Byakugan 2025:

malware altamente evasivo mira setor financeiro e cripto

AXUR

Em 2025, pesquisadores da Axur Research Team (ART) identificaram uma nova campanha de phishing brasileira distribuindo uma variante altamente evasiva do malware Byakugan. Essa versão do trojan apresenta um baixo índice de detecção em soluções antivírus, tornando-se uma ameaça significativa para empresas de todos os setores.

Os operadores dessa campanha exploram técnicas avançadas de engenharia social e phishing, utilizando infraestruturas comprometidas para simular comunicações legítimas de fornecedores. Dessa forma, conseguem enganar vítimas e induzi-las a executar arquivos maliciosos. Além disso, evidências indicam que o adversário emprega mecanismos de ofuscação e anti-análise, dificultando a detecção e a engenharia reversa do malware.

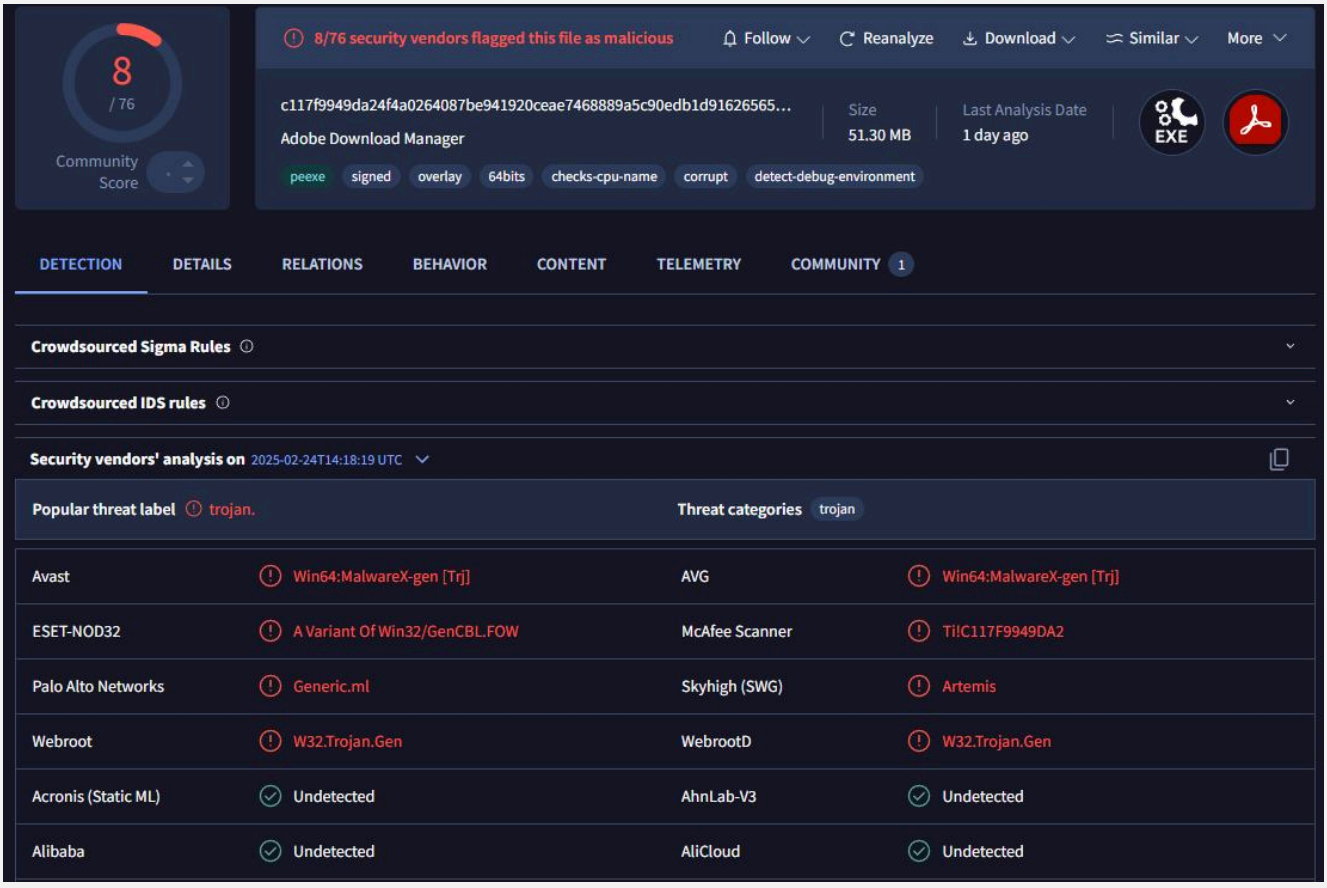
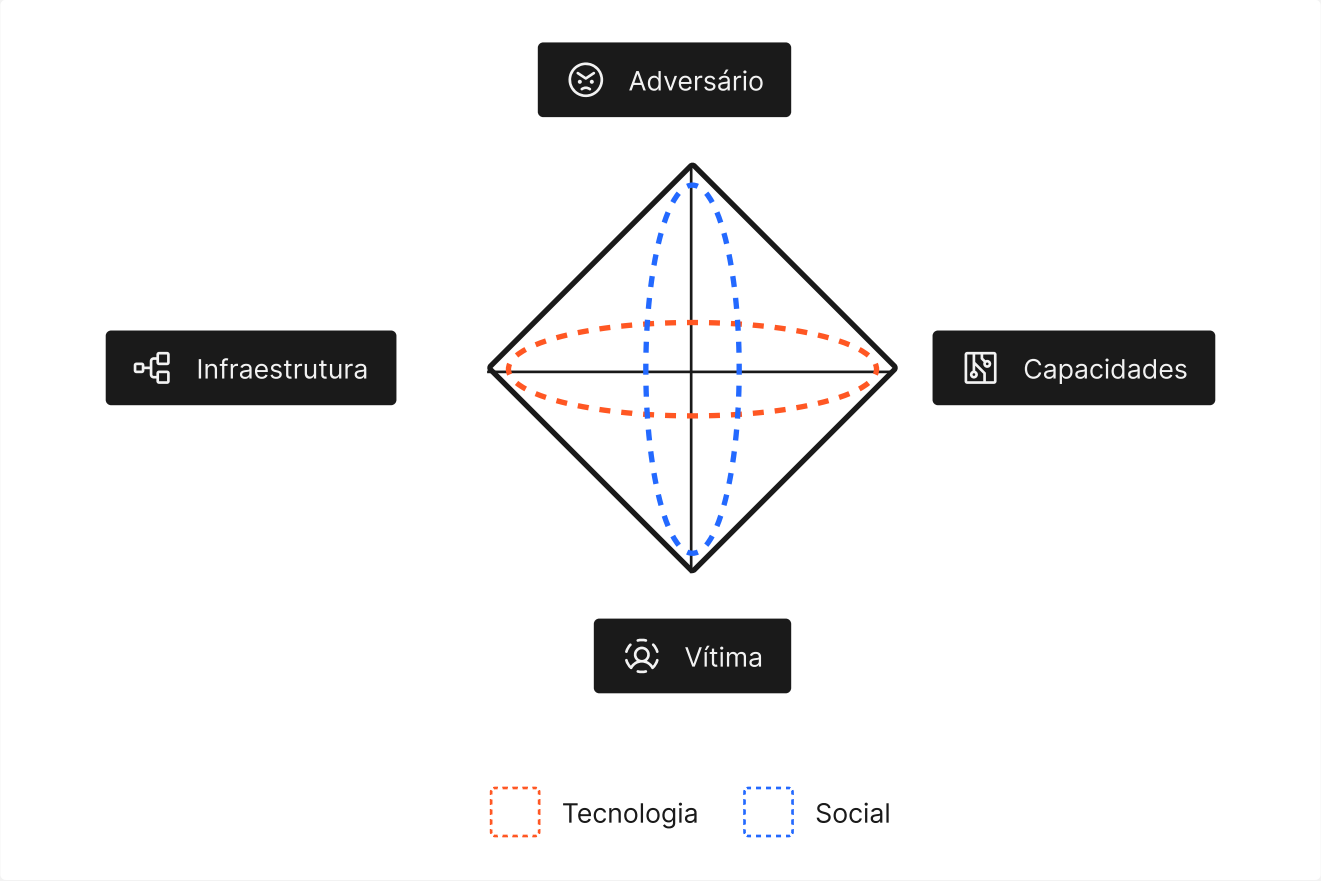


Imagem 1 - detecção do arquivo malicioso



Adversário	Operador Byakugan Stealer
Vítima	Empresas do setor financeiro e criptomoedas
Infraestrutura	Servidores de C2, malwares indetectáveis e infraestruturas comprometidas.
Capacidades	Habilidades em técnicas de phishing como envio de e-mails utilizando técnicas de engenharia social, habilidades técnicas de manipulação de arquivos maliciosos, e manipulação do malware para evitar que seja feita a engenharia reversa em máquinas virtuais. Servidores de C2. Utilização de infraestrutura comprometida para simulação de fornecedores e possíveis ataques de supply chain.

Embora os indícios apontem para um desenvolvedor brasileiro, a campanha não está restrita ao Brasil, com infecções registradas em países como Ucrânia, Estados Unidos, Holanda e Alemanha. Este relatório analisa em detalhes os vetores de ataque, a infraestrutura utilizada e as capacidades do Byakugan, buscando compreender seu impacto e possíveis medidas de mitigação.

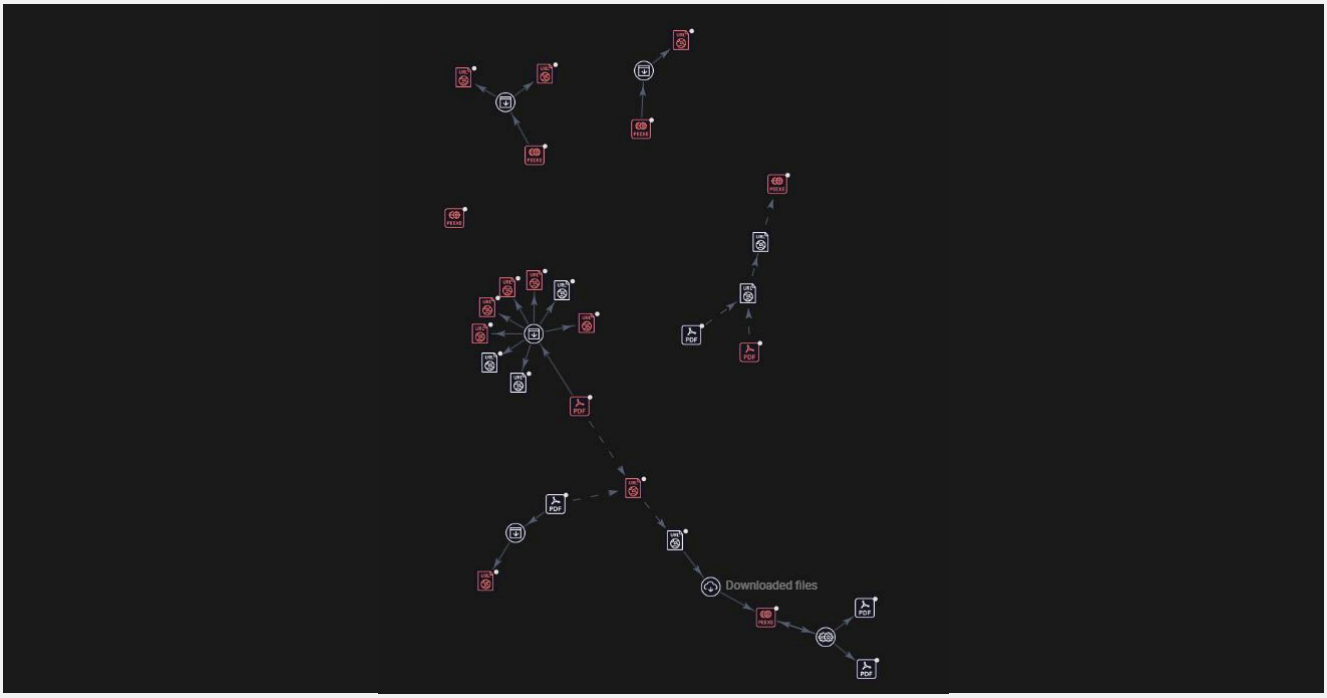


Imagem 2 - Mapa da campanha

O time ART identificou conexões diretas entre repositórios de código, infraestruturas de comando e controle (C2) e arquivos maliciosos utilizados na operação. A estrutura da campanha sugere um alto grau de sofisticação, combinando técnicas avançadas de phishing, evasão de análise e utilização de infraestrutura comprometida para mascarar suas atividades.

A campanha tem início por meio de e-mails de phishing enviados a partir de empresas comprometidas, explorando a confiança das vítimas na legitimidade do remetente. O ataque se aproveita de um contexto corporativo ao falsificar uma suposta nota fiscal, alegadamente gerada para pagamento no CNPJ da empresa-alvo.

A Figura 3 exibe um PDF falso, escrito em português, que contém uma mensagem instruindo o usuário a baixar e instalar uma suposta versão do Adobe Reader. A mensagem engana o usuário, afirmando que o download é necessário para visualizar o arquivo.

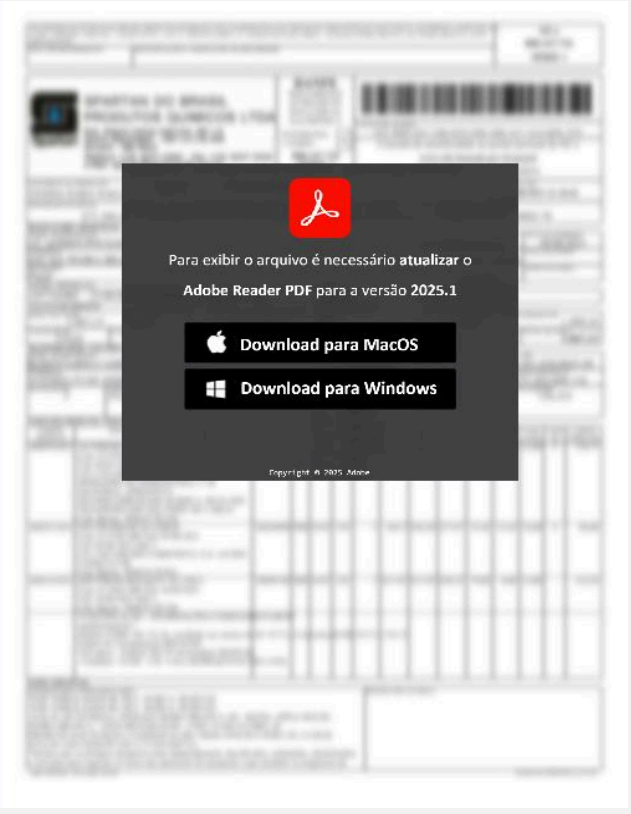


Imagem 3 - arquivo PDF malicioso

O Ator malicioso abusa de encurtadores URL para ofuscar a URL original do download. Após clicar no botão como mostrado na imagem 3, o usuário é redirecionado para uma das seguintes páginas:

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

No qual será redirecionado para uma página de download do github como mostra a url a seguir:

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

O arquivo baixado assume a forma do ícone do Adobe Reader e seu nome é definido como Reader_2025_instal.exe. Ao se disfarçar como o instalador do Adobe Reader, ele induz o usuário a executá-lo.

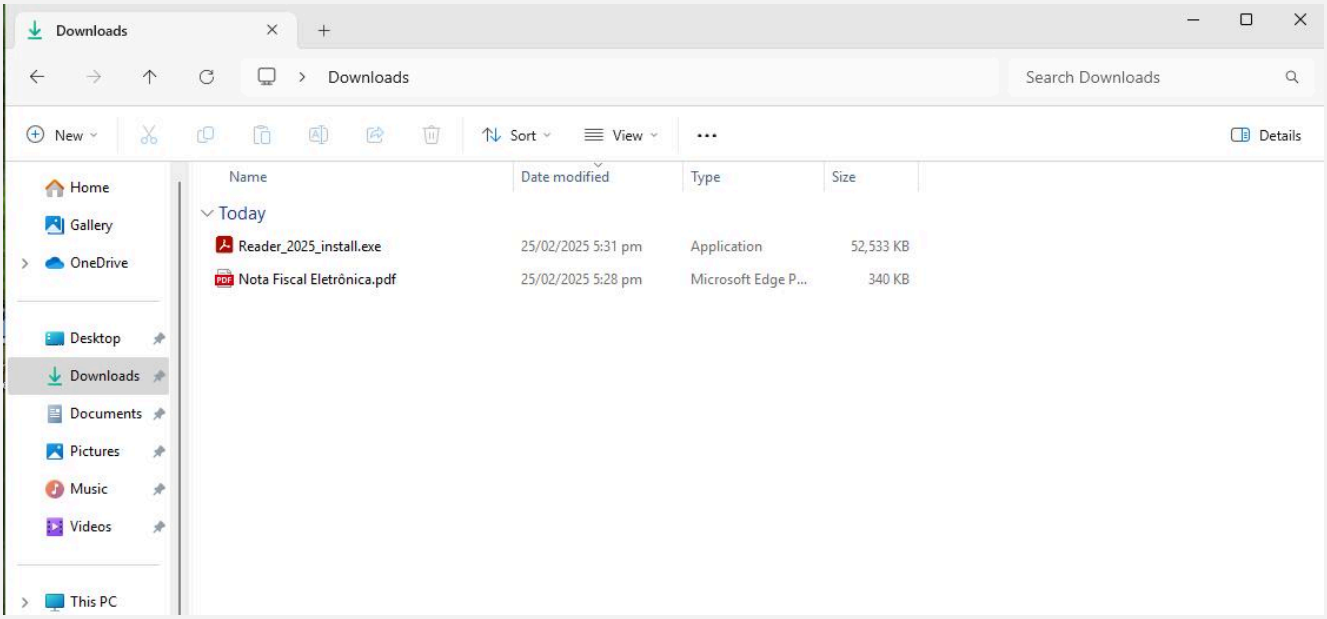


Imagem 4 - arquivos baixados

O malware Byakugan foi analisado pela Axur em 2023 e por Fortinet e Ahnlab em 2024. O fluxo de funcionamento do Malware pode ser compreendido na figura abaixo:

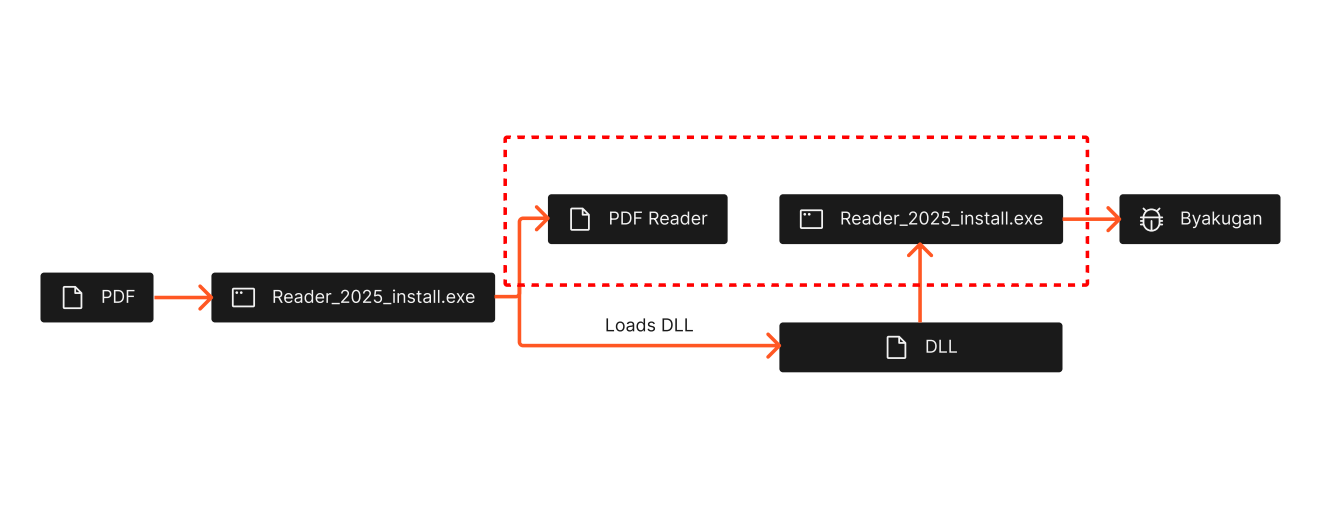


Imagem 5 - cadeia do ataque

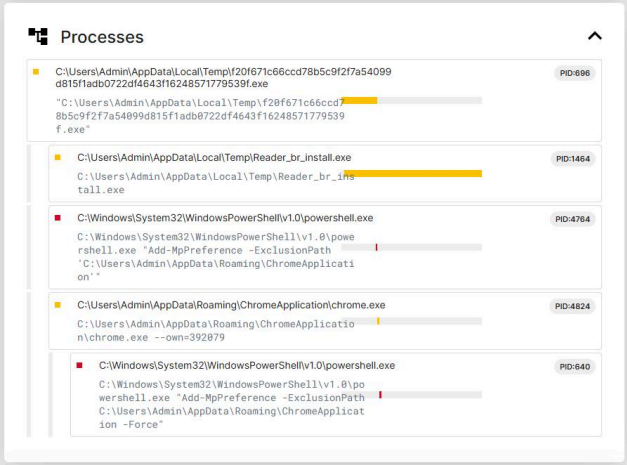


Imagem 6 - Execução do Malware

Possuindo as mesmas três fases de execução:

1. Criação do arquivo em PDF que aloca o Malware

2. DLL Hijacking & UAC Bypass

3. Vazamento das informações

A imagem demonstra que, durante a execução do Malware, uma cópia dele é transferida para a pasta “\\\\Temp”, onde recebe novas instruções. O Malware inclui uma exceção no Windows Defender e executa um processo “chrome.exe” que é o Byakugan Malware.

Imagem 7 - conexões TCP feitas pelo arquivo

Analisando ambas URLs tunneleep[.]com.br e floravirtual[.]com.br no qual o malware se comunica, observamos que a primeira não possui nenhuma detecção no VirusTotal, já a segunda possui um baixo nível de detecção. Abaixo podemos observar o grau de detecção das URLs como os IPs por trás dos domínios.

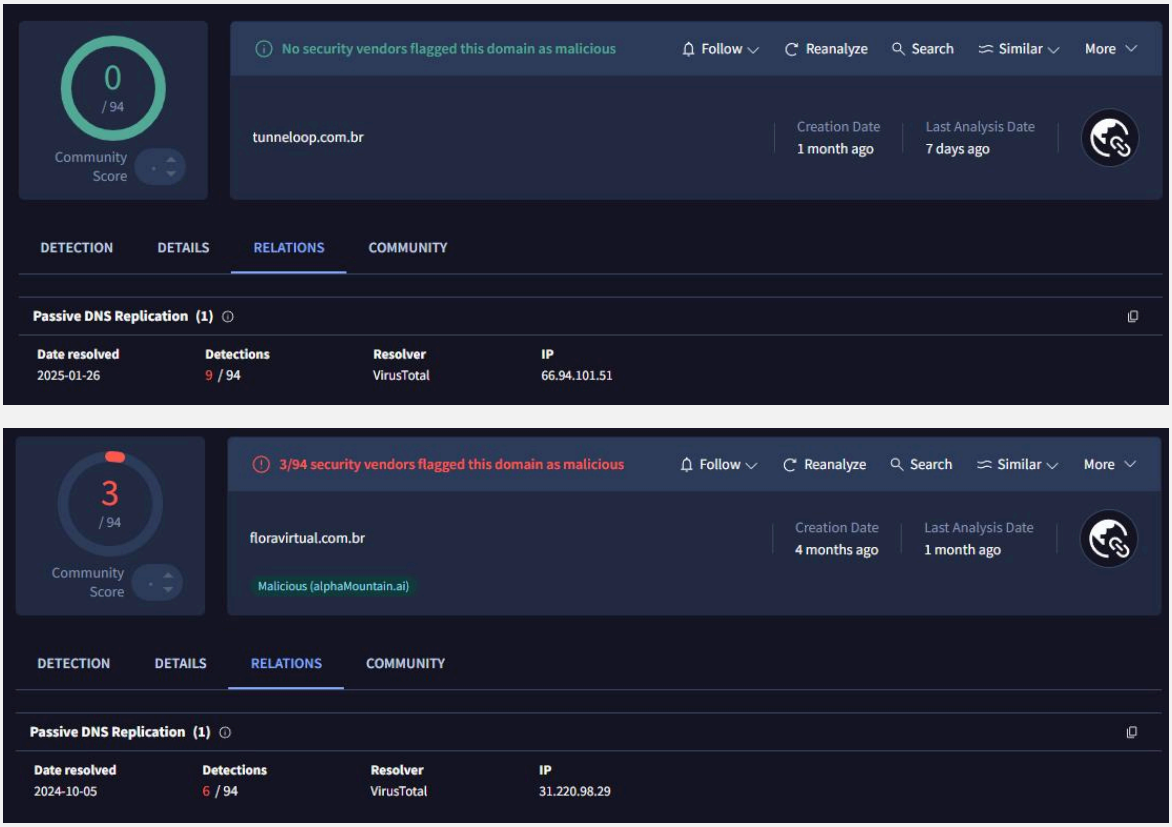
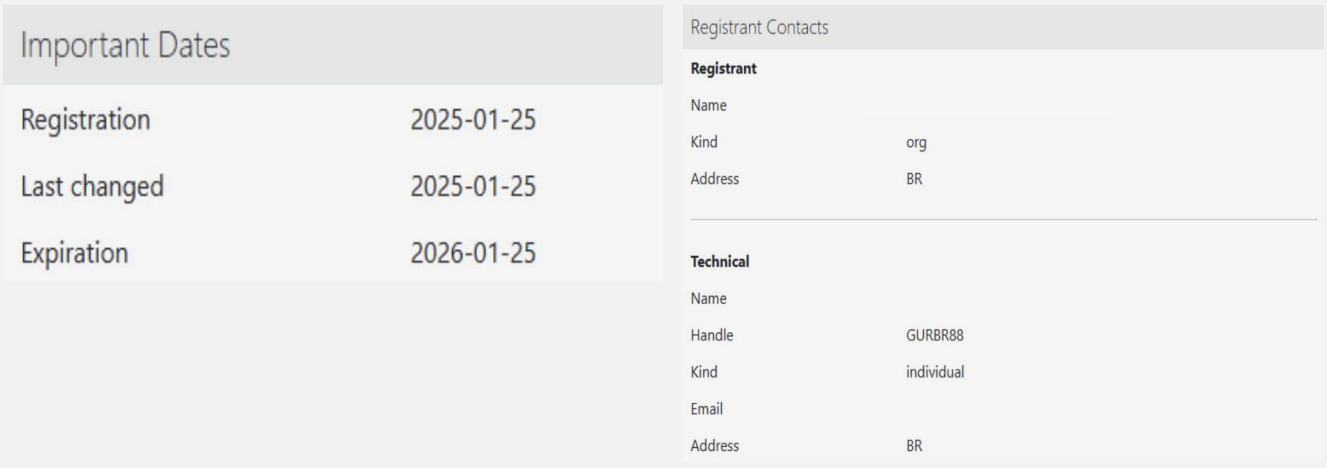


Imagem 8 - VT dos servidores de comando e controle

Verificando as informações do WHOIS é possível identificar os responsáveis, bem como os seus e-mails de contato. Importante notar também que o domínio tunneleep[.]com.br foi registrado em 25/01/2025 e o domínio floravirtual[.]com.br foi registrado em 03/10/2024.



Important Dates

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

Registrant Contacts

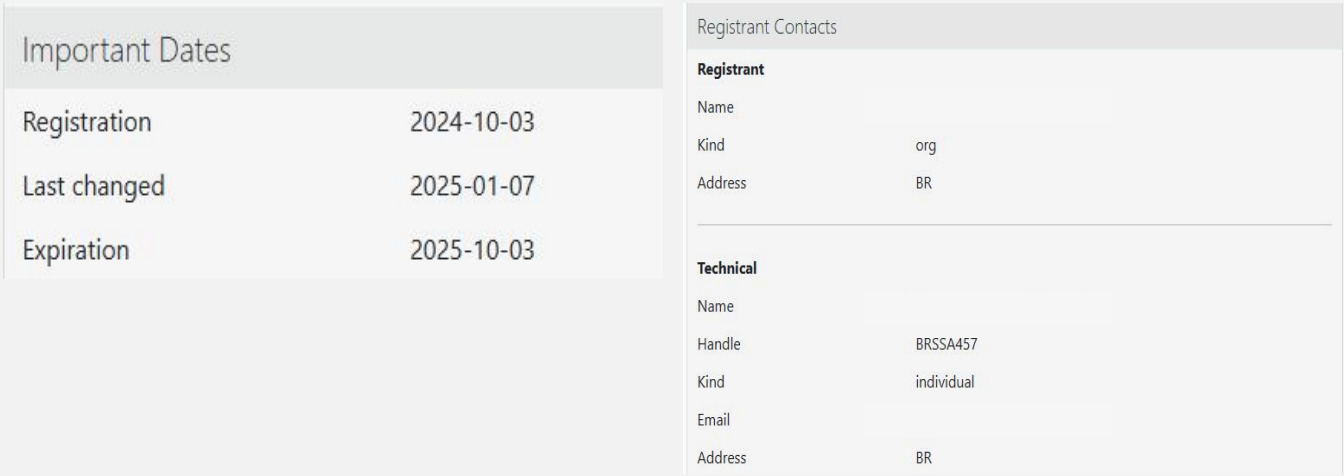
Registrant

Name	
Kind	org
Address	BR

Technical

Name	
Handle	GURBR88
Kind	individual
Email	
Address	BR

Imagem 9 - Resultado do Whois 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

Imagem 10 - Resultado do Whois floravirtual[.]com.br

Analisando ambos endereços IP 66.94.101[.]51 e 31.220.98[.]29, observamos que a porta 8080 está executando o servidor de comando e controle do Byakugan.

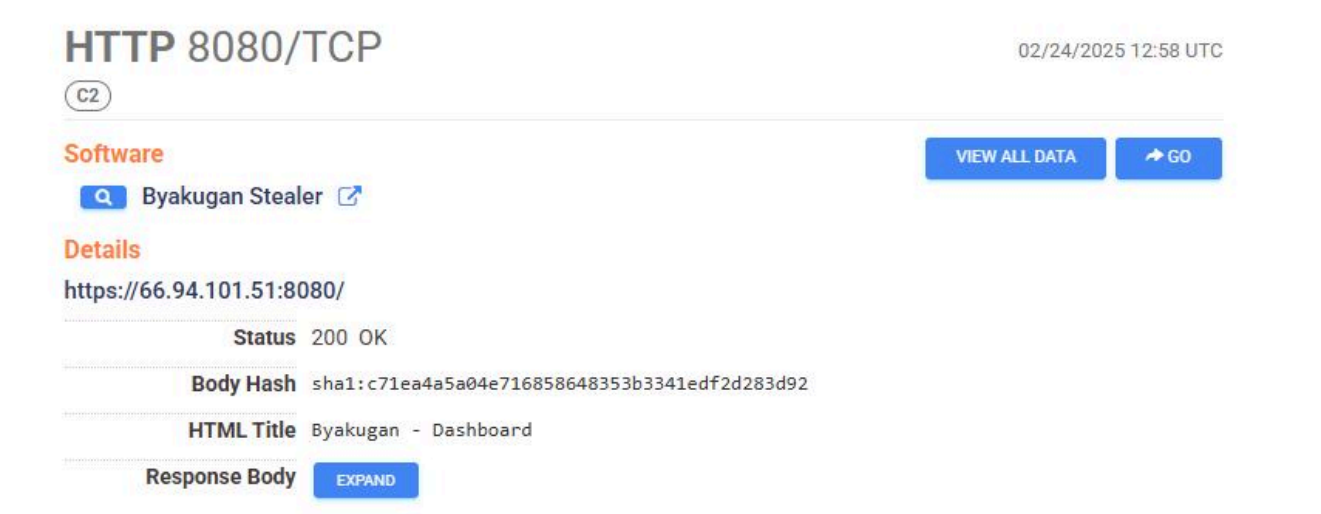


Imagem 11 - Descoberta do Byakugan através do endereço IP

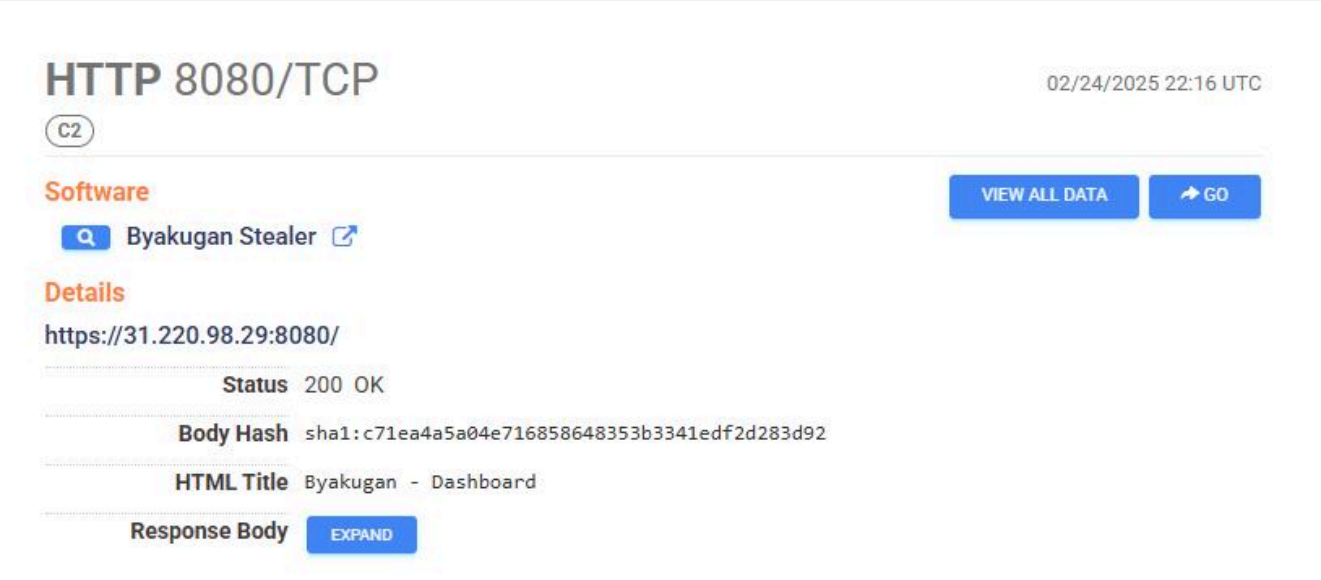


Imagem 12 - Descoberta do Byakugan através do endereço IP

Acessando os dashboards encontrados, é possível verificar que o mesmo possui uma tela de login, e que a opção de cadastro é feita mediante um código de convite.

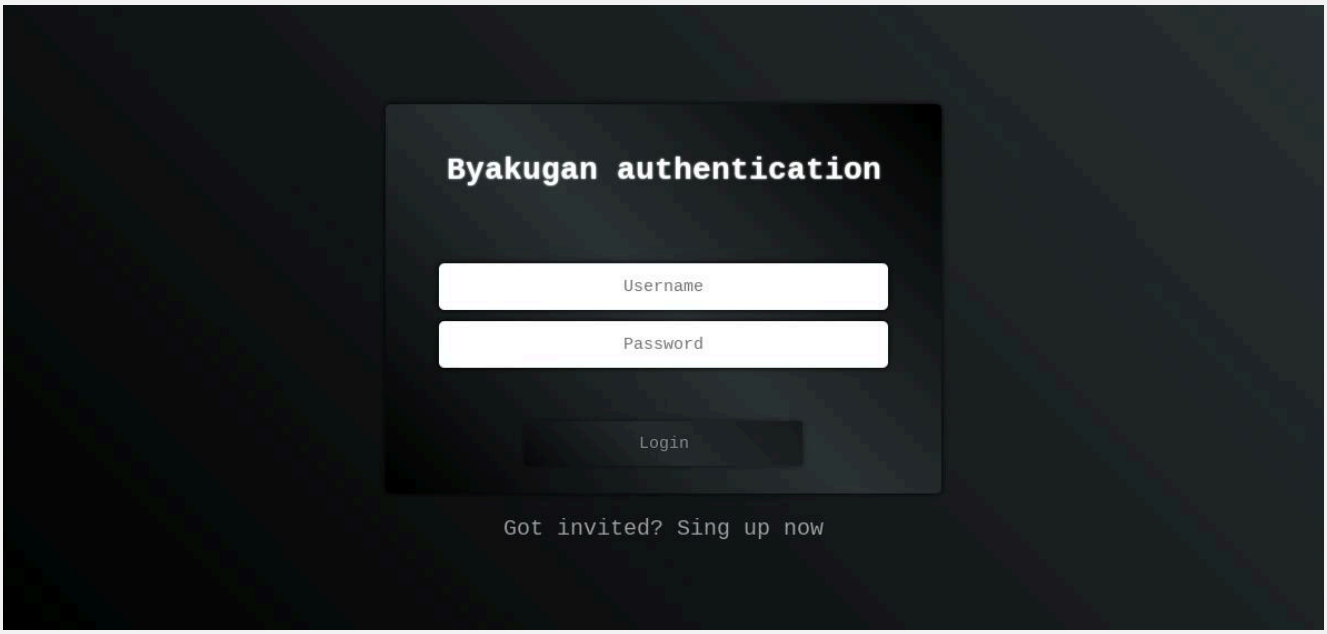


Imagem 13 - Painel de login do Byakugan

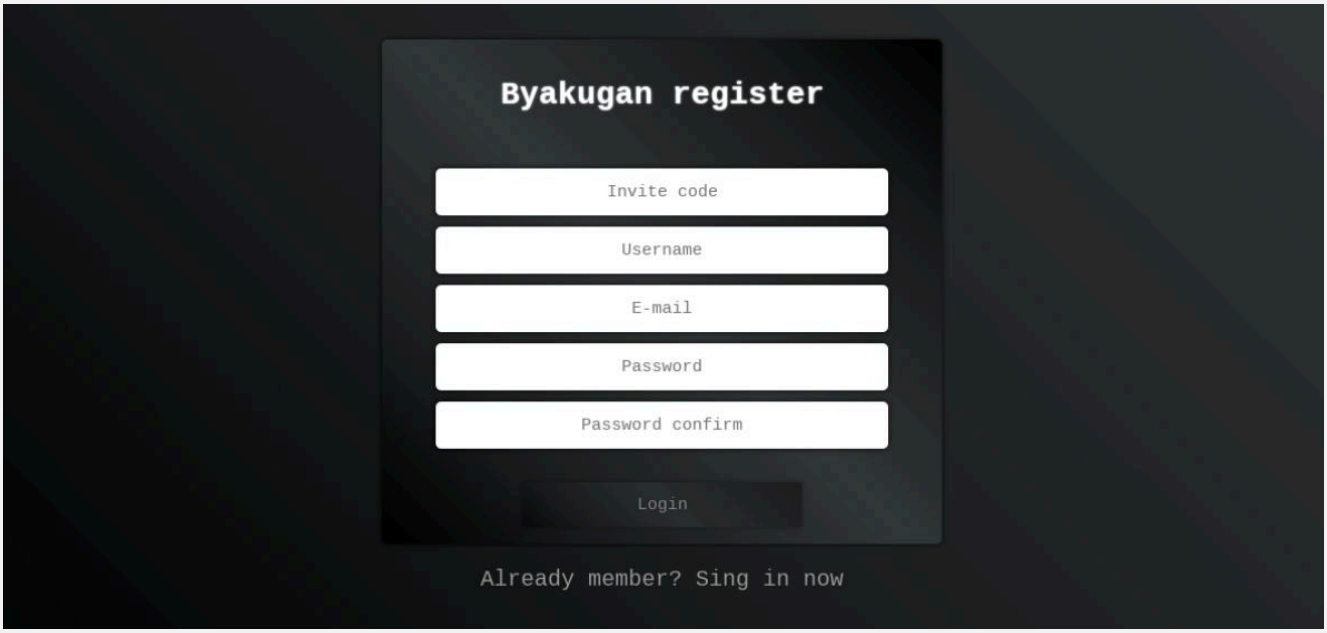


Imagem 14 - Painel de cadastro do Byakugan

Foi encontrado um vídeo hospedado no Vimeo pelo usuário wellington souza, o qual foi enviado em 13 de setembro de 2022 e nele contém uma demonstração da utilização do dashboard. O vídeo está disponível pelo link hxxps://vimeo[.]com/749297709.

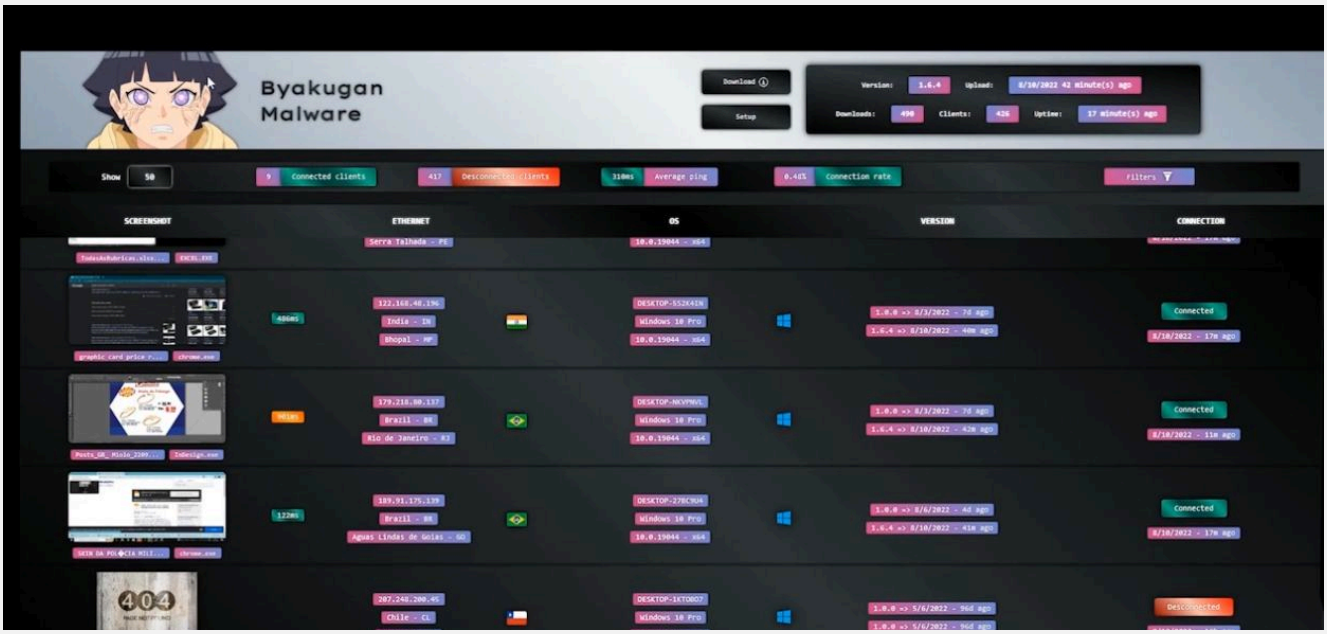


Imagem 15 - Painel do Byakugan

No vídeo são mostradas tanto a tela onde aparecem os dispositivos infectados, quanto a tela onde mostram as ações que podem ser realizadas em cada dispositivo.

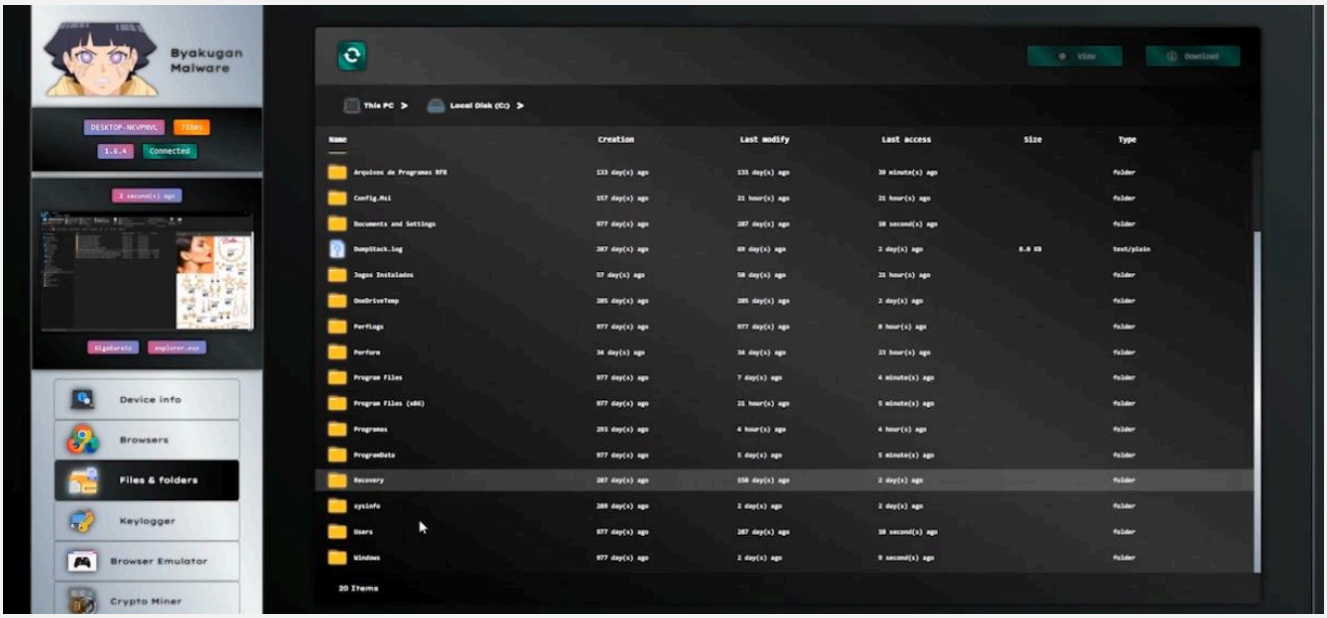


Imagem 16 - Painel do Byakugan

Dentre as opções de ações que podem ser realizadas após a infecção estão as capturas de informação da máquina e dos navegadores, a listagem de arquivos e diretórios, a emulação de navegador, e as funcionalidades de keylogger e de mineração de criptomoedas.

MITRE ATT&CK

Táticas	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

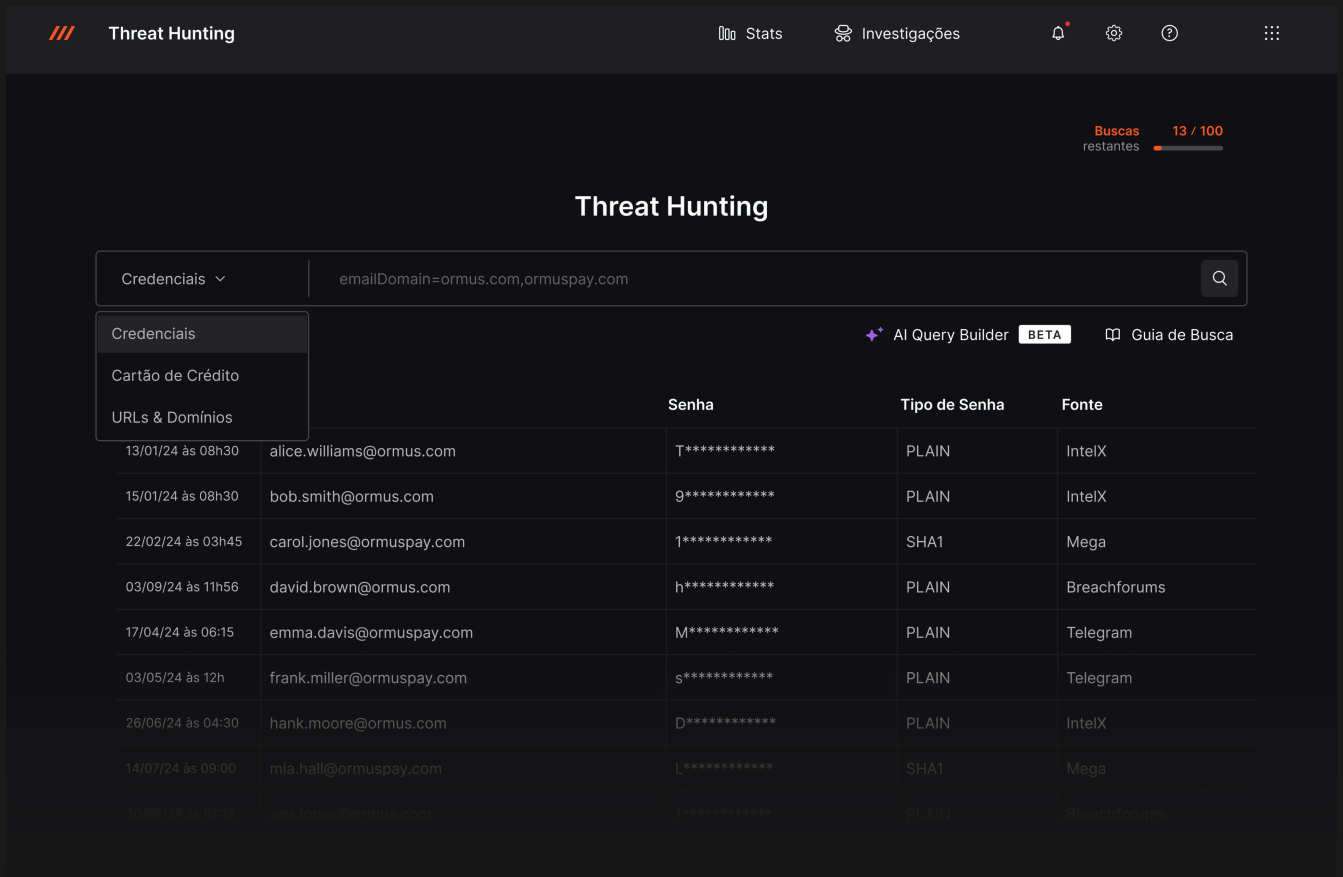
C2 Server

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 a Axur

A Axur é uma solução líder em cibersegurança externa que empodera equipes de segurança para tratar ameaças fora do perímetro. Nossa plataforma detecta, inspeciona e responde a fraudes digitais, phishing, menções na deep & dark web, vulnerabilidades e mais.

Com fluxos automatizados e o melhor takedown do mercado, a Axur remove conteúdo malicioso de forma rápida e eficiente, 24×7, gerenciando 86% das detecções sem toque humano. Nossas soluções utilizam Inteligência Artificial para escalar a inteligência de ameaças 180 vezes, liberando a sua equipe para se concentrar nas iniciativas mais estratégicas.

Descubra como nossas soluções irão transformar sua estratégia de segurança

AGENDE UMA DEMO

Gartner Peer Insights 4.9

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

///AXUR