Information Thieves

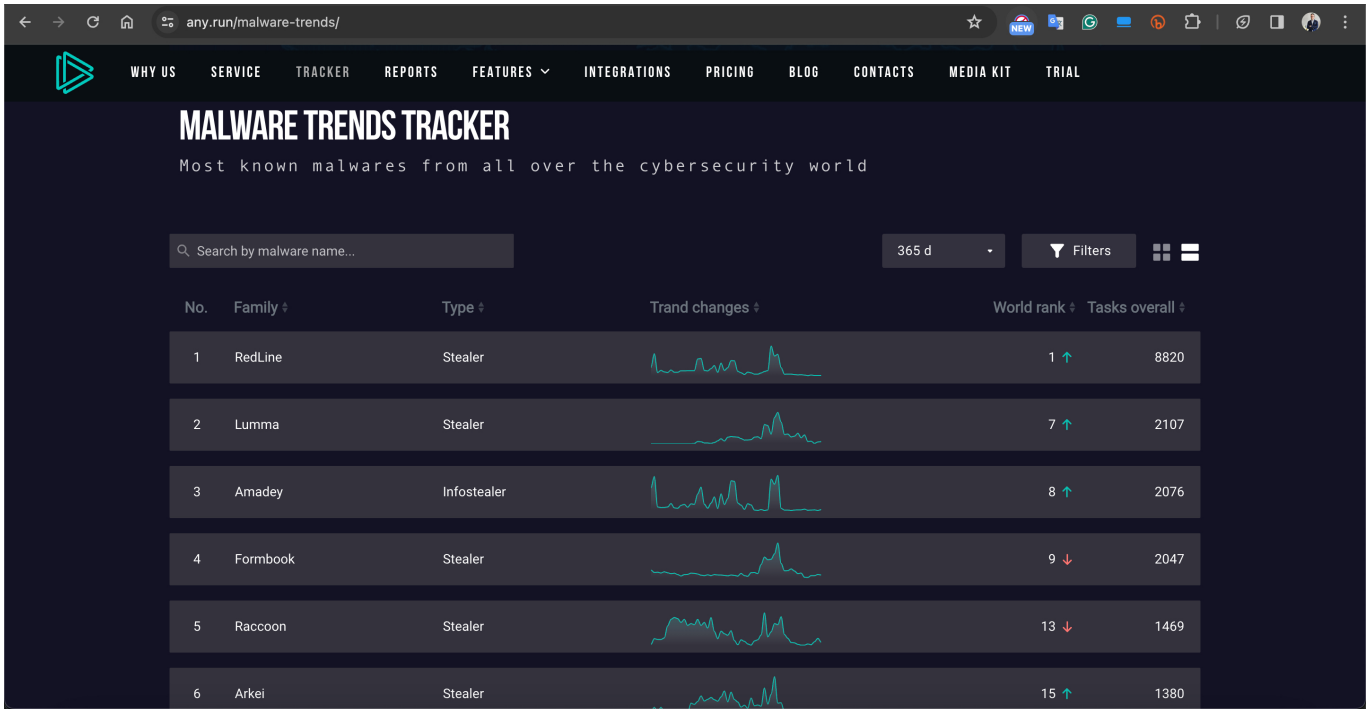
written by Mert SARICA | 2 September 2024

Table of Contents

Introduction

In recent years, when we look at cybersecurity incidents involving prominent entities such as Uber, Airbus, Grand Theft Auto VI, and similar cases, we observe that malicious software, specifically infostealers designed for information theft, has come to the forefront. These types of malware are increasingly playing infostealers a significant role in the cybercrime ecosystem.

Research indicates that in 2023, cybersecurity incidents related to this type of malicious software doubled compared to the year 2022. Particularly in Russian markets, there is a notable increase, with logs stolen and offered for sale by these malicious programs showing a 690% surge since 2021.

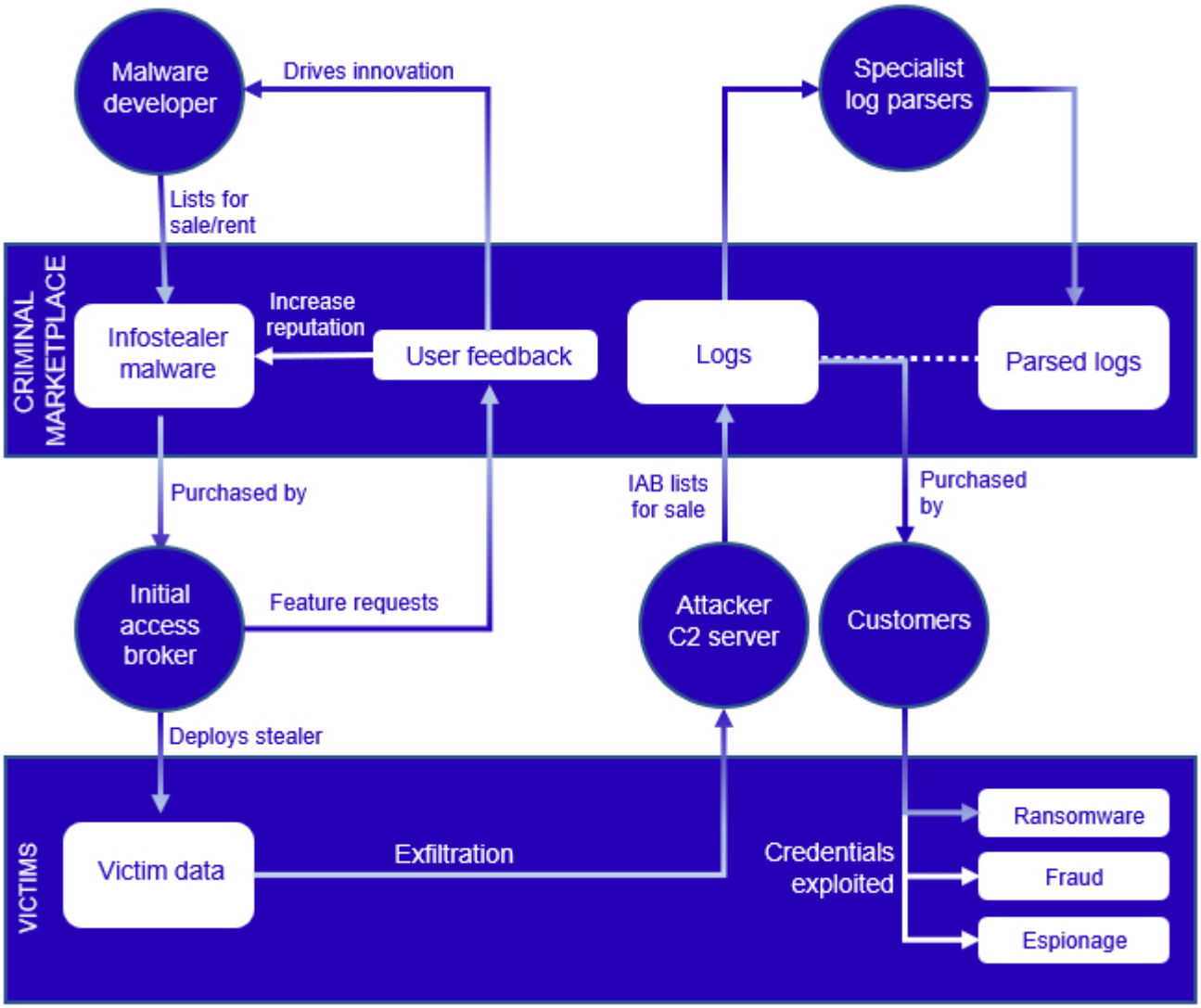


Reference: ANY.RUN

What is Information Stealer Malware?

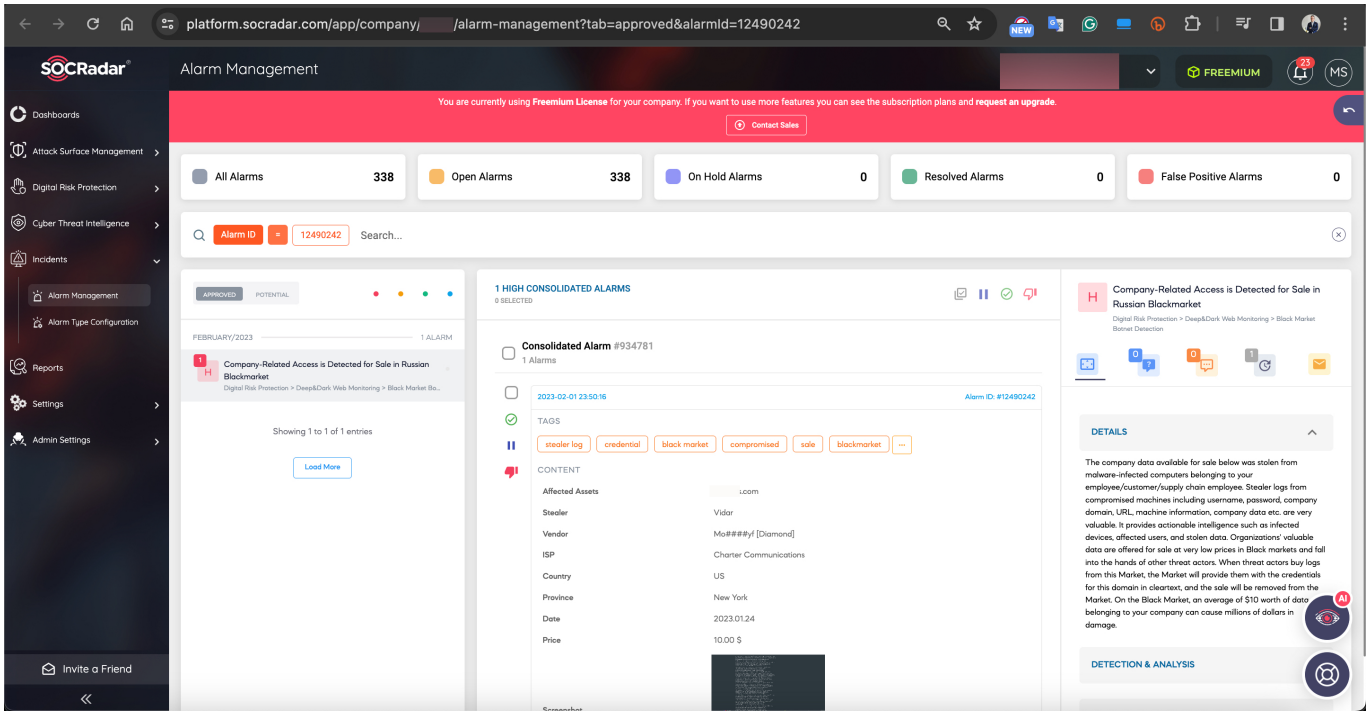
Information stealer malware is a type of software that steals personal and financial information, including usernames and passwords related to applications and systems such as VPN, RDP, and SSH. Subsequently, this stolen information is sent to the malware's developer. Often, these malicious programs are sold or leased by their developers as a malware-as-a-service (MaaS) model on a weekly or monthly basis to initial access brokers (IAB).

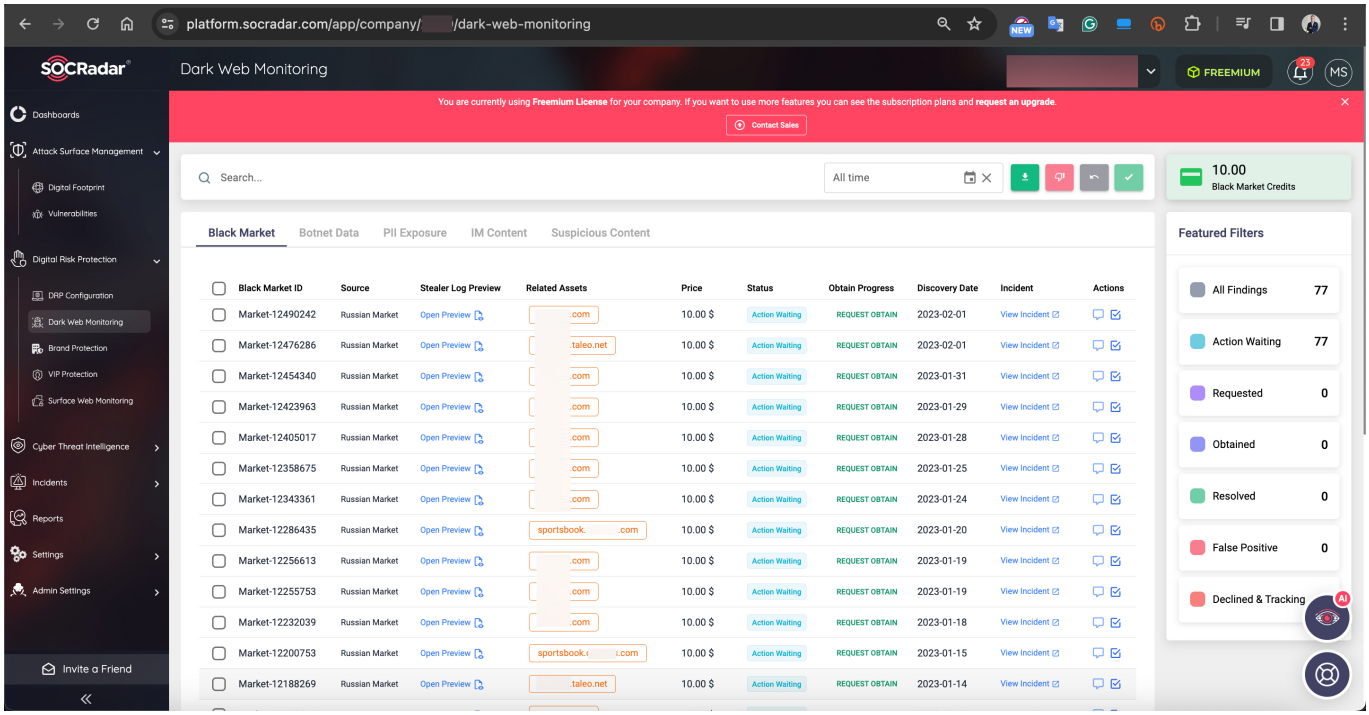
The information stolen by malware is later sold to threat actors, operators (customers), on underground forums, and Russian marketplaces (Russian Market) by initial access brokers (IAB), which are common meeting places for cybercriminals.

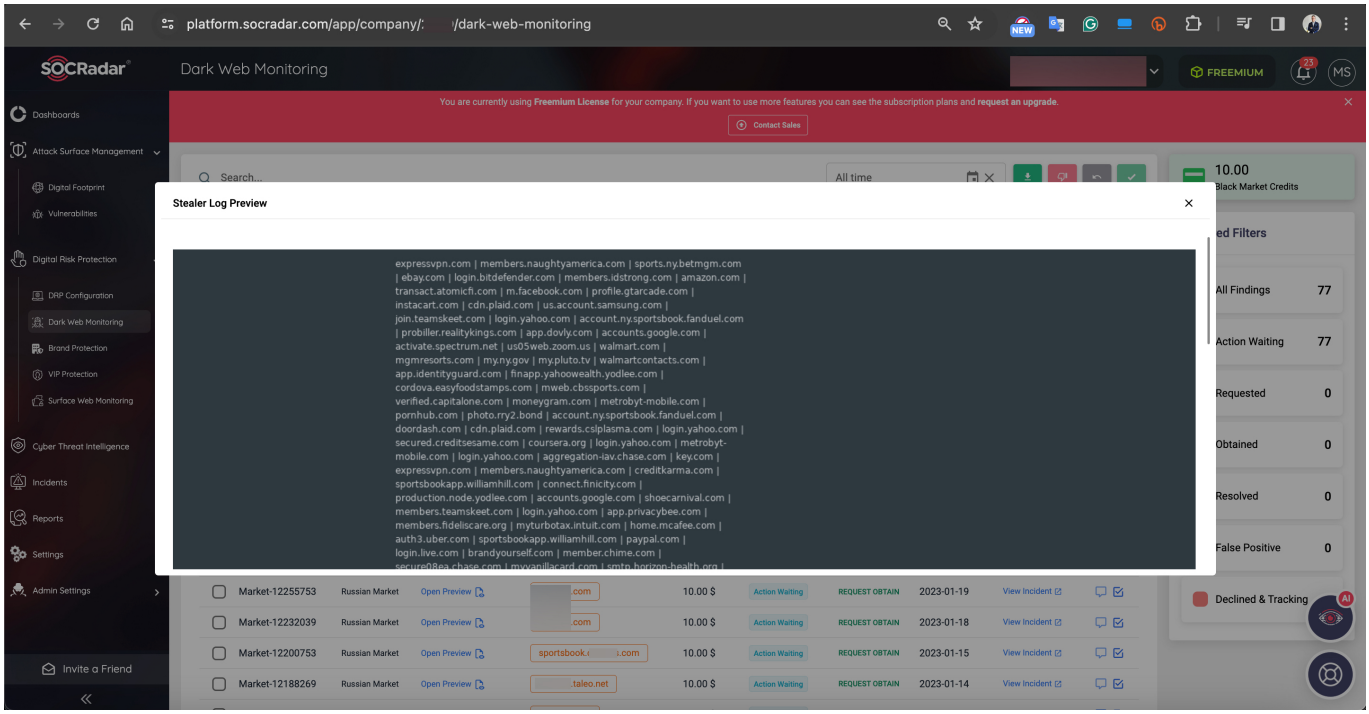


Reference: Secureworks

Particularly, cyber threat intelligence firms like SOCRadar closely monitor these places and warn their clients about the information offered for sale. Thanks to these alerts, enterprises can quickly identify and freeze the accounts of their employees, customers and suppliers, preventing the misuse of this information by cybercriminals. Otherwise, for example, a threat actor who plans to carry out a ransom attack on enterprise X can easily realize his evil ambitions with this access information purchased from the initial access broker for $10.


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



Reference: SOCRadar XTI

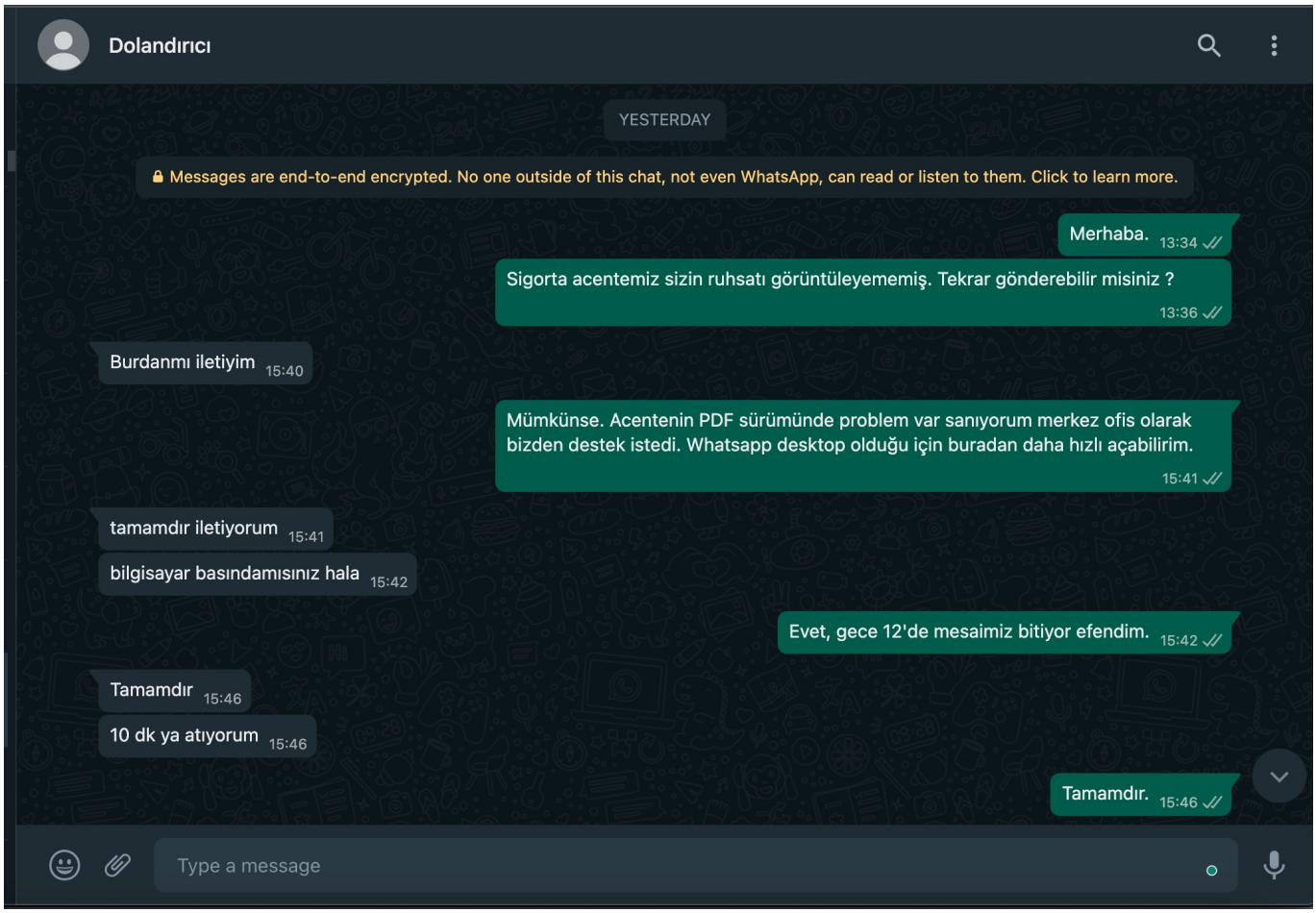
3-2-1 Action!

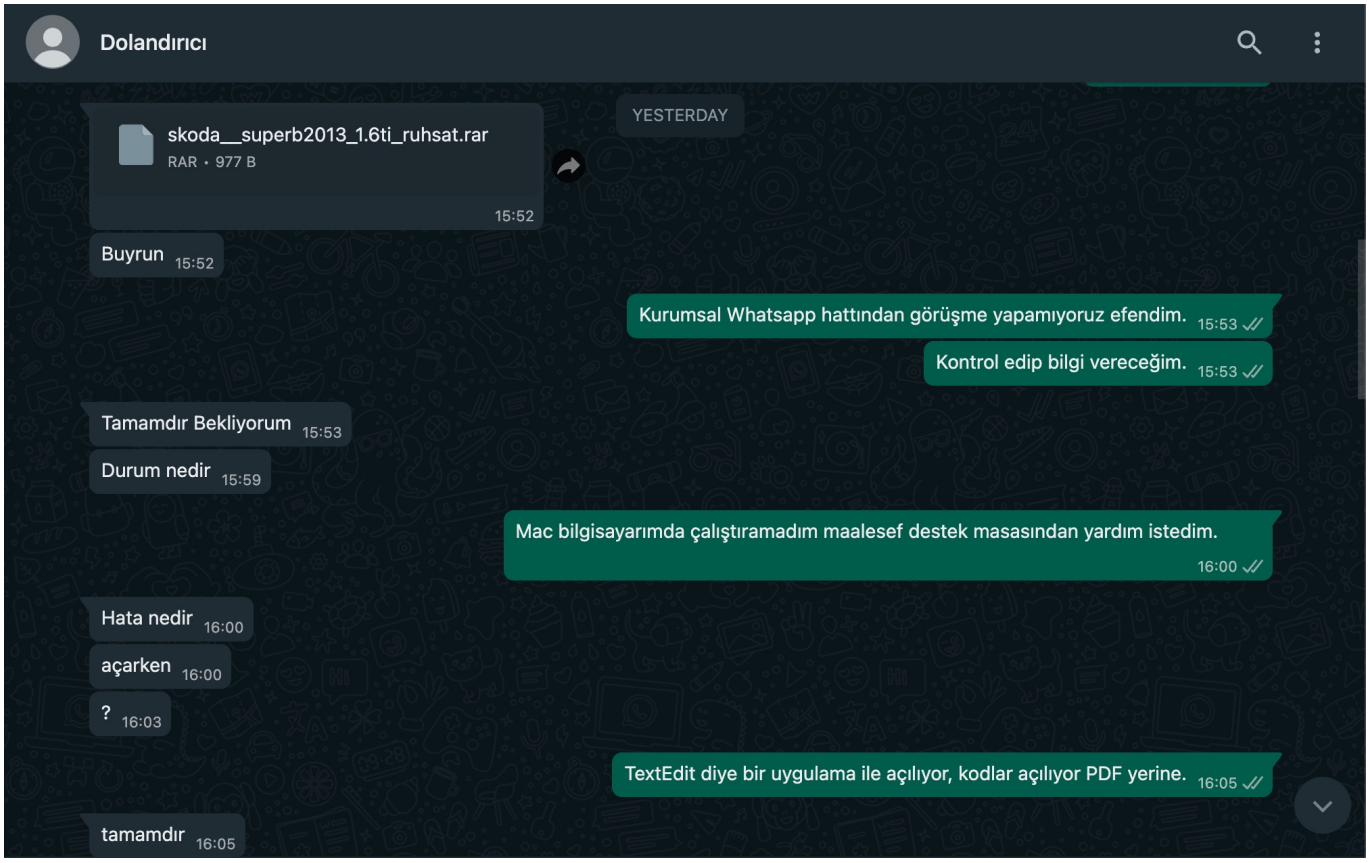
Our story begins on July 25, 2023, with a WhatsApp message from Bartu KILIÇ‘s relative. His relative, who is an insurance consultant, becomes suspicious when someone seeking to get car insurance sends a file (skoda__superb2013_1.6ti_ruhsat.rar) labeled as a registration through WhatsApp. Deciding to bring this matter to Bartu, who is a cybersecurity expert, the relative shares the details. Bartu, during a conversation about recent attempts of fraud, shares this story with me, sparking my interest. Subsequently, as I begin to investigate, events unfold around this intriguing topic.

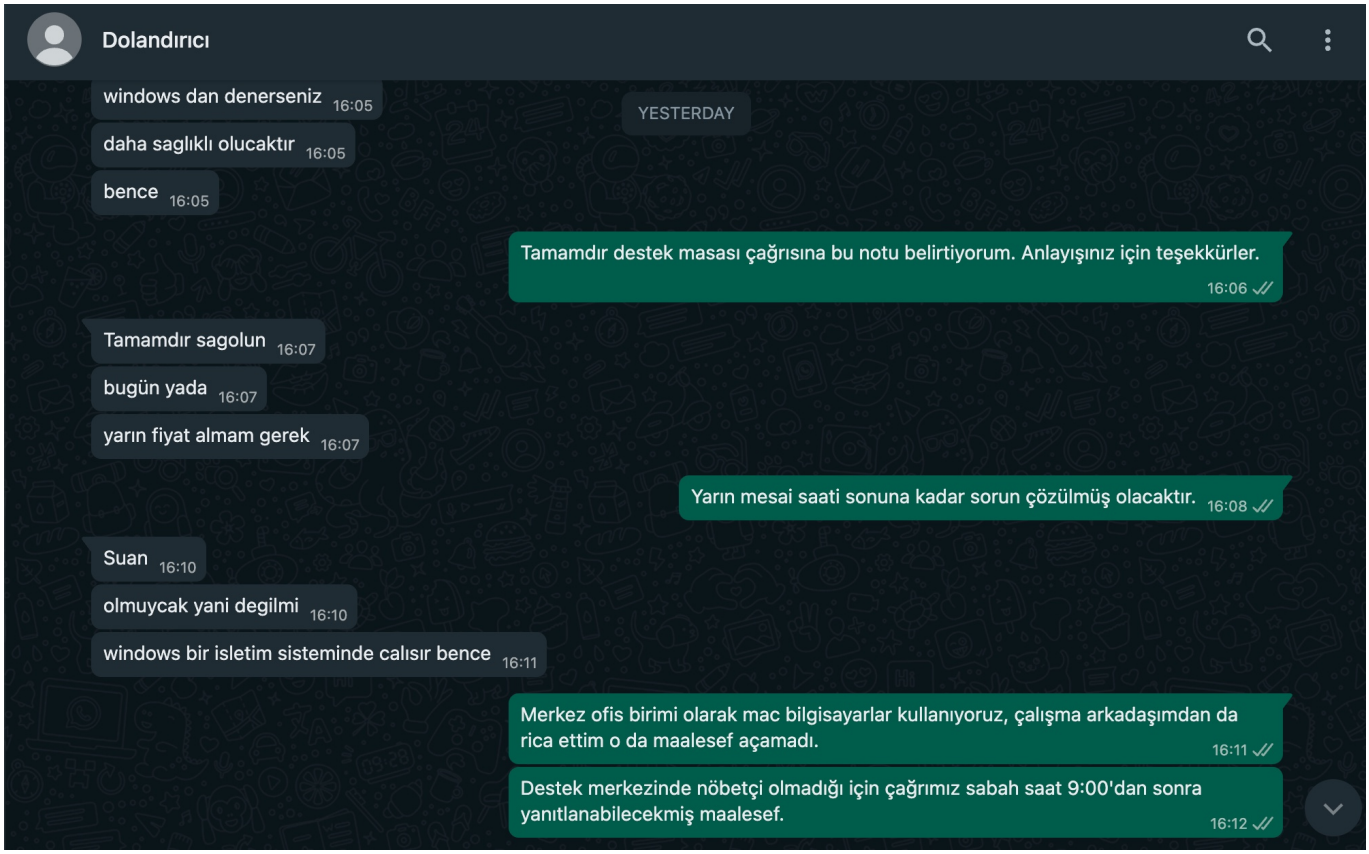
Our story begins with a WhatsApp message from Bartu KILIÇ‘s relative on July 25, 2023. His relative, who is an insurance consultant, is suspicious of a file (skoda__superb2013_1.6ti_ruhsat.rar) sent to him via WhatsApp under the name of a registration by a person who wants to get car insurance and decides to bring the issue to Bartu, a cyber security expert. Bartu shared this story with me while we were chatting about recent fraud attempts, and events unfolded as I started to investigate this topic, which intrigued me very much.

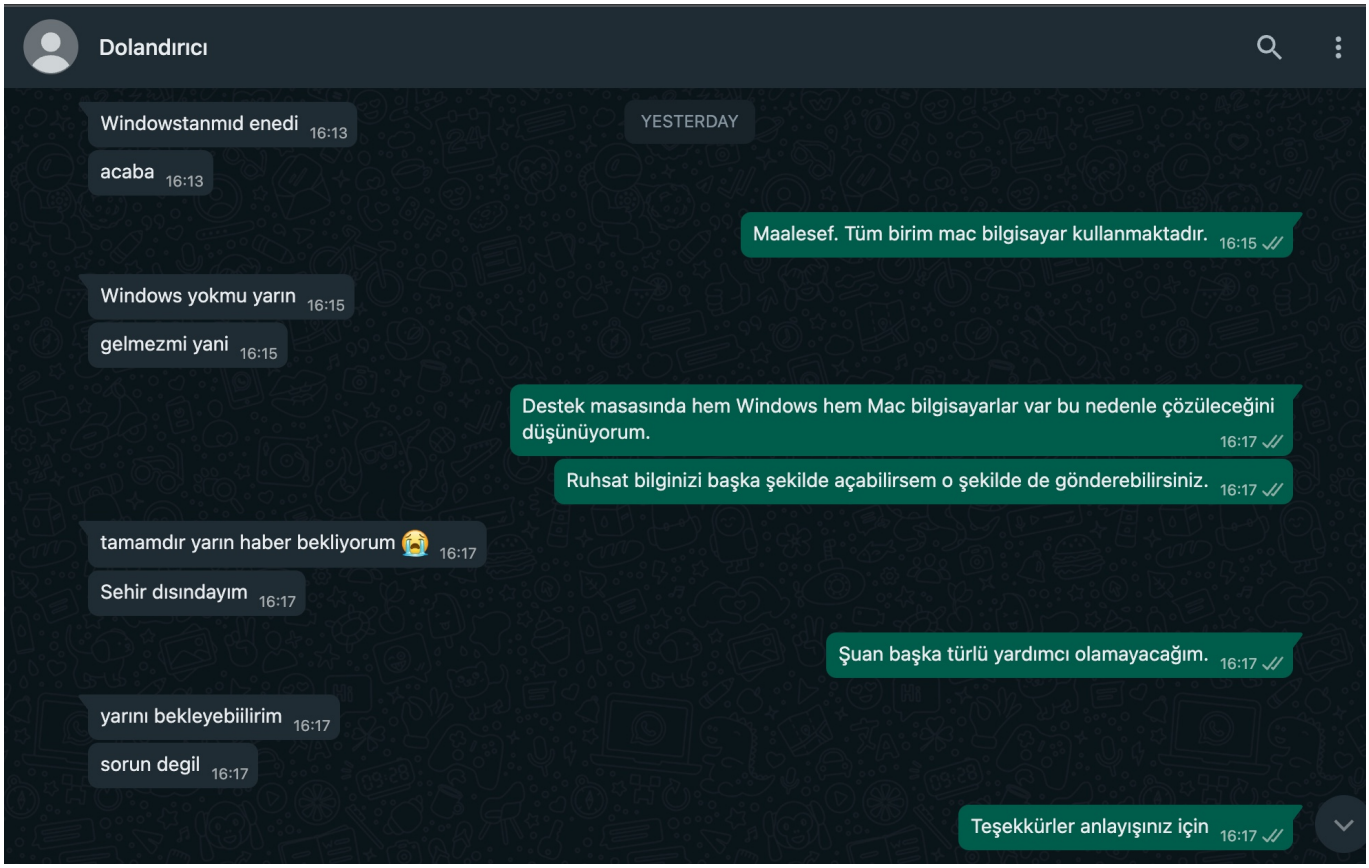
Some time after I asked Bartu to ask his relative to review the file, he shared that the file had been deleted and therefore he was unable to obtain it. Since I had the scammer’s mobile phone number (+90 545 466 89 52), I

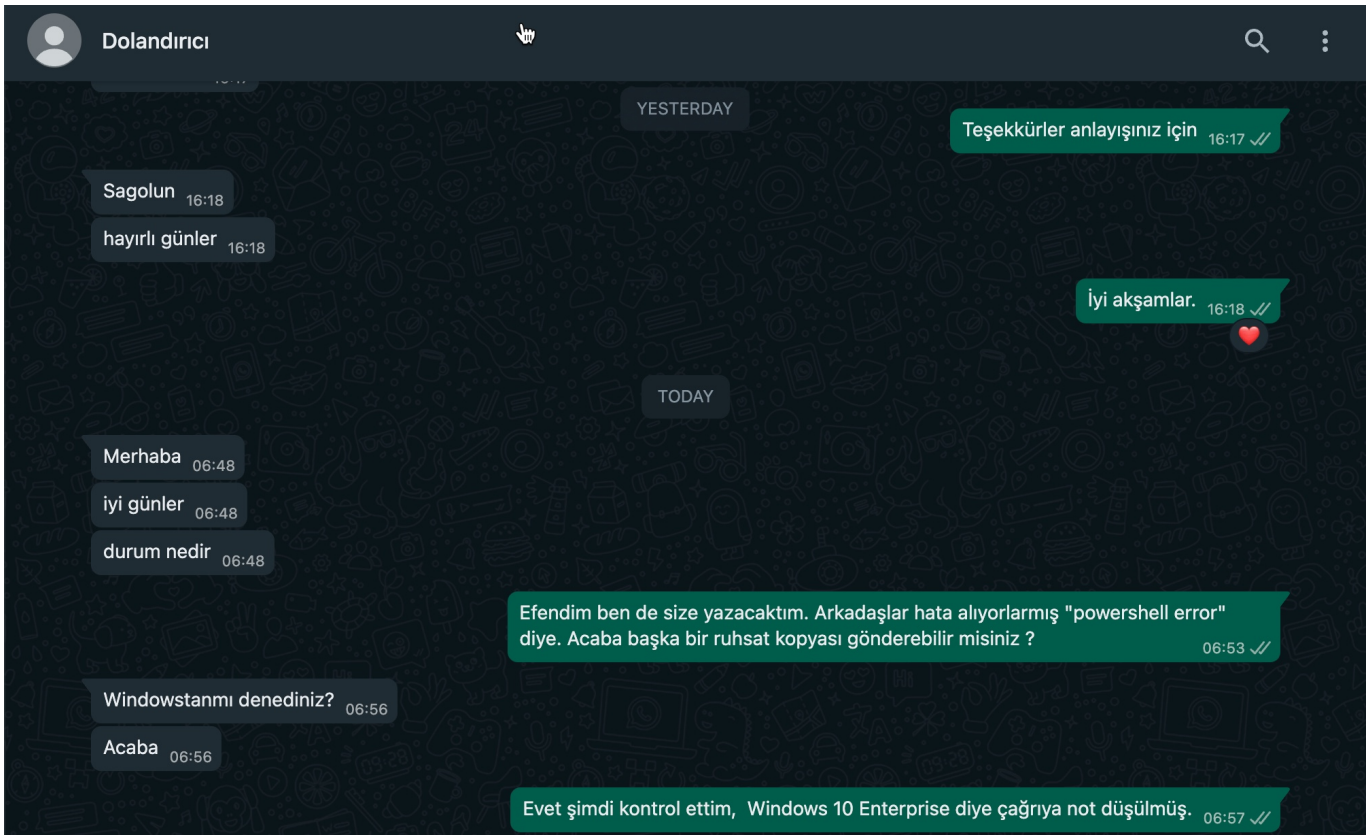
decided to contact the threat actor via WhatsApp. Introducing myself as an employee of the insurance company’s headquarters (not only scammers or threat actors impersonate trusted officials, customer service representatives :)), I started to correspond with the threat actor and soon I was able to obtain the suspicious file that is the subject of the story.




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





Time Period 7/25/23, 13:34 – 7/26/23, 06:57 | Translation in English

Mert: Hello.

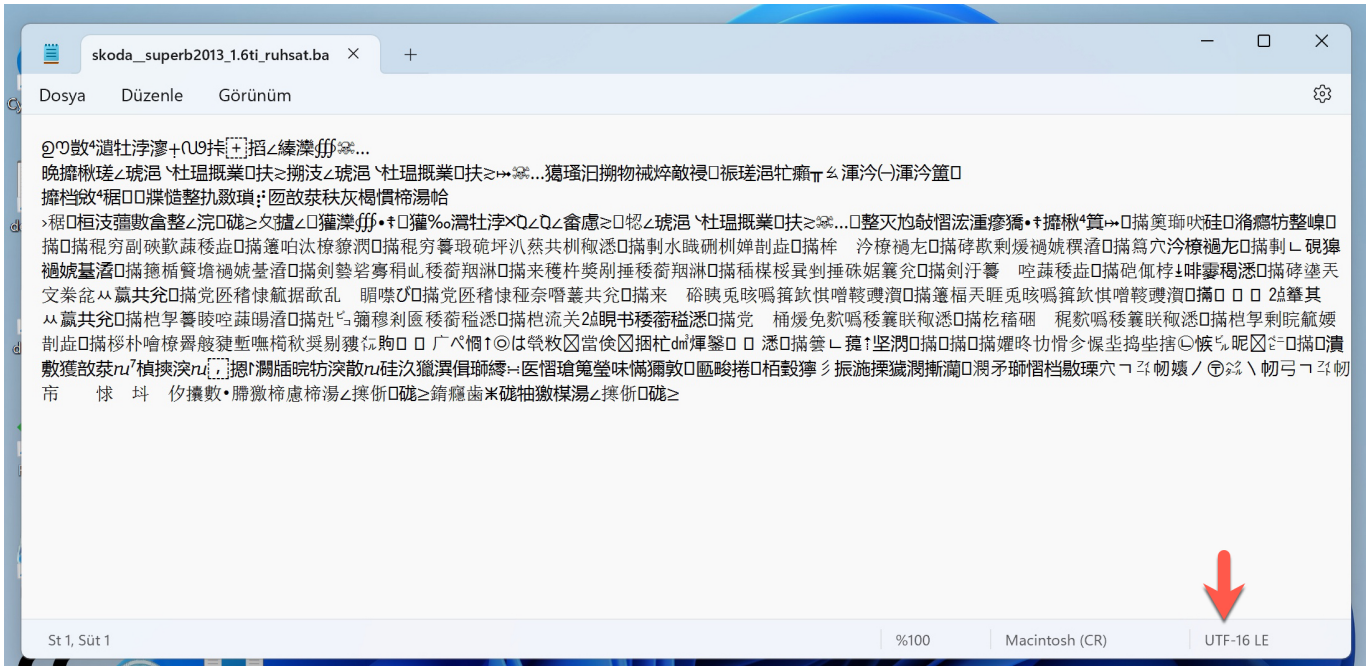
Mert: Our insurance agency couldn’t view your registration file. Could you

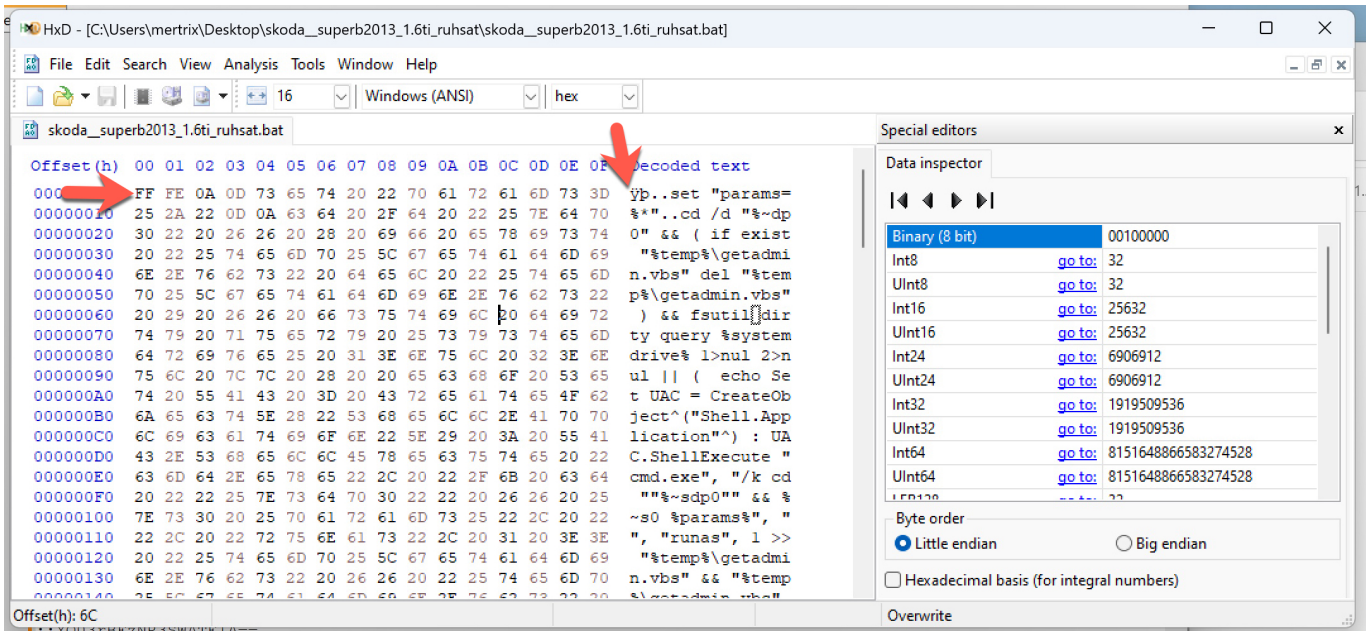
resend it, please?
Threat Actor: Shall I send it from here?
Mert: If possible. I think there’s an issue with the PDF version at the agency; they requested support from us at the headquarters. Since I’m on WhatsApp desktop, I can open it easily from here.
Threat Actor: Alright, I’ll send it.
Threat Actor: Are you still at the computer?
Mert: Yes, sir. Our working hours end at midnight.
Threat Actor: Okay.
Threat Actor: I’ll send it in 10 minutes.
Mert: Alright.
Threat Actor: skoda__superb2013_1.6ti_ruhsat.rar (file attached)
skoda__superb2013_1.6ti_ruhsat.rar
Threat Actor: Here you go.
Mert: Unfortunately, we cannot receive calls from the corporate WhatsApp line.
Mert: I will check and provide information.
Threat Actor: Alright, I’ll be waiting.
Threat Actor: What’s the status?
Mert: I couldn’t run it on my Mac; unfortunately, I asked for help from the support team.
Threat Actor: What’s the error when opening it?
Threat Actor: ?
Mert: It opens with an application called TextEdit; codes are displayed on the screen instead of a PDF.
Threat Actor: Alright.
Threat Actor: If you try on Windows, it will be more reliable, I think.
Mert: Alright, I’ll drop this note into the support team ticket. Thank you for your understanding.
Threat Actor: Alright, thank you.
Threat Actor: I need to get a quote today or tomorrow.
Mert: The issue will be resolved by the end of business hours tomorrow.
Threat Actor: I think it works on a Windows operating system.
Mert: As the headquarters team, we only use Mac computers. I also asked my colleague, but unfortunately, he couldn’t open it either.
Mert: Since there’s no one on duty at the support team, our ticket can only be answered after 9:00 in the morning.
Threat Actor: Did it work on Windows, by any chance?
Threat Actor: I wonder.

Mert: Unfortunately not. All teams use Mac computers.
Threat Actor: Is there anyway to run it on Windows tomorrow?
Mert: In the support team, there are both Windows and Mac computers, so I think it will be resolved.
Mert: If I can open your registraton file in another way, I'll send it that way.
Threat Actor: Alright, I'll wait for tomorrow
Threat Actor: I'm out of town.
Mert: At the moment, I can't help in any other way.
Threat Actor: I can wait for tomorrow.
Threat Actor: No problem.
Mert: Thank you for your understanding.
Threat Actor: Thank you.
Threat Actor: Have a good day.
Mert: Good evening.
Threat Actor: Hello.
Threat Actor: Good day.
Threat Actor: What's the status?
Mert: Sir, I was about to write to you as well. My colleagues are encountering an error, something about a "powershell error." Could you send another copy of the registration file?
Threat Actor: Have you tried it on Windows?
Threat Actor: Maybe.
Mert: Yes, I just checked, and it's noted as "Windows 10 Enterprise" in the ticket.

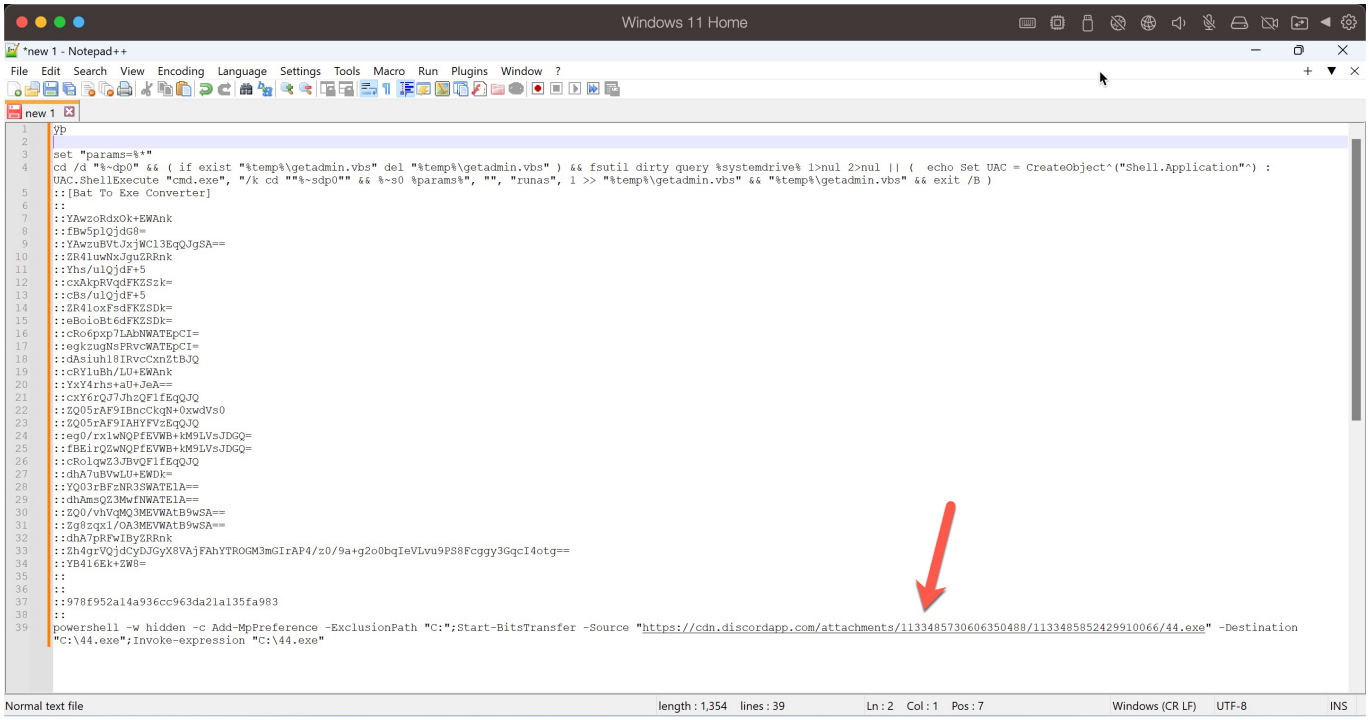
Static Suspicious File Analysis (44.exe)

After opening the "skoda__superb2013_1.6ti_ruhsat.rar" file on a virtual Windows 11 operating system, I immediately noticed the "skoda__superb2013_1.6ti_ruhsat.bat" file. When I opened the file with Notepad, a character string encoded in UTF-16 appeared. Upon examining the BAT file with the HxD hex editor, I observed that the threat actor utilized the byte-order mark (BOM) method to prevent the disclosure of commands with text editors.





When I examined the commands hidden behind this encoding, I observed that, when the BAT file is executed, it first utilizes PowerShell commands to add the C: directory to the exception list of Microsoft Defender, preventing the detection of this malicious software by Microsoft Defender. Subsequently, it downloads and executes a file named 44.exe from the instant messaging and VoIP social platform Discord.

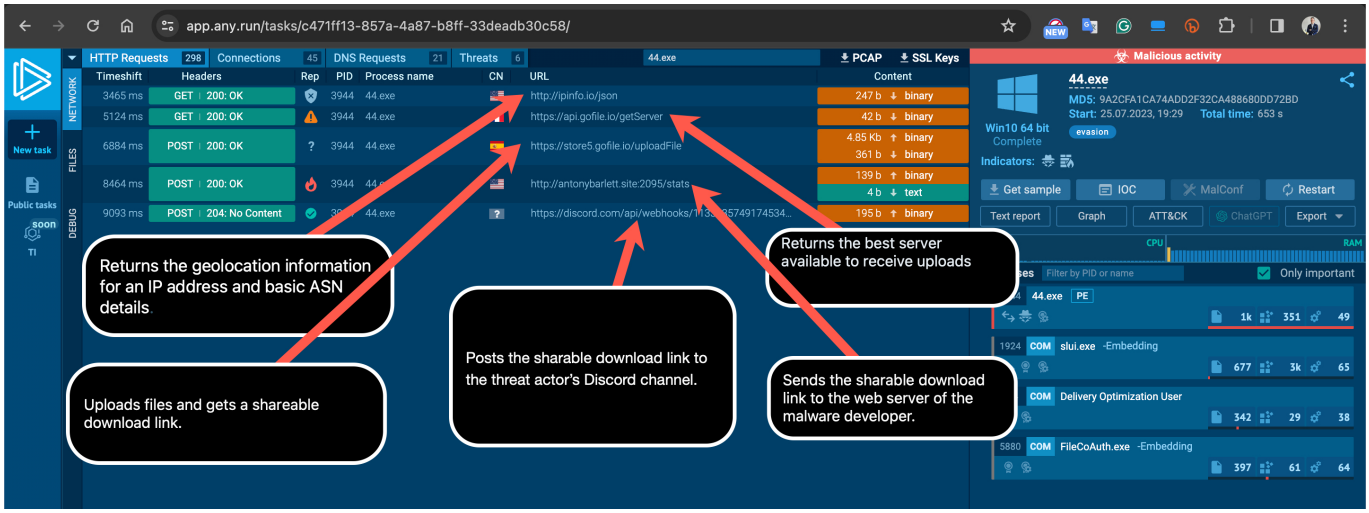


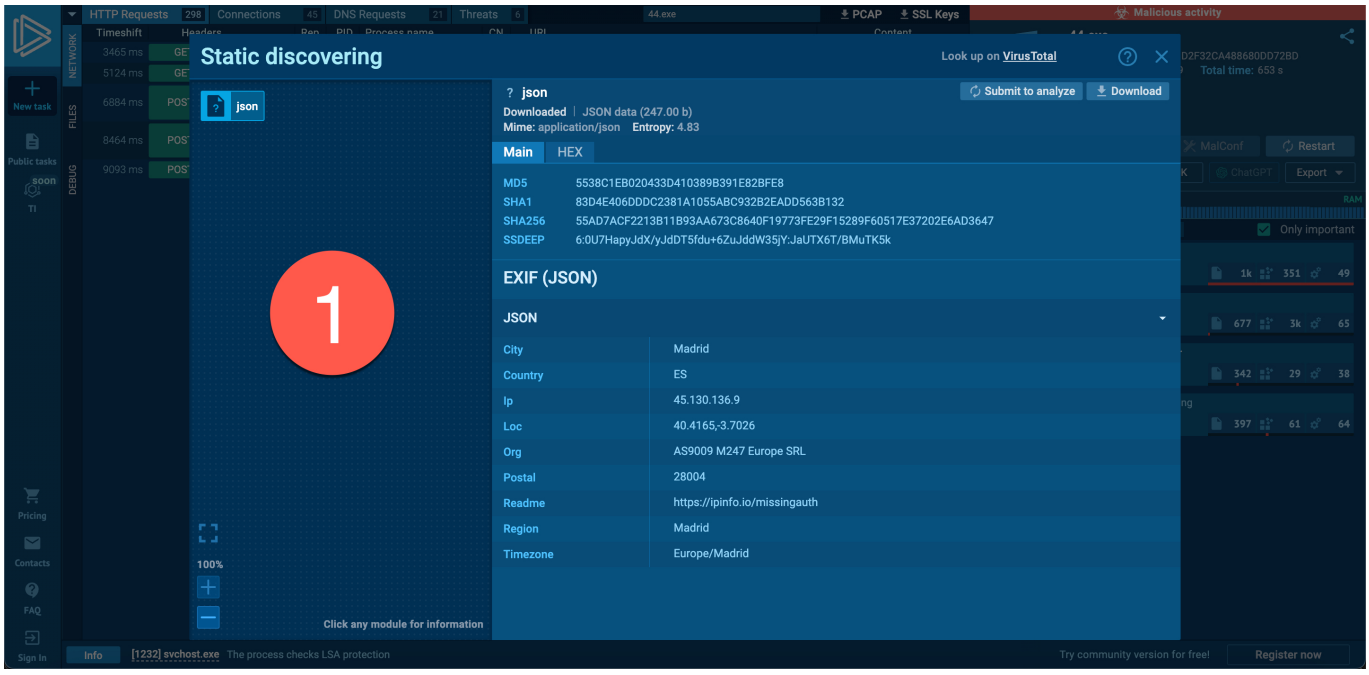
Dynamic Suspicious File Analysis (44.exe)

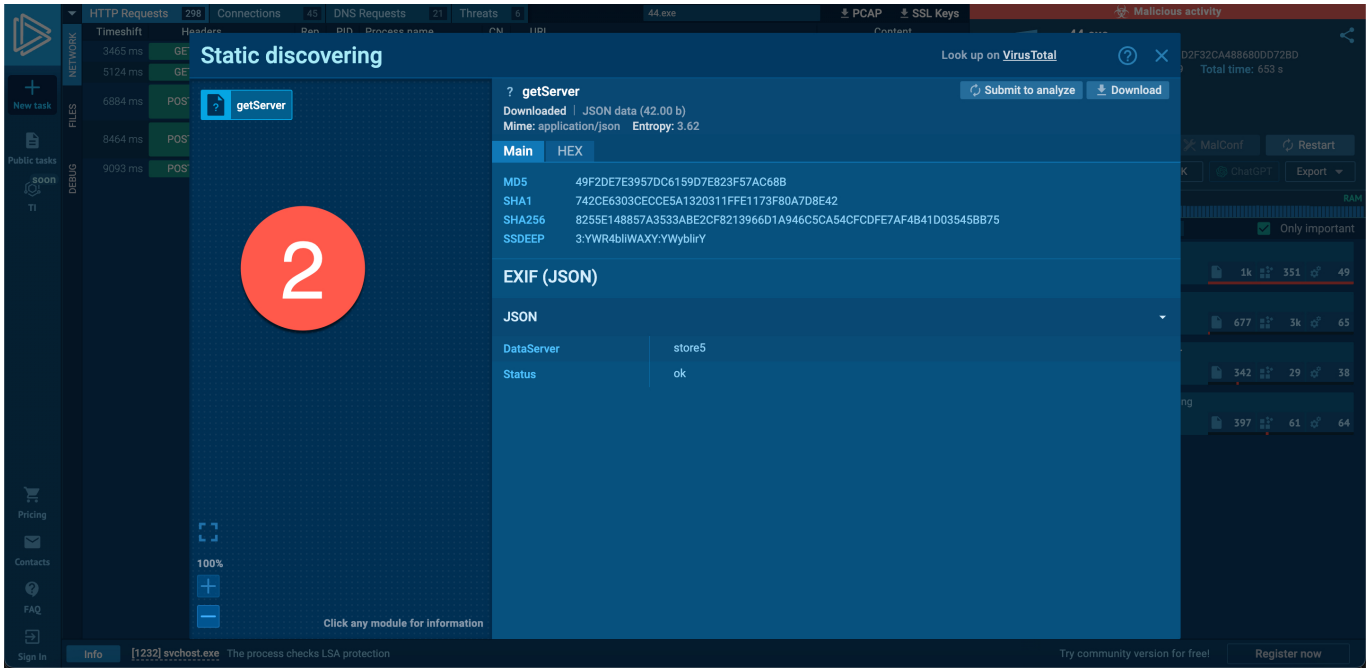
Up to this point, setting aside this BAT file, which has been clearly designed for highly suspicious operations, I decided to download the file named 44.exe, upload it to the interactive malware analysis platform called ANY.RUN, run it, and examine the logs.

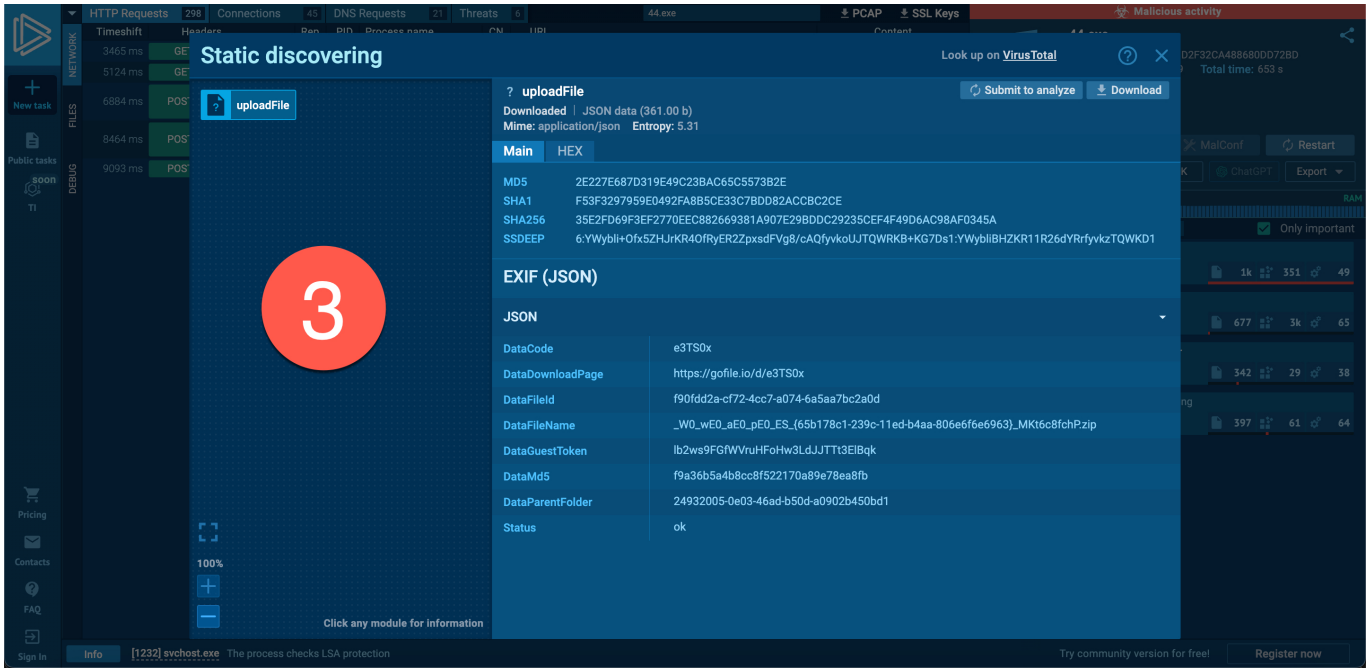
When I looked at the logs created on the operating system by the 44.exe process, the significant ones include:

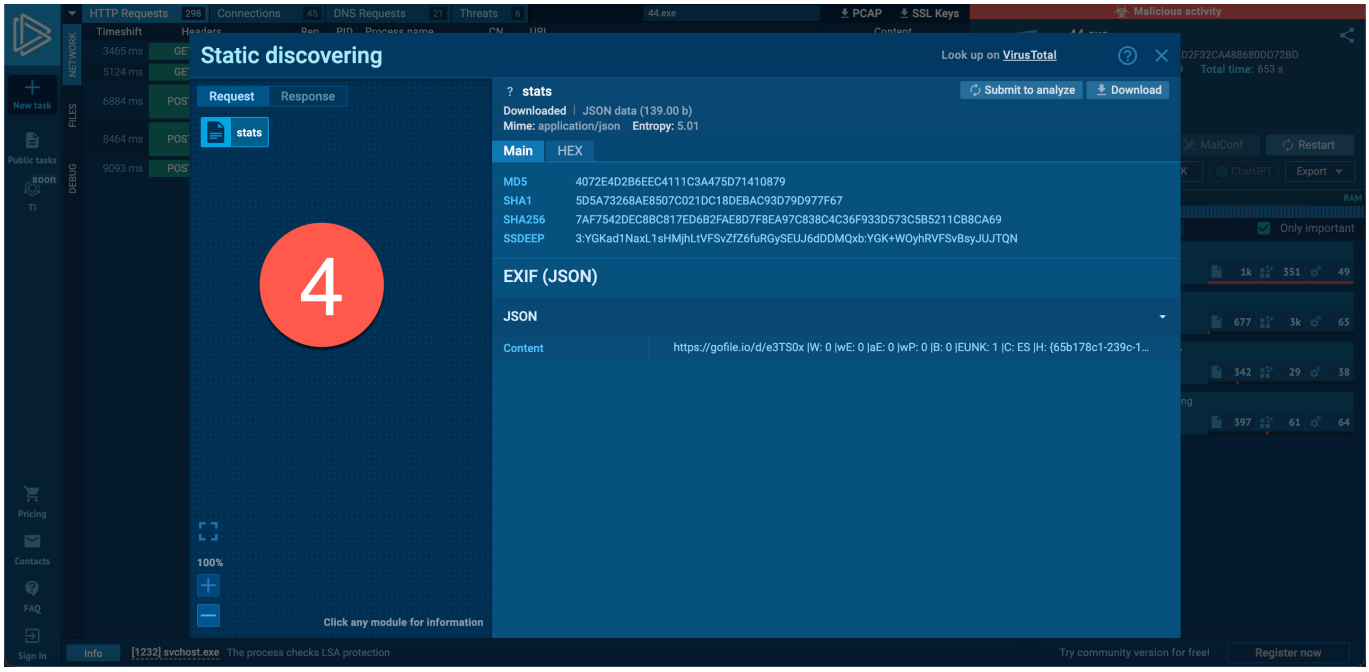
1. It was retrieving the geographical location information and basic ASN details of the IP address of the system it was executed through IPinfo.
2. It was obtaining the available Gofile server information to upload the stolen files from the operating system to the Gofile file-sharing platform.
3. The stolen files were uploaded to the Gofile platform, and it was obtaining the shareable download link.
4. The download link was being sent to the developer of the malware. (http://antonybarlett[.]site:2095/stats).
5. The download link address was being sent to the Discord channel of the threat actor through a Webhook.

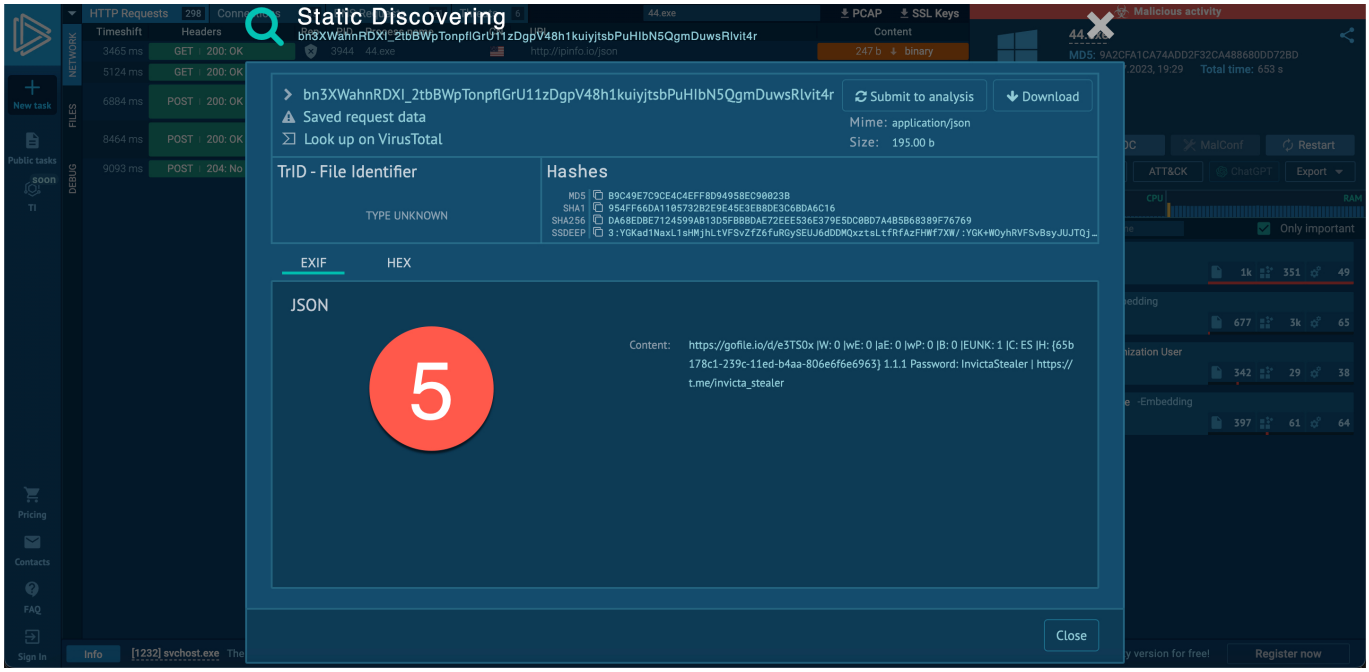

app.any.run/tasks/c471ff13-857a-4a87-b8ff-33deadb30c58/
HTTP Requests 298
Connections 45
DNS Requests 21
Threats 6
44.exe
PCAP
SSL Keys
Timeshift
Headers
Rep
PID
Process name
CN
URL
Content
3465 ms GET 200: OK 3944 44.exe http://ipinfo.io/json 247 b binary
5124 ms GET 200: OK 3944 44.exe https://api.gofile.io/getServer 42 b binary
6884 ms POST 200: OK 3944 44.exe https://store5.gofile.io/uploadFile 4.85 Kb binary 361 b binary
8464 ms POST 200: OK 3944 http://antonybarlett.site:2095/stats 139 b binary 4 b text
9093 ms POST 204: No Content 44.exe https://discord.com/api/webhooks/ 195 b binary
Malicious activity
44.exe
MD5: 9A2CFA1CA74ADD2F32CA488680DD72BD
Start: 25.07.2023, 19:29
Total time: 653 s
Win10 64 bit
Complete
evasion
Indicators:
Get sample
IOC
MalConf
Restart
Text report
Graph
ATT&CK
ChatGPT
Export
CPU
RAM
Filter by PID or name
Only important
Returns the geolocation information for an IP address and basic ASN details.
Uploads files and gets a shareable download link.
Posts the sharable download link to the threat actor's Discord channel.
Returns the best server available to receive uploads
Sends the sharable download link to the web server of the malware developer.


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
Info
[1232] svchost.exe The process checks LSA protection
Try community version for free!
Register now


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:YWybliriY
EXIF (JSON)
JSON
DataServer store5
Status ok
2
100%
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 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



When examining the fifth entry, I noticed the InvictaStealer tag in the HTTP request and the Telegram address https://t.me/invicta_stealer. Upon visiting the Telegram channel, it became clear that this software is an information-stealing malware (infostealer) of Russian origin, developed in the C++ programming language. The builder for this malware was freely available on the GitHub storage platform.

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

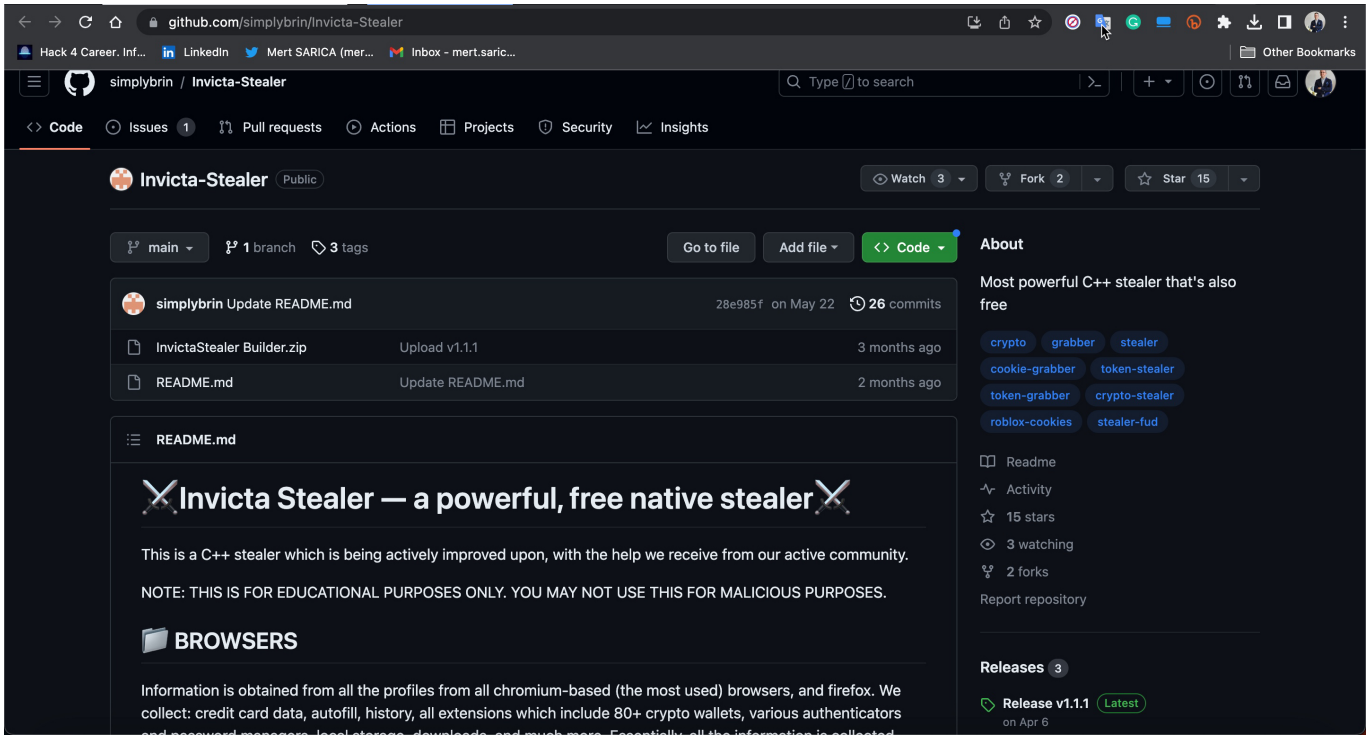
https://github.com/simplybrin/Invicta-Stealer

❤️ 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

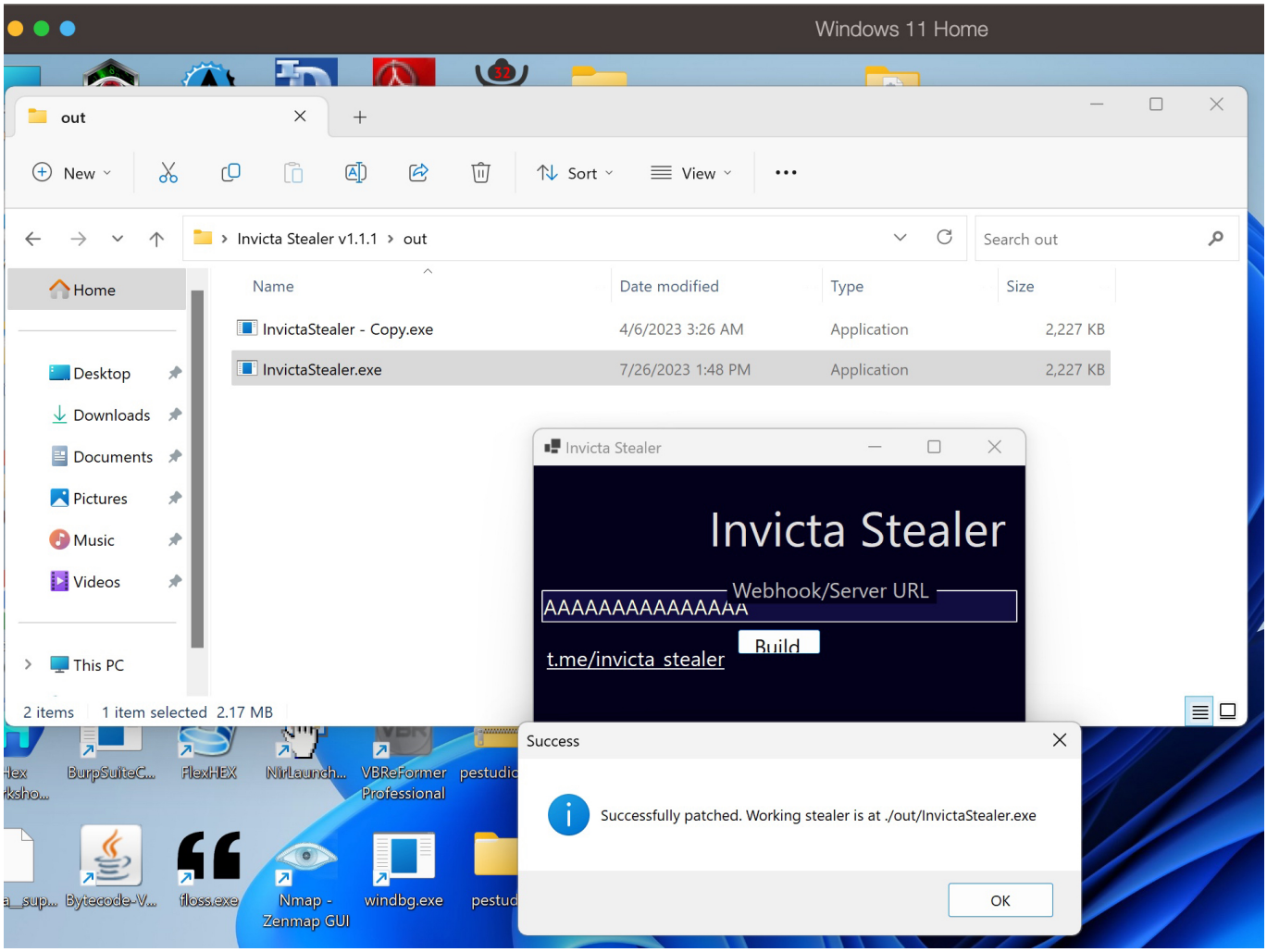
❤️ 4 523 13:18



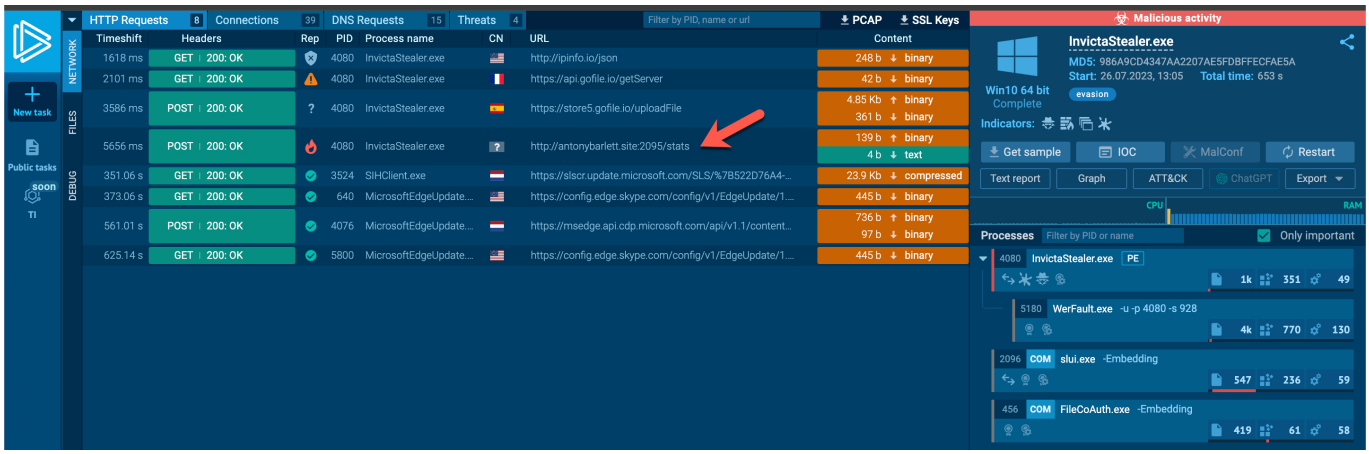
Invicta Stealer’s promotional video on its YouTube channel

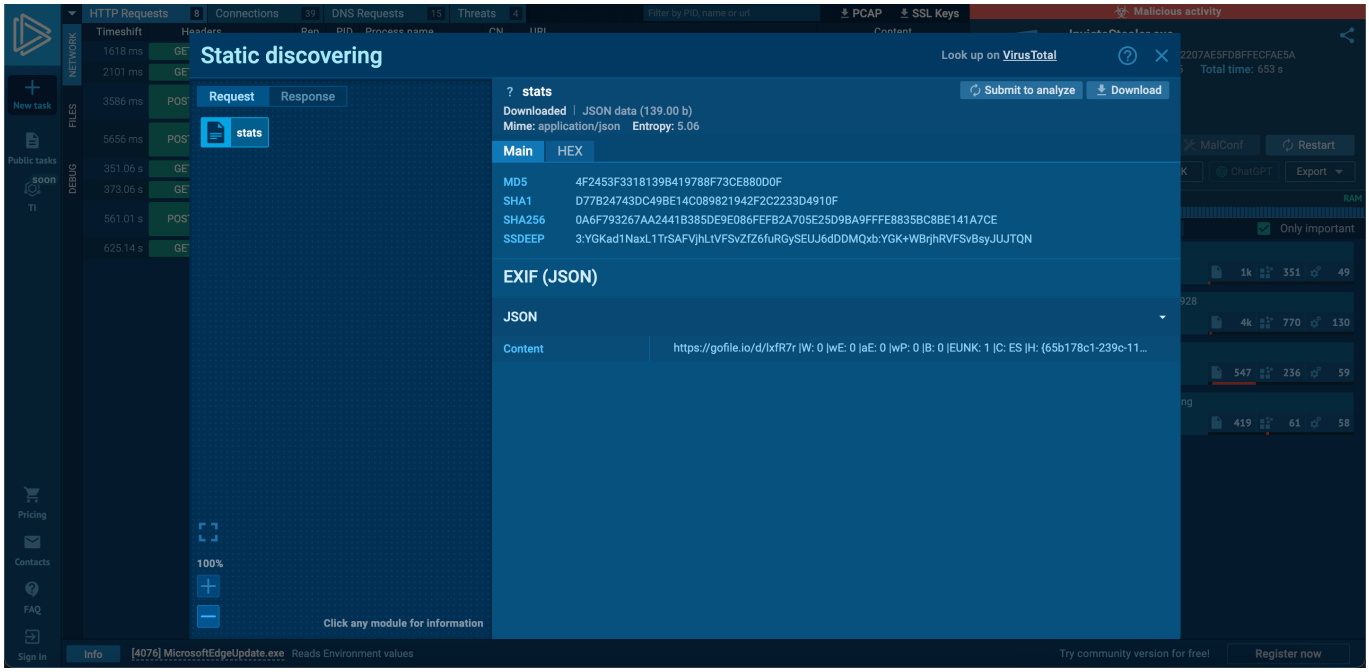
Dynamic Malicious File Analysis (Builder.exe)

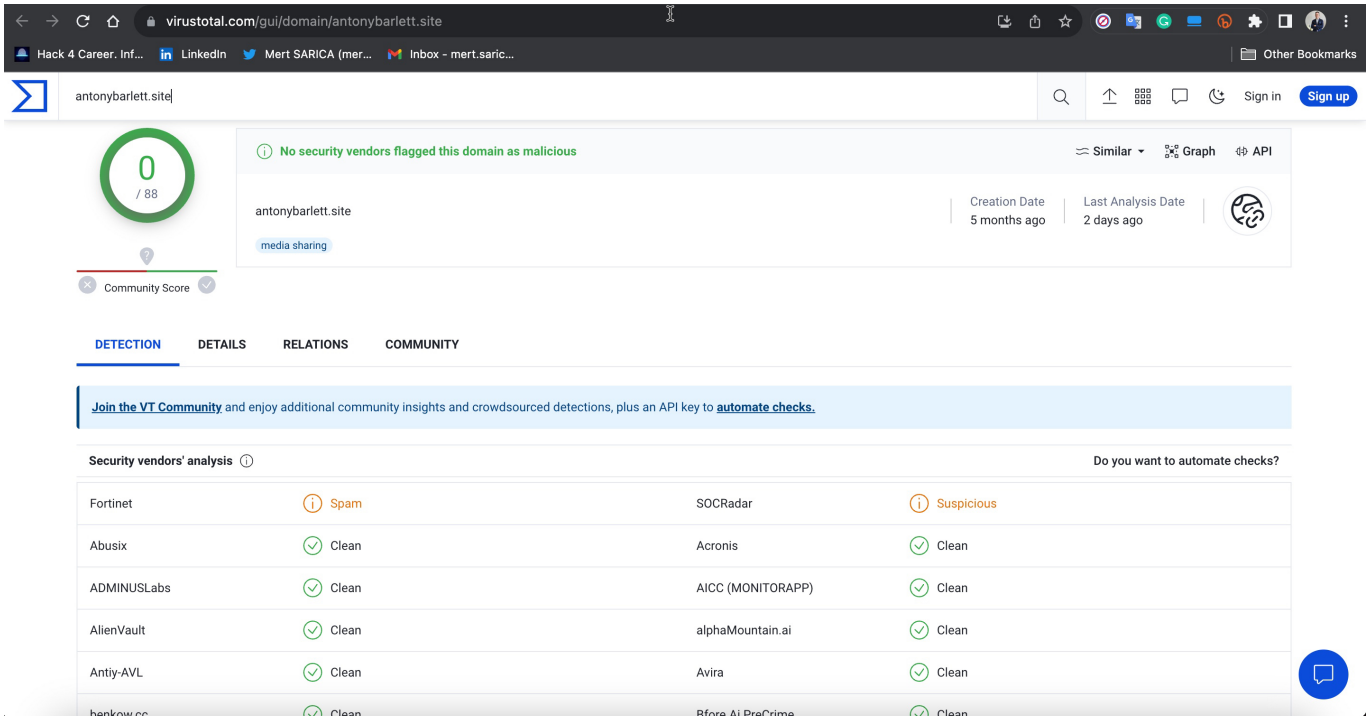
I downloaded the InvictaStealer Builder.zip file from the GitHub repository belonging to the malware developer and began examining it by running it on my virtual system. When the application is opened, it prompts the user to enter a Discord Webhook or a URL, and upon pressing the Build button, it builds the malicious software. For testing purposes, I entered AAAAAA… in the Webhook/Server URL section and successfully created the malicious software.



When I uploaded the malicious software to ANY.RUN to discover similarities with 44.exe, I noticed a commonality in both pieces of software, which is the web address http://antonybarlett[.]site:2095/stats. When I searched this address on the VirusTotal malicious software analysis platform, I found that it was flagged as suspicious by only SOCRadar and marked as unwanted (spam) by Fortinet among security vendors.



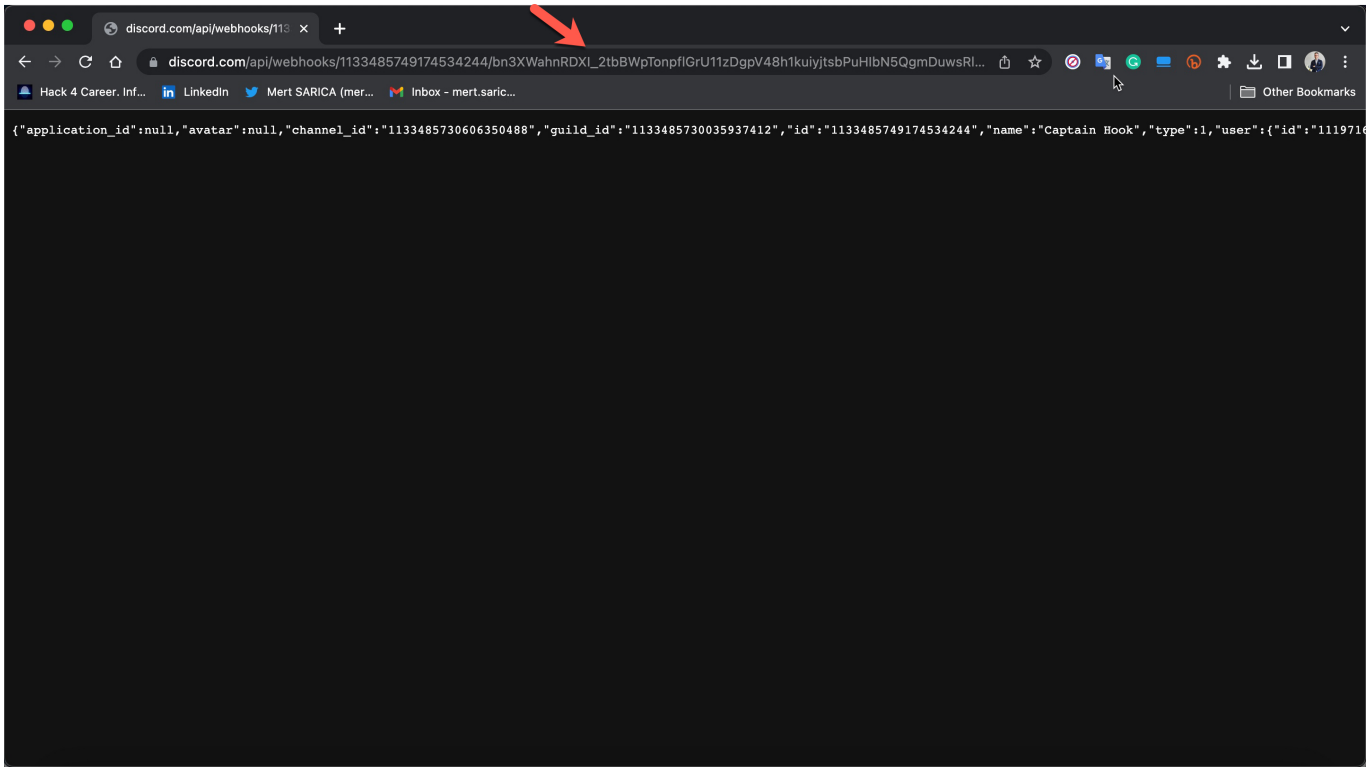


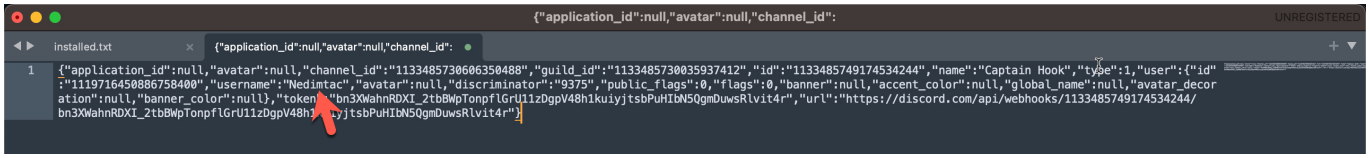


This web address is common to two different malware samples, which I'm sure doesn't surprise me and the readers of my article "Was Turkey's e-Government Hacked?" because in that article we saw that threat actors often embed backdoors in the files they share. In this malware, the developers didn't neglect to ensure they also receive the addresses of files stolen and uploaded to the Gofile file-sharing platform. :)

Threat Actor Targeting the Insurance Consultant – Who is it?

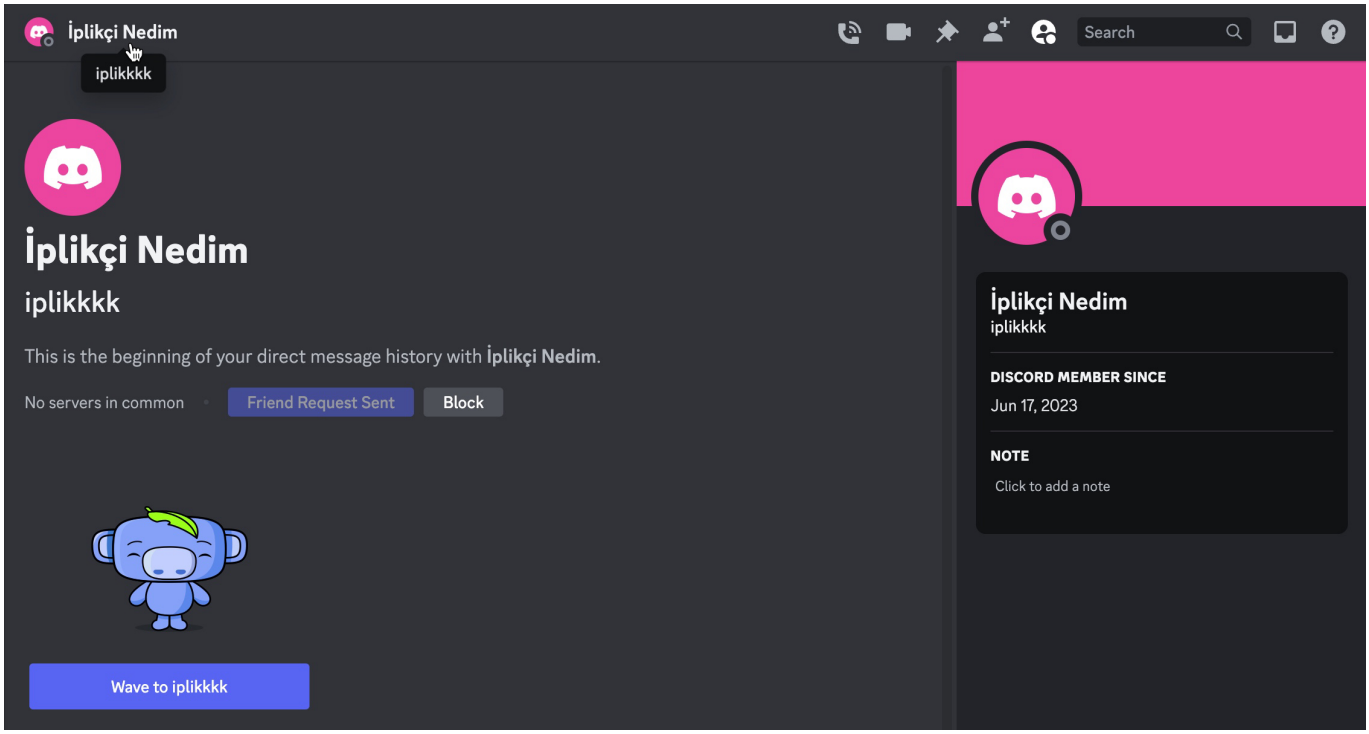
After obtaining this information, it was time to find answers to the crucial questions that had been lingering in my mind. Who was the threat actor that downloaded and created this malicious software from the GitHub repository, targeting the insurance consultant? To answer this, I decided to leverage the Discord Webhook address embedded in the malicious software. When I visited this address, the Discord API revealed that the user who created this Webhook, with the username Nedimtac, joined Discord on June 17, 2023. The individual displayed as “İplikçi Nedim” in the display name.

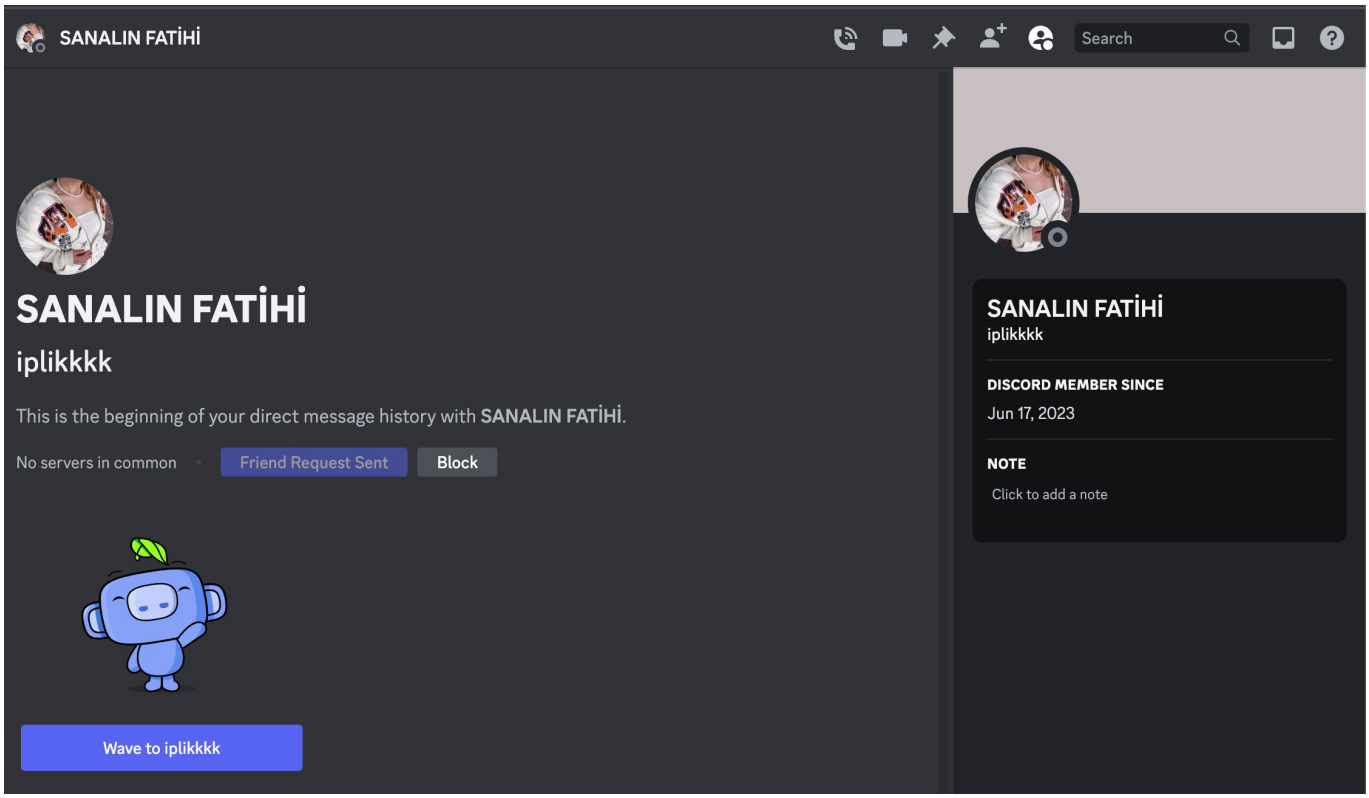


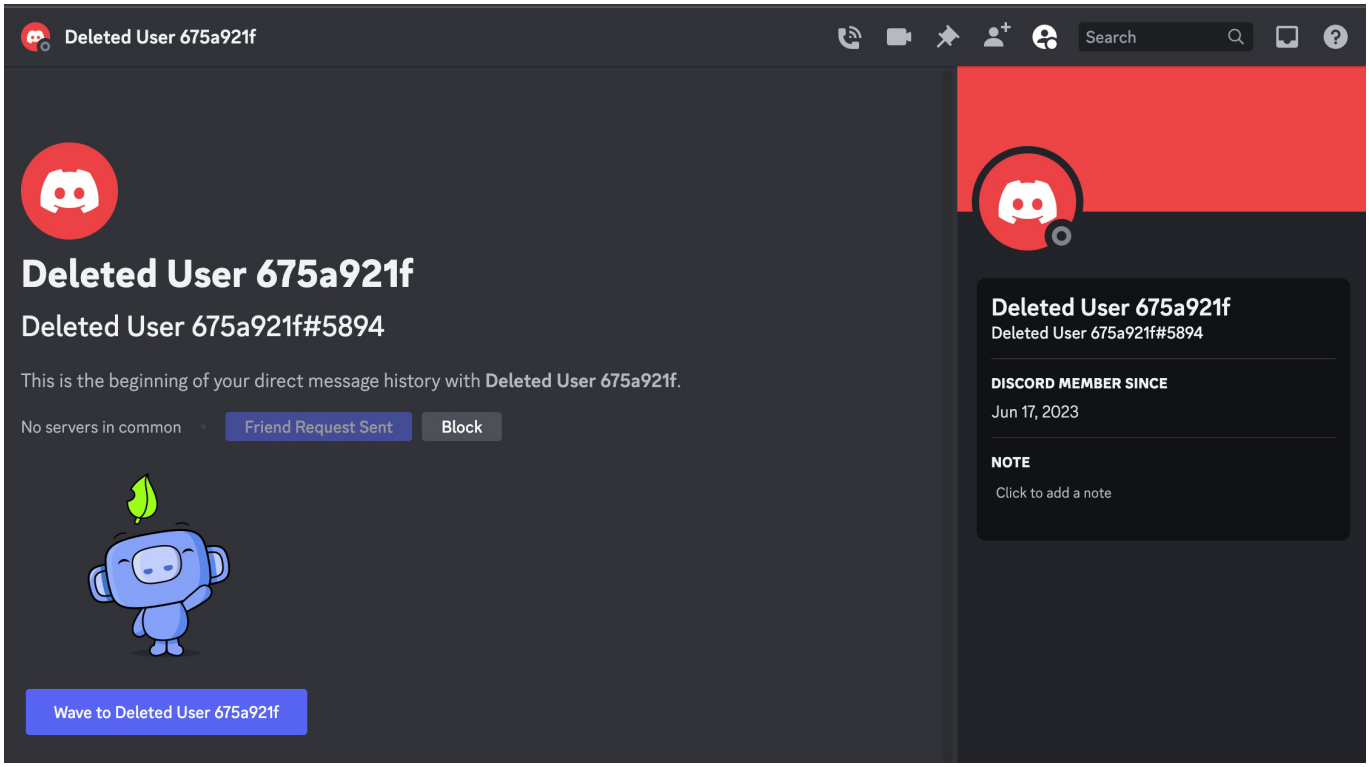


The username of this person was “iplikkkk” in July 2023, and after changing the display name to “SANALIN FATİHİ” in August, the account was completely deleted in September. Although I tried to contact this person, unfortunately, I couldn’t have the chance to chat with him as he did not accept my invitation.


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

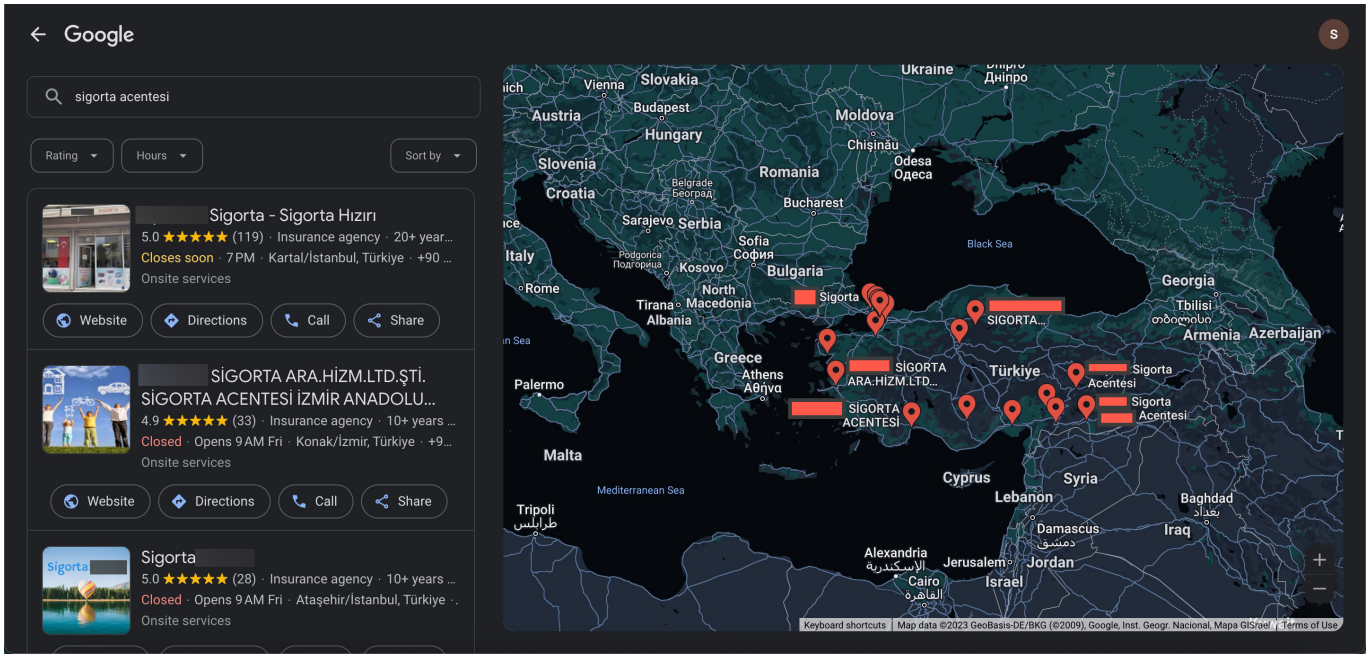


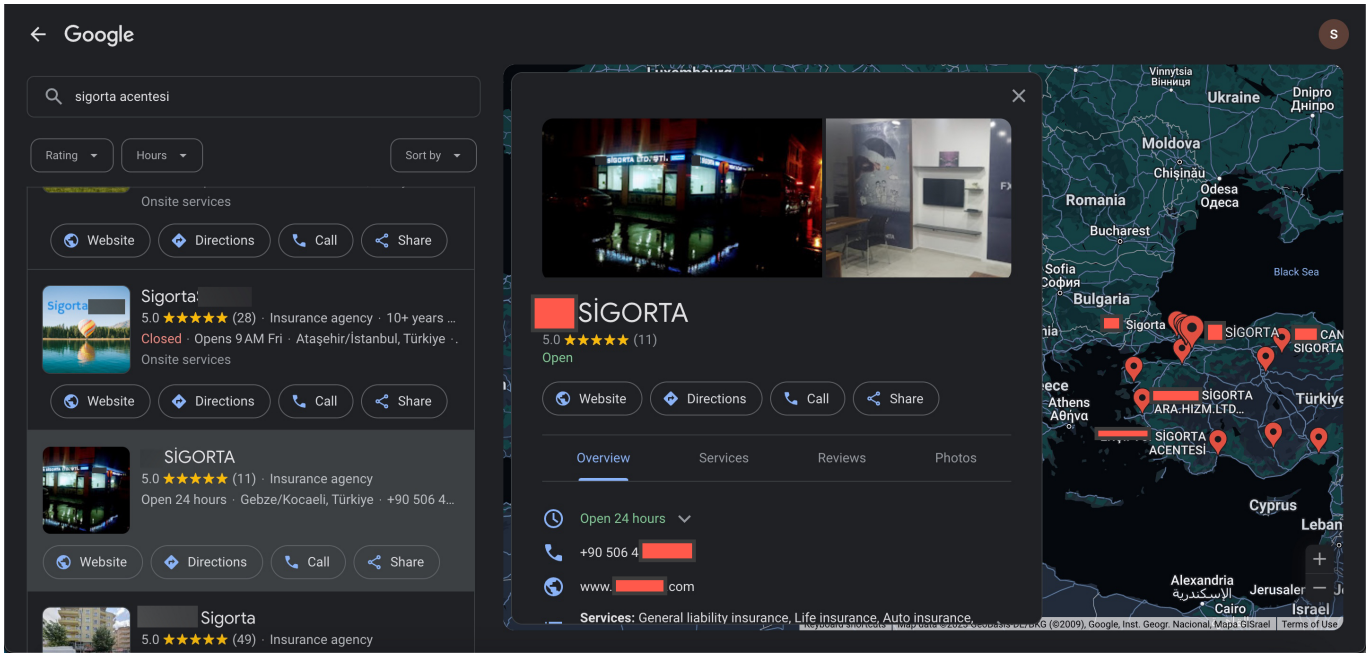
Why Might an Insurance Consultant/Agency Be Targeted?

It was time to find an answer to another question. How could the threat actor have found and obtained the mobile phone number of the insurance consultant? In recent years, with a wealth of information circulating in the hands of cyber criminals, it might not be too difficult to guess who has access to our mobile phone information. However, I decided to delve a bit more into this particular issue.

When it comes to the insurance consultant, just like real estate agents, their mobile phone information should be easily findable and reachable on the internet, in publicly accessible places. If this threat actor is targeting insurance agents, then one would assume their first stop could be the Google search engine. Could they easily obtain this information from there?”

For this, when I searched with the keyword “insurance agency” on the Google search engine, I observed that there were numerous insurance agencies sharing their mobile phone information. Seeing that threat actors targeting insurance consultants and agencies could potentially exploit systems they hacked using this method and, through those systems, gain access to the internal systems of insurance companies, it was more than enough to deeply concern me.





Conclusion

When I thought about why insurance consultants and agencies are targeted by threat actors with information-stealing malware, I thought of the high potential of converting this information into query panels and/or selling it to fraudsters or threat actors, as in my article “Was Turkey’s e-Government Hacked?“. Whether this possibility is low or high, the undeniable truth of today is that threat actors target our personal data and the organizations that have access.

In conclusion, regardless of the likelihood, it is crucial for everyone to think twice before clicking on links or opening files from unknown sources.

Hope to see you in the following articles.