Bilgi Hırsızları

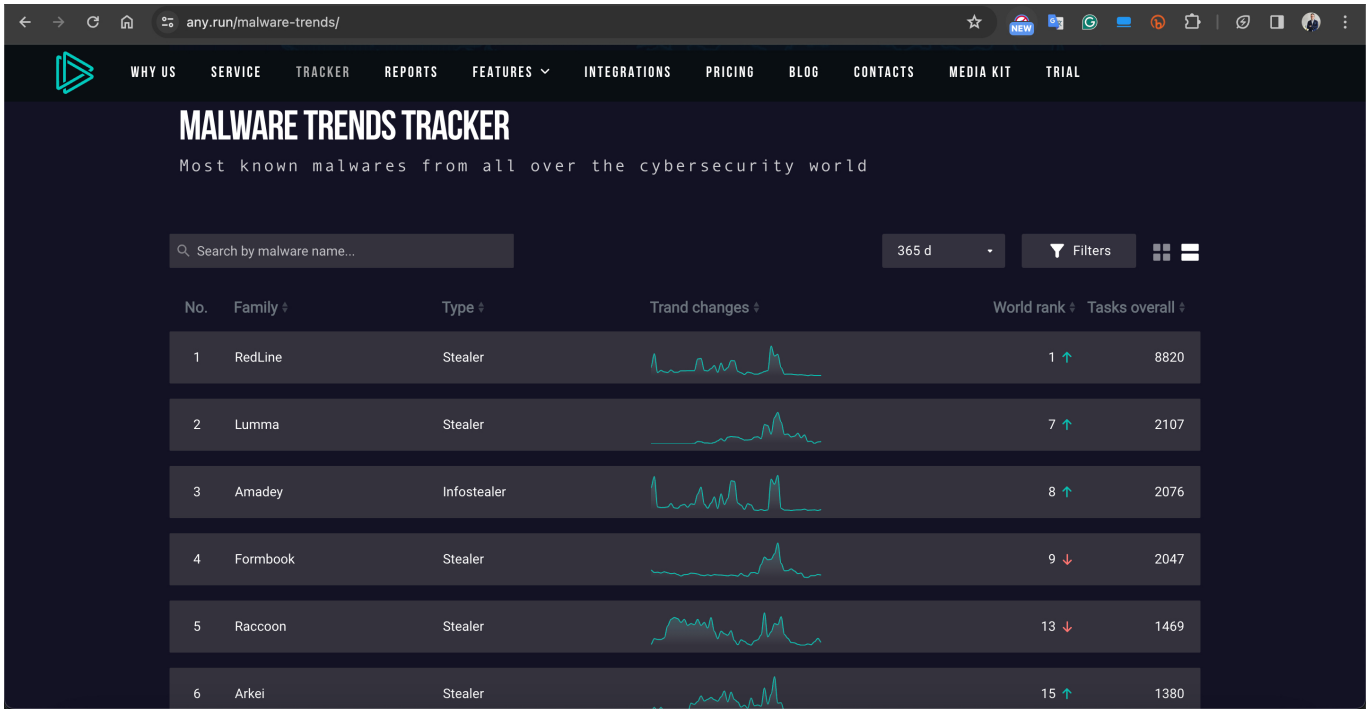
written by Mert SARICA | 2 September 2024
If you are looking for an English version of this article, please visit here.

İÇİNDEKİLER

Başlangıç

Son yıllarda karşılaşılan Uber, Airbus, Grand Theft Auto VI ve benzer siber güvenlik vakalarına baktığımızda, infostealers yani bilgi hırsızlığı amacıyla kullanılan zararlı yazılımların ön plana çıktığını ve siber suç ekosisteminde giderek daha önemli bir rol oynadığını görüyoruz.

Yapılan araştırmalar da 2023 yılında bu türdeki zararlı yazılım kaynaklı siber güvenlik vakalarının 2022 yılına kıyasla iki kat arttığını, Rus market yerlerinde (Russian Market) bu zararlı yazılımlar tarafından çalınan ve satışa sunulan kayıt dosyalarının (logs) 2021 yılından bu yana %690 arttığına dikkat çekiyor.

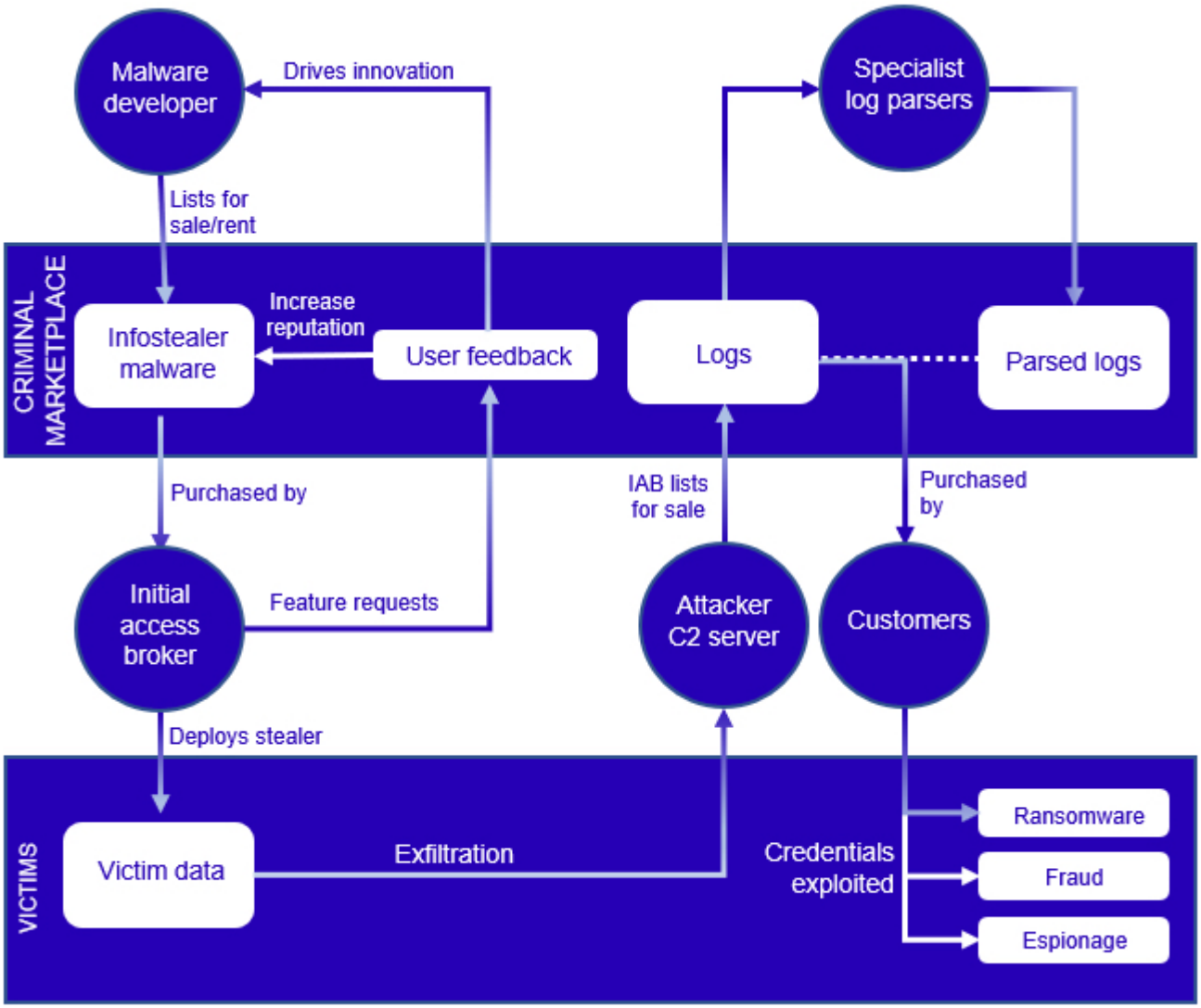


Referans: ANY.RUN

Bilgi Hırsızı Zararlı Yazılımı Nedir?

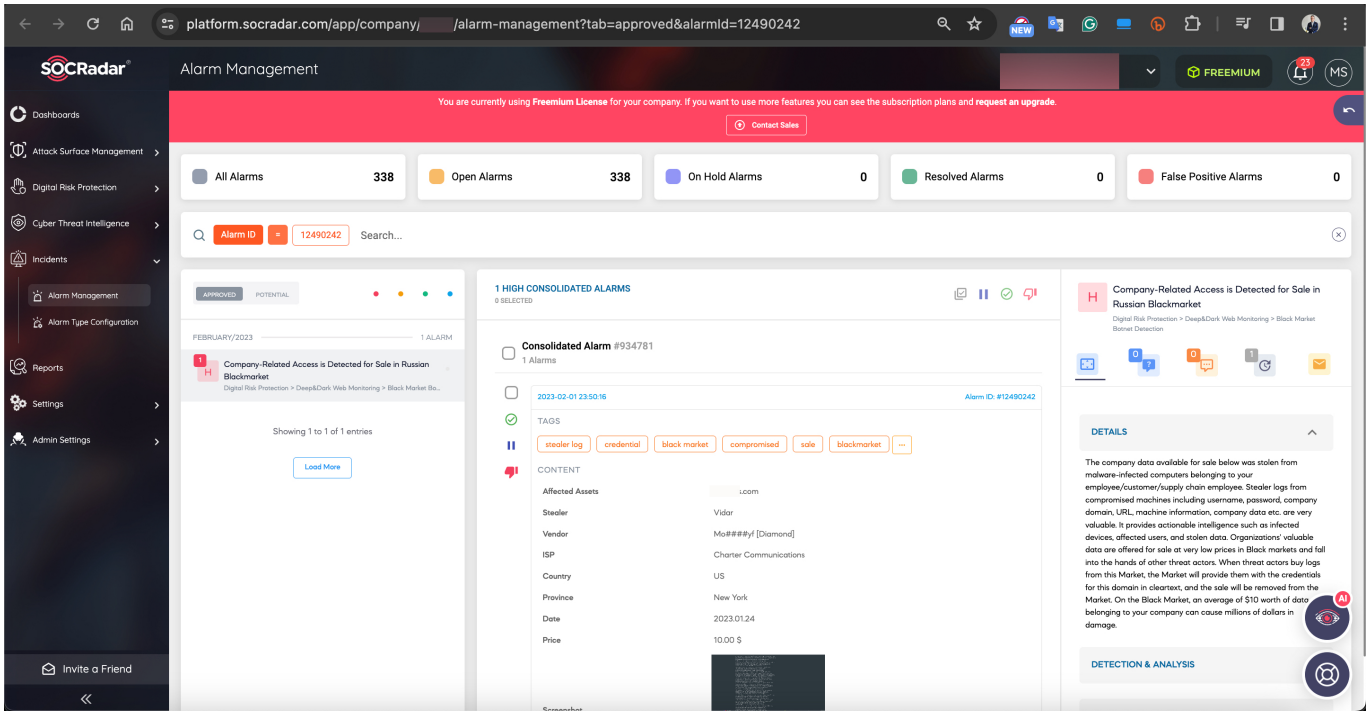
Bilgi hırsızı zararlı yazılımı, başta bulaştığı işletim sistemindeki uygulamalara, sistemlere (VPN, RDP, SSH) ait kullanıcı adı, parola bilgileri olmak üzere kişisel, finansal bilgileri de çalan ve ardından bunları geliştiricisine gönderen bir yazılımdır. Bu zararlı yazılımlar çoğu zaman geliştiricileri tarafından zararlı yazılım servis (MaaS) modeli olarak haftalık ve aylık olarak erişim aracılarına (IAB) satılmakta veya kiralanmaktadırlar.

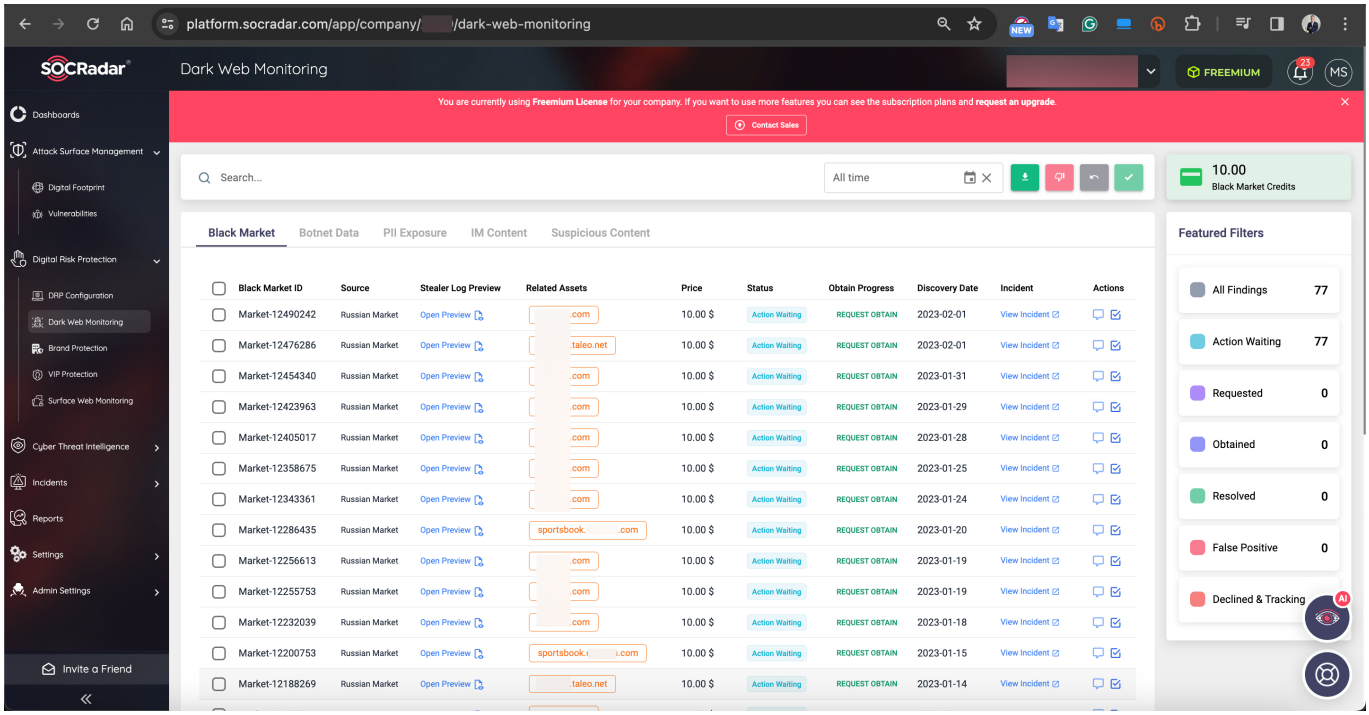
Zararlı yazılımlar tarafından çalınan bu bilgiler daha sonra erişim aracıları (IAB) tarafından siber suçluların uğrak yeri olan yeraltı forumlarında, Rus pazar yerlerinde (Russian Market) tehdit aktörlerine, operatörlere (müşteriler) satılmaktadırlar.

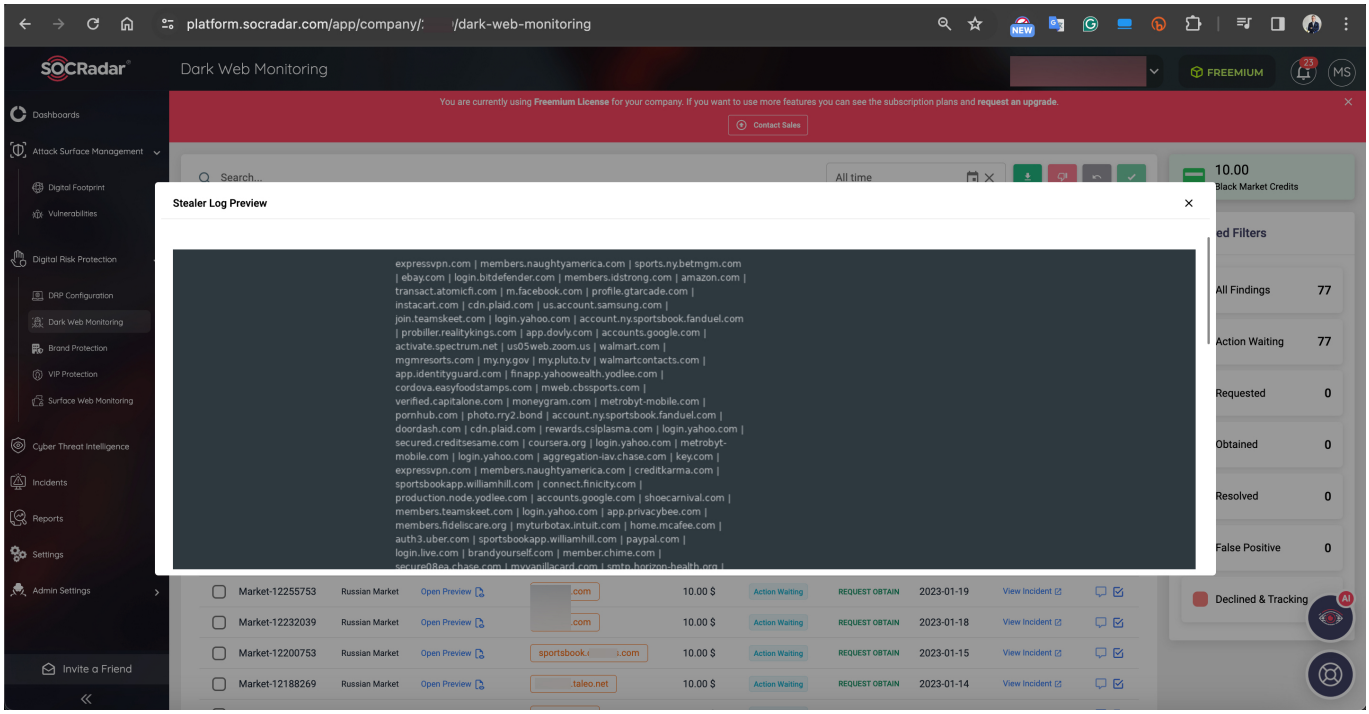


Referans: Secureworks

Özellikle SOCRadar gibi siber tehdit istihbaratı firmaları bu yerleri yakından takip ederek müşterilerini, satışa sunulan bilgileri hakkında uyarmaktadırlar. Bu uyarılar sayesinde kurumsal firmalar, çalışanlarına, müşterilerine, tedarikçilerine ait hesapları hızlıca tespit edip, dondurarak bu bilgilerin siber suçlular tarafından kötüye kullanılmasının önüne geçmektedirler. Aksi durumlarda ise örneğin X firmasına fidye saldırısı gerçekleştirmeyi planlayan bir tehdit aktörü, erişim aracısından 10$'a satın aldığı bu erişim bilgileri ile kötü emellerini kolaylıkla hayata geçirebilmektedir.


platform.socradar.com/app/company/ /alarm-management?tab=approved&alarmId=12490242
SOCRadar
Alarm Management
FREEMIUM
You are currently using Freemium License for your company. If you want to use more features you can see the subscription plans and request an upgrade.
Contact Sales
Dashboards
Attack Surface Management
Digital Risk Protection
Cyber Threat Intelligence
Incidents
Alarm Management
Alarm Type Configuration
Reports
Settings
Admin Settings
Invite a Friend
All Alarms 338
Open Alarms 338
On Hold Alarms 0
Resolved Alarms 0
False Positive Alarms 0
Alarm ID = 12490242 Search...
APPROVED POTENTIAL
FEBRUARY/2023 1 ALARM
Company-Related Access is Detected for Sale in Russian Blackmarket
Showing 1 to 1 of 1 entries
Load More
1 HIGH CONSOLIDATED ALARMS
0 SELECTED
Consolidated Alarm #934781
1 Alarms
2023-02-01 23:50:16
Alarm ID: #12490242
TAGS
stealer log
credential
black market
compromised
sale
blackmarket
CONTENT
Affected Assets .com
Stealer Vidar
Vendor Mo####yf [Diamond]
ISP Charter Communications
Country US
Province New York
Date 2023.01.24
Price 10.00 $
Company-Related Access is Detected for Sale in Russian Blackmarket
DETAILS
The company data available for sale below was stolen from malware-infected computers belonging to your employee/customer/supply chain employee. Stealer logs from compromised machines including username, password, company domain, URL, machine information, company data etc. are very valuable. It provides actionable intelligence such as infected devices, affected users, and stolen data. Organizations' valuable data are offered for sale at very low prices in Black markets and fall into the hands of other threat actors. When threat actors buy logs from this Market, the Market will provide them with the credentials for this domain in cleartext, and the sale will be removed from the Market. On the Black Market, an average of $10 worth of data belonging to your company can cause millions of dollars in damage.
DETECTION & ANALYSIS


platform.socradar.com/app/company/ /dark-web-monitoring
SOCRadar
Dark Web Monitoring
FREEMIUM
You are currently using Freemium License for your company. If you want to use more features you can see the subscription plans and request an upgrade.
Contact Sales
Dashboards
Attack Surface Management
Digital Footprint
Vulnerabilities
Digital Risk Protection
DRP Configuration
Dark Web Monitoring
Brand Protection
VIP Protection
Surface Web Monitoring
Cyber Threat Intelligence
Incidents
Reports
Settings
Admin Settings
Invite a Friend
Search...
All time
10.00
Black Market Credits
Black Market
Botnet Data
PII Exposure
IM Content
Suspicious Content
Black Market ID
Source
Stealer Log Preview
Related Assets
Price
Status
Obtain Progress
Discovery Date
Incident
Actions
Market-12490242 Russian Market Open Preview .com 10.00 $ Action Waiting REQUEST OBTAIN 2023-02-01 View Incident
Market-12476286 Russian Market Open Preview taleo.net 10.00 $ Action Waiting REQUEST OBTAIN 2023-02-01 View Incident
Market-12454340 Russian Market Open Preview .com 10.00 $ Action Waiting REQUEST OBTAIN 2023-01-31 View Incident
Market-12423963 Russian Market Open Preview .com 10.00 $ Action Waiting REQUEST OBTAIN 2023-01-29 View Incident
Market-12405017 Russian Market Open Preview .com 10.00 $ Action Waiting REQUEST OBTAIN 2023-01-28 View Incident
Market-12358675 Russian Market Open Preview .com 10.00 $ Action Waiting REQUEST OBTAIN 2023-01-25 View Incident
Market-12343361 Russian Market Open Preview .com 10.00 $ Action Waiting REQUEST OBTAIN 2023-01-24 View Incident
Market-12286435 Russian Market Open Preview sportsbook. .com 10.00 $ Action Waiting REQUEST OBTAIN 2023-01-20 View Incident
Market-12256613 Russian Market Open Preview .com 10.00 $ Action Waiting REQUEST OBTAIN 2023-01-19 View Incident
Market-12255753 Russian Market Open Preview .com 10.00 $ Action Waiting REQUEST OBTAIN 2023-01-19 View Incident
Market-12232039 Russian Market Open Preview .com 10.00 $ Action Waiting REQUEST OBTAIN 2023-01-18 View Incident
Market-12200753 Russian Market Open Preview sportsbook. .com 10.00 $ Action Waiting REQUEST OBTAIN 2023-01-15 View Incident
Market-12188269 Russian Market Open Preview taleo.net 10.00 $ Action Waiting REQUEST OBTAIN 2023-01-14 View Incident
Featured Filters
All Findings 77
Action Waiting 77
Requested 0
Obtained 0
Resolved 0
False Positive 0
Declined & Tracking

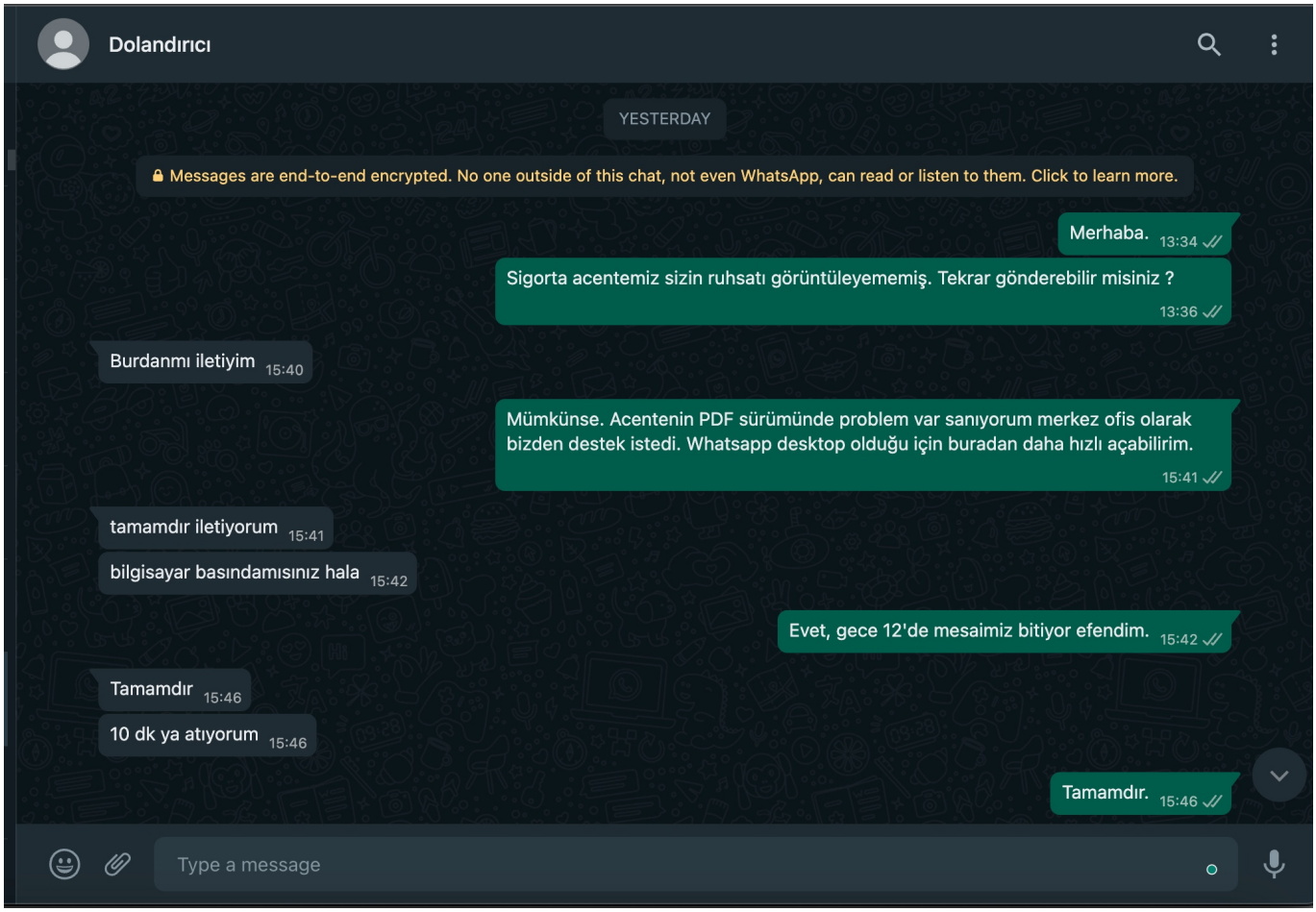


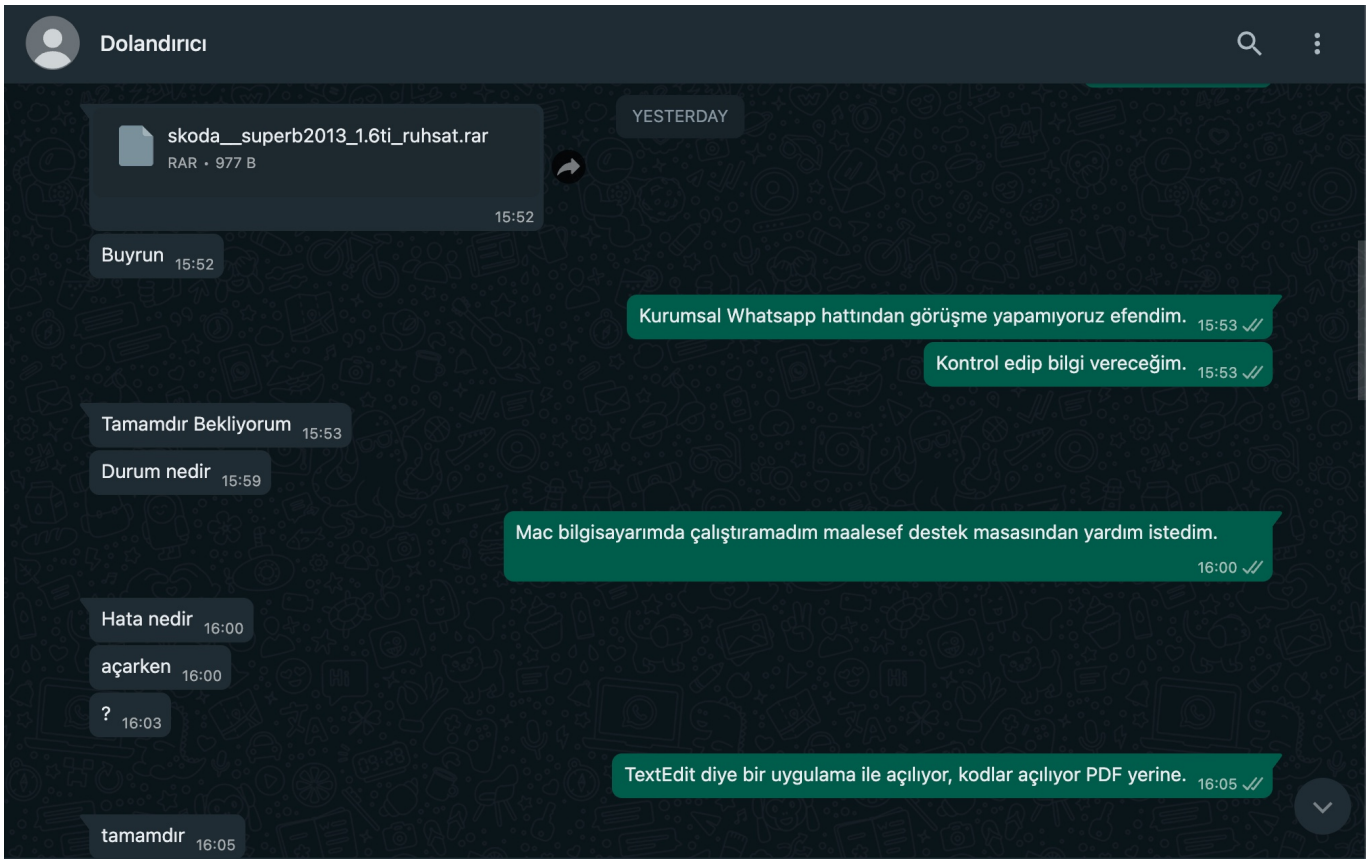
Referans: SOCRadar XTI

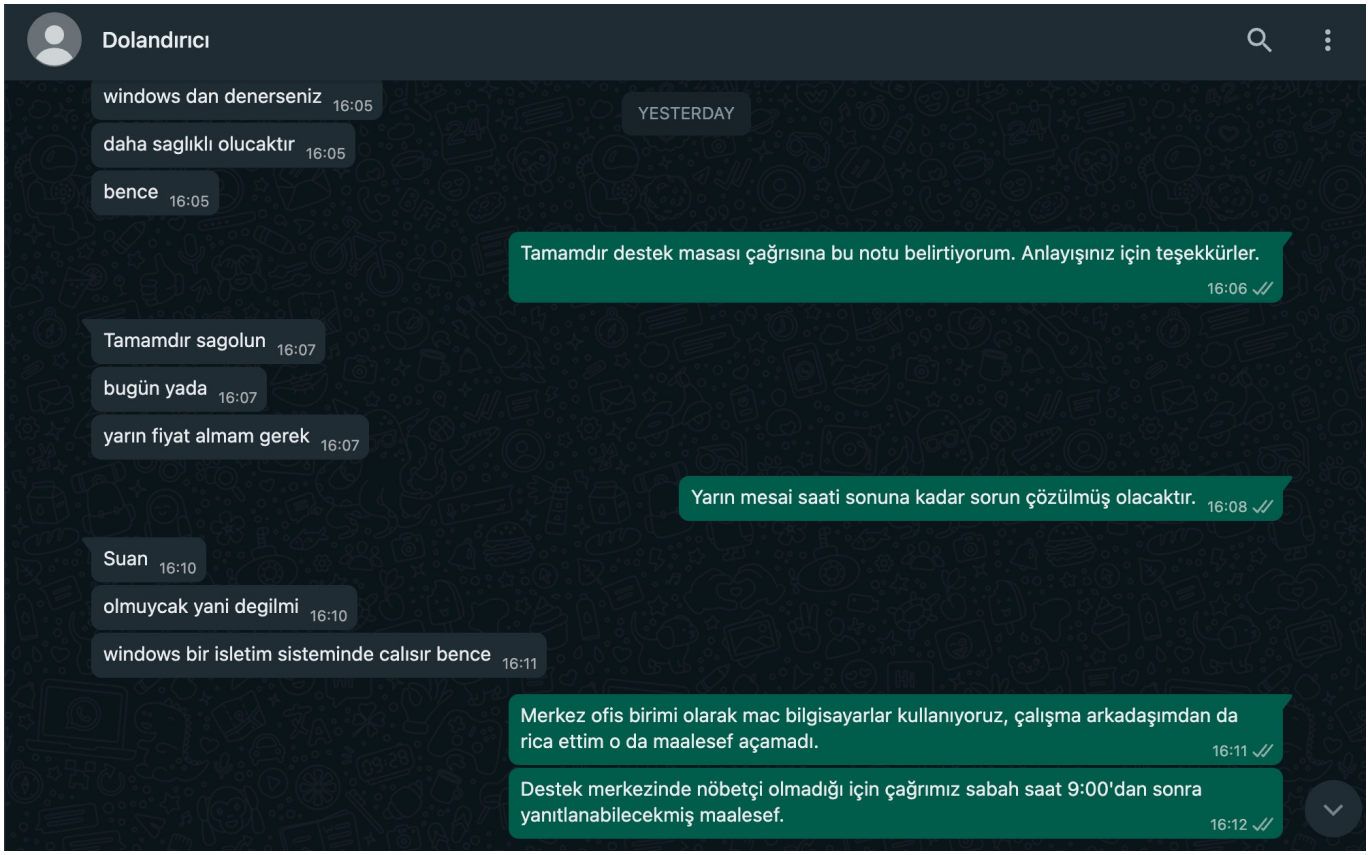
3-2-1 Kayıt!

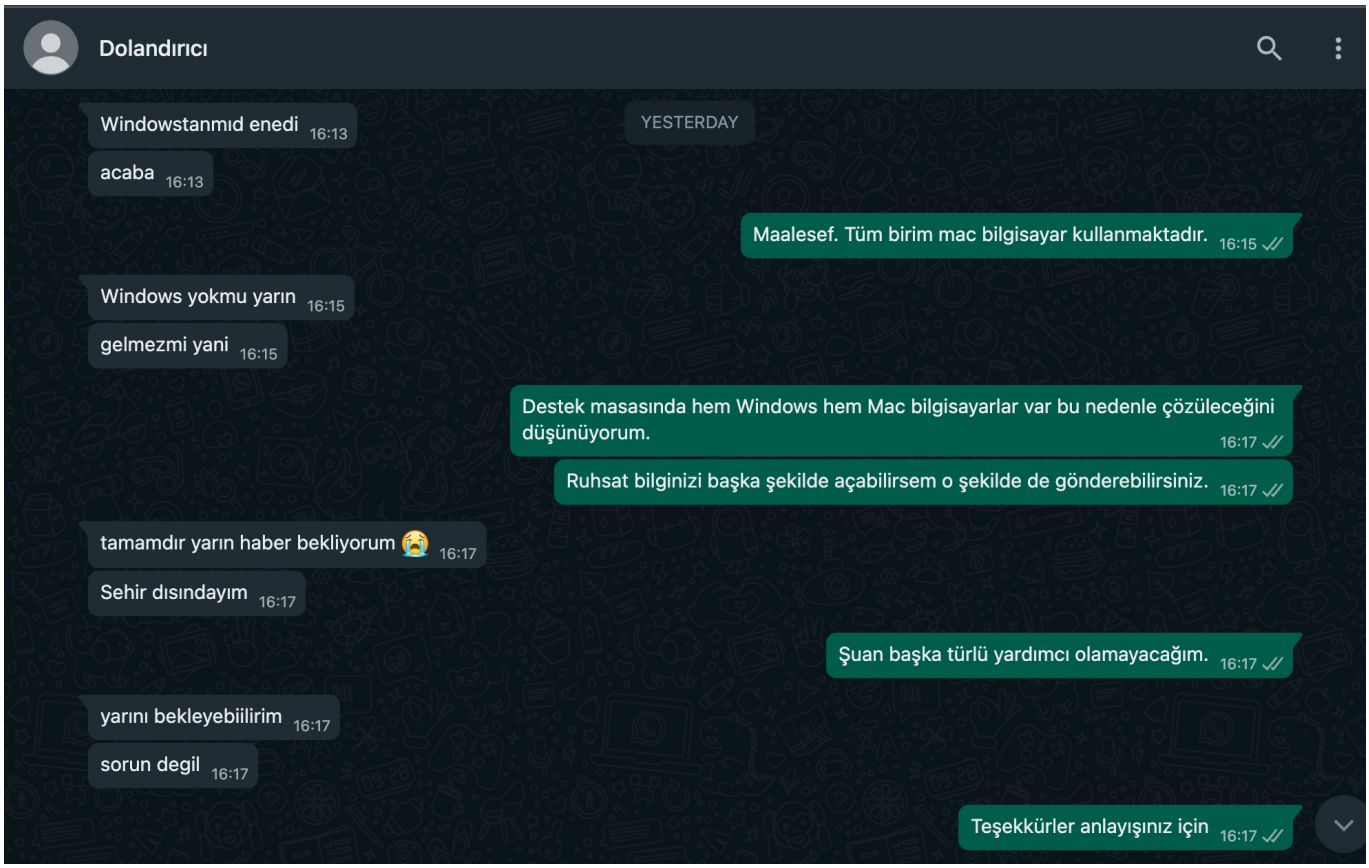
Hikayemiz, 25 Temmuz 2023 tarihinde Bartu KILIÇ'ın akrabasından gelen bir WhatsApp mesajı ile başlar. Sigorta danışmanı olan akrabası, araç sigortası yaptırmak isteyen bir kişinin WhatsApp üzerinden kendisine ruhsat adı altında gönderdiği bir dosyadan (skoda__superb2013_1.6ti_ruhsat.rar) şüphelenerek konuyu siber güvenlik uzmanı olan Bartu'ya taşımaya karar verir. Bartu da bu hikayeyi, kendisi ile son zamanlarda yaşanılan dolandırıcılık girişimlerine dair sohbet ettiğimiz bir esnada benimle paylaşır ve ilgimi fazlasıyla çeken bu konuyu araştırmaya başlamam üzerine olaylar gelişir.

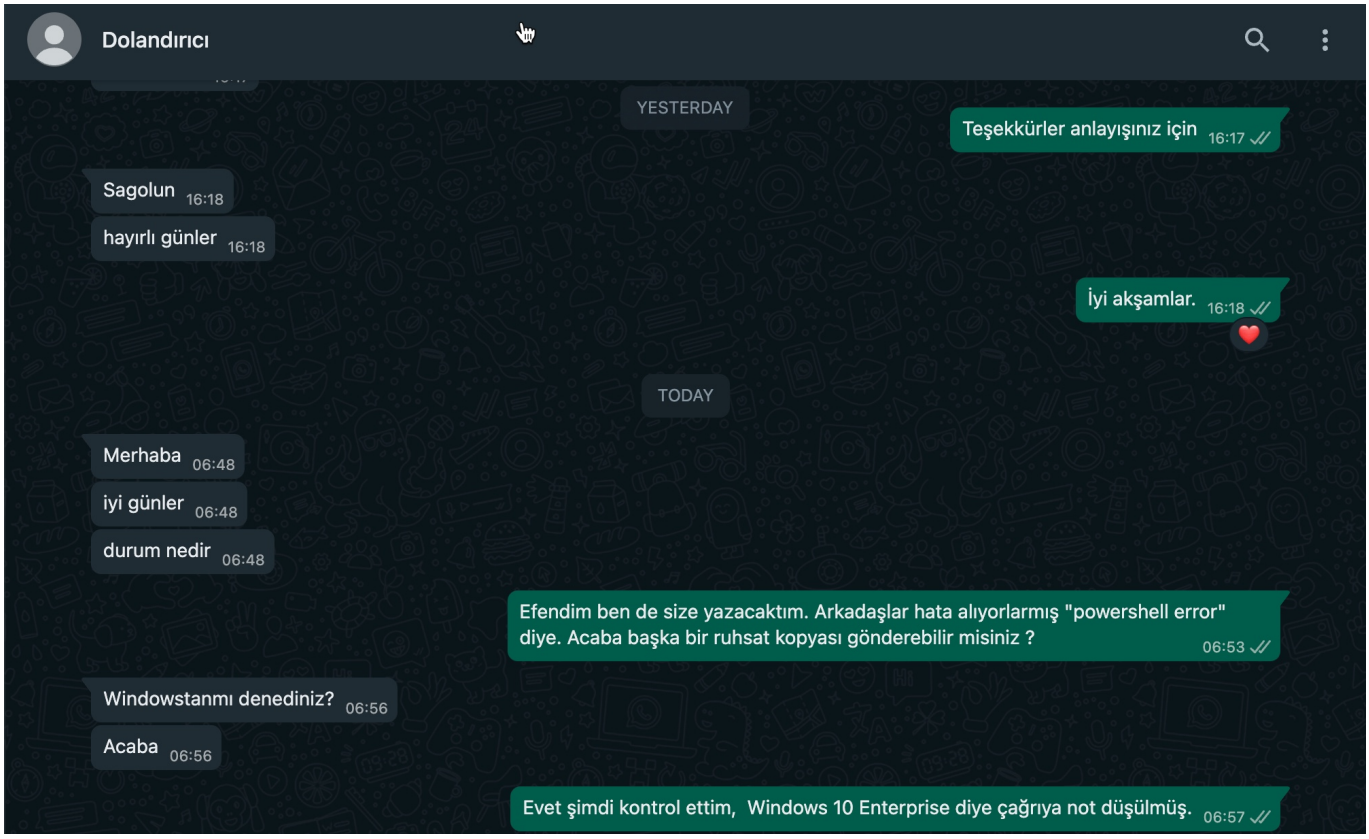
Bartu'dan dosyayı incelemek için akrabasından talep etmesini rica ettikten bir süre sonra dosyanın silindiğini bu nedenle dosyayı elde edemediğini paylaştı. Bunun üzerine elinde dolandırıcının cep telefonu numarası (+90 545 466 89 52) olduğu için ben de dolandırıcı ile WhatsApp üzerinden iletişime geçmeye karar verdim. Kendimi sigorta şirketinin genel merkez çalışanı olarak tanıtarak (her zaman dolandırıcılar sosyal mühendislik yapacak değiller ya :)) dolandırıcı ile yazışmaya başladım ve çok geçmeden hikayeye konu olan şüpheli dosyayı elde edebildim.


Dolandırıcı
YESTERDAY
Messages are end-to-end encrypted. No one outside of this chat, not even WhatsApp, can read or listen to them. Click to learn more.
Merhaba. 13:34
Sigorta acentemiz sizin ruhsatı görüntüleyememiş. Tekrar gönderebilir misiniz ? 13:36
Burdanmı iletiyim 15:40
Mümkünse. Acentenin PDF sürümünde problem var sanıyorum merkez ofis olarak bizden destek istedi. Whatsapp desktop olduğu için buradan daha hızlı açabilirim. 15:41
tamamdır iletiyorum 15:41
bilgisayar basındamısınız hala 15:42
Evet, gece 12'de mesaimiz bitiyor efendim. 15:42
Tamamdır 15:46
10 dk ya atıyorum 15:46
Tamamdır. 15:46
Type a message


Dolandırıcı
YESTERDAY
skoda__superb2013_1.6ti_ruhsat.rar
RAR • 977 B
15:52
Buyrun 15:52
Kurumsal Whatsapp hattından görüşme yapamıyoruz efendim. 15:53
Kontrol edip bilgi vereceğim. 15:53
Tamamdır Bekliyorum 15:53
Durum nedir 15:59
Mac bilgisayarımda çalıştıramadım maalesef destek masasından yardım istedim. 16:00
Hata nedir 16:00
açarken 16:00
? 16:03
TextEdit diye bir uygulama ile açılıyor, kodlar açılıyor PDF yerine. 16:05
tamamdır 16:05

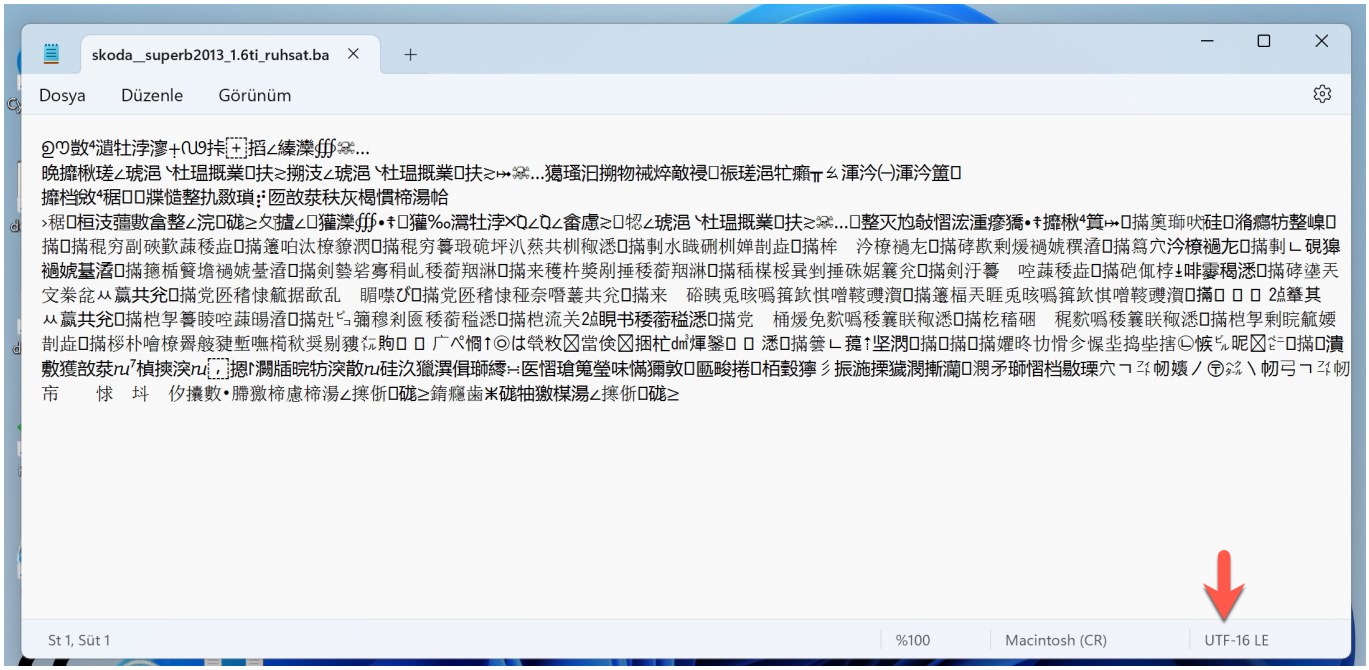

Dolandırıcı
windows dan denerseniz 16:05
daha saglıklı olucaktır 16:05
bence 16:05
YESTERDAY
Tamamdır destek masası çağrısına bu notu belirtiyorum. Anlayışınız için teşekkürler. 16:06
Tamamdır sagolun 16:07
bugün yada 16:07
yarın fiyat almam gerek 16:07
Yarın mesai saati sonuna kadar sorun çözülmüş olacaktır. 16:08
Suan 16:10
olmuycak yani degilmi 16:10
windows bir isletim sisteminde calısır bence 16:11
Merkez ofis birimi olarak mac bilgisayarlar kullanıyoruz, çalışma arkadaşımdan da rica ettim o da maalesef açamadı. 16:11
Destek merkezinde nöbetçi olmadığı için çağrımız sabah saat 9:00'dan sonra yanıtlanabilecekmiş maalesef. 16:12

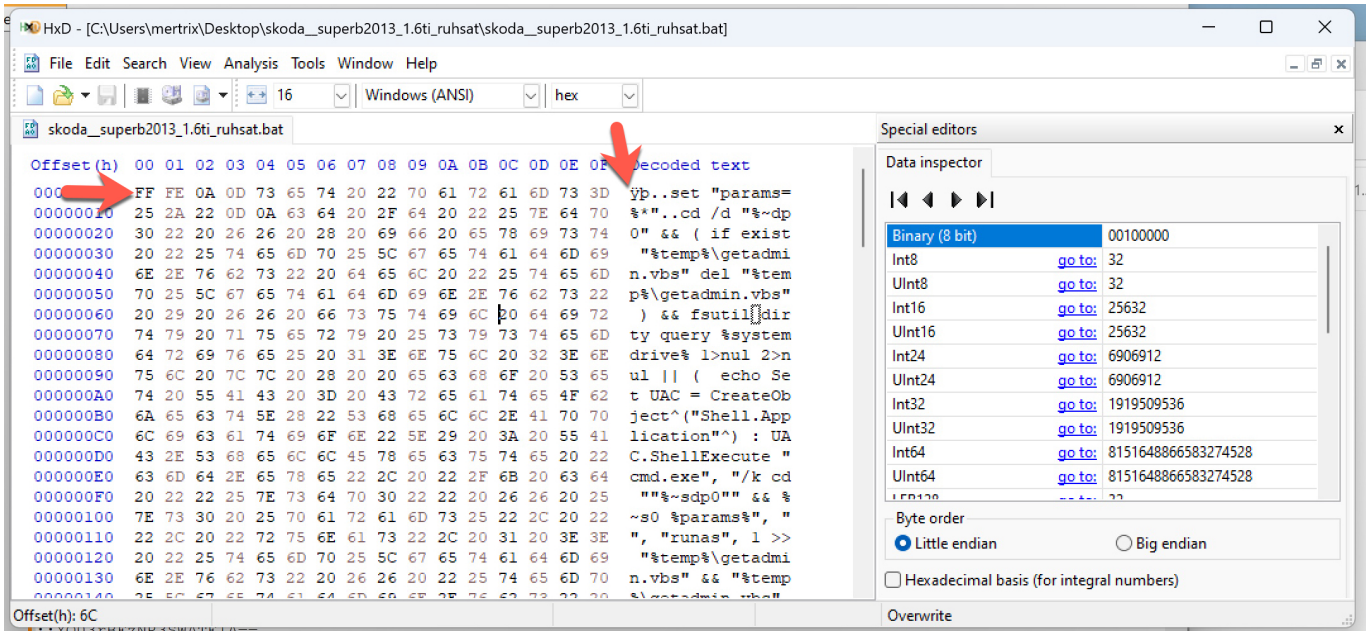

Dolandırıcı
Windowstanmıd enedi 16:13
acaba 16:13
YESTERDAY
Maalesef. Tüm birim mac bilgisayar kullanmaktadır. 16:15
Windows yokmu yarın 16:15
gelmezmi yani 16:15
Destek masasında hem Windows hem Mac bilgisayarlar var bu nedenle çözüleceğini düşünüyorum. 16:17
Ruhsat bilginizi başka şekilde açabilirsem o şekilde de gönderebilirsiniz. 16:17
tamamdır yarın haber bekliyorum 16:17
Sehir dısındayım 16:17
Şuan başka türlü yardımcı olamayacağım. 16:17
yarını bekleyebiilirim 16:17
sorun degil 16:17
Teşekkürler anlayışınız için 16:17



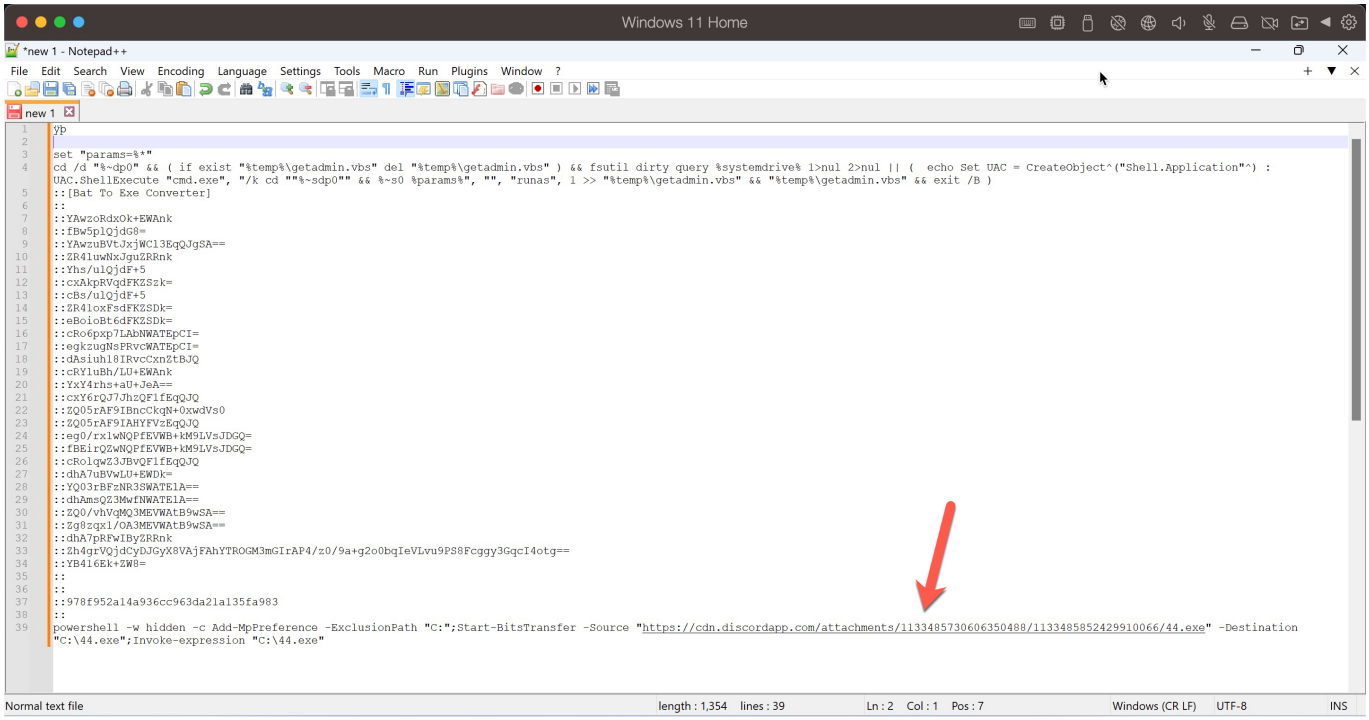
Statik Şüpheli Dosya Analizi (44.exe)

skoda__superb2013_1.6ti_ruhsat.rar dosyasını sanal Windows 11 işletim sistemi üzerinde açtıktan sonra skoda__superb2013_1.6ti_ruhsat.bat dosyası hemen dikkatimi çekti. Notepad ile dosyayı açtığımda karşıma UTF-16 kodlanmış bir karakter dizisi çıktı. HxD hex editörü ile BAT dosyasını incelediğimde, tehdit aktörünün metin editörleri ile komutların açığa çıkmasını engellemek için byte-order mark (BOM) yönteminden faydalandığını gördüm.





Bu kodlamanın arkasına gizlenen komutları incelediğimde, BAT dosyasının çalıştırıldığında öncelikle zararlı yazılımın Microsoft Defender ile tespit edilmesini engellemek için PowerShell komutlarından faydalanarak C: dizinini Microsoft Defender'ın istisna listesine eklediğini daha sonra ise Discord isimli iletişim platformundan 44.exe isimli bir dosya indirip çalıştırdığını gördüm.



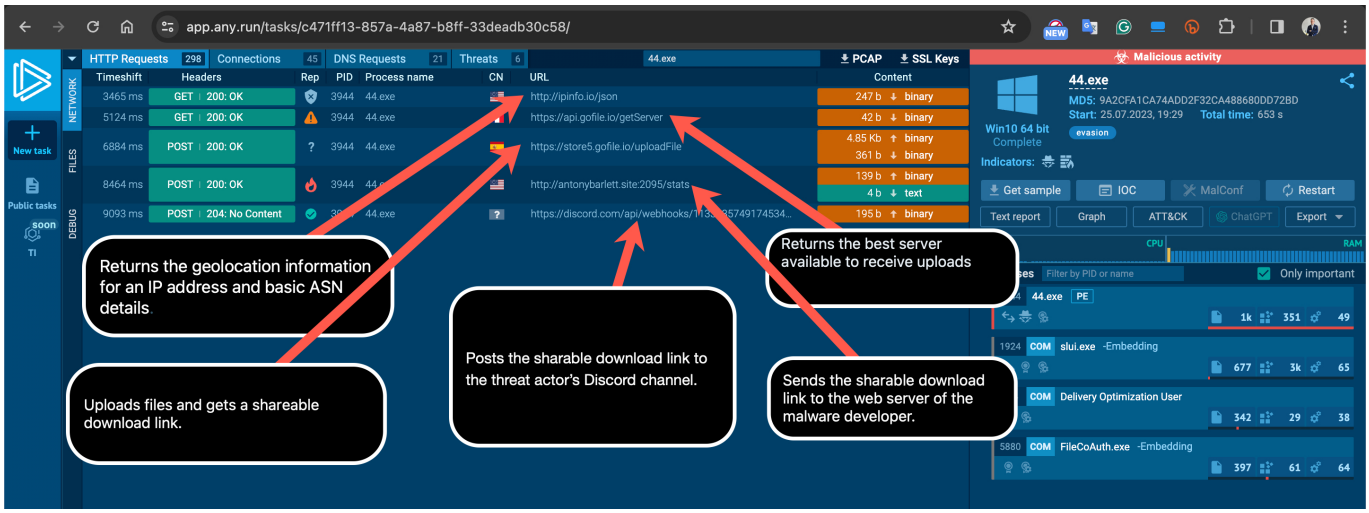
Dinamik Şüpheli Dosya Analizi (44.exe)

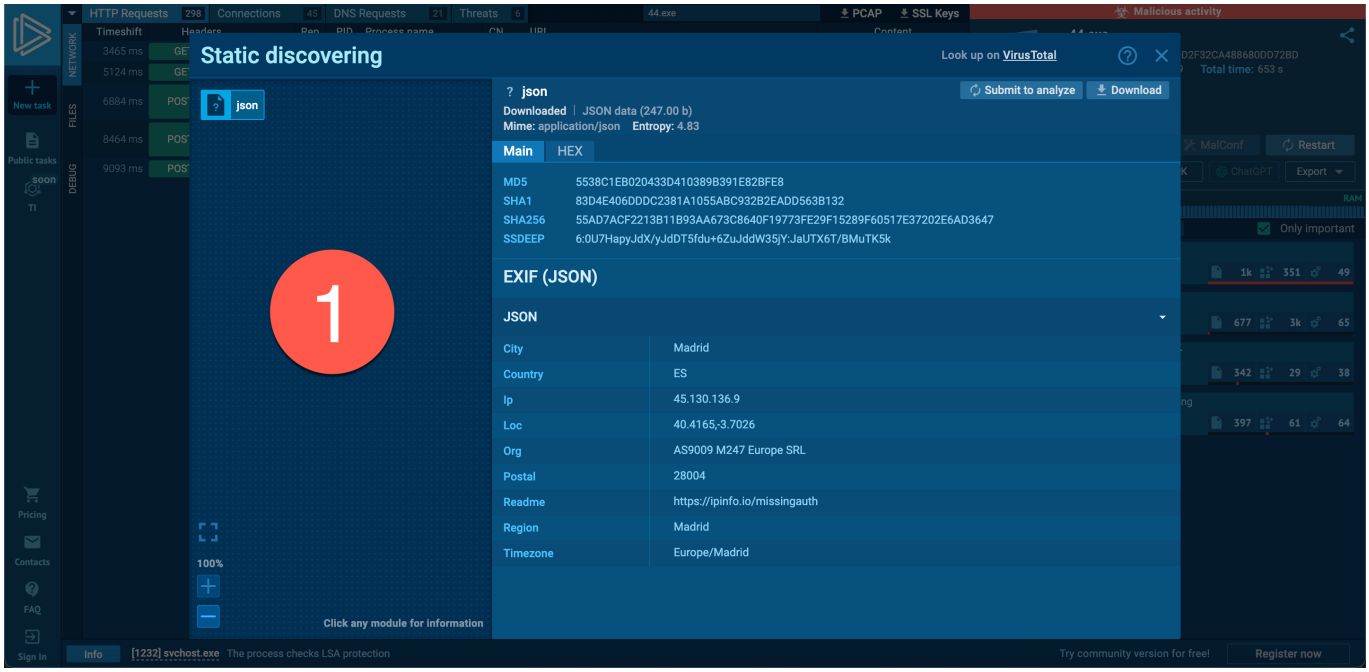
Buraya kadar fazlasıyla şüpheli işlem yapmak için oluşturulmuş bu BAT dosyasını bir kenara koyup, 44.exe isimli dosyayı indirip, ANY.RUN isimli

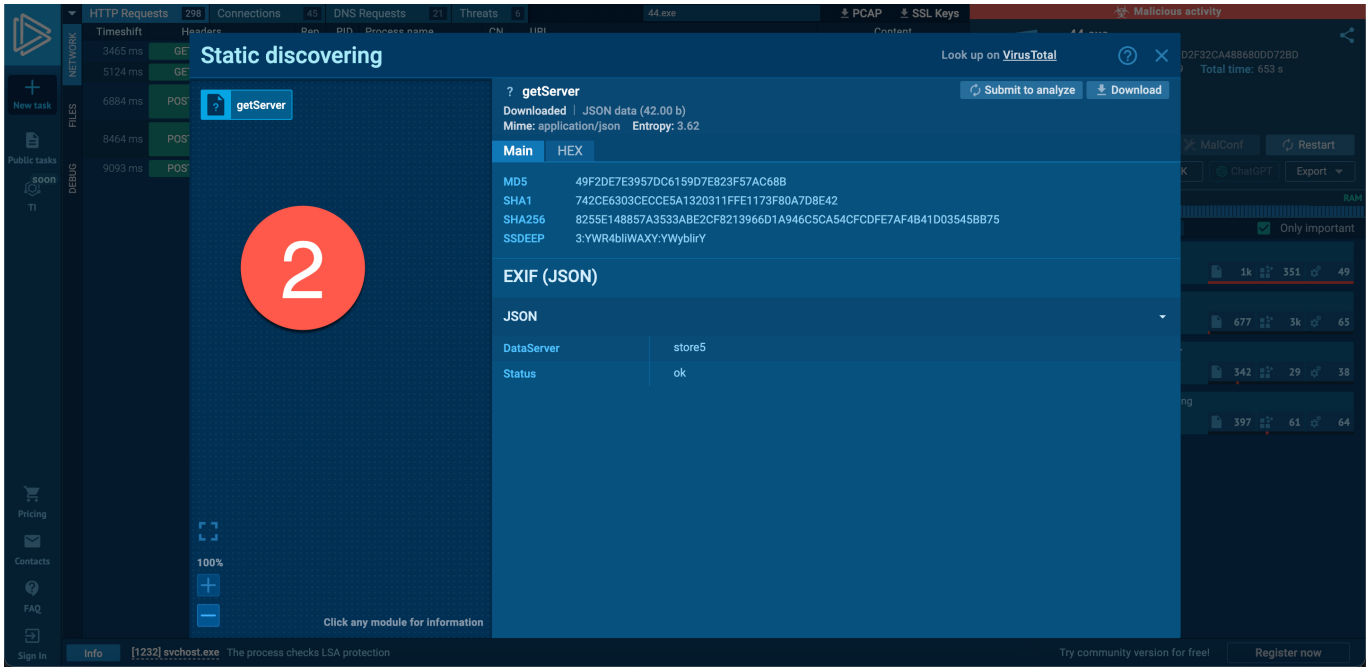
interaktif zararlı yazılım analizi platformuna yüklemeye ve çalıştırıp, kayıtlarını incelemeye karar verdim.

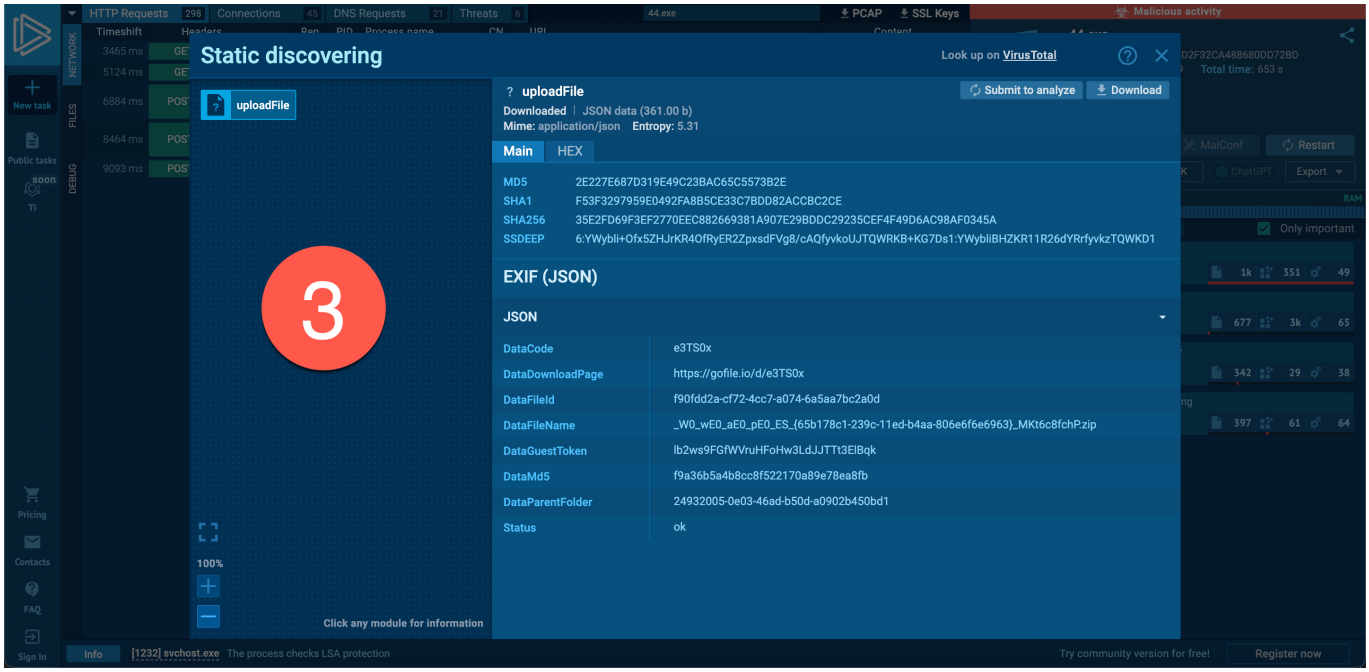
44.exe işlemi (process) tarafından işletim sistemi üzerinde oluşturulan kayıtlardan önemli olanlara baktığımda;

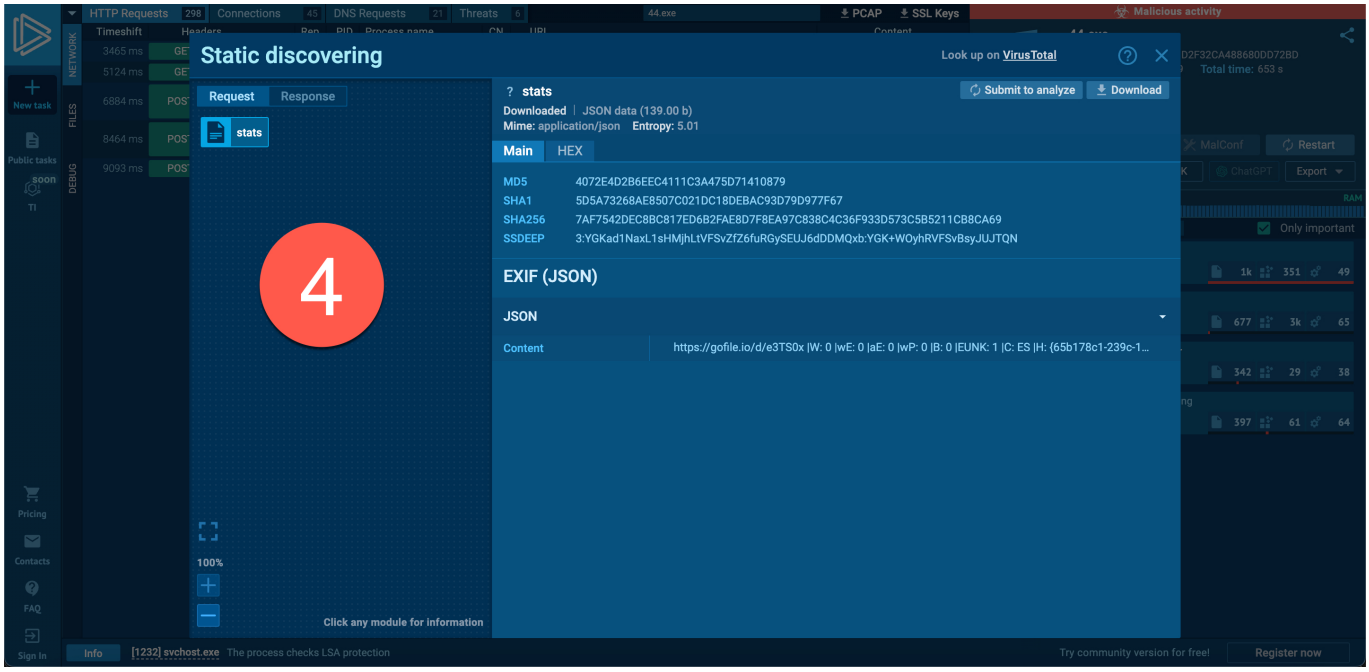
1. Çalıştığı sistemin IP adresinin coğrafi konum bilgilerini ve temel ASN ayrıntılarını IPinfo üzerinden alıyordu.
2. Gofile dosya paylaşım platformuna işletim sisteminden çaldığı dosyaları yüklemek için müsait olan Gofile sunucu bilgisini alıyordu.
3. Çalınan dosyaları Gofile platformuna yükler ve paylaşılabilir indirme bağlantı adresini (link) alıyordu.
4. İndirme bağlantı adresini, zararlı yazılım geliştiricisinin web sunucusuna (http://antonybarlett[.]site:2095/stats) gönderiyordu.
5. Bağlantı adresini, tehdit aktörünün Discord kanalına Webhook ile gönderiyordu.

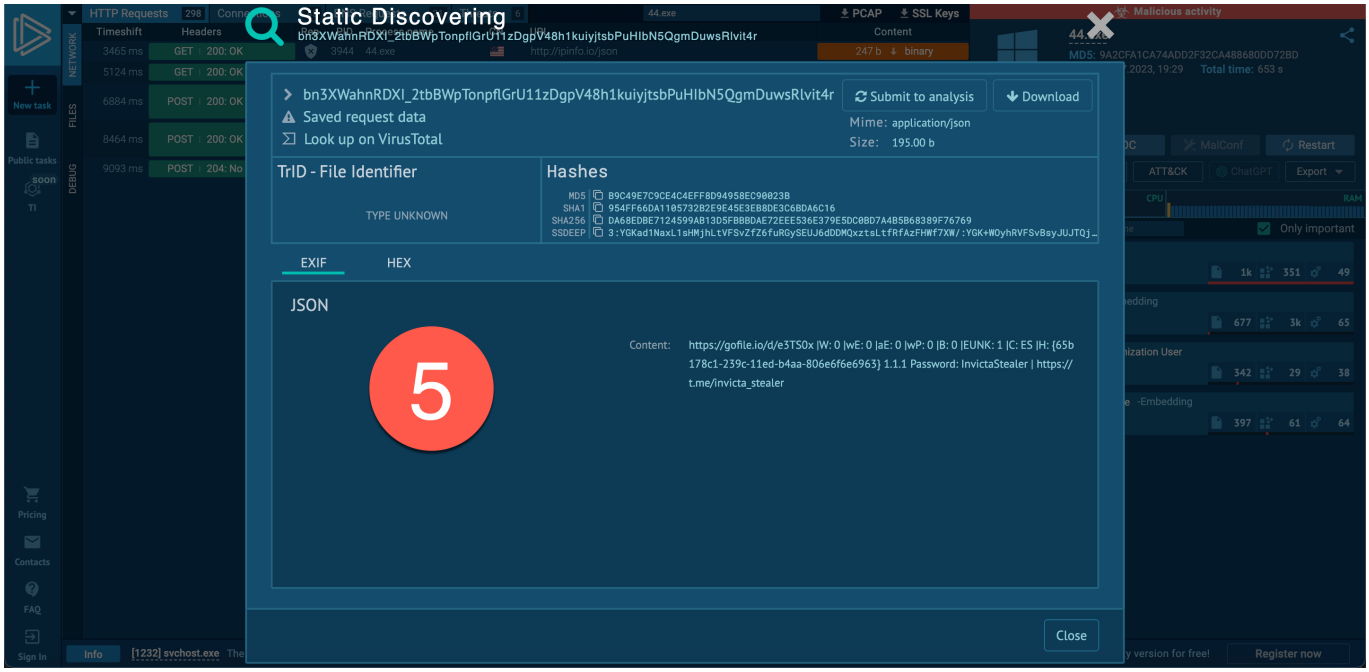



Static discovering
Look up on VirusTotal
json
Submit to analyze
Download
Downloaded | JSON data (247.00 b)
Mime: application/json Entropy: 4.83
Main
HEX
MD5 5538C1EB020433D410389B391E82BFE8
SHA1 83D4E406DDDC2381A1055ABC932B2EADD563B132
SHA256 55AD7ACF2213B11B93AA673C8640F19773FE29F15289F60517E37202E6AD3647
SSDEEP 6:0U7HapyJdX/yJdDT5fdu+6ZuJddW35jY:JaUTX6T/BMuTK5k
EXIF (JSON)
JSON
City Madrid
Country ES
Ip 45.130.136.9
Loc 40.4165,-3.7026
Org AS9009 M247 Europe SRL
Postal 28004
Readme https://ipinfo.io/missingauth
Region Madrid
Timezone Europe/Madrid
1
100%
Click any module for information


Static discovering
Look up on VirusTotal
getServer
Submit to analyze
Download
Downloaded | JSON data (42.00 b)
Mime: application/json Entropy: 3.62
Main
HEX
MD5 49F2DE7E3957DC6159D7E823F57AC68B
SHA1 742CE6303CECCE5A1320311FFE1173F80A7D8E42
SHA256 8255E148857A3533ABE2CF8213966D1A946C5CA54CFCDFE7AF4B41D03545BB75
SSDEEP 3:YWR4bliWAXY:YWybliY
EXIF (JSON)
JSON
DataServer store5
Status ok
2
100%
Click any module for information


Static discovering
Look up on VirusTotal
uploadFile
Submit to analyze
Download
Downloaded | JSON data (361.00 b)
Mime: application/json Entropy: 5.31
Main
HEX
MD5 2E227E687D319E49C23BAC65C5573B2E
SHA1 F53F3297959E0492FA8B5CE33C7BDD82ACCBC2CE
SHA256 35E2FD69F3EF2770EEC882669381A907E29BDDC29235CEF4F49D6AC98AF0345A
SSDEEP 6:YWybli+Ofx5ZHJrKR4OfRyER2ZpxsdFVg8/cAQfyvkoUJTQWRKB+KG7Ds1:YWybliBHZKR11R26dYRrfyvkzTQWKD1
EXIF (JSON)
JSON
DataCode e3TS0x
DataDownloadPage https://gofile.io/d/e3TS0x
DataFileId f90fdd2a-cf72-4cc7-a074-6a5aa7bc2a0d
DataFileName _W0_wE0_aE0_pE0_ES_{65b178c1-239c-11ed-b4aa-806e6f6e6963}_MKt6c8fchP.zip
DataGuestToken lb2ws9FGfWVruHFoHw3LdJJTTt3ElBqk
DataMd5 f9a36b5a4b8cc8f522170a89e78ea8fb
DataParentFolder 24932005-0e03-46ad-b50d-a0902b450bd1
Status ok
3
100%
Click any module for information


Static discovering
Look up on VirusTotal
Request
Response
stats
Submit to analyze
Download
Downloaded | JSON data (139.00 b)
Mime: application/json Entropy: 5.01
Main
HEX
MD5 4072E4D2B6EEC4111C3A475D71410879
SHA1 5D5A73268AE8507C021DC18DEBAC93D79D977F67
SHA256 7AF7542DEC8BC817ED6B2FAE8D7F8EA97C838C4C36F933D573C5B5211CB8CA69
SSDEEP 3:YGKad1NaxL1sHMjhLtVFSvZfZ6fuRGySEUJ6dDDMQxb:YGK+WOyhRVFSvBsyJUJTQN
EXIF (JSON)
JSON
Content https://gofile.io/d/e3TS0x |W: 0 |wE: 0 |aE: 0 |wP: 0 |B: 0 |EUNK: 1 |C: ES |H: {65b178c1-239c-1...
4
100%
Click any module for information



5. kayda baktığımda, HTTP isteğinde yer alan InvictaStealer etiketi ve https://t.me/invicta_stealer Telegram adresi dikkatimi çekti. Telegram kanalını ziyaret ettiğimde, bu yazılımın C++ programlama dili ile geliştirilmiş, oluşturucusu (builder) ücretsiz olarak GitHub depolama platformunda sunulan, Rus menşeili bilgi hırsızı zararlı yazılımı (infostealer) olduğu netleşmiş oldu.

Invicta Stealer [🇬🇧/🇷🇺]
201 subscribers

Previous message
⚔️Invicta Stealer — мощный бесплатный нативный стилер⚔️ Это стилер C+

Invicta Stealer [🇬🇧/🇷🇺]
⚔️Invicta Stealer — a powerful, free native stealer⚔️

This is a C++ stealer which is being actively improved upon, with the help we receive from our active community.

📁 **BROWSERS**
Information is obtained from all the profiles from all chromium-based (the most used) browsers, and firefox.
We collect: credit card data, autofill, history, all extensions which include **71 crypto wallets** and various authenticators, local storage, downloads, and much more. Essentially, all the information is collected.

📁 **DISCORD**
All of the discord tokens are extracted from: the regular client, discord canary, ptb discord and browser local storage

📁 **CRYPTO**
Wallet information is collected from 25 wallets, with new ones being actively added.

📁 **SENSITIVE DIRECTORIES AND FILES**
We have studied real world scenarios, and came up with advanced filters that will fetch you sensitive information related to cryptocurrency wallets, bank accounts, passwords, private keys, etc. The stealer gets recently opened .txt files, recursively iterates through the computer to find sensitive information, steals github and visual studio code repositories (with bloat removed), gets .txt files from desktop, documents, etc

📁 **FTP CLIENTS**

Invicta Stealer [🇬🇧/🇷🇺]

201 subscribers

Pinned message

⚔️**Invicta Stealer — a powerful, free native stealer**⚔️ This is a C++ stealer whic

files from desktop, documents, etc

📁 **FTP CLIENTS**
Information is obtained from WinSCP and FileZilla

📁 **SYSTEM INFORMATION**
We collect system information, which includes the HWID, IP, timezone, computer language, RAM, CPU information, etc

📁 **ANTI-DEBUGGING, EVASION TECHNIQUES**
We use anti-debug/anti-virustotal/anti-vm techniques which complicate analysis of the malware. Your link will be encrypted in the stealer file.
Sensitive operations are performed through syscalls, which make them harder to detect by AVs and analysts, and all strings are encrypted.

💰 **PRICE**
We made the base version free to eliminate certain low quality stealers from being used, and to drive future customers to our paid version.
A paid version featuring a convenient HTTP panel and a custom file filter will be released soon.

Install and use instructions are included in the channel

Contact us if you need help or have suggestions. We strive to be the best.

@invicta_stealer

🔥 3 👍 1 ❤️ 1

632 edited 19:28

Invicta Stealer [🇬🇧/🇷🇺]
201 subscribers

Pinned message
⚔️Invicta Stealer — a powerful, free native stealer⚔️ This is a C++ stealer which

❤️ 3 👍 1 ❤️ 1 632 edited 19:28

April 5

Invicta Stealer [🇬🇧/🇷🇺]
TUTORIAL

1. Download the Builder ZIP file
2. Run Builder.exe
3. Input discord webhook, or an URL to your HTTP server into the box
4. Click build
5. Patched stealer will be available in out/InvictaStealer.exe

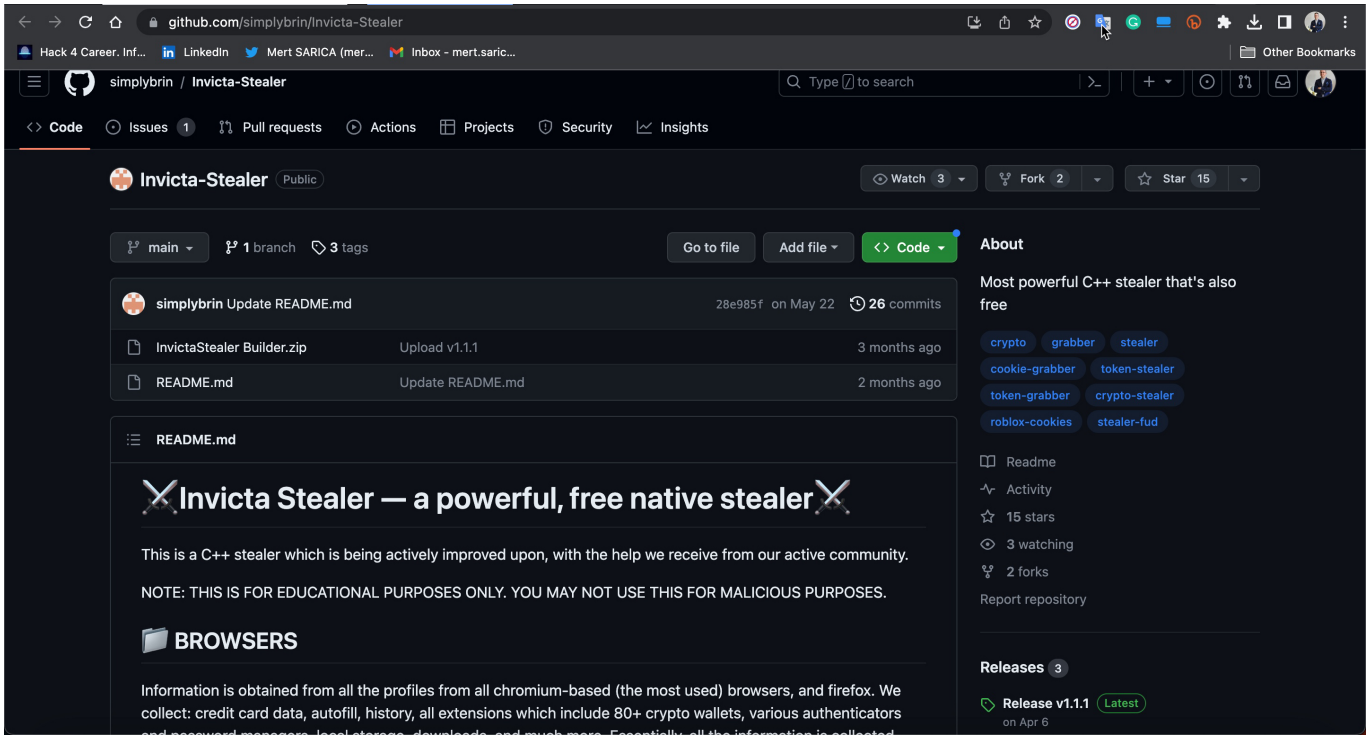
https://github.com/simplybrin/Invicta-Stealer

❤️ 3 506 13:12

Invicta Stealer [🇬🇧/🇷🇺]
Update v1.1.0

- Bug fixes
- Add password manager support: keepass
- Steam: steal sessions, get installed games list and username
- System information: list all installed apps, get path of running stealer, get windows version

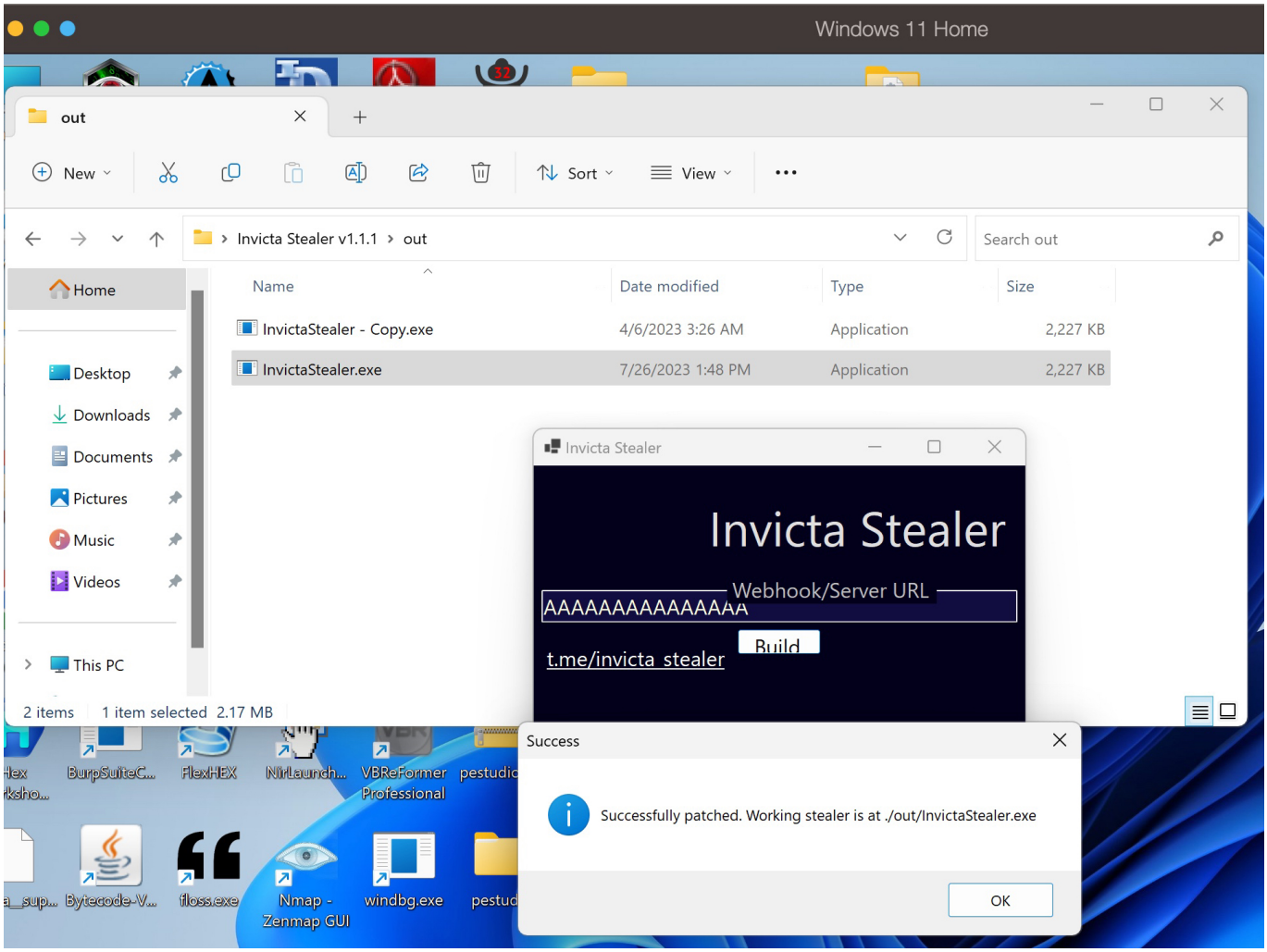
❤️ 4 523 13:18



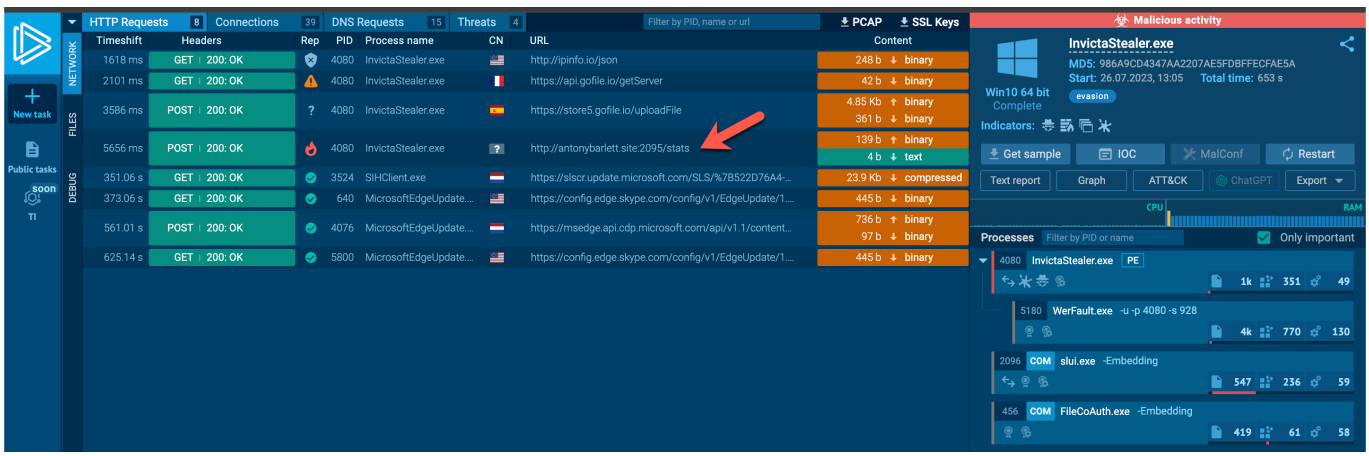
Invicta Stealer'ın YouTube kanalındaki tanıtım videosu

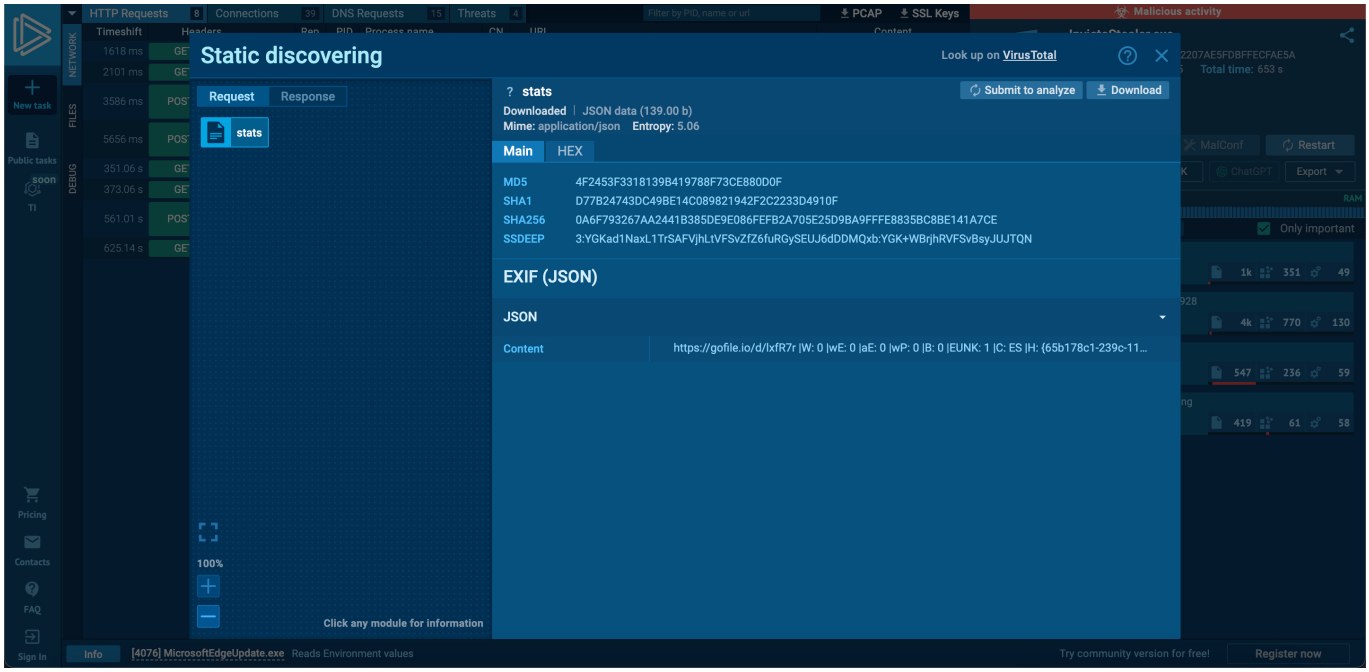
Dinamik Zararlı Dosya Analizi (Builder.exe)

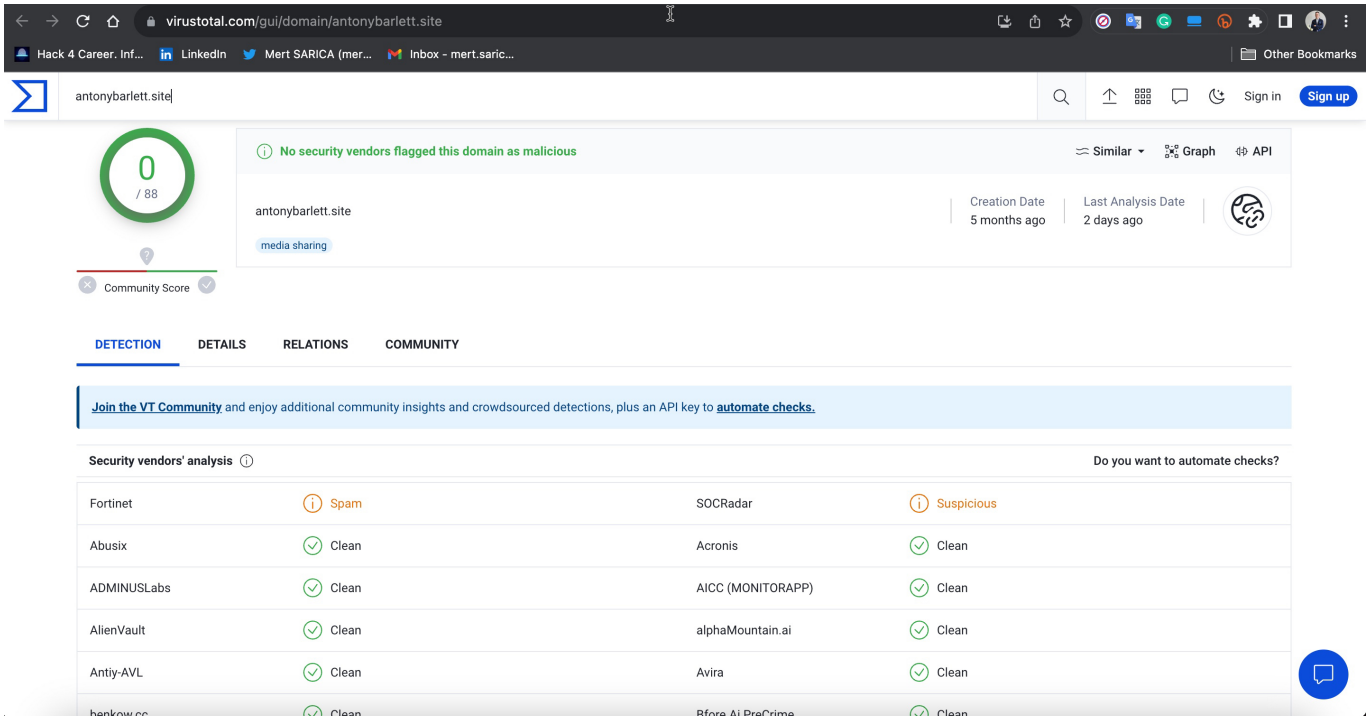
Zararlı yazılımın geliştiricisine ait olan GitHub alanından InvictaStealer Builder.zip dosyasını indirip sanal sistemimde çalıştırıp incelemeye başladım. Uygulama açıldığında kullanıcıdan Discord Webhook veya bir URL girmesini istiyor ve ardından Build butonuna basılınca zararlı yazılımı oluşturuyordu. Test için Webhook/Server URL kısmına AAAAAA… girip, zararlı yazılımı oluşturdum.



Oluşturulan zararlı yazılımın 44.exe ile benzer noktalarını keşfetmek için ANY.RUN'a yüklediğimde, iki yazılımda da ortak olan http://antonybarlett[.]site:2095/stats web adresi dikkatimi çekti. Bu adresi VirusTotal zararlı yazılım analiz platformunda arattığımda, güvenlik üreticilerinden sadece SOCRadar tarafından şüpheli, Fortinet tarafından ise istenmeyen (spam) olarak damgalandığını gördüm.



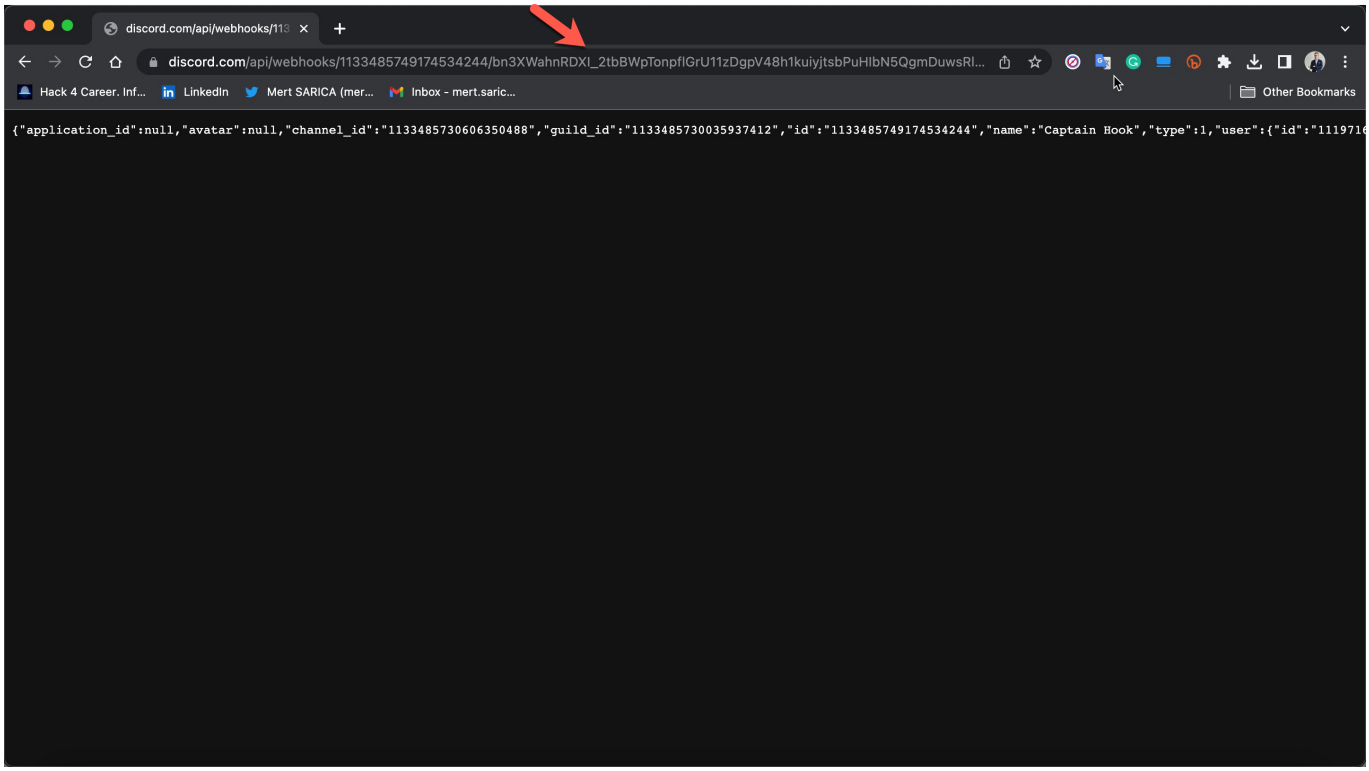


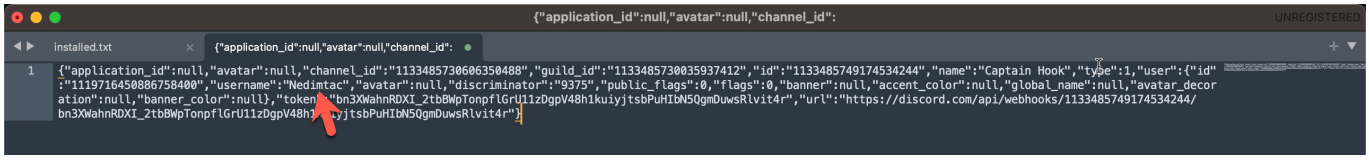


İki farklı zararlı yazılım örneğinde ortak olan bu web adresi beni ve e-Devlet Hacklendi mi? yazımı okuyanları eminim ki pek şaşırtmamıştır çünkü o yazıda dolandırıcıların paylaştıkları dosyalara çoğu zaman arka kapı yerleştirdiklerini görmüştük. Bu zararlı yazılımda ise geliştiriciler, tehdit aktörleri tarafından GitHub alanından indirilip, oluşturulan bu zararlı yazılım tarafından çalınan ve Gofile dosya paylaşım platformuna yüklenen dosyaların adresini kendilerine de almayı, suça ortak olmayı ihmal etmemişlerdi. :)

Sigorta Danışmanını Hedef Alan Tehdit Aktörü Kim?

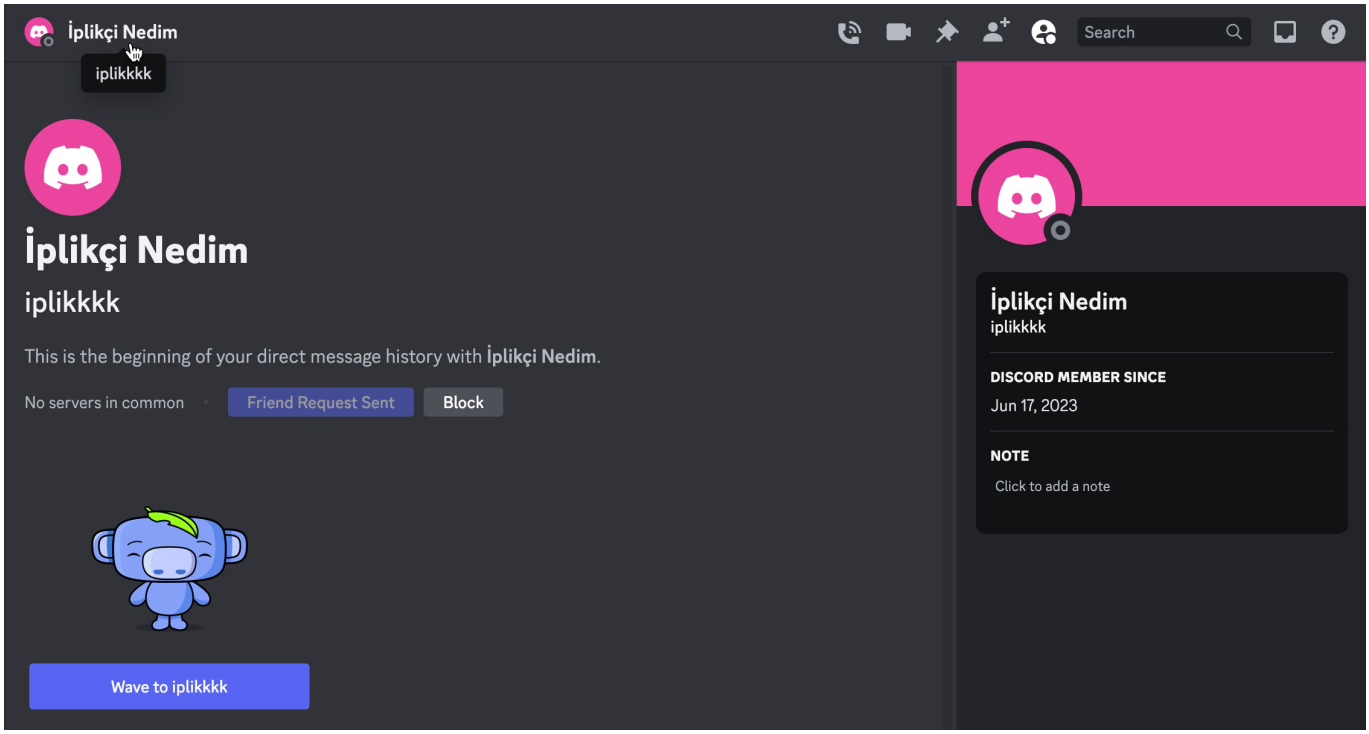
Bu bilgileri elde ettikten sonra sıra aklıma takılan önemli sorulara yanıt bulmaya gelmişti. Bu zararlı yazılımı GitHub alanından indirip, oluşturan ve sigorta danışmanını hedef alan tehdit aktörü kimdi? Bunun için zararlı yazılıma gömülmüş olan Discord Webhook adresinden faydalanmaya karar verdim. Bu adrese gittiğimde Discord API, bu Webhook'u oluşturan kullanıcının 17 Haziran 2023 tarihinde Discord'a katılan Nedimtac kullanıcı adına, İplikçi Nedim görünen adına (display name) sahip bir kişi olduğunu gösterdi.

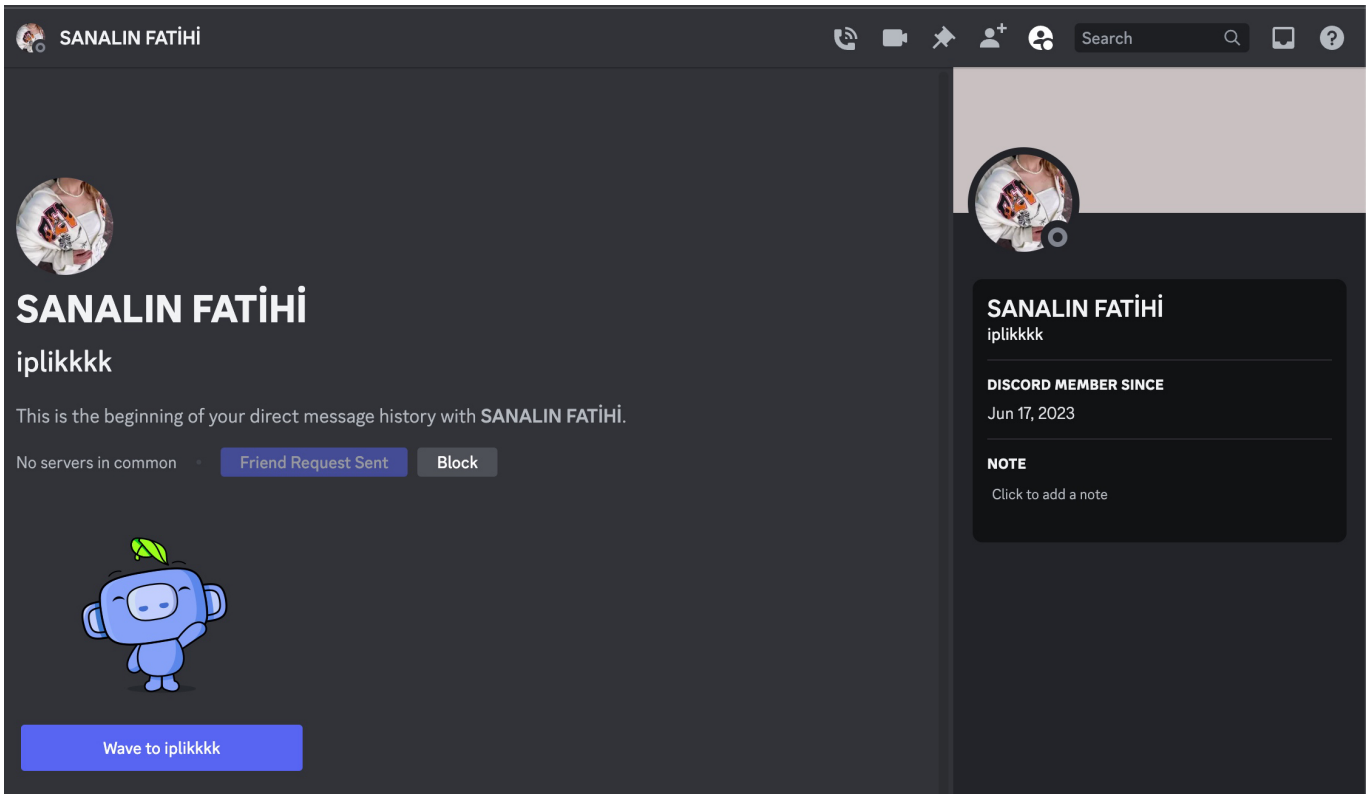


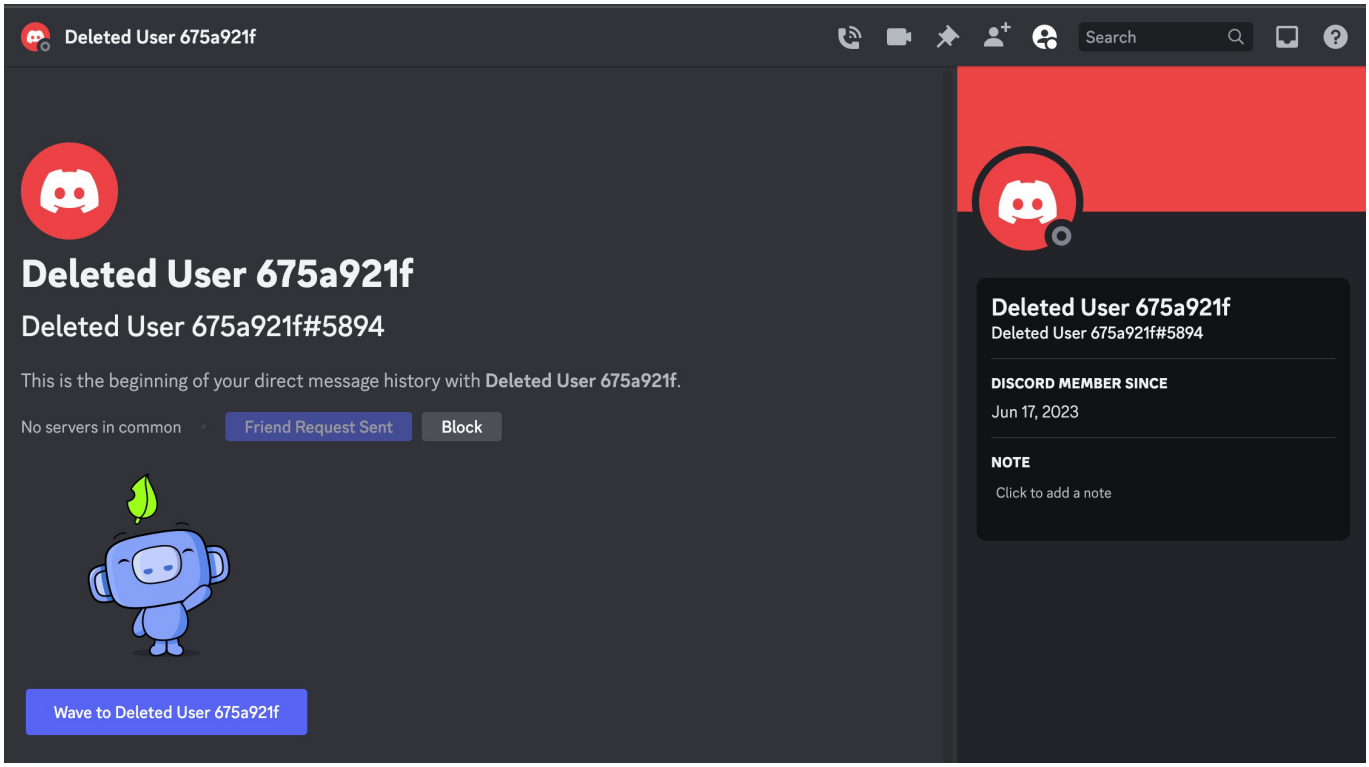


Bu kişinin kullanıcı adı 2023 yılının Temmuz ayında iplikkkk, Ağustos ayında görünen adı SANALIN FATİHİ olarak değiştikten sonra Eylül ayında ise hesabı tamamen silindi. Bu kişiyle iletişime geçmeye çalışsam da davetimi kabul etmediği için sohbet etme şansım maalesef olamadı.


Friend Request Sent
İplikçi Nedim
Nedimtac#9375
User Info
Mutual Servers
Mutual Friends
DISCORD MEMBER SINCE
Jun 17, 2023
NOTE
Click to add a note


İplikçi Nedim
iplikkkk
Search
İplikçi Nedim
iplikkkk
This is the beginning of your direct message history with İplikçi Nedim.
No servers in common
Friend Request Sent
Block
Wave to iplikkkk
İplikçi Nedim
iplikkkk
DISCORD MEMBER SINCE
Jun 17, 2023
NOTE
Click to add a note


SANALIN FATİHİ
Search
SANALIN FATİHİ
iplikkkk
This is the beginning of your direct message history with SANALIN FATİHİ.
No servers in common
Friend Request Sent
Block
Wave to iplikkkk
SANALIN FATİHİ
iplikkkk
DISCORD MEMBER SINCE
Jun 17, 2023
NOTE
Click to add a note

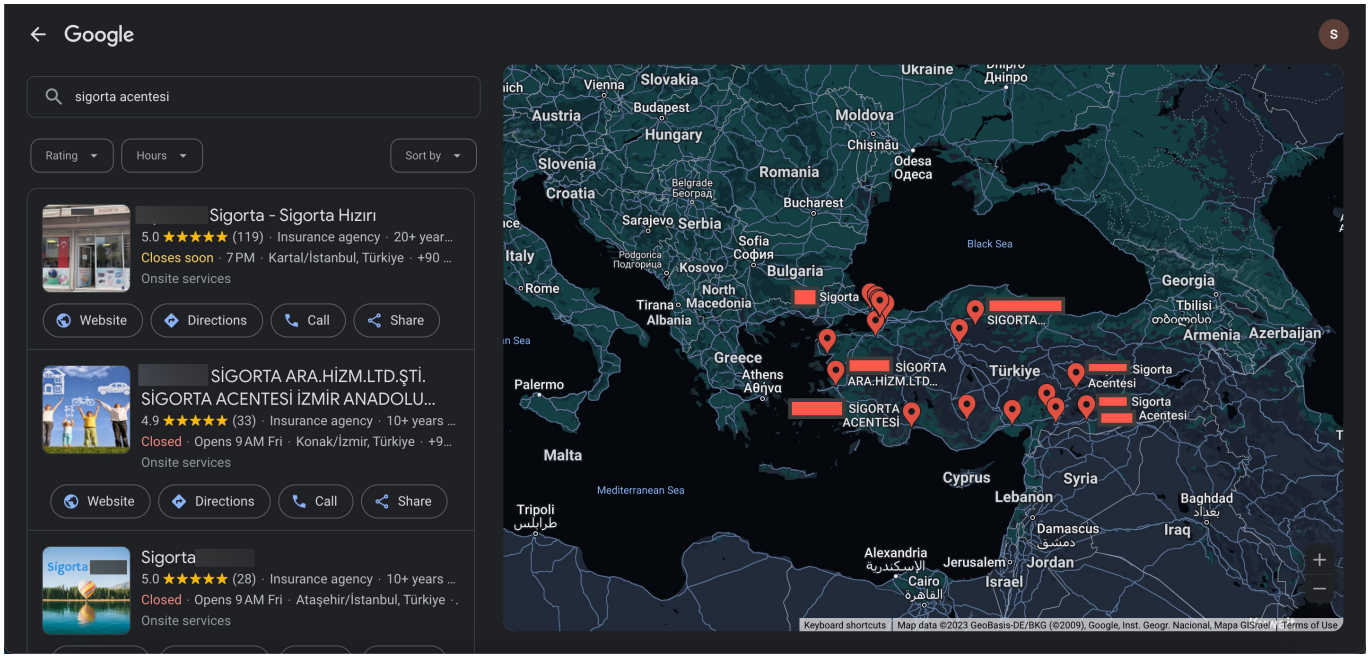


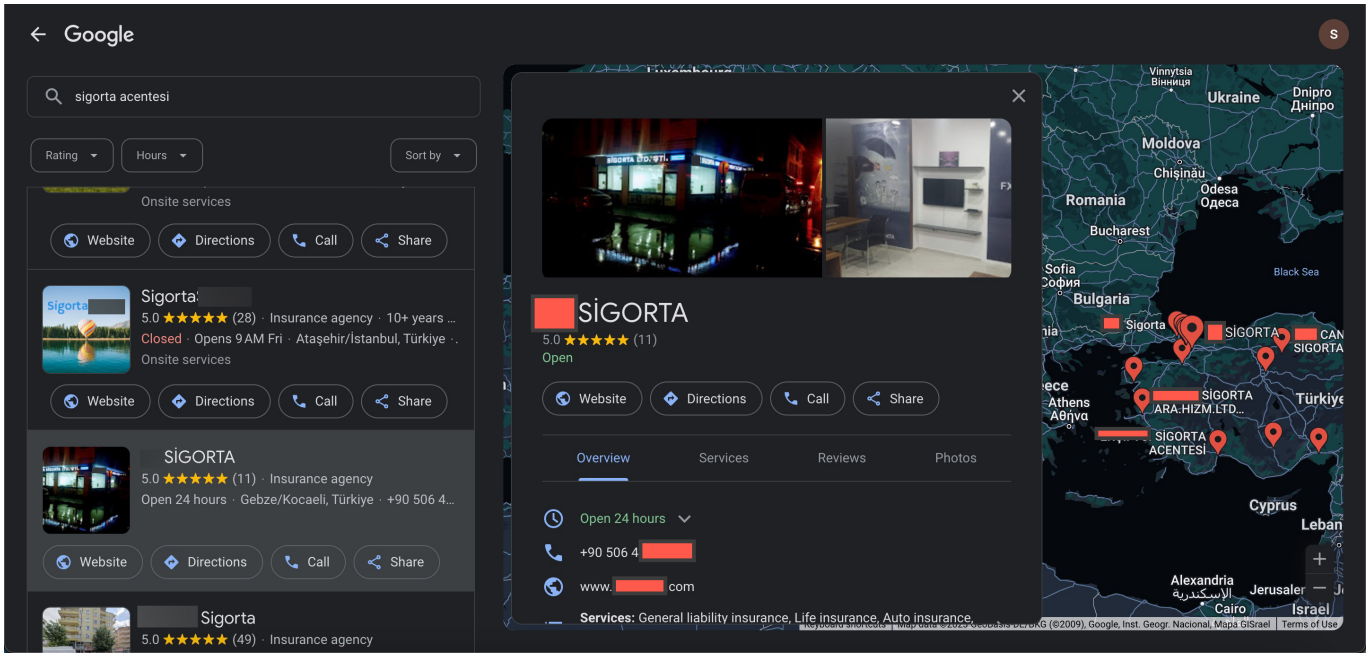
Sigorta Danışmanı / Acentesi Neden Hedef Alınmış Olabilir?

Sıra diğer bir soruya yanıt bulmaya gelmişti. Tehdit aktörü, sigorta danışmanının cep telefonunu nereden ve nasıl bulmuş olabilirdi? Bundan çok daha fazla bilginin dolandırıcıların ellerinde gezdiği son yıllarda, cep telefonu bilgimizin kimlerin elinde olduğunu tahmin etmek çok zor olmasa da bu konu özelinde biraz kafa yormaya karar verdim.

Mevzu bahis sigorta danışmanı olduğunda aynı emlak danışmanlarında olduğu gibi muhtemelen cep telefonu bilgisi internette, genele açık bir yerlerde kolay bulanabilir ve iletişim kurulabilir olmalıydı. Bu tehdit aktörü sigorta acentelerini hedef alıyorsa o halde bunun için ilk başvuracağı yer Google arama motoru olduysa rahtalıkla bu bilgiyi buradan elde etmiş olabilir miydi?

Bunun için Google arama motorunda “sigorta acentesi” anahtar kelimesiyle arama yaptığımda cep telefonu bilgisini paylaşan çok sayıda sigorta acentesi olduğunu gördüm. Sigorta danışmanlarını, acentelerini hedef alan tehdit aktörünün bu yöntemle hacklediği sistemleri ve o sistemler üzerinden sigorta şirketlerinin iç sistemlerine bağlanarak hangi bilgilerimizi sorgulayabileceklerini düşündüğümde, bu konu beni fazlasıyla endişelendirmeye yetti de arttı.





Sonuç

Sigorta danışmanlarının, acentelerinin tehdit aktörleri tarafından bilgi hırsızı zararlı yazılımları ile neden hedef alındığı üzerine biraz düşündüğümde aklıma, elde ettikleri bu bilgileri e-Devlet Hacklendi mi? yazımdaki gibi sorgulanabilir panellere dönüştürme ve/veya dolandırıcılara satma potansiyelinin oldukça yüksek olma ihtimali geldi. Bu ihtimal düşük de olsa yüksek de olsa, tehdit aktörlerinin kişisel verilerimize göz diktiği, bu verilere erişebilen kurumları hedef aldığı maalesef günümüzün yadsınamaz bir gerçeğidir.

Sonuç olarak siz siz olun, cep telefonunuza tanımadığınız kişilerden gelen

bağlantı adreslerine (link) tıklamadan, dosyaları açmadan, çalıştırmadan önce iki defa düşünmeyi ihmal etmeyin.

Bir sonraki yazıda görüşmek dileğiyle herkese güvenli günler dilerim.