Bilgi Yönetimi Dergisi

Cilt: 2 Sayı: 1 Yıl: 2019

https://dergipark.org.tr/by

Hakemli Makaleler
Araştırma Makalesi

Makale Bilgisi

Gönderildiği tarih: 21.03. 2019
Kabul tarihi: 29.05. 2019
Yayınlanma tarihi: 28.06. 2019

Article Info

Date submitted: 21.03.2019
Date accepted: 29.05.2019
Date published: 28.06.2019

Anahtar sözcükler

Siber tehdit, zararlı yazılımlar, uzaktan erişim truva atları (UETA)

Keywords

Cyber threat, malware, remote access trojans (RAT)

DOI numarası

10.33721/by.542743

ORCID

0000-0003-3700-4825

Truva Atı Zararlı Yazılımlarının Tespit, Teknik Analiz ve Çözüm Önerileri

Detection, Technical Analysis and Recommended Solutions of Trojan Horse Malware

İlker KARA

Hacette Üniversitesi Bilişim Enstitüsü Öğretim Görevlisi,
karaikab@gmail.com

Öz

Teknolojik cihazların kullanımı arttıkça kötü niyetli kişiler de bu cihazlara ve kullanıcılarına zarar vermek amacıyla her geçen gün yeni tür zararlı yazılımlar geliştirerek piyasaya sürmektedir. Kişi ve kurumları etkileyen geniş çaplı bu saldırılara karşı tedbirler alınmaya çalışılsa da güvenlik zafiyetleri halen devam etmektedir. Pek çok siber saldırgan, mevcut güvenlik zafiyetlerinden faydalanarak saldırılarını gerçekleştirmek için zararlı yazılımları kullanmaktadır. Kendisini zararsız bir dosya uzantısı altına gizleyerek kurban sisteme sızan Truva Atları son derece tehlikeli bir tür zararlı yazılımdır. Uzak Erişim Truva Atı ise, kurban sisteme sızdıktan sonra saldırgana uzak erişim imkânı sağlamaktadır. Bu sayede saldırgan kurban sistemdeki dosyalara ve kayıtlı şifreleri ulaşabilmekte, kurban sistem üzerine düzenli, koordineli saldırılar yapabilen köle bir sisteme dönüştürebilmektedir. Bu çalışmada, Uzak Erişim Truva Atlarını tanımlayarak, kurban sisteme sızma yöntemleri ve bu tehditte karşı alınabilecek önlemleri açıklayıp kullanıcı farkındalığı yaratması amaçlanmıştır.

Abstract

As the use of technological devices increases, malicious people develop and spread new types of malicious software every day in order to harm these devices and their users. Although security measures are taken against these widespread threats affecting individuals and institutions, the vulnerabilities continue to exist. Many of the cyberattackers uses malware to attack by exploiting existing security vulnerabilities. Trojans are extremely dangerous kind of malicious software that infiltrates the victim system by hiding themselves inside a seemingly harmless file extension. The Remote Access Trojan Horse, however, provides remote access to the attacker after infecting the victim system. In this way, the attacker can access the files and passwords in the system, and convert the victim system into a slave system that can perform regular, coordinated attacks. In this study, it is aimed to define Remote Access Trojans, to explain their methods of infiltration into the victim system and the measures that can be taken against this threat and to raise user awareness.

1. Giriş

İnternetin getirdiği birçok yeniliğin yansıra bir o kadar da ön görülemeyen risklerin ve zararlarının olduğunu zaman içinde görülmüştür. Alınan güvenlik önlemlerine rağmen sanal ortamda kullanıcılar, gizlilik ve güvenlik kaygıları başta olmak üzere çeşitli tehdit ve tehlikelere açık haldedirler. Günümüzde saldırganların en çok tercih ettiği zararlı yazılım türlerinden birisi truva atı saldırılarıdır. İsmini mitolojideki truva atından alan bu zararlı yazılımların en tehlikelisi saldırganın kurban sistemle uzak bağlantı kurmaya olanak tanıyan uzak erişim truva atı (UETA) versiyonudur.

UETA sayesinde saldırgan, mağdurun sistemine (bilgisayar, cep telefonu, kamera veya mikrofon gibi elektronik cihazlara erişimine imkân sağlamasıdır. UETA güvenlik duvarı veya anti virüs gibi uygulamaların çoğunu atlatabilmektedir (Adachi & Omote, 2016). UETA sayesinde saldırgan, mağdurun sistemiyle gerçek zamanlı iletişim kurabilmekte ve sistemde kayıtlı kişisel verilerine erişim sağlayarak, casusluk ya da şantaj gibi amaçlarla kullanabilmektedir.

Otomatik çalışan zararlı yazılımlarının aksine (Spam ve DDoS gibi) UETA'ları, mağdura özel olarak dizayn edilebilmektedir(Wangen, 2015). Sadece basit saldırılar olarak değil, istihbarat örgütleri, aktivist gruplar da UETA'ları şantaj, istihbarat ve casusluk gibi amaçlara kullanabilmektedir (Kara, & Aydos, 2019).

Saldırganın amacına bağlı olarak tasarlanan UETA'ları sisteme sızmak için saldırı türü ve yöntemin de değiştirebilmektedir (Thompson, 2005; Villeneuve, 2011; Saarinen, 2015; Jiang, & Omote, 2015). UETA saldırıları en basit şekilde, mağdurun kamerasının kontrolünden başlayıp, uluslararası istihbarı bilgi toplamaya kadar geniş bir alanda kullanılabilmektedir (Chen, & Delis, 2008; Wang, & Kao, 2007; Thompson, 2005; Emm, vd. 2015; Barabosch, vd. 2017; Smith, & Smith-, 2019; Kaur, vd. 2015).

Bu çalışmada son zamanlarda dünyada ve ülkemizde giderek artan UETA saldırılarına karşı gerek siber güvenlik uzmanları gerekse basit internet kullanıcılar üzerinde farkındalık yaratılmak amaçlanmıştır.

2. Uzaktan Erişim Truva Atlarının Sızma Yöntemleri

Sızdıkları sistemde, saldırganlara sınırsız yetki sağlayan UETA'ları, kullanıcıya ait erişim yetkilerini kullanarak sistemde bulunan birçok önemli verinin kontrolüne saldırganın ulaşmasına imkân sağlamaktadır (Öztürk, 2018). Zararlı yazılım saldırıları hedefli veya hedefsiz olmak üzere iki çeşit yöntemle tasarlanmaktadır. Hedefsiz otomatik siber saldırılar çoğunlukla web tabanlı olduğundan kullanıcıyla etkileşimine gerek duymaktadırlar [Man-in-the-Browser gibi] (Öztürk, 2018; Qamar, Karim, & Chang, 2019; Vinay, & Kok, 2018; Jain, vd. 2014). UETA'larınbu saldırı tipinden farkı olarak, kurban sisteme erişimin sağlanması ve saldırının gerçekleşmesi için sanki kullanıcının kendisi yetki vermiş gibi çalışmaktadır. UETA saldırıları, bazı otoritelerce gerçekleşen en büyük sayıda, uzun süreli ve organize saldırılardan biri olarak görülmektedir (Ma, vd. 2016). UETA'rı sızdıkları sistemde aylarca hatta yıllarca fark edilmeden kalabilmektedir.

UETA saldırısını yakından incelendiğinde, 3 ana safhadan oluştuğu görülmektedir.

1. Aşama: Saldırı yapılacak olan kuruluş seçildikten sonra hedef kuruluşta kritik görev ve yetkilerde çalışan yöneticiler ile ilgili sosyal mühendislik yardımıyla veriler toplanmaktadır. Bu veriler kullanılarak seçilen kurban kişilerin ilgisini çekebilecek konu veya konular tespit edilmektedir. İlk bakışta zararsız gibi görünen içerik olarak da kurban kişinin ilgisini çekecek bir e-posta hazırlanarak hedefe gönderilmektedir. Bu e-posta ekinde Word, Excel ya da PDF uzantılı gibi görünen bir expoit (kötüye kullanım) kodu içeren dosya bulunmaktadır. Bu dosyanın kullanıcı tarafından açıldığı anda kurban sisteme zararlı yazılım sızmaktadır. Bu noktadan sonra kurban sistemde güvenlik açığı oluşmaktadır.

2. Aşama: Kurban sistemde aktif hale gelen UETA, saldırgan tarafından tahrip edilmiş bir internet sitesiyle bağlantı kurmaya çalışmaktadır. Bu internet sitesi saldırganlar tarafından özel olarak tasarlanmış, ilk bakışta sadece basit bir resim veya html sayfaları olarak görülen içeriklerin bulunmaktadır. Bu sayede güvenlik duvarı ya da anti virüs programları tarafından da zararsız olarak algılanmaktadır. UETA, kurban sistemin İnternet Protokolü (IP) adres ve port bilgisi ile uzak erişime açtığı andan itibaren saldırının 3. aşaması başlamaktadır.

3. Aşama: UETA'ları tasarımında belirlenen PORT ve IP'ye bağlanarak 'active' komutunu beklemeye başlamaktadır. Bu aşamadan sonra UETA ve saldırgan arasında 'handshake (tokalaşma)' meydana gelmekte ve bağlantı tamamlanmaktadır. UETA sayesinde IP:PORT komutu ile uzak erişim sağlandığında saldırgan kurban sistem üzerinde komut çalıştırması yetkisi tamamlanmış olmaktadır. Bu aşamadan sonra saldırgan, kurban sistemde kullanıcının haberi olmadan 'shell' komutlarını çalıştırarak istediği bilgiyi erişebilecek duruma gelmektedir. Bu döngü tamamlandığında kurbanların böyle bir olayın farkına varılması oldukça güçtür.

UETA saldırıları hemen her gün karşılaşılan kişisel ve kurumsal anlamda önemli güvenlik sorunları oluşturmaktadır [20]. Takibi zor olan bu siber saldırılardan toplamda kaç kişi veya kuruluşun etkilediğini sonuçlarının neler olduğu hakkında kesin bilgi bulunmamakla beraber saldırının arkasında da kimler olduğu ve ne amaçla yapıldığı da bilinmemektedir (Wangen, 2015).

3. Uzaktan Erişim Truva Atlarına Karşı Alınabilecek Önlemler

Kullanıcının izni olmadan sistemi kontrol etmesine ve kullanıcıya ait bilgilere ulaşmasına olanak sağlayan UETA'ları saldırı şekillerini sürekli gelişmektedir. Birçok anti virüs ve güvenlik duvarları sadece internet ağı katmanında değil diğer ağ katmanda aktif tarama yaparak UETA saldırılara karşı önlem almaya çalışmaktadır. Bu kapsamda dikkat edilmesi gerekenler ise şu şekilde sıralanabilir;

Protokol seviyesinde tespitler: Birçok UETA'ın erişim için 80 Hiper Metin Transfer Protokolü (HTTP) ve 443 Hiper Metin Transfer Protokolü Servisi (HTTPS) portlarını kullanmaktadır. Güvenlik duvarları, bu portları rutin internet kullanımlarında aktif olarak kullanıldığı için UETA'rı saldırganla iletişim halinde iken zararlı trafik tespit edilememektedir. Eğer bu portlar üzerinden HTTP ve HTTPS protokol trafiği haricinde şüpheli bir trafik tespit edilirse bu noktaya dikkat edilmeli, eğer şüpheli bir trafik varsa incelenmesi güvenlik açısından önemlidir.

HTTP başlıkları: HTTP başlıkları üzerinden Uygulama Programları Ara yüzü (API) çağrısı yapan bir trafik normal tarayıcı trafiğinden farklı olduğundan şüphelidir. Eğer sistemde bu tip istekler yapan başlıklar varsa şüpheli olarak değerlendirmeli ve zararlı yazılım olabileceğinden dikkat edilmelidir.

Sıkıştırılmış Arşiv Dosyaları: Saldırganlar, şifre korumalı sıkıştırılmış ".rar" uzantılı dosyalar kurban sistemden genellikle kişisel verileri çalmak için tasarlanmaktadır. Zararlı içeriğinin bulunduğu bu dosya sisteme yüklenip açıldığı anda sızma işlemi gerçekleşmekte ve sistemde bulunan tüm verilerin güvenliği tehlikeye girmektedir. Mevcut anti virüsler ve sandbox'lar (kum havuzu) bu tarz risklere karşı zararsız ".rar" dosyalarına sıklıkla yanlış alarm verse de gerçek bir zararlı yazılımın olması olasılığı nedeniyle mutlaka kontrol edilmelidir.

Zamanlama ve Paket Boyutu: Uzaktan erişim araçları daha büyük bir saldırının sadece başlangıcı olduğu için, belirli aralıklarla yapılan Domain İsim Servisi (DNS) isteklerinde şüpheli bir aktivite olabileceğinden kullanıcı tarafından kontrol edilmelidir. Günümüzde birçok saldırı tipi artık HTTP ve HTTPS protokol üzerinden gerçekleştiği için, yapılan isteklerin zaman aralığı ve boyutlarına bakılarak anlamlı veriler çıkarılabilir. Şüpheli dosya paketlerinin anormal boyutlar ve zaman aralıklarının çok sık olması kullanıcı tarafından yapılan kontrollerde tespit edilebilir.

UETA'nın saldırı tipleri ve senaryoları çeşitlendikçe, alınan tedbirler ve saldırı tespit sistemleri de gelişmektedir. UETA saldırı tespit sistemleri özellikle tehdit istihbaratına (threat intelligence) dayanmaktadır. Bu yöntemde genellikle tespit sistemlerinde yanlış alarm (false positive) olarak adlandırılan uyarılar sıklıkla görülse de güvenlik söz konusu olduğu için her uyarının dikkate alınması gereklidir.

UETA saldırıları, sistemde tespit edilmemek için olağan kullanılan ağ trafiğini tercih etmektedir. Eğer ağ trafiğinde olağan dışı davranışlar varsa dikkate alınmalıdır. Kullanılan güvenlik programların güncel olması olası UETA saldırıları tespit edilebilmesi açısından önemlidir.

4. Örnek Olay İncelemesi

UETA saldırısına uğramış bilgisayarın incelemesi ilk olarak zararlı yazılımın tespitiyle başlamaktadır. Tespit edilen UETA yazılımının karakteristik davranış analizi için yapılan incelemelerde adli bilişim incelemelerinde en çok tercih edilen programlardan "AccessData Forensic Toolkit v6.2.1.10 (FTK)", "Process Explorer", "Wireshark" aracılığıyla gerçekleştirilmiştir. İncelenen örnek gerçek bir siber saldırıdan seçildiğinden tespit edilen bilgiler bulanıklaştırma (gizlenmiş) yapılarak çalışmada sunulmuştur.

İnceleme ilk olarak kurban bilgisayarda son yapılan işlemler araştırılmıştır. Son indirme işlemler incelendiğinde şüpheli bir dosya görülmüştür. Yapılan analizler sonucunda "IMAGE__.001/Partition1/NONAME[NTFS]/[root]/Users/Administer/Downloads/" dizini altında bulunan "NjRat 0.7d Golden Edition C432.zip" isimli dosyanın olduğu tespit edilmiştir.

Şüpheli dosyanın kullanıcı tarafından indirildikten sonra kullanıcıya ait sosyal medya hesaplarınıa (Twitter ve Facebook) ulaşılamadığı daha önceden bilinmektedir. Bu aşamadan sonra tespiti yapılan zararlı yazılıma ait incelemelere başlanmıştır.

İşlem adı	Dosya Bilgileri
Dosya Adı	NjRat 0.7d Golden Edition C432.zip
Oluşturma Tarihi	2018-08-15 14:55:02 UTC
Dosya Boyutu (Byte)	1.9 MB (1987855 bytes
MD5 Doğrulama Değeri	276717364a8dba92604a5f6d63f06370
SHA1 Doğrulama Değeri	1d532635fdb4364fc05675c60da2242103f7b677
Dosya Yolu	IMAGE__.001/Partition 1/NONAME [NTFS]/ [root]/Users/Administer/Desktop/ NjRat 0.7d Golden Edition C432.zip

Tablo 1. Şüpheli Dosya Bilgileri (NjRat 0.7d Golden Edition C432.zip)

FTK ve Process Explorer programları kullanılarak şüpheli "NjRat 0.7d Golden Edition C432.zip" dosyasının statik analizi yapılmıştır (Tablo 1). Tablo 1'deki kod mimarisi incelendiğinde "NjRat 0.7d Golden Edition C432.zip" isimli dosyanın ilk olarak "C:\ Users\Administer\Desktop\" dosyası olarak kendisini yaratma işlemi yapmaktadır. "NjRat 0.7d Golden Edition C432.zip" dosya 1.9 MB boyutuyla dikkat çekmektedir. Şüpheli bir dosya olarak görülen "NjRat 0.7d Golden Edition C432.zip" hakkında bilgi edinmek için incelemeler yapılmıştır. Şüpheli dosya hakkında ilk önce statik analiz yapılmıştır. Statik analizde amaç şüpheli dosya çalıştırılmadan önceki yapısal analizini içermektedir. Statik analiz sayesinde şüpheli dosyanın içerdiği ve daha önce tespit edilmiş olabileceği için internet geçmişine ulaşılabilmektedir.

Tablo 1'de detaylı bilgileri verilen "NjRat 0.7d Golden Edition C432.zip" isimli dosyanın, bünyesinde farklı antivirüs firmalarına ait tarama bilgileri barından "www.virustotal.com" web sayfası üzerinden online sorgulaması yapılmış olup söz konu dosyanın zararlı yazılım olduğu tespit edilmiştir (Tablo 2).

47 firma tarafından tespit edilmiştir.	
MD5 Doğrulama Değeri	276717364a8dba92604a5f6d63f06370
Dosya Adı	NjRat 0.7d Golden Edition C432.zip
Son Analiz	2018-08-15 14:55:02 UTC
Antivirüs	**Sonuç**
AegisLab	Trojan.Win32.Generic.4!c
AhnLab-V3	Spyware/Win32.Keylogger.R205645
ALYac	Gen:Variant.MSILPerseus.75191
Antiy-AVL	Trojan/Win32.TGeneric
Arcabit	Trojan.MSILPerseus.D125B7
Avast	Win32:Malware-gen
AVG	Win32:Malware-gen
Avira (no cloud)	TR/Agent.16384.1079
AVware	Trojan.Win32.Generic!BT
BitDefender	Application.Htool.WJX
Bkav	W32.eHeur.Virus02
AegisLab	Trojan.Win32.Generic.4!c
AhnLab-V3	Spyware/Win32.Keylogger.R205645
ALYac	Gen:Variant.MSILPerseus.75191
Antiy-AVL	Trojan/Win32.TGeneric
Arcabit	Trojan.MSILPerseus.D125B7
Avast	Win32:Malware-gen
AVG	Win32:Malware-gen

Tablo 2. www.virüstotal.com Web Adresi Üzerinden Yapılan Sorgulama Sonuç Örneği

Statik analiz aşaması tamamlandıktan sonra zararlı yazılımın özelliklerini, hareket kabiliyetini, aktivitesini ve kapasitesini tam olarak görebilmek için dinamik analiz yapılmıştır. Dinamik analiz, zararlı yazılım çalıştırıldıktan sonra IP trafiği ve ağ aktivitelerinin analiz yapılmasına imkân sağlamaktadır (Tablo 3).

No	Zaman	Kaynak	Hedef	Protokol	Uzunluk	Bilgi
1	2912390	192.168.0.2	186.22.56.64	TCP	66	Standard query A xfbdc: A vipfelfegpx7gb..ru
2	2912359	192.168.0.2	224.0.0.22	TCP	62	Standard query A xfbdc: youndatamyda. ru
3	0445560	192.168.0.1	186.22.56.64	TCP	66	Standard query A xfbdc: youndatamydata. ru
4	0486522	192.168.0.2	192.168.0.2	DNS	66	Standard query A Bgsa
5	2261156	192.168.0.2	192.168.0.2	DNS	66	Standard query A Bgsa
6	2261284	192.168.0.2	186.22.56.64	TCP	66	Standard query A xfbdc: youndatamydata. ru

Tablo 3. "NjRat 0.7d Golden Edition C432.zip" Zararlı Yazlımın Wireshark Programı İle Yapılan Network (Ağ) Hareketleri

"NjRat 0.7d Golden Edition C432.zip" dosyası "Wireshark" programıyla zararlı yazılımın ağ hareketleri incelenmiştir. Wireshark programı ile yapılan incelemelerde "NjRat 0.7d Golden Edition C432.zip" zararlı yazılımın ağ hareketleri incelendiğinde saldırganla iletişime geçtiği görülmüştür. Bu aşamadan sonra saldırgan hedef sistemde erişim sağladığı tespit edilmiştir. Saldırgan, tespit edilmemek ve kendini gizlemek için arkasında iz bırakmamaktadır. Bu çalışmada yapılan incelemelerde saldırgana ait Whois (sahip olunan alan adının ya da IP adres bilgilerini gösteren kayıtlar) bilgilerine ulaşılabileceği görülmüştür (Tablo 3).

5. Sonuç ve Öneriler

UETA saldırıları diğer siber saldırılardan ayıran en önemli özelliği mağdurun kullanmakta olduğu sisteme özel olarak tasarlanması ve geleneksel antivirüs veya sandbox gibi programlar ile tespit edilmesinin zorluğudur. Saldırıya uğramış sistemde bulunan UETA'ları mağdura fark ettirmeden saldırgana hizmet etmektedir. Saldırgan, UETA yardımıyla sızdıkları sistemlerde kayıtlı verileri görüntüleme, dosya alma-gönderme-silme gibi işlemler dâhil birçok işlemleri yapabilmelerine olanak sağlamaktadır.

UETA saldırılarına karşı yapılan akademik çalışmalar genellikle teorik çalışmalar olmakla beraber tespit ve analiz boyutu zayıf kalmıştır. Bu çalışmada UETA'larının, kurban sisteme sızma yöntemleri ve bu tehditte karşı alınabilecek önlemleri açıklayarak en güncel UETA saldırısı örnek olay incelerek zararlı yazılımın tespiti, teknik analizi ve çözüm önerileri sunulmuştur. Yapılan analizler sonucunda saldırgana ait bilgilerinin izinin sürülebilir olduğu gösterilmiştir. Çalışma bu sonuçlarıyla gelecekte olabilecek muhtemel saldırılara karşı alınabilecek güvenlik önlemlerinin geliştirilmesinde ve kullanıcı farkındalığı oluşturması açısından önemlidir.

Kaynakça

Adachi, D., ve Omote, K. (2016). A host-based detection method of remote access trojan in the early stage. *In International Conference on Information Security Practice and Experience* (s. 110-121). Springer, Cham.

Barabosch, T., Bergmann, N., Dombeck, A., ve Padilla, E. (2017). Quincy: Detecting host-based code injection attacks in memory dumps. *In International Conference on Detection of Intrusions and Malware, and Vulnerability Assessment* (s. 209-229). Springer, Cham.

Chen, Z., Wei, P. ve Delis, A. (2008). Catching remote administration trojans (RATs). *Software: Practice and Experience*, 38(7), 667-703.

Emm, D., Garnaeva, M., Ivanov, A., Makrushin, D. ve Unuchek, R. (2015). *IT threat evolution in Q2 2015*. Moscow, 125212, Russian Federation: Kaspersky Lab HQ.

Jain, N., Stiller, B., Khan, I., Makarov, V., Marquardt, C. ve Leuchs, G. (2014). Risk analysis of Trojan-horse attacks on practical quantum key distribution systems. *IEEE Journal of Selected Topics in Quantum Electronics*, 21(3), 168-177.

Jiang, D. ve Omote, K. (2015, March). An approach to detect remote access trojan in the early stage of communication. *In 2015 IEEE 29th International Conference on Advanced Information Networking and Applications* (pp. 706-713). IEEE.

Kara, İ. (2018). Teslacrypt fidye yazilim virüsünün tespiti, teknik analizi ve çözümü. *Uluslararası Yönetim Bilişim Sistemleri ve Bilgisayar Bilimleri Dergisi*, 2(2), 87-94.

Kara, İ., ve Aydos, M. (2019). The ghost in the system: Techical analysis of remote access Trojan. *International Journal on Information Technologies & Security*, 11(1).

Kaur, R., Nagpal, E. S., ve Chamotra, S. (2015, December). Malicious traffic detection in a private organizational network using honeynet system. *In 2015 Annual IEEE India Conference (INDICON)* (s. 1-6). IEEE.

Ma, H. X., Bao, W. S., Li, H. W., ve Chou, C. (2016). Quantum hacking of two-way continuous-variable quantum key distribution using Trojan-horse attack. *Chinese Physics B.* 25(8), 080309.

Öztürk, M. S. (2018). Siber saldırılar, siber güvenlik denetimleri ve bütüncül bir denetim modeli önerisi. *Muhasebe ve Vergi Uygulamaları Dergisi,* 208-232.

Saarinen, M. J. O. (2013, November). Developing a grey hat C2 and RAT for APT security training and assessment. *In GreHack 2013 Hacking Conference* (Vol. 15).

Smith-Ditizio, A. A. ve Smith, A. D. (2019). Computer fraud challenges and ıts legal ımplications. ın advanced methodologies and technologies in system security, *Information Privacy, and Forensics* (s. 152-165). IGI Global.

Thompson, R. (2005). Why spyware poses multiple threats to security. Communications of the ACM, 48(8), 41-43.

Villeneuve, N. (2011). Trends in targeted attacks. *Trend Micro*.(October).

Qamar, A., Karim, A., ve Chang, V. (2019). Mobile malware attacks: Review, taxonomy & future directions. *Future Generation Computer Systems*.

Vinay, S. E., ve Kok, P. (2018). Extended analysis of the Trojan-horse attack in quantum key distribution. *Physical Review A*. 97(4), 042335.

Wang, S. J., ve Kao, D. Y. (2007). Internet forensics on the basis of evidence gathering with Peep attacks. *Computer Standards & Interfaces,* 29(4), 423-429.

Wangen, G. (2015). The role of malware in reported cyber espionage: a review of the impact and mechanism. *Information*, 6(2), 183-211.