

Byakugan 2025:

highly evasive
malware targets the
financial and crypto
sectors





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:

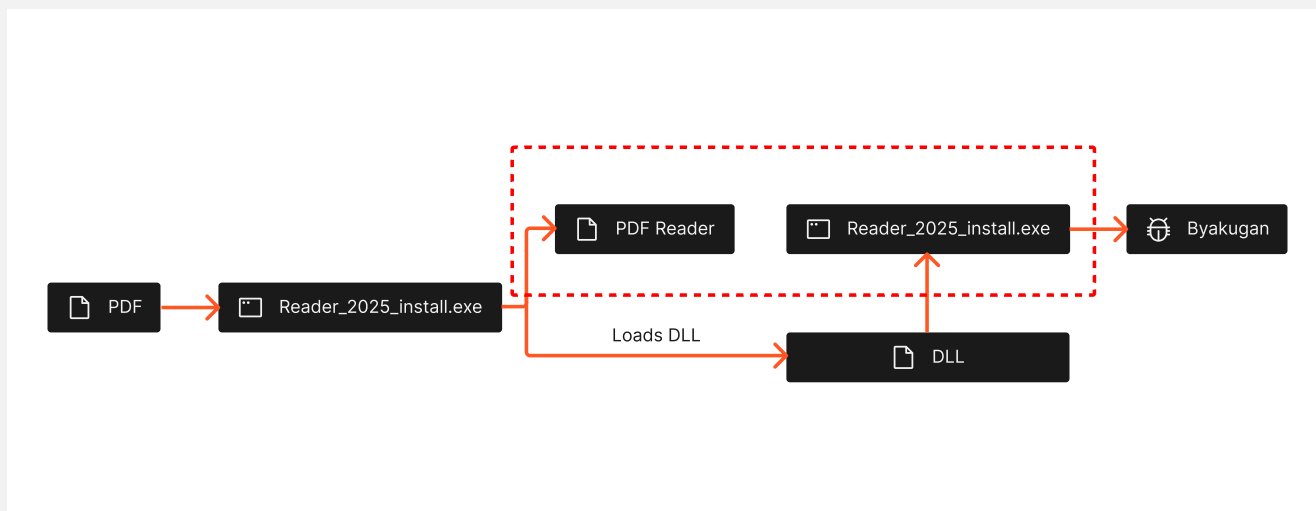


Figure 5 – Attack chain

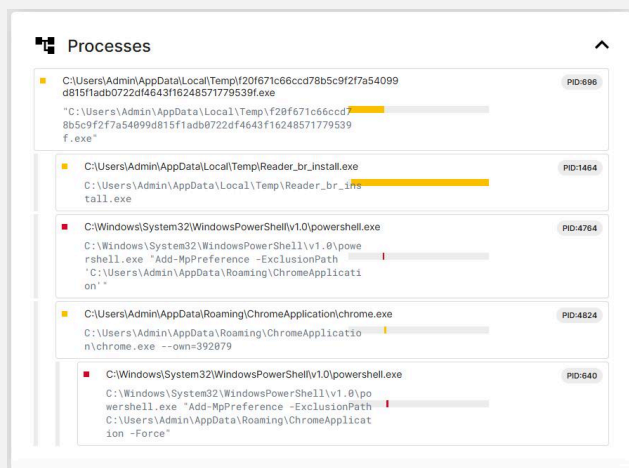


Figure 6 – Malware execution

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.



Network

Requests **TCP** UDP

| | | | | | |
|--|------------------|--------------------------------|------------|------------------|---|
| | 208.95.112.1:80 | http://ip-api.com/json | http | READER_PDF_20... | ▼ |
| | 66.94.101.51:443 | tunneleop.com.br | tls | READER_PDF_20... | ▼ |
| | 2.19.117.12:443 | https://use.typekit.net/bxf... | tls, http | READER_BR_INS... | ▼ |
| | 2.16.34.114:443 | https://www.bing.com/th?i... | tls, http2 | | ▼ |
| | 31.220.98.29:443 | floravirtual.com.br | | CHROME.EXE | ▼ |

Figure 7 – TCP connections made by the file

Analyzing both URLs — tunneleop[.]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.

The figure shows two screenshots of the VirusTotal interface. The top screenshot is for the domain **tunneleop.com.br**. It shows a Community Score of 0/94, indicating no security vendors flagged this domain as malicious. The last analysis date is 7 days ago. The 'RELATIONS' tab is active, showing 'Passive DNS Replication (1)' with a table of detection data:

| Date resolved | Detections | Resolver | IP |
|---------------|------------|------------|--------------|
| 2025-01-26 | 9 / 94 | VirusTotal | 66.94.101.51 |

The bottom screenshot is for the domain **floravirtual.com.br**. It shows a Community Score of 3/94, with a warning that 3/94 security vendors flagged this domain as malicious. The last analysis date is 1 month ago. The 'RELATIONS' tab is active, showing 'Passive DNS Replication (1)' with a table of detection data:

| Date resolved | Detections | Resolver | IP |
|---------------|------------|------------|--------------|
| 2024-10-05 | 6 / 94 | VirusTotal | 31.220.98.29 |

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 |
| <hr/> | |
| 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 |
| <hr/> | |
| 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.

The screenshot shows an analysis interface for an HTTP 8080/TCP connection. At the top, it displays 'HTTP 8080/TCP' and the timestamp '02/24/2025 12:58 UTC'. Below this, there is a 'C2' indicator in a circle. The 'Software' section identifies the application as 'Byakugan Stealer' with a search icon and an external link icon. To the right of this section are two buttons: 'VIEW ALL DATA' and 'GO'. The 'Details' section shows the URL 'https://66.94.101.51:8080/'. Below the URL, several fields are listed: 'Status' is '200 OK', 'Body Hash' is 'sha1:c71ea4a5a04e716858648353b3341edf2d283d92', and 'HTML Title' is 'Byakugan - Dashboard'. At the bottom, the 'Response Body' field is visible with an 'EXPAND' button.

Figure 11 – Byakugan discovery via IP address

The screenshot shows an analysis interface for an HTTP 8080/TCP connection. At the top, it displays 'HTTP 8080/TCP' and the timestamp '02/24/2025 22:16 UTC'. Below this, there is a 'C2' indicator in a circle. The 'Software' section identifies the application as 'Byakugan Stealer' with a search icon and an external link icon. To the right of this section are two buttons: 'VIEW ALL DATA' and 'GO'. The 'Details' section shows the URL 'https://31.220.98.29:8080/'. Below the URL, several fields are listed: 'Status' is '200 OK', 'Body Hash' is 'sha1:c71ea4a5a04e716858648353b3341edf2d283d92', and 'HTML Title' is 'Byakugan - Dashboard'. At the bottom, the 'Response Body' field is visible with an 'EXPAND' button.

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.

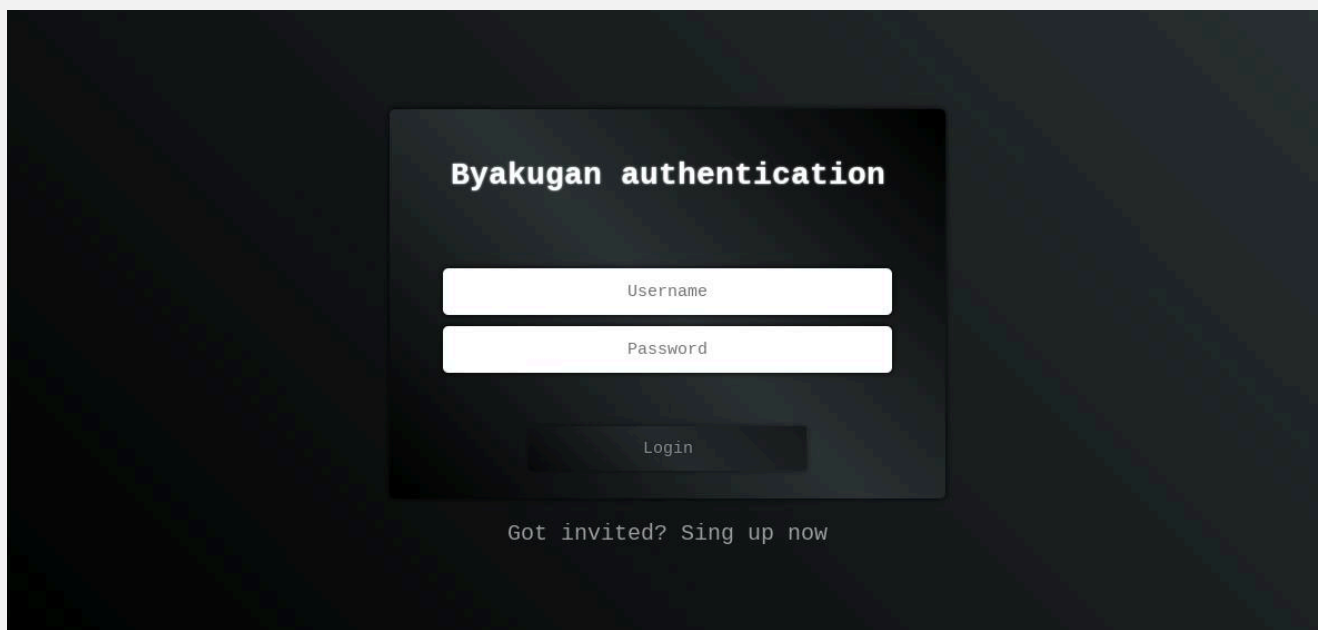


Figure 13 – Byakugan login panel

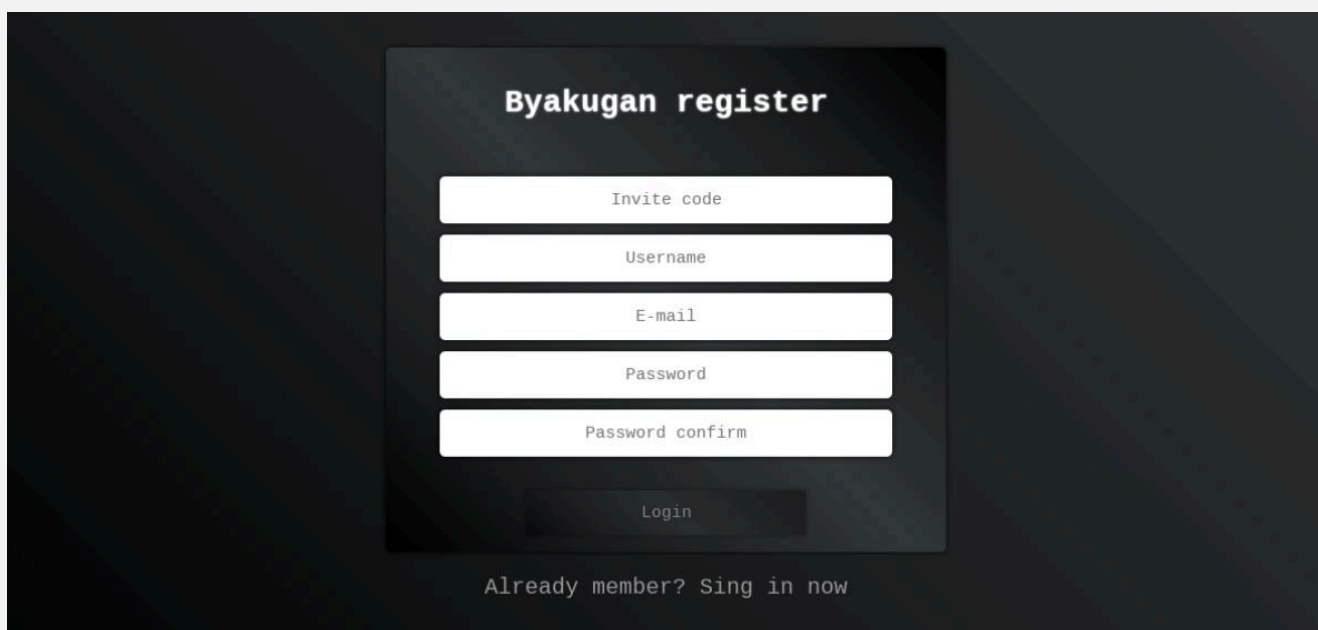


Figure 14 – Byakugan registration panel



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: <https://vimeo.com/749297709>

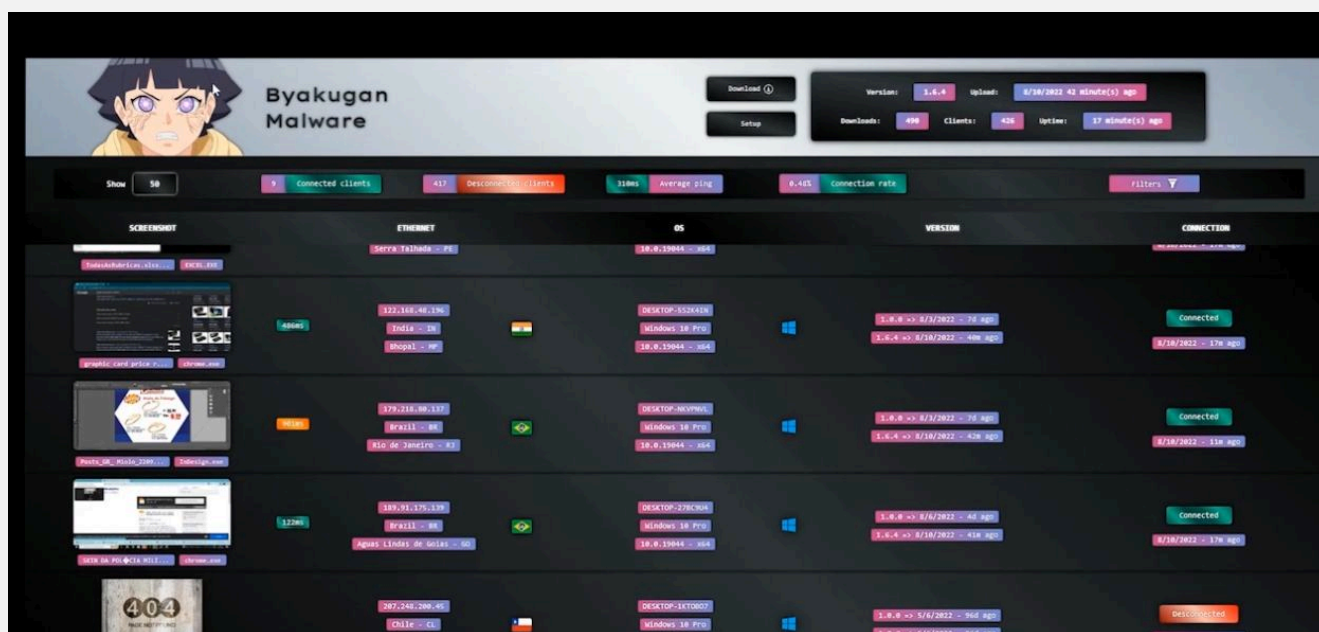


Figure 15 – Byakugan dashboard

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

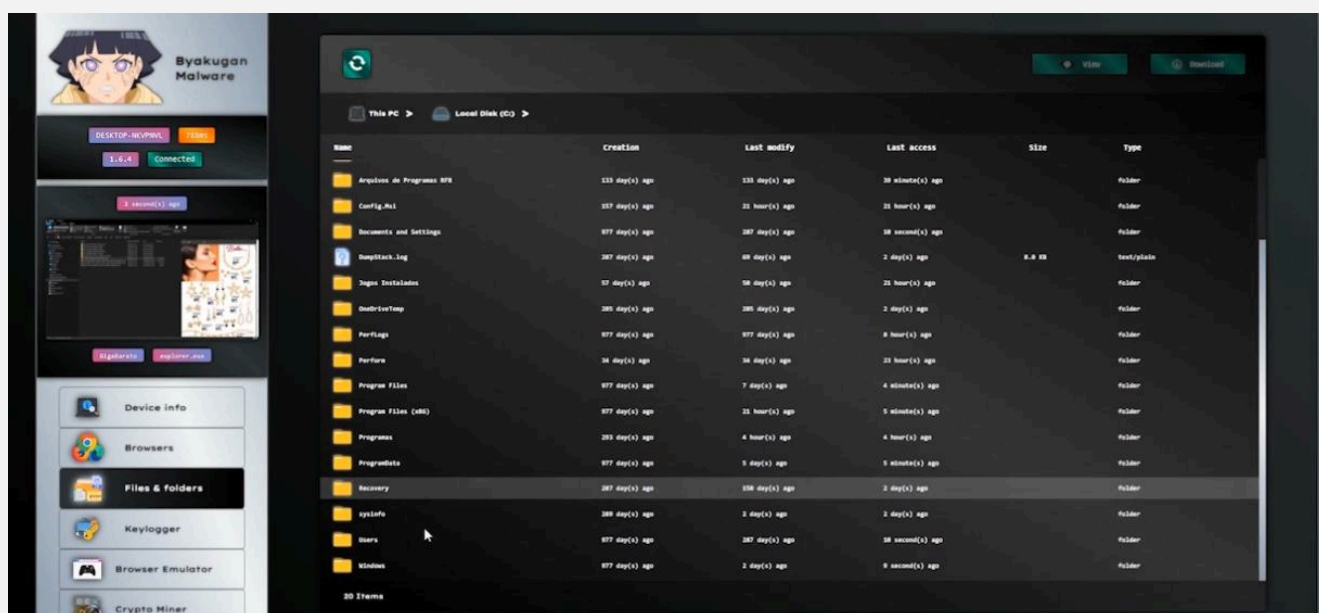


Figure 16 – Byakugan dashboard



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

Tunnelloop[.]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://thinkforce[.]com.br)
<https://31.220.98.29>
<https://66.94.101.51>

Files

PDF:
39a4968ae07b7c62c74efe10f5f7f6448c6486ce
47738d7da1a529e124f7dd3e9a73f08008f95fbc
d274c2b5f3ec57f6a221782ecf14a077b4515066
e1d2842454cf792402e62e3f16fdcf5a4813e9c8
ee1a1240eacac48f030a078d8af1de010ab016b5
d7c9726594d7cf821adafe05d7e1974897fbfa8b3
58d6b6d276b1554Fbe6b7dd32b7326b80c1205f
9d7a40effe4fd26fb0f3476a885e9cb9b3ab2eb9
c9be783d70015d57bb10957f1ca782c0cb86e55
4b6f13a2b770362e3a3e02b45

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

Buscas restantes 13 / 100

Threat Hunting

| Credenciais | | Senha | Tipo de Senha | Fonte |
|-------------------|---------------------------|--------|---------------|--------------|
| 13/01/24 às 08h30 | alice.williams@ormus.com | T***** | PLAIN | IntelX |
| 15/01/24 às 08h30 | bob.smith@ormus.com | g***** | PLAIN | IntelX |
| 22/02/24 às 03h45 | carol.jones@ormuspay.com | 1***** | SHA1 | Mega |
| 03/09/24 às 11h56 | david.brown@ormus.com | h***** | PLAIN | Breachforums |
| 17/04/24 às 06:15 | emma.davis@ormuspay.com | M***** | PLAIN | Telegram |
| 03/05/24 às 12h | frank.miller@ormuspay.com | s***** | PLAIN | Telegram |
| 26/06/24 às 04:30 | hank.moore@ormus.com | D***** | PLAIN | IntelX |
| 14/07/24 às 09:00 | mia.hall@ormuspay.com | L***** | SHA1 | Mega |
| 01/08/24 às 01:15 | anna.thompson@ormus.com | ***** | PLAIN | Breachforums |

Credenciais

emailDomain=ormus.com,ormuspay.com



Credenciais

Cartão de Crédito

URLs & Domínios

AI Query Builder

BETA

Guia de Busca

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 24x7, 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
★★★★★

