

# Bilgi Hırsızları

written by Mert SARICA | 2 September 2024

If you are looking for an English version of this article, please visit [here](#).

## İÇİNDEKİLER

1. Başlangıç
2. Bilgi Hırsızları Zararlı Yazılımı Nedir?
3. 3-2-1 Kayıt!
4. Statik Şüpheli Dosya Analizi (44.exe)
5. Dinamik Şüpheli Dosya Analizi (44.exe)
6. Dinamik Zararlı Dosya Analizi (Builder.exe)
7. Sigorta Danışmanını Hedef Alan Tehdit Aktörü Kim?
8. Sigorta Danışmanı / Acentesi Neden Hedef Alınmış Olabilir?
9. Sonuç

## 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.

any.run/malware-trends/

WHY US SERVICE TRACKER REPORTS FEATURES INTEGRATIONS PRICING BLOG CONTACTS MEDIA KIT TRIAL

## MALWARE TRENDS TRACKER

Most known malwares from all over the cybersecurity world

Search by malware name... 365 d Filters

No.	Family	Type	Trend changes	World rank	Tasks overall
1	RedLine	Stealer		1 ↑	8820
2	Lumma	Stealer		7 ↑	2107
3	Amadey	Infostealer		8 ↑	2076
4	Formbook	Stealer		9 ↓	2047
5	Raccoon	Stealer		13 ↓	1469
6	Arkei	Stealer		15 ↑	1380

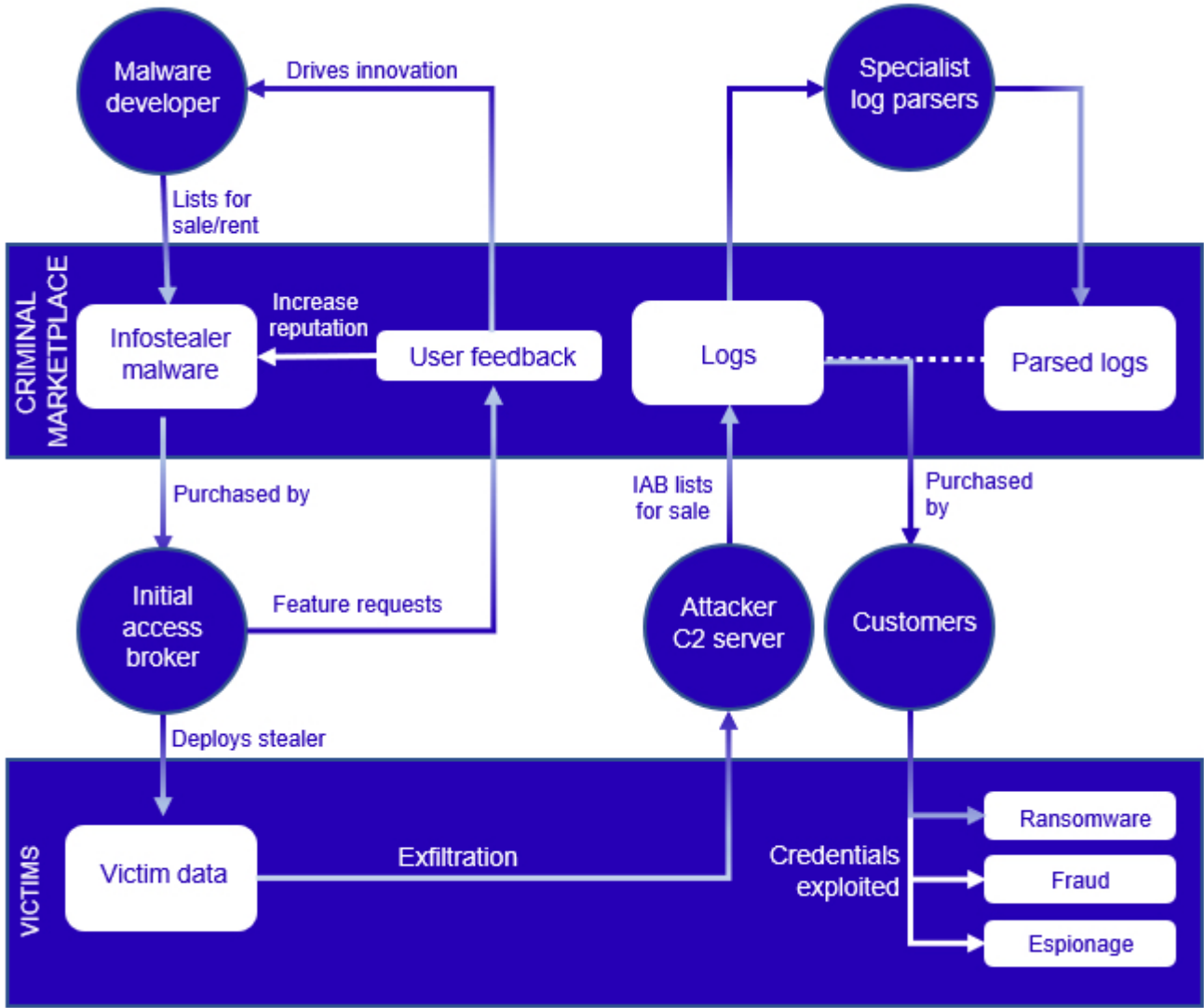
Referans: ANY.RUN

## Bilgi Hırsızlı Zararlı Yazılımı Nedir?

Bilgi hırsızlı 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 araçlarına (IAB) satılmakta veya kiralanmaktadır.

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





Referans: Secureworks

Özellikle SOCRadar gibi siber tehdit istihbaratı firmaları bu yerleri yakından takip ederek müşterilerini, satışa sunulan bilgileri hakkında uyarılmaktadırlar. 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

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**.

338 All Alarms | 338 Open Alarms | 0 On Hold Alarms | 0 Resolved Alarms | 0 False Positive Alarms

Alarm ID: 12490242

**1 HIGH CONSOLIDATED ALARMS**

Consolidated Alarm #934781

2023-02-01 23:50:16

TAGS: stealer log, credential, black market, compromised, sale, blackmarket

CONTENT:

Affected Assets: l.com

Stealer: Vidar

Vendor: Mo####y! [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

Digital Risk Protection > Deep&Dark Web Monitoring > Black Market Botnet Detection

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 clear-text, 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

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**.

10.00 Black Market Credits

Search... All time

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	<a href="#">Open Preview</a>	.com	10.00 \$	Action Waiting	REQUEST OBTAIN	2023-02-01	<a href="#">View Incident</a>	<a href="#">Copy</a>
Market-12476286	Russian Market	<a href="#">Open Preview</a>	.talao.net	10.00 \$	Action Waiting	REQUEST OBTAIN	2023-02-01	<a href="#">View Incident</a>	<a href="#">Copy</a>
Market-12454340	Russian Market	<a href="#">Open Preview</a>	.com	10.00 \$	Action Waiting	REQUEST OBTAIN	2023-01-31	<a href="#">View Incident</a>	<a href="#">Copy</a>
Market-12423963	Russian Market	<a href="#">Open Preview</a>	.com	10.00 \$	Action Waiting	REQUEST OBTAIN	2023-01-29	<a href="#">View Incident</a>	<a href="#">Copy</a>
Market-12405017	Russian Market	<a href="#">Open Preview</a>	.com	10.00 \$	Action Waiting	REQUEST OBTAIN	2023-01-28	<a href="#">View Incident</a>	<a href="#">Copy</a>
Market-12358675	Russian Market	<a href="#">Open Preview</a>	.com	10.00 \$	Action Waiting	REQUEST OBTAIN	2023-01-25	<a href="#">View Incident</a>	<a href="#">Copy</a>
Market-12343361	Russian Market	<a href="#">Open Preview</a>	.com	10.00 \$	Action Waiting	REQUEST OBTAIN	2023-01-24	<a href="#">View Incident</a>	<a href="#">Copy</a>
Market-12286435	Russian Market	<a href="#">Open Preview</a>	sportsbook.com	10.00 \$	Action Waiting	REQUEST OBTAIN	2023-01-20	<a href="#">View Incident</a>	<a href="#">Copy</a>
Market-12256613	Russian Market	<a href="#">Open Preview</a>	.com	10.00 \$	Action Waiting	REQUEST OBTAIN	2023-01-19	<a href="#">View Incident</a>	<a href="#">Copy</a>
Market-12255753	Russian Market	<a href="#">Open Preview</a>	.com	10.00 \$	Action Waiting	REQUEST OBTAIN	2023-01-19	<a href="#">View Incident</a>	<a href="#">Copy</a>
Market-12232039	Russian Market	<a href="#">Open Preview</a>	.com	10.00 \$	Action Waiting	REQUEST OBTAIN	2023-01-18	<a href="#">View Incident</a>	<a href="#">Copy</a>
Market-12200753	Russian Market	<a href="#">Open Preview</a>	sportsbook.com	10.00 \$	Action Waiting	REQUEST OBTAIN	2023-01-15	<a href="#">View Incident</a>	<a href="#">Copy</a>
Market-12188269	Russian Market	<a href="#">Open Preview</a>	.talao.net	10.00 \$	Action Waiting	REQUEST OBTAIN	2023-01-14	<a href="#">View Incident</a>	<a href="#">Copy</a>

Featured Filters:

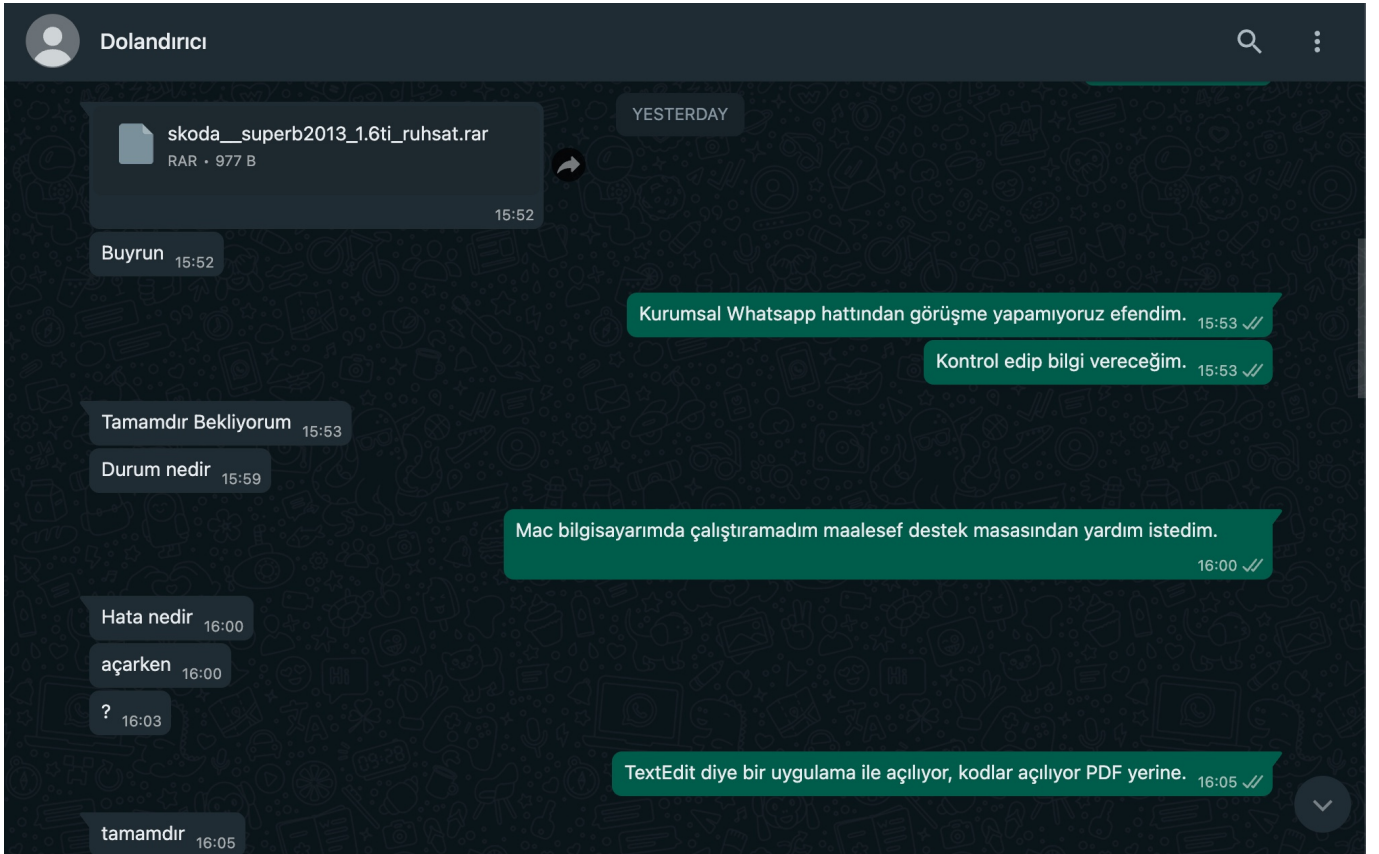
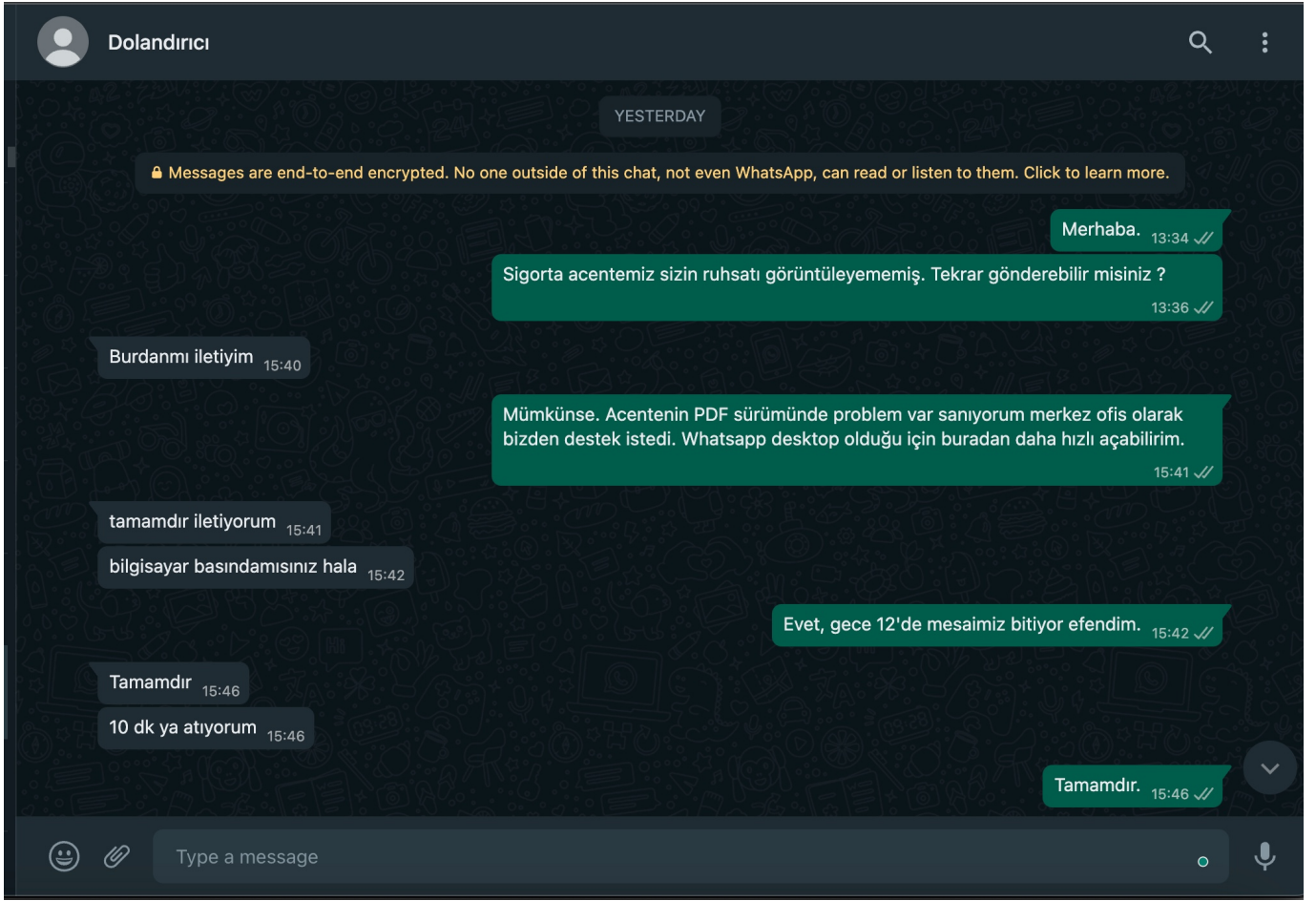
- All Findings: 77
- Action Waiting: 77
- Requested: 0
- Obtained: 0
- Resolved: 0
- False Positive: 0
- Declined & Tracking: 0

Referans: SOCRadar XTI

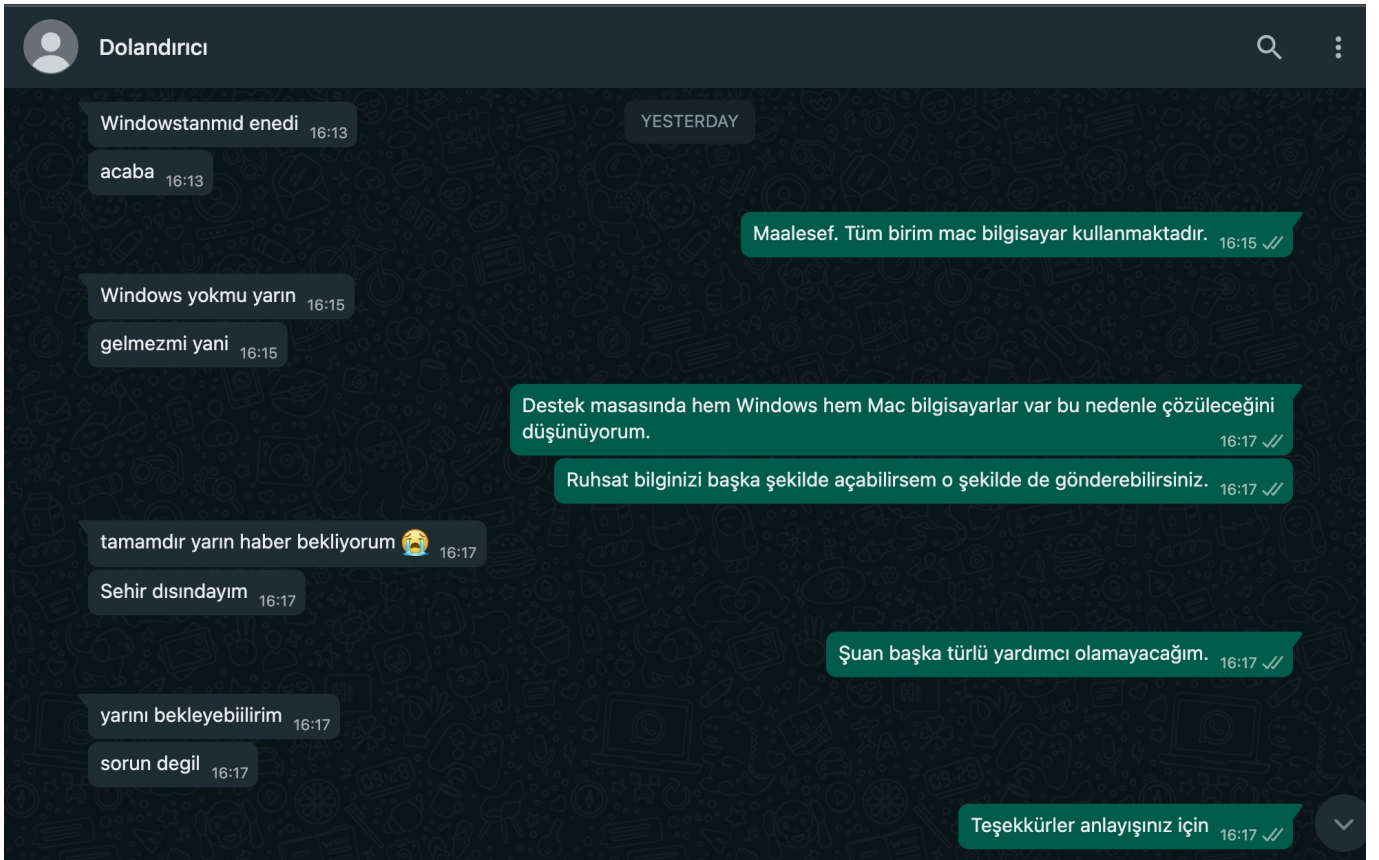
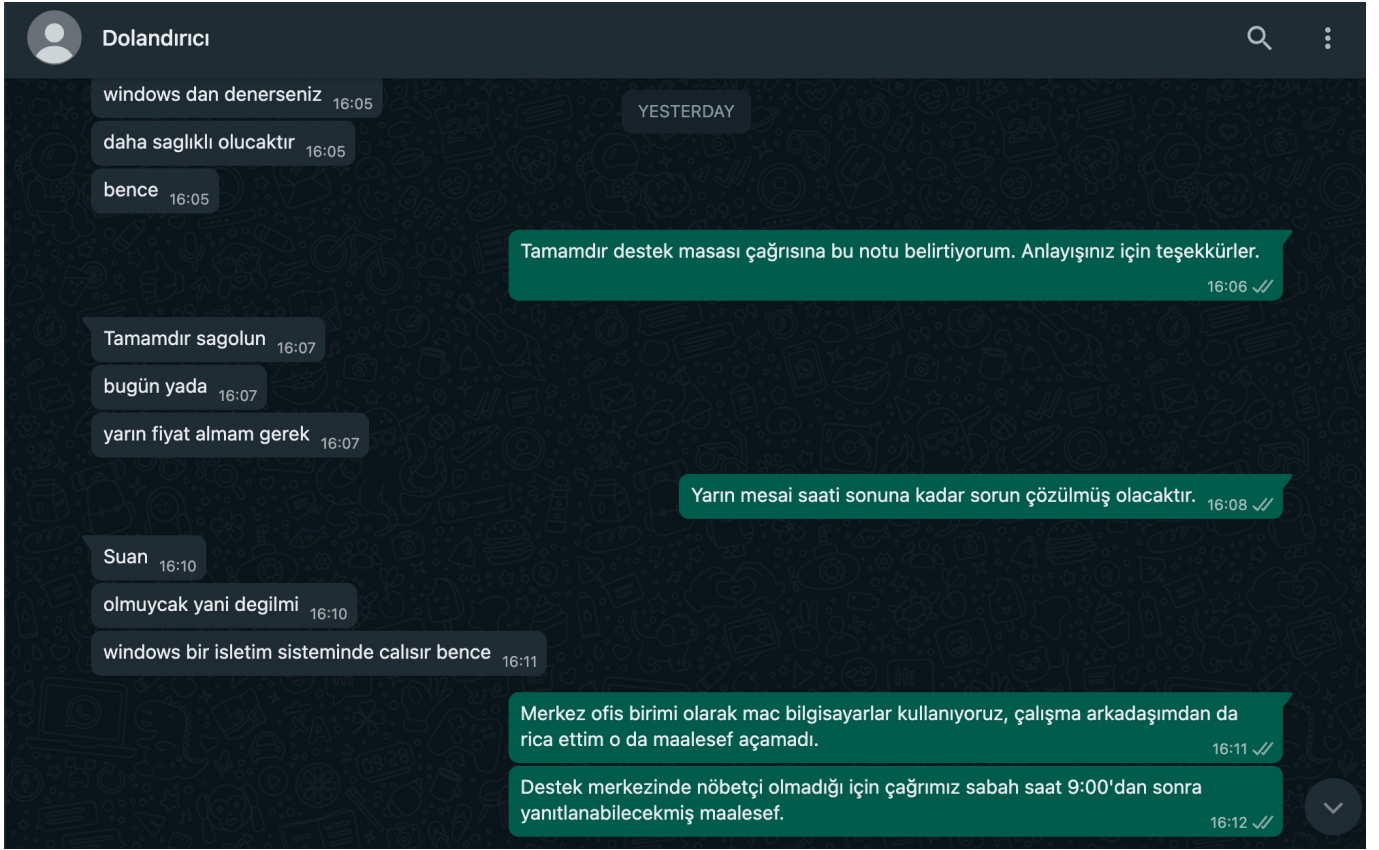
## 3-2-1 Kayıt!

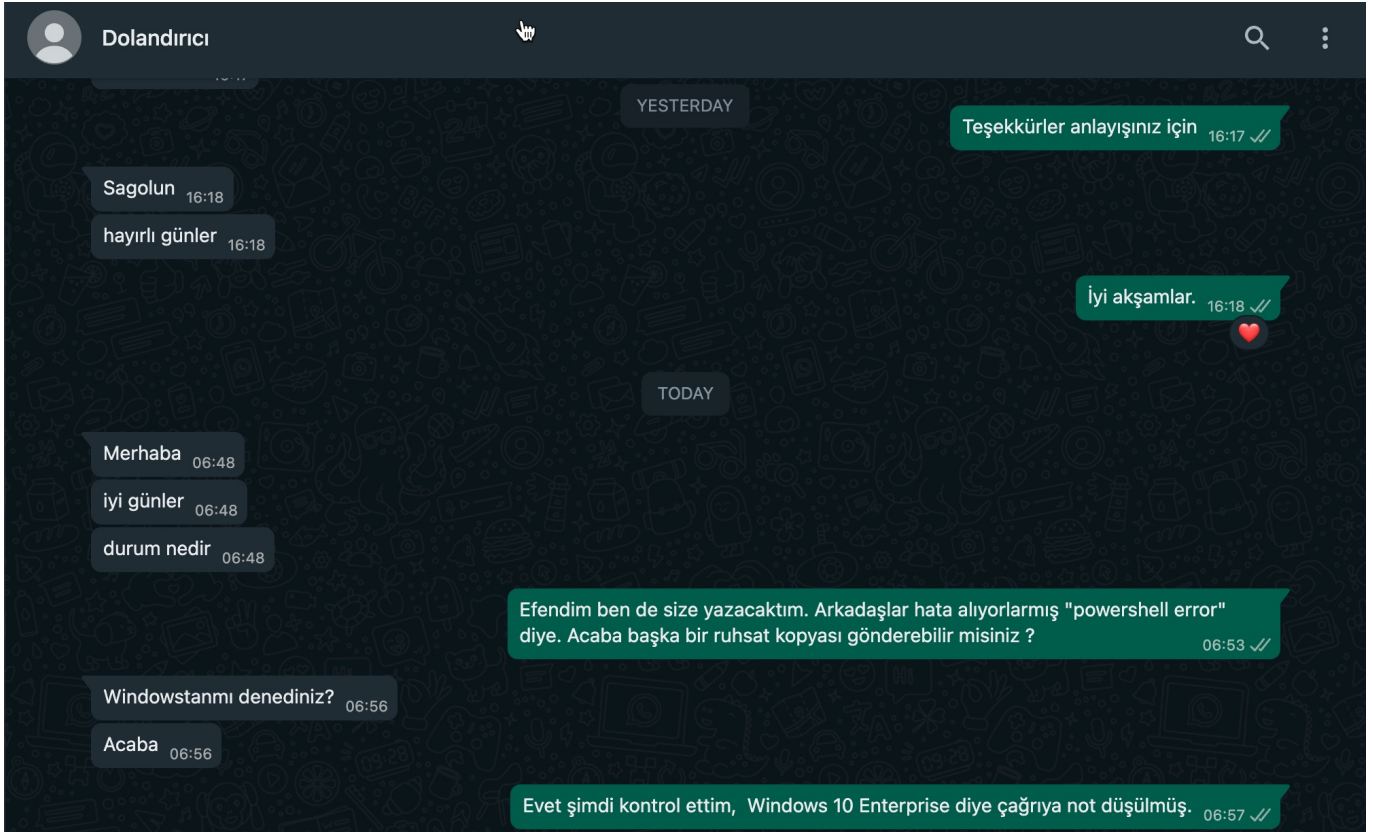
Hikayemiz, 25 Temmuz 2023 tarihinde Bartu KILIÇ'ın akrabasından gelen bir WhatsApp mesajı ile başlar. Sigorta danışmanı olan akrabası, araç sigortası yaptırmak isteyen bir kişinin WhatsApp üzerinden kendisine ruhsat adı altında gönderdiği bir dosyadan (skoda\_\_superb2013\_1.6ti\_ruhsat.rar) şüphelenerek konuyu siber güvenlik uzmanı olan Bartu'ya taşımaya karar verir. Bartu da bu hikayeyi, kendisi ile son zamanlarda yaşanan 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 değil ya :) dolandırıcı ile yazışmaya başladım ve çok geçmeden hikayeye konu olan şüpheli dosyayı elde edebildim.



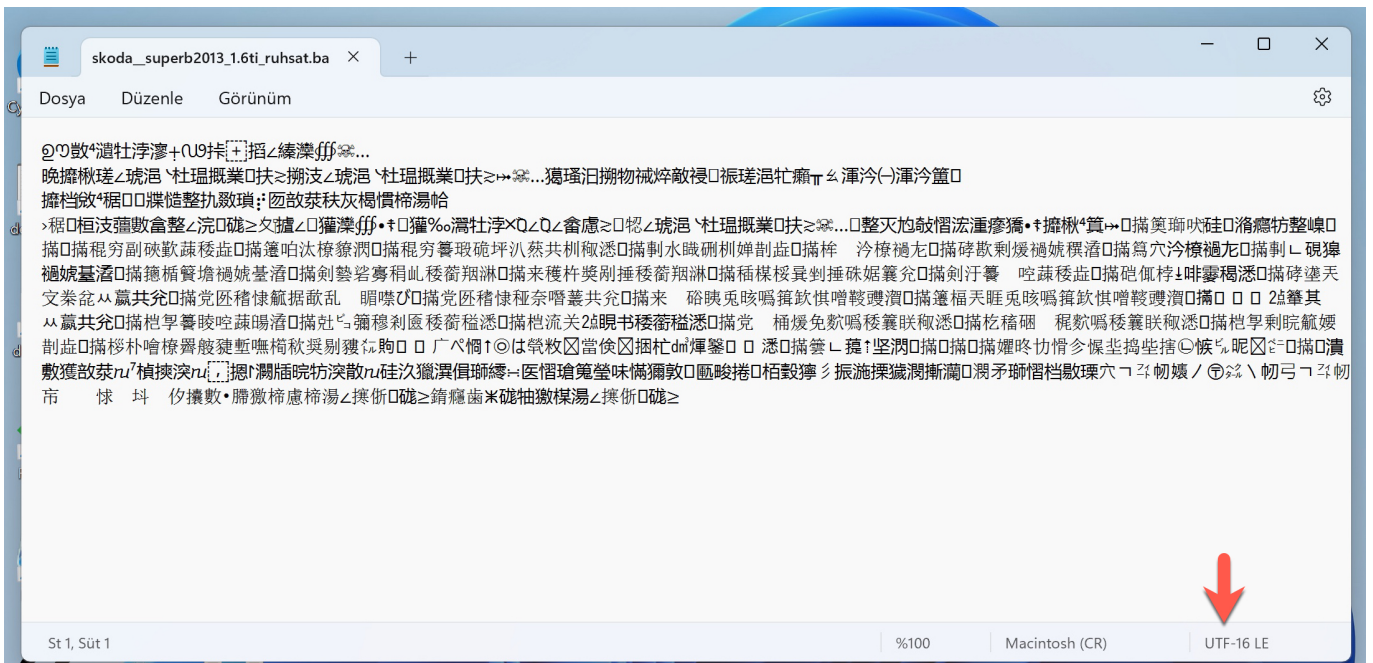




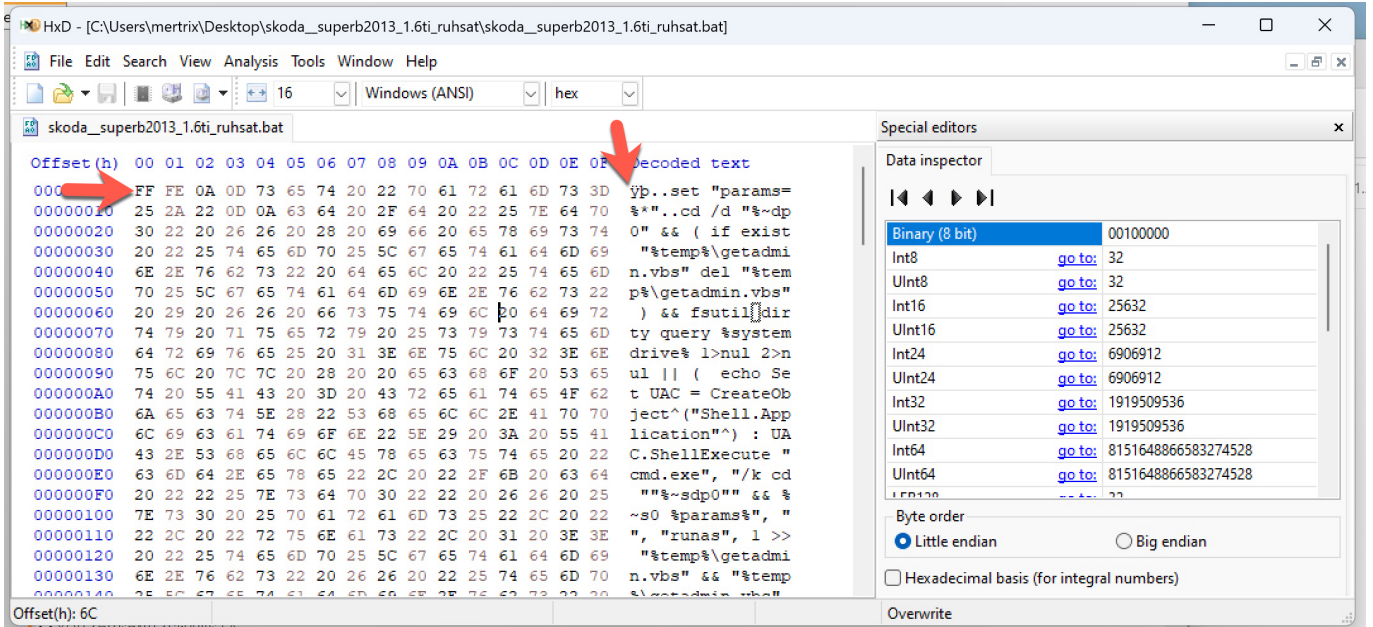


## Statik Şüpheli Dosya Analizi (44.exe)

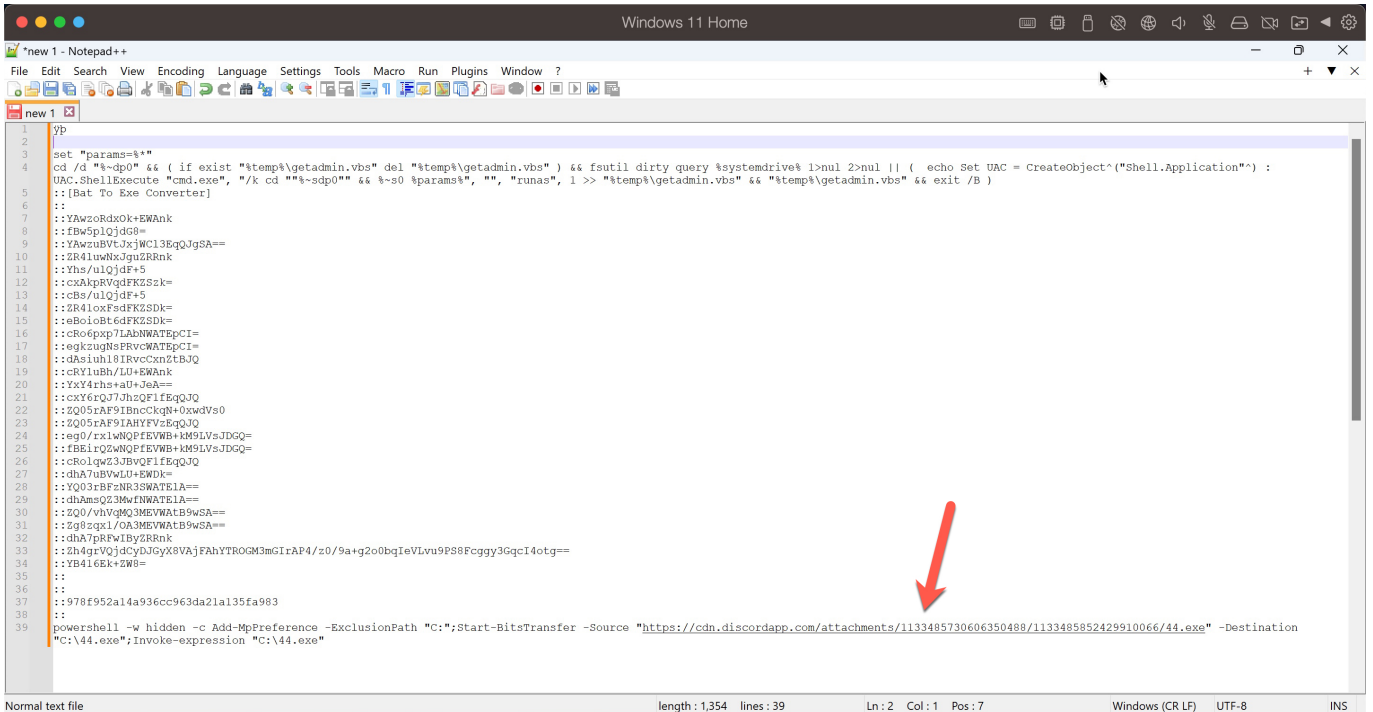
skoda\_\_superb2013\_1.6ti\_ruhsat.rar dosyasını sanal Windows 11 işletim sistemi üzerinde açtıktan sonra skoda\_\_superb2013\_1.6ti\_ruhsat.bat dosyası hemen dikkatimi çekti. Notepad ile dosyayı açtığımda karşıma UTF-16 kodlanmış bir karakter dizisi çıktı. HxD hex editörü ile BAT dosyasını incelediğimde, 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](http://antonybarlett[.]site:2095/stats)) gönderiyordu.
5. Bağlantı adresini, tehdit aktörünün Discord kanalına Webhook ile gönderiyordu.

The screenshot displays a network analysis tool interface with the following components:

- HTTP Requests Table:**

Timeshift	Headers	Rep	PID	Process name	CN	URL
3465 ms	GET   200: OK	3944	44.exe			<a href="http://ipinfo.io/json">http://ipinfo.io/json</a>
5124 ms	GET   200: OK	3944	44.exe			<a href="https://api.gofile.io/getServer">https://api.gofile.io/getServer</a>
6884 ms	POST   200: OK	3944	44.exe			<a href="https://store5.gofile.io/uploadFile">https://store5.gofile.io/uploadFile</a>
8464 ms	POST   200: OK	3944	44.exe			<a href="http://antonybarlett.site:2095/stats">http://antonybarlett.site:2095/stats</a>
9093 ms	POST   204: No Content	3944	44.exe			<a href="https://discord.com/api/webhooks/146.../85749174534">https://discord.com/api/webhooks/146.../85749174534</a>
- Process Details (44.exe):**

Content	Size	Type
247 b	247 b	binary
42 b	42 b	binary
4.85 Kb	4.85 Kb	binary
361 b	361 b	binary
139 b	139 b	binary
4 b	4 b	text
195 b	195 b	binary
- Callout Boxes:**
  - Returns the geolocation information for an IP address and basic ASN details (points to <http://ipinfo.io/json>)
  - Uploads files and gets a shareable download link. (points to <https://store5.gofile.io/uploadFile>)
  - Posts the shareable download link to the threat actor's Discord channel. (points to <https://discord.com/api/webhooks/146.../85749174534>)
  - Returns the best server available to receive uploads (points to <https://api.gofile.io/getServer>)
  - Sends the shareable download link to the web server of the malware developer. (points to <http://antonybarlett.site:2095/stats>)



**Static discovering**

Look up on [VirusTotal](#)

Submit to analyze Download

Downloaded | JSON data (247.00 b)  
Mime: application/json Entropy: 4.83

Main HEX

MD5 5538C1EB020433D410389B391E82BFE8  
SHA1 83D4F406DDDC2381A1055ABC932B2EADD563B132  
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

Click any module for information

Info [1232] svchost.exe The process checks LSA protection

Try community version for free! Register now

**Static discovering**

Look up on [VirusTotal](#)

Submit to analyze Download

Downloaded | JSON data (42.00 b)  
Mime: application/json Entropy: 3.62

Main HEX

MD5 49F2DE7E3957DC6159D7E823F57AC68B  
SHA1 742CE6303CECCE5A1320311FFE1173F80A7D8E42  
SHA256 8255E148857A3533ABE2CF8213966D1A946C5CA54CFDCF7AF4B41D035458B75  
SSDEEP 3:YWR4blllWAXY:YWylrlrY

EXIF (JSON)

JSON

DataServer	store5
Status	ok

Click any module for information

Info [1232] svchost.exe The process checks LSA protection

Try community version for free! Register now

**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 F53F3297959E0492FA8B5CE33C7BDD82ACBC2CE  
 SHA256 35E2FD69F3EF2770EEC882669381A907E29BDDC29235CEF4F49D6AC98AF0345A  
 SSDEEP 6:YWybll+Ofx5ZHJrKR40fRyER2ZpxsdFVg8/cAQfykoUJTQWRKB+KG7Ds1:YWybllBHZKR11R26dYRfykzTQWKD1

**EXIF (JSON)**

**JSON**

DataCode	e3TS0x
DataDownloadPage	https://gofile.io/d/e3TS0x
DataFileid	f90fd2a-cf72-4cc7-a074-6a5aa7bc2a0d
DataFileName	.._W0_wE0_aE0_pE0_ES_(65b178c1-239c-11ed-b4aa-806e6f6e6963)_MKt6c8fchPzzip
DataGuestToken	lb2ws9FGfWVnuHFoHw3LdJTT13EIBqk
DataMd5	f9a36b5a4b8cc8f522170a89e78ea8fb
DataParentFolder	24932005-0e03-46ad-b50d-a0902b450bd1
Status	ok

Click any module for information

Info [1232] svchost.exe The process checks LSA protection

**Static discovering**

Look up on [VirusTotal](#)

**stats** [Submit to analyze](#) [Download](#)

Downloaded | JSON data (139.00 b)  
 Mime: application/json Entropy: 5.01

**Main** **HEX**

MD5 4072E4D2B6EEC4111C3A475D71410879  
 SHA1 5D5A73268AE8507C021DC18DEBAC93D79D977F67  
 SHA256 7AF7542DEC8BC817ED682FAE8D7F8EA97C838C4C36F933D573C5B5211CB8CA69  
 SSDEEP 3:YgKad1NaxL1sHMjhLVfSVzZfufRgYSEUJ6dDDMQxb:YgK+WoyhRVFSvBsyJUJTQN

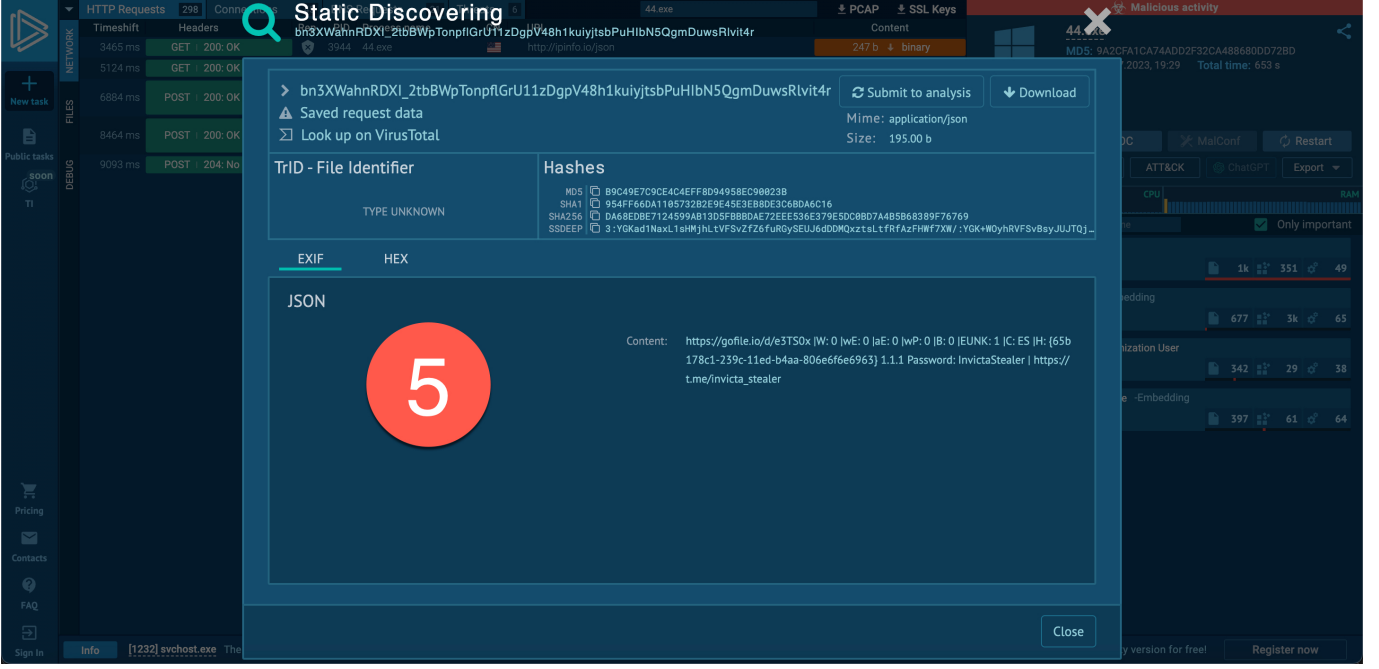
**EXIF (JSON)**

**JSON**

Content	https://gofile.io/d/e3TS0x  W: 0  wE: 0  jaE: 0  wP: 0  B: 0  EUNK: 1  C: ES  H: (65b178c1-239c-1...
---------	--

Click any module for information

Info [1232] svchost.exe The process checks LSA protection



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 menşeli bilgi hırsızları 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 which  
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](#)



👁 632 ⭐ edited 19:28





Invicta Stealer [🇬🇧/🇷🇺]

201 subscribers

Pinned message

~~xx~~ Invicta Stealer — a powerful, free native stealer ~~xx~~ This is a C++ stealer which



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>



506 13:12

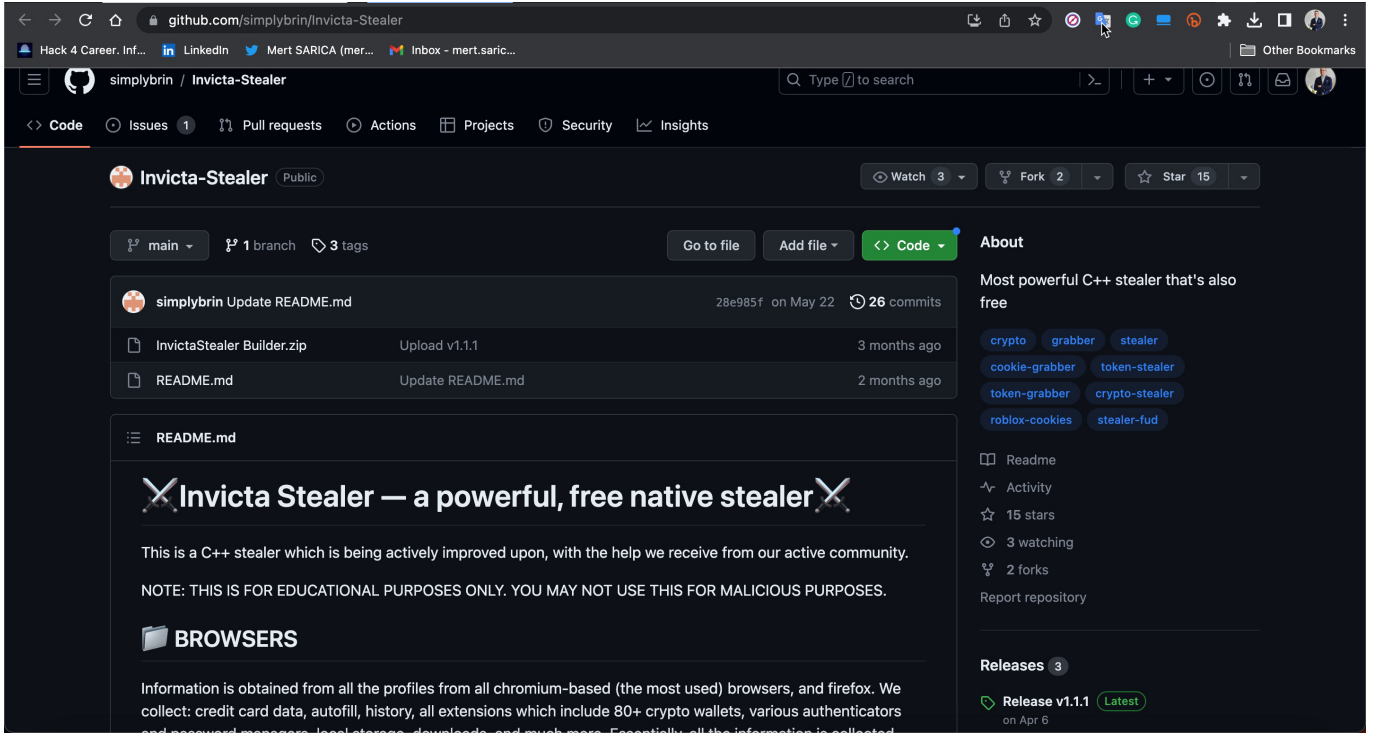
Invicta Stealer [🇬🇧/🇷🇺]

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



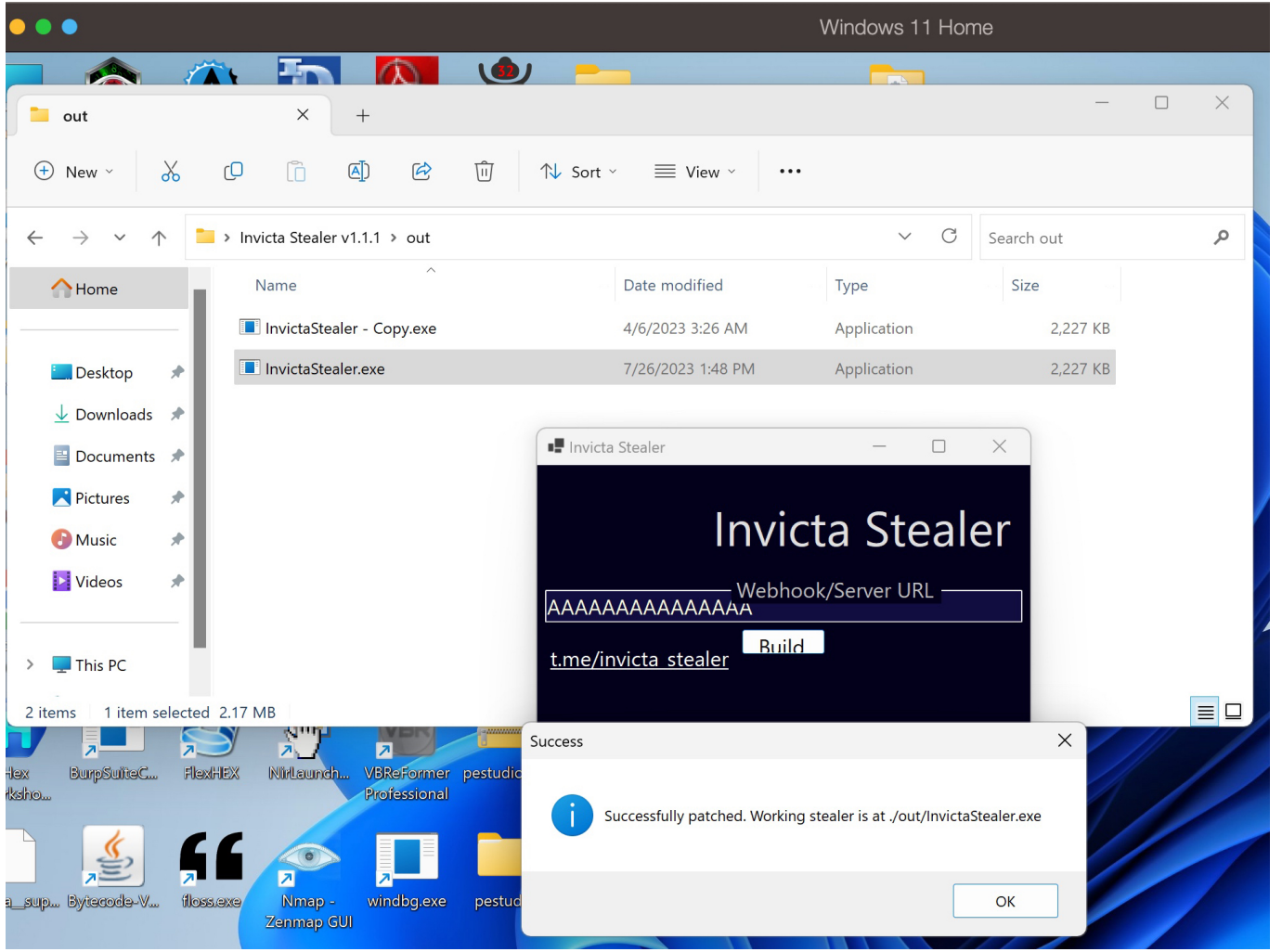
523 13:18



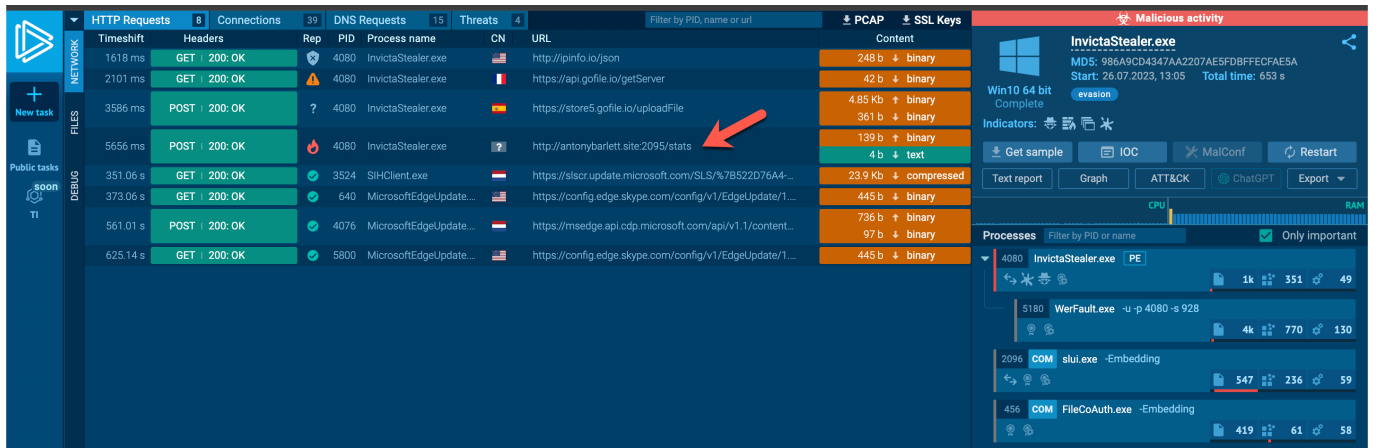
\*Invicta Stealer'ın YouTube kanalındaki tanıtım videosu\*

## 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](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.





Static discovering

Request Response

stats

Downloaded | JSON data (139.00 b)  
Mime: application/json Entropy: 5.06

Main HEX

MD5 4F2453F3318139B419788F73CE880D0F  
SHA1 D77B24743DC49BE14C089821942F2C2233D4910F  
SHA256 0A6F793267AA2441B385DE9E086FEFB2A705E25D9BA9FFFE8835BC8BE141A7CE  
SSDEEP 3:YgKad1NaXL1TRSAFVjhlLVFSvZfZ6fURGySEUJ6dDDMQxb:YgK+WBjhrVFSvBsyJUJTQN

EXIF (JSON)

JSON

Content https://gofile.io/d/lxR7r7 [W: 0 |wE: 0 |aE: 0 |wP: 0 |B: 0 |EUNK: 1 |C: ES |H: {65b178c1-239c-11...

antonybarlett.site

0 / 88

No security vendors flagged this domain as malicious

Creation Date 5 months ago Last Analysis Date 2 days ago

Community Score

DETECTION DETAILS RELATIONS COMMUNITY

Join the VT Community and enjoy additional community insights and crowdsourced detections, plus an API key to automate checks.

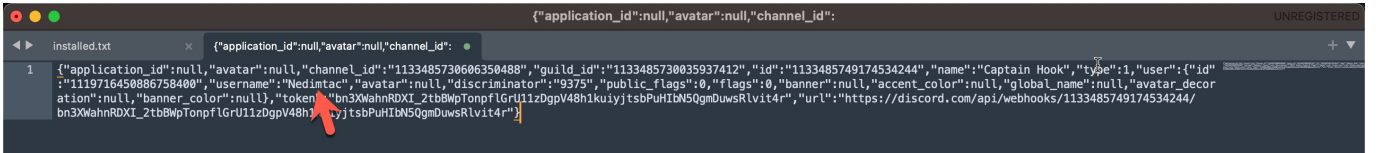
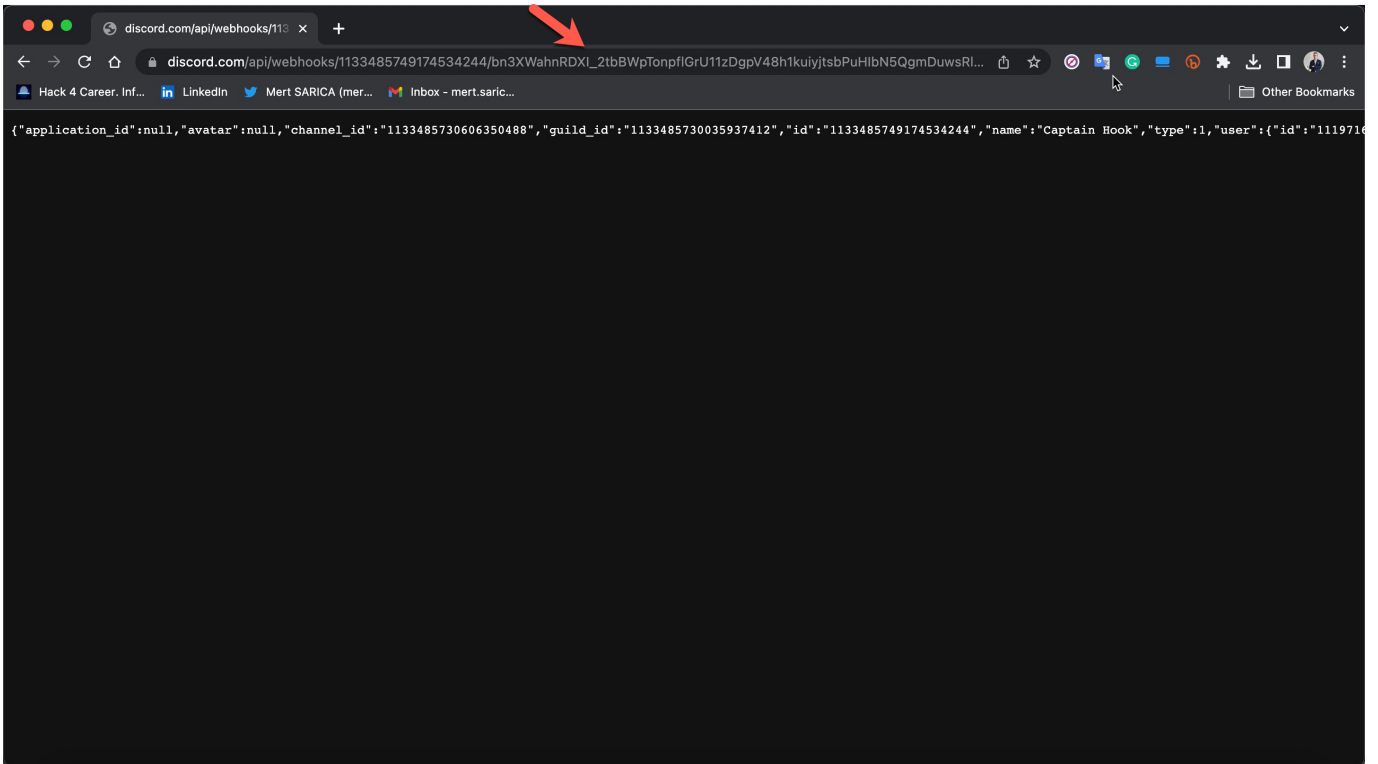
Security vendors' analysis

Vendor	Status	Vendor	Status
Fortinet	Spam	SOCRadar	Suspicious
Abusix	Clean	Acronis	Clean
ADMINUSLabs	Clean	AICC (MONITORAPP)	Clean
AlienVault	Clean	alphaMountain.ai	Clean
Antiy-AVL	Clean	Avira	Clean
benkov...	Clean	Bfor AI ProCrime	Clean

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 olmadı.



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




# 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  
iplikkkk




# SANALIN FATİHİ

iplikkkk

This is the beginning of your direct message history with SANALIN FATİHİ.

No servers in common [Friend Request Sent](#) [Block](#)

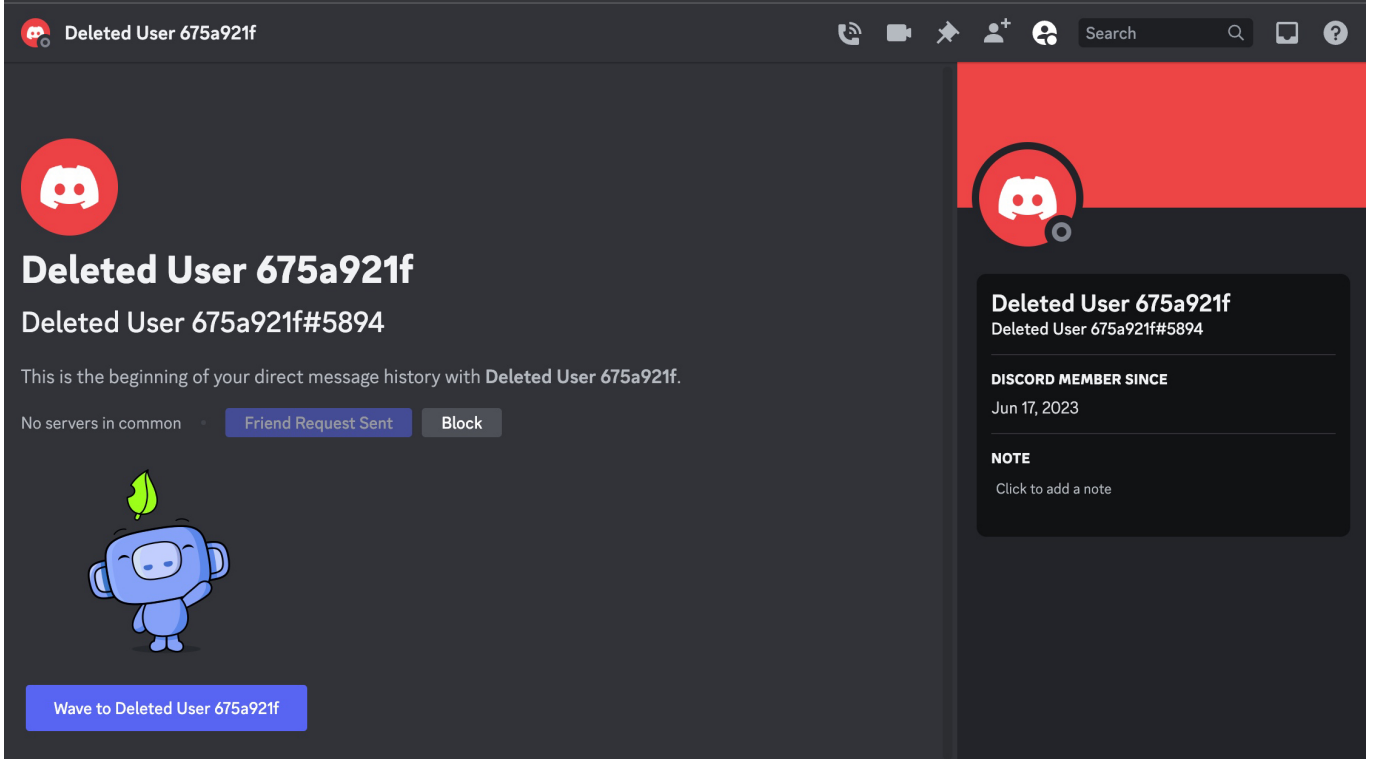


Wave to iplikkkk

SANALIN FATİHİ  
iplikkkk

**DISCORD MEMBER SINCE**  
Jun 17, 2023

**NOTE**  
Click to add a note

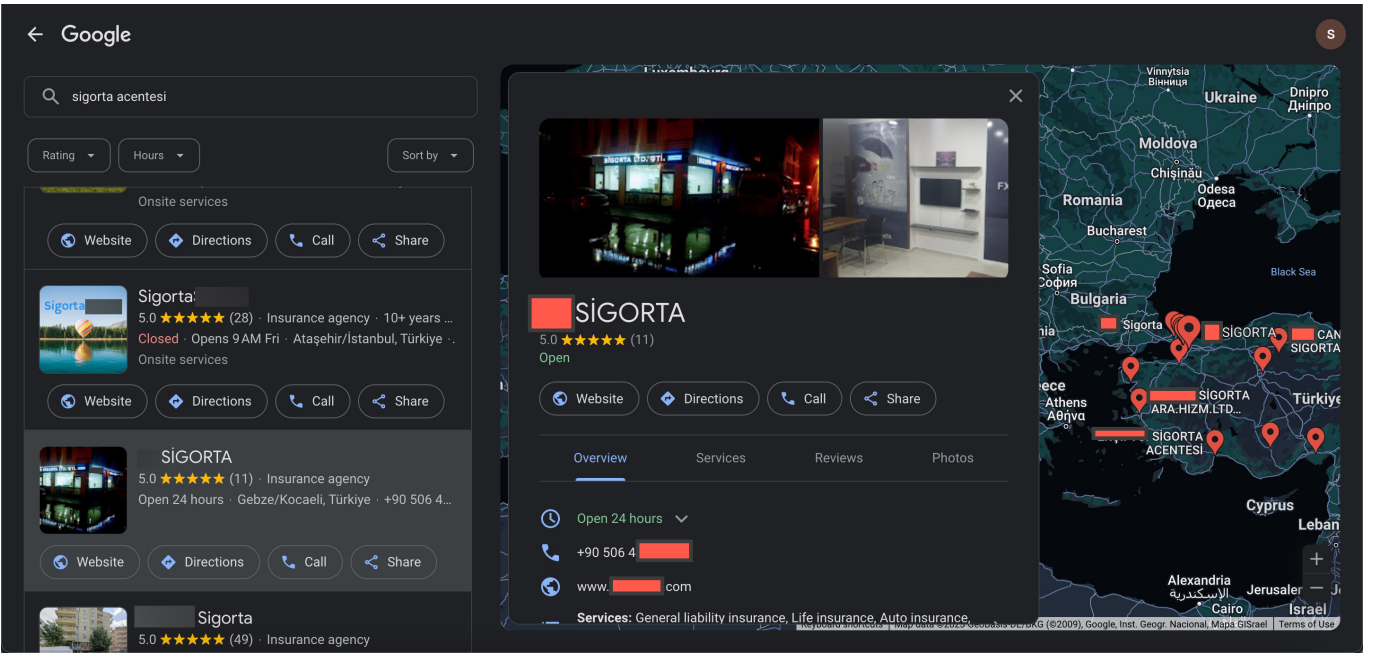
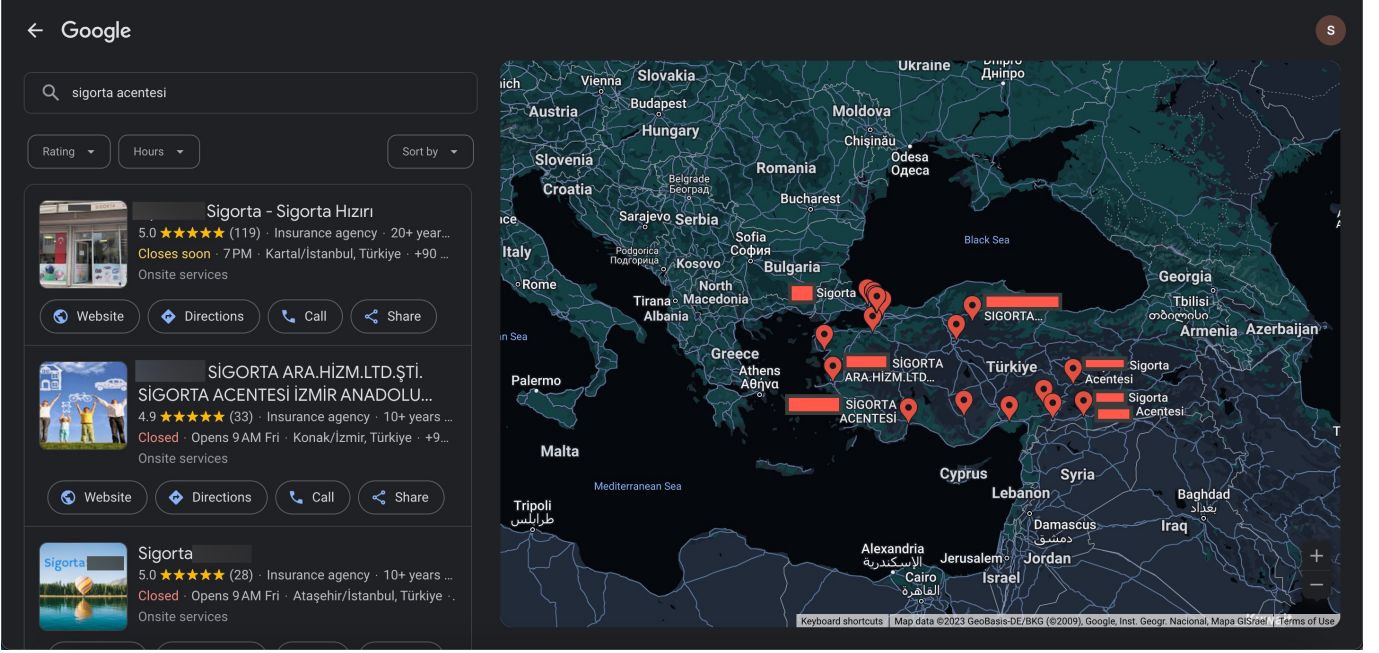


## Sigorta Danışmanı / Acentesi Neden Hedef Alınmış Olabilir?

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 yerde kolay bulunabilir ve iletişim kurulabilir olmalıydı. Bu tehdit aktörü sigorta acentelerini hedef alıyorsa o halde bunun için ilk başvuracağı yer Google arama motoru olduysa rahatlıkla 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 hırsızlığı 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 yadsınmaz bir gerçeğidir.

Sonuç olarak siz siz olun, cep telefonunuza tanımadığınız kişilerden gelen

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

Bir sonraki yazıda görüşmek dileęiyle herkese güvenli günler dilerim.