Byakugan 2025:

highly evasive malware targets the financial and crypto sectors

AXUR

In 2025, researchers from the Axur Research Team (ART) identified a new phishing campaign delivering a highly evasive variant of the Byakugan malware. This version of the trojan exhibits a low detection rate by antivirus solutions, making it a significant threat to companies across all sectors.

The operators behind this campaign leverage advanced phishing and social engineering techniques, using compromised infrastructure to mimic legitimate supplier communications. This approach deceives victims and leads them to execute malicious files. Furthermore, evidence suggests the adversary is employing obfuscation and anti-analysis mechanisms, making the malware harder to detect and reverse-engineer.

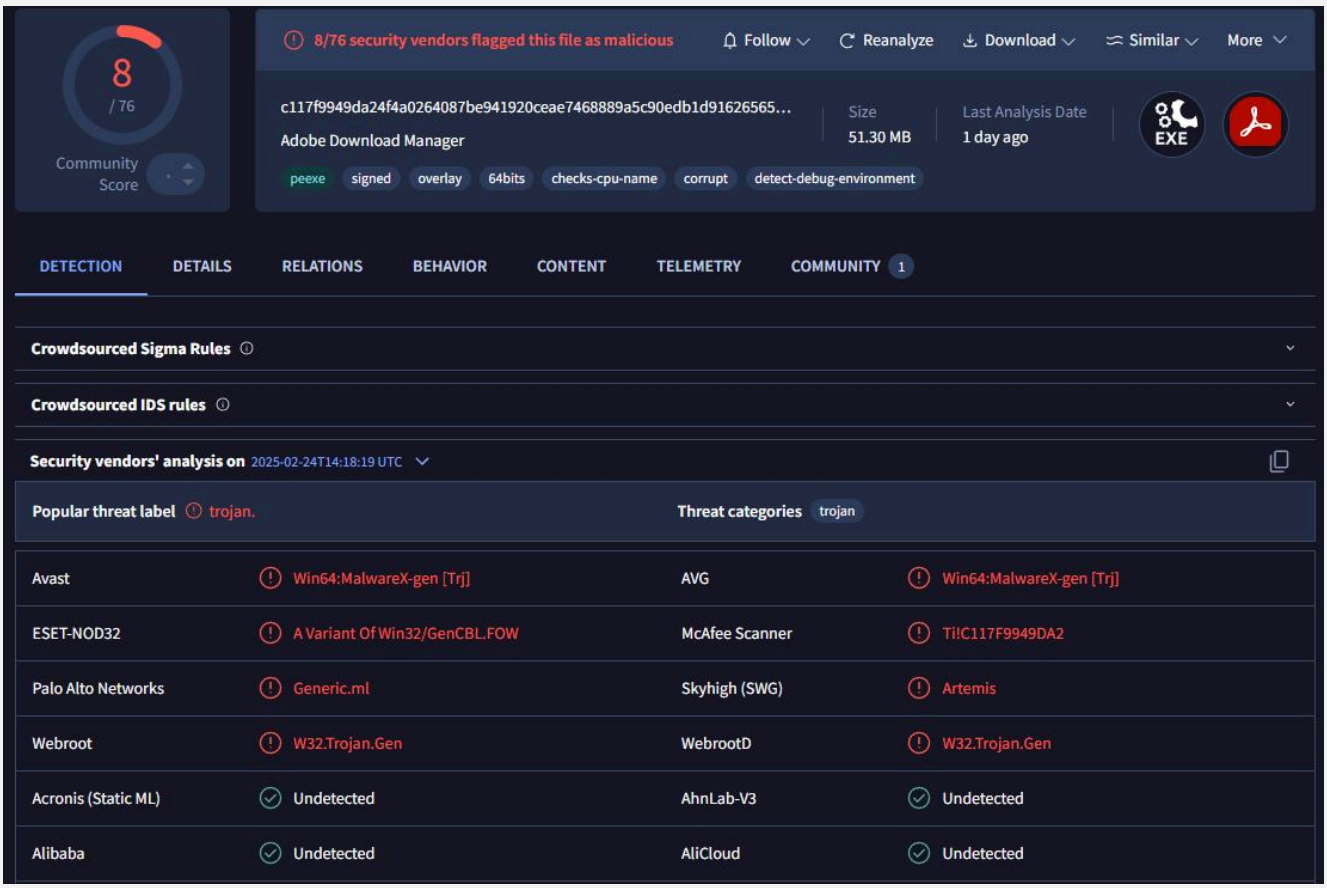
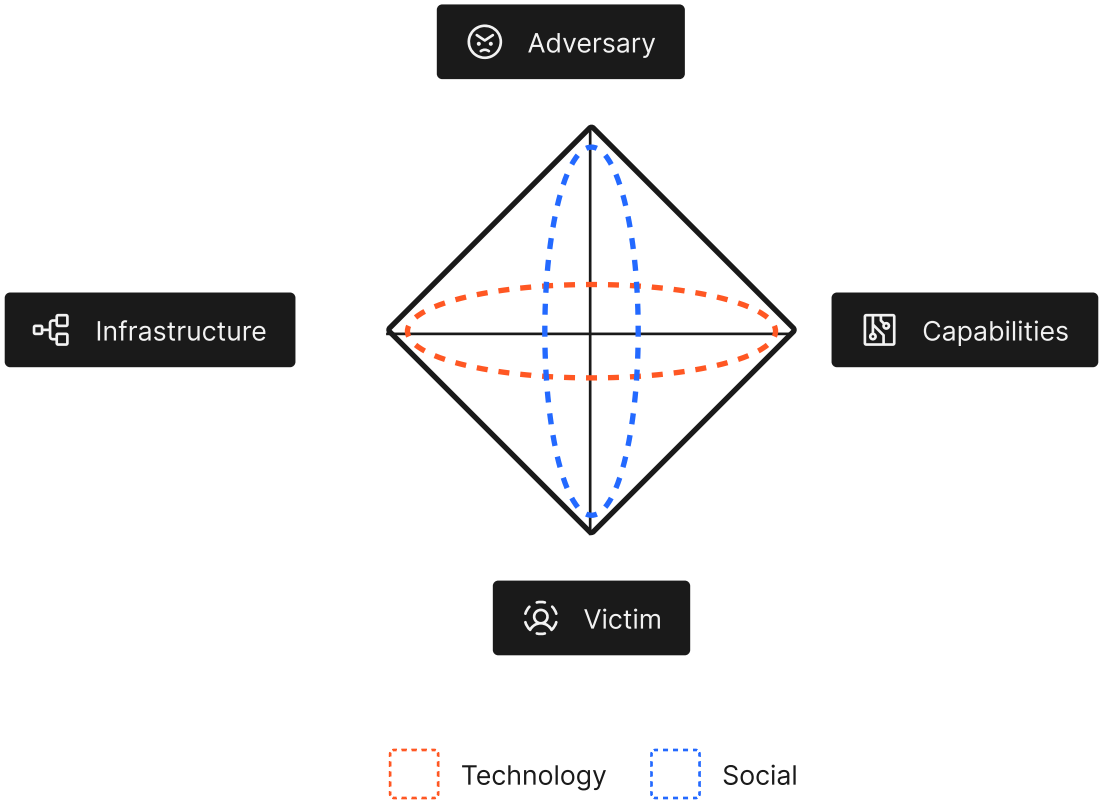


Figure 1 – Detection of the malicious file



Adversary	Byakugan Stealer operator
Victim	Companies in the financial and cryptocurrency sectors
Infrastructure	C2 servers, undetectable malware, and compromised infrastructure
Capabilities	Expertise in phishing techniques, including email delivery using social engineering; technical skills for crafting malicious files; and malware manipulation to evade reverse engineering in virtualized environments. Use of C2 servers and compromised infrastructure to impersonate vendors, enabling potential supply chain attacks.

Although evidence points to a Brazilian developer, infections from the campaign have been recorded in countries such as Ukraine, the United States, the Netherlands, and Germany. This report provides a detailed analysis of Byakugan's attack vectors, underlying infrastructure, and capabilities — aiming to understand its impact and identify potential mitigation measures.

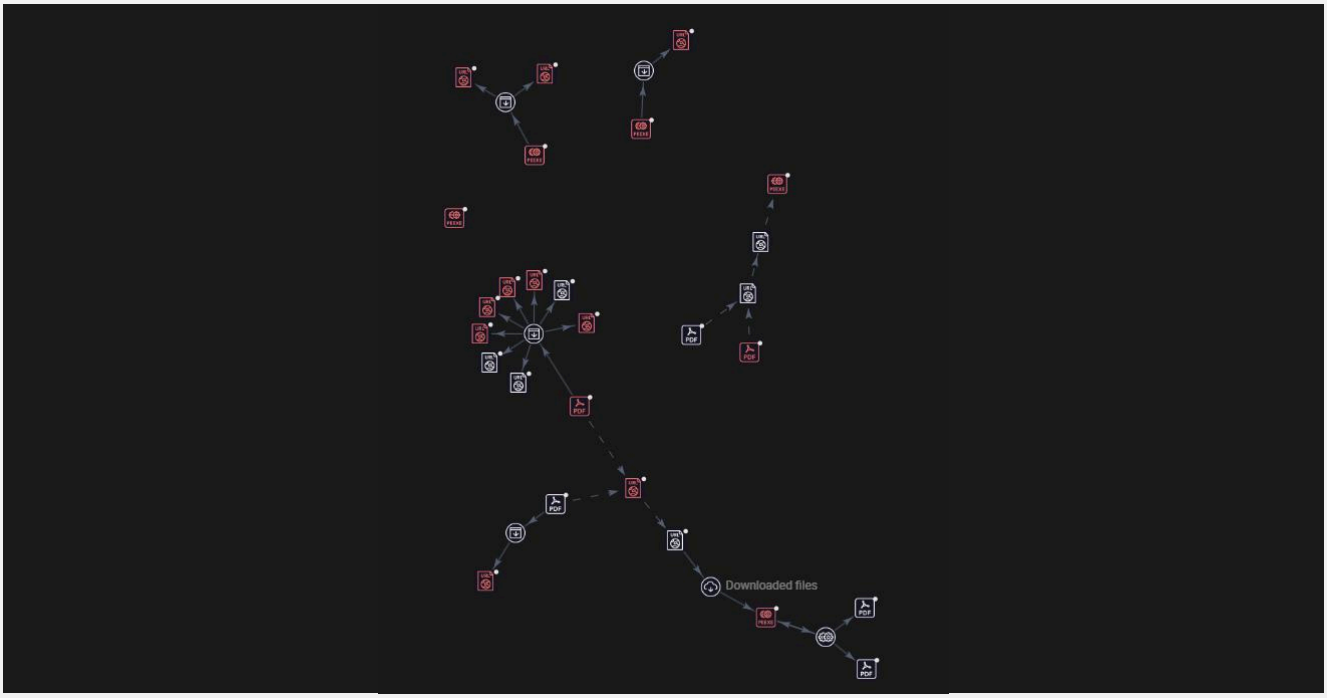


Figure 2 – Campaign map

The ART team identified direct links between code repositories, command-and-control (C2) infrastructure, and malicious files used in the operation.

The campaign's structure indicates a high level of sophistication, combining advanced phishing techniques, analysis evasion, and the use of compromised infrastructure to conceal its activities. The attack begins with phishing emails sent from compromised companies, exploiting the victim's trust in the sender's legitimacy. The message leverages a corporate context by impersonating a billing notice allegedly issued for payment under the target company's tax ID (CNPJ).

Figure 3 shows a fake PDF file containing a message that instructs the user to download and install a supposed version of Adobe Reader. The message deceives the user by claiming that the download is required to view the document.

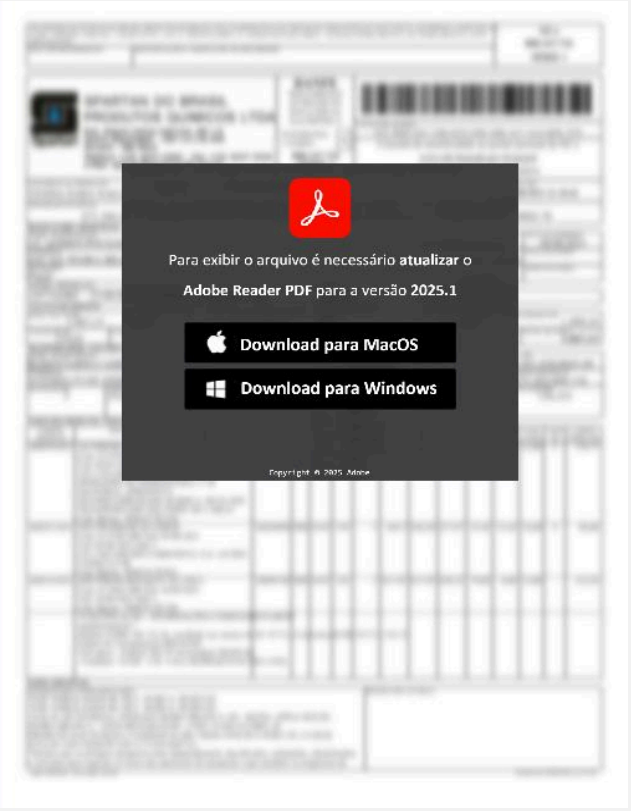


Figure 3 – Malicious PDF file

The malicious actor abuses URL shorteners to obfuscate the original download link. After clicking the button shown in Figure 3, the user is redirected to one of the following pages:

- https://rebrand[.]ly/reader-pdf-2025-download
- https://rebrand[.]ly/reader-2025-1-setup
- https://rebrand[.]ly/reader2025
- http://rebrand[.]ly/reader2025setup

They are then redirected to a GitHub download page, as indicated by the following URL:

- https://github[.]com/SarahSaldanhaReader/pdf-nota-fiscal/blob/main/Nota%20Fiscal%20Eletr%C3%B4nica.pdf

The downloaded file uses the Adobe Reader icon and is named Reader_2025_instal.exe. By disguising itself as an Adobe Reader installer, it tricks the user into executing the file.

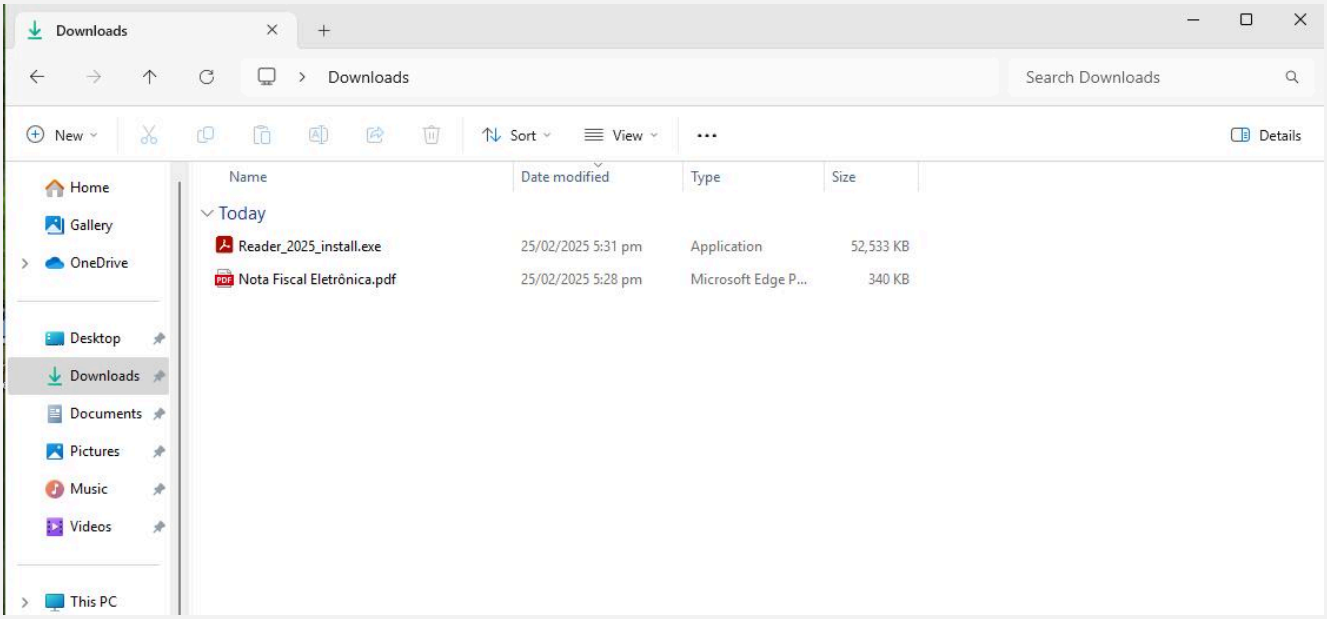


Figure 4 – Downloaded files

The Byakugan malware was analyzed by Axur in 2023 and by Fortinet and AhnLab in 2024. Its operational flow can be understood in the figure below:

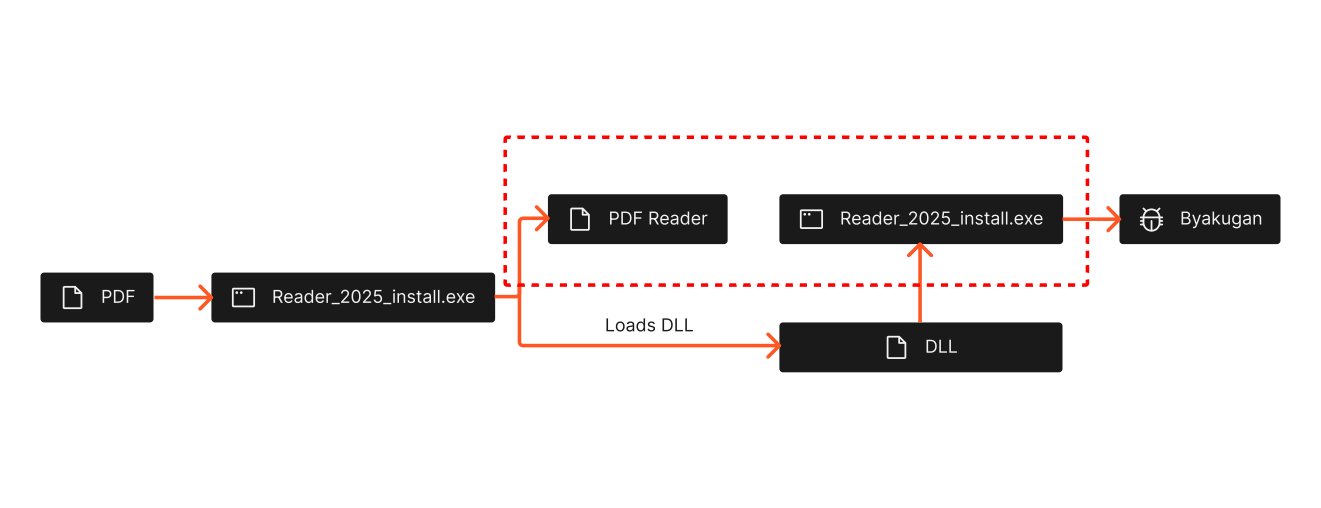


Figure 5 – Attack chain

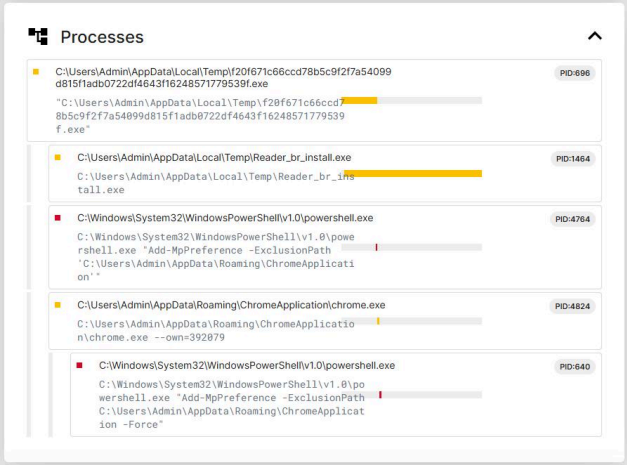


Figure 6 – Malware execution

It follows the same three execution phases:

1. Creation of the PDF file that delivers the malware

2. DLL Hijacking & UAC Bypass

3. Data exfiltration

The image shows that, during execution, a copy of the malware is moved to the “\Temp” folder, where it receives new instructions.

The malware adds an exception to Windows Defender and runs a process named “chrome.exe” — which is, in fact, the Byakugan malware.

Figure 7 – TCP connections made by the file

Analyzing both URLs — tunneleep[.]com.br and floravirtual[.]com.br — which the malware communicates with, we observed that the first one has no detections on VirusTotal, while the second shows a low detection rate. Below, we present the detection status of the URLs along with the IP addresses behind the domains.

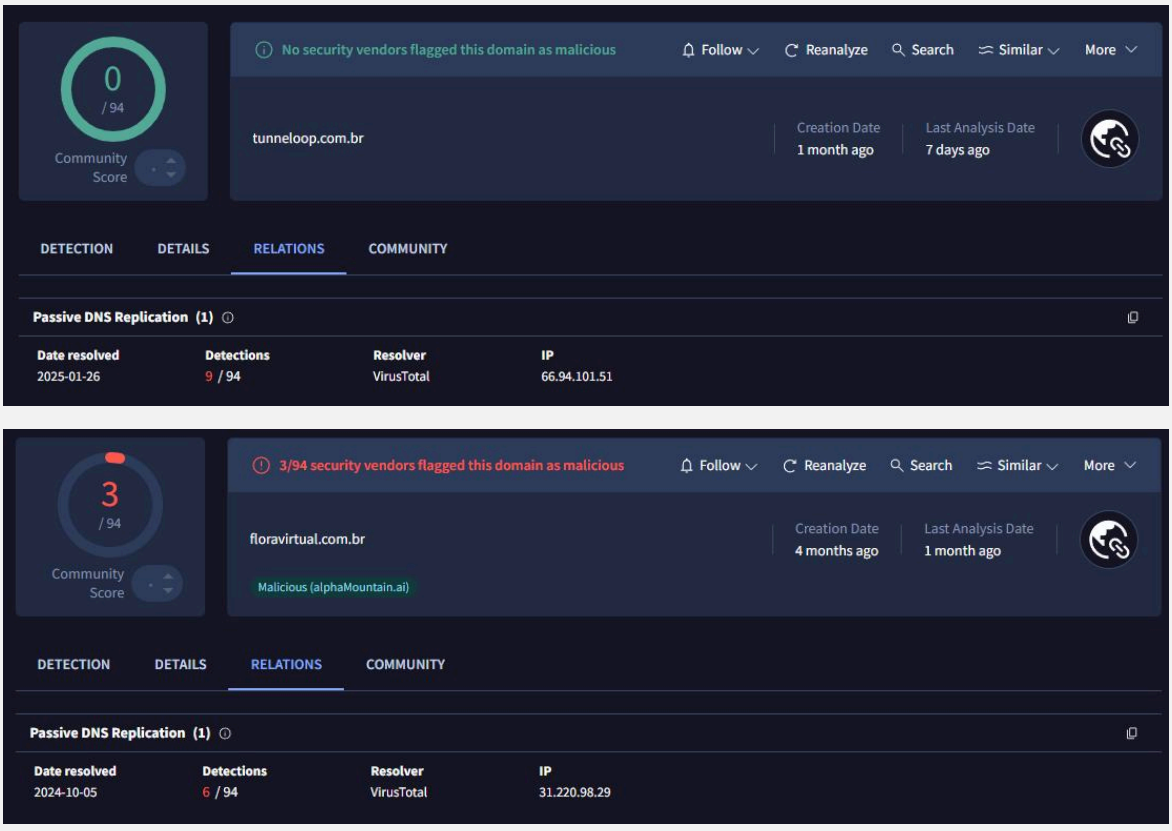
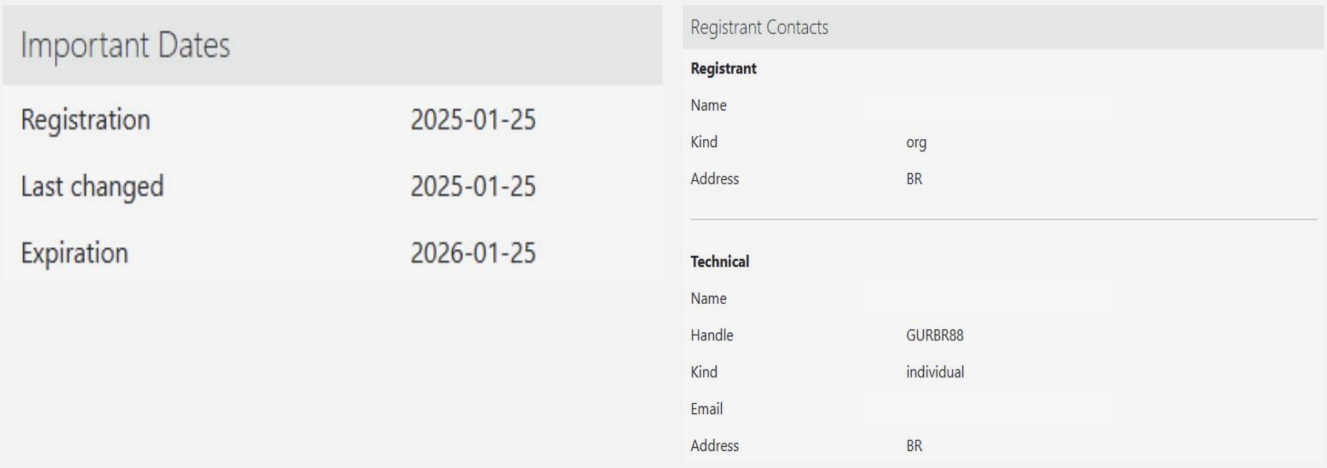


Figure 8 – VirusTotal results for the command-and-control servers

By checking the WHOIS information, it is possible to identify the registrants as well as their contact email addresses. It is also worth noting that the domain tunneleep[.]com.br was registered on January 25, 2025, and floravirtual[.]com.br was registered on October 3, 2024.



Important Dates	
Registration	2025-01-25
Last changed	2025-01-25
Expiration	2026-01-25

Registrant Contacts

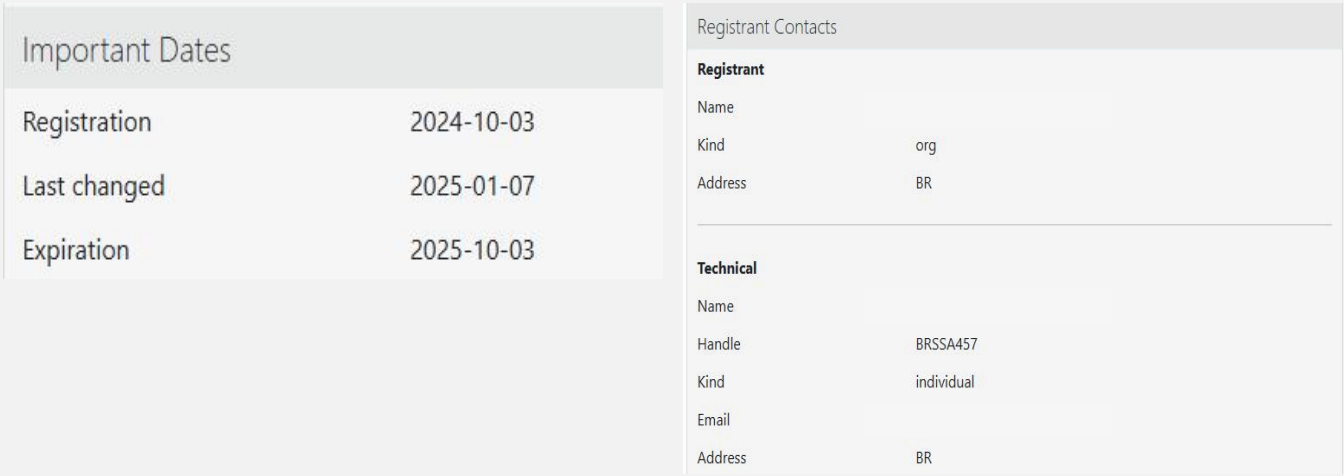
Registrant

Name	
Kind	org
Address	BR

Technical

Name	
Handle	GURBR88
Kind	individual
Email	
Address	BR

Figure 9 – WHOIS record for tunneleep[.]com.br



Important Dates	
Registration	2024-10-03
Last changed	2025-01-07
Expiration	2025-10-03

Registrant Contacts

Registrant

Name	
Kind	org
Address	BR

Technical

Name	
Handle	BRSSA457
Kind	individual
Email	
Address	BR

Figure 10 – WHOIS record for floravirtual[.]com.br

Analyzing both IP addresses — 66.94.101[.]51 and 31.220.98[.]29 — we observed that port 8080 is running the Byakugan command-and-control server.

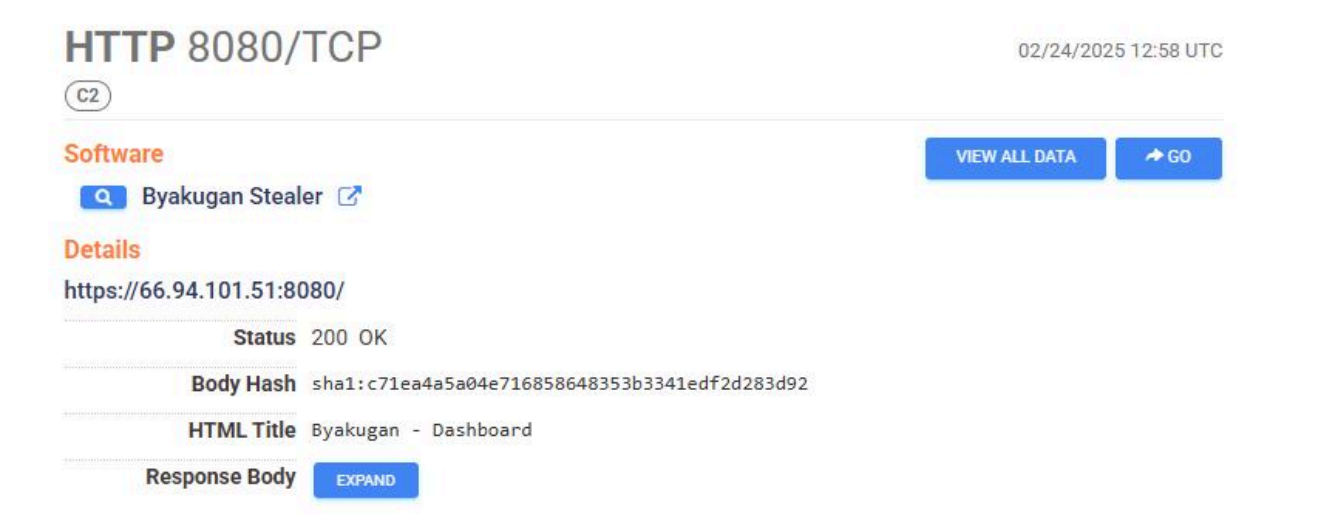


Figure 11 – Byakugan discovery via IP address

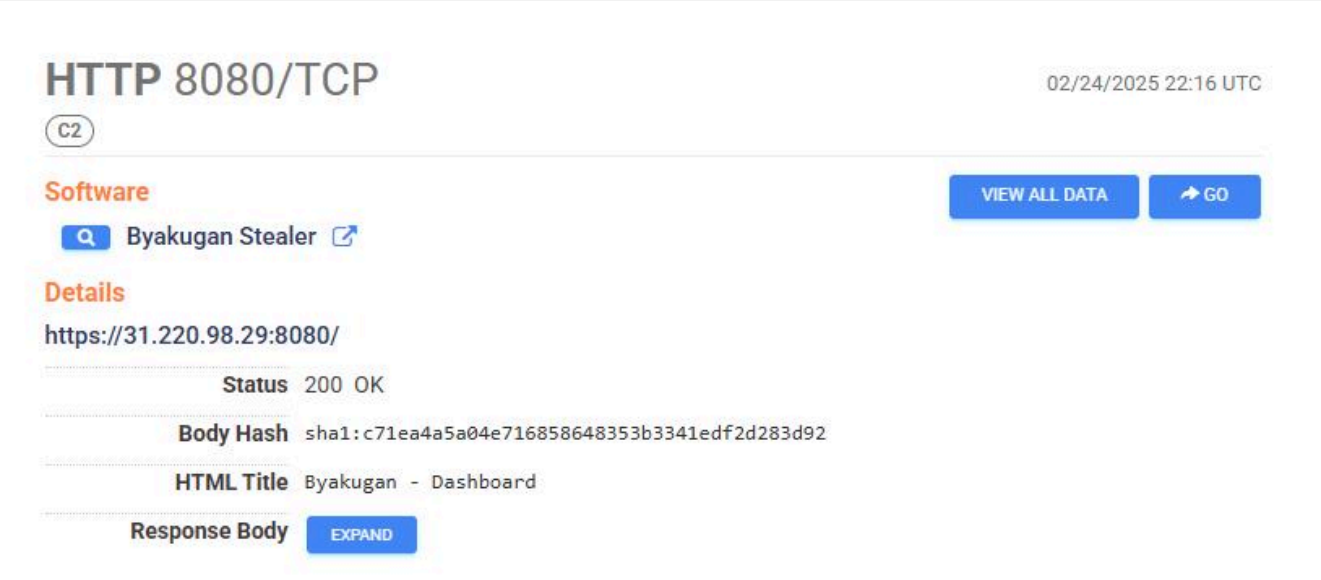


Figure 12 – Byakugan discovery via IP address

By accessing the discovered dashboards, it is possible to verify the presence of a login screen, with account registration requiring an invitation code.

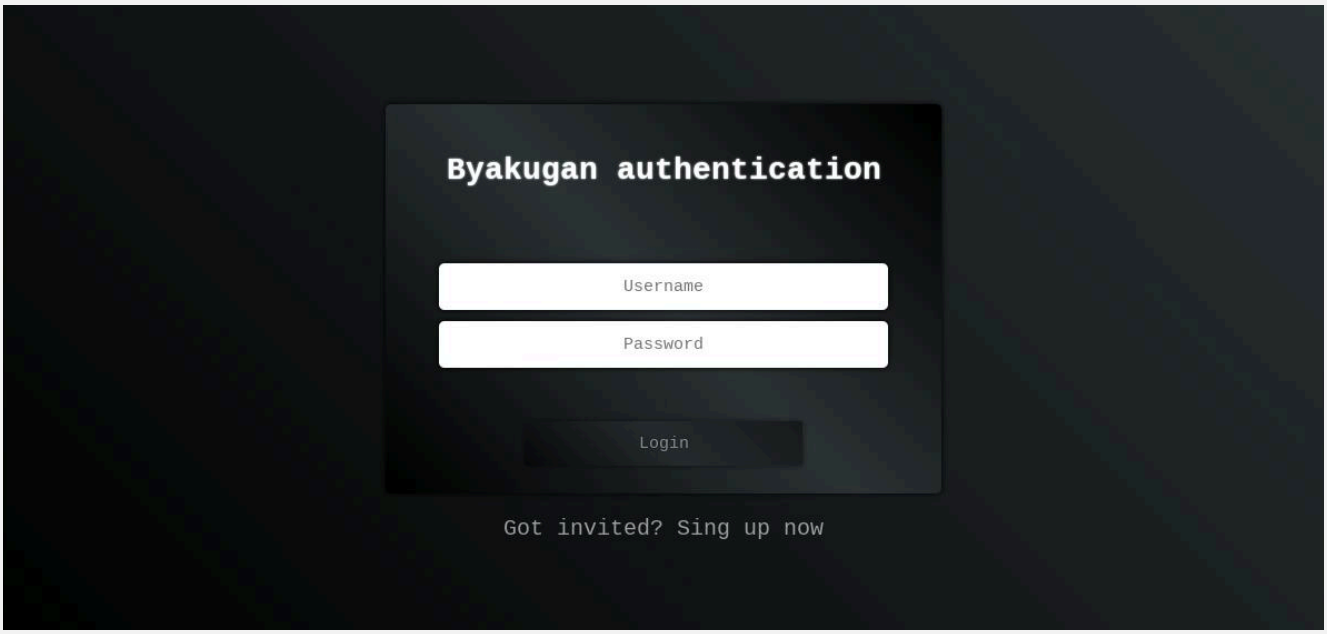


Figure 13 – Byakugan login panel

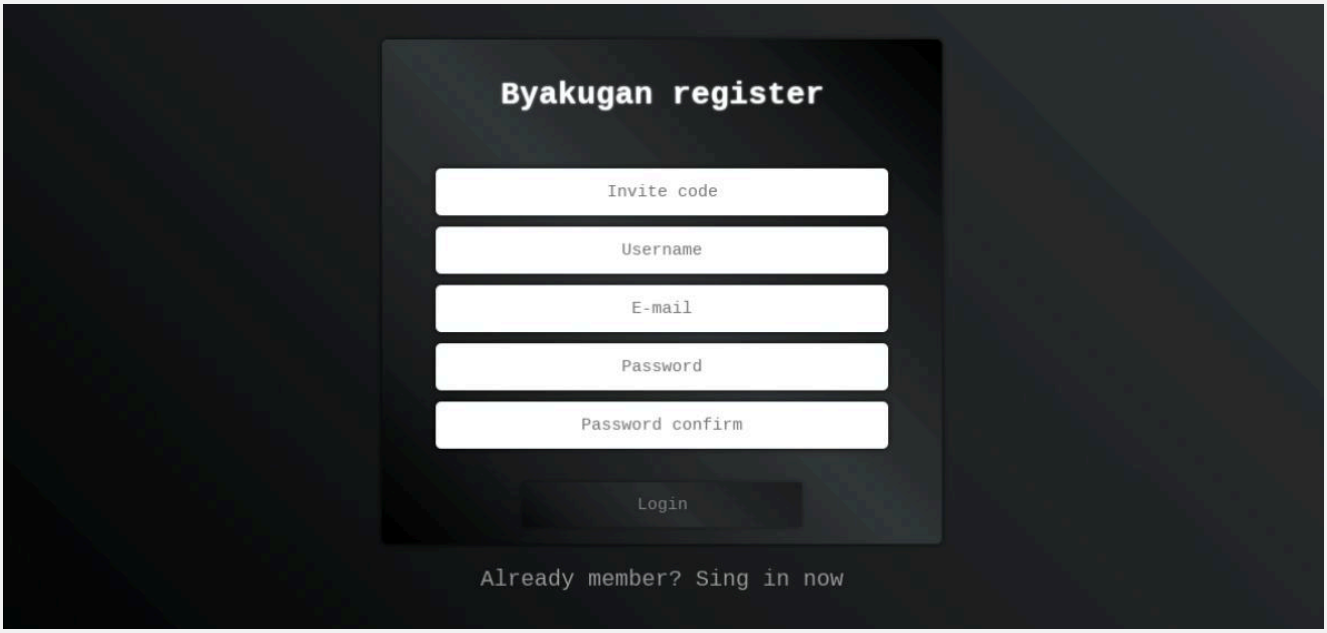


Figure 14 – Byakugan registration panel

A video hosted on Vimeo by the user Wellington Souza, uploaded on September 13, 2022, was found containing a demonstration of the dashboard in use. The video is available at the following link: hxxps://vimeo[.]com/749297709

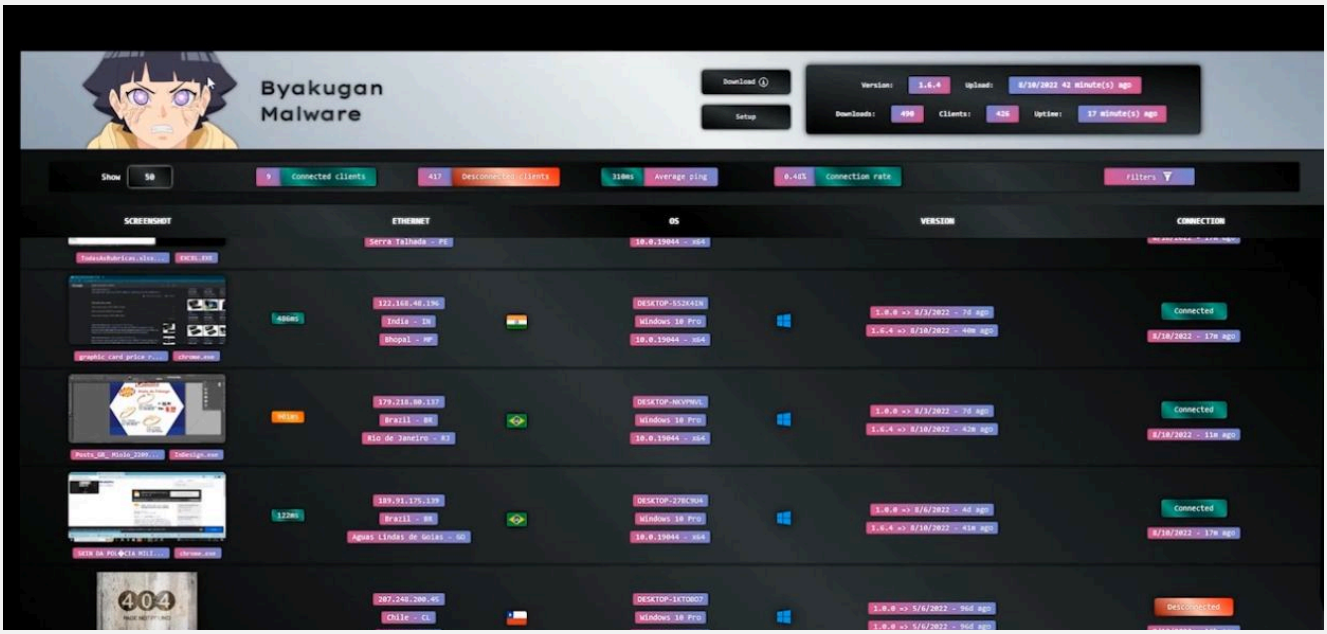


Figure 15 – Byakugan dashboard

The video shows both the screen displaying the infected devices and the screen listing the actions that can be performed on each device.

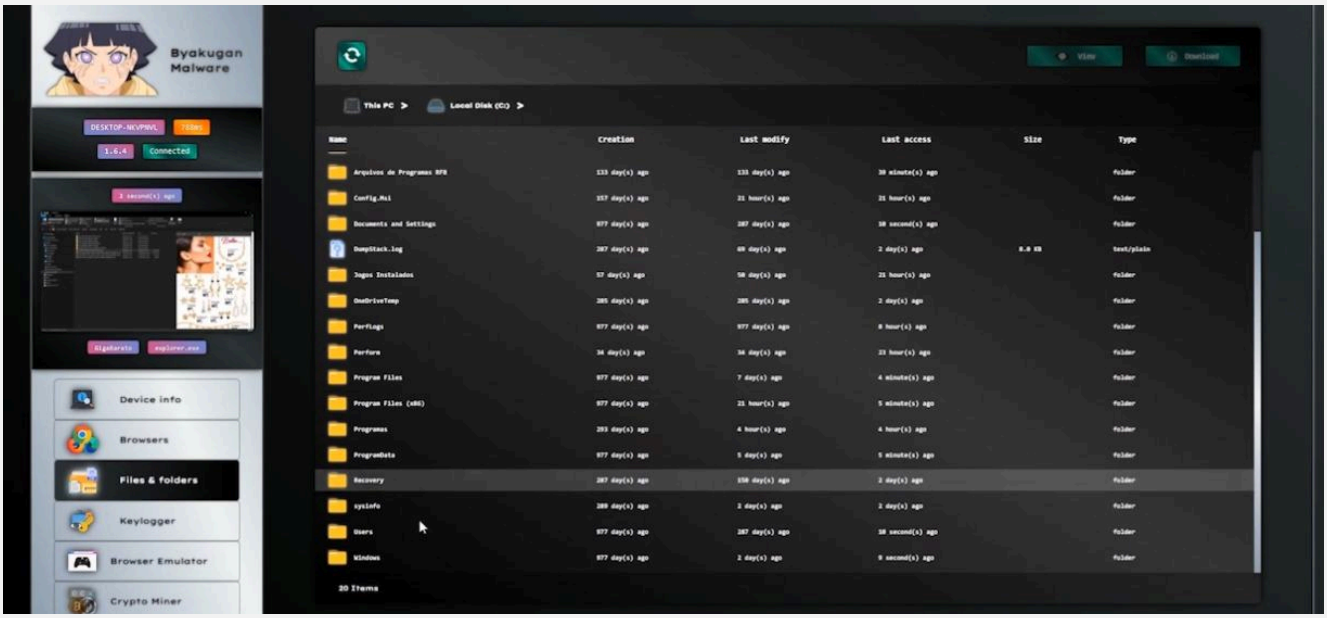


Figure 16 – Byakugan dashboard

Among the available post-infection actions are machine and browser data capture, file and directory listing, browser emulation, as well as keylogging and cryptocurrency mining functionalities.

MITRE ATT&CK

Tactics	Techniques
Initial Access	**T1566.002** - Phishing: Spearphishing Link
Defense Evasion	**T1036** - Masquerading **T1027** - Obfuscated Files or Information **T1497** - Virtualization/Sandbox Evasion
Discovery	**T1082** - System Information Discovery **T1057** - Process Discovery
Command and Control	**T1071.001** - Application Layer Protocol: Web Protocols **T1095** - Non-Application Layer Protocol **T1573** - Encrypted Channel **T1219** - Remote Access Software

IOCs

Git repository

https://github.com/SarahSaldanhaReader

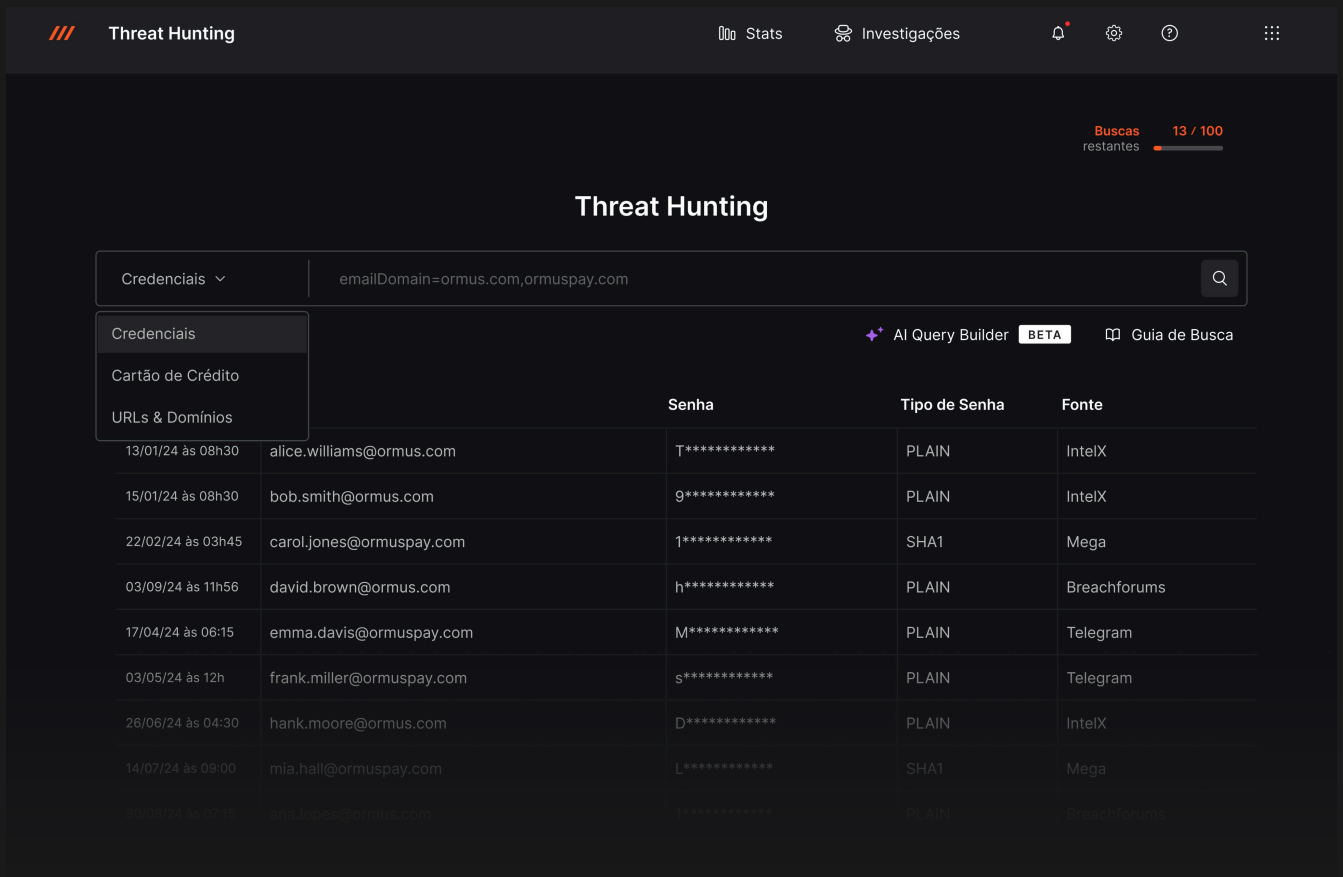
C2 Server

Tunneloop[.]com[.]br
https://66.94.101.51
https://a.floravirtual.com.br
https://89.117.72.231
https://157.173.205.223
https://207.244.251.87
https://209.145.55.141
https://thinkforce[.]com.br
https://31.220.98.29
https://66.94.101.51

Files

PDF:
39a4968ae07b7c62c74efe10f5f7f6448c6486ce
47738d7da1a529e124f7dd3e9a73f08008f95fbc
d274c2b5f3ec57f6a221782ecf14a077b4515066
e1d2842454cf792402e62e3f16fdfc5a4813e9c8
ee1a1240eacac48f030a078d8af1de010ab016b5
d7c9726594d7cf821adafe05d7e1974897fbfa8b3
58d6b6d276b1554Fbe6b7dd32b7326b80c1205f
9d7a40effe4fd26fb0f3476a885e9cb9b3ab2eb9
c9be783d70015d57bb10957f1ca782c0cb86e55
4b6f13a2b770362e3a3e02b45

exe:
C117f9949da24f4a0264087be941920ceae7468
889a5c90edb1d916265656846B1ce70df9679c2
7de5cc3bb6e19dd4666b5a28196dea4f53491ae
63b75d944d29799f04cbd1fecdd51063cce5fa8a
e6a3ee54ba7b9ca9d435b07911373ba2e59360f
7e374bfc91194d51095e83bcf7b784fb916cdd9f7
162d13321dbfe408a4ef20f671c66ccd78b5c9f2f
7a54099d815f1adb0722df4643f1624857177939f



About Axur

Axur is a cost-effective external cybersecurity solution that empowers security teams to handle threats beyond the perimeter. Our platform detects, inspects, and responds to brand impersonation, phishing scams, dark web mentions, threat intel vulnerabilities, and more.

With the world's best takedown, Axur removes malicious content quickly and efficiently 24×7, automatically handling 86% of detections. Our AI-powered tools scale threat intelligence 180x, freeing your security team to focus on strategic initiatives.

Discover how our solutions can transform your security strategy

BOOK A DEMO

Gartner Peer Insights 4.9

Descubra todas as soluções em **axur.com**

///AXUR