WEB SAYFASI HACKLEME(HACKİNG) SALDIRILARI

İlker KARA[1]

ÖZET

Modern dünyanın alt yapısını oluşturan internet, toplumun her seviyesinde karşılık bulmakta ve kullanıcılar hayatını kolaylaştırmaktadır. Fakat bu sanal dünya birçok riskleri de barındırmaktadır. Kötü niyetli kişiler amaçlarına ulaşmak için internetti kullanmaktadır. Günümüzde bu siber saldırılar web hizmetlerine yoğunlaşmaktadır. Web sayfaları, kişi ya da ticari işletmeler ürünlerini sergilediği, pazarladığı ve bilgilendirdiği kamu kuruluşları ise online uygulama ve hizmetlerini sergilemektedir. Literatürde, web hizmetlerine yönelik siber saldırılar hakkında teorik çalışmalar yapılmış olsa da bu saldırıların tespiti ve teknik analizi boyutu hakkında çalışmalar sınırlı sayıdadır. Bu çalışmada web hizmetlerini hackleme yöntemiyle yapılmış gerçek bir saldırı örneği tespiti ve teknik analizi detaylı olarak incelenmiştir. Gerçek saldırıların tespit ve analizi olası benzer saldırıların önlenmesinde önemli rol oynayacaktır.

Anahtar Kelimeler: Web, Hackleme, Saldırı Tespit ve Analizi.

WEB PAGE HACKING ATTACKS

As it forms the information infrastructure of the modern world, the Internet is adopted at all levels of society, making the lives of users easier. However, this virtual world holds many risks. Malicious people use the Internet to achieve their goals. Today, these cyberattacks concentrate on the web services. In web pages, individuals or commercial enterprises display their products, market and information, whereas public organizations display their online applications and services. Although there are theoretical studies in the literature on cyberattacks against web services, studies on the detection and technical analysis of these attacks are limited. In this study, the detection and technical analysis of an actual attack, carried out by hacking web services, was investigated in detail. Detection and analysis of actual attacks will play an important role in preventing potential similar attacks.

Keywords: Web, Hacking, Attacks Detection and Analysis.

[1] karaikab@gmail.com

GİRİŞ

Hack saldırıları, saldırganın hedef sistemde olası açıkları bularak, sistemi kendi çıkarları için kullanmasına denilmektedir [1]. Hackleme kurban sistemin yavaşlatabilir, sistemden verileri çalabilir, kullanıcıları takip edebilir ya da sistemi tamamen kullanılmaz hale getirebilmektedir. Saldırıyı gerçekleştiren kişiye ise hacker denilmektedir [2]. Hackleme saldırıları zaman içerisinde farklı amaçlar için yeni metotlar geliştirmişlerdir.

Saldırı türleri genel olarak iki başlık altında toplanabilmektedir [3]. Bunlar;

a) Fiziksel Saldırılar: Hedef sistemlere internet ortamı olmaksızın bluetooth, iletim kablosu gibi araçlar ile yapılan saldırılara denilmekledir. Bu yöntem ile hedef sisteme iletişim kurularak zarar vermek amaçlanmaktadır. Bu saldırı yönteminde saldırgan hedef sistemlere temas kuracak kadar yakın olmak zorundadır.

b) İnternet Tabanlı Sanal Saldırılar: İnternet tabanlı yapılan bu saldırılarda saldırgan hedef sisteme saldırmak için mekân sınırı olmaksızın internette bağlı olması yeterli olmaktadır. Bu amaçla hedef sistem doğrudan veya dolaylı olarak hedef alınarak amacına ulaşmaktadır. İnternet tabanlı sanal saldırılar fiziksel saldırılara göre daha avantajlı olması nedeniyle saldırganlar tarafından daha çok tercih edilmekte ve bu amaç için geliştirilmiş birçok yöntem bulunmaktadır. Bu yöntemlerden en çok tercih edilenleri şunlardır:

Zararlı Yazılım Saldırıları: Saldırganlar amaçları doğrultusunda birçok zararlı yazılım saldırıları türü tasarlamışlardır [4-7]. En çok bilinen türleri şunlardır:

- **Keylogger**: Klavyede hareketlerini kaydedilen ve belirli aralıklarla saldırgana e-posta ile göndermek üzerine tasarlanmışlardır.
- **Adware:** Kullanıcıya ekranında zorla reklam gösteren zararlı yazılımdır. Tek başına zararlı yazılım olarak tanımlanmasa da istenirse farklı zararlı yazılımlara dönüştürülebilmektedir.
- **Virüsler:** Hedef sisteme bulaştıktan sonra sistemde bulunan dosyaları silmek ya da sistemin tamamen çalışmasını engellemek için tasarlanmışlardır.
- **Bot:** Hedef sistemi saldırgan tarafından kullanılmasını ya da belirli bir işlemi yapmasına imkân sağlayan zararlı yazılımlardır.
- **Truva Atları:** Adını mitolojideki gizli saldırıdan alan bu zararlı yazılım, hedef sisteme sızdıktan sonra saldırganın sisteme ulaşması için bağlantı kurmasını sağlamaktadır.
- **Solucanlar:** Virüslerden farklı olarak kendilerini başka sistemeler bulaştırabilmekte hedef sistemlere zarar vermek için tasarlanmışlardır.
- **Fidye Yazılımlar:** Saldırganın kullanıcılardan fidye alabilmek için bulaştığı sistemde dosyaları ya da sistemi şifreleyerek kullanılmaz hale getiren zararlı yazılımlardır.

XSS (Cross Site Scripting- Siteler Arası Betik) Saldırıları: Web sayfalarına yönelik bu saldırı türünde saldırgan önceden tahrip edilmiş bir web sayfası sayesinde saldırılarını gerçekleştirmektedir [8-10]. Bu web sayfasını ziyaret eden kullanıcıların sistemlerine XSS zararlı kodlar ile sızmakta ve hedef sistemdeki kayıtlı şifre ve parola elde etmeyi amaçlamaktadır.

Phishing (Oltalama) Saldırıları: Saldırgan tarafından tahrip edilmiş bir web sayfası, zararlı yazılım içeren bir e-posta ya da paylaşım sitelerinden indirilen bir program aracılığıyla hedef sisteme sızmakta ve sistemde bulunan dosyaları veya kayıtlı şifreleri (bankacılık işlemleri, sosyal medya hesapları gibi) ele geçirmek için kullanılmaktadır [10-11].

SQL (Yapısal Sorgulama Dili) Enjeksiyon Saldırıları: Web sistemlerine yönelik düzenlenen bu saldırılar web sitesini tahrip etmek, içerilerine zararlı kodlar veya içerikler yüklemek için yaygın olarak kullanılmaktadır [12]. SQL enjeksiyon yöntemi oldukça basit ve etkili bir yöntem olması nedeniyle sıklıkla tercih edilmektedir [13-14].

ÖRNEK OLAY İNCELEMESİ

Web sitelerine yönelik hackleme saldırıları için saldırganlar sürekli yeni yöntemler geliştirmeye devam etmekle beraber bu yöntemlerde temel amaç hedef web sitesinde bulunan açıkları tespit edip bu açıklardan faydalanarak hackleme saldırıları yapmaktır. Bu çalışmada web sitesine gerçek bir saldırı örneği seçilerek tespiti

ve teknik analizi detaylı incelenmiştir. Seçilen örnekte hacker kurumsal web sitesini ele geçirerek kurumda çalışanlara sahte e-postalar göndermiştir.

Tespit ve teknik analizler için ilk adım olarak kurban web sitesinin sunucu bilgisayarının adli kopyası alınmıştır. Gerçek sunucu üzerinde yapılacak işlemler tahrip olması, değiştirilme ve verilerin silinmesi gibi olası riskleri içermesinde dolayı tüm analizler adli kopya üzerinde yapılmıştır. İncelemelerde, adli kopya alma işlemi FTK Imager (Free version) analizler ise, "AccessData Forensic Toolkit Version:7.0.0.163 ve FormosaAuditor" programları kullanılmıştır.

Tablo 1. Cihaz Bilgileri

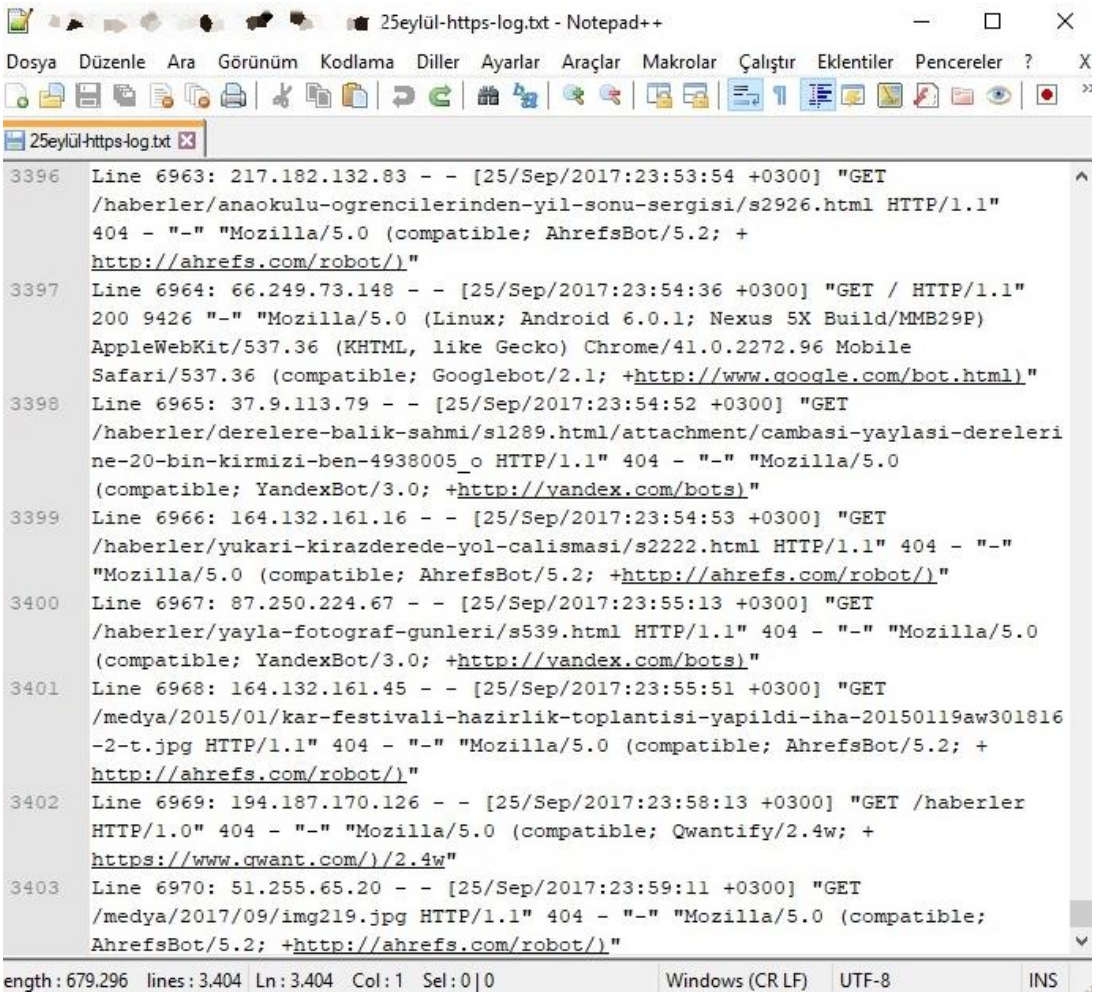
Açıklama	Physical Disk, 1.432.112.128 Sectors 764,3 GB
Toplam Kapasite	1.0234.340.306.404 Bytes (764,3 GB)
Toplam Sektör	1.432.112.128
MD5 Değeri	4eddfece650173e8c6174ac3a69b94dff2
MD5 Doğrulama	4eddfece650173e8c6174ac3a69b94dff2
SHA1 Değeri	2124b3bf5b fd83a6ee04b5aa65c42459b83a6e
SHA1 Doğrulama	2124b3bf5b fd83a6ee04b5aa65c42459b83a6e

Tespit için hedef bilgisayarın son kullanım tarihlerindeki internet geçmişlerini ve şüpheli işlemleri incelemek için log kayıt dosyaları analiz edilmiştir.

Tablo 2. Log Kayıt Dosyaları.

No	Adı	Dosya boyutu	Hash (Doğrulama) Değeri
1	24eylül-http-log.txt	167 KB (173.939 bayt)	24304f5a7c8a9b0f9a9c3c8a1b7ae3b2
2	24eylül-https-log.txt	732 KB (751.153 bayt)	ae6e7c2e5c0f1a5ec3b8e0a16ae6c1b3
3	25eylül-http-log.txt	239 KB (251.591 bayt)	16ff6ef0a2b3c45ae7f5a3e41c1a8ec3c
4	25eylül-https-log.txt	543 KB (579.074 bayt)	4e59e1b4c5a2e8e1ce9e0ff2ec7a3bbe4

Tablo2'de teknik bilgileri verilmiş olan log dosyalarından "25eylül-https-log.txt" isimli log dosyası üzerinde yapılan incelemelerde şüpheli işlemleri rastlanmış olup analizler bu dosya üzerine yoğunlaşırmıştır. "25eylül-https-log.txt" isimli log dosyasına ait analiz sonuçları Şekil1'de verilmiştir.



Şekil 1. "25eylül-https-log.txt" isimli log dosyasına ait analiz sonuçları.

"25eylül-https-log.txt" isimli log dosyası üzerinde yapılan analizlerde web sayfaları üzerinde açıklık(zafiyet) tespit etmeye için kullanılan "FormosaAuditor" isimli yazılım kullanıldığı görülmüştür (Şekil 2). "FormosaAuditor" isimli yazılım hedef web sayfasında tespit edilen açıklıkları kullanarak verileri hackleme eyleminde kullanılmaktadır.

Şekil 2. Hackleme eyleminde kullanılan "FormosaAuditor" isimli yazılım tespiti.

Hedef web sayfasının hackleme eylemi tespit edildikten sonra yapılan hackleme eylemin detaylı inceleme aşamasına geçilmiştir. Saldırgan web sayfasını ele geçirdikten sonra kayıtlı kurumsal e-posta servisini kullanarak kurumda çalışan kullanıcılara sahte mailler göndermiştir (Şekil 3).

```
Line 3[redacted].229 - - [25/Sep[redacted]:00:18:05 +0300] "GET /mesajlar/belediye-baskani-
bayram-mesaji/s6[redacted].html HTTP/1.1" 200 [redacted]
"http://r.search.yahoo.com/_ylt=A9mSs2zjIMhZy0sAHAIpHBg5;_ylu=X3oDMTByZzJoOXByBGNvbG8DaXIyB
HBvc[redacted]--/RV=2/RE=[redacted]4/RO=10/RU=http%3a%2f%2fwww.[redacted]bel.tr
%2fmesajlar%2fbelediye-baskani-bayram-mesaji
```

Şekil 3. Saldırgan göndermiş olduğu sahte e-posta mesajları.

Saldırgana ait bilgileri tespit etmek için yapılan incelemelerde saldırganın kullanmış olduğu "nick name" ve hackleme eyleminin yapıldığı bilgisayarın IP(İnternet Portokol) tespiti üzerine yoğunlaşırmıştır. İncelemeler sonucunda saldırganın kullandığı "nick name" ve IP adresi tespit edilmiştir (Şekil 4).

```
19  Line 3586: [redacted] - - [25/Sep/2[redacted]:00:15:40 +0300] "GET
    /xampp/lang.php?Hacked_bY_KkKl[redacted] HTTP/1.0" 200 2655 "-" "Mozilla/4.0 (compatible; MSIE
    8.0; Windows NT 6.1) FormosaAuditor"
20  Line 3587: [redacted] - - [25/Sep/20[redacted]:00:15:40 +0300] "GET
    /security/lang.php?Hacked_bY_KkKl[redacted] HTTP/1.0" 200 2655 "-" "Mozilla/4.0 (compatible; MSIE
    8.0; Windows NT 6.1) FormosaAuditor"
```

Şekil 4. Hackleme eylemini yapan saldırgana ait "nick name" ve IP adresinin tespiti.

Web sayfasını hackleme eyleminde bulunduğu anlaşılan şüpheliye ait "9.19X.XX.XXX" numaralı IP adresinin WHOIS (Kayıtlı Alan Adı ya da IP adresinin sahiplik bilgileri kayıtları) sorgusu www.domaintools.com web sayfası üzerinden sorgulanmıştır. Sorgulama sonucunda saldırgana ait yer ve kullanıcı bilgilerine tespit edilmiştir (Şekil 5).

Şekil 5. Hackleme eylemini yapan saldırgana ait yer ve kullanıcı bilgilerine tespiti.

SONUÇLAR VE DEĞERLENDİRME

Web hizmetleri sayesinde kullanıcılar birçok hizmete kolaylıkla ulaşabilmektedir. Bu sonuç saldırganlarında ilgisini çekmekte ve kendi çıkarları için kullanmak istemektedir. Web sayfalarının barındırdıkları güvenlik açıklarını (yazılım hataları, bağlanılan ağlar ve yer güvenlik zafiyetleri gibi) saldırganlar hedef almakta ve çeşitli saldırı yöntemleriyle bu hizmetleri sabote etmektedirler.

Web hackleme saldırıları saldırganın ego tatmininden uluslararası bir silah olarak geniş bir uygulama alanında kullanılmaktadır. Web hackleme saldırılarına karşı alınabilecek tedbirler yazılım tabanlıdır. Başlıca alınacak önlemler şunlardır:

- Web sayfaları oluşturulurken güvenlik açıkları bırakmamak için güncel sızma testlerinin periyodik olarak yapılması
- Tespit edilen güvenlik açıkların kapatılması için gerekli çalışmaların yapılması
- Sunucu bilgisayarlarda kullanılan işletim sistemi, ofis programları ve kullanılan programların güncel ve lisanslı olması
- Zararlı yazılımların tehditlinden korunmak için güncel bir anti virüs ya da sandbox programların kullanılması
- Arama motorlarında tahrip edilmiş olan web sitelerin IP adreslerini engelleyecek filtre kullanmak

Bu ve benzeri önlemleri alarak olası web hackleme saldırılarında tam olarak korunmamakla birlikte farkındalık oluşturması açısından önemlidir. Bu çalışmada web hackleme saldırılarıyla ilgili detaylı bilgi verildikten sonra gerçek bir web hackleme saldırısı tespiti ve teknik analizi detaylı analizleri gerçekleştirilmiştir. Çalışma bu açıdan olası web hackleme saldırıların önlenmesi ve kullanıcılarda farkındalık oluşturulması beklenmektedir.

KAYNAKLAR

[1]. Lévesque, Fanny Lalonde, et al. "Technological and Human Factors of Malware Attacks: A Computer Security
Clinical Trial Approach." ACM Transactions on Privacy and Security (TOPS) 21.4 (2018):18.

[2]. Young, Adam L., and Moti Yung. "Cryptovirology: The birth, neglect, and explosion of ransomware." Communications of the ACM 60.7 (2017): 24-26.

[3]. Nakamura, Yoshitaka, et al. "Classification of unknown web sites based on yearly changes of distribution information of malicious IP addresses." New Technologies, Mobility and Security (NTMS), 2018 9th International Conference on IFIP, IEEE, 2018.

[4]. Canbek, Gürol, ve Şeref Sağıroğlu. "Casus Yazılımlar: Bulaşma Yöntemleri Ve Önlemler." Gazi Üniversitesi Mühendislik-Mimarlık Fakültesi Dergisi 23:1 (2008).

[5]. Kara, İ., & Aydos, M. (2019). The ghost in the system: technical analysis of remote access trojan. International Journal on Information Technologies & Security, 11(1).

[6]. Richardson, Ronny, and Max North. "Ransomware: Evolution, mitigation and prevention." International Management Review 13.1 (2017): 10-21.

[7]. Aurangzeb, Sana, et al. "Ransomware: A Survey and Trends." Journal of Information Assurance & Security 6(2) (2017).

[8]. Bulazel, Alexei, and Bülent Yener. "A Survey On Automated Dynamic Malware Analysis Evasion and Counter-Evasion: PC, Mobile, and Web." Proceedings of the 1st Reversing and Offensive-oriented Trends Symposium. ACM, 2017.

[9]. Aneja, Leesha, and Sakshi Babbar. "Research Trends in Malware Detection on Android Devices." International Conference on Recent Developments in Science, Engineering and Technology. Springer, Singapore, 2017.

[10]. Aurangzeb, S., Aleem, M., Iqbal, M. A., & Islam, M. A. (2017). Ransomware: A Survey and Trends. Journal of Information Assurance & Security, 6(2).

[11]. Kara, İ. Kaba Kuvvet Saldırı Tespiti ve Teknik Analizi. Sakarya University Journal of Computer and Information Sciences, 2(2) (2019): 61-69.

[12]. Hartmann, B., Doorley, S., & Klemmer, S. R. Hacking, mashing, gluing: Understanding opportunistic design. IEEE Pervasive Computing, 7(3) (2008): 46-54.

[13]. Ford, R., & Ray, H. Googling for gold: Web crawlers, hacking and defense explained. Network Security, (1) 2004: 10-13.

[14]. Álvarez, G., & Petrović, S. A new taxonomy of web attacks suitable for efficient encoding. Computers & Security, 22(5) (2003): 435-449.