SAKARYA UNIVERSITY JOURNAL OF COMPUTER AND INFORMATION SCIENCES
VOL. 2, NO. 2, AUGUST 2019
DOI: 10.35377/saucis.02.02.561844

Detection, Technical Analysis of Brute Force Attack

İlker KARA[1]
[1]Hacettepe Üniversitesi, Bilişim Enstitüsü;
https://orcid.org/0000-0003-3700-4825;
karaikab@gmail.com, +90 312 297 71 93

Received 8 May 2019; Revised 10 July 2019; Accepted 11 July 2019; Published online 29 August 2019

Abstract

Brute force attack is the most frequently used cyberattack tool to break passwords stored in the target system (such as computer user information, credit card information, social account information, corporate information). Brute force attacks are simple and reliable. Therefore, they are widely used. The majority of the studies on the brute force attacks is theoretical and weak in practice. In this study, the detection and analysis of a real brute force attack against a computer used by a senior manager working in an official institution was performed. According to the research findings, the study is of importance in creating user awareness against similar attacks.

Keywords: Brute Force Attack, Cyber security, Attack Detection and Analysis Method.

Kaba Kuvvet Saldırı Tespiti ve Teknik Analizi

Öz

Kaba kuvvet saldırıları, hedef sistemde kayıtlı şifre ve parolaları (bilgisayar kullanıcı bilgileri, kayıtlı kredi kartı bilgiler, sosyal hesap bilgileri, kurumsal bilgiler gibi) kırmak için en sık tercih edilen siber saldırı aracıdır. Kaba kuvvet saldırıları basit ve güvenilirdir. Bu nedenle geniş bir alanda kullanılmaktadır. Kaba kuvvet saldırıları yönelik yapılan çalışmaların büyük bir kısmı teorik ağırlıklı olup uygulama yönünden zayıf kalmaktadır. Bu çalışmada, resmi kurumda çalışan üst düzey yöneticinin kullandığı bilgisayara karşı yapılan gerçek bir kaba kuvvet saldırısının tespiti ve analizi yapılmıştır. Çalışma sonuçları itibari ile benzer saldırılara karşı kullanıcı farkındalığı yaratması açısından önemlidir.

Anahtar Kelimeler: Kaba kuvvet saldırıları, Siber güvenlik, Saldırı Tespit ve Analizi Metodu.

1. Giriş

Saldırı kavramı insanlık tarihi kadar eskiye dayanmaktadır. Saldırı; en genel haliyle yıpratmak, zarar vermek kullanılmaz hale getirmek veya yok etmek gibi amaçlarla birine veya bir hedefe karşı amaçlı olarak yapılan eylemlerdir [1]. Gelişen teknoloji saldırı şekillerini de kökten değiştirmiştir. Teknolojik ilerlemelerin bir sonucu olarak siber atak (saldırı) kavramı ortaya çıkmıştır [2]. Günümüzde çok önemli bir kavram olarak görülen siber saldırılar sahip olduğu yüksek potansiyeli nedeniyle gelecekte de önemi giderek artacaktır [3].

İnternet ağı üzerinden; sisteme zarar vermek, sistemlerin yavaşlatma, kullanılmaz hale getirmek ya da veri çalmak için yapılan faaliyetlere siber saldırı olarak tanımlanmaktadır. Siber saldırılar, sanal dünyanın en tehlike silahı olarak görülmektedir. Siber saldırılar genel olarak [4];

- Devletlerarası Terörizm,
- Ticari ve Sanayi Casusluğu,
- İstihbarat Amaçlı Casusluk,
- Veri Hırsızlığı,
- Sistemleri Tamamen Kullanılmaz Hale Getirmek,
- Fidye Amaçlı,
- Ego Tatmini (Meşhur Olmak),
- Hedefsiz Saldırılar,

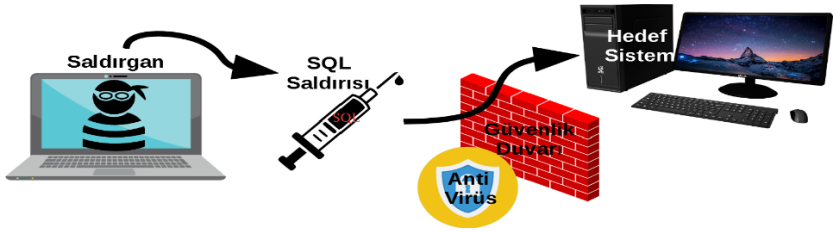
amaçlarıyla yapılmaktadır.

2. Siber Saldırı Şekilleri

Siber saldırı çok fazla türü olmakla beraber temel olarak sekiz grupta toplanabilir. Bunlar:

2.1 SQL İnjection(Structured Query Language, Yapılandırılmış Sorgu Dili) Saldırısı

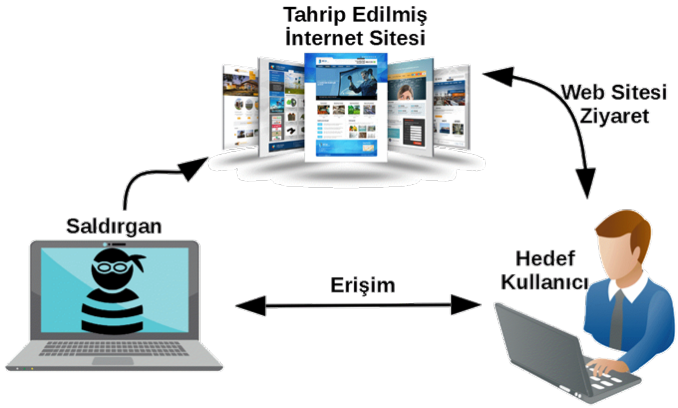
Hedef sistemin kullandığı işletim sistemine sızmak amacıyla yapılan siber saldırılardır [5]. Saldırı başarılı olduğunda saldırgan bilgisayarın tüm yetkilerine ulaşma imkânı bulmaktadır (Şekil 1).



Şekil 1 SQL Saldırı Algoritması

2.2 XSS (Cross site scripting, Çapraz Site Betik) Saldırısı

Genellikle saldırgan tarafından tahrip edilmiş bir internet sitesi ziyaret edildiğinde hedef bilgisayara sızan XSS zararlı kodlar ile hedef sistemde kayıtlı şifre ve parolara ulaşmak için yapılan siber saldırı türüdür [6].

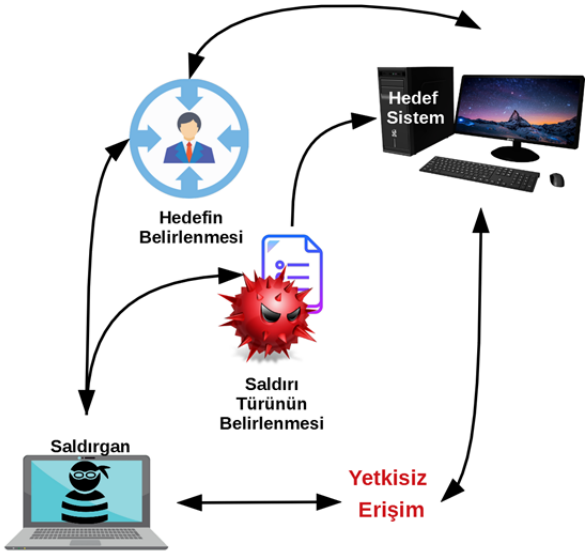


Şekil 2 XSS Saldırı Algoritması

2.3 Kaba Kuvvet (Brute Force) Saldırısı

Kaba kuvvet saldırısında amaç hedef sistem üzerinde “Administrator” (Yönetici) yetkisine erişim sağlamaktır [7]. Administrator yetkisi, bilgisayarda bulunan tüm özel ayarları görebilir ve istediği dosyalara tam erişim sağlayabilmektedir. Saldırgan, hedef bilgisayara uzak erişim sağlayabilmesi için başarılı bir kaba kuvvet saldırısı gerçekleştirmesi gerekir. Uzak erişim sadece saldırgan ile iletişime geçmek dışında birçok faaliyetleri yapabilmesine imkân sağlayabilmektedir [8]. Bunlar; dosya veya klasörleri paylaşıma açarak iletimi sağlayabilir. Saldırgana erişim izni vererek kamera, fare veya klavye gibi araçları kontrol edebilir [9].

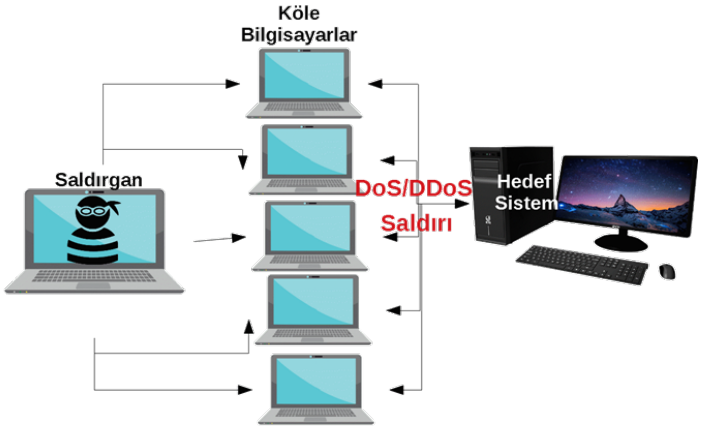
Administrator parola ile korunuyorsa Kaba kuvvet saldırısıyla bu şifrenin kırılması gereklidir. Bu amaç için daha önceden hazırlanmış sayılar, harfler ve özel karakterler bulunan bir "Pass List " hazırlanır [10]. Şifreye ulaşmak için denemeler yapılır ve doğru şifreyi bulunduğu anda Kaba kuvvet saldırı işlemi durulmaktadır.



Şekil 3 Kaba Kuvvet (Brute Force) Saldırı Algoritması

2.4 DoS/DDoS (Distributed Denial of Service, Dağıtık Hizmet Aksatma) Saldırısı

DoS/DDoS saldırısı önceden belirlenmiş hedef bilgisayar ve kullandığı ağları adım adım yavaşlatma ve tamamen kullanılmaz hale getirmeyi amaçlamaktadır [11]. İlk zamanlar DoS (Denial of Service, Hizmet Aksatma), sadece tek bir kaynaktan hedefe saldırı yapılırken günümüzde aynı anda birden fazla kaynaktan(DDos) hedef bilgisayar ve ağlarına saldırılar gerçekleştirilmektedir [12].

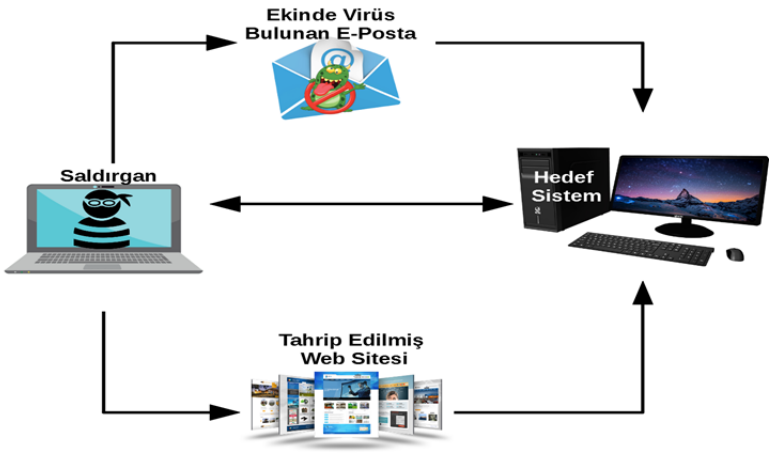


Şekil 4 DoS/DDoS Saldırı Algoritması

2.5 Phishing (Oltalama/Yemleme) Saldırıları

Phishing saldırıları, Virüs, Truva atı, Arka kapı Trojeni, fidye yazılım gibi zararlı yazılımlar aracılığıyla kullanıcıya ait banka şifreleri, kredi kartı bilgileri ya da kişisel dosyalarına ulaşmak için yapılan siber saldırılardır [13]. Phishing saldırıları, önceden tahrip edilmiş bir web sitesi, lisanssız kullanılan

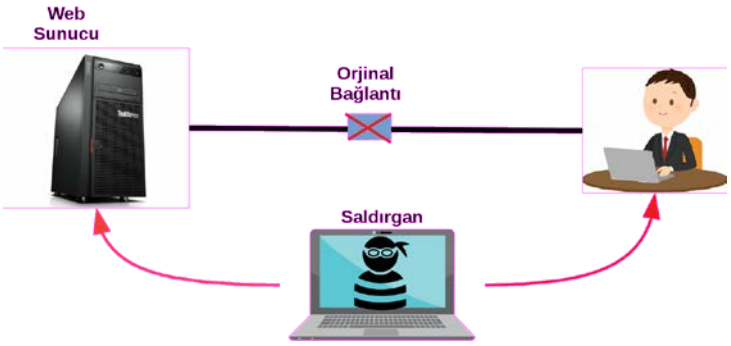
programları yama yapmak isterken ya da ilk bakışta zararsız gibi görülen ekinde bulunan zararlı yazılımı kullanıcı tarafından açılması için özel tasarlanmış bir e-posta yoluyla yapılabilmektedir [14].



Şekil 5 Phishing Saldırı Algoritması

2.6 Man in The Mıddle Attack (MITM, Ortadaki Adam) Saldırıları

MITM saldırıları, saldırganın kullanıcı bilgisayar ile iletişime geçtiği birim arasına girerek iletiler verilere ulaşılabildiği veya verileri değiştirebildiği aradaki trafiği dinleyebildiği saldırı türüdür. MITM saldırıları, başarıyla uygulanması halinde saldırgana büyük avantajlar sağlar. Bu saldırı türü oldukça yaygın olmakla birlikte en az önlem alınan saldırılar arasındadır [15].



Şekil 6 MITM Saldırı Algoritması

2.7 Insider (İçerden) Saldırıları

Insider saldırıları, kurban bilgisayar sistemine veya ağına erişmeye yetkisi olan kişierlerce yapılan kötü niyetli saldırılarılardır [15]. Bu saldırıların en büyük dezavantajı alınan tüm güvenlik önlemlerin geçersiz kalmasıdır. Çünkü saldırgan saldırıyı yapmak için hiçbir güç harcamaz çünkü hedef sisteme ulaşmak için yetkilidir. bir kişi tarafından gerçekleştirilen kötü amaçlı saldırılardır. Kurum ve kuruluşlar güvenlik önlemlerini genelikle dışarıdan gelebilecek saldırılara karşı önlem almaktadırlar.

2.8 Sıfırıncı Gün Saldırıları

Sıfırıncı gün saldırıları, kullanılan yazılımın zafiyetinin tespit edildiği gün başlamaktadır. Yazılım geliştiriciler böyle bir zafiyet olduğu tespit edildiğinde bu güvenlik açığını gidermek için güvenlik yamaları geliştirmekte ve kullanıcıların bu güvenlik yamaları ile güncelleme yapmasını istemektedirler.

Saldırganlar, yazılımlarda olası "Sıfırıncı Gün" açıklarını tespit etmeye ve bu zafiyetti kullanarak kurban sistemlere sızmaya çalışmaktadırlar.

3. Örnek Olay İncelemesi

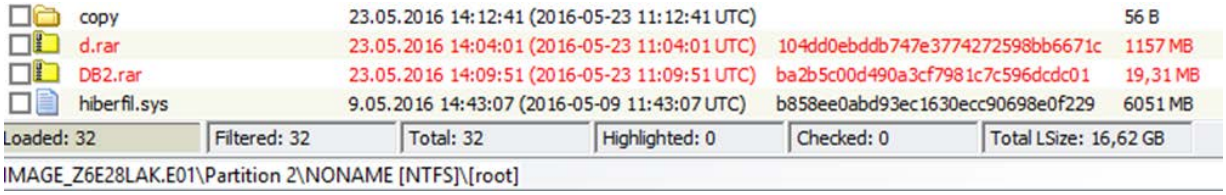
Kaba kuvvet saldırıları her geçen gün yeni yöntemlerle hedeflerine sessizce sızarak amaçlarına ulaşma yolları bulurken bu yazılımların tespiti ve analizleri için alınan tedbirler yeterli olmamaktadır. Bu çalışmada Kaba kuvvet saldırısıyla resmi kuruma yapılan gerçek bir saldırı örneği tespiti ve analiz detaylı olarak incelenmiştir. Analizler için ilk olarak resmi kurumdaki bilgisayarlar kontrol edilerek şüpheli dosya ve ağ trafiği kontrol edilmiştir. Yapılan incelemelerde üst düzey yöneticinin kullandığı bilgisayarda son yapılan internet geçmişinde şüpheli bir dosyanın indirildiği tespit edilmiştir.

Analizler için ilk olarak şüpheli bilgisayarın FTK Imager programı kullanılarak imaj kopyası alınmıştır. İncelemesi yapılacak bilgisayarın kopyasını alarak güvenli bir ortamda çalıştırmak olası zararları en aza indirmek için güvenli bir seçenektir. Alınan kopya, Windows 7 işletim sistemi yüklü sanal bilgisayarda çalıştırılarak tüm analizler yapılmıştır [16].

Analizler "AccessData Forensic Toolkit Version:7.0.0.163 ve Event Log Explorer Version 4.5" programları aracılığıyla gerçekleştirilmiştir. İncelenen örnek gerçek bir siber saldırıdan seçildiğinden tespit edilen bilgiler blur (gizlenmiş) edilerek çalışmada sunulmuştur. Alınan imaj kopyaları analiz işlemleri yapabilmek için sanal bilgisayarda imaj kopyaların canlandırılması gereklidir. Bu işlem, alınan imaj kopyasının içeriğinin detaylı olarak görüntülenebilmesi anlamına gelmektedir.

Tablo 1 Şüpheli Bilgisayar Bilgileri

Kullanıcı Adı	Administrator
Güvenlik Kimliği	500
Son Giriş Zamanı	21.11.2015 03:47:20 UTC
Son Şifre Değiştirme Zamanı	21.11.2015 03:57:24 UTC
Geçersiz Giriş Sayısı	244
Son Geçersiz Giriş Zamanı	20.05.2016 12:18:00 UTC



Şekil 6 Şüpheli Dosyalar

Yapılan analizlerde şüpheli bilgisayarda internet geçmişi incelendiğinde "IMAGE_Z6E28LAK.E01\Partition 2\NONAME [NTFS]\[root]" dizini altında yer alan "DB2.rar, d.rar" isimli dosyaların ve "IMAGE_Z6E28LAK.E01\Partition 2\NONAME [NTFS]\[root]\copy" dizini altında indirildiği tespit edilmiştir (Şekil 6).

Şüpheli dosyalar tespit edildikten sonra, şüpheliye ait IP(İnternet Protokol) adresini tespit etmek amacıyla "IMAGE_Z6E28LAK.E01/Partition 2/NONAME [NTFS]/[root]/Windows/System32/winevt/Logs/" dizini altında yer alan "security.evtx" ve "Microsoft-Windows-TerminalServices-RemoteConnectionManager%4Operational.evtx" isimli log dosyaları "Event Log Explorer Version 4.5" programıyla analiz yapılmıştır.

Tablo 2 Şüpheli "security.evtx" Ait Dosya-Dizin Hareketleri

Creates: C:\ Users\Admin\AppData \security.evtx
Creates: C:\Users\ security.evtx
Creates: C:\Users\Public\Read_ security.evtx
Writes to: C:\Users\desktop.ini
Opens: C:\Windows\Prefetch\ security.evtx

Writes to: C:\Users\Admin\AppData\ security.evtx
Writes to: C:\ security.evtx
Writes to: C:\Users\desktop.ini
Writes to: C:\Users\Public\Recorded TV\Sample Media\desktop.ini
Writes to: C:\Users\Public\Recorded TV\Sample Media\win7_scenic-demoshort_raw.wtv
Deletes: C:\ security.evtx.log
Deletes: C:\Users\desktop.ini
Deletes: C:\Users\Public\desktop.ini

Tablo 2'deki kod mimarisi incelendiğinde "security.evtx" isimli dosyanın ilk olarak C:\ Users\Admin\AppData \security.evtx dosyası olarak kendisini yaratma işlemi yapmaktadır. Daha sonra masaüstünde "security.evtx" isimli dosya oluşturmaktadır. Kurban sisteme sızma işlemini tamamladıktan sonra C:\Windows\security.evtx altında aktif hale gelmektedir. Yaratma işlemlerini yaptıktan sonra C:\ security.evtx.log komutu ile yapılan işlemlerin kayıtlarını silmektedir.

"Microsoft-Windows-TerminalServices-RemoteConnectionManager%4Operational.evtx" isimli log dosyası üzerinde yapılan incelemelerde "20.05.2016" ve "23.05.2016" tarihlerinde hedef bilgisayara, uzaktan erişimde bulunmak amacıyla "5.19X.XX.XXX, 155.9X.XXX.XX ve 19X.XXX.XXX.XX" numaralı IP adreslerini kullanan şüpheliler tarafından kaba kuvvet saldırıları yapıldığı tespit edilmiştir (Şekil 6).

Microsoft-Windows-TerminalServices-RemoteConnectionManager%4Operational.evtx

Filtered: showing 965 of 1938 event(s)

Date	Time	Event	Computer	Target User Name	IP Address
23.05.2016	14:03:33	1149	server	admin	5.1
23.05.2016	13:46:53	1149	server	admin	5.19
23.05.2016	13:46:51	1149	server	admin	5.19
23.05.2016	13:46:48	1149	server	admin	5.19
23.05.2016	13:46:46	1149	server	admin	5.19
23.05.2016	13:46:43	1149	server	admin	5.1
23.05.2016	13:46:41	1149	server	admin	5.19
23.05.2016	13:46:38	1149	server	admin	5.19
20.05.2016	15:04:57	1149	server	administrator	190.2
20.05.2016	15:04:15	1149	server	administrator	190.2
20.05.2016	15:04:12	1149	server	administrator	190.2
20.05.2016	14:36:18	1149	server	administrator	155.9
20.05.2016	14:36:03	1149	server	administrator	155.
20.05.2016	13:49:23	1149	server	user	5.19
20.05.2016	13:49:20	1149	server	user	5.1
20.05.2016	13:49:18	1149	server	user	5.1
20.05.2016	13:49:15	1149	server	user	5.1
20.05.2016	13:49:13	1149	server	user	5.1
23.05.2016	13:44:01	1149	server	adem	5.1
23.05.2016	13:43:58	1149	server	adem	5.1
23.05.2016	13:43:56	1149	server	adem	5.1
23.05.2016	13:43:53	1149	server	adem	5.1
23.05.2016	13:43:50	1149	server	adem	5.19
23.05.2016	13:43:48	1149	server	adem	5.1
23.05.2016	13:43:45	1149	server	adem	5.1
23.05.2016	13:43:43	1149	server	adem	5.1
23.05.2016	13:43:41	1149	server	adem	5.1

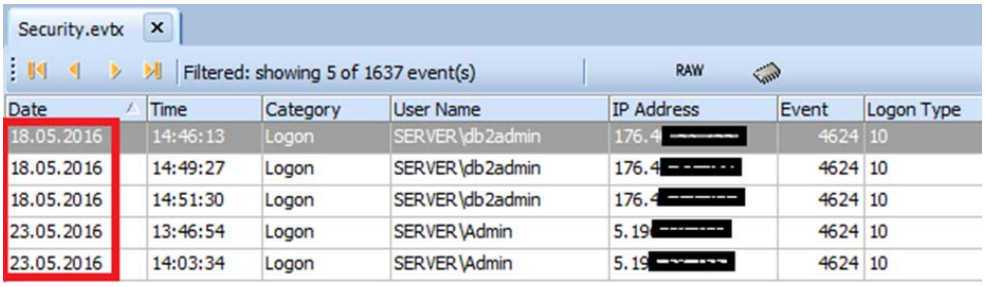
Şekil 6 Hedef Bilgisayara Yapılan Kaba Kuvvet Saldırısı

Şekil 6'da verilen log kayıtlarından görüleceği gibi "5.19X.XX.XXX" IP adresini kullanan şüpheli tarafından, adem ve admin kullanıcıları kullanılarak, hedef bilgisayarda tanımlı bulunan şifre tespit edilmeye çalışılmıştır.

"Microsoft-Windows-TerminalServices-RemoteConnectionManager%4Operational.evtx" isimli log dosyası üzerinde yapılan incelemelerde hedef bilgisayara erişimde bulunmak istediği tespit edilen "5.19X.XX.XXX, 155.9X.XXX.XX ve 190.2XX.XXX.XX" numaralı IP adresleri kullanılarak erişim

yapılmış olabileceği şüphesiyle "security.evtx" isimli log dosyası üzerinde incelemeler gerçekleştirilmiştir.

"security.evtx" isimli log dosyası üzerinde yapılan incelemelerde, yetkisiz erişimde bulunan saldırgana ait IP adresini tespit etmek amacıyla "Event ID=4624", "Logon Type=10" filtresi uygulanmış olup, yapılan filtreleme işlemi neticesinde "18.05.2016" günü "176.4X.XX.XX" numaralı IP adresi üzerinden ve "23.05.2016" günü "5.19X.XX.XXX" numaralı IP adresleri üzerinden erişim yapıldığı tespit edilmiştir (Şekil 7).


Security.evtx

Filtered: showing 5 of 1637 event(s) RAW

Date	Time	Category	User Name	IP Address	Event	Logon Type
18.05.2016	14:46:13	Logon	SERVER\db2admin	176.4[redacted]	4624	10
18.05.2016	14:49:27	Logon	SERVER\db2admin	176.4[redacted]	4624	10
18.05.2016	14:51:30	Logon	SERVER\db2admin	176.4[redacted]	4624	10
23.05.2016	13:46:54	Logon	SERVER\Admin	5.19[redacted]	4624	10
23.05.2016	14:03:34	Logon	SERVER\Admin	5.19[redacted]	4624	10

Şekil 7 "security.evtx" İsimli Log Dosyası Üzerinde Yapılan İncelemeler

Yapılan incelemeler neticesinde Şekil 6 ve Şekil 7'de görülebileceği gibi "23.05.2016" tarihinde şifrelendiğinin ve müştekiye ait bilgisayara 23.05.2016 tarihinde "5.19X.XX.XXX" numaralı IP adresini kullanan saldırgan tarafından erişim yapıldığının tespit edilmiştir.

Kaba kuvvet saldırısı ile yetkisiz erişimde bulunduğu anlaşılan şüpheliye ait "5.19X.XX.XXX" numaralı IP adresinin WHOIS (kayıtlı alan adı ya da IP adresinin sahiplik bilgileri kayıtları) sorgusu www.domaintools.com web sayfası üzerinden sorgulanmış olup, yapılan sorgulama saldırgana ulaşılabileceği tespit edilmiştir.

4. Sonuçlar

Kaba kuvvet saldırıları, hedef sistemde kayıtlı şifre ve parolaları kırmak için tasarlanmış yazılımlar olarak bilinmektedir. Kaba kuvvet saldırısıyla, hedef bilgisayarlarda ki tüm bilgilerin alınması ve istenen bilgilerin değiştirilmesine olanak sağlamaktadır. Bu saldırıların kimin yaptığını belirlemek oldukça zordur, çünkü saldırganlar nadiren arkalarında iz bırakmaktadır.

Son yıllarda yapılan siber saldırılarında en etkili silah olarak kullanılan kaba kuvvet saldırıları, alınan tüm klasik güvenlik önlemlerine rağmen sistemde ve yazılımlarda bulunan hatalar, bağlanılan ağlar, yer güvenlik zafiyetleri ve son kullanıcının dikkatsizliği gibi nedenlerle hedef sistemlere sızmaktadır.

Kaba kuvvet saldırılarına karşı alınabilecek başlıca önlemler;

- Kullanıcı adı ve parolasını sistemin izin verdiği maksimum karakter sayısını kullanarak güçlü bir şifre oluşturmak,
- Uzak masaüstü erişim portuna güçlü bir şifre oluşturmak eğer kullanılmıyorsa tamamen kapatmak,
- Kullanılan yazılımların orijinal ve güncel sürümlerini kullanmak,
- Bilinen ve kaliteli bir anti virüs programı kullanmak,
- Şüpheli web sitelerin erişim IP sınırlaması getirmek.

Bu gibi önlemleri alarak kaba kuvvet saldırılarında korunmamakla birlikte kullanıcılar için farkındalık oluşturması açısından önemlidir. Seçilen örnekte resmi bir kuruluşa sızma ve saldırı yöntemi detaylı olarak verilmiştir. Hedefe sızmak için önce üst düzey bir yönetici belirlenmiş kullanıcıyı aldatıcı bir e-posta hazırlanmış ve ekinde bulunan zararlı yazılımın bilgisayara fark edilmeden yüklenmesi

sağlanmıştır. Bu senaryo güncel kaba saldırılarda sıkça kullanılmaktadır. İncelenen örnekte saldırgana ait bilgilerin ulaşılabilir olduğu görülmüştür.

Kaba kuvvet saldırılarına karşı oluşturulacak etkili bir tespit ve analiz yaklaşımı bu tehdit ile mücadeleye önemli katkı sağlayacaktır. Bu çalışmada kaba kuvvet saldırısının tespit ve analiz yaklaşımın başarılı bir şekilde uygulanabilir olduğu seçilen gerçek siber saldırı örneği üzerine yapılan analizlerle test edilmiştir.

Bu çalışma kapsamında, gerçek bir kaba kuvvet saldırısının tespit ve analizinin nasıl yapıldığı, saldırgannın amaçlarını ve kullandığı yöntemleri detaylı olarak tartışılmıştır. Bu çalışma sonuçlarıyla birlikte, benzer saldırıların engellemesi ve alınacak güvenlik mekanizmalarının geliştirlmesine katkı sağlayacağı düşünülmektedir.

Kaynaklar

[1] Ö. M. Nesip ve A. Kaya, "Siber Güvenliğin Milli Güvenlik Açısından Önemi ve Alınabilecek Tedbirler," Security Strategies Journal, pp. 9.18, 2013.

[2] İ. Kara ve M. Aydos, "The Ghost In The System: Technıcal Analysıs Of Remote Access Trojan," International Journal on Information Technologies & Security, pp.11.1, 2019.

[3] İ. Kara ve M. Aydos, "Static and Dynamic Analysis of Third Generation Cerber Ransomware," In 2018 International Congress on Big Data, Deep Learning and Fighting Cyber Terrorism (IBIGDELFT), pp. 12-17, IEEE, December, 2018.

[4] K. Şahin, "Realizm Ve Liberalizm Işiğinda Siber Savaş ve Alternatif Bir Kavram Olarak Siber Bariş'in Değerlendirilmesi," TURAN-SAM, 2017, 9.35, pp. 287-297.

[5] A. Chris, "Advanced SQL injection in SQL server applications," 2002.

[6] B. Muhammet, G. Sebahattin, "Applications for detecting XSS attacks on different web platforms," In: 2018 6th International Symposium on Digital Forensic and Security (ISDFS), pp. 1-6, IEEE, 2018.

[7] H. J Loesch, A. Remscheid. "Brute force in molecular reaction dynamics: A novel technique for measuring steric effects," The Journal of Chemical Physics, 93(7), pp. 4779-4790, 1990.

[8] K. Mark AR, "When brute force fails: How to have less crime and less punishment," Princeton University Press, 2009.

[9] B. Roberto, "Brute-Force Mining of High-Confidence Classification Rules. In: KDD," pp. 123-126, 1997.

[10] W. Matt, et al. "Password cracking using probabilistic context-free grammars," In: 2009 30th IEEE Symposium on Security and Privacy, pp. 391-405, IEEE, 2009.

[11] S. Theodoros, et al. "A game theoretic defence framework against DoS/DDoS cyber attacks," Computers & Security, 38, pp.39-50, 2013.

[12] I. Alireza, O. Mohamed, R. Mohd, A. Fadlee, "Accurate ICMP traceback model under DoS/DDoS attack," In: 15th International Conference on Advanced Computing and Communications (ADCOM 2007). pp. 441-446, IEEE, 2007.

[13] J. Markus, "Modeling and preventing phishing attacks," In: Financial Cryptography, 2005.

[14] D. Rachna ve T. J. D. Marti, "Why phishing works," In: Proceedings of the SIGCHI conference on Human Factors in computing systems, pp. 581-590, ACM, 2006.

[15] B. Wu et all, "A survey of attacks and countermeasures in mobile ad hoc networks," In Wireless network security, pp. 103-135, 2007.

[16] İ. Kara, "Teslacrypt Fidye Yazılım Virüsünün Tespiti, Teknik Analizi ve Çözümü," Uluslararası Yönetim Bilişim Sistemleri ve Bilgisayar Bilimleri Dergisi, 2.2: pp. 87-94.