WEB TABANLI ZARARLI YAZILIMLARIN SALDIRI YÖNTEMLERİ VE ANALİZ TEKNİKLERİ

İlker KARA
Çankırı Üniversitesi, Eldivan Sağlık Hizmetleri MYO, Çankırı, TÜRKİYE
karaikab@gmail.com

ÖZET

Son yıllarda bilişim teknolojilerinin gelişmesi ve yaygınlaşmasıyla birlikte zararlı yazılımlar, basit birkaç saldırıdan daha karmaşık büyük kitleleri hedef alan geniş çaplı bir tehdit olarak görülmeye başlamıştır. Bu zararlı yazılımlar amaçlarına daha hızlı ulaşmak için saldırı yöntemlerini sürekli geliştirmektedir. Bu durum kişi ve kurumların siber saldırı suçuna maruz kalma olasılığını artırmaktadır. Son günlerde dünya genelinde web tabanlı yeni nesil siber saldırı vakaları sıkça görülmeye başlamıştır. Web tabanlı bu saldırılardan korunmak için çalışmalar devam etmekle birlikte kabul edilebilir bir çözüm ne yazık ki bulunamamıştır. Bu çalışma, web tabanlı zararlı yazılım ve zararlı yazılımın analiz yöntemlerini, gerçek dünyadan seçilen siber saldırı örneklerini içermektedir. Bu çalışmada sunulan, web tabanlı zararlı yazılımların saldırı ve analiz yöntemleri ve bunların uygulamasının kullanıcı farkındalığını arttıracağı, karşılaşılabilecek olumsuz örneklerin giderilmesine katkılar sağlayacağı değerlendirilmektedir.

Anahtar Kelimeler - Web Tabanlı Zararlı Yazılım Analizi, Zararlı Yazılım Yöntemleri, Zararlı Yazılım Atakları

Analysis Techniques of Web Based Malware and Attack Methods

ABSTRACT

In recent years, given the rapid advances and the increased popularity on information technology, malwares has become more complex threat and large-scale attack targeting large population than a few simple attacks. These malwares are always changing and improving their attack methods to achieve their goals rapidly. For this reason, the number of people and institutions being exposed in crime attack has been increased by day by in nowadays. Furthermore, around the world, new generation web-based cyber-attacks are frequently seen. Researches are ongoing to defend against web-based attack, but any acceptable solution and tangible result cannot be obtained. In this article, web-based cyber-attack and how to analyze them are presented. The analysis methods are applied to real-life cyber attack cases. It is expected that this study introduced in this work might help users to handle cyber-attacks by analysing them and also creates user awareness.

Keywords— Web Based Malware Analysis, Malware Attack Methods, Malware Attacks

I. GİRİŞ (INTRODUCTION)

Günümüzde saldırı kavramı yeni bir olgu değildir. İnsanlık tarihi boyunca saldırı, ilk çağlarda hayatta kalmak ve sömürge olayları için saldırganların kullandığı yaygın bir taktik olmuştur. Bugün ise kötü niyetli saldırganlar bu taktiği bilişim dünyasında yaygın olarak uygulamaya başlamıştır [1,2]**.** Kullanıcılar web sitelerini, bilgi paylaşımı, eğlence, iletişim kurmak, hizmet vermek ve kendilerini tanıtmak gibi birçok ihtiyacı karşılarken saldırganlar ise bu siteleri, kendilerine kazanç sağlamak, kişisel verileri çalmak ve hedef sisteme zarar vermek amacıyla kullanmaktadır.

Bu amaç için özel olarak tasarlanmış zararlı yazılımlar; reklamlar, bilgilendirme mailleri ve sosyal mühendislik saldırıları gibi çeşitli yöntemlerle kurban sisteme kolayca sızabilmektedir [3-6]. Web tabanlı siber saldırıları diğer siber saldırılardan ayıran en önemli özelliği ise; mağdurun kullanmakta olduğu sisteme özel olarak tasarlanması ve geleneksel anti virüs programlarının güvenlik anlayışı ile tespit edilmesinin zorluğundur. Saldırganın amacına

bağlı olarak, zararlı yazılımın türü ve yöntemi de değişkenlik göstermektedir [7].

Virüs, solucan, truva atı, RootKit (uzaktan kontrol virüsü) gibi zararlı yazılım türleri son zamanlarda yaygın olarak görülmektedir. Kötü niyetli saldırganlar; para, şantaj, ülkelerarası terör saldırıları veya bilgi hırsızlığı gibi gerekçelerle kişiler ya da kurumlara saldırı ataklarında bulunmaktalardır. Bu hedefli saldırılara ek olarak hiçbir amaç gözetmeden tamamen zarar vermek ya da saldırganların egolarını tatmin etmek için düzenlene saldırılarda görülmeye devam etmektedir.

Siber saldırılar amaçlarına göre sıralandığında temel olarak altı başlık altında toplanabilir. Bunlar;

i. Ticari amaçlı kullanıcı eğilimlerin belirlenmesi amacıyla bilgi toplamak,
ii. Kişisel bilgilerin ele geçirmek (Kayıtlı e-posta şifreleri, banka şifreleri, sosyal medya şifreler vb.)
iii. Şantaj yaparak para kazanmak,
iv. Hedef sistemi yavaşlatmak ya da tamamen kullanılmaz hale getirmek,
v. Terör faaliyetleri, siyasi aktivist gruplar faaliyetleri, ve
vi. Amaç gözetmeden zarar vermektir.

Zararlı yazılımlar genellikle oltalama yöntemlerini kullanarak hedef sistemlere sızmaktadır. Bu amaç için tasarlanmış ilk bakışta zararsız bir içerik gibi görülen e-postalar kullanıcılara gönderilerek e-posta ekinde bulunan zararlı yazılımın kullanıcı tarafından aktif hale getirilmesi amaçlanmaktadır. Son günlerde ülkemizde sıklıkla görülmeye başlanan web tabanlı zararlı yazılım oldukça tehlikeli sonuçlara ve sonuçlarıyla birçok mağduriyetlere sebep olmaktadır [8-10]. Web tabanlı zararlı yazılımlar, genellikle maddi çıkar sağlamak (fidye yazılımlar) ya da orijinal yazılım ürünlerini yasa dışı olarak çoğaltmak ve kullanım sağlayacak şekilde tasarlanmaya yöneliktir [11-12]. Fidye yazılımlar, hedef sistemdeki dosyaları şifrelendikten sonra kullanıcıya ait özel dosyaların şifrelenmektedir [13-16]. Bu dosyalara tekrar erişim sağlanabilmesi için mağdur saldırgana fidye ödemesi gereklidir [18-20]. Ödeme sanal para denilen bitcoin ile yapılmaktadır [21-23].

II. WEB TABANLI ZARARLI YAZILIMLAR NASIL BULAŞIR?

Web tabanlı zararlı yazılımın **saldırı yöntemlerini genel olarak şöyle sıralanabilir;**

- Rapidshare, Hotfile gibi web sitelerinden indirilen oyun, film, müzik dosyaları ile
- Birçok türü olan Torrent sitelerinden indirilen dosyalar ile,
- Resmi veya resmi olmayan film, dizi izleme bloklarını kullanabilmek için indirilen programlar (flash/java gibi) ile
- Saldırganlar tarafından zarar verilerek kaynakları değiştirilmiş uygulamaların indirilmesiyle,
- İlk bakışta zararsız gibi görülen hizmet (alışveriş, emlak, sosyal paylaşım blokları gibi)sitelerine ziyaretler sırasında (istemsiz olarak), kurban sisteme sızmaktadır.

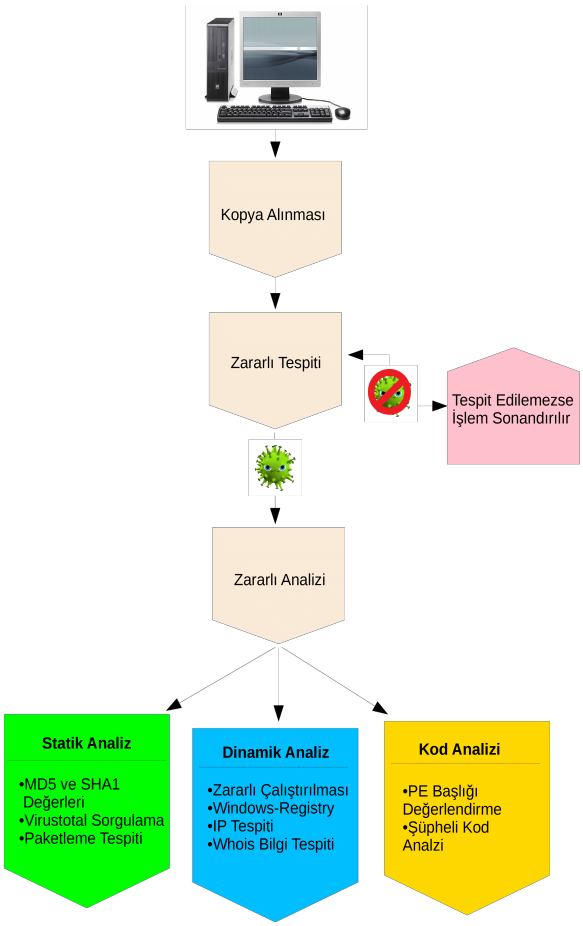
Bu çalışmada, web tabanlı zararlı yazılımın kurban sistemde tespit edilmesi, sisteme sızması ve davranış analizi detaylı olarak incelenmiş olup çalışma sonunda ise bu zararlı yazılımlardan korunma yöntemlerine yer verilmiştir. Seçilen siber saldırı örneklerinin gerçek olaylardan ve en yaygın görülen saldırı örnekleri olmasına özellikle dikkat edilmiştir.

III. METOT (METHOD)

Zararlı yazılımlar, her geçen gün yeni yöntemlerle hedeflerine sessizce ve daha hızlı ulaşma yolları bulurken bu yazılımların tespiti ve analizleri için standart olarak uygulanan bir analiz metodu bulunmamaktadır. Zararlı yazılım analiz uzmanları kendilerine özgü metotlar kullanmakla birlikte en çok kabul gören yöntem basitten karmaşığa doğru yapılan analizlerdir. Bu amaçla zararlı yazılım çalıştırmadan elde edilebilecek tüm bilgilere ulaşmak için statik analiz, ikinci olarak sanal bir makinede zararlı yazılımı çalıştırarak yapılan davranış hareketlerinin (dosya-dizin hareketleri) analiz edildiği dinamik analiz ve son aşama olarak ta kod analizi yapılmaktadır.

Zararlı yazılım olduğu düşünülen bilgisayarın ilk olarak kopyası alınır. Yapılacak tüm analizler bu kopya üzerinde olmaktadır. Bu çalışmada web tabanlı zararlı yazılım saldırısına maruz kalmış bilgisayarın, FTK Imager (free version) programı kullanılarak kopyası alınmıştır. Tüm incelemeler, zararlı yazılımın olası ataklarından etkilenmemesi için inceleme bilgisayarı sanal makine modunda yapılmıştır. Wen tabanlı zararlı

yazılımının karakteristik davranış analizi için yapılan incelemeler "AccessData Forensic Toolkit v6.2.1.10 (FTK)", "Process Explorer" "Cuckoo" aracılığıyla gerçekleştirilmiştir. Zararlı yazılım analizlerinde kullanmak üzere analiz adımlarını gösteren bir model önerilmiş ve önerilen model algoritmasının benzer tüm senaryolarda uygulanabileceği öngörülmektedir (Şekil 1).



Şekil 1. Önerilen zararlı yazılım analiz model algoritması.

3.1. Zararlı Yazılım Analizi

Zararlı yazılım analizi, zararlı yazılımın özelliklerini inceleyerek davranış analizi için kullanılan bir işlemdir. Genel olarak üç adımda yapılabilir. Bunlar;

i) Statik Analiz

Statik analiz, zararlı yazılımın çalıştırılmadan önceki yapısal analizini içermektedir. Statik analiz sayesinde zararlı yazılımın içerdiği metinsel ifadeler, kullandığı fonksiyonları, dosya-dizin yapı içeriğini ve paketlenmiş olup olmaması, hash (doğrulama) değerleri, hedef sisteme yüklenme tarihi gibi verilere ulaşılabilir. Bu aşamada elde edilen bilgiler diğer adımlarda yapılacak analizler için rehber niteliğindedir.

ii) Dinamik Analiz

Dinamik analiz, zararlı yazılımın kontrollü bir alanda (sanal makine ya da sandbox üzerinde) çalıştırılmasıyla yapılan analizdir. Analizler sonucunda zararlı yazılım çalışırken kurban sistemdeki dosya-dizin hareketleri, kayıt defteri girdileri, IP trafiği ve ağ aktivitelerini elde edilebilmektedir. Dinamik analiz ile zararlı yazılımın hareket kabiliyetini ve kapasitesini tam olarak görebilme imkânı sağlamaktadır.

iii) Kod Analizi

Kod analizi, zararlı yazılımın son aşaması olarak değerlendirilir. Kod analizi, zararlı yazılımın kod mimarisi ve davranış aktivitelerinin anlaşılması olanak sağlaması açısından oldukça önemlidir. Zararlı yazılımlar farklı sistemlerde (Windows, Linux, IOS vb.) farklı davranış gösterdiğinden inceleme yapan bilişim uzmanlarının işletim sistemlerine hâkimiyeti son derece önemlidir.

IV. BULGULAR

Zararlı yazılım analizi için önerilen model algoritması doğrultusunda incelemelerde ilk olarak kurban bilgisayardan kopya alınmıştır. Daha sonra kurban bilgisayarda zararlı yazılımın tespiti yapılmıştır. Zararlı yazılım olduğu şüphelenilen dosyalar için statik analiz yapılmıştır. Statik analiz sonucunda, web tabanlı zararlı yazılımın bulunduğu kurban bilgisayara ait bilgiler, FTK ve Process Explorer programları kullanılarak elde edilmiştir (Tablo 1 ve Tablo 2).

Tablo 1 ve 2'de web tabanlı zararlı yazılımların bulunduğu kurban bilgisayara ait bilgiler gösterilmektedir. Bu bilgiler temel ve ileri analizler için önem içermektedir. Ayrıca bu bilgiler yapılacak analizlerin temelini oluşturmakta, yapılacak analizler için hangi programların kullanılmasına ve ilgili versiyonlarına karar verilmesini sağlamaktadır.

Bilişim sistemini engelleme, bozma, verileri yok etme veya değiştirme işlemlerini gerçekleştirebilecek türden zararlı yazılımların {RAT (Uzak Erişim Trojeni), Truva Atı vb.} mevcut olup olmadığı tespit etmek amacıyla kurban bilgisayarda tüm executable (çalıştırılabilir dosya) dosyalar tespit edilmiştir. Tespit edilen executable dosyalar, bünyesinde çok sayıda antivirüs firmasına ait veritabanı

bilgisini barındıran www.virustotal.com web sayfasından sorgulanmıştır. Sorgulama sonucunda şüpheli olabileceği düşünülen executable dosya görüntüleri Şekil 2'de verilmiştir.

Tablo 1. Cihaz Bilgileri

Açıklama	Physical Disk, 976.773.168 Sectors 465,8 GB
Toplam Kapasite	500.107.862.016 Bytes (465,8 GB)
Toplam Sektör	976.773.168
MD5 Değeri	4e2869cf5a7509ca28c616b48b78bdd3
MD5 Doğrulama	4e2869cf5a7509ca28c616b48b78bdd3
SHA1 Değeri	4e5946160896c23f20238919ec9c7c26c350f41d
SHA1 Doğrulama	4e5946160896c23f20238919ec9c7c26c350f41d

Şekil 2'de tespit edilen şüpheli executable dosyaları incelenmeye başlamıştır. Yapılan literatür araştırmalarında "AutoKMS.exe ve install.exe" isimli dosyaların işletim sistemlerini yasal olmayan yollardan lisanslamaya yarayan türden zararlı yazılım oldukları, "setup_id3525585ids1s.exe" ile "yet_another_cleaner_rkla.exe" isimli dosyaların ise "Adware" yani firmalar tarafından sağlanan reklamları programın içeriğine gömerek kullanıcıya sunan ve gelir elde etmeyi amaçlayan türden zararlı yazılım oldukları tespit edilmiştir.

Tablo 2. İşletim Sistemi Bilgileri

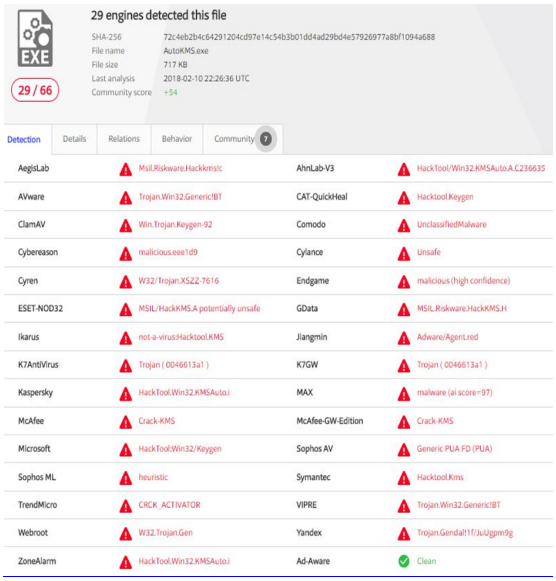
Ürün Adı	Windows 7 Ultimate
Kayıtlı Sahip	Pc
Sistem Kökü	C:\Windows
Güncel Veriyonu	6.1
CSD Versiyonu	Service Pack 1
Kurulum Tarihi	29.08.2015 - 07:10:38 UTC
Son Kapanma Tarihi	20.11.2015 - 11:59:09 UTC

Şekil 2. Tespit edilen şüpheli executable dosyaları.

Dosya Yolu	Sonuç	Hash Değeri
IMAGE.001/Partition 2/NONAME [NTFS]/[root]/Windows/AutoKMS/AutoKMS.exe	27	3cb03c134f7307866b3c52735cdfae76
IMAGE.001/Partition 3/NONAME [NTFS]/[root]/Kutlay hoca yedekleri/29.08.2015 yedekleri/Downloads/setup_id3525585ids1s.exe	27	32f376facba35c1f1ec651c2e6fcde84
IMAGE.001/Partition 3/NONAME [NTFS]/[root]/Kutlay hoca yedekleri/yedekler/Downloads/yet_another_cleaner_rkla.exe	22	e713142712b31512f78b6877ec962391
IMAGE.001/Partition 2/NONAME [NTFS]/[root]/Windows/Setup/scripts/install.exe	21	fbef084c3c3bff6c87bfa8dc209ee776

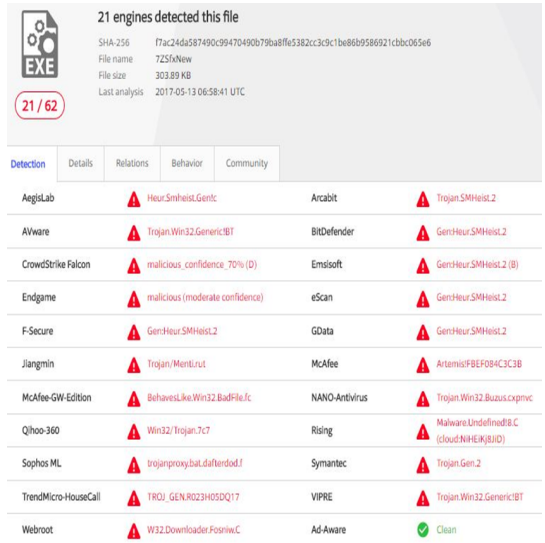
- **"AutoKMS.exe", "install.exe" (Yazılım korsanlığı);** Kötü niyetli kişiler tarafından telif haklarıyla korunan lisanslı yazılımlar, yetkisiz kopyalama ile üzerinde gerekli değiştirmeler yaparak kullanıcılara indirme, paylaşma, satma veya yükleme de dahil olmak üzere maddi çıkar elde etmek üzere yapılan yasa dışı işlemlerdir. Yazılım korsanlığı, ayrıca web tabanlı yazılım uygulamaları için gerekli olan bilgileri (kullanıcı kimlikleri, parolalar, yazılım lisans kodları ve aktivasyon anahtarları) yasa dışı paylaşma ihlalini de kapsamaktadır. Yazılım korsanlığı, Türk Ceza Kanununda (TCK) siber suçlar kapsamında değerlendirilmektedir. Yazılım korsanlığı, saldırganların amaçlarına ulaşmak için izlediği bir yol olarak kullanılmaktadır. Hedeflenen amaç doğrultusunda modifiye edilen dosyalar, kullanıcıya fark ettirilmeden birçok işlemi (dinleme, verileri çalma, verileri şifreleme gibi) yerine getirebilmektedir. Bu nedenle yazılım korsanlığı; zararlı yazılım, fidye yazılım, casus yazılım veya bilgisayar virüsleri kapsamında değerlendirilip kullanıcı açısından yüksek güvenlik tehditlerine maruz kalmasına yol açmaktadır.
- **"setup_id3525585ids1s.exe", "yet_another_cleaner_rkla.exe" (Adware; Advertasing Software):** Adware adından da anlaşılabileceği gibi reklam yazılımıdır. Kullanıcının bilgisi olmadan çoğu zaman bir yazılım içine gömülerek kurban bilgisayara sızmaktadır. Temel olarak dinleme, verileri çalma, verileri şifreleme gibi bir amacı olmamakla birlikte özel olarak tasarlanabilme imkânı da vardır. Adware zararlı yazılım, çalışmaya başladığında kullanıcının internet tarayıcısını işgal ederek tasarım amacına göre hareket etmeye başlamaktadır. İstediği internet sitelerini sürekli açarak saldırganın maddi kazanç elde etmesini sağlamaya çalışmaktadır.

Şekil 2'de tespit edilen web tabanlı zararlı yazılımlar hakkında daha fazla bilgi edinmek için statik analiz kapsamında www.virustotal.com sorgulaması yapılmıştır.



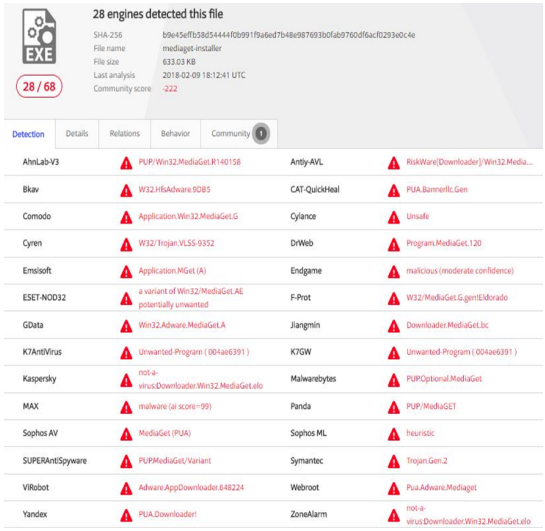
Şekil 3. "AutoKMS.exe" ait www.virustotal.com sorgulaması.

"AutoKMS.exe" ait www.virustotal.com sorgulama sonucunda 29 antivirüs programı tarafından tespit edildiği görülmüştür.



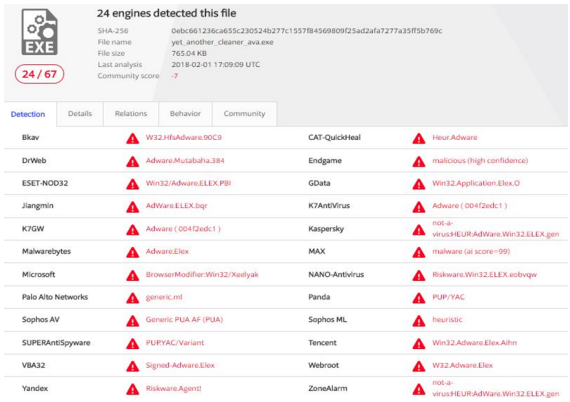
Şekil 4. "7ZSfxNew.exe" ait www.virustotal.com sorgulaması.

"install.exe" web tabanlı zararlı yazılım PEİD programı ile analiz edildiğinde paketlenmiş bir yapıya sahip olduğu görülmüştür. "install.exe" çalıştırıldığında paket içerisine gömülü olan "7ZSfxNew.exe" yi çalıştırmaktadır. Bu nedenle www.virustotal.com sorgulaması "7ZSfxNew.exe" üzerinden yapılmıştır. Sorgulama sonucunda 21 antivirüs programı tarafından tespit edildiği görülmüştür.



Şekil 5. "mediaget.installer" ait www.virustotal.com sorgulaması.

"setup_id3525585ids1s.exe", web tabanlı zararlı yazılım PEİD programı ile analiz edildiğinde paketlenmiş bir yapıya sahip olduğu ve çift tıklandığında paket içerisine gömülü olan "mediaget.installer"ı çalıştırmaktadır. Bu nedenle www.virustotal.com sorgulaması "mediaget.installer" üzerinden yapılmış olup sorgulama sonucunda 28 antivirüs programı tarafından tespit edildiği görülmüştür.



Şekil 6. "yet_another_cleaner_rkla.exe" ait www.virustotal.com sorgulaması.

"yet_another_cleaner_rkla.exe" ait www.virustotal.com sorgulama sonucunda 24 antivirüs programı tarafından tespit edildiği görülmüştür. Önerilen model algoritması doğrultusunda incelemelerin ikinci aşaması

olarak dinamik analiz yapılmıştır. Dinamik yazılımlar çalıştırıldığında davranış analizleri incelenmiştir. Seçilen örnekler işlevleri analiz için web tabanlı zararlı bakımından iki grupta değerlendirildiğinden her bir gruptan bir örneğe yer verilmiştir.

Tablo 3. "AutoKMS.exe" process ve dosya-dizin hareketleri.

İşlem	**DOSYA – DİZİN HAREKETLERİ**
Creates key:	HKCU\software\microsoft\windows\currentversion\internet settings
Creates key:	HKLM\software\microsoft\ AutoKMS.exe
Creates key:	HKLM\software\microsoft\tracing
Creates key:	HKCU\software\microsoft\windows\currentversion\runonce
Deletes value:	HKCU\software\microsoft\windows\currentversion\internet settings\ AutoKMS.exe]
Deletes value:	HKLM\software\microsoft\windows\currentversion\internet settings\
Deletes value:	HKCU\software\microsoft\windows\currentversion\internet settings\zonemap[runonce]
Deletes value:	HKLM\software\microsoft\windows\currentversion\internet settings\zonemap[runonce]
Deletes value:	HKCU\software\microsoft\windows\software\microsoft\windows nt\currentversion\]
Value changes	HKCU\software\microsoft\windows\ software\microsoft\windows\settings
Value changes	HKCU\software\microsoft\windows\currentversion\ software\microsoft\windows nt\currentversion\change file execution options
Value changes	HKCU\software\microsoft\windows\currentversion\internet settings

Tablo 4. "yet_another_cleaner_rkla.exe" process ve dosya-dizin hareketleri.

İşlem	**PROCESS HAREKETLERİ**
Creates process:	C:\windows\temp\ yet_another_cleaner_rkla.exe
Creates process:	["C:\windows\temp\ yet_another_cleaner_rkla.exe"]
Terminates process:	C:\Windows\Temp\ yet_another_cleaner_rkla.exe
	DOSYA – DİZİN HAREKETLERİ
Creates:	C:\Users\Admin
Creates:	C:\Users\Admin\AppData\Local
Creates:	C:\Users\Admin\AppData\Local\Microsoft\Windows\Temporary Internet Files
Creates:	C:\Users\Admin\AppData\Roaming
Creates:	C:\Users\Admin\AppData\Roaming\Microsoft\Windows\Cookies
Reads from:	C:\Windows\System32\drivers\etc\hosts

Önerilen model algoritması doğrultusunda incelemelerin son aşaması olarak zararlı yazılımın kod analizi yapılmıştır. Tablo 3'de görüleceği gibi, "AutoKMS.exe" process ve dosya-dizin hareketleri incelendiğinde web tabanlı zararlı yazılım ilk olarak Windows altında internet setting klasöründe kendisini yaratma işlemini yapmaktadır. Bu işlem ile zararlı yazılım kurban bilgisayara sızma işlemini gerçekleştirmektedir. Davranış hareketleri incelendiğinde Windows altında "software" dosyasının "setting" ayarlarını değiştirdiği görülmektedir.

Tablo 4'de görüleceği gibi, "yet_another_cleaner_rkla.exe" process ve dosya-dizin hareketleri incelendiğinde web tabanlı zararlı yazılım ilk olarak Windows

altında temp klasöründe kendisini yaratma işlemi yapmaktadır. Dosya-dizin hareketlerinden görüleceği gibi sızma işlemleri Temporary Internet Files dosyası altındaki Cookies (Çerezler) alanında kendisini yaratmaktadır.

V. SONUÇLAR VE DEĞERLENDİRME (CONCLUSIONS AND EVALUATIONS)

Son on yılda tüm dünyada büyük artış gösteren zararlı yazılım saldırıları, geniş güvenlik bütçeli büyük firmalarından resmi kurum, kuruluşun veya basit internet kullanıcılarının sistemlerini web tabanlı akıllı siber saldırganlardan tamamen koruyamadıklarını göstermektedir. Gelişen teknoloji ile güvenlik açıklarının daha da artmasıyla birlikte hedef sistemlerin güvenlik sistemlerinin kırılgan ve savunmasız kalması saldırganların ilgi odağı haline gelmekte ve zararlı yazılımların her geçen gün yeni türler geliştirerek piyasaya sürülmektedir.

Zararlı yazılımlar, bulaştığı sistemde veya ağ üzerindeki diğer makinelerde zarara yol açmak veya onların çalışmalarını aksatmak amacıyla özel olarak tasarlanmış yazılımlar olarak bilinmektedir. İnternet tabanlı cihazlar hayatımızda olduğu sürece zararlı yazılım tehdidi ile karşılaşmak zorunda olduğumuz bir gerçek olarak karşımıza çıkmaktadır. Alınan tüm tedbirler ve son kullanıcıyı bilinçlendirme çabalarına karşı, kullanılan cihazlarda bulunan ilk gün açıkları, gerek kullanılan yazılımlarda barınan hatalar gerekse bağlanılan ağlar ve güvenlik zafiyetleri nedeniyle saldırganları durdurmaya yeterli olmamaktadır. Zararlı yazılımlara karşı oluşturulan savunma mekanizmaları, gerçek siber saldırıları örnekleri üzerine yapılan analizler ile geliştirildiğinde zararlı yazılımlarla etkin mücadeleye önemli katkı sağlayacaktır.

Son günlerde artan özellikle web tabanlı saldırılar birçok mağdurun oluşmasına neden olmuştur. Ülkemizde bu saldırılar ağırlıklı olarak yazılım korsanlığı ve Adware zararlı yazılımlar olarak görülmektedir. Bu nedenle çalışmada, en güncel gerçek siber saldırı örnekleri detaylı olarak incelenmiştir. Zararlı yazılım analizi ve zararlı yazılımla etkin mücadele boyutunda yapılan çalışmalara teknik analiz boyutunun gerekli olduğu sunulmuştur.

Kullanıcıları ve işletmelerin saldırganlara karşı alabileceği önlemler olmakla birlikte en önemli adımın son kullanıcı farkındalığı olmaktadır. Zararlı yazılımlarla korunma yöntemleri i) Önleme, ii) Zararlı en aza indirme, iii) İlk hale geri dönüş olarak üç basamakta düşünülebilir. Önleme özel tasarlanmış programlar (Güvenlik duvarı, antivirüs programları, Sandbox gibi) ve kullanıcı farkındalığı ile oluşturulabilir. Zararlı yazılımların en çok kurban sistemlere sızma yöntemleri bilinerek kullanıcı farkındalığı oluşturulabilmektedir. Güvenlik açıklarını minimuma indirmek için kullanılmayan özelliklerin (uzak ağ bağlantıları gibi) kapatılması gereklidir. Ayrıca kaynağı bilinmeyen şüpheli e-postaların açılmaması ve lisanslı yazılımların güncel versiyonları ile kullanmakta oldukça önemlidir. Zararlı yazılımın sisteme sızdığı fark edildiğinde verdikleri zararlar genellikle geri dönülmez olmaktadır. Bu nedenle en kötü senaryo durumunu düşünülerek önemli dosya ve bilgileri korumak gereklidir. Son olarak tüm bilgi ve belgelere tekrar ulaşılabilir olması için farklı bir kapalı sistemde güncel (en fazla 30 günlük) yedekler almak, sistemin zararlı yazılıma maruz kalmadan ilk haline geri dönmesini sağlayabilmektedir.

Bu çalışmanın yalnızca zararlı yazılım analizcileri üzerinde değil, olası mağdur birçok bireysel internet kullanıcıları üzerinde de farkındalık yaratması beklenmektedir.

KAYNAKLAR (REFERENCES)

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

[2]. Kara, İlker, "Türkiye'de Zararlı Yazılımlarla Mücadelenin Uygulama Ve Hukuki Boyutunun Değerlendirilmesi." Akademik Bakış Uluslararası Hakemli Sosyal Bilimler Dergisi, 52: 87-98.

[3]. Lashkari, Arash Habibi, et al. "Towards a Network-Based Framework for Android Malware Detection and Characterization." Proceeding of the 15th International Conference on Privacy, Security and Trust. 2017.

[4]. Mariconti, Enrico, et al. "The cause of all evils: Assessing causality between user actions and malware activity." USENIX Workshop on Cyber Security Experimentation and Test (CSET). Vol. 10. USENIX, 2017.

[5]. Salem, Aleieldin, and Alexander Pretschner. "Poking the bear: lessons learned from

probing three Android malware datasets." Proceedings of the 1st International Workshop on Advances in Mobile App Analysis. ACM, 2018.

[6]. 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.

[7]. Tam, Kimberly, et al. "The evolution of android malware and android analysis techniques." ACM Computing Surveys (CSUR) 49.4 (2017): 76.

[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]. 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.

[10]. 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.

[11]. Kara, İ., & Aydos, M. (2019). THE GHOST IN THE SYSTEM: TECHNICAL ANALYSIS OF REMOTE ACCESS TROJAN. International Journal on Information Technologies & Security, 11(1).

[12]. Kara, I., & Aydos, M. (2018, December). 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.

[13]. Villeneuve, N. (2015). TeslaCrypt: Following the Money Trail and Learning the Human Costs of Ransomware. Threat Research Blog.

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

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

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

[17]. Conti, Mauro, Ankit Gangwal, and Sushmita Ruj. "On the economic significance of ransomware campaigns: A Bitcoin transactions perspective." Computers & Security (2018).

[18]. Bursztein, Elie, Kylie McRoberts, and Luca Invernizzi. "Tracking desktop ransomware payments." Black Hat USA, Las Vegas, United States (2017).

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

[20]. Bhardwaj, Akashdeep. "Ransomware: A rising threat of new age digital extortion." Online Banking Security Measures and Data Protection. IGI Global, 2017. 189-221.

[21]. Adamov, Alexander, and Anders Carlsson. "The state of ransomware. Trends and mitigation techniques." East-West Design & Test Symposium (EWDTS), 2017 IEEE. IEEE, 2017.

[22]. Pletinckx, Stijn, Cyril Trap, and Christian Doerr. "Malware Coordination using the Blockchain: An Analysis of the Cerber Ransomware." 2018 IEEE Conference on Communications and Network Security (*CNS)*. IEEE, 2018.

[23]. Aurangzeb, Sana, et al. "Ransomware: A Survey and Trends." Journal of Information Assurance & Security 6.2 (2017).