GELİŞMİŞ ISRARCI TEHDİTLER VE GIT ÖRNEKLERİNİN KARŞILAŞTIRILMASI

Esra Söğüt[1], O. Ayhan Erdem[2]

1 Gazi Üniversitesi, Teknoloji Fakültesi Bilgisayar Mühendisliği Bölümü 06500, Teknikokullar, Ankara-Türkiye, Telefon: +90 312-2028561, esrasogut@gazi.edu.tr

2 Gazi Üniversitesi, Teknoloji Fakültesi Bilgisayar Mühendisliği Bölümü 06500, Teknikokullar, Ankara-Türkiye, ayerdem@gazi.edu.tr

Özet — Gelişmiş Israrcı Tehdit (GIT) bilgisayarların, bilgisayar sistemlerinin ve kullanıcıların karşılaştığı en büyük tehditlerden birisidir. Son derece gelişmiş nitelikte, özel olarak ve az sayıda hazırlanmış GIT'lerin tespit edilebilmesi de kolay olmamaktadır. Deneyimli ve sabırlı saldırganlar tarafından oluşturulan GIT'ler dünya genelinde farklı yerlerde ve farklı alanlarda karşımıza çıkabilmektedir. Kullanıcılarda farkındalık oluşturmak amacıyla bu çalışmada GIT hakkında detaylı bilgi verilmiştir. Ayrıca dünya genelinde büyük etkiler meydana getiren GIT örnekleri incelenmiş ve bu örneklerin çalışma yapılarına göre karşılaştırılmaları yapılmıştır.

Anahtar Kelimeler — Gelişmiş Israrcı Tehdit, Siber Savaş, Siber Güvenlik, Stuxnet

Abstract — The Advanced Persistent Threat (APT) is one of the greatest threats faced by computers, computer systems and users. APT has highly advanced qualities and a small number of specially crafted so APT cannot be detected easily. APTs can appear in different places and areas worlwide which are created by experienced and patient attackers. This study aims to create awareness about the APT. In addition, APT samples which constituting larger impact on the world are analyzed and comparisons are made according to the working structures.

Index Terms — Advanced Persistent Threats, Cyber Warfare, Cyber Security, Stuxnet

I. GİRİŞ

Günümüzde internetin ve bilgisayarın kullanıldığı alanlar giderek artmaktadır. Kullanılan ve saklanılan bilgiler de birikmekte ve bunların güvenliği büyük bir sorun haline gelmektedir. Kişilere olabileceği gibi kamu kurum ve kuruluşlarına, kritik altyapılara veya büyük şirketlere yönelik siber saldırılar gerçekleşebilmektedir. Sahip olunan bilginin önemine göre saldırılar da değişebilmektedir.

Özellikle kritik altyapılar, büyük şirketler, telekom operatörleri ve kamu kurumlarına yönelik saldırılar büyük zararlar verebilecek boyutlarda olabilmektedir. Bu alanda yeni bir saldırı türü sayılabilecek Gelişmiş Israrcı Tehdit(GIT)'i gösterebiliriz [1]-[10]. Bu tehdit hedefini belirleyip, başarılı oluncaya kadar çalışmasını sürdürmektedir. Gelişmiş Israrcı Tehdit'in hedefe sızdığını ve orada çalıştığını anlamak kolay olmamaktadır. Bu sebeplerle etkisi diğer saldırı türlerine göre çok daha büyük olabilmektedir.

Bu çalışmada GIT hakkında bilgi verilmiştir. Birinci bölüm giriş olarak düzenlenmiş ve bu bölümde çalışma hakkında genel bilgiler sunulmuştur. Çalışmanın ikinci bölümünde GIT'lerin ne olduğundan ve GIT'lerin çalışma yapılarının nasıl olduğundan bahsedilmiştir. Üçüncü bölümde ise ele alınan GIT örnekleri incelenmiş ve belirlenen özelliklere göre kıyaslama yapilmiştir. Seçilmiş olan Stuxnet, Duqu, Flame, Red October ve MiniDuke uygulamaları hakkında bilgi verilip karşılaştırmalı olarak incelemeler yapılmıştır. Çalışmanın son bölümünde GIT örneklerinin incelenmesi sonucunda elde edilen sonuçlar aktarılmış ve sonuç verileri tabloda gösterilmiştir.

II. GELİŞMİŞ ISRARCI TEHDİT VE ÇALIŞMA YAPISI

Gelişmiş Israrcı Tehdit (GIT), günümüzün siber dünyasında büyük bir tehdit oluşturmakta ve etkisi giderek artan bir saldırı haline gelmektedir. ABD Ulusal Standartlar ve Teknolojisi Enstitüsü (NIST) tarafından GIT için yapılan tanım şu şekildedir: Bilgi seviyesi ve tecrübesi yüksek olan saldırgan, gerekli kaynakları kullanarak çoklu saldırı vektörleri (siber, fiziksel gibi) ile amaçlarına ulaşmak için kendisine uygun fırsatlar oluşturur. Buradaki amaçlar genellikle, hedeflenen kuruluşların bilgi teknoloji altyapısını oluşturan ve onu kapsayan sistemin içinde bulunmak ve ileriki zamanlarda da faaliyete geçebilmek için doğru şekilde konumlanmaktır. Gelişmiş Israrcı Tehdit: (i) amaçlarını gerçekleştirmek için uzun süre takipte kalır, (ii) hedefin savunma sistemine uyum sağlar, (iii) belirlenen amacı gerçekleştirmek için gerekli olan etkileşim seviyesini sağlar ve onu korur [2].

Yukarıda yer alan tanımdan da anlaşılacağı üzere GIT, kaynağı iyi şekilde sağlanmış yetenekli ve kararlı saldırgan ya da saldırganlar tarafından gerçekleştirilen saldırılardır. Etkisi, yol açabileceği zararları ve oluşabilecek sonuçlar tam olarak bilinememekte veya tahmin edilememektedir. Özel olarak hazırlanmış ve birçok aşaması olan GIT'ler farklı özelliklere sahip olsa da çalışma yapıları olarak benzerlik göstermektedir. GIT saldırı evrelerini tanımlamak için kullanılan yönteme Saldırı Ölüm Zinciri (Intrusion Kill Chain) denilmektedir ve tipik bir GIT saldırısı şu altı evreden oluşmaktadır: keşif ve silahlanma, teslim ve dağıtım, ilk sızma ve saldırı, komuta ve kontrol, yanal hareket ve veri çekme. Bu evrelerin sıralı haldeki gösterimine, GIT akış şeması olarak Şekil1'de yer verilmektedir [3]-[5].



Şekil 1 : Gelişmiş Israrcı Tehdidin Akış Şeması [3]-[5]

A. Keşif ve Silahlanma (Bilgi Toplama)

GIT için en önemli adımdır ve saldırıya başlamadan önce gerekli olan hazırlık evresidir. Saldırganın saldıracağı hedefi tanıması için gerekli olan işlemler bu evrede gerçekleştirilir. Kurbanla ilgili olabildiğince araştırmanın yapılması ve elde edilen bilgilerin toplanması gerekmektedir. Bunun için açık kaynak istihbarat araçları, sosyal mühendislik yöntemleri kullanılmakta ve zaafiyet tarama işlemleri yapılmaktadır.

B. Dağıtma

Bu aşama hedef belirlendikten ve hedefle ilgili bilgiler toplandıktan sonra gerçekleşir. Bu evrede saldırganlar hazırladıkları, sistemde açık bulma kodlarını veya sistemi sömürme kod parçacıklarını (exploit) hedeflerine yönlendirmektedir. 2004-2010 yılları arasında Lockheed Martin Computer Incident Response Team (LM-CIRT)'in yaptığı gözlemlere göre yaygın olarak kullanılan dağıtma yöntemlerinden üç tanesi e-posta eklentileri, web siteleri ve USB taşınabilir medya araçları olarak belirlenmiştir [3].

C. İlk Sızma-Saldırı

Dağıtma aşamasında silah olarak kullanılan istismar ve sömürü kod parçacıkları hedef sistemde başarıya ulaşınca bu evreye geçilir. Saldırgan, hedef sisteme yetkisiz erişim hakkını ilk kez elde ettikten sonra ilk sızma işlemine sıra gelmektedir. Bu evrede hedef sistemin güvenlik açığından, işletim sistemi veya uygulama açığından faydalanılabilir ya da hedef farkında olmadan kendisi kodları çalıştırarak sızmayı başlatabilir.

D. Komuta ve Kontrol

Hedef sistemde yetkisiz izinler elde edilerek, uzaktan erişim özelliğine sahip trojan veya arkakapı sisteme yerleştirilerek kurban sistemde kalıcılık sağlanmaya çalışılır. GIT, başarılı bir arkakapı kurulması ile komuta ve kontrol sistemini kullanabilmektedir. Komuta ve kontrol sistemi kurulunca kendi hâkimiyetini yitirmiş hedef sistem ele geçirilmiş olur. Saldırgan, hedef sistemde tespit edilmemek ve dikkat çekmemek için yasal hizmetleri veya herkesin kullanımına açık olan araçları tercih etmektedir.

E. Yayılma

Yayılma aşaması diğer aşamalara göre daha fazla zaman almaktadır. Saldırgan istediği bilgileri elde edinceye kadar kendini belli etmeden uzun süre boyunca çalışabilmektedir. Ele geçirilmek istenen sistem ile kontrol-komuta sunucuları arasında iletişim kurulması, GIT unsurlarının hedef ağ içerisinde hareket etmesine zemin hazırlamaktadır. Hedef sistem üzerinde kontrolün sağlanıp ağ üzerinden kontrolün genişletilmesi, sistemin özelliklerini keşfetmek ve sistemle ilgili önemli bilgileri toplamak için olanak sağlamaktadır.

F. Veri Çekme

Hassas, önemli veya gizli bilgilerin ele geçirilmesini amaçlayan saldırganlar için veri çekme aşaması kritik öneme sahiptir. Bilgiler dışarıya aktarılırken genellikle test amaçlı kullanılan deneme sunucuları kullanılmaktadır. Bilgiler genellikle sıkıştırılmış ve şifrelenmiş halde iletilir ve saldırgan deneme sunucusundan kendi sistemine bilgileri geçirir.

III. GIT UYGULAMALARI VE ÇALIŞMA YAPILARINA GÖRE KARŞILAŞTIRILMALARI

Gelişmiş Israrcı Tehditler siber dünyadaki savaş için çok büyük tehlike oluşturmaktadır. GIT'lerin meydana getirdikleri ya da getirecekleri etkiler hemen anında anlaşılamamaktadır. Siber savaş aracı olarak kullanılan GIT uygulamaları giderek artmakta ve saldırıya uğrayan kurbanlar büyük zarar görebilmektedir. Günümüze yakın zamanlarda tespit edilmiş ve siber güvenlik alanında önemli yer edinmiş GIT uygulamaları ele alınmaktadır. Sahip olduğu özelliklerine ve çalışma yapılarına göre incelenen ve karşılaştırılan uygulamalar meydana getirdikleri etkilerine ve tespit edilme tarihlerine göre seçilmiştir. Ele alınan GIT'ler Stuxnet, Duqu, Flame, Red October ve MiniDuke uygulamalarıdır. Bu uygulamalar incelenerek elde edilen bilgiler Tablo1 üzerine karşılaştırılmalı olarak yerleştirilmiştir.

A. Stuxnet

İlk olarak ele alınan GIT uygulaması olan Stuxnet Haziran 2010'da tespit edilmiş ve güvenlik alanında büyük yankı uyandırmıştır. İran'daki SCADA (Merkezi Denetleme, Kontrol ve Veri Toplama) sistemlerini hedef alan bu GIT'in, incelemeler sonucunda sahip olduğu karmaşık yapısı ile diğer sıradan kötücül yazılımlardan farklı olduğu anlaşılmıştır [6]. Programlanabilir mantık denetleyicisi (PLC) sistemlerini, endüstriyel kontrol sistemlerini (ICS) ve Windows sisteminin kullandığı Siemens Step-7 yazılımını da kontrol altına alarak İran'ın nükleer yakıt tesisine zarar vermeyi amaçlamıştır [7]. Uranyum zenginleştirmede kullanılan ve önemli görevleri olan santrefüjlerin çalışmasını bozarak tesise fiziksel olarak zarar vermiş ve yaklaşık iki ile dört yıl olarak sistemi geriye itmiştir [8]. Stuxnet'in sisteme nasıl bulaştığı tam olarak bilinmemekte fakat taşınabilir sürücülerle sisteme bulaştığı tahmin edilmektedir [9].

Bulaştığı sistemde kendi kendini çoğaltabilme becerisine sahip olan Stuxnet, karşılaştırılan diğer GIT uygulamaları arasında bu yönüyle farklılık oluşturmaktadır. Sistem içerisinde taşınabilir medya ile veya ağ üzerinden çoğalabilmektedir. Bir diğer farklılık ise keylogger özelliğine sahip olmamasıdır. Keylogger özelliği ile kurbana ait hassas ve önemli bilgiler (şifreler, kullanıcı bilgileri gibi) toplanabilmekte veya çalınabilmektedir. Keylogger bileşenleri ile kurban sisteme ait ekran görüntüsü alma, e-posta mesajlarını yakalama, konuşmaları kaydetmek için bilgisayara ait mikrofonu kullanma gibi işlemler yapılabilmektedir. Stuxnet için bu işlemlerden söz edilmemektedir. Şifreleme yöntemi olarak diğer GIT uygulamaları gibi dizi şifreleme algoritması kullanılmıştır [9],[10]. Veri güvenliğinde kullanılan şifreleme algoritmalarından biri olan dizi şifrelemesi, bir anahtardan üretilen anahtar dizisi ile mesajda yer alan tüm harflerin özel bir algoritma (XOR işlemi gibi) kullanılarak sırayla şifrelenmesidir. Dizi şifreleme algoritması simetrik şifreleme ailesinden kabul edilmektedir [11]-[15]. Stuxnet, verileri komuta-kontrol sunucularına gönderirken kodlamak için ve kendi küçük parçalarının şifresini çözmek için de dizi şifreleme algoritmasını kullanmaktadır.

B. Duqu

Eylül 2011 tarihinde tespit edilen Duqu, hedef sistemlere sızmak için MS Word yöntemini kullanmaktadır [16]. Microsoft Word dosyalarının içerdiği True Type yazı tipi ayrıştırma sıfırıncı gün açıklığı (CVE-2011-3402) ilk saldırı vektörü olarak kullanılmıştır [9],[17]. Duqu da Stuxnet gibi SCADA sistemlerini hedef almakta fakat sistemlere zarar vermek yerine casusluk yaparak bilgi toplamayı amaçlamaktadır. Duqu uygulamasının, Stuxnet gibi sistemlere zarar verme amacı taşıyan saldırılar için istihbarat sağlamak amacıyla ve oluşacak saldırının etkinliğini arttırmak amacıyla hazırlandığı düşünülmektedir. Ayrıca SCADA sistemleri ile ilgili kritik bilgilerin tespiti yapılarak saldırı yapılacak sistemin zayıf ve güçlü yönlerinin ele geçirilmesi bu uygulama ile sağlanmıştır. Bulaştığı sistemde Stuxnet gibi kendi kendini çoğaltma özelliğine sahip olmayan Duqu otomatik olarak ağ içinde veya system içinde kopyalanamamaktadır. Keylogger özelliği ile kurbanla ilgili bilgiler çeşitli yollarla ele geçirilmektedir [9],[16]. Çalınan bilgilerin ve yapılandırma dosyalarının şifrelenmesi için diğer GIT uygulamaları gibi dizi şifreleme algoritması kullanılmıştır [18]. Bunun yanında diğer GIT uygulamalarından farklı olarak AES-CBC (Gelişmiş Şifreleme Standardı-Blok Şifreleme Zinciri) modu kullanılmıştır [10]. Bilgileri şifreleyebilen ve deşifre edebilen bir simetrik blok şifrelemesi olan AES, elektronik verileri korumak için kullanılabilecek şifreli bir algoritma belirtir [19]. CBC modu, daha önce şifrelenmiş bloklar ile düz metin bloklarını zincirleyerek birleştiren ve bu şekilde şifreleme işlemi yapan gizlilik modudur [20],[21]. AES'e ait beş güvenlik modundan biri olan CBC modu Duqu tarafından kullanılmaktadır.

C. Flame

Karşılaştırılan diğer bir GIT uygulaması olan Flame 2012 yılının Mayıs ayında tespit edilmiştir. İran, İsrail, Batı Şeria, Sudan, Suriye, Lübnan, Suudi Arabistan ve Mısır gibi Orta Doğu ülkelerini hedef alan Flame devlet kuruluşları ve eğitim kurumları gibi önemli yerlere ulaşmıştır [6],[22],[23]. Stuxnet gibi bulaştığı sisteme zarar vermek amacı gütmeyen Flame, bilgi toplamak amacıyla hareket etmiştir. Bulaştığı çok sayıda bilgisayardan veri sızdırmış ve hırsızlık yapmayı sürdürmüştür. Tespit edildiği zamandan beş ile sekiz yıl öncesinden beri aktif olduğu tahmin edilmektedir [22]. Flame'in sistemlere nasıl bulaştığı tam olarak bilinmemekte ama taşınabilir sürücülerle veya oltalama saldırılarıyla bulaştığı tahmin edilmektedir.

Flame, kurban sistemde kendi kendini çoğaltma özelliğine sahip değildir. Bulaştığı sistemde manuel olarak kopyalanabilmektedir. Sahip olduğu keylogger özelliği ile bulaştığı sistemdeki önemli bilgileri çalabilmektedir [9]. Diğer GIT uygulamalarından farklı olarak, keylogger bileşenleri ile web kamerasını (ses ve görüntü kaydetmek için) da kullanabilmektedir. Ayrıca Bluetooth ve Wifi özelliklerini, USB ve depolama aygıtlarını da veri çalmak için kullanabilmektedir. Bluetooth özelliği aktif olduğunda çevredeki cihazlara da ulaşıp sızma ve çalma işlemlerini gerçekleştirebilmektedir. Bu özellikler de Flame'in etkisini ve önemini arttırmaktadır. Yapılandırma dosyalarını ve yakaladığı verileri şifrelemek için dizi şifreleme algoritması, RC4 algoritması ve Substitution şifrelemesi kullanmıştır [6],[22]. Diğer GIT uygulamalarından farklı olarak kullanılan Substitution şifrelemesi, verilerede bayt bayt değiştirme yaparak şifreleme anlamına gelir. Burada her karakterin yerine farklı karakter konularak şifreleme yapılır ve uygun bir tablo oluşturularak her karaktere karşılık gelen karakter bu tabloda saklanır. RC4 algoritması ise şifrelenecek veriyi akan bir bit dizisi olarak algılar ve önceden belirlenen anahtar ile veriyi şifreler. RC4, rastgele olarak ürettiği anahtar akışlarını, hem şifreleme hem de şifreyi çözme sırasında XOR işlemi ile mesaja uygulamaktadır [24]-[27].

D. Red October

Ele alınan GIT uygulamalarından olan Red October Ekim 2012 tarihinde tespit edilmiş ve Doğu Avrupa, Batı Avrupa, Kuzey Amerika gibi bölgeleri etkisi altına almıştır. Bu bölgelerdeki kamu kurumlarına, devlet birimlerine, bilimsel araştırma merkezlerine, diplomatik birimlere, askeri birimlere, enerji/nükleer araştırma birimlerine gibi çok sayıda yere sızarak casusluk faaliyetleri sürdürmüştür. Bulaştığı sistemleri ele geçirmek veya çökertmek amacı gütmemektedir. Oldukça geniş bölgelerde çalışan bu GIT uygulamasının, gizli bilgileri ve jeopolitik öneme sahip istihbaratları 2007 yılından beri topladığı bilinmektedir [28],[29]. Yüksek profilli kurbanlar seçen Red October'ın çaldığı bilgileri ne için kullandığı veya kullanacağı tam olarak bilinememektedir. Elde edilen bu bilgiler karaborsada satılabilir veya doğrudan kullanılabilir niteliktedir. Hedef sistemlere sızma yöntemi olarak MS Word (CVE-2012-0158, CVE-2010-3333), MS Excel (CVE-2009-3129) ve Java (CVE-2011-3544) güvenlik açıklıkları kullanılmıştır [30]. Geleneksel saldırı hedeflerine ek olarak akıllı telefonlar da etki altında kalmıştır. İphone, Nokia veya Windows Mobile gibi mobil cihazlardan veri çalma özelliğine de sahiptir. Çalınan bilgiler telefona ait özellikler, telefon defteri, kişiler, arama geçmişleri, ajanda veya mesajlar olabilmektedir [28],[29].

Red October, kurban sistemde kendi kendini çoğaltma özelliğine sahip değildir ve bulaştığı sistemde manuel olarak çoğalabilmektedir. Keylogger özelliğine sayesinde bulaştığı sistemdeki bilgileri, klavye hareketlerini kaydederek veya ekran görüntüsü alarak çalabilmektedir [9],[28]. Yakaladığı verileri şifrelemek için dizi şifreleme algoritmasının yanında ROR işlemi de kullanılmıştır (XOR+ROR) [31],[32]. Diğer GIT uygulamalarından farklı olarak kullanılan ROR işlemi, sağ tarafta yer alan bitlerden belirtilen kadarının düşmesiyle solda açılan yere belirtilen bitlerin yerleşmesi işlemidir. Red October şifreleme işleminde bu algoritmalardan faydalanmaktadır [33]-[35].

E. MiniDuke

İncelenen son GIT uygulaması olan MiniDuke Şubat 2013 tarihinde tespit edilmiştir [36]. Almanya, Ukrayna, Portekiz, Romanya, Çek Cumhuriyeti, İrlanda, Birleşik Krallık, Macaristan ve Türkiye'nin de dâhil olduğu 23 ayrı ülkeyi hedef alan MiniDuke devlet kuruluşlarını, büyükelçilikleri, araştırma merkezlerini, sağlık kuruluşlarını, sosyal vakıfları ve özel şirketleri kurban olarak seçerek önemli yerlere ulaşmıştır. Bulaştığı sisteme zarar vermek amacı gütmeyen fakat bilgi toplama amacı taşıyan bir GIT uygulamasıdır. Bulaştığı çok sayıda bilgisayardan veri sızdırmakta ve casusluk faaliyetlerini sürdürmektedir. Bu GIT uygulamasının saldırganlardan komuta almak için birisi Panama'da diğeri ise Türkiye'de bulunan iki sunucuya bağlandığı bilinmektedir [37]. MiniDuke diğer GIT'lerden farklı olarak Twitter'ı ve

Google Arama özelliğini kullanabilmektedir. Twitter'a girerek (kullanıcıdan bağımsız olarak) önceden oluşturulan hesaplara tweet atılmasını ve bu şekilde saldırgan-kurban arasında iletişim kurulmasını sağlamaktadır [38]. Twitter aktif olmadığında ise Google Arama uygulamasını kullanmaktadır [39]. Kurban sistemlere sızma yöntemi olarak PDF dosyaları sosyal mühendislik yöntemleriyle gönderilmektedir. PDF dosyalarına ait güvenlik açıklığından (CVE-2013-6040) faydalanılarak sistemlere sızılmaktadır [36],[38].

Kurban sistemde kendi kendini çoğaltma özelliğine sahip olmayan MiniDuke, bulaştığı sistemde manuel olarak çoğalabilmektedir. Keylogger özelliğine sahiptir. Bu özellik sayesinde bulaştığı sistemdeki bilgileri veya ekran görüntülerini çalabilmektedir [10]. Yakaladığı verileri şifrelemek için dizi şifreleme algoritmasını kullanmaktadır. Sahip olduğu arka kapılar ile dizin oluşturma, dosya kopyalama, dosya taşıma, dosya kaldırma, süreçleri durdurma, yeni kötücül yazılımları indirme ve onları çalıştırma gibi işlemleri gerçekleştirebilmektedir. Tüm bunları yapabilen MiniDuke uygulaması 20KB boyutundadır [36],[38].

F. GIT Uygulamalarının Çalışma Yapılarına Göre Karşılaştırılması

Farklı zamanlarda yapılmış GIT örnekleri karşılaştırılarak, elde edilen bilgilere Tablo1'de yer verilmiştir. Karşılaştıma işlemi birçok farklı özelliğe göre yapılmaktadır. Karşılaştırılan GIT'ler için Stuxnet, Duqu, Flame, Red October ve MiniDuke uygulamaları seçilmiştir [9],[10]. Bu örnekler seçilirken her bir GIT uygulaması için tespit edilme tarihleri ve oluşturdukları etkileri göz önüne alınmıştır.

Farklı GIT uygulamaları sahip oldukları özelliklere göre karşılaştırılmakta ve elde edilen sonuçlar Tablo1'de gösterilmektedir. Farklı GIT uygulamaları kıyaslanırken, bu uygulamaları birbirinden ayırabilecek nitelikte olan ve her bir uygulama için önemli olan temel özellikler ele alınmaktadır. Bunlar: ilk sızma şekli, şifreleme yöntemleri, kendini çoğaltma yöntemleri, tespit edilme tarihi, hedefleri, amacı, etkileri ve keylogger özelliğine sahip olup olmamasıdır. İncelenen GIT uygulamaları 2010, 2011, 2012 ve 2013 yıllarında tespit edilen ve dünya genelinde önemli etkiler oluşturan uygulamalardır.

GIT Uygulamaları	Stuxnet	Duqu	Flame	Red October	MiniDuke
İlk Sızma Şekli	Bilinmiyor	MS Word	Bilinmiyor	MS Word, Excel ve Java	PDF
Şifreleme Yöntemleri	Dizi şifreleme	Dizi şifreleme, AES-CBC	Dizi şifreleme, RC4, Substitution	Dizi şifreleme, XOR+ROR	Dizi şifreleme
Kendini Çoğaltma Yöntemi	Taşınabilir medya ile veya ağ üzerinden	El ile	El ile	El ile	El ile
Tespit Edilme Tarihi	Haziran 2010	Eylül 2011	Mayıs 2012	Ekim 2012	Şubat 2013
Hedef / Kurban	İran'daki SCADA sistemleri	İran'daki SCADA sistemleri	Orta Doğu ülkeleri (Devlet kuruluşları, eğitim kurumları...)	Doğu Avrupa, Batı Avrupa bölgeleri... (Hükümetler, bilimsel araştırma merkezleri...)	Almanya, Ukrayna, Portekiz, Türkiye... (Hükümetler, özel şirketler...)
Amaç	Sistemi ele geçirme ve çökertme	Bilgi toplama	Bilgi toplama	Bilgi toplama	Bilgi toplama
Etkileri	Nükleer yakıt tesisine sızarak arızalara sebep olması	SCADA sistemleri ile ilgili kritik bilgilerin tespiti	Bulaştığı çok sayıda bilgisayardan veri sızdırması	Oldukça geniş alanlarda gizli bilgileri toplaması	Bulaştığı çok sayıda bilgisayardan veri sızdırması
Keylogger Özelliği	Hayır	Evet	Evet	Evet	Evet

Tablo 1 - Farklı GIT'lerin karşılaştırılması [9,10]

IV. SONUÇ VE TARTIŞMA

Bu çalışmada, siber dünyada görülen ve siber savaş için kullanılan GIT adını alan uygulamalar incelenmiştir. Bu uygulamaların sahip olduğu çalışma yapıları, oluşturduğu etkiler, gösterdikleri faaliyetler ve tipik özellikleri hakkında farkındalık oluşturulmaya çalışılmıştır. Ele alınan Stuxnet, Duqu, Flame, Red October ve MiniDuke uygulamaları belirlenen özelliklere göre karşılaştırıldığında ortak olan ve farklı olan durumlarla karşılaşılmıştır.

GIT uygulamalarının ilk sızma şekillerine bakıldığında MS Word güvenlik açıklığının Duqu ve Red October uygulamalarında kullanıldığı, Stuxnet ve Flame hakkında kesin bilginin bulunamadığı ve MiniDuke için PDF güvenlik açığının kullanıldığı görülmektedir. Şifreleme yöntemleri olarak XOR algoritmasının ele alınan uygulamalar için ortak olduğu ve buna ek olarak kullanılan şifrelemelerin de olduğu bilinmektedir. Kendi kendine çoğalma becerisine Stuxnet dışındaki uygulamaların sahip olmadığı ve her uygulamanın tespit edilme tarihinin farklı olduğu anlaşılmaktadır. Hedef olarak görülen alanların değişkenlik gösterdiği ve genel olarak devlet kurumlarına ve alt yapı sistemlerine saldırı yapıldığı elde edilen sonuçlar arasında yer almaktadır. Uygulamaların amaçları ve keylogger özelliğine sahip olup olmamaları karşılaştırıldığında ise diğerlerine göre Stuxnet uygulaması farklılık göstermektedir.

Siber saldırıların gelecekte evrensel olarak daha kolay yöntemlerle yapılacağı ve etkilerinin daha da artacağı tahmin edilmektedir. Siber savaş aracı olarak kullanılan GIT'lere karşı tam koruma sağlayabilmek mümkün olamayabilir fakat gerekli önlemlerin alınması ve oluşabilecek etkilerin azaltılması sağlanabilir. Örneğin kurum veya kuruluşlar için doğrudan internete bağlanılmadan önce, kullanılacak ağın denetlenmesi yapılabilir. Güvenilir ve onaylanmış kaynaklar dışındaki kaynaklardan yazılım indirilmesi engellenebilir. Geleneksel korunma yöntemlerinin yeterli kalmadığı durumlar olduğu için yeni nesil çözümler kullanan yazılımlar tercih edilebilir. Çalışanların olduğu kadar bireysel kullanıcıların da bilinçlendirilmesi sağlanabilir. Çok ayrıntılı ve kapsamlı özelliklere sahip olan GIT'ler ile ilgili yapılan çalışmalar arttırılarak ülkemiz için yeni araştırmacıların bu konularda yetiştirilmesi sağlanabilir.

KAYNAKÇA

[1] FireEye Inc., "FireEye Advanced Threat Report: 2013," The FireEye Threat Prevention Platform, Special Report, 2013.

[2] Joint Task Force Transformation Initiative, "Managing Information Security Risk: Organization, Mission, and Information System View," NIST Special Publication, (800-39), 800-39, 2011.

[3] E. M. Hutchins, M. J. Cloppert, ve R. M. Amin, "Intelligence-driven computer network defense informed by analysis of adversary campaigns and intrusion kill chains," Leading Issues in Information Warfare & Security Research, 1, 80, 2011.

[4] P. Chen, L. Desmet, ve C. Huygens, A study on advanced persistent threats. Berlin: Springer-Heidelberg, 2014, pp. 63-72.

[5] Mandiant Research Lab., A.P.T. Exposing One of China's Cyber Espionage Units, 2013.

[6] Bencsáth, B., Pék, G., Buttyán, L., & Felegyhazi, M. (2012). The cousins of stuxnet: Duqu, flame, and gauss. Future Internet, 4, 971-1003.

[7] Faisal, M., & Ibrahim, M. (2012). Stuxnet, Duqu and Beyond. International Journal of Science and Engineering Investigations, 2, 75-78.

[8] Kara, M. (2013). Siber Saldırılar Siber Savaşlar ve Etkileri (Doktora tezi, İstanbul Bilgi Üniversitesi).

[9] Virvilis, N., & Gritzalis, D. (2013, September). The big four-what we did wrong in advanced persistent threat detection?. In Availability, Reliability and Security (ARES), 2013 Eighth International Conference. IEEE.

[10] Adebayo, O. S., & AbdulAziz, N. (2014, November). An intelligence based model for the prevention of advanced cyber-attacks. In Information and Communication Technology for The Muslim World (ICT4M), 2014 The 5th International Conference. IEEE.

[11] CodingUnit Programming Tutorials. (2010, 10 Mart). Exclusive-OR (XOR) Encryption. Erişim Tarihi: 1 Temmuz 2015, http://www.codingunit.com/exclusive-or-xor-encryption.

[12] Wikipedia. (2014, 2 Haziran). XOR Cipher. Erişim Tarihi: 1 Temmuz 2015, https://en.wikipedia.org/wiki/XOR_cipher

[13] Wikipedia. (2015, 5 Mayıs). Drcrypt. Erişim Tarihi: 2 Temmuz 2015, https://tr.wikipedia.org/wiki/Drcrypt

[14] İTÜBİDB. (2013, 7 Eylül). Şifreleme Yöntemleri. Erişim Tarihi: 2 Ağustos 2015, http://bidb.itu.edu.tr/seyirdefteri/blog/2013/09/07/şifreleme-yöntemleri

[15] Cryptography Beta.(2014, 4 Ekim). How is XOR used for encryption? Erişim Tarihi: 2 Temmuz 2015, http://crypto.stackexchange.com/questions/19470/how-is-xor-used-for-encryption

[16] Bencsáth, B., Pék, G., Buttyán, L., & Félegyházi, M. (2012, April). Duqu: Analysis, detection, and lessons learned. In ACM European Workshop on System Security (EuroSec) (Vol. 2012).

[17] Thakur, Vikram. Symantec Official Blog. (2011, 1 Kasım). Duqu: Status Updates Including Installer with Zero-Day Exploit Found. Erişim Tarihi: 20 Temmuz 2015, http://www.symantec.com/connect/w32-duqu_status-updates_installer-zero-day-exploit

[18] Symantec Security Response. W32.Duqu: The precursor to the next Stuxnet. Technical Report Version 1.4, Symantec, 23 Kasım 2011.

[19] NIST, FIPS PUB 197. Advanced Encryption Standard (AES). Kasım 2001.

[20] Dworkin, M. Recommendation for Block Cipher Modes of Operation: Methods and Techniques. NIST Special Publication 800-38A, Aralık 2001.

[21] S. Frankel, R. Glenn, NIST, S. Kelly. Network Working Group. (2003, Eylül). The AES-CBC Cipher Algorithm and Its Use with IPsec. Erişim Tarihi: 3 Temmuz 2015, https://tools.ietf.org/html/rfc3602#section-2.1

[22] sKyWIper Analysis Team. sKyWIper (a.k.a. Flame a.k.a. Flamer): A complex malware for targeted attacks. Technical Report Version 1.05, CrySyS Lab, Budapest University of Technology and Economics Department of Telecommunications, May 31 2012.

[23] Gostev, A. Securelist Official Blog. (2012, 28 Mayıs). The Flame: Questions and Answers. Erişim Tarihi: 26 Haziran 2015, https://www.securelist.com/en/blog/208193522/The_Flame_Questions_and_Answers

[24] K. Avi. Lecture 8: AES: The Advanced Encryption Standard. Lecture Notes on "Computer and Network Security", Purdue University. 1 Mayıs 2015.

[25] Evren, Ş. (2008, 21 Şubat). Yerine Koyma Şifrelemesi (Substitution Cipher). Erişim Tarihi: 1 Ağustos 2015, http://bilgisayarkavramlari.sadievrenseker.com/2008/02/21/yerine-koyma-sifrelemesi-substitution-cipher/

[26] Karataş, A. (2013, 28 Eylül). Şifreleme Algoritmaları. Erişim Tarihi: 20 Haziran 2015, https://adnankaratas.wordpress.com/2013/09/28/sifreleme-alogoritmalari/

[27] Evren, Ş. (2008, 17 Nisan). YRC4 Şifrelemesi (RC4 Cipher, ARC4, ARCFOUR). Erişim Tariihi: 3 Ağustos 2015, http://bilgisayarkavramlari.sadievrenseker.com/2008/04/17/rc4-sifrelemesi-rc4-cipher-arc4-arcfour/

[28] Kaspersky Labs' Global Research & Analysis Team. (14 Ocak 2013). The "Red October" Campaign – An Advanced Cyber Espionage Network Targeting Diplomatic and Government Agencies. GReAT Report. Erişim Tarihi: 28 Mayıs 2015, https://securelist.com/blog/incidents/57647/the-red-october-campaign/

[29] Kaspersky Labs' Global Research & Analysis Team. (14 Ocak 2013). "Red October" Diplomatic Cyber Attacks Investigation. GReAT Report. Erişim Tarihi: 28 Mayıs 2015, https://securelist.com/analysis/publications/36740/red-october-diplomatic-cyber-attacks-investigation/

[30] McAfee Labs. Operation Red October. McAfee Labs Threat Advisory Report, 2013.

[31] Kaspersky Labs' Global Research & Analysis Team. (17 Ocak 2013). "Red October". Detailed Malware Description 1. First Stage of Attack. GReAT Report. Erişim Tarihi: 29 Mayıs 2015, https://securelist.com/analysis/publications/36830/red-october-detailed-malware-description-1-first-stage-of-attack/#1

[32] Kaspersky Labs' Global Research & Analysis Team. (17 Ocak 2013). "Red October". Detailed Malware Description 3. Second Stage of Attack. GReAT Report. Erişim Tarihi: 30 Mayıs 2015, https://securelist.com/analysis/publications/36802/redoctober-detailed-malware-description-3-second-stage-of-attack/

[33] Yliluoma, J. (2014, Ocak). Bit mathematics cookbook. Erişim Tarihi: 20 Temmuz 2015. http://bisqwit.iki.fi/story/howto/bitmath/

[34] Atmel Resmi Websitesi. ROR- Rotate Right through Carry. AVR Assembler Instructions. Erişim Tarihi: 17 Haziran 2015, http://www.atmel.com/webdoc/avrassembler/avrassembler.wb_ROR.html

[35] R. Rivest. Network Working Group. (1998, Mart). A Description of the RC2(r) Encryption Algorithm. Erişim Tarihi: 27 Temmuz 2015, https://www.ietf.org/rfc/rfc2268.txt

[36] Raiu C., Soumenkov I., Baumgartner K., Kamluk V. Global Research and Analysis Team., "The MiniDuke Mystery: PDF 0-day Government Spy Assembler 0x29A Micro Backdoor," Technical Report, Kaspersky Lab, 2013.

[37] Kaspersky Labs' Global Research & Analysis Team. (3 Haziran 2014). Miniduke is back: Nemesis Gemina and the Botgen Studio. GReAT Report. Erişim Tarihi: 11 Haziran 2015, https://securelist.com/blog/incidents/64107/miniduke-is-back-nemesis-gemina-and-the-botgen-studio/

[38] Kaspersky Lab. (27 Şubat 2013). Kaspersky Lab Identifies 'MiniDuke', a New Malicious Program Designed for Spying on Multiple Government Entities and Institutions Across the World. Report. Erişim Tarihi: 11 Haziran 2015, http://www.kaspersky.com/about/news/virus/2013/Kaspersky_Lab_Identifies_MiniDuke_a_New_Malicious_Program_Designed_for_Spying_on_Multiple_Government_Entities_and_Institutions_Across_the_World

[39] CrySyS Malware Intelligence Team, Kaspersky Labs GREAT Team. Miniduke: Indicators. Technical Report Version 1.00, CrySyS Lab, Budapest University of Technology and Economics Department of Telecommunications, 2013.

Esra SÖĞÜT, Eskişehir'de doğdu. İlk, orta ve yüksek öğrenimini Eskişehir'de tamamladı. 2012 yılında Eskişehir Osmangazi Üniversitesi Bilgisayar Mühendisliği Bölümü'nden mezun oldu. Bir yıl sonra, Gazi Üniversitesi Bilgisayar Mühendisliği Anabilim Dalı'nda yüksek lisans eğitimine başladı. 2013 yılında Gazi Üniversitesi Teknoloji Fakültesi Bilgisayar Mühendisliği Bölümü'ne araştırma görevlisi olarak atandı. Halen, Gazi Üniversitesi Teknoloji Fakültesi Bilgisayar Mühendisliği Bölümü'nde araştırma görevlisidir. İlgi alanları: bilgisayar ağları, kötücül yazılımlar.

Prof. Dr. O. Ayhan ERDEM, Ankara'da doğdu. İlk, orta ve yüksek öğrenimini Ankara'da tamamladı. 1989 yılında Gazi Üniversitesi Fen Bilimleri Enstitüsü'nden Yüksek Lisans, 2001 Yılında doktora derecesi aldı. Amerika Birleşik Devletleri, 1990 yılında İndiana Üniversitesinde yoğun İngilizce eğitimini, Purdue Üniversitesinde Bilgisayar Teknolojisi Eğitimini tamamladı. Bilgisayar programlama dilleri, bilgisayar ağları, temel bilgi teknolojileri, bilgisayar sistemleri konularında çok sayıda kitapları, uluslararası ve ulusal dergilerde makaleleri bulunmaktadır. Halen Gazi Üniversitesi Teknoloji Fakültesi, Bilgisayar Mühendisliği Bölümünde Profesör ünvanlı öğretim üyesi olarak çalışmaktadır. Evli ve üç çocuk babasıdır.