Byakugan 2025:

malware altamente evasivo apunta al sector financiero y de criptomonedas

AXUR

En 2025, investigadores del Axur Research Team (ART) identificaron una nueva campaña de phishing que distribuye una variante altamente evasiva del malware Byakugan. Esta versión del troyano presenta una baja tasa de detección por soluciones antivirus, lo que la convierte en una amenaza significativa para empresas de todos los sectores.

Los operadores de esta campaña emplean técnicas avanzadas de ingeniería social y phishing, utilizando infraestructuras comprometidas para simular comunicaciones legítimas de proveedores. De este modo, logran engañar a las víctimas e inducirlas a ejecutar archivos maliciosos. Además, hay evidencia de que el adversario emplea mecanismos de ofuscación y anti-análisis, dificultando su detección y la ingeniería inversa del malware.

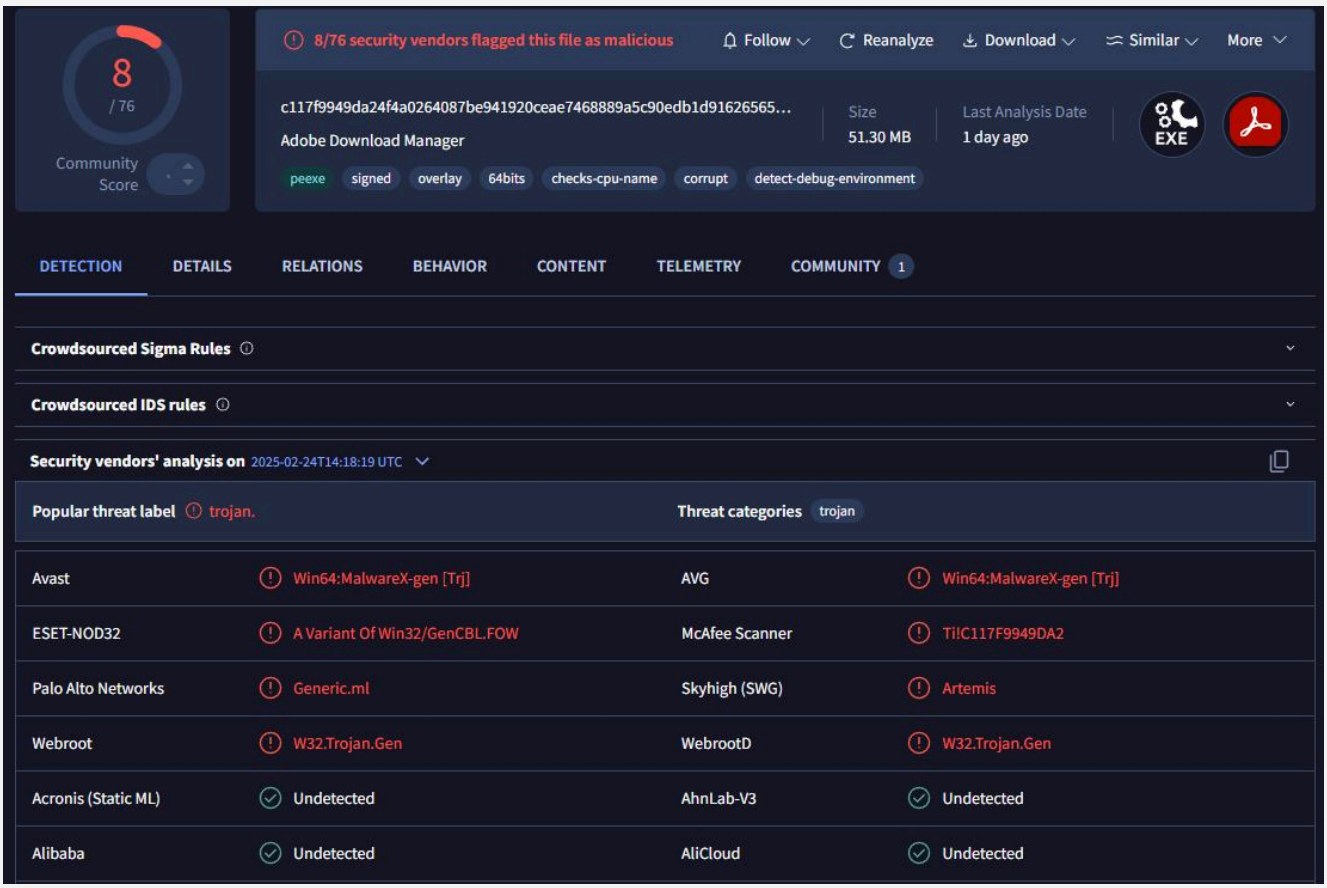
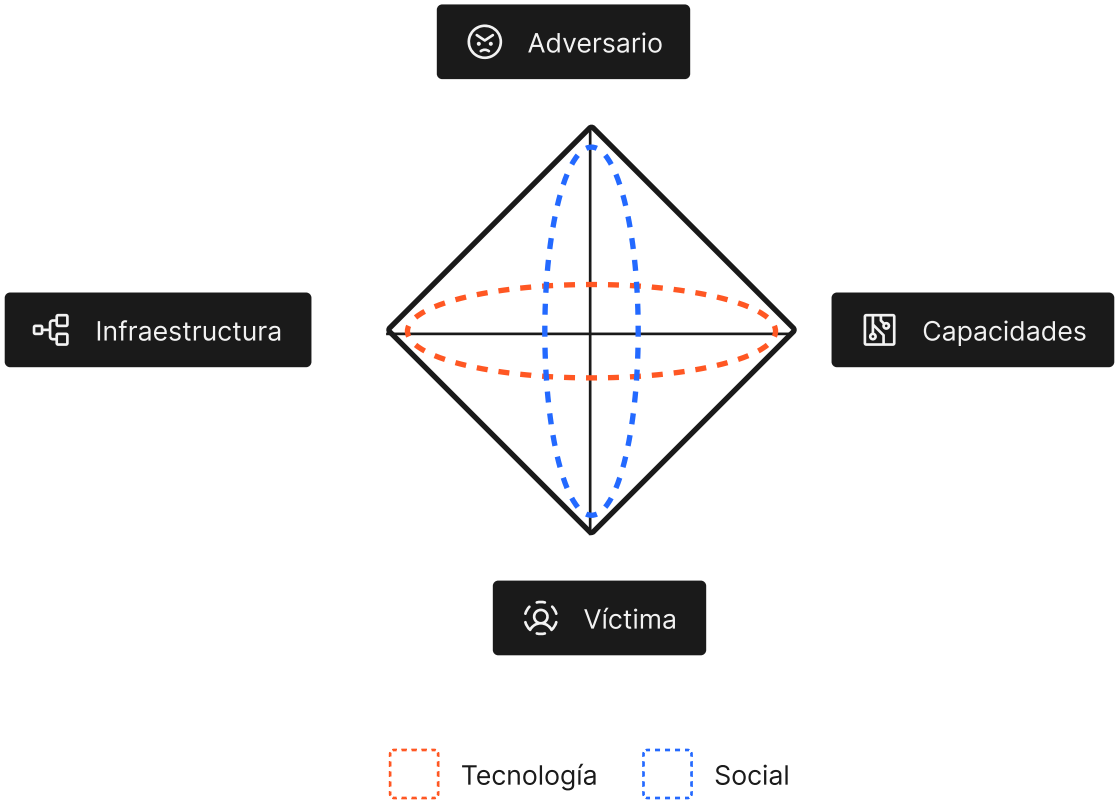


Figura 1 – Detección del archivo malicioso



Adversario	Operador de Byakugan Stealer
Víctima	Empresas del sector financiero y de criptomonedas
Infraestructura	Servidores C2, malware indetectable e infraestructuras comprometidas
Capacidades	Dominio de técnicas de phishing (incluido el envío de correos con ingeniería social), manipulación de archivos maliciosos y modificación del malware para dificultar su análisis en entornos virtuales. Uso de servidores C2 e infraestructura comprometida para simular proveedores y posibilitar ataques a la cadena de suministro.

Aunque los indicios apuntan a un desarrollador brasileño, se han registrado infecciones de la campaña en países como Ucrania, Estados Unidos, Países Bajos y Alemania. Este informe analiza en detalle los vectores de ataque, la infraestructura utilizada y las capacidades de Byakugan, con el objetivo de comprender su impacto y posibles medidas de mitigación.

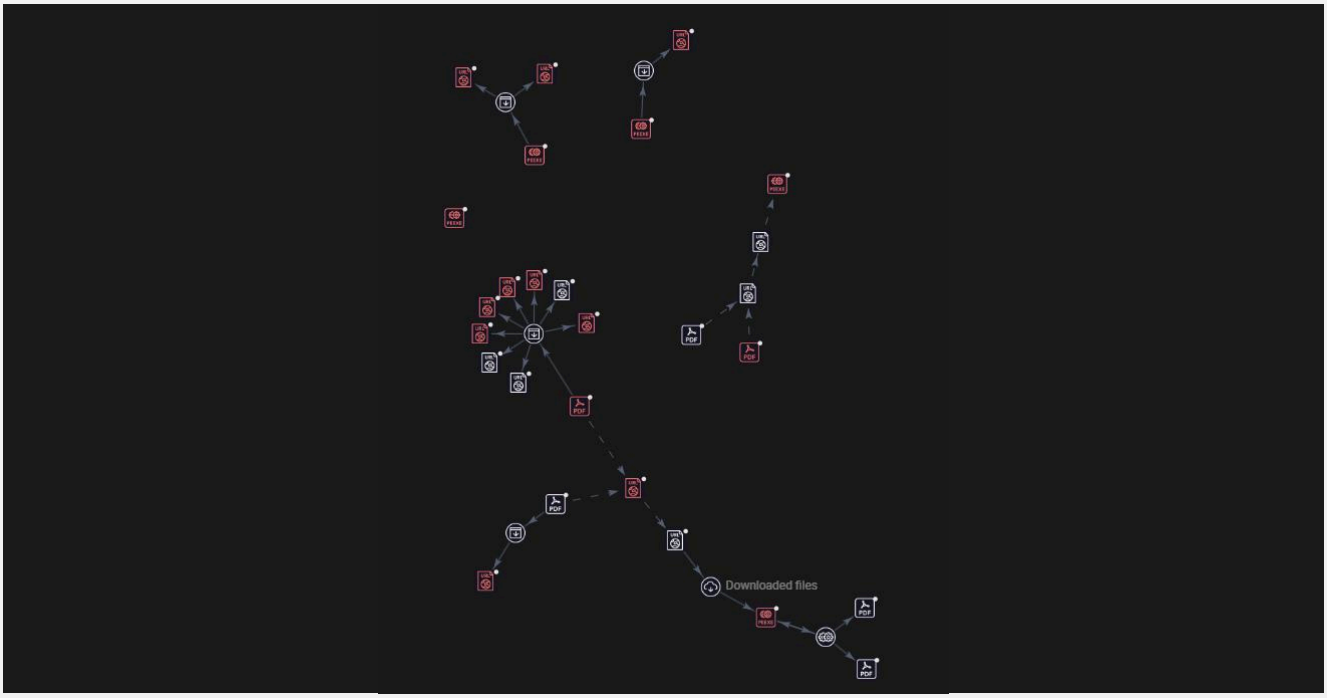


Figura 2 – Mapa de la campaña

El equipo de ART identificó conexiones directas entre repositorios de código, infraestructuras de comando y control (C2) y archivos maliciosos utilizados en la operación.

La estructura de la campaña sugiere un alto grado de sofisticación, combinando phishing avanzado, evasión de análisis y uso de infraestructura comprometida para ocultar actividades.

La campaña comienza con correos de phishing enviados desde empresas comprometidas, aprovechando la confianza de las víctimas en el remitente. El mensaje falsifica una supuesta factura generada para el CNPJ de la empresa objetivo, reforzando el contexto corporativo.

El archivo PDF falso, escrito en portugués, contiene un mensaje que instruye al usuario a descargar e instalar una supuesta versión de Adobe Reader. La víctima es engañada con el argumento de que el software es necesario para visualizar el documento.

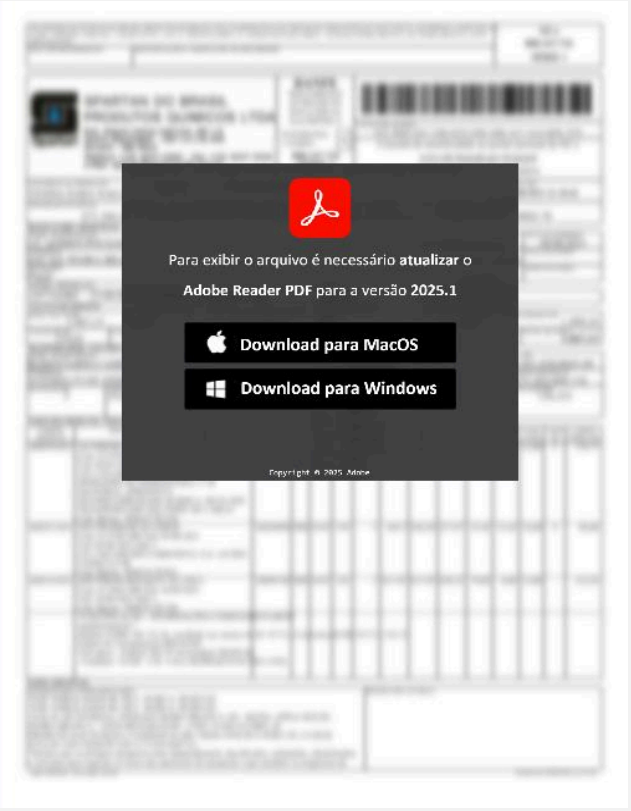


Figura 3 – Archivo PDF malicioso

El actor malicioso abusa de acortadores de URL para ocultar el enlace de descarga original. Tras hacer clic en el botón mostrado en la Figura 3.

https://rebrand[.]ly/reader-pdf-2025-download

https://rebrand[.]ly/reader-2025-1-setup

https://rebrand[.]ly/reader2025

http://rebrand[.]ly/reader2025setup

El usuario es redirigido a páginas que, a su vez, apuntan a un enlace de descarga en GitHub.

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

El archivo descargado tiene el nombre Reader_2025_instal.exe y utiliza el ícono de Adobe Reader para parecer legítimo. Este disfraz induce al usuario a ejecutarlo.

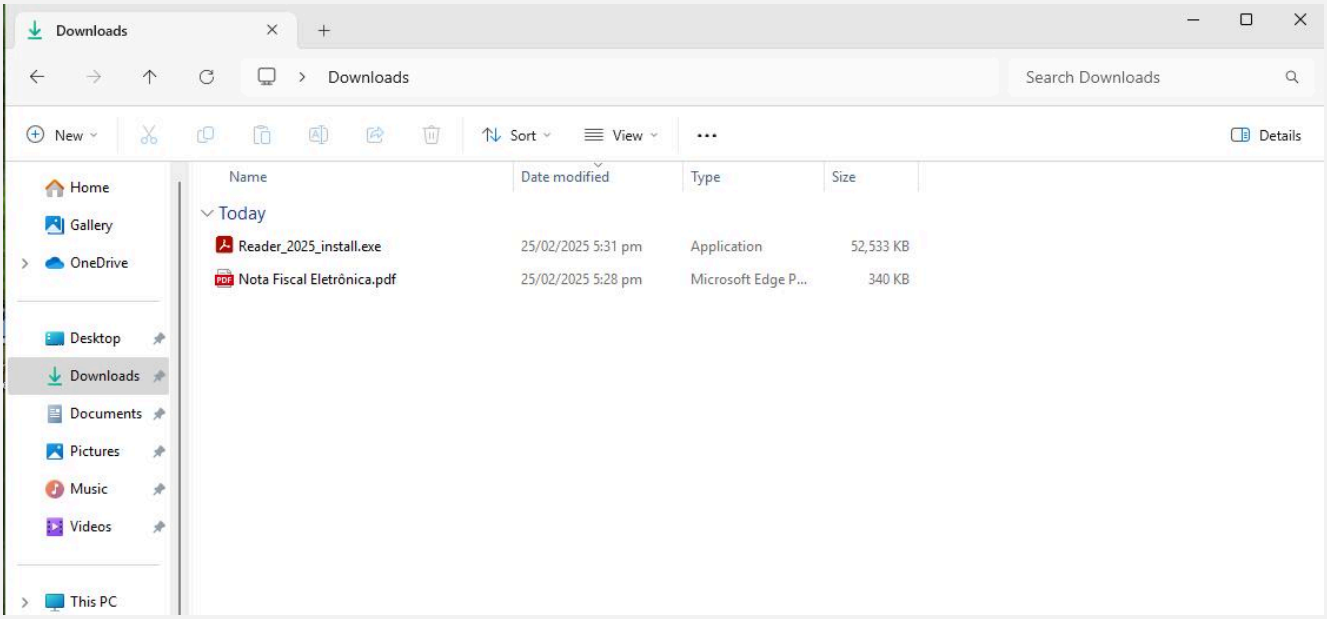


Figura 4 – Archivos descargados

El malware Byakugan fue analizado por Axur en 2023 y por Fortinet y AhnLab en 2024. El flujo de funcionamiento del malware puede observarse en la figura siguiente:

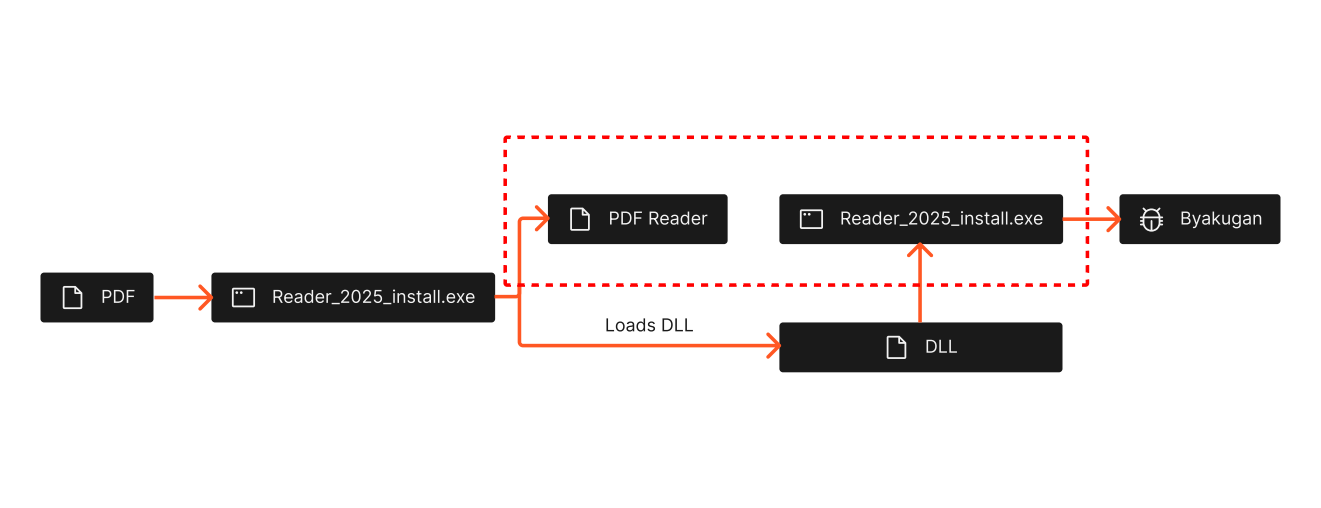


Figura 5 – Cadena de ataque

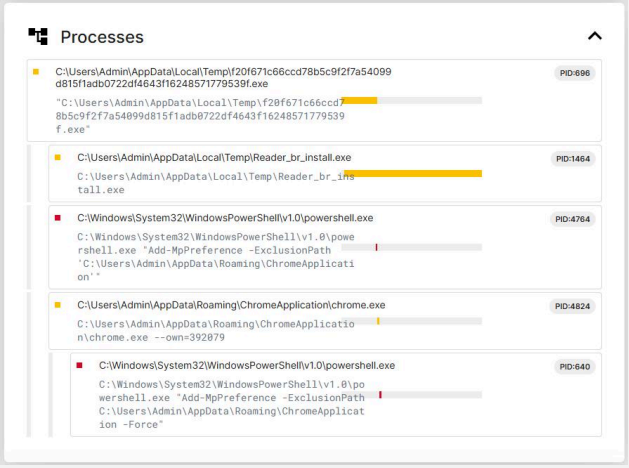


Figura 6 – Ejecución del malware

Su funcionamiento consta de tres fases:

1. Creación del archivo PDF que distribuye el malware

2. DLL Hijacking & UAC Bypass

3. Exfiltración de información

Durante la ejecución, una copia del malware se mueve a la carpeta \\Temp, donde recibe nuevas instrucciones. También agrega una exclusión en Windows Defender y ejecuta un proceso chrome.exe, que corresponde al propio malware.

Figura 7 – Conexiones TCP realizadas por el archivo

Al analizar ambas URLs tunneleep[.]com.br y floravirtual[.]com.br con las que el malware se comunica, observamos que la primera no presenta ninguna detección en VirusTotal, mientras que la segunda tiene un bajo nivel de detección. A continuación, se muestra el grado de detección de las URLs, así como las direcciones IP asociadas a esos dominios.

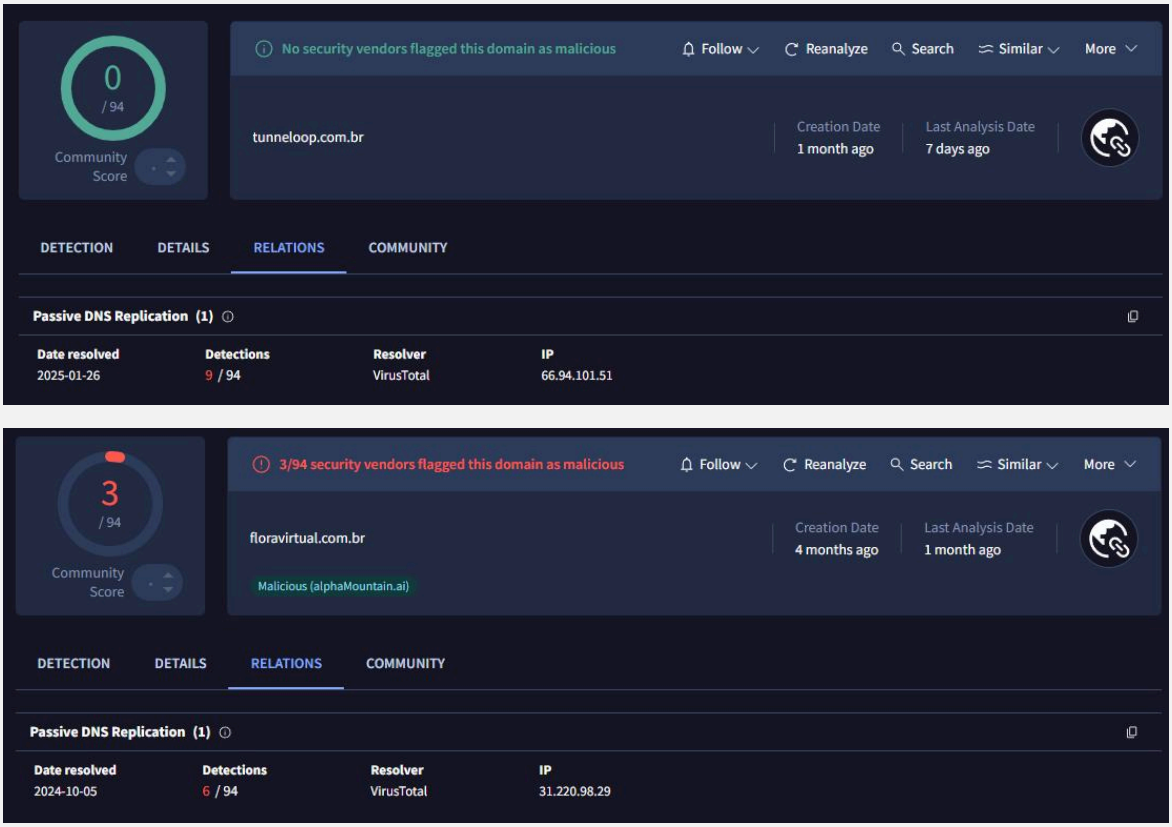
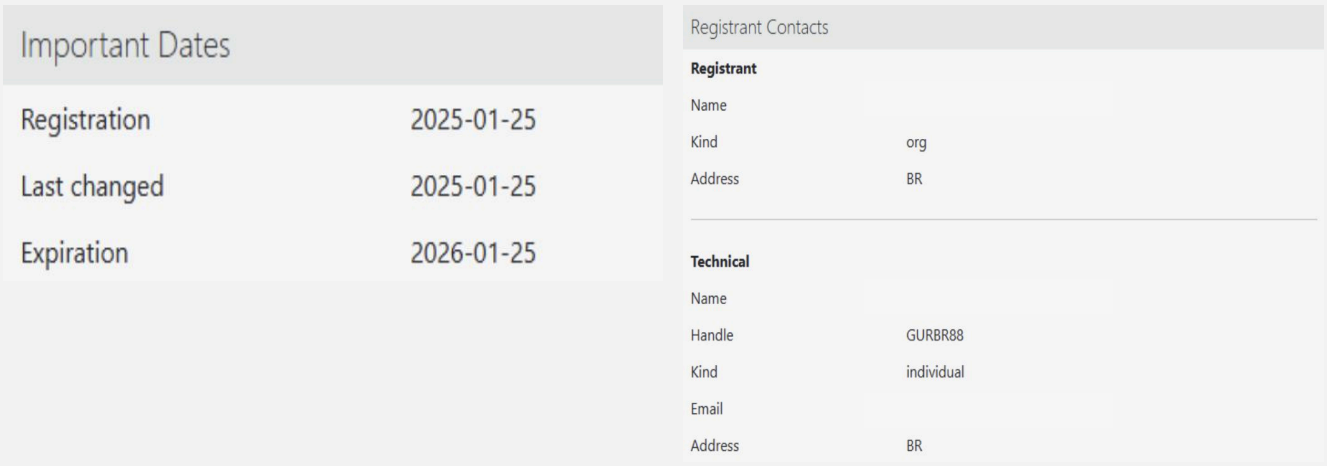


Figura 8 – Resultados de VirusTotal para los servidores de comando y control

Al verificar la información de WHOIS, es posible identificar a los responsables, así como sus correos electrónicos de contacto. También es importante destacar que el dominio tunneleep[.]com.br fue registrado el 25 de enero de 2025, y el dominio floravirtual[.]com.br fue registrado el 3 de octubre de 2024.



Important Dates

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

Registrant Contacts

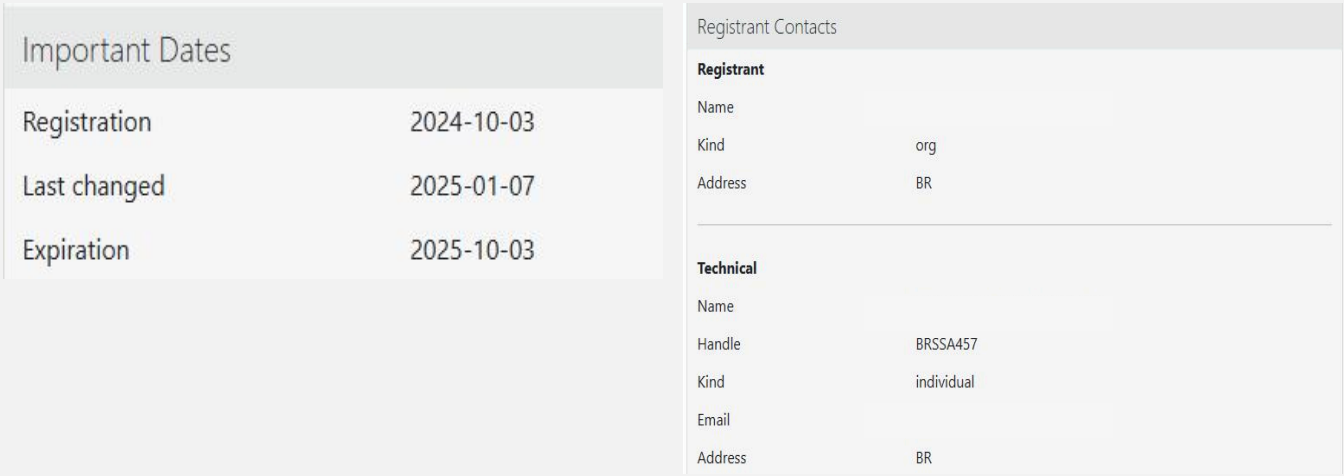
Registrant

Name	
Kind	org
Address	BR

Technical

Name	
Handle	GURBR88
Kind	individual
Email	
Address	BR

Figura 9 – Registro WHOIS de 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

Figura 10 – Registro WHOIS de floravirtual[.]com.br

Al analizar ambas direcciones IP — 66.94.101[.]51 y 31.220.98[.]29 — se observó que el puerto 8080 está ejecutando el servidor de comando y control (C2) de Byakugan.

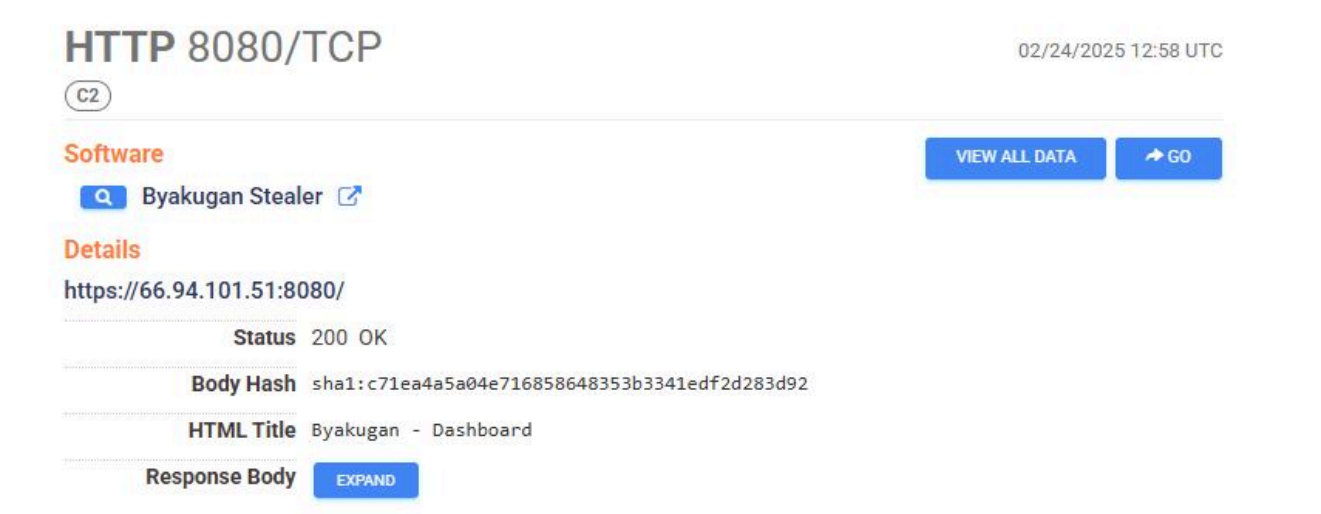


Figura 11 – Identificación de Byakugan a través de la dirección IP

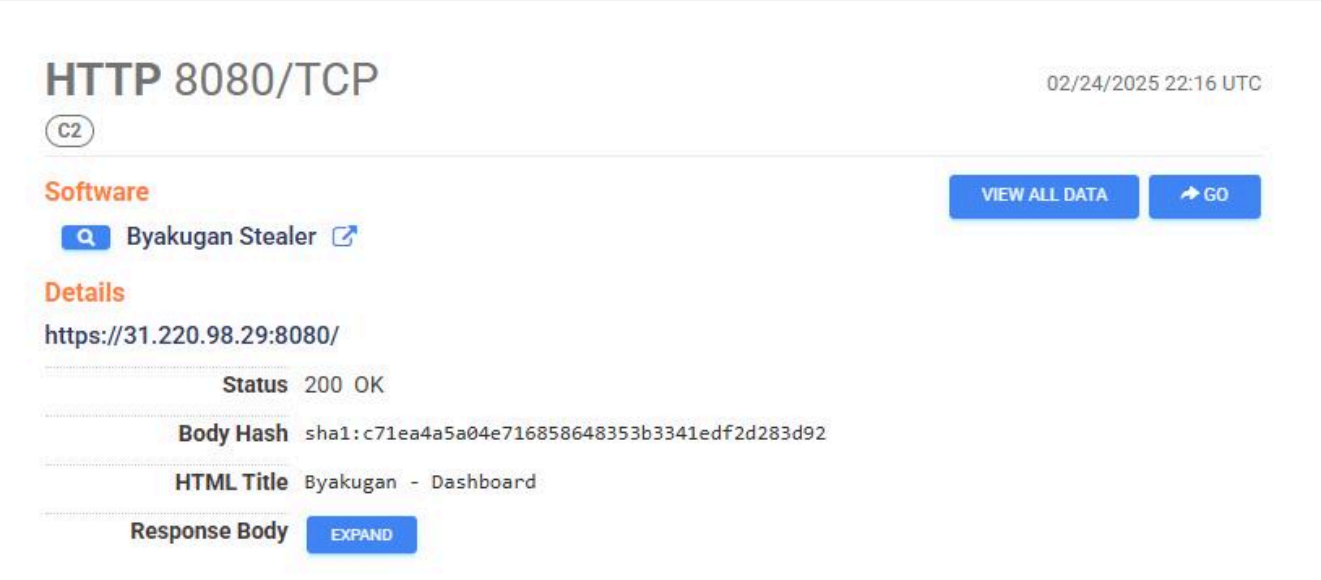


Figura 12 – Identificación de Byakugan mediante análisis de IP

Al acceder a los paneles encontrados, se puede verificar que cuentan con una pantalla de inicio de sesión y que el registro de nuevos usuarios requiere un código de invitación.

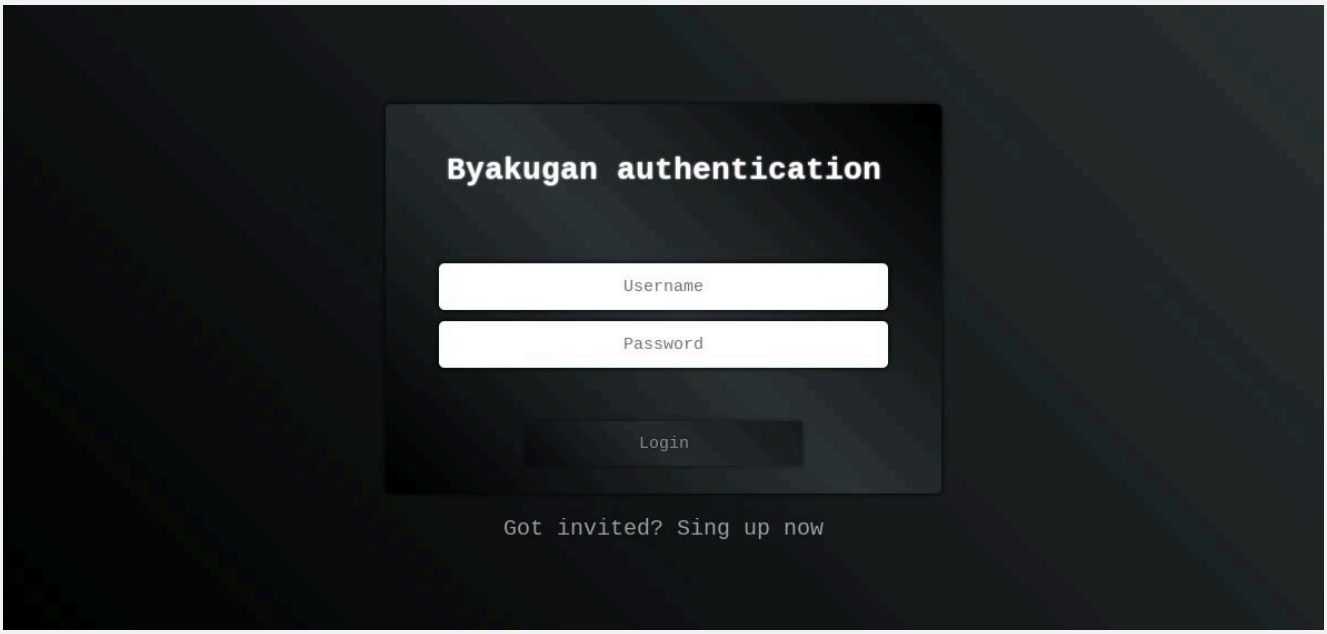


Figura 13 – Panel de inicio de sesión de Byakugan

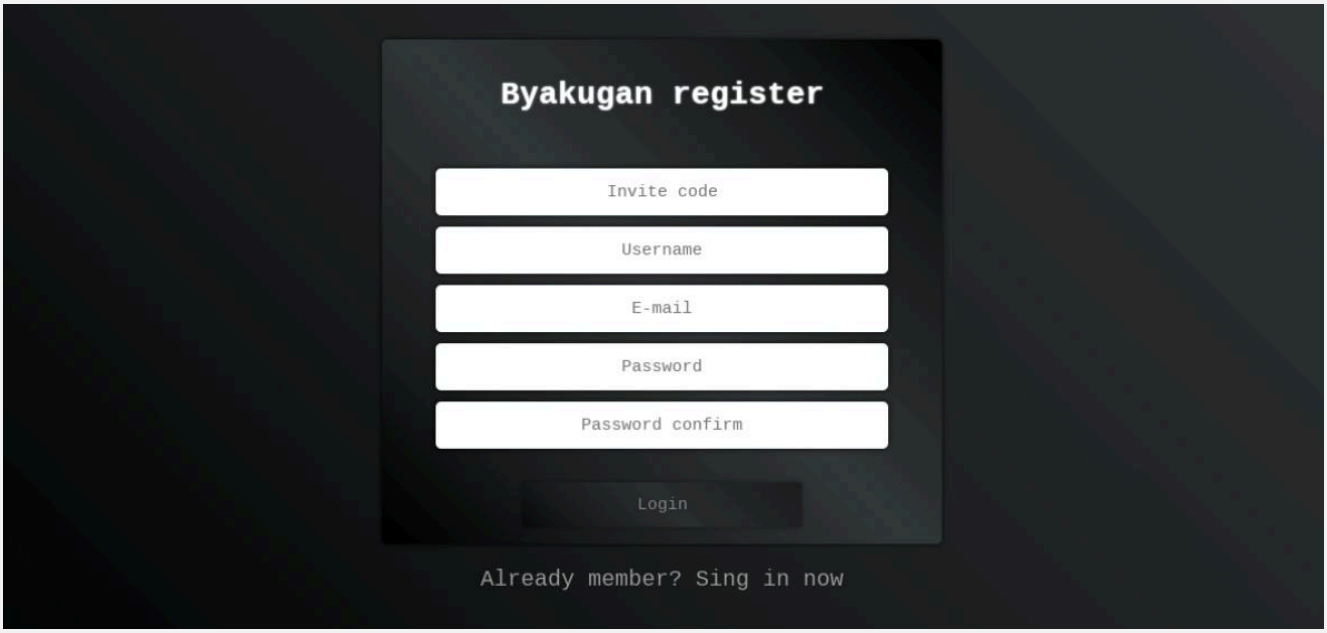


Figura 14 – Pantalla de registro de Byakugan

Se encontró un video alojado en Vimeo por el usuario Wellington Souza, publicado el 13 de septiembre de 2022, que contiene una demostración del uso del panel de control. El video está disponible en el siguiente enlace: hxxps://vimeo[.]com/749297709

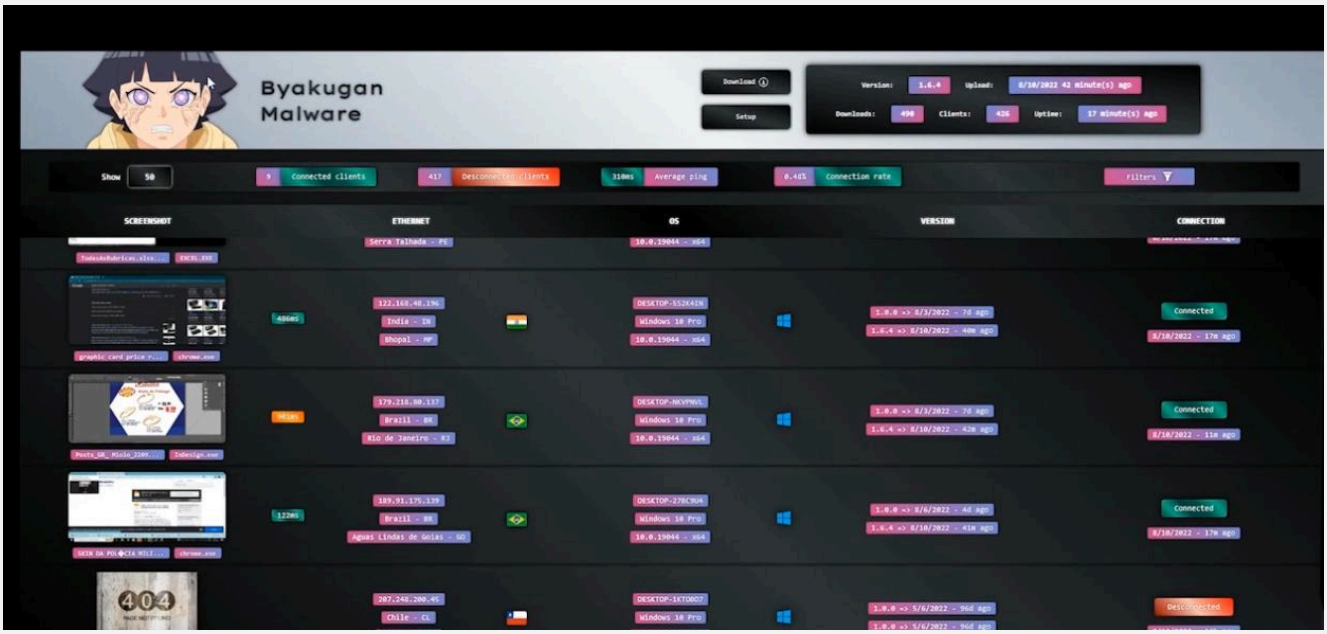


Figura 15 – Panel de control de Byakugan

En el video se muestran tanto la pantalla con los dispositivos infectados como la interfaz que presenta las acciones que pueden ejecutarse en cada uno de ellos.

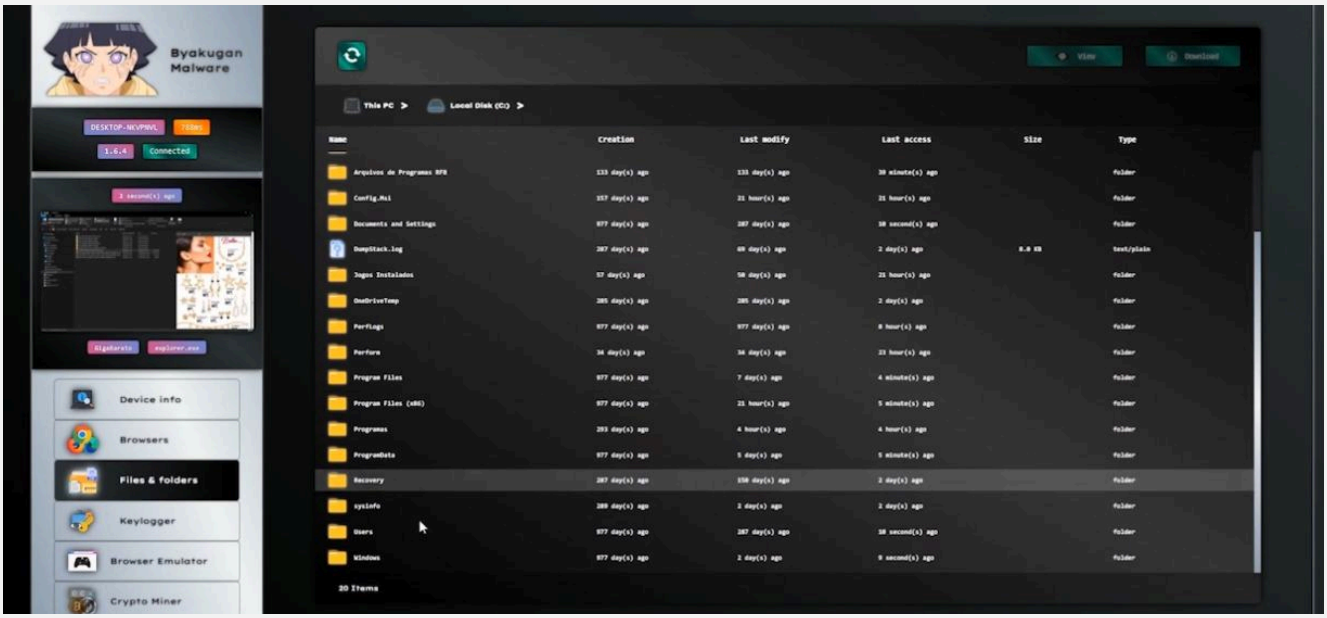


Figura 16 – Panel de dispositivos infectados y acciones disponibles

Entre las acciones que pueden ejecutarse tras la infección se encuentran la captura de información del sistema y de los navegadores, el listado de archivos y directorios, la emulación de navegador, así como funcionalidades de keylogger y minería de criptomonedas.

MITRE ATT&CK

Tácticas	Técnicas
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

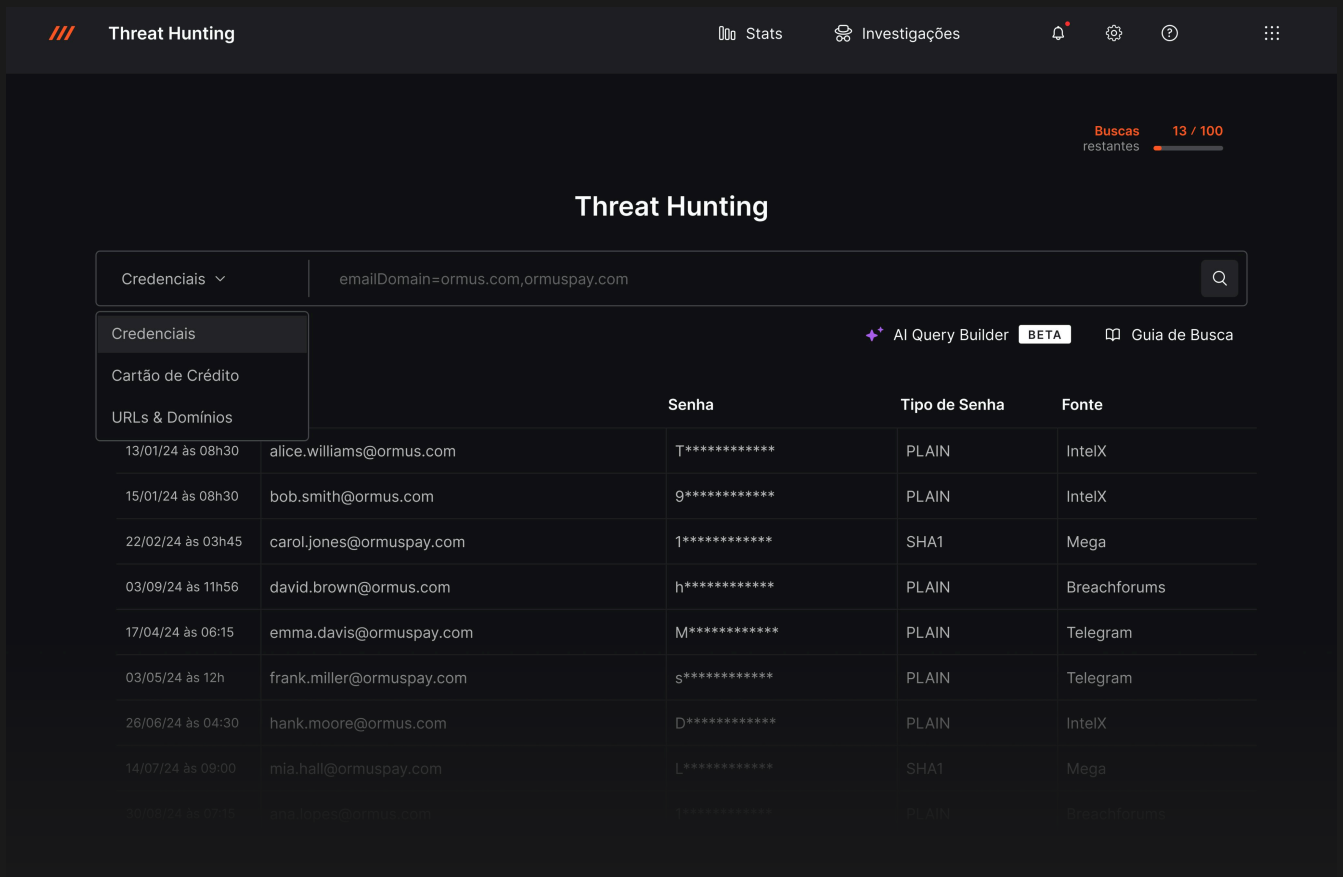
C2 Server

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



Sobre Axur

Axur es la empresa líder de ciberseguridad externa que empodera a los equipos de seguridad de la información para gestionar amenazas más allá del perímetro. Nuestra plataforma detecta, inspecciona y responde a la suplantación de marca, estafas de phishing, menciones en la deep & dark web, vulnerabilidades, exposiciones y más.

Con flujos automatizados y el mejor takedown del mercado funcionando 24/7, Axur elimina contenido malicioso de manera rápida y eficiente, gestionando el 86% de las detecciones automáticamente. Nuestras herramientas potenciadas por IA escalan la inteligencia de amenazas x180 veces, liberando a su equipo para que se concentre en iniciativas estratégicas.

Descubra cómo transformar la estrategia de seguridad de su organización

AGENDE UNA DEMO

Gartner Peer Insights. 4.9 ★★★★★

Explore todas nuestras soluciones: **axur.com**

///AXUR