistemlerinin yeteneklerinin daha iyi kavranması ve zararlı kullanımlarının önlenmesinin nasıl sağlanacağının daha etkin bir şekilde belirlenmesi için geliştirilen bu sistemin, piyasada mevcut bulunan yüzlerce klavye dinleme sistemi arasında, oldukça ileri yeteneklere sahip olduğu ve Türkiye'de bu kapsamda gerçekleştirilen ilk klavye dinleme sistemi olduğu görülmüştür. Bazı özelliklerinin ise şu an itibariyle hiç bir klavye dinleme sistemi veya faaliyet izleme aracında bulunmadığı tespit edilmiştir.

Oldukça faydalı kullanım olanakları dışında, kötü niyetli bir şekilde kullanılabilecek klavye dinleme sistemlerinin, sisteme girişinin veya bulaşmasının önlenmesi, sistemden atılmasını ya da işlev görmemesinin sağlanması da oldukça önemli olduğundan, bu çalışmada, bu tür özellikleri destekleyen klavye dinleme önleme sistemlerinin nasıl geliştirilebileceği araştırılmıştır. Casus sava yazılımların özel olarak klavye dinleme sistemlerine karşı yeterli önlemleri almadığı saptanmıştır. Bu çalışmada, piyasada çok az sayıda bulunan ve sadece klavye dinlemeyi önlemek amacıyla geliştirilen sistemlerin özellikleri incelenmiş ve sunulmuştur. Bu yazılımların TürkSpyware gibi çeşitli klavye dinleme sistemlerine karşı yeterli seviyede güvenlik sağlamadığı sonucuna varılmıştır.

Klavye dinleme önleme sistemleri hakkında yapılan bu analiz ve değerlendirmeler sonucunda, klavye ve fare dinlemeyi önleyecek bir sistem olan TürkAntiSpyware

yazılımı geliştirilmiştir. Klavye dinleme sistemlerinin çoğuna karşı ileri seviyede güvenlik sağlamasının yanında; diğer türde casus yazılımların sisteme bulaşmalarını da engelleyebilecek ve kişisel gizliliği temin edecek bazı kullanışlı araçlar da Türkçe kullanıcı arabirimi ile geliştirilen yazılıma dahil edilmiştir.

İleri seviyede güvenlik sistemi sağlayabilmek için kendi güvenlik sistemlerimizi oluşturmamız şarttır. Gerçekleştirilen TürkAntiSpyware yazılım çalışmasıyla, klavye dinleme yöntemi ve fare dinleme yoluyla bilgi kaçıran klavye dinleme sistemlerine karşı güvenli bir bilgi girişi modu sağlanmaktadır. TürkAntiSpyware, mevcut klavye dinleme önleme sistemlerinden farklı olarak yazılım ve donanım klavye dinleme sistem türleri ve yöntemlerine karşı ileri derecede güvenlik sağlayacak "güvenli klavye" adında bir çözüm de sunmaktadır. Bu yaklaşım ile, özellikle, banka İnternet giriş sayfaları gibi önemli bilgi girişleri sırasında girilen bilginin elde edilmesi zorlaştırılabilmektedir. Bu açıdan bakıldığında TürkAntiSpyware'in diğer klavye dinleme önleme sistemlerine karşı ayrıcalıklı bir özelliğe sahip olduğu düşünülmektedir. Geliştirilen bu yazılımın, özellikle, bankalar tarafından müşterilerinin zarar görmesini önlemek amacıyla kullanılması için önerilebilecek türde bir yazılım olmaya aday olduğu değerlendirilmektedir.

Bu tez çalışması genel olarak değerlendirildiğinde;

- Bilgi ve bilgisayar güvenliği kapsamında, çoğunlukla göz ardı edilen insan-makine arayüzünde gerçekleştirilen en önemli saldırı türlerinden biri olan klavye dinleme sistemleri bütün yönleriyle değerlendirilmiş; gerçekleştirilen klavye dinleme sistemi TürkSpyware ve klavye dinleme önleme sistemi TürkAntiSpyware ile konu tüm yönleriyle gözler önüne serilmeye çalışılmıştır. Bu tez çalışmasının bilgi ve bilgisayar güvenliği ve klavye dinleme sistemleri konusunda var olan eksikliği giderip, bu konuda varılan sonuçların ve sunulan önerilerin hayata geçirilmesi ile ileride yapılacak çalışmalara örnek ve temel oluşturacağı değerlendirilmektedir.

- Mevcut klavye dinleme ve önleme sistemleri her açıdan incelenmiş; gerçekleştirilen muhtemel saldırıların analizi ve bu saldırılar sonucunda oluşabilecek zararlar gözden geçirilmiş; karşılaşılan korkunç tablonun ülkemiz bilgisayar teknolojileri kullanıcılarının başlarına gelmemesi ve bu tür sistemlerden mümkün olduğunca az etkilenilmesi için somut ve kapsamlı çözüm önerileri sunulmuştur. Klavye dinleme sistemlerinin zararlı yönlerinin yanı sıra oldukça faydalı kullanım alanlarının da ayrıntıları ile gözler önüne serildiği bu çalışmada, bu amaçların hepsini gerçekleştirmeye yönelik TürkSpyware ve TürkAntiSpyware yazılımları geliştirilmiş ve farklı seviyedeki isteklere cevap verebilecek bir yazılım oluşturulmaya çalışılmıştır.

- Bu yazılımların gerçekleştirilmesindeki temel amaç, Türk kamuoyunun, güvenlik birimlerinin, üniversitelerin, bilgisayar mühendislerinin, ebeveynlerinin, işverenlerin, çalışanların velhasıl bütün kullanıcıların, bilgi ve bilgisayar güvenliği konusunda karşılaşabilecekleri tehlikelere dikkatlerini çekmek ve kişisel gizlilik ve bilgi güvenliği konusunda bilgilendirme ve bilinçlendirme çalışmalarına destek olabilmektir.

- Bu çalışma sırasında bir çok güçlükle karşılaşılmıştır. Öncelikle klavye dinleme sistemleri konusunda bir tez çalışmasının olmaması, insanlar arasında böyle bir çalışmaya ihtiyaç da bulunmadığı şeklinde yanlış bir kanı doğurduğu gözlemlenmiştir. Bu konu hakkında, kulaktan dolma bilgi sahibi olan kişilerin tez konusu olarak seçilebilecek rahat bir alan nitelemeleri başlangıçta olumsuz bir motivasyona sebep olmuştur. Fakat konu bütün kapsamı ile değerlendirilip, olması gereken çerçeveye oturtulunca ve çalışmanın ana hatları ortaya çıkınca, sanılanın aksine konunun oldukça kapsamlı, önemli kavram ve yeni teknolojilerle yakından ilişkili, çok boyutlu ve devingen bir konu olduğu fark edilmiştir. Ele alınan ilişkili her konunun, özellikle ülkemizde çoğunlukla bilinmemesi ya da çok nadir ele alınmış olması, hayret verici bir durum olarak değerlendirilmiş ve bu konular olabildiğince net bir şekilde, önemli yönleri ile; çoğu durumda ilk kez aktarılmaya çalışılmıştır. Özellikle klavye dinleme sistemlerinin de içinde ve

etkileşimde bulunduğu kötücül yazılımlar araştırılırken, incelenen türlerin, çoğu yabancı kaynaklarda sıralandığı gibi az sayıda değil, elli kadar temel türde bulunması, bütün bu türlerin bir araya getirilmesinde ve türler hakkında ayrıntılı bilgi alınmasını zorlaştırmıştır.

- Bu tez çalışmasında açıklanan kötücül yazılımların İngilizce adları yanı sıra, bunlara karşılık olarak kullanılabilecek özgün Türkçe ifadeler belirlenip kullanılmıştır.

- Tez çalışması sırasında yeterli yerli ve yabancı akademik çalışmaya rastlanmaması karşılaşılan en önemli güçlüklerden biridir. Konunun dinamik bir yapı taşıması sebebi ile İnternet üzerinde çok sayıda kaynak araştırılmış ve bunlar arasında en doğru ve güncel bilgi içeren kaynaklar değerlendirmeye alınmıştır. Yine yararlanılan kaynakların hemen hemen tamamının İngilizce olması, belirli bir İngilizce seviyesine sahip olunduğundan her ne kadar aşırı zorluk çıkarmasa da bunların daha doğru değerlendirilmesi için biraz daha fazla çaba harcandığı da bir gerçektir.

- Ülkemiz üniversitelerinde yapılan kapsamlı tez taraması oldukça uzun sürmüş; buna rağmen, klavye dinleme ve önleme sistemleri hakkında hiç bir çalışmaya rastlanmamış olması, bu tez çalışmasına, taşıması gerektiği kapsam ve nitelik bakımından daha da büyük bir sorumluluk yüklemiş ve bu çerçevede bir tez çalışması sunulmaya çalışılmıştır.

- Araştırma ve inceleme alanındaki zorluklar dışında, bizzat klavye dinleme ve önleme sistemlerinin tasarlanması ve geliştirilmesinde de bir çok güçlükle karşılaşılmıştır. Klavye dinleme ve önleme sistemlerinin özellikleri icabı, oldukça ileri seviyede programlamaya ihtiyaç duyulmuştur. Bir, iki cümle ile ifade edilebilen bir yeteneğin, gerçekleştirilen klavye dinleme ve önleme sistemine bütünleştirilmesi, bazen haftalar süren araştırma ve kodlama gerektirmiştir. Bunun için sayısız testler yapılmış ve binlerce satır kod yazılmıştır. Bu yazılımların ülkemizde gerçekleştirilen ilk klavye dinleme ve

önleme sistemi olması taşınan sorumluluğu daha da artırmış; sonuçta çıkan ürünün kapsamından ve kalitesinden ödün verilmemeye çalışılmıştır.

- Bütün bu zorluklara rağmen, sonuç itibariyle gerek kişisel gerek ülkemiz açısından çok büyük kazanımlar elde edildiği değerlendirilmektedir. Tamamen güncel bir konuda, bilimsel bir çalışma yapmanın ve güçlükleri teker teker aşmanın getirileri yanında; ülkemiz bilgi ve bilgisayar güvenliğine yönelik kapsamlı bir çalışmanın sunulmasının konuya büyük bir katkı sağlayabileceği değerlendirilmektedir.

Bu tez çalışması sırasında elde edilen sonuç ve değerlendirmeler ışığında; bilgi ve bilgisayar güvenliği, kötücül, casus yazılımlar ve klavye dinleme ve önleme sistemleri hakkında aşağıdaki öneriler sunulmaktadır:

- Bilgi ve bilgisayar güvenliğine ülkemizde, devlet, üniversite, kurum ve kuruluşların gereken önemi vermesi için bu ve buna benzer çalışmaların sayısı arttırılmalıdır. Bilgi ve bilgisayar güvenliğine yönelik en önemli tehditlerden biri olan kötücül yazılımlar konusunda güncel gelişmeler dünya ile birlikte takip edilmeli; alınması gereken önlemler hakkında gerekli çalışmalar zaman kaybetmeden yerine getirilmelidir. Çok hızlı bir şekilde gerçekleşen yeni gelişmelerden, zamanında haberdar olmamanın ve bu gelişmelere karşı alınacak tedbirlerin doğru bir şekilde ve hızla uygulamamanın çok büyük zararlar oluşturabileceği ve bunun faturasının da yüksek olacağı unutulmamalıdır.

- Bilgi ve bilgisayar güvenliği ile ileride muhakkak yüzleşecek bilgisayar mühendislerinin bu konuda bilinçlendirilmesi çok önemli bir konudur. Bilgisayar mühendisliği lisans eğitiminde bilgi ve bilgisayar güvenliği konusunda öğrenciler mutlaka bilinçlendirilmeli ve mümkünse bu konuda zorunlu ya da seçmeli dersler açılmalıdır. Özellikle işletim sistemlerinde Windows çengel mekanizması gibi, klavye dinleme, faaliyet izleme ve diğer kötücül amaçlarla çalışan casus programların çalışma yöntemlerini ve bu

yöntemleri önlemeye yönelik içeriğe sahip eğitim faaliyetleri düzenlenmelidir.

- Kurum ve kuruluşlardaki güvenlik uzmanları, casus yazılımlar ve bunlara karşı alınabilecek tedbirler açısından sistemlerini düzenlemeli ve bilgisayar kullanıcılarını bu konuda eğitmelidir.

- Donanım ve yazılım klavye dinleme sistemlerine karşı, ülkemizdeki bütün bilgisayar kullanıcıları bilgilendirilmeli ve bilinçlendirilmelidir. Bu konuda özellikle yurt dışında çalışan ve yurt dışındaki şirketlerle münasebette olan kişilerin sahip oldukları bilginin başkaların eline geçmesini önleyecek şekilde yapılanmaları şarttır. Güvenli bilgi akışına yönelik bu tehdide karşı alınması gereken önlemlerin, tamamen kullanıcıların inisiyatifine bırakılmasından ziyade, bu çalışmada temel çatısıyla oluşturulan klavye dinleme önleme sistemi gibi yazılımlar geliştirilmeli ve bu yazılımların kullanılması teşvik edilmelidir.

- Ülkemizde İnternet üzerinde çevrimiçi faaliyet gösteren bankaların çoğu, klavye dinleme sistemlerine karşı kapsamlı bir şekilde önlem almalıdır. Yine e-ticaret yapmak isteyen siteler, bu tür casus yazılımlara karşı gerekli önlemleri almalı veyahut en azından bu konuda müşterilerini kendi önlemlerini almaları için uyarmalıdırlar. Bu konuda tek kullanımlık şifre, cep telefonu şifresi gibi yeni gelişmeler takip edilmelidir. Güvenli bilgi akışını sağlayacak e-imza gibi yeni yapılara geçiş süreci hızlandırılmalıdır.

- Klavye dinleme sistemlerinin oldukça faydalı bir şekilde kullanılabileceği alanlar, gerekli kişi ve kuruluşların bilgisine sunulmalıdır. Bu alanlardan özellikle işyeri gözetleme ve çocukların bilgi ve bilgisayar güvenliğinin sağlanması en kritik ve klavye dinleme sistemlerinin en doğru çözümü ürettiği iki alandır. Gerek işyeri gözetlemede gerekse çocukların güvenliğinde, bu çalışmada gerçekleştirilen ve oldukça kapsamlı özellikleri

olan klavye dinleme sistemi TürkSpyware, ülkemizde kolaylıkla kullanılabilecektir.

- Virüs korumasında ülkemizde var olan bilgi, tecrübe ve ürün geliştirme eksikliği, yeni gelişmekte olan ve oldukça büyük bir pazar payı olan casus savar yazılım konusunda da aynı akıbete uğramamalıdır. Bu amaçla casus savar yazılım geliştiren şirketlerin oluşturulması ve bu konuda dünya ile rekabet edecek yazılımların üretilmesi gereklidir.

- Ülkemizde bilgi ve bilgisayar güvenliği konusunda faaliyet göstermek isteyen ve gösteren firmaların bu tez çalışmasından faydalanabileceği bir çok konunun bulunduğu değerlendirilmektedir.

Sonuç olarak; klavye dinleme ve önleme sistemleri hakkında yapılan bu kapsamlı çalışmanın, getirdiği somut önerileri ve gerçekleştirilen yazılımları ile bilgi ve bilgisayar güvenliği ve klavye dinleme ve önleme sistemleri konularında var olan duyarlılığı ve bilgi seviyesini artırması; bu konuda yapılacak her türlü çalışmaya temel oluşturması; klavye dinleme sistemlerinin kötü kullanımlarından korunularak faydalı yönlerinden en yüksek verimin alınmasına katkılar sağlayacağı değerlendirilmektedir.

KAYNAKLAR

1. Nagurney, A., Dong, J. and Mokhtarian, P.L. "Multicriteria Network Equilibrium Modeling with Variable Weights for Decision-Making in the Information Age with Applications to Telecommuting and Teleshopping", ***Journal of Economic Dynamics & Control***, 1629-1650 (2002).

2. Subrahmanyam, K., Kraut, R. E., Greenfield, P. M., Gross, E. F., "The Impact of Home Computer Use on Children's Activities and Development", ***Children and Computer Technology***, 10 (2): 123-144 (Fall/Winter 2000).

3. Wheeler, C. H., "Technology and Industrial Agglomeration: Evidence from Computer Usage", Working Paper, ***Federal Reserve Bank of St. Louis Publications***, (16): 1-36 (2005).

4. Belanger, F., Slyke, C. V., "End-User Learning through Application Play", ***Information Technology, Learning, and Performance Journal***, 18 (1): 61-70, (Spring 2000).

5. Al-Gahtani, S.S., "Computer Technology Acceptance Success factors in Saudi Arabia: An Exploratory Study", ***Journal of Global Information Technology Management***, 7 (1): 5-29 (2004).

6. Canbek, G., Sağıroğlu, Ş., "Şifre Bilimi Tarihine Genel Bakış – I", Mayıs, ***Telekom Dünyası***, 26-44 (2005).

7. Brykczynski, B., Small, B., "Securing Your Organization's Information Assets", ***CROSSTALK The Journal of Defense Software Engineering***, 16 (5): 12-16 (May 2003).

8. Mason, S., "Trusting your computer to be trusted", ***Computer Fraud & Security Journal***, 2005 (1): 7-11 (2005).

9. Sağıroğlu, Ş., "Bilgi ve Bilgisayar Güvenliği Ders Notları", ***Gazi Üniversitesi Fen Bilimleri Enstitüsü***, Ankara, (2005).

10. Koç.net Haberleşme Teknolojileri ve İletişim Hizmetleri A.Ş., "Türkiye İnternet Güvenliği Araştırma Sonuçları 2004", ***Koç.net, İstanbul***, 1-9 (2004).

11. Türkiye Bilimsel ve Teknik Araştırma Kurumu, "Ulusal Bilim ve Teknoloji Politikaları, 2003-2023 Strateji Belgesi", ***Versiyon 19 [2 Kasım 2004], TÜBİTAK, Ankara***, 1-137 (2004).

12. Housman, E. M., "The Nature of Information", ***Bulletin of The American Society for Information Science***, 26 (4): (April/May 2000).

13. Schuler, A. J., "How to Build Wisdom and Prosper in an "Information Age"", ***"What's Up, Doc?" e-Newsletter***, 3 (6): 5-7 (June 2003).

14. İnternet: "Data, Information, Knowledge and Knowledge Management", The OR (Operational Research) Society. http://www.theorsociety.com/about/topic/projects/notorious/2_2_Data_Info.htm (19.04.2005).

15. İnternet: "Euclid", Encyclopedia Britannica from Encyclopedia Britannica Premium Service. http://www.britannica.com/eb/article?tocId=2176 (19.04.2005).

16. International Organization for Standardization, "Information technology -- Code of practice for information security management", ***ISO-17799, ISO***, (2000).

17. Guttman, E., Leong, L., Malkin, G., "Request for Comments: 2504, Users' Security Handbook", ***ISOC, RFC 2504***, 31 (1999).

18. Shamir, A., "Turing Lecture on Cryptology: A Status Report", ***ACM, 2002 A.M. Turing Award Winners***, 8 (2002).

19. Lipner S. B., "The Trustworthy Computing Security Development Lifecycle", ACSAC, ***20th Annual Computer Security Applications Conference***, Tucson, AZ, USA, 2-13 (2004).

20. "Microsoft to invest more in security: Bill Gates", April 15, ***Hindustan Times***, (2005).

21. Granger S., "Social Engineering Fundamentals, Part I: Hacker Tactics", ***SecurityFocus Infocus***, Article No: 1527 (2001).

22. Granger S., "Social Engineering Fundamentals, Part II: Combat Strategies", ***SecurityFocus Infocus***, Article No: 1533 (2002).

23. İnternet: "Anti-Site". http://www.antisitenet.com (03.06.2005).

24. Türkiye Büyük Millet Meclisi İnsan Haklarını İnceleme Komisyonu, "Uluslararası Temel İnsan Hakları Belgeleri", ***TBMM***, Ankara, 203-208 (2001).

25. Electronic Privacy Information Center, "Privacy & Human Rights 2004: An International Survey of Privacy Laws and Developments", ***EPIC, in association with Privacy International***, (2004).

26. 12 Ekim, "Türk Ceza Kanunu", ***T.C. Resmi Gazete***, 25611 (2005).

27. İnternet: Bankalararası Kart Merkezi, "Sanal POS İle Yapılan E-Ticaret İşlemleri", ***BKM***, (2005). http://www.bkm.com.tr/istatistik/sanal_pos_ile_yapilan_eticaret_islemleri.asp (27.07.2005).

28. Erdağ, A. İ., "Ekonomi Sanayi ve Ticarete İlişkin Suçlar ve Bilişim Alanında Suçlar", ***Yeni Türk Ceza Adaleti Sistemi Tanıtım Makaleleri***, 100: 1-22 (2005).

29. Sun Tzu, "Savaş Sanatı", Kılıçarslan, Ş., ***İntermedya Kültür Serisi***, 1, 23, 65 (1997).

30. İnternet: "Malware Directory - Winword/Concept", Virus Bulletin Ltd. http://www.virusbtn.com/resources/malwareDirectory/variants/Winword-Concept.xml (30.04.2005).

31. İnternet: Gostev A., "Malware Evolution: January - March 2005", Kaspersky Lab. http://www.viruslist.com/en/analysis?pubid=162454316 (30.04.2005).

32. İnternet: "Binder", SearchWin2000, TechTarget. http://searchwin2000.techtarget.com/sDefinition/0,,sid1_gci948478,00.html (05.05.2005).

33. İnternet: 23 Temmuz, "10 bin kişinin banka bilgilerini kopyalayan şebeke yakalandı", Milliyet Gazetesi, 2005. http://www.milliyet.com.tr/2005/07/23/son/sontur23.html (23.07.2005).

34. İnternet: "Sanal Dolandırıcılıkta Son Nokta Phishing", İstanbul Emniyet Müdürlüğü. http://www.iem.gov.tr/iem/?idno=147 (15.05.2005).

35. İnternet: “Macromedia Flash content reaches 98.3% of Internet viewers”, Flash Player Penetration Survey, March 2005, NPD Research. http://www.macromedia.com/software/player_census/flashplayer/ (18.06.2005).

36. İnternet: “Malware Threats Triangle”, November 2004, Antisource. http://www.antisource.com/staticpages/index.php/malware-triangle (30.04.2005).

37. İnternet: Read J., “Spyware Explained”, May 2004, Pearson Education, Informit. http://www.informit.com/articles/article.asp?p=174140 (05.05.2005).

38. İnternet: Federal Trade Commission, “FTC Cracks down On Spyware Operation”, FTC, October 12, 2004. http://www.ftc.gov/opa/2004/10/spyware.htm (05.05.2005).

39. İnternet: Computer Crime and Intellectual Property Section, “CyberCrime”, CCIPS of the Criminal Division of the U.S. Department of Justice. http://www.usdoj.gov/criminal/cybercrime/index.html (05.05.2005).

40. İnternet: America Online and the National Cyber Security Alliance, “AOL/NCSA Online Safety Study”, AOL/NCSA, October 2004. http://www.staysafeonline.info/news/safety_study_v04.pdf (05.05.2005).

41. İnternet: Martins J., “The year of spyware”, SurveilleTech Software, December 2004. http://www.e-surveiller.com/pr_the_year_of_spyware.htm (05.05.2005).

42. İnternet: “Top Spyware Threats”, Webroot Software Inc.. http://www.webroot.com/spywareinformation/spywaretopthreats/ (06.05.2005).

43. İnternet: CA Security Advisory Team, “Top 5 Spyware Threats”, Computer Associates International, Inc., 2005. http://www3.ca.com/securityadvisor/pest/ (06.05.2005).

44. İnternet: Chick, D., “2004's Most Popular Viruses, and Hacking Tools”, The Network Administrator. http://www.thenetworkadministrator.com/top2004hackertools.htm (06.05.2005).

45. İnternet: Olsen S., "Gator rushes to court over ad technology", CNET News.com, August 28, 2001. http://news.com.com/2100-1023-272296.html?legacy=cnet&tag=txt (06.05.2005).

46. İnternet: Magid L., "It Pays To Read License Agreements", PC Pitstop Newsletter, February 2005, http://www.pcpitstop.com/spycheck/eula.asp (07.05.2005).

47. İnternet: Edelman B., "Gator's EULA Gone Bad", November 29, 2004, http://www.benedelman.org/news/112904-1.html (07.05.2005).

48. İnternet: Bailey B., "Optimal Line Length", UI Design Newsletter, Human Factors International Inc., November 2002. http://www.humanfactors.com/downloads/nov02.asp#tpe (07.05.2005).

49. İnternet: Edelman B., "Comparison of Unwanted Software Installed by P2P Programs", March 2005, http://www.benedelman.org/spyware/p2p/ (08.05.2005).

50. İnternet: "Tough Questions and Bad Behavior", FaceTime Communications, Inc., 2005. http://www.spywareguide.com/articles/tough_questions_and_bad_behavi_37.html (07.05.2005).

51. İnternet: "How to stop an ActiveX control from running in Internet Explorer", Microsoft Knowledge Base article 240797, Microsoft, April 4, 2005. http://support.microsoft.com/default.aspx?scid=kb;en-us;240797 (08.05.2005).

52. İnternet: MVPS, "hosts Dosyası", Microsoft Most Valuable Professional. http://www.mvps.org/winhelp2002/hosts.txt (07.05.2005).

53. Landesman, M., "Beta Update: Future Windows AntiSpyware Looks Like a Winner", ***PC World***, (April 2005).

54. İnternet: Spyware Eliminator 4.0, Aluria Associates. http://www.aluriasoftware.com/homeproducts/spyware/ (15.05.2005).

55. İnternet: "Aluria Spyware Eliminator 4.0 Review", Adware Report. http://www.adwarereport.com/mt/archives/000008.html (15.05.2005).

56. İnternet: CounterSpy 1.0.29, Sunbelt Software. http://www.sunbelt-software.com/CounterSpy.cfm (15.05.2005).

57. İnternet: Spy Sweeper 3.5, Webroot Software. http://www.webroot.com/products/spysweeper/ (15.05.2005).

58. İnternet: SpySubtract 2.51, InterMute. http://www.intermute.com/products/spysubtract.html (15.05.2005).

59. İnternet: Spyware Doctor 3.2, PC Tools. http://www.pctools.com/spyware-doctor/ (15.05.2005).

60. İnternet: PestPatrol 5.0, Computer Associates International. http://www.pestpatrol.com/Products/PestPatrolHE/ (15.05.2005).

61. İnternet: Ad-Aware SE Pro, LavaSoft. http://www.lavasoftusa.com/software/adawareprofessional/ (15.05.2005).

62. İnternet: ZoneLab Pro, ZoneLab. http://www.zonelabs.com (15.05.2005).

63. İnternet: Outpost Firewall Pro, Aginitum. http://www.agnitum.com (15.05.2005).

64. İnternet: Sygate, Sygate Personal Firewall Pro. http://smb.sygate.com (15.05.2005).

65. İnternet: Norton Personal Firewall 2005, Symantec. http://www.symantec.com (15.05.2005).

66. İnternet: Anti-Spyware Coalition, "Spyware Definitions and Supporting Documents", ASC, Public Comment Document. http://www.antispywarecoalition.org/definitions.pdf (18.06.2005).

67. Canbek, G., Sağıroğlu, Ş., "Şifre Bilimi Tarihine Genel Bakış – II", Haziran, ***Telekom Dünyası***, 26-44 (2005).

68. İnternet: Wurtzel, J., "Bugging your keyboard", BBC News, Science/Nature. http://news.bbc.co.uk/1/hi/sci/tech/1638795.stm (07.06.2005).

69. Say, M., Sağıroğlu, Ş., "Bilgisayar Veri Güvenliği Üzerine Bir İnceleme: Klavye Dinleme Sistemleri", ***Akademik Bilişim 2004***, Trabzon, (2004).

70. İnternet: Happy Hacking Keyboard, PFU Limited. http://www.pfu.fujitsu.com/en/hhkeyboard/hhkbpro/nokeytop.html (08.06.2005).

71. İnternet: “Hardware KeyLogger", Amecisco, Inc.. http://www.amecisco.com/ (08.06.2005).

72. İnternet: “Key logger tools and hardware key loggers for PC KeyGhost SX Spyware scanners cannot detect hardware!”, KeyGhost Ltd.. http://www.keyghost.com/sx/ (08.06.2005).

73. İnternet: “Using the KEYKatcher is easy”, Allen Concepts, Inc.. http://www.keykatcher.com/tutorial/index.html (08.06.2005).

74. Microsoft Developer Network Library, “Hooks”, ***MSDN***, Microsoft Corporation, (2002).

75. İnternet: McGann, R., “Online Banking Increased 47 Percent Since 2002”, ClickZ Network, February 9, 2005. www.clickz.com/stats/sectors/security/article.php/3481976 (01.05.2005).

76. İnternet: Türkiye Bankalar Birliği, “Banka Bilgileri”, TBD, 2005. http://www.tbb.org.tr/asp/bankalar.asp (01.05.2005).

77. İnternet: McGann, R., “Phishing Attacks Surge in Last Six Months”, ClickZ Network, January 12, 2005. www.clickz.com/stats/sectors/finance/article.php/3458321 (02.05.2005).

78. İnternet: Cyber Patrol. http://www.cyberpatrol.com (10.05.2005).

79. İnternet: “Child Safety On The Information Superhighway”. http://www.spyarsenal.com/child-safety.html (15.05.2005).

80. İnternet: Magid, L. J., “Child Safety on the Information Highway”, National Center for Missing and Exploited Children (NCMEC) broşürü, 2003. http://www.safekids.com/child_safety.htm (16.05.2005).

81. İnternet: Dubicki, P., “Acceptable Use Policies and Workplace Privacy: Legal and ethical Considerations”, Global Information Assurance Certification, November 27, 2003.

http://www.giac.org/practical/GSEC/Patrick_Dubicki_GSEC.pdf (03.06.2005).

82. Wakefield, R. L., "Computer Monitoring and Surveillance, Balancing Privacy with Security", ***CPA Journal***, 74 (7): 52-55 (July 2004).

83. İnternet: "NOP World Culture Score(TM) Index Examines Global Media Habits...Uncovers Who's Tuning In, Logging On and Hitting the Books". http://www.nopworld.com/news.asp?go=news_item&key=179 (04.06.2005).

84. İnternet: Kawamoto D., "Companies increase IM surveillance", CNET News, October 26, 2004. http://insight.zdnet.co.uk/communications/networks/0,39020427,39171535,00.htm (29.05.2005).

85. İnternet: "WebSense URL Categories", Websense, Inc.. http://ww2.websense.com/docs/Datasheets/en/v5.5/WebsenseURLCats.pdf (31.05.2005).

86. İnternet: "Cost Savings Calculator" Websense, Inc.. http://ww2.websense.com/global/en/ResourceCenter/CostSavingsCalc/index.php (30.05.2005).

87. İnternet: Bonsor K., "How Workplace Surveillance Works", http://computer.howstuffworks.com/workplace-surveillance.htm (29.05.2005).

88. İnternet: "2001 AMA Survey: Workplace Monitoring & Surveillance", American Management Association. http://www.amanet.org/research/pdfs/ems_short2001.pdf (03.06.2005).

89. İnternet: "2005 Electronic Monitoring & Surveillance Survey", AMA/ePolicy Institute Research, June 2005. http://www.amanet.org/research/pdfs/EMS_summary05.pdf (03.06.2005).

90. İnternet: Oste, J., "Agreement on protection of employees' on-line privacy", Institut des Sciences du Travail. http://www.eiro.eurofound.eu.int/about/2002/09/feature/be0209302f.html (03.06.2005).

91. İnternet: Broughton, A., "UNI highlights on-line rights at work", Industrial Relations Services.

http://www.eiro.eurofound.eu.int/2002/10/feature/eu0210205f.html (03.06.2005).

92. İnternet: "Privacy in Cyberspace: Rules of the Road for the Information Superhighway" Privacy Rights Clearinghouse/UCAN. http://www.privacyrights.org/fs/fs18-cyb.htm (03.06.2005).

93. İnternet: Broughton, A. "Commission issues second stage consultation on data protection", Industrial Relations Services. http://www.eiro.eurofound.eu.int/2002/11/feature/eu0211206f.html (03.06.2005).

94. İnternet: "Klavye Dinleme Sistemleri Veritabanı", Dedicated 2-spyware.com project, JSC. http://www.2-spyware.com/keyloggers-removal (03.06.2005).

95. İnternet: "Testing and reviews of keyloggers, monitoring products and spy software", Security Technology Ltd., 2005. http://keylogger.org/reviews.cgi (09.06.2005).

96. Betteridge, I., "Police Foil $420 Million Keylogger Scam", March, ***eWeek***, Ziff Davis Publishing Holdings Inc., (2005).

97. Brandt, A. "Wireless Keyboards That Blab", March, ***PC World magazine***, (2003).

98. İnternet: "Microsoft Bluetooth Klavye". http://www.microsoft.com/hardware/mouseandkeyboard/features/docs/bluetooth.html (15.06.2005).

99. İnternet: "Virtual Keyboard". http://www.virtual-laser-keyboard.com/index.asp (15.06.2005).

100. İnternet: Madentec Limited. http://www.madentec.com/products/comaccess/screendoors/about.html (10.04.2005).

101. İnternet: Advanced Anti Keylogger, Spydex, Inc.. http://www.anti-keylogger.net/ (15.06.2005).

102. İnternet: Anti-keylogger, Raytown Corporation LLC.. http://www.anti-keyloggers.com/ (15.06.2005).

103. İnternet: Keylogger Hunter, Alexander G. Styopkin. http://www.styopkin.com/keylogger_hunter.html (15.06.2005).

104. Idrees R. N., Baig, M., Aslam. M., "Anti-Hook Shield Against The Software Key Loggers", ***National Conference on Emerging Technologies (NCET 2004)***, Pakistan, 189-191 (2004).

105. Tan, C. K., "Windows Key Logging and Counter-Measures", ***SIG^2 Secure Code Study Report***, (2004).

106. İnternet: Kaplan, Y. "API Spying Techniques for Windows 9x, NT and 2000". http://www.internals.com/articles/apispy/apispy.htm (20.06.2005).

107. Tan, C. K., "Defeating kernel native API hookers by direct service dispatch table restoration", ***SIG^2 Secure Code Study Report***, (2004).

108. Russinovich, M., "Inside Win32 Services", ***Windows IT Pro Magazine***, June, (2000).

109. Rutkowski, J.K., "Advanced Windows 2000 Rootkits Detection", Presentation, ***Black Hat USA 2003 Conference***, (2003).

110. İnternet: Windows Hardware Quality Labs (WHQL). http://www.microsoft.com/whdc/whql/default.mspx (20.06.2005).

111. İnternet: ServerLock, WatchGuard Technologies. http://www.watchguard.com/help/docs/ServerLock.pdf (20.06.2005).

EKLER

EK – 1. 2005 Yılı Casus Savar Yazılım Derecelendirme

Spyware Eliminator (SE), Counter Spy (CS), Spy Sweeper (SS1), Spy Subtract (SS2), Anti Spy (AS), Spy Doctor (SD), Pest Patrol (PP), Ad-aware Pro (AP), Spyware Begone (SB), McAfee AntiSpy (MA)

	SE	CS	SS1	SS2	AS	SD	PP	AP	SB	MA
Derece	**1**	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**10**
Yıllık Fiyat	29,99$	19,95$	29,95$	29,95$	29,99$	29,95$	29,95$	41,91$	39,95$	29,99$
Toplam Derecelendirme										
Derecelendirme										
Özellik Takımı										
Etkinlik										
Kolay Kullanım										
Uyarlama										
Kolay Kurulum										
Yardım/Destek										
Özellikler										
Aranılan bileşenler	36 000	?	53 248*	37 691	22 984	23 675	?	36 254	?	?
Geri Alma/Geri Yükleme Yeteneği	✓	✓	✓	✓				✓	✓	✓
Casus Yazılım Önem Derecesi	✓	✓	✓	✓	✓	✓		✓		
Bulunan Casus Yazılımın Açıklaması	✓	✓	✓	✓	✓	✓	✓	✓		
Tarama Zamanlaması	✓	✓	✓	✓	✓	✓	✓			✓
Otomatik Güncelleme	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
İz Sürme Çerez Engellemesi	✓	✓	✓		✓	✓	✓		✓	
Gerçek Zamanlı Engelleme ve Koruma	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Çıkarılabilir Ortam Tarama	✓	✓	✓	✓	✓			✓		
Saptama ve Silme Yetenekleri										
Reklam yazılım	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Casus yazılım	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Klavye dinleme	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Truva	✓	✓	✓	✓	✓	✓	✓	✓		
ActiveX Yapılandırma	✓	✓	✓	✓	✓	✓	✓	✓	✓	
Kirli yazılım	✓	✓	✓	✓	✓	✓		✓		
Telefon çeviriciler	✓	✓	✓	✓	✓	✓	✓	✓		
Kötücül yazılım	✓	✓	✓	✓	✓	✓		✓	✓	
Veri Gömme	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Parazitler	✓	✓	✓	✓	✓	✓		✓		
Araç çubukları	✓	✓	✓	✓	✓	✓	✓	✓	✓	
İndirme ile Sürücü	✓	✓	✓	✓	✓	✓	✓	✓		
İz Sürme Çerezleri	✓	✓	✓	✓	✓	✓	✓	✓	✓	
Casus yazılım sistem kütüğü anahtarları	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Tarayıcı Soyma/BHO	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓

* Diğer çoğu casus savar yazılımın aksine Spy Sweeper aradığı bileşenlere çerezleri de eklemektedir.

	SE	CS	SS1	SS2	AS	SD	PP	AP	SB	MA
Yararlanılan Teknik Destek										
Ücretsiz telefon	✓	✓	✓							✓
Yerleşik Uygulama Yardımı	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Özbilgi Tabanı/SSS	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Forum/E-posta	✓	✓	✓	✓		✓	✓	✓	✓	✓
Çevrimiçi sohbet	✓	✓	✓		✓					✓
Desteklenen Yapılandırmalar										
XP	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
2000	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
98	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
95				✓		✓		✓	✓	
NT	✓		✓	✓	✓		✓		✓	
ME	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓

EK – 2. Sanal Klavye Tuş Kodları

Sanal Tuş Kodu	*Değeri (Onaltılık)*	*Fare veya Tuş Karşılığı*	*Sanal Tuş Kodu*	*Değeri (Onaltılık)*	*Fare veya Tuş Karşılığı*
VK_LBUTTON	1	Sol fare tuşu	VK_W	57	w tuşu
VK_RBUTTON	2	Sağ fare tuşu	VK_X	58	x tuşu
VK_CANCEL	3	Control-break işleme	VK_Y	59	y tuşu
VK_MBUTTON	4	Orta fare tuşu	VK_Z	5A	z tuşu
—	05–07	Tanımsız	VK_LWIN	5B	Sol Windows tuşu
VK_BACK	8	geri silme tuşu	VK_RWIN	5C	Sağ Windows tuşu
VK_TAB	9	sekme tuşu	VK_APPS	5D	Uygulamalar tuşu
—	0A–0B	Tanımsız	—	5E–5F	Tanımsız
VK_CLEAR	0C	temizleme tuşu	VK_NUMPAD0	60	Nümerik 0 tuşu
VK_RETURN	0D	giriş tuşu	VK_NUMPAD1	61	Nümerik 1 tuşu
—	0E–0F	Tanımsız	VK_NUMPAD2	62	Nümerik 2 tuşu
VK_SHIFT	10	üst simge tuşu	VK_NUMPAD3	63	Nümerik 3 tuşu
VK_CONTROL	11	kontrol tuşu	VK_NUMPAD4	64	Nümerik 4 tuşu
VK_MENU	12	alternatif tuşu	VK_NUMPAD5	65	Nümerik 5 tuşu
VK_PAUSE	13	duraklatma tuşu	VK_NUMPAD6	66	Nümerik 6 tuşu
VK_CAPITAL	14	büyük harf kilidi tuşu	VK_NUMPAD7	67	Nümerik 7 tuşu
—	15–19	Kanji sistemleri için ayrılmış	VK_NUMPAD8	68	Nümerik 8 tuşu
—	1A	Tanımsız	VK_NUMPAD9	69	Nümerik 9 tuşu
VK_ESCAPE	1B	esc (kaçış) tuşu	VK_MULTIPLY	6A	Çarpım tuşu
—	1C–1F	Kanji sistemleri için ayrılmış	VK_ADD	6B	Ekleme tuşu
VK_SPACE	20	boşluk çubuğu	VK_SEPARATOR	6C	Ayıraç tuşu
VK_PRIOR	21	yukarı sayfa tuşu	VK_SUBTRACT	6D	Çıkarma tuşu
VK_NEXT	22	aşağı sayfa tuşu	VK_DECIMAL	6E	Ondalık tuşu
VK_END	23	son tuşu	VK_DIVIDE	6F	Bölme tuşu
VK_HOME	24	baş tuşu	VK_F1	70	f1 tuşu
VK_LEFT	25	sol ok tuşu	VK_F2	71	f2 tuşu
VK_UP	26	yukarı ok tuşu	VK_F3	72	f3 tuşu
VK_RIGHT	27	sağ ok tuşu	VK_F4	73	f4 tuşu
VK_DOWN	28	aşağı ok tuşu	VK_F5	74	f5 tuşu
VK_SELECT	29	seçme tuşu	VK_F6	75	f6 tuşu
—	2A	OEM belirli	VK_F7	76	f7 tuşu
VK_EXECUTE	2B	yürütme tuşu	VK_F8	77	f8 tuşu
VK_SNAPSHOT	2C	ekran çıktısı tuşu	VK_F9	78	f9 tuşu
VK_INSERT	2D	araya ekleme tuşu	VK_F10	79	f10 tuşu
VK_DELETE	2E	silme tuşu	VK_F11	7A	f11 tuşu
VK_HELP	2F	yardım tuşu	VK_F12	7B	f12 tuşu
VK_0	30	0 tuşu	VK_F13	7C	f13 tuşu
VK_1	31	1 tuşu	VK_F14	7D	f14 tuşu
VK_2	32	2 tuşu	VK_F15	7E	f15 tuşu
VK_3	33	3 tuşu	VK_F16	7F	f16 tuşu
VK_4	34	4 tuşu	VK_F17	80H	f17 tuşu
VK_5	35	5 tuşu	VK_F18	81H	f18 tuşu
VK_6	36	6 tuşu	VK_F19	82H	f19 tuşu
VK_7	37	7 tuşu	VK_F20	83H	f20 tuşu

Sanal Tuş Kodu	*Değeri*	*Fare veya Tuş Karşılığı*	*Sanal Tuş Kodu*	*Değeri*	*Fare veya Tuş Karşılığı*
	(Onaltılık)			*(Onaltılık)*	
VK_8	38	8 tuşu	VK_F21	84H	f21 tuşu
VK_9	39	9 tuşu	VK_F22	85H	f22 tuşu
—	3A–40	Tanımsız	VK_F23	86H	f23 tuşu
VK_A	41	a tuşu	VK_F24	87H	f24 tuşu
VK_B	42	b tuşu	—	88–8F	Atanmamış
VK_C	43	c tuşu	VK_NUMLOCK	90	Rakam kilidi tuşu
VK_D	44	d tuşu	VK_SCROLL	91	Kaydırma kilidi tuşu
VK_E	45	e tuşu	—	92–B9	Atanmamış
VK_F	46	f tuşu	—	BA–C0	OEM belirli
VK_G	47	g tuşu	—	C1–DA	Atanmamış
VK_H	48	h tuşu	—	DB–E4	OEM belirli
VK_I	49	i tuşu	—	E5	Atanmamış
VK_J	4A	j tuşu	—	E6	OEM belirli
VK_K	4B	k tuşu	—	E7–E8	Atanmamış
VK_L	4C	l tuşu	—	E9–F5	OEM belirli
VK_M	4D	m tuşu	VK_ATTN	F6	Attn tuşu
VK_N	4E	n tuşu	VK_CRSEL	F7	CrSel tuşu
VK_O	4F	o tuşu	VK_EXSEL	F8	ExSel tuşu
VK_P	50	p tuşu	VK_EREOF	F9	Erase EOF tuşu
VK_Q	51	q tuşu	VK_PLAY	FA	Oynatma tuşu
VK_R	52	r tuşu	VK_ZOOM	FB	Yakınlaşma tuşu
VK_S	53	s tuşu	VK_NONAME	FC	Gelecek kullanımlar için ayrılmış
VK_T	54	t tuşu	VK_PA1	FD	PA1 tuşu
VK_U	55	u tuşu	VK_OEM_CLEAR	FE	OEM Temizleme tuşu
VK_V	56	v tuşu			

ÖZGEÇMİŞ

Gürol CANBEK, 1974 yılında Malatya'da doğdu. 1996 yılında bir yıllık İngilizce hazırlık ile beraber, İstanbul Teknik Üniversitesi, Kontrol ve Bilgisayar Mühendisliği bölümünden mezun oldu. İMKB (İstanbul Menkul Kıymetler Borsası) TAKASBANK A.Ş.'de yazılım uzmanı olarak Özel Projeler bölümünde, borsa işlemlerinin gözetimi, döviz alım-satım işlemleri, vadeli işlemler piyasası ve kaydî sisteme geçiş projelerinde etkin bir şekilde görev aldı. 1998 yılında, Milli Savunma Bakanlığı'nda, bilgisayar sistemleri üzerine Proje Subayı olarak askerlik görevini yerine getirdi. İnönü Üniversitesi, Malatya Meslek Yüksek Okulu, Bilgisayar Programcılığı Programı'nda öğretim görevlisi olarak çalıştı. Görevi sırasında, "Temel Bilgi Teknolojileri" ders kitabının bölüm yazarlığını ve "AutoCAD R.14 ile Tasarım" adlı ders kitabının yazarlığını yaptı. İsrail'de ELBIT Inc. firmasında bir yıl askeri bir projede yazılım uzmanı olarak başarı ile görev aldı. Hali hazırda HAVELSAN A.Ş.'de kıdemli mühendis olarak çalışmaktadır. Firmanın bir uçar platform üzerinde geliştirip, entegre ederek, kurulum yaptığı ilk proje olan uluslararası Açık Semalar (Open Skies) projesinde ve (EHTES) Elektronik Harp Test ve Eğitim Sahası projesinde, veritabanı sistemleri, nesne tabanlı programlama ve coğrafi bilgi sistemleri konularında uzman olarak yazılım sistemi geliştirme süreçlerinin tamamında etkin bir şekilde görev almıştır.