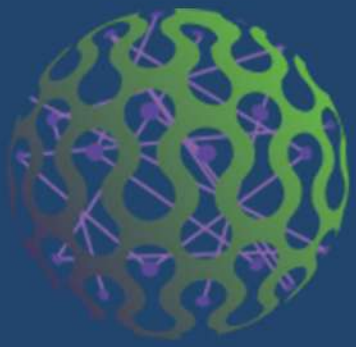


INTER
PROBE
INTELLIGENCE & ANALYTICS

# Zararlı Yazılım Trendleri

Hazırlayan
INTERPROBE

Kasım, 2022

# İçindekiler

# INTELLIGENCE ANALYTICS

InterProbe

Kasım 2022 – Zararlı Yazılım Trendleri

# 01 InterProbe Hakkında



InterProbe, özellikle hassas faaliyet alanlarında çalışan kuruluşlarla beraber her sektörden kuruluşların değişen teknolojik ihtiyaçlarını karşılamak için benzersiz ürünler, çözümler ve hizmetler tasarlar. Yüksek nitelikli mühendisler ve uzmanlardan oluşan ekibimiz ile yeni nesil teknolojileri tasarlamakta ve üretmekteyiz. Geliştirdiğimiz yazılımlarımız ile işinize değer katmak için çalışan gerçek bir ortağız.

Ankara'daki merkez ofisimiz, İstanbul Teknopark şubemiz ve yurt dışında Azerbaycan, Katar ve Kazakistan'daki ofislerimiz ile dünyadaki tüm kuruluşlara stratejik çözümler sunmaktayız. Ar-Ge yatırımlarımız ve güvenlik teknolojilerindeki trendleri yakından takip etmemizden dolayı uluslararası çaptaki kuruluşlarla iş birliği yapmaktayız. Türkiye'nin kalkınması ve büyümesi için güçlü bir sorumluluk duygusuna sahibiz; bu duygu, çalışmalarımıza yön veren en güçlü arzudur. InterProbe, özellikle genç mezunların ve üniversite öğrencilerinin yetkinlik ve becerilerini geliştirmeye yönelik eğitim ve staj programları düzenlemektedir. Ayrıca genç yazılımcılara proje desteği vermek için kaynak ayırmaktayız.

Birçok başarılı projeye imza atan Pavo Grup şirketlerinin bir parçası olarak ulusal kaynak ve yeteneklerle geliştirilmiş uçtan uca çözümleri bünyemizde sunmaktayız:

Savunma sanayiinde uzun yıllardır faaliyet gösteren ve ağırlıklı olarak dijital iletişim ve gömülü yazılım alanlarında hizmet veren **PAVOTEK**,

Elektromekanik üretim, montaj (SMD,THT) ve test konusunda uzmanlaşmış olan **PANOD**,

Aviyonik sistemler, askeri elektronik ve iletişim sistemleri, biyomedikal çözümler, güç elektroniği ve IoT alanlarında faaliyet gösteren **PAVELSIS**,

Ağ güvenliği ürünleri ve anahtarlama yönlendirme cihazları tasarlayan ve üreten **PNETWORKS**,

Veri merkezleri için inşaat, altyapı ve kurulum hizmetleri sunan InterData olmak üzere geleceğe emin adımlarla ilerlemekteyiz.

# 02 Giriş



Siber güvenlik her geçen gün daha fazla önem kazanmakta. Artık bir sistemi ele geçirmek ya da o sistemi saldırganlardan korumak çok daha zor. 2000'li yıllarda basit telnet zafiyeti ile ele geçirilebilen sistemler, standartlaşmış kütüphanelerin kullanımının yaygınlaşması ve siber güvenlik bilincinin artması gibi sebeplerden dolayı artık eskisi kadar yaygın değil. Bu nedenle saldırganlar da yeni stratejiler edindiler. Artık güvenliğin en zayıf halkalarından birinin insan olduğu daha fazla göze çarptı ve oltalama saldırılarının etkinliğinin arttığı görüldü. Saldırganlar bunun yanında yeni bir zafiyet bulunduğunda güncellenmesi zaman alacak sistemlerinde peşinde koşar oldular. Tabi her ne kadar bu teknikler etkili olsa da saldırganlar bununla beraber tekniklerini farklı yollarla değiştirmek durumundalar aksi takdirde imza tabanlı tarama sistemleri tarafından hızlıca tespit edilirler. Bu nedenle saldırganlar gönderdikleri zararlı kodları değiştirmenin hızlı yollarını geliştirdiler. İmza tabanlı sistemler bu tehditleri tespit etmekte yetersiz olduğundan hamle yapma sırasının onlara geldiğini anlayan siber güvenlik ekipleri zararlı yazılımların davranışlarını takip etmenin daha etkili olduğunu fark ettiler.

Bu noktada siber güvenlik ekiplerinin mevcut trendleri takip etmesini kolaylaştırmak adına InterProbe Fusion Center ekibi olarak InterProbe Zararlı Yazılım Bülteni'nin ikinci sayısı ile karşınızdayız. Bültenimiz teknik detaylar ile fazla meşgul olmayan ve siber güvenliğe dair ilgisi olan hemen herkesin anlayabileceği bir dilde, trend olan zararlı yazılımları, zararlıyı kullanan tehdit aktörlerinin mevcut aktiviteleri ve kullandıkları yeni teknikleri bulunduracak şekilde aylık olarak yayınlanacak.

**Keyifli okumalar.**

.

# Yönetici Özeti



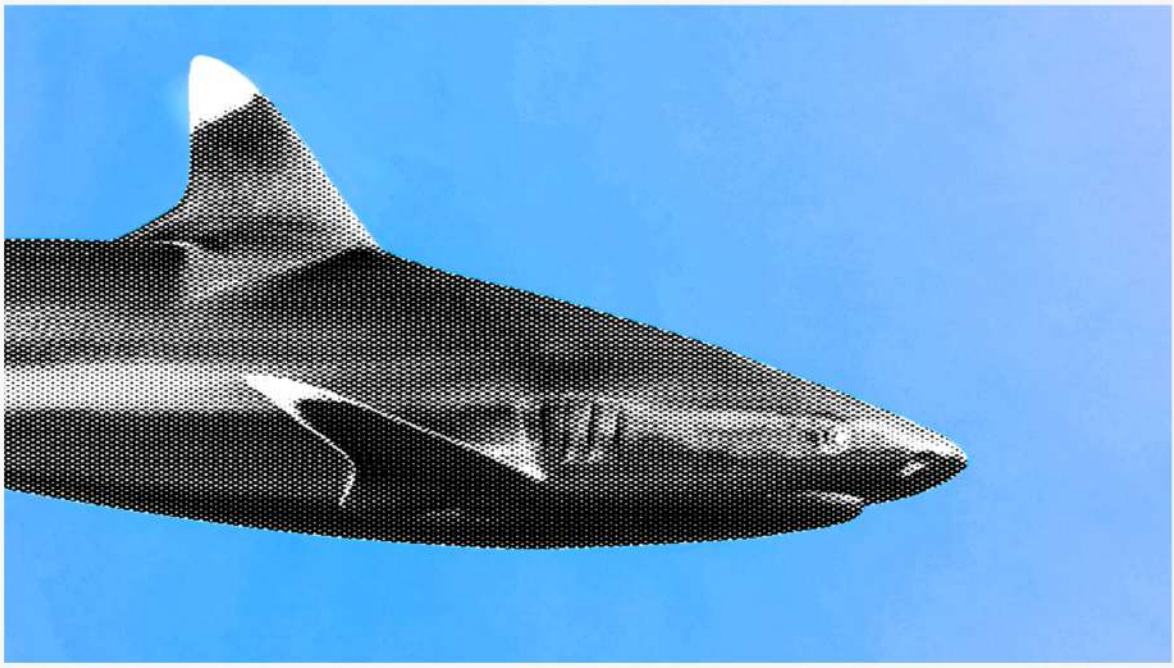
Siber güvenlik evreni her zamanki gibi yine hareketli geçiyor. Bu ay sizler için derlediğimiz araştırmalarımız:

- Bitdefender, Google Play Store'da bulunan yeni zararlılar keşfetti. Araştırmacılara göre bu uygulamalar Sharkbot ailesine ait.
- Cyble şirketindeki araştırmacılar AXLocker adında yeni bir fidye yazılımı keşfetti.
- Donut Leak sitesini yönetmekte olan tehdit aktörünün yeni bir fidye yazılımı geliştirdiği öğrenildi.
- Multi fonksiyonel olması planlanan Aurora zararlısı stealer olarak geri döndü
- Araştırmacılar qbot'un bazı sıfırıncı-gün zafiyetleri kullanarak saldırılar gerçekleştirdiğini keşfetti.

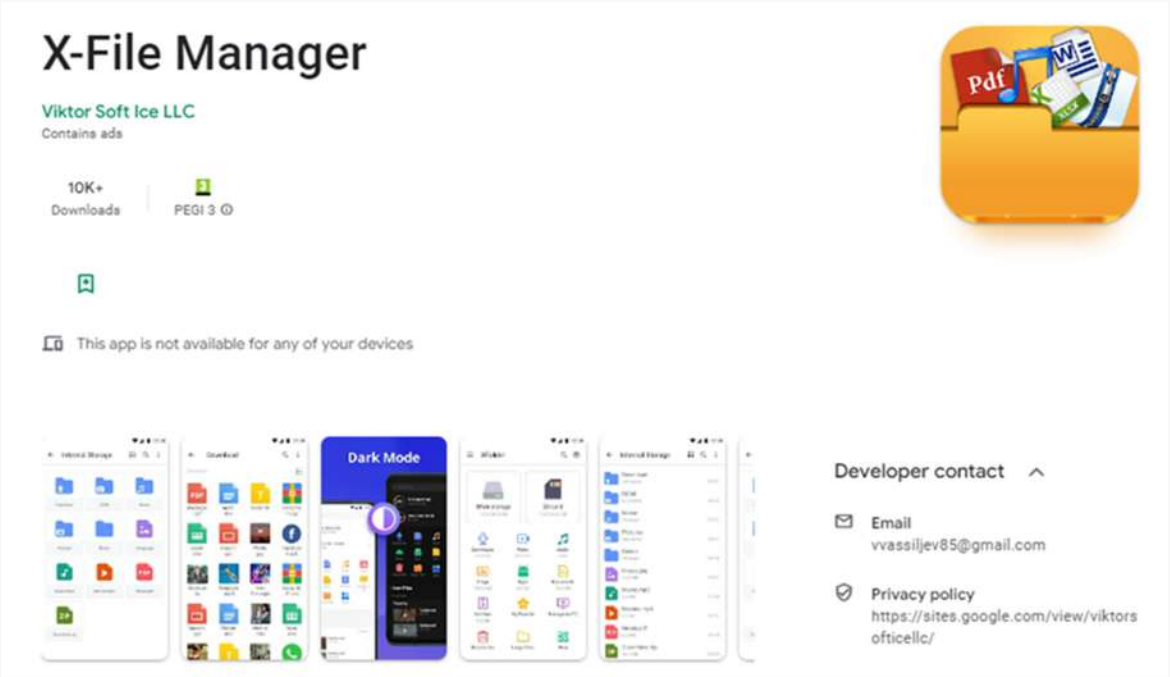
SharkBot

# 03 SharkBot

InterProbe



Geçtiğimiz günlerde Bitdefender tarafından Google Play Store üzerindeki yeni zararlı uygulamalar ele geçirildi. Bu kez "Dosya Yöneticisi" uygulamaları adı altında yayılan zararlı yazılımlar kullanıcıların cihazlarını enfekte etti.



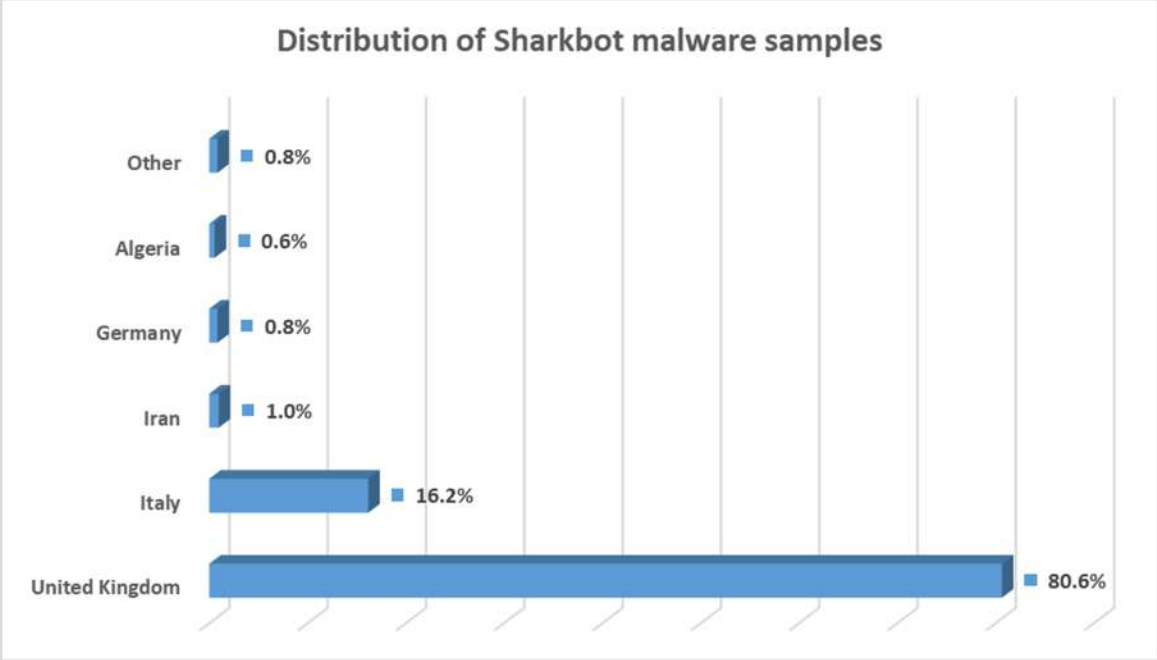

*Şekil 1. Zararlı uygulamaya ait görsel. (https://www.bitdefender.com/blog/labs/android-sharkbot-droppers-on-google-play-underlines-platforms-security-needs/ )*

SharkBot

Bitdefender tarafından yapılan araştırmaya göre bu zararlı uygulamalar "SharkBot" zararlı yazılım ailesinin bir üyesi olarak karşımıza çıkıyor. SharkBot zararlısı bir "Bankacılık" yazılımı olarak biliniyor. Bu zararlı yazılım kullanıcıların cihazlarında bulunan bankacılık uygulamalarının verilerini çalmak ve bu verileri tehdit aktörlerine göndermek gibi yetkinliklere sahiptir.

Zararlı uygulamalar cihazlara kurulduğu zaman normal bir dosya yöneticisi gibi görünürken arka planda aslında başka bir zararlı bir yazılımı uzaktan indirerek kullanıcıların cihazlarında faaliyet göstermeye başlıyor bu sayede sistemdeki gizliliğini ve kalıcılığını sağlıyor.

Bitdefender telemetry verilerine bakarak SharkBot zararlı yazılımının bu yöntemi kullanarak İngiltere, İtalya, İran ve Almanya gibi ülkelerde daha çok faaliyet gösterdiğini açıkladı.




*Şekil 2. SharkBot yazılımının en çok faaliyet gösterdiği ülkeler. (https://www.bitdefender.com/blog/labs/android-sharkbot-droppers-on-google-play-underlines-platforms-security-needs/)*

SharkBot

| Package name | Financial institution |
|---|---|
| com.barclays.android.barclaysmobilebanking | Barclays |
| com.bankofireland.mobilebanking | Bank of Ireland Mobile Banking |
| com.cooperativebank.bank | The Co-operative Bank |
| ftb.ibank.android | AIB (NI) Mobile |
| com.nearform.ptsb | permanent tsb |
| uk.co.mbna.cardservices.android | MBNA Mobile App |
| com.danskebank.mobilebank3.uk | Mobile Bank UK – Danske Bank |
| com.barclays.bca | Barclaycard |
| com.tescobank.mobile | Tesco Bank and Clubcard Pay+ |
| com.virginmoney.uk.mobile.android | Virgin Money Mobile Banking |
| com.cooperativebank.smile | "smile - the internet bank" |
| com.starlingbank.android | Starling Bank - Mobile Banking |
| uk.co.metrobankonline.mobile.android.production | Metro Bank |
| uk.co.santander.santanderUK | Santander Mobile Banking |
| uk.co.hsbc.hsbcukmobilebanking | HSBC UK Mobile Banking |
| uk.co.tsb.newmobilebank | TSB Mobile Banking |
| com.grppl.android.shell.BOS | Bank of Scotland Mobile App |
| com.grppl.android.shell.halifax | Halifax Mobile Banking |
| com.grppl.android.shell.CMBlloydsTSB73 | Lloyds Bank Mobile Banking |
| it.copergmps.rt.pf.android.sp.bmps | Banca MPS |
| it.extrabanca.mobile | NewExtraMobileBank |
| it.relaxbanking | RelaxBanking Mobile |
| it.bnl.apps.banking | BNL |
| it.bnl.apps.enterprise.hellobank | Hello Bank! |
| it.ingdirect.app | ING Italia |
| it.popso.SCRIGNOapp | SCRIGNOapp |
| posteitaliane.posteapp.appbpol | BancoPosta |
| com.latuabancaperandroid | Intesa Sanpaolo Mobile |
| com.latuabancaperandroid.pg | Intesa Sanpaolo Business |
| com.latuabancaperandroid.ispb | Intesa Sanpaolo Private |
| com.fineco.it | Fineco |
| com.CredemMobile | Credem |
| com.bmo.mobile | BMO Mobile Banking |
| com.fideuram.alfabetobanking | Alfabeto Banking |
| com.lynxspa.bancopopolare | YouApp - Mobile Banking |
| com.vipera.chebanca | CheBanca! |

*Şekil 3. SharkBot zararlı yazılımı tarafından hedef alınan bankacılık uygulamaları. (https://www.bitdefender.com/blog/labs/android-sharkbot-droppers-on-google-play-underlines-platforms-security-needs/)*

Bitdefender şirketinin araştırmalarına göre Google Play Store üzerinde bulunan diğer uygulamaların isimleri:

- File Voyager (com.potsepko9.FileManagerApp) 5.000+ indirme
- X-File Manager (com.victorsoftice.llc) 10.000+ indirme
- LiteCleaner M (com.ltdevelopergroups.litecleaner.m) 1.000+ indirme

SharkBot

# Özellikleri

- Komuta kontrol bağlantısı oluşturma
- Bankacılık verilerini çalmak
- Cihaz üzerindeki izleri temizleme
- Sanal ortam tespiti ve atlatma
- Sistem ile ilgili bilgileri toplama
- Konum bilgisi toplama

# MITRE ATT&CK Matrix

**Mitre Att&ck Matrix**

| Initial Access | Execution | Persistence | Privilege Escalation | Defense Evasion | Credential Access | Discovery | Lateral Movement | Collection | Exfiltration | Command and Control | Network Effects | Remote Service Effects | Impact |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| Valid Accounts | Windows Management Instrumentation | Path Interception | Path Interception | 2 Application Discovery | OS Credential Dumping | 1 System Network Connections Discovery | Remote Services | 1 Location Tracking | Exfiltration Over Other Network Medium | 1 Encrypted Channel | Eavesdrop on Insecure Network Communication | Remotely Track Device Without Authorization | 1 Generate Fraudulent Advertising Revenue |
| Default Accounts | Scheduled Task/Job | Boot or Logon Initialization Scripts | Boot or Logon Initialization Scripts | 1 Obfuscated Files or Information | LSASS Memory | 1 Location Tracking | Remote Desktop Protocol | 2 Network Information Discovery | Exfiltration Over Bluetooth | 1 Non-Standard Port | Exploit SS7 to Redirect Phone Calls/SMS | Remotely Wipe Data Without Authorization | 1 Delete Device Data |
| Domain Accounts | At (Linux) | Logon Script (Windows) | Logon Script (Windows) | Obfuscated Files or Information | Security Account Manager | 2 Application Discovery | SMB/Windows Admin Shares | Data from Network Shared Drive | Automated Exfiltration | 1 Ingress Tool Transfer | Exploit SS7 to Track Device Location | Obtain Device Cloud Backups | Delete Device Data |
| Local Accounts | At (Windows) | Logon Script (Mac) | Logon Script (Mac) | Binary Padding | NTDS | 1 System Information Discovery | Distributed Component Object Model | Input Capture | Scheduled Transfer | 2 Non-Application Layer Protocol | SIM Card Swap | | Carrier Billing Fraud |
| Cloud Accounts | Cron | Network Logon Script | Network Logon Script | Software Packing | LSA Secrets | 1 Process Discovery | SSH | Keylogging | Data Transfer Size Limits | 3 Application Layer Protocol | Manipulate Device Communication | | Manipulate App Store Rankings or Ratings |

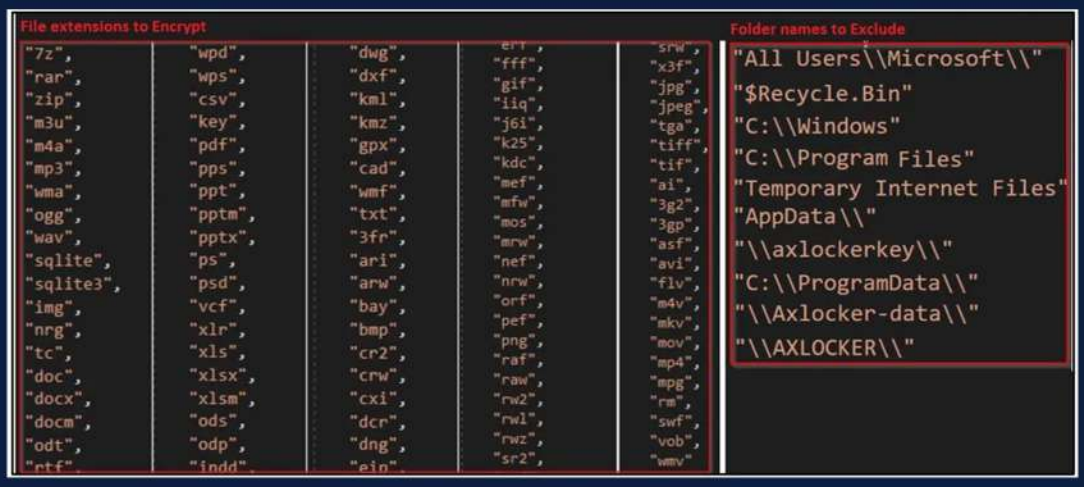
*Hash: fa7947933a3561b7174f1d94472dcf8633a03749c14342ce65dafe94db361140*

# Önlemler ve İyileştirmeler

- Cihazınıza uygulama kurmadan önce uygulamaya ait olan yorumları gözden geçirin.
- Bilinmeyen kaynaklardan uygulama kurmayın.
- Cihazınızda mutlaka güvenlik yazılımları kullanın.
- Uygulama kurarken uygulamanın istemiş olduğu izinleri gözden geçirin.

# 04 AXLocker

Cyble şirketi Kasım ayında yeni fidye yazılımı ailesi bulduğunu açıkladı. "AXLocker" adı verilen zararlı yazılım kullanıcıların sistemlerinde bulunan dosyaları şifreleyip fidye istemenin yanı sıra Discord hesaplarına ait olan bilgileri de çalıp tehdit aktörlerine göndermektedir.




*Şekil 1. AXLocker zararlı yazılımının hedef aldığı dosya uzantıları. (https://blog.cyble.com/2022/11/18/ax-locker-octocrypt-and-alice-leading-a-new-wave-of-ransomware-campaigns/)*

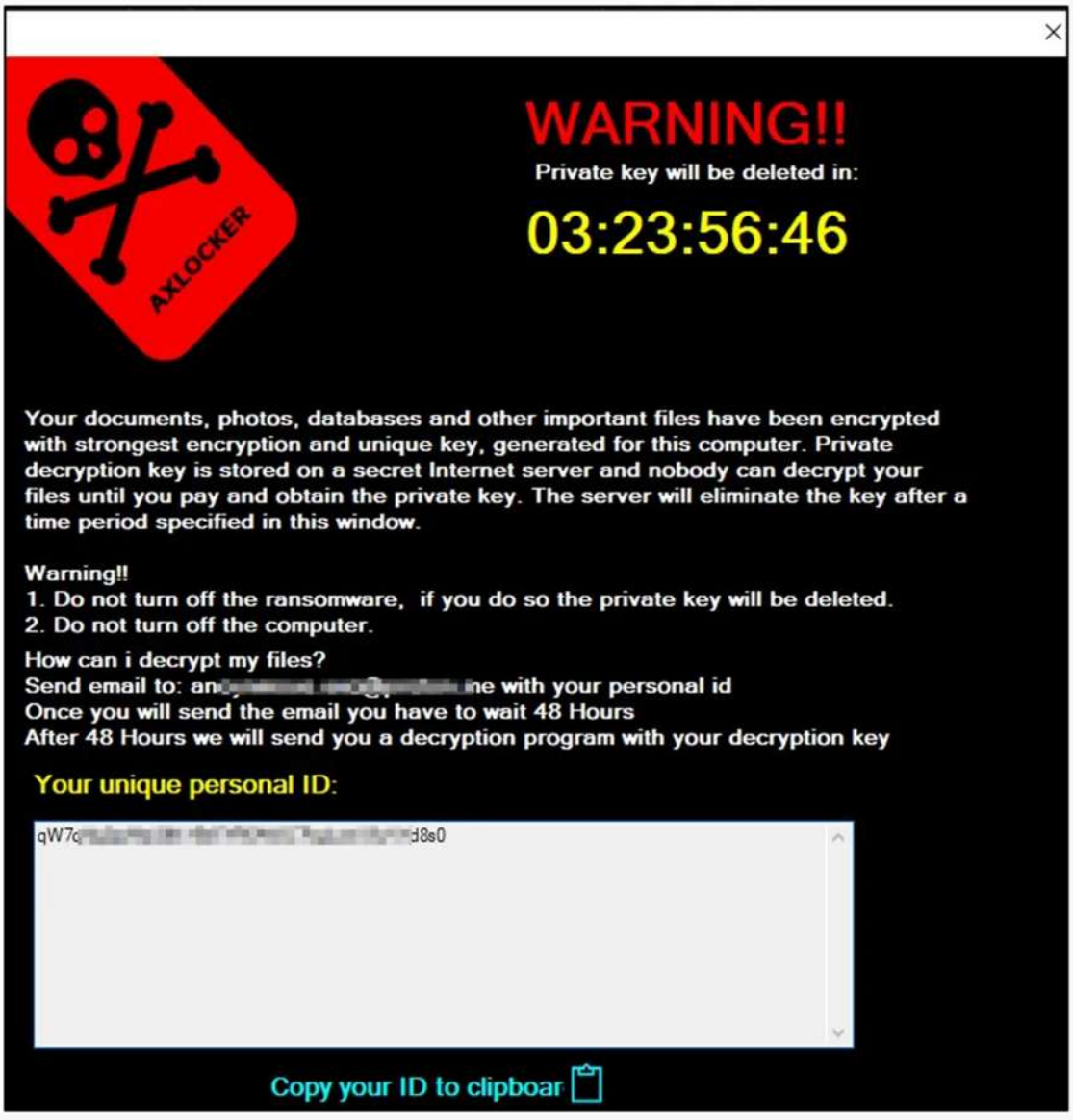
AXLocker zararlısının Discord hesaplarını el geçirmesinin nedenini "zararlı yazılımın bu hesaplar üzerinden yayılması ve daha çok kullanıcıyı hedeflemesi" olarak düşünen uzmanlar kullanıcıların Discord hesaplarının parolalarını değiştirmesini öneriyor.

Discord verilerini çalmak için zararlı yazılımın incelemiş olduğu dizinler:

- Discord\Local Storage\leveldb
- discordcanary\Local Storage\leveldb
- discordptb\leveldb
- Opera Software\Opera Stable\Local Storage\leveldb
- Google\Chrome\User Data\\Default\Local Storage\leveldb
- BraveSoftware\Brave-Browser\User Data\Default\Local Storage\leveldb
- Yandex\YandexBrowser\User Data\Default\Local Storage\leveldb

AXLocker

AXLocker .NET teknolojisi kullanılarak geliştirilmiştir. Dosyaları AES (Advanced Encryption System) algoritması ile şifrelerken diğer fidye yazılımlarının aksine dosya isimlerinde herhangi bir değişiklik yapmamaktadır. Şifreleme işlemi bittikten sonra kullanıcıların karşılarına tehdit aktörleri ile görüşmeleri için gerekli bilgilerin olduğu bir ekran çıkar. Bu ekranda kullanıcıların 48 saat içerisinde belirtilen e-posta adresi ile iletişime geçmeleri gerektiğini anlatan bir metin vardır fakat bu metnin içeriğinde fidye miktarı veya cüzdan adresi gibi bilgiler bulunmamaktadır.




*Şekil 2. AXLocker zararlısına ait fidye metni. (https://blog.cyble.com/2022/11/18/axlocker-octocrypt-and-alice-leading-a-new-wave-of-ransomware-campaigns/)*

## Özellikleri

- Discord verilerini ele geçirmek.
- Dosyaları şifrelemek.
- Discord verilerini ve sisteme ait bilgileri toplayıp tehdit aktörlerine göndermek.
- Sistemde bulunan güvenlik yazılımlarını tespit etmek.

AXLocker

# MITRE ATT&CK Matrix

**Mitre Att&ck Matrix**

| Initial Access | Execution | Persistence | Privilege Escalation | Defense Evasion | Credential Access | Discovery | Lateral Movement | Collection | Exfiltration | Command and Control | Network Effects | Remote Service Effects | Impact |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| Valid Accounts | Windows Management Instrumentation | Path Interception | Path Interception | 1 Disable or Modify Tools | OS Credential Dumping | 1 Security Software Discovery | Remote Services | 1 Archive Collected Data | Exfiltration Over Other Network Medium | Data Obfuscation | Eavesdrop on Insecure Network Communication | Remotely Track Device Without Authorization | 1 Data Encrypted for Impact |
| Default Accounts | Scheduled Task/Job | Boot or Logon Initialization Scripts | Boot or Logon Initialization Scripts | 2 Software Packing | LSASS Memory | 1 2 System Information Discovery | Remote Desktop Protocol | Data from Removable Media | Exfiltration Over Bluetooth | Junk Data | Exploit SS7 to Redirect Phone Calls/SMS | Remotely Wipe Data Without Authorization | Device Lockout |
| Domain Accounts | At (Linux) | Logon Script (Windows) | Logon Script (Windows) | 1 Deobfuscate/Decode Files or Information | Security Account Manager | Query Registry | SMB/Windows Admin Shares | Data from Network Shared Drive | Automated Exfiltration | Steganography | Exploit SS7 to Track Device Location | Obtain Device Cloud Backups | Delete Device Data |
| Local Accounts | At (Windows) | Logon Script (Mac) | Logon Script (Mac) | 1 Timestomp | NTDS | System Network Configuration Discovery | Distributed Component Object Model | Input Capture | Scheduled Transfer | Protocol Impersonation | SIM Card Swap | | Carrier Billing Fraud |
| Cloud Accounts | Cron | Network Logon Script | Network Logon Script | 2 Obfuscated Files or Information | LSA Secrets | Remote System Discovery | SSH | Keylogging | Data Transfer Size Limits | Fallback Channels | Manipulate Device Communication | | Manipulate App Store Rankings or Ratings |

*Hash: d51297c4525a9ce3127500059de3596417d031916eb9a52b737a62fb159f61e0*

# Önlemler ve İyileştirmeler

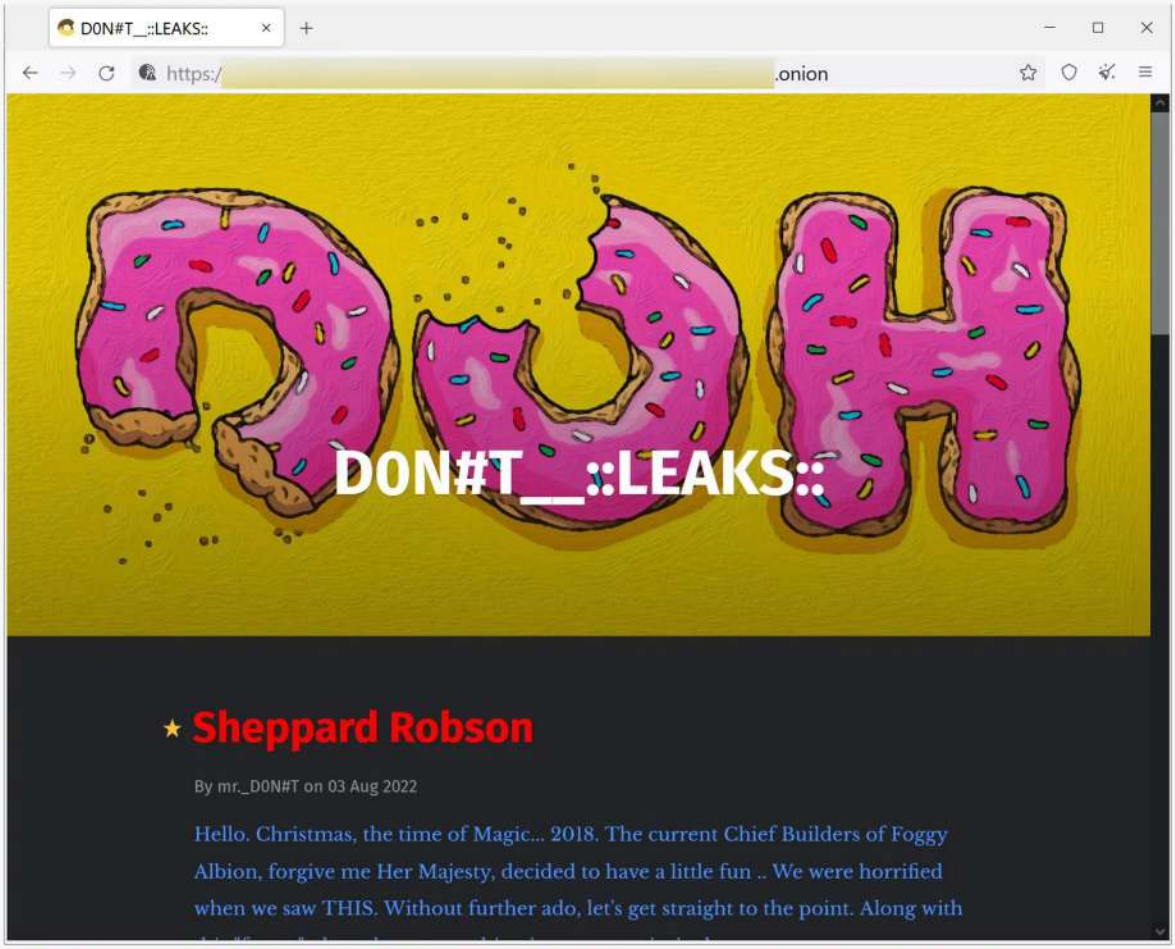
- Fidye yazılımı saldırıları için önlem olarak her zaman sisteminizin yedeğini alın.
- Eğer sisteminize AXLocker fidye yazılımı bulaştıysa Discord parolasını hemen değiştirin.
- Bilinmeyen kaynaklardan gelen yazılımları sisteminize kurmayın.
- Sisteminizde bulunan güvenlik yazılımlarının her zaman güncel olduğundan emin olun.

# 05 Donut Ransomware




Bu yılın ağustos ayında Yunan doğalgaz şirketi DESFA, İngiltere merkezli bir mimarlık firması olan Sheppard Robson ve bir inşaat sektörü devi olan Sando'ya yapılan fidye saldırılarıyla ilişkilendirilmiş olan Donut veri hırsızlığı grubunun yeni bir fidye yazılımı geliştirdiği keşfedildi.

Geçmiş ağustos ayında yapılan bu saldırılardan Sando'ya yapılan saldırı Hive ransomware grubu, DESFA'ya yapılan ise Rangar Locker tarafından üstlenilmiş olmasına karşın bu saldırılara ilişkin önemli miktarda verinin Donut veri hırsızlığı grubunun sızıntı sayfası olan Donut Leaks üzerinde yayınlandığı görüldü. Ağustos ayında sitede 2.8TB'a yakın boyutta sızıntı bulunduğu biliniyor.




*Şekil 1. Donut Leaks Websitesi Kaynak: https://www.bleepingcomputer.com/news/security/new-donut-leaks-extortion-gang-linked-to-recent-ransomware-attacks/*

Palo Alto'nun Unit 42 takımındaki araştırmacılardan Doel Santos'un paylaştığı bilgilere göre yeni fidye yazılımının iletişim için HelloXD fidye yazılımı ile benzer bir fidye metnine sahip olduğu ve iletişim için aynı TOX ID'yi kullandığını belirtti.

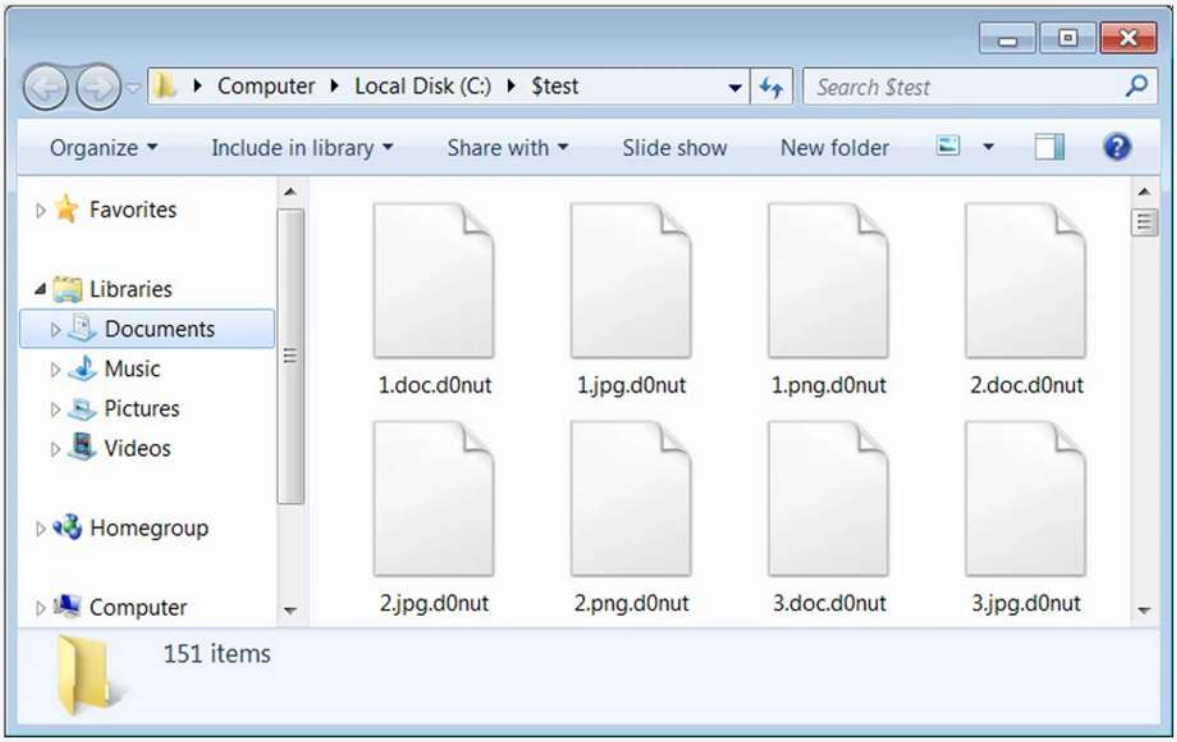
Ragnar Locker'ın tehdit aktörleri, birden fazla RaaS (Ransomware-as-a-Service) operasyonu için sızma işlemi gerçekleştirdiklerini belirtmişti. Bu bilgilerin ışığında Donut veri hırsızlığı grubunun Hive Ransomware ve Ragnar Locker ile ortak çalışan bir tehdit aktörü tarafından yönetildiğini ve bu aktörün işini büyütmek için bir fidye yazılımı geliştirdiğini söyleyebiliriz.

Zararlı çalıştırıldığında, bozulması durumunda sistemin çalışmasını olumsuz etkileyebilecek dosyaların şifrelenmesini önlemek amacıyla aşağıdaki listede bulunan stringleri içeren bütün dosya ve klasörleri atlamaktadır:

```
Edge
ntldr
Opera
bootsect.bak
Chrome
BOOTSTAT.DAT
boot.ini
AllUsers
Chromium
bootmgr
Windows
thumbs.db
ntuser.ini
ntuser.dat
desktop.ini
bootmgr.efi
autorun.inf
```

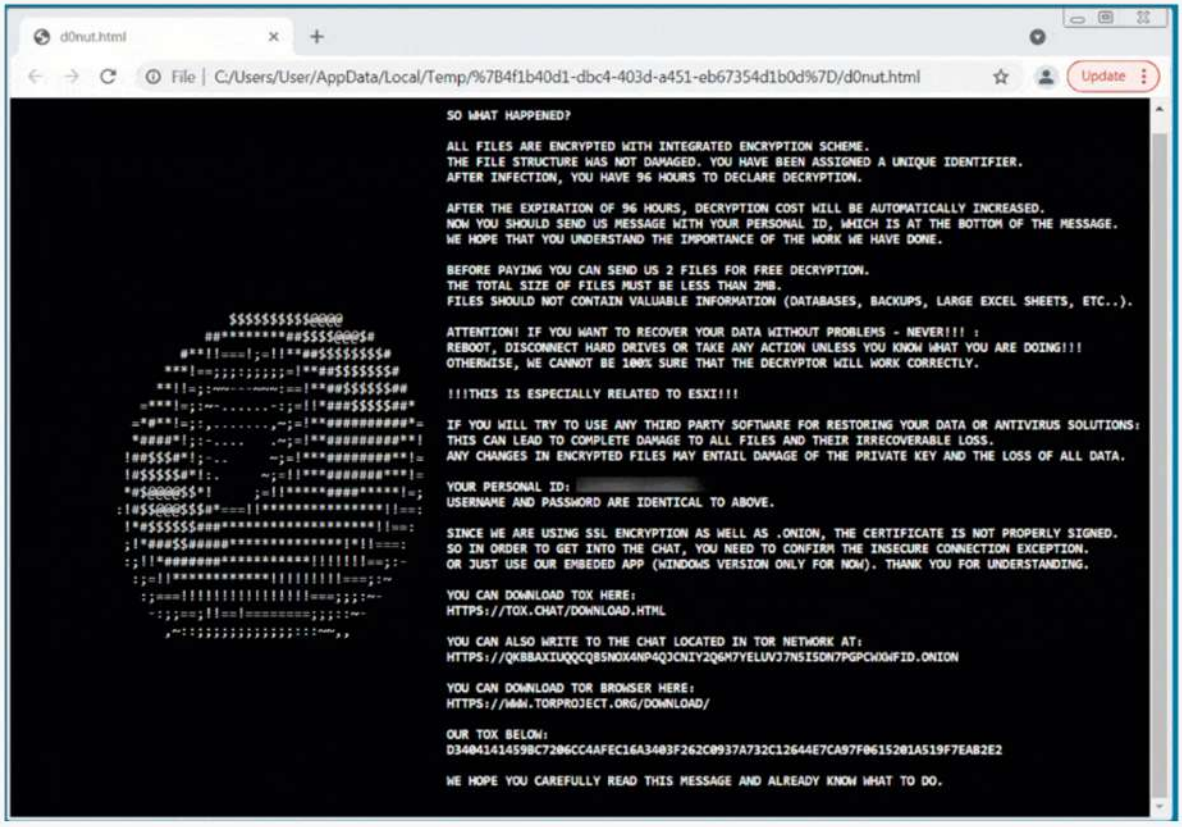
*Şekil 2. Donut fidye yazılımı tarafından kontrol edilen stringler. Kaynak: https://www.bleepingcomputer.com/news/security/donut-extortion-group-also-targets-victims-with-ransomware/*

Zararlı, bir dosyayı şifreledikten sonra dosyanın ismine ".d0nut" ekini koymaktadır.

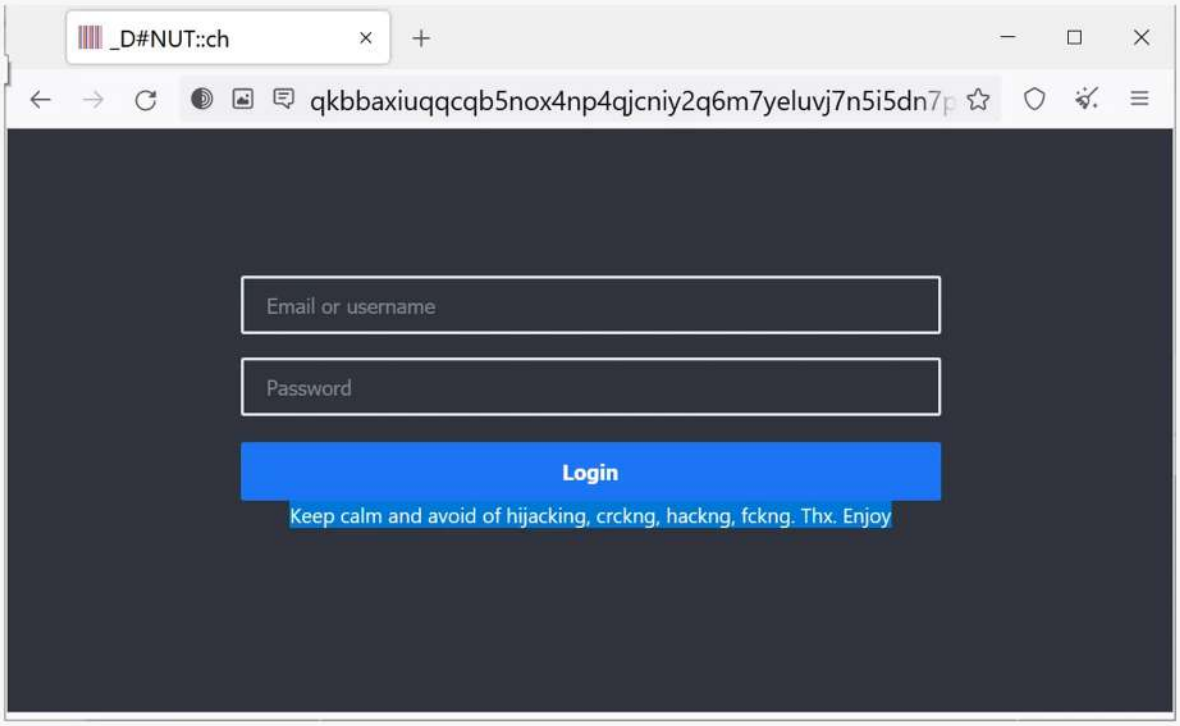



*Şekil 3. Zararlı şifrelenmiş dosyalara .d0nut uzantısı eklemekte. Kaynak:https://www.bleepingcomputer.com/news/security/donut-extortion-group-also-targets-victims-with-ransomware/*

Zararlının fidye notunda ise "donut.c" (Daha fazla bilgi için: "Donut math: how donut.c works" makalesine ulaşabilirsiniz.) adıyla bilinen bir kod ile oluşturulmuş olan animasyon ile aynı algoritmaya sahip olduğunu tahmin ettiğimiz bir üç boyutlu donut animasyonunun yanında iletişim için Tox ID'si ve .onion linki eklenmiş. Tehdit aktörü fidye yazılımının içine sızıntı sayfası için gateway görevi gören bir yazılım da eklemiştir.

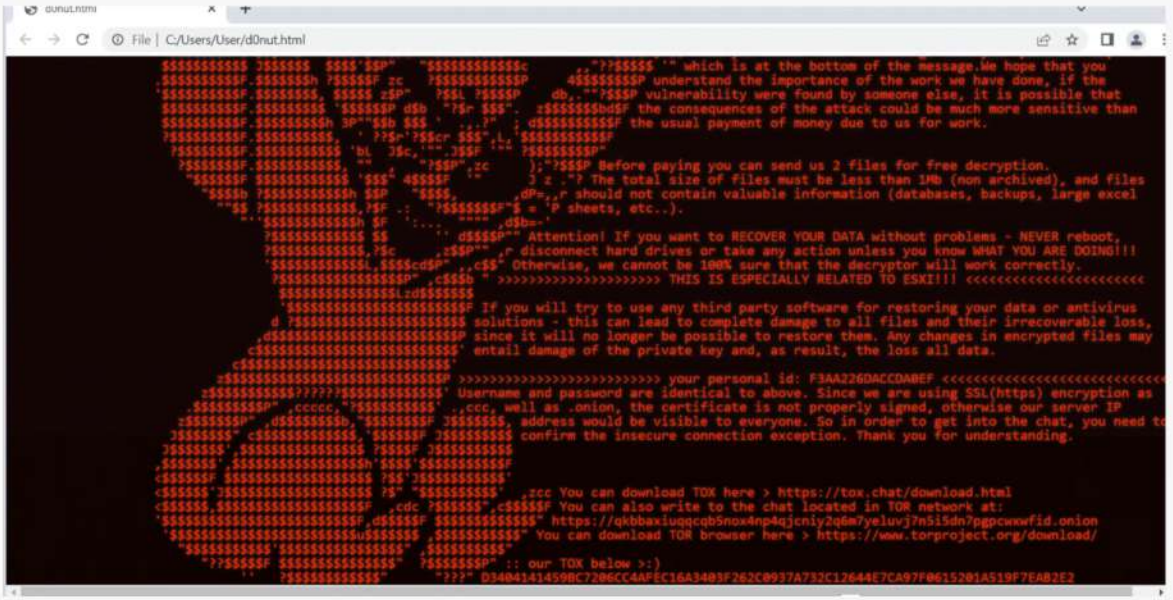



*Şekil 4. Fidye notu Kaynak: https://www.bleepingcomputer.com/news/security/donut-extortion-group-also-targets-victims-with-ransomware/*




*Şekil 5. İletişim için kullanılan onion sitesi. Kaynak: https://www.bleepingcomputer.com/news/security/donut-extortion-group-also-targets-victims-with-ransomware/*

Zararlının bazı varyasyonlarında kırmızı bir komut ekranı üzerinde fidye notu ve bir hayalet çizimi yazdıran farklı bir fidye notu bulunmaktadır.




*Şekil 6. Fidye notu. Kaynak: https://www.bleepingcomputer.com/news/security/donut-extortion-group-also-targets-victims-with-ransomware/*

Fidye notları, tarayıcı tarafından açıldığında javascript kullanılarak çözümlenecek şekilde kodlanmıştır.

Donut Ransomware

# MITRE ATT&CK Matrix

MITRE ATT&CK™ Techniques Detection

**Execution**

| ATT&CK ID | Name | Tactics | Description | Malicious Indicators | Suspicious Indicators | Informative Indicators |
|---|---|---|---|---|---|---|
| T1106 | Native API | • Execution | Adversaries may interact with the native OS application programming interface (API) to execute behaviors. Learn more | • Contains native function calls | | |

**Privilege Escalation**

| ATT&CK ID | Name | Tactics | Description | Malicious Indicators | Suspicious Indicators | Informative Indicators |
|---|---|---|---|---|---|---|
| T1055.001 | Dynamic-link Library Injection | • Privilege Escalation<br>• Defense Evasion | Adversaries may inject dynamic-link libraries (DLLs) into processes in order to evade process-based defenses as well as possibly elevate privileges. Learn more | | • Contains ability to create a remote thread (often used for process injection) | |

**Defense Evasion**

| ATT&CK ID | Name | Tactics | Description | Malicious Indicators | Suspicious Indicators | Informative Indicators |
|---|---|---|---|---|---|---|
| T1006 | Direct Volume Access | • Defense Evasion | Adversaries may directly access a volume to bypass file access controls and file system monitoring. Learn more | | • Contains ability to enumerate volumes | |
| T1055.001 | Dynamic-link Library Injection | • Privilege Escalation<br>• Defense Evasion | Adversaries may inject dynamic-link libraries (DLLs) into processes in order to evade process-based defenses as well as possibly elevate privileges. Learn more | | • Contains ability to create a remote thread (often used for process injection) | |
| T1027.002 | Software Packing | • Defense Evasion | Adversaries may perform software packing or virtual machine software protection to conceal their code. Learn more | | • PE file has unusual entropy sections | |
| T1497 | Virtualization/Sandbox Evasion | • Defense Evasion<br>• Discovery | Adversaries may employ various means to detect and avoid virtualization and analysis environments. Learn more | | | • Contains ability to delay the execution of current thread |

**Credential Access**

| ATT&CK ID | Name | Tactics | Description | Malicious Indicators | Suspicious Indicators | Informative Indicators |
|---|---|---|---|---|---|---|
| T1056.004 | Credential API Hooking | • Credential Access<br>• Collection | Adversaries may hook into Windows application programming interface (API) functions to collect user credentials. Learn more | | • Hooks API calls<br>• Installs hooks/patches the running | |

**Discovery**

| ATT&CK ID | Name | Tactics | Description | Malicious Indicators | Suspicious Indicators | Informative Indicators |
|---|---|---|---|---|---|---|
| T1083 | File and Directory Discovery | • Discovery | Adversaries may enumerate files and directories or may search in specific locations of a host or network share for certain information within a file system. Learn more | | • Calls an API's typically used for searching a directory for a files<br>• Tries to access non-existent files | • Contains ability to enumerates all mounted drives |
| T1057 | Process Discovery | • Discovery | Adversaries may attempt to get information about running processes on a system. Learn more | | • Calls an API typically used for taking snapshot of the specified processes<br>• Queries process information | |
| T1082 | System Information Discovery | • Discovery | An adversary may attempt to get detailed information about the operating system and hardware, including version, patches, hotfixes, service packs, and architecture. Learn more | | • Calls an API typically used to get product type<br>• Calls an API typically get system version information | • Contains ability to read software policies |
| T1497 | Virtualization/Sandbox Evasion | • Defense Evasion<br>• Discovery | Adversaries may employ various means to detect and avoid virtualization and analysis environments. Learn more | | | • Contains ability to delay the execution of current thread |

**Collection**

| ATT&CK ID | Name | Tactics | Description | Malicious Indicators | Suspicious Indicators | Informative Indicators |
|---|---|---|---|---|---|---|
| T1056.004 | Credential API Hooking | • Credential Access<br>• Collection | Adversaries may hook into Windows application programming interface (API) functions to collect user credentials. Learn more | | • Hooks API calls<br>• Installs hooks/patches the running process | |

# Önlemler ve İyileştirmeler

- Bir yedekleme politikası belirleyin ve bu politika çerçevesinde dosyalarınızı yedekleyin.
- Sistemlerinizi güncel tutun.

# 06 Aurora

InterProbe

SEKOIA şirketinde çalışan araştırmacılar Aurora zararlısı hakkında önemli bilgiler elde etti. Go programlama diliyle geliştirilmiş olan Aurora zararlısının aslen veri hırsızlığının yanında uzaktan erişim ve yükleme gibi özellikleri olan çok fonksiyonlu bir botnet zararlısı olarak sunulmaktaydı. Aurora zararlısının "Cheshire" adı verilen tehdit aktörü tarafından Malware-as-a-Service iş modeli kullanılarak pazarlandığı bilinmekte.

Araştırmacıların bulgularına göre Aurora zararlısı ağustos ayında stealer zararlısı olarak yeniden piyasaya sürüldü. Bu yıl Nisan ayında Rusça forumlarda pazaralanmaya başlayan Aurora, çok fonksiyonlu bir botnet olarak piyasaya sürülmüştü. Yılın devamında haziran ayına gelindiğinde tehdit aktörü Aurora'nın reklamlarını durdurdu. Temmuz ayında ise araştırmacılar Aurora zararlısının aktif komuta kontrol merkezi sayısının bir düzineden az olduğunu gözlemlediler.

**AURORA STEALER is the best styler on the market!**

**What makes my product so unique? Let me tell you!**

**Description:**

- AURORA STEALER has POLYMORN COMPILATION (scantime is reduced to 0)
- AURORA STEALER decrypts data on the server (no detectable runtime)
- AURORA STEALER collects more than 40 cryptocurrency wallets (DESKTOP/WEB versions!)
- AURORA STEALER at reception Metamask purse automatically picks up a password from a log, and also deduces SEED phrase, balance and address of a purse!
- AURORA STEALER collects passwords by reverse lookup (this method is much better than prepared scripts)
- AURORA STEALER runs on TCP sockets, it has an internal logs sorter and RunPe (.exe) Launcher
- AURORA STEALER only communicates with the server during license check, no further communication!
- AURORA STEALER is fully native and has no dependencies!
- THE UNIQUE OPPORTUNITY OF MY STEALER: the styler can be used without crypt because polymorph cleans the file to FUD!
- AURORA STEALER writen in GO language, weight of the raw stub ~4,2 mb

**COST:**

**$250** - one month license.

**$1500** - LifeTime license.

*Şekil 1. Aurora Stealer reklamının ingilizceye çevirilmiş hali. Kaynak: https://blog.sekoia.io/aurora-a-rising-stealer-flying-under-the-radar/*

Aurora

Ağustos ayına gelindiğinde ise hiç aktif komuta kontrol merkezi kalmamıştı ta ki Aurora zararlısı bir stealer olarak piyasaya tekrar sürülene kadar. Araştırmacılara göre Aurora, ağustos ayındaki çıkışından bu yana oldukça fazla sayıda tehdit aktörü tarafından sahiplenilmiş durumda. SEKOIA araştırmacıları bu gruplardan 9 tanesini saptamayı başardı:

| Traffers Team | Malware arsenal | Launch date | Last observed activity |
|---|---|---|---|
| SpaceTeam | Aurora | 18/11/2022 | 25/11/2022 |
| BrazzzersLogs | Aurora, Raccoon | 14/11/2022 | 14/11/2022 |
| DevilsTraff | Aurora, Raccoon | 30/10/2022 | 14/11/2022 |
| BartLogs | Aurora | 25/10/2022 | 25/10/2022 |
| RavenLogs | Aurora, Redline | 17/10/2022 | 24/11/2022 |
| Gfbg6 | Aurora | 14/09/2022 | 24/10/2022 |
| SAKURA | Aurora | 10/08/2022 | 04/11/2022 |
| HellRide | Aurora | 09/07/2022 | 21/11/2022 |
| YungRussia | Aurora | 05/04/2022 | 31/10/2022 |

*Şekil 2. Aurora zararlısını kullandığı tespit edilen tehdit aktörlerinin listesi. Kaynak: https://blog.sekoia.io/aurora-a-rising-stealer-flying-under-the-radar/*

Aurora için 2 farklı ödeme metodu bulunuyor. Bunlardan birincisi aylığı 250 dolardan abonelik sistemi iken ikincisi 1500 dolarlık ömür boyu lisans şeklinde pazarlanmakta.

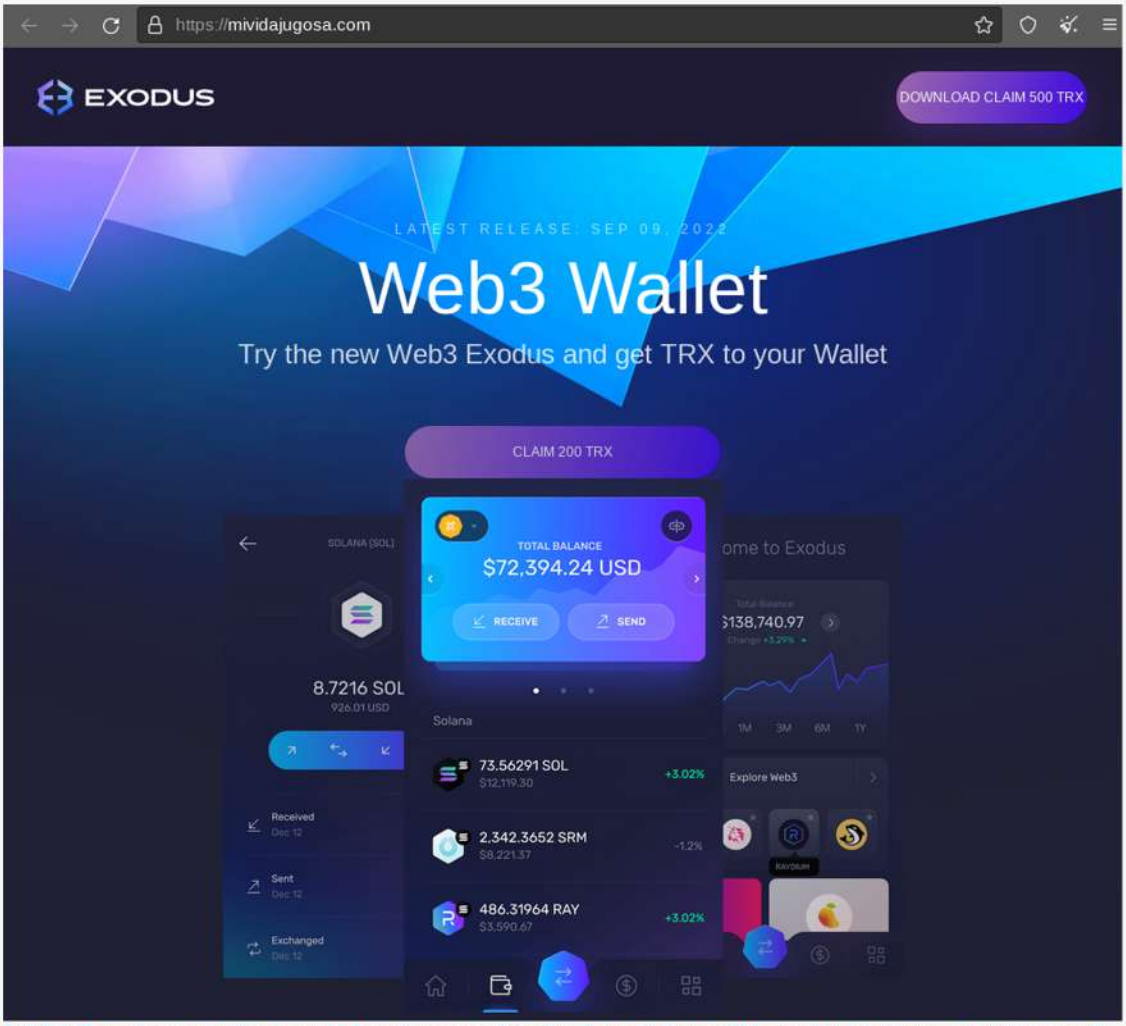
Zararlıyı kullanan tehdit aktörlerinin zararlı üzerinden prim yaptığı reklamlarda bulunmakta. Aşağıda Yeni bir grup olan BrazzersLogs grubunun Racoon Stealer ve Aurora Stealer kullandığını belirleterek prim yapmaya çalıştığı bir reklamı görebilirsiniz.


*Şekil 3. Brazzers Logs tehdit aktörünün bir reklamı. Kaynak:https://blog.sekoia.io/aurora-a-rising-stealer-flying-under-the-radar/*

Zararlının reklamlarında belirtilen özelliklere göre gizlilik ve veri toplayabildiği uygulama havuzunun genişliğinin zararlıyı öne çıkaran noktalar olduğu söylenebilir.

Aurora, tarayıcı verileri, donanım bilgileri, sistem bilgileri ve kripto cüzdanlardan veri toplayabilme becerilerine sahip. Komuta kontrol iletişimi ise 8081 daha yaygın olmakla beraber 8081 ve 9865 portlarından gerçekleştirilmekte.

Zararlının nasıl yayıldığı konusunda SEKOIA araştırmacıları 2 farklı metot keşfetmişler. 1. si sahte web siteleri üzerinden zararlıyı indirmeye ikna etmek iken 2. si son zamanlarda yaygınlaşmaya başlamış olan bir programın nasıl indirileceğini anlatarak kullanıcıları zararlı programlar indirmeye yönlendiren videolar üzerinden yayılma gibi görünüyor.




*Şekil 4. Zararlıyı yaymak amacıyla hazırlanmış sahte site. Kaynak:https://blog.sekoia.io/aurora-a-rising-stealer-flying-under-the-radar/*

# MITRE ATT&CK Matrix

MITRE ATT&CK™ Techniques Detection

### Execution

| ATT&CK ID | Name | Tactics | Description | Malicious Indicators | Suspicious Indicators | Informative Indicators |
|---|---|---|---|---|---|---|
| T1047 | Windows Management Instrumentation | • Execution | Adversaries may abuse Windows Management Instrumentation (WMI) to execute malicious commands and payloads. Learn more | | • Contains references to WMI/WMIC<br>• Found a reference to a WMI query string known to be used for VM detection<br>• Gets WMI data known to be used for VM detection via WMIC<br>• 1 confidential indicators | |
| T1106 | Native API | • Execution | Adversaries may interact with the native OS application programming interface (API) to execute behaviors. Learn more | | • 1 confidential indicators | • Calls an API typically used to create a process<br>• Contains ability to retrieve the NetBIOS name of the local computer (API string) |
| T1059.003 | Windows Command Shell | • Execution | Adversaries may abuse the Windows command shell for execution. Learn more | | | • Runs shell commands |

### Privilege Escalation

| ATT&CK ID | Name | Tactics | Description | Malicious Indicators | Suspicious Indicators | Informative Indicators |
|---|---|---|---|---|---|---|
| T1055.012 | Process Hollowing | • Privilege Escalation<br>• Defense Evasion | Adversaries may inject malicious code into suspended and hollowed processes in order to evade process-based defenses. Learn more | | | • Contains ability to write data into process memory (API string) |
| T1055 | Process Injection | • Privilege Escalation<br>• Defense Evasion | Adversaries may inject code into processes in order to evade process-based defenses as well as possibly elevate privileges. Learn more | • Writes data to a remote process | | |
| T1134 | Access Token Manipulation | • Privilege Escalation<br>• Defense Evasion | Adversaries may modify access tokens to operate under a different user or system security context to perform actions and bypass access controls. Learn more | | | • Contains ability to enable or disable privileges in the specified access token (API string) |

### Defense Evasion

| ATT&CK ID | Name | Tactics | Description | Malicious Indicators | Suspicious Indicators | Informative Indicators |
|---|---|---|---|---|---|---|
| T1497 | Virtualization/Sandbox Evasion | • Defense Evasion<br>• Discovery | Adversaries may employ various means to detect and avoid virtualization and analysis environments. Learn more | | | • The input sample possibly contains the ROTSCP instruction |
| T1027.002 | Software Packing | • Defense Evasion | Adversaries may perform software packing or virtual machine software protection to conceal their code. Learn more | | • 1 confidential indicators | • Matched Compiler/Packer signature |
| T1055.012 | Process Hollowing | • Privilege Escalation<br>• Defense Evasion | Adversaries may inject malicious code into suspended and hollowed processes in order to evade process-based defenses. Learn more | | | • Contains ability to write data into process memory (API string) |
| T1055 | Process Injection | • Privilege Escalation<br>• Defense Evasion | Adversaries may inject code into processes in order to evade process-based defenses as well as possibly elevate privileges. Learn more | • Writes data to a remote process | | |
| T1134 | Access Token Manipulation | • Privilege Escalation<br>• Defense Evasion | Adversaries may modify access tokens to operate under a different user or system security context to perform actions and bypass access controls. Learn more | | | • Contains ability to enable or disable privileges in the specified access token (API string) |
| T1112 | Modify Registry | • Defense Evasion | Adversaries may interact with the Windows Registry to hide configuration information within Registry keys, remove information as part of cleaning up, or as part of other techniques to aid in persistence and execution. Learn more | | | • Creates or modifies windows services |

### Credential Access

| ATT&CK ID | Name | Tactics | Description | Malicious Indicators | Suspicious Indicators | Informative Indicators |
|---|---|---|---|---|---|---|
| T1056.004 | Credential API Hooking | • Credential Access<br>• Collection | Adversaries may hook into Windows application programming interface (API) functions to collect user credentials. Learn more | | • Hooks API calls<br>• Installs hooks/patches the running process | |
| T1056.001 | Keylogging | • Credential Access<br>• Collection | Adversaries may log user keystrokes to intercept credentials as the user types them. Learn more | | | • Contains ability to retrieve information about pressed keystrokes (API string) |

Aurora

### Discovery

| ATT&CK ID | Name | Tactics | Description | Malicious Indicators | Suspicious Indicators | Informative Indicators |
|---|---|---|---|---|---|---|
| T1083 | File and Directory Discovery | • Discovery | Adversaries may enumerate files and directories or may search in specific locations of a host or network share for certain information within a file system. Learn more | | • 3 confidential indicators | • Contains ability to enumerate files on disk (API string) |
| T1012 | Query Registry | • Discovery | Adversaries may interact with the Windows Registry to gather information about the system, configuration, and installed software. Learn more | | • Reads information about supported languages<br>• Reads the active computer name<br>• Monitors specific registry key for changes | • Contains registry location strings |
| T1497 | Virtualization/Sandbox Evasion | • Defense Evasion<br>• Discovery | Adversaries may employ various means to detect and avoid virtualization and analysis environments. Learn more | | | • The input sample possibly contains the RDTSCP instruction |
| T1057 | Process Discovery | • Discovery | Adversaries may attempt to get information about running processes on a system. Learn more | | • Queries process information<br>• 1 confidential indicators | • Contains ability to enumerate processes (API string) |
| T1016 | System Network Configuration Discovery | • Discovery | Adversaries may look for details about the network configuration and settings, such as IP and/or MAC addresses, of systems they access or through information discovery of remote systems. Learn more | | | • Contains ability to query network adapter information (API string) |
| T1082 | System Information Discovery | • Discovery | An adversary may attempt to get detailed information about the operating system and hardware, including version, patches, hotfixes, service packs, and architecture. Learn more | | • Calls an API typically used to get product type<br>• Calls an API typically get system version information<br>• Reads the cryptographic machine GUID<br>• 2 confidential indicators | • Contains ability to retrieve information about operating system (API string)<br>• Contains ability to retrieve the specified system metric or system configuration setting (API string)<br>• Contains ability to read software policies<br>• Contains ability to find logical drives of the machine (API string)<br>• Contains ability to determine disk drive type (API string)<br>• Contains ability to retrieve the host's architecture (API string) |
| T1087.001 | Local Account | • Discovery | Adversaries may attempt to get a listing of local system accounts. Learn more | | | • Contains ability to retrieve information about user accounts on a server (API string) |
| T1518.001 | Security Software Discovery | • Discovery | Adversaries may attempt to get a listing of security software, configurations, defensive tools, and sensors that are installed on a system or in a cloud environment. Learn more | | • Possibly checks for known debuggers/analysis tools | |
| T1120 | Peripheral Device Discovery | • Discovery | Adversaries may attempt to gather information about attached peripheral devices and components connected to a computer system. Learn more | | | • Queries volume information |
| T1049 | System Network Connections Discovery | • Discovery | Adversaries may attempt to get a listing of network connections to or from the compromised system they are currently accessing or from remote systems by querying for information over the network. Learn more | | | • Contains ability to retrieve a list of sessions on a remote server (API string) |

### Collection

| ATT&CK ID | Name | Tactics | Description | Malicious Indicators | Suspicious Indicators | Informative Indicators |
|---|---|---|---|---|---|---|
| T1113 | Screen Capture | • Collection | Adversaries may attempt to take screen captures of the desktop to gather information over the course of an operation. Learn more | | | • Contains ability to take screen capture of the target machine (API string)<br>• Calls an API possibly used to take screenshots |
| T1005 | Data from Local System | • Collection | Adversaries may search local system sources, such as file systems and configuration files or local databases, to find files of interest and sensitive data prior to Exfiltration. Learn more | • Tries to steal browser sensitive information (file access)<br>• Tries to steal Crypto currency wallets information (file access) | • Accesses potentially sensitive information from local browsers<br>• 3 confidential indicators | • Found mail information locations related strings |
| T1056.004 | Credential API Hooking | • Credential Access<br>• Collection | Adversaries may hook into Windows application programming interface (API) functions to collect user credentials. Learn more | | • Hooks API calls<br>• Installs hooks/patches the running process | |
| T1114 | Email Collection | • Collection | Adversaries may target user email to collect sensitive information. Learn more | | • 1 confidential indicators | |
| T1056.001 | Keylogging | • Credential Access<br>• Collection | Adversaries may log user keystrokes to intercept credentials as the user types them. Learn more | | | • Contains ability to retrieve information about pressed keystrokes (API string) |

### Command and Control

| ATT&CK ID | Name | Tactics | Description | Malicious Indicators | Suspicious Indicators | Informative Indicators |
|---|---|---|---|---|---|---|
| T1571 | Non-Standard Port | • Command and Control | Adversaries may communicate using a protocol and port pairing that are typically not associated. Learn more | • Uses network protocols on unusual ports | | |
| T1071.001 | Web Protocols | • Command and Control | Adversaries may communicate using application layer protocols associated with web traffic to avoid detection/network filtering by blending in with existing traffic. Learn more | | | • Found user-agent related strings |

### Impact

| ATT&CK ID | Name | Tactics | Description | Malicious Indicators | Suspicious Indicators | Informative Indicators |
|---|---|---|---|---|---|---|
| T1471 | Data Encrypted for Impact | • Impact | An adversary may encrypt files stored on a mobile device to prevent the user from accessing them. Learn more | | | • Contains ability to perform encryption (API string) |

# Önlemler ve İyileştirmeler

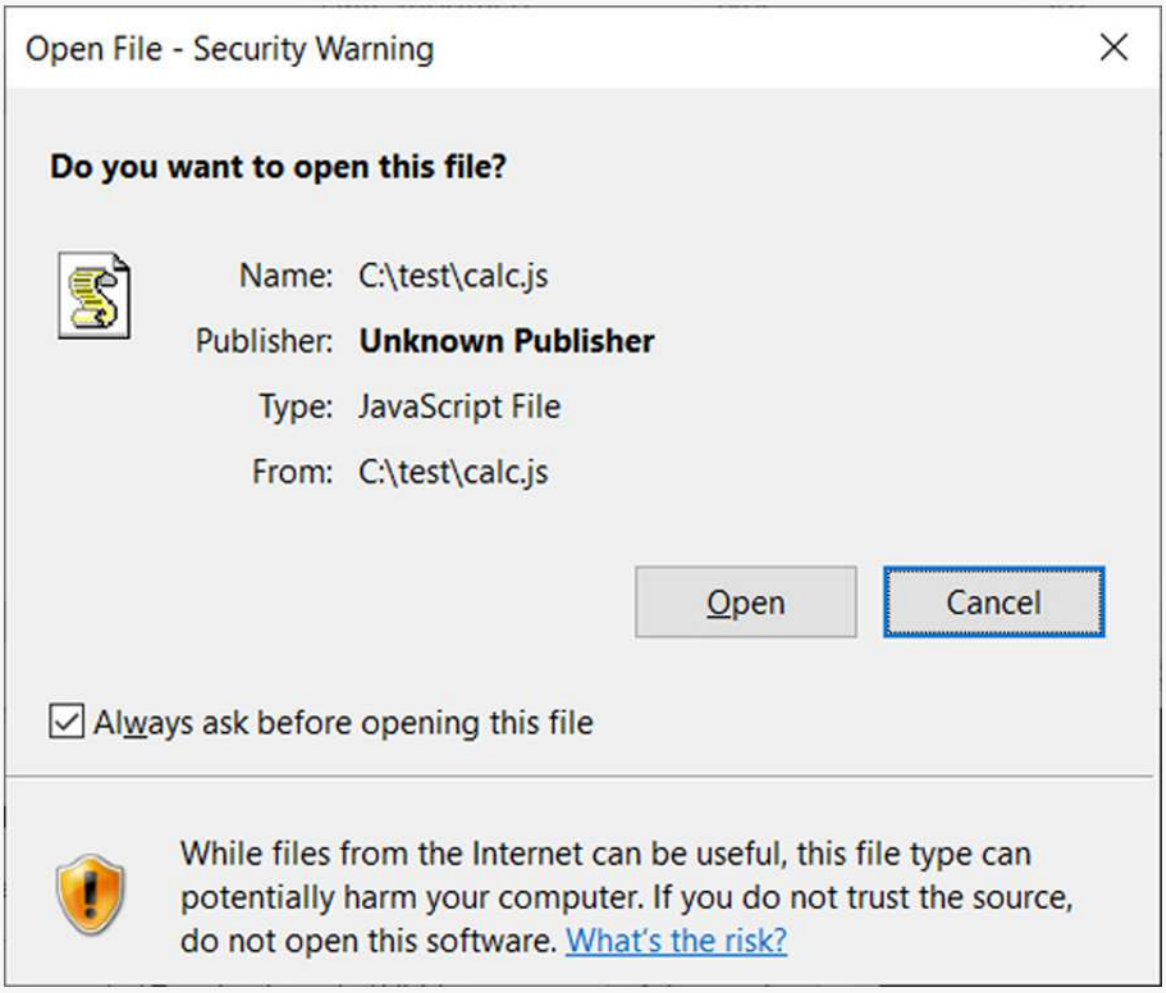
- Bulunduğunuz sitenin alan adını kontrol edin.
- Sistemde zararlıları aktif olarak araması amacıyla EDR veya antivirüs yazılımı edinin.
- Korsan yazılım indirmekten kaçının.
- Sisteminizi güncel tutun.

# 07 Qbot



Araştırmacılar qbot'un yeni varyasyonlarını keşfetti. Bu yeni qbot varyantlarının Windows sistemlerde bulunan Mark of The Web denilen bir sistemi etkisiz kılmak amacıyla sıfırıncı-gün zafiyetleri kullanıldığı görüldü.

Mark of the Web Windows sistemlerde bulunan bir çeşit işaretleme mekanizmasıdır. Amacı, internetten indirilen dosyaların indirildikleri konuma göre bir sınıflandırma yapmak ve güvenilirliklerini ölçmektir. Bu sistem sayesinde internetten indirilen güvenli görülmeyen dosyalar kullanıcı tarafından çalıştırılmak istendiğinde Windows, kullanıcıyı dosyanın kaynağına güvenmiyorsa çalıştırmaması gerektiği ile ilgili bir bildiri gönderebilmektedir.




*Şekil 1. Mark of the Web ile işaretlenmiş bir dosyanın açılması durumunda çıkan uyarı. Kaynak: https://www.bleepingcomputer.com/news/security/new-attacks-use-windows-security-bypass-zero-day-to-drop-malware/*

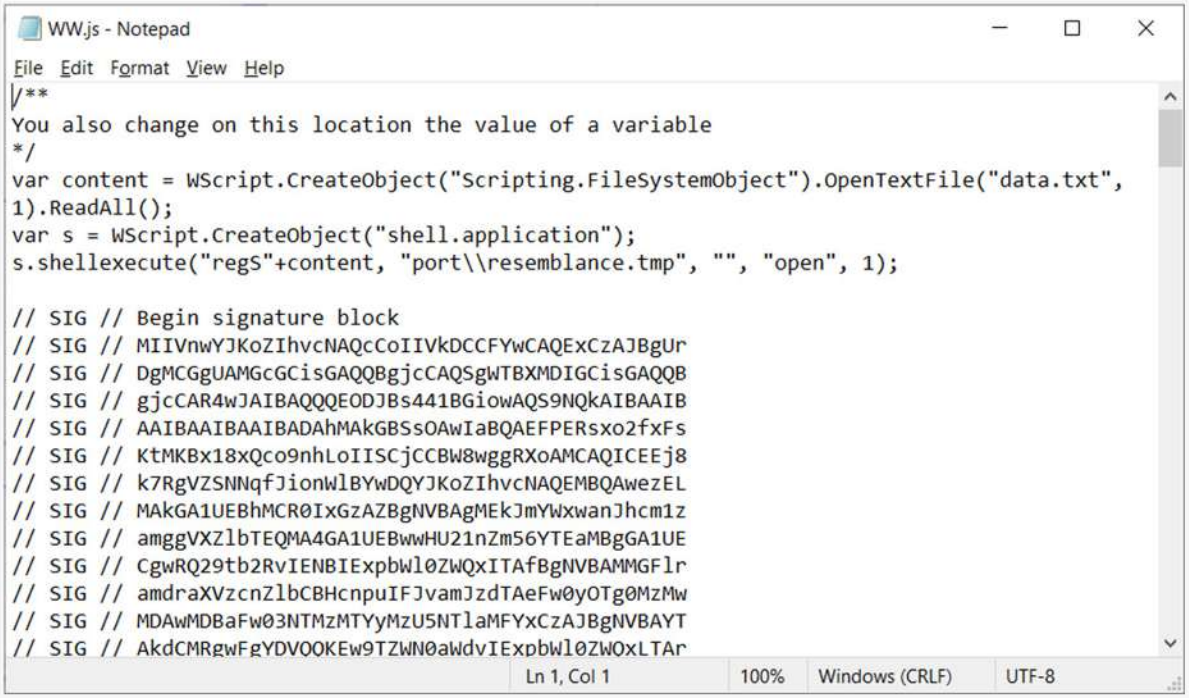
qbot

# Qbot Tarafından Kullanılan Zafiyetler

Qbot'un son zamanlarda kullandığı 2 farklı zafiyet ise bu sistemi atlatarak internetten indirilen dosyaların hiçbir uyarı penceresi olmaksızın çalıştırılabilmesine olanak sağlamaktadır.

Birinci zafiyet internetten indirilen ISO dosyalarının içinde bulunan dosyaların MotW(Mark of the Web) ile işaretlenmemesi dolayısıyla bu dosyaların içine yerleştirilmiş olan uygulamaların uyarı olmaksızın çalıştırılmasına olanak sağlamasıydı. Microsoft, bu açığı Kasım ayı güncellemeleri ile giderdi.

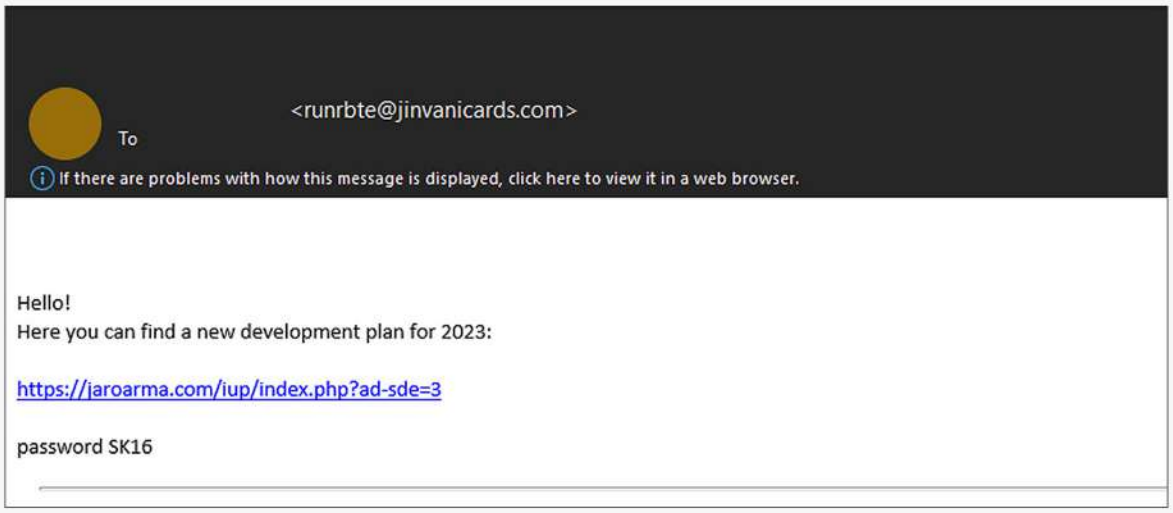
Diğer zafiyet ise Windows'ta bulunan bir dijital imzalama metodunu kullanarak imzalanan zararlı scriptlerin çalıştırılması durumunda uyarı ekranının görüntülenmesini önleyebilmekte. Bu imzalama metodu imzanın dosyanın içine base64 ile kodlanmış bir şekilde gömülmesine olanak sağlamakta.




*Şekil 2. Sıfırıncı gün zafiyetini sömüren bir örnek. Kaynak: https://www.bleepingcomputer.com/news/security/new-attacks-use-windows-security-bypass-zero-day-to-drop-malware/*

ProxyLife adındaki bir güvenlik araştırmacısının keşfetmiş olduğu yeni qbot saldırılarının bu zafiyeti sömürdüğü görülüyor. Saldırı, bir bağlantı üzerinden paylaşılan zararlı arşiv dosyası ve bu dosyanın şifresini içeren bir oltalama e-postası ile başlıyor.

qbot




*Şekil 3. Oltalama e-postası. Kaynak: https://www.bleepingcomputer.com/news/security/new-attacks-use-windows-security-bypass-zero-day-to-drop-malware/*

Şifrelenmiş arşiv dosyasının içinden bir başka arşiv dosyası ve onun da içinden bir IMG dosyası çıkıyor. IMG dosyası çift tıklanarak bir harici depolama olarak sisteme takıldığında ise içinde bir javascript dosyası, DLL (dynamic linked library) ve data.txt adında bir metin belgesi olduğu görülüyor. Qbot burada bulunan javascript dosyasını kullanarak sisteme bir DLL yüklemekte.

# MITRE ATT&CK Matrix

MITRE ATT&CK™ Techniques Detection

**Execution**

| ATT&CK ID | Name | Tactics | Description | Malicious Indicators | Suspicious Indicators | Informative Indicators |
|---|---|---|---|---|---|---|
| T1106 | Native API | • Execution | Adversaries may interact with the native OS application programming interface (API) to execute behaviors. Learn more | • Contains native function calls | • 1 confidential indicators | • Imports GetCommandLine API<br>• Calls an API typically used to create a process |
| T1059.003 | Windows Command Shell | • Execution | Adversaries may abuse the Windows command shell for execution. Learn more | | | • Runs shell commands |

**Privilege Escalation**

| ATT&CK ID | Name | Tactics | Description | Malicious Indicators | Suspicious Indicators | Informative Indicators |
|---|---|---|---|---|---|---|
| T1055.012 | Process Hollowing | • Privilege Escalation<br>• Defense Evasion | Adversaries may inject malicious code into suspended and hollowed processes in order to evade process-based defenses. Learn more | • Creates a process in suspended mode (likely for process injection) | | |
| T1055 | Process Injection | • Privilege Escalation<br>• Defense Evasion | Adversaries may inject code into processes in order to evade process-based defenses as well as possibly elevate privileges. Learn more | • Writes data to a remote process | | |

**Defense Evasion**

| ATT&CK ID | Name | Tactics | Description | Malicious Indicators | Suspicious Indicators | Informative Indicators |
|---|---|---|---|---|---|---|
| T1027.002 | Software Packing | • Defense Evasion | Adversaries may perform software packing or virtual machine software protection to conceal their code. Learn more | | • PE file has unusual entropy resources | • Matched Compiler/Packer signature |
| T1055.012 | Process Hollowing | • Privilege Escalation<br>• Defense Evasion | Adversaries may inject malicious code into suspended and hollowed processes in order to evade process-based defenses. Learn more | • Creates a process in suspended mode (likely for process injection) | | |
| T1140 | Deobfuscate/Decode Files or Information | • Defense Evasion | Adversaries may use Obfuscated Files or Information to hide artifacts of an intrusion from analysis. Learn more | | • Contains escaped byte string (often part of obfuscated shellcode) | |
| T1055 | Process Injection | • Privilege Escalation<br>• Defense Evasion | Adversaries may inject code into processes in order to evade process-based defenses as well as possibly elevate privileges. Learn more | • Writes data to a remote process | | |
| T1112 | Modify Registry | • Defense Evasion | Adversaries may interact with the Windows Registry to hide configuration information within Registry keys, remove information as part of cleaning up, or as part of other techniques to aid in persistence and execution. Learn more | | • Modifies Software Policy Settings<br>• Modifies proxy settings | • Creates or modifies windows services<br>• Accesses System Certificates Settings |
| T1070.004 | File Deletion | • Defense Evasion | Adversaries may delete files left behind by the actions of their intrusion activity. Learn more | | • Marks file for deletion<br>• Opens file with deletion access rights | |

**Credential Access**

| ATT&CK ID | Name | Tactics | Description | Malicious Indicators | Suspicious Indicators | Informative Indicators |
|---|---|---|---|---|---|---|
| T1056.004 | Credential API Hooking | • Credential Access<br>• Collection | Adversaries may hook into Windows application programming interface (API) functions to collect user credentials. Learn more | | • Installs hooks/patches the running process<br>• Hooks API calls | |

Discovery

| ATT&CK ID | Name | Tactics | Description | Malicious Indicators | Suspicious Indicators | Informative Indicators |
|---|---|---|---|---|---|---|
| T1082 | System Information Discovery | • Discovery | An adversary may attempt to get detailed information about the operating system and hardware, including version, patches, hotfixes, service packs, and architecture. Learn more | | • Reads the cryptographic machine GUID<br>• 5 confidential indicators | • Contains ability to read software policies<br>• Contains ability to query the machine version |
| T1057 | Process Discovery | • Discovery | Adversaries may attempt to get information about running processes on a system. Learn more | | • 2 confidential indicators | |
| T1016 | System Network Configuration Discovery | • Discovery | Adversaries may look for details about the network configuration and settings, such as IP and/or MAC addresses, of systems they access or through information discovery of remote systems. Learn more | • Tries to gather system network configuration using IPCONFIG<br>• Detected network related fingerprinting/snooping attempt<br>• Calls an API typically used to retrieve the IPv4 to physical address mapping table | | |
| T1012 | Query Registry | • Discovery | Adversaries may interact with the Windows Registry to gather information about the system, configuration, and installed software. Learn more | | • Reads information about supported languages<br>• Checks warning level of secure to non-secure traffic redirection<br>• Queries the internet cache settings (often used to hide footprints in index.dat or internet cache)<br>• Queries sensitive IE security settings<br>• 2 confidential indicators | • Reads Windows Trust Settings<br>• Accesses Software Policy Settings |
| T1135 | Network Share Discovery | • Discovery | Adversaries may look for folders and drives shared on remote systems as a means of identifying sources of information to gather as a precursor for Collection and to identify potential systems of interest for Lateral Movement. Learn more | | • 1 confidential indicators | |
| T1083 | File and Directory Discovery | • Discovery | Adversaries may enumerate files and directories or may search in specific locations of a host or network share for certain information within a file system. Learn more | | • 2 confidential indicators | • Contains ability to enumerate files on disk (API string) |
| T1010 | Application Window Discovery | • Discovery | Adversaries may attempt to get a listing of open application windows. Learn more | | | • Scanning for window names |

Collection

| ATT&CK ID | Name | Tactics | Description | Malicious Indicators | Suspicious Indicators | Informative Indicators |
|---|---|---|---|---|---|---|
| T1056.004 | Credential API Hooking | • Credential Access<br>• Collection | Adversaries may hook into Windows application programming interface (API) functions to collect user credentials. Learn more | | • Installs hooks/patches the running process<br>• Hooks API calls | |
| T1114 | Email Collection | • Collection | Adversaries may target user email to collect sensitive information. Learn more | | • Found a potential E-Mail address in binary/memory | |
| T1113 | Screen Capture | • Collection | Adversaries may attempt to take screen captures of the desktop to gather information over the course of an operation. Learn more | | | • Calls an API possibly used to take screenshots |

Command and Control

| ATT&CK ID | Name | Tactics | Description | Malicious Indicators | Suspicious Indicators | Informative Indicators |
|---|---|---|---|---|---|---|
| T1573 | Encrypted Channel | • Command and Control | Adversaries may employ a known encryption algorithm to conceal command and control traffic rather than relying on any inherent protections provided by a communication protocol. Learn more | | | • Possibly tries to communicate over SSL connection (HTTPS)<br>• Uses HTTPS for communication |
| T1071.004 | DNS | • Command and Control | Adversaries may communicate using the Domain Name System (DNS) application layer protocol to avoid detection/network filtering by blending in with existing traffic. Learn more | | | • Queries DNS server |
| T1571 | Non-Standard Port | • Command and Control | Adversaries may communicate using a protocol and port pairing that are typically not associated. Learn more | • Uses network protocols on unusual ports | | |
| T1095 | Non-Application Layer Protocol | • Command and Control | Adversaries may use a non-application layer protocol for communication between host and C2 server or among infected hosts within a network. Learn more | | • Contains indicators of bot communication commands | |
| T1071.001 | Web Protocols | • Command and Control | Adversaries may communicate using application layer protocols associated with web traffic to avoid detection/network filtering by blending in with existing traffic. Learn more | | | • GETs files from a webserver |

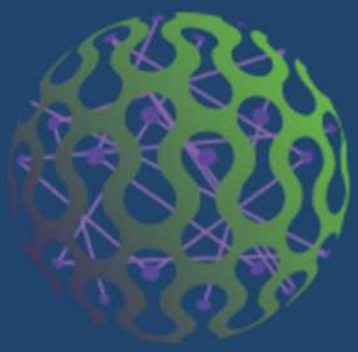
bot

# Önlemler ve İyileştirmeler

- Sisteminizi güncel tutun.
- Şirket personelinizi bilinçlendirmek için eğitimler düzenleyin.
- Dış ağdan gelen e-postaların daha dikkatli incelenmesi adına dış ağdan geldiğine dair bir işaret yerleştirin.

# Referanslar


- https://www.hybrid-analysis.com/sample/8ca16991684f7384c12b6622b8d1bcd23bc27f186f499c2059770ddd3031f274
- https://www.bleepingcomputer.com/news/security/new-attacks-use-windows-security-bypass-zero-day-to-drop-malware/
- https://www.bleepingcomputer.com/news/security/aurora-infostealer-malware-increasingly-adopted-by-cybergangs/
- https://www.hybrid-analysis.com/sample/459a8faa7924a25a15f64c34910324baed5c24d2fe68badd9a4a320628c08cb8/638d4d3408a2f9081373e6e0
- https://blog.sekoia.io/aurora-a-rising-stealer-flying-under-the-radar/
- https://www.bleepingcomputer.com/news/security/donut-extortion-group-also-targets-victims-with-ransomware/
- https://www.hybrid-analysis.com/sample/9455b7fcf93f0a5a6f9c099fbe938f5a9169f8d3dcc83833aa2c0f903518cfa3/63848e8c53bfbd53873fcd7d
- https://www.bleepingcomputer.com/news/security/new-donut-leaks-extortion-gang-linked-to-recent-ransomware-attacks/
- https://infosec.exchange/@santosdoel/109388990804963479
- https://blog.cyble.com/2022/11/18/axlocker-octocrypt-and-alice-leading-a-new-wave-of-ransomware-campaigns/
- https://www.bleepingcomputer.com/news/security/new-ransomware-encrypts-files-then-steals-your-discord-account/
- https://www.joesandbox.com/analysis/747203/0/html
- https://www.joesandbox.com/analysis/753089/0/html
- https://www.bitdefender.com/blog/labs/android-sharkbot-droppers-on-google-play-underlines-platforms-security-needs/
- https://www.bleepingcomputer.com/news/security/android-file-manager-apps-infect-thousands-with-sharkbot-malware/



INTER
PROBE
INTELLIGENCE & ANALYTICS

Mutlukent Mah. Fesleğen Sok. No:9 Çankaya Ankara Türkiye
**Phone:** +90 312 225 10 93, **Email:** info@interprobe.com.tr, **Web:** https://interprobe.com.tr