

Anatomy of BraZetsu: How Cybercriminals Fuel the Underground Ecosystem

By Julio Guapo Menezes, Miguel Salazar

Published: 2026-08-31 · Archived: 2026-09-03 02:00:33 UTC



Introduction

The [Group-IB Threat Intelligence](#) team has identified BraZetsu, a sophisticated Python-based Windows malware framework that we attribute, with high confidence, to the Brazilian threat actor known as Exilware. Unlike the standard infostealer model, BraZetsu is a comprehensive master toolkit that empowers Initial Access Brokers (IABs) by turning compromised systems into highly valuable commercial assets. The framework exhibits high operational maturity, utilizing a modular architecture and stealth techniques that allowed some samples to remain fully undetectable on VirusTotal at the time of analysis.

BraZetsu's operational scope is specifically calibrated to target Iberian and Latin American targets in corporate, financial, industrial, law enforcement, and other environments. Notably, the malware employs deep reconnaissance capabilities to scan for standardized financial remittance files, such as those in the Brazilian CNAB format, and extracts detailed browser histories to map victim activity. The framework's codebase and operational logs indicate heavy reliance on generative AI, not only for development but potentially also for backend data triage and target prioritization. This technique distinguishes it from traditional threats currently active in the Latin American landscape.

This framework is the primary technical engine behind the "Infected Marketplace" (also known as "Banco de Infects"), a platform where Exilware commercializes initial access to compromised hosts. By functioning as a service-enabled platform, the marketplace allows criminal customers to remotely execute secondary malicious payloads on purchased access, creating a persistent threat-multiplier effect across the regional ecosystem.

Our analysis tracks BraZetsu's evolution from February 2026, documenting a rapid technical progression from basic remote access functionality to the current, AI-enhanced intelligence-gathering platform. This report details the framework's technical components, its integration with the Infected Marketplace, and the strategic implications of this AI-driven threat model for organizations operating within the Iberian and LATAM landscape.

Key discoveries

- BraZetsu is a malicious framework supporting Initial Access Broker (IAB) operations. It allows cybercriminals to conduct extensive reconnaissance on compromised systems.

- The malware scans banking, ERP, e-commerce, industrial (SCADA), and other systems to identify high-value assets.
- The emojis in the codebase and the verbose logging suggest extensive AI employment during the development lifecycle.
- BraZetsu is a stealthy malware framework that steals sensitive data from compromised machines, including browser history, financial files (CNAB), and digital certificates, which is then monetized through the Infected Marketplace.

Who may find this blog interesting:

- Cybersecurity analysts and corporate security teams
- Malware analysts
- Threat intelligence specialists
- Cyber investigators
- Computer Emergency Response Teams (CERT)
- Law enforcement investigators
- Cyber police forces

Group-IB Threat Intelligence Portal: ExilWare / BraZetsu

Group-IB customers can access our Threat Intelligence portal for more information about BraZetsu, Exilware, and other topics mentioned within this blog.

- [BraZetsu Malware](#)
- [Infect Marketplace](#)
- [Exilware](#)
- [CNABHunter](#)

Public Malware Detonations

Access free detonation reports linked to BraZetsu and watch malware operate in real time through detailed insights from the [Group-IB Malware Detonation Platform](#):

- [BraZetsu Detonation Report](#)

Threat Actor Profile



Exilware

First seen

02 February 2026

Exilware is a Brazilian, financially motivated adversary allegedly responsible for administering Infect Marketplace. Based on its activity in Telegram groups and its domain registration date, Exilware has been active under this moniker since February 2026.

The cybercriminal's historical activity suggests an established capability to advertise bulk spam distribution services through Telegram. Furthermore, your victim list on the Infected Marketplace has primarily featured compromised hosts located in Spanish and Portuguese-speaking countries.

Toolset

Brazetsu Malware Telegram
Infect Online Marketplace

Skillset

Spammer Vibe coding Malware Development
Initial Access Broker Windows-based targets

Motivation

Financial gain

Targeted Countries

Brazil Portugal Spain
Argentina Paraguay

Modus Operandi

The marketplace functions as an access-as-a-service operation, in which other criminals can purchase entry points into victims' systems. Once a criminal purchases access through the marketplace, they can deploy malicious payloads via a specialized platform feature. This allows buyers to remotely execute their own malware or tools on the compromised systems without needing to establish the initial foothold themselves.

This business model is powered by the BraZetsu malware framework, which serves as the primary infection vector for generating new inventory. Regarding Exilware's potential involvement in malware development, a message he posted in the Infect Marketplace Telegram group indicates he provided maintenance for the loader after it became unavailable. This activity suggests Exilware has an operational role in maintaining the loader infrastructure. However, the statement alone is insufficient to establish broader responsibility for malware development or administration.



Group-IB, 2026

Malware Profile



BraZetsu

Platforms

Windows

First seen

08 May 2026

BraZetsu is a modular Brazilian Python malware framework compiled via Nuitka. Serving as the core technical engine for the "Infected Marketplace," it operates on an access-as-a-service model, cataloging compromised systems as tradable assets for secondary threat actors.

- **AI-Driven Reconnaissance:** Scans infected hosts and uses generative AI to triage data, prioritizing high-value targets for Initial Access Brokers (IABs).
- **Continuous Exfiltration:** Harvests digital certificates, browser history, and financial files while tracking user behavior through screen captures.
- **Banking File Extraction:** Specifically hunts for corporate financial remittance files in the Brazilian Federation of Banks' CNAB format.
- **WebSocket C2 Infrastructure:** Relies on the WebSocket protocol to maintain persistent communication with the Infected Marketplace.

Used by

Exilware

Techniques

T1204.002 - User Execution: Malicious File

T1059.001 - Command and Scripting Interpreter: PowerShell

T1059.003 - Command and Scripting Interpreter: Windows Command Shell

T1547.001 - Boot or Logon Autostart Execution: Registry Run Keys / Startup Folder

T1027.002 - Obfuscated Files or Information: Software Packing

T1564.003 - Hide Artifacts: Hidden Window

T1012 - Query Registry

T1518 - Software Discovery

T1082 - System Information Discovery

T1016 - System Network Configuration Discovery

T1046 - Network Service Discovery

T1083 - File and Directory Discovery

T1010 - Application Window Discovery

T1217 - Browser Information Discovery

T1113 - Screen Capture

T1071.001 - Application Layer Protocol: Web Protocols



Group-IB, 2026

From the Underground to the Spotlight

Dissecting the BraZetsu Framework

Overlaps and Stumbles: Two tools with different goals

During continuous threat monitoring operations conducted by Group-IB's Threat Intelligence team, the BraZetsu framework was identified due to overlapping characteristics with a malicious fraud-enabling tool known as CNABHunter, which a security researcher initially disclosed in a [Twitter/X post](#) on 7 May 2026. [For more details about CNABHunter, visit our Threat Intelligence portal.](#)

The connection between these two campaigns remains unknown at the time of this report. However, the two malware families share similarities because they target specific directory paths where business management (ERP) solutions typically store financial remittance files. These remittance files are an automated way for businesses to bulk-transmit daily financial instructions to a bank without entering them individually. Such files follow the

Centro Nacional de Automação Bancária (CNAB) file format established by the Federação Brasileira de Bancos (FEBRABAN).

RETROHUNT MATCHES							
		Rule	Detections	Size	First seen	Last seen	Submitters
6a5db602b9f4e59a3393c4d0af9c4f80104e8c3d71e...	cliente.dll	CNABHunter Sample	38 / 69	12.73 MB	2026-05-07 05:22:31	2026-05-12 01:21:50	2
54e313434a7f3fa349e439857e23ab536a95c9927cf...	temp_agente.dll	BraZetsu Sample	0 / 72	18.74 MB	2026-05-08 21:37:25	2026-05-08 21:37:25	1

Figure 1. Retrohunt matches common remittance paths.

81	"C:\\TOTVS\\Protheus_Data\\outbox",	1327	"%USERPROFILE%\\Downloads",
82	"C:\\TOTVS\\Protheus_Data\\system",	1328	"%USERPROFILE%\\Desktop",
83	"C:\\TOTVS\\Protheus_Data\\workflow",	1329	"%USERPROFILE%\\Documents",
84	"C:\\CorporerM\\GeracaoBancaria",	1330	"%USERPROFILE%\\AppData\\Local\\Temp",
85	"C:\\CorporerM\\RM.Net\\Remessas",	1331	"%USERPROFILE%\\AppData\\Local\\Google\\Chrome\\User Data\\Default\\Downloads",
86	"\\\\SERVERIDOR\\Protheus_Data\\outbox",	1332	"%USERPROFILE%\\AppData\\Local\\Microsoft\\Edge\\User Data\\Default\\Downloads",
87	"\\\\SERVERIDOR\\CorporerM\\GeracaoBancaria",	1333	"C:\\Users\\Public\\Downloads",
88	"\\\\SERVERIDOR\\TOTVS\\Remessa",	1334	"C:\\Users\\Public\\Documents",
89	"C:\\TOTVS12\\bin\\appserver\\remessa",	1335	"C:\\TOTVS\\Protheus_Data\\outbox",
90	"C:\\TOTVS12\\bin\\appserver\\retorno",	1336	"C:\\TOTVS\\Protheus_Data\\system",
91	"C:\\Program Files\\SAP\\SAP Business One\\AddOns\\Bancos",	1337	"C:\\TOTVS\\Protheus_Data\\workflow",
92	"C:\\B1_SHR\\Attachments",	1338	"C:\\CorporerM\\GeracaoBancaria",
93	"C:\\B1_SHR\\BankFiles",	1339	"C:\\CorporerM\\RM.Net\\Remessas",
94	"C:\\SAP_WorkDir",	1340	"C:\\TOTVS12\\bin\\appserver\\remessa",
95	"C:\\ProgramData\\SAP\\BankExport",	1341	"C:\\Program Files\\SAP\\SAP Business One\\AddOns\\Bancos",
96	"\\\\SERVERIDOR\\B1_SHR\\Attachments",	1342	"C:\\B1_SHR\\Attachments",
97	"\\\\SERVERIDOR\\B1_SHR\\BankFiles",	1343	"C:\\B1_SHR\\BankFiles",
98	"\\\\SERVERIDOR\\SAP_Export\\CNAB",	1344	"C:\\ProgramData\\SAP\\BankExport",
99	"\\\\SERVERIDOR\\SAP_SHR\\Remessas",	1345	"C:\\Senior\\Sapiens\\Exportacao",
100	"C:\\Users\\Public\\SAP\\Export",	1346	"C:\\Senior\\Sapiens\\Arquivos\\CNAB",
101	"C:\\Senior\\Sapiens\\Exportacao",	1347	"C:\\Sankhya\\Sankhya\\Exportacao",
102	"C:\\Senior\\Sapiens\\Arquivos\\CNAB",	1348	"C:\\WK\\Radar\\Financeiro\\Arquivos",
103	"C:\\Sankhya\\Sankhya\\Exportacao",	1349	"C:\\Mega\\Arquivos\\Bancos",
104	"\\\\SERVERIDOR\\Sankhya\\Remessas",	1350	"C:\\Alterdata\\ERP\\Remessas",
105	"C:\\WK\\Radar\\Financeiro\\Arquivos",	1351	"C:\\Nexxera\\Envio",
106	"C:\\Mega\\Arquivos\\Bancos",	1352	"C:\\Nexxera\\Arquivos\\Remessa",
107	"\\\\SERVERIDOR\\Mega\\Financeiro\\Remessa",	1353	"C:\\Banco_Brasil\\Autoatendimento",
108	"C:\\Alterdata\\ERP\\Remessas",	1354	"C:\\Bradesco\\NetEmpresa",
109	"C:\\Cigam\\Arquivos\\Bancos",	1355	"C:\\Itau\\Office\\Arquivos",
110	"\\\\SERVERIDOR\\Cigam\\Export\\REM",	1356	"F:\\Financeiro\\Remessa",
111	"C:\\WinThor\\Exportacao",	1357	"S:\\Sistemas\\Remessas",
112	"C:\\WinThor\\Bancos\\Remessa",	1358	"Z:\\Financeiro\\Remessa",
113	"\\\\SERVERIDOR\\WinThor\\Remessa",	1359	],
114	"C:\\Logix\\Financeiro\\Remessa",	1360	[
115	"\\\\SERVERIDOR\\Logix\\Arquivos\\Bancos",	1361	"TOTVS",
116	"C:\\Nexxera\\Envio",	1362	"SAP",
117	"C:\\Nexxera\\Arquivos\\Remessa",	1363	"Sankhya",
118	"C:\\Invoicy\\Remessas",	1364	"Senior",
119	"C:\\DDA\\Arquivos",	1365	"Alterdata",
120	"C:\\Banco_Brasil\\Autoatendimento",	1366	"Nasajon",
121	"C:\\Bradesco\\NetEmpresa",	1367	],
122	"C:\\Itau\\Office\\Arquivos",	1368	"ERP_INSTALL_PATHS",
123	"C:\\Inter\\APIBancaria\\Remessas",	1369	[
124	"C:\\Safe2Pay\\CNAB",	1370	".rem",
125	"C:\\PJBank\\Arquivos",	1371	".ret",
126	"F:\\Financeiro\\Remessa",	1372	".cnab",
127	"S:\\Sistemas\\Remessas",	1373	".240",
128	"Z:\\Financeiro\\Remessa",	1374	".400",
129	"P:\\Publico\\Financeiro\\CNAB",	1375	".pfx",
130	"G:\\Bancos\\Envio",	1376	".p12",
131	],	1377	],
132	"caminhos_mapeados",	1378	"FINANCIAL_EXTENSIONS",
		1379	[

Figure 2. Comparison between CNABHunter and BraZetsu remittance paths.

Beyond their targeting directories, the two strains share identical foundational technologies:

- **Programming Language:** Both are written in Python 3 (with only minor variations in the specific Python version used).
- **Compilation:** Both use Nuitka to compile their Python code into standalone executables, a technique often used to bypass traditional signature-based detection and complicate reverse engineering.

Although both artifacts contain code to locate CNAB-related files and share technologies, their architectures, operational workflows, and objectives differ significantly. CNABHunter is a purpose-built fraud tool that

systematically searches local and network directories for CNAB files, parses financial transaction records, exfiltrates payment metadata to a dedicated HTTP-based infrastructure, and continuously polls its Command and Control (C2) server for operator-issued orders. When instructed, it automatically rewrites the original CNAB files by replacing legitimate payment information with attacker-controlled banking details, PIX keys, or barcodes. This workflow is specifically designed to facilitate financial fraud against corporate payment processes.

BraZetsu, by contrast, operates as an Initial Access Broker (IAB) malware framework rather than a financial fraud tool. It establishes a persistent WebSocket connection to its C2 infrastructure, performs broad host reconnaissance to identify valuable assets, including CNAB-related files, and supports both autonomous data collection and interactive, hands-on operations through remote shell command execution. While BraZetsu can deploy additional worker modules, it does not autonomously parse, modify, or inject fraudulent payment instructions into CNAB files as part of its reconnaissance workflow.

Group-IB analysis indicates that the only notable code overlap between the two artifacts is the directory list used to locate CNAB-related files. Beyond this shared component, they rely on distinct C2 infrastructures, implement different communication protocols, and contain separate codebases that support fundamentally different operational objectives.

So, why the similarities? It all comes down to timing. BraZetsu was discovered in the wild almost immediately after the public disclosure of CNABHunter, suggesting the developers behind BraZetsu saw a profitable opportunity to upgrade their malware by directly incorporating the specific ERP directory paths that CNABHunter targets. Additionally, at the time of writing this threat report, the latest identified version of BraZetsu is fully undetectable (FUD) by VirusTotal engines.

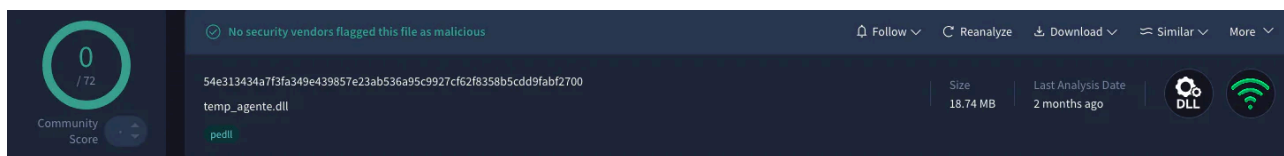


Figure 3. Two months following the discovery of BraZetsu, the framework remains fully undetectable (FUD) by VirusTotal engines.

Initial Infection Vector

While the precise mechanism of BraZetsu’s initial infection vector remains unknown, Group-IB identified a distribution domain, caixaentradas1inboxshop[.]site, by tracking filename patterns such as *msdege[0-9].exe* and *wifi_driver.exe*. These observed domain and filename patterns strongly suggest that the threat actor leveraged social engineering tactics, a common methodology among local cybercriminals in the LATAM region.

The Group-IB Threat Intelligence team named this new malware BraZetsu; “Bra” is derived from its country of origin, Brazil, and “Zetsu”, a fictional character known for orchestrating events from the shadows to pave the way for a far greater threat. Operating stealthily as an initial access tool, BraZetsu malware infiltrates networks to lay the groundwork for subsequent highly destructive attacks.

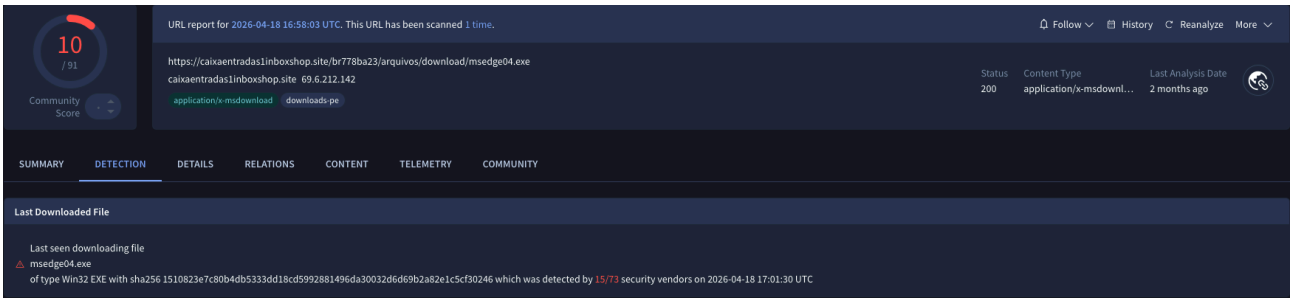


Figure 4. Infrastructure used to distribute and deliver BraZetsu loaders.

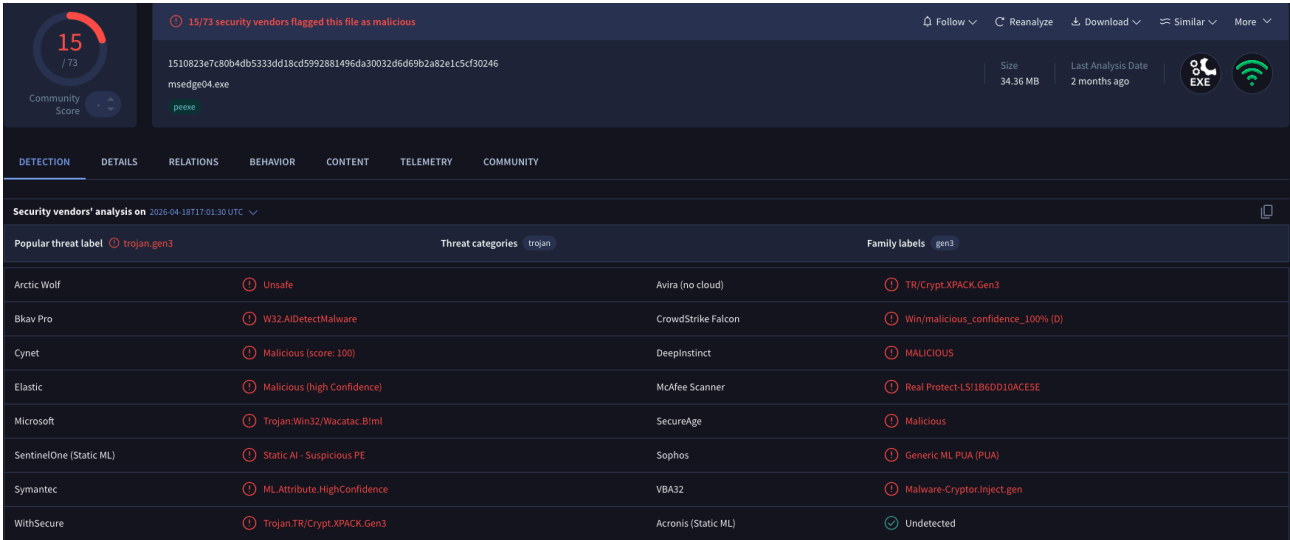


Figure 5. BraZetsu loader masquerading as a Microsoft Edge browser.

Analysis of the files interacting with this domain reveals several Visual Basic Script (VBS) files that download the next stage of the attack and also overlap with an Ousaban banking trojan sample delivered from this domain. Furthermore, the naming conventions of these VBS scripts substantiate the deployment of social engineering tactics, as they masquerade as a notification process (in Portuguese, “processo de intimação”).

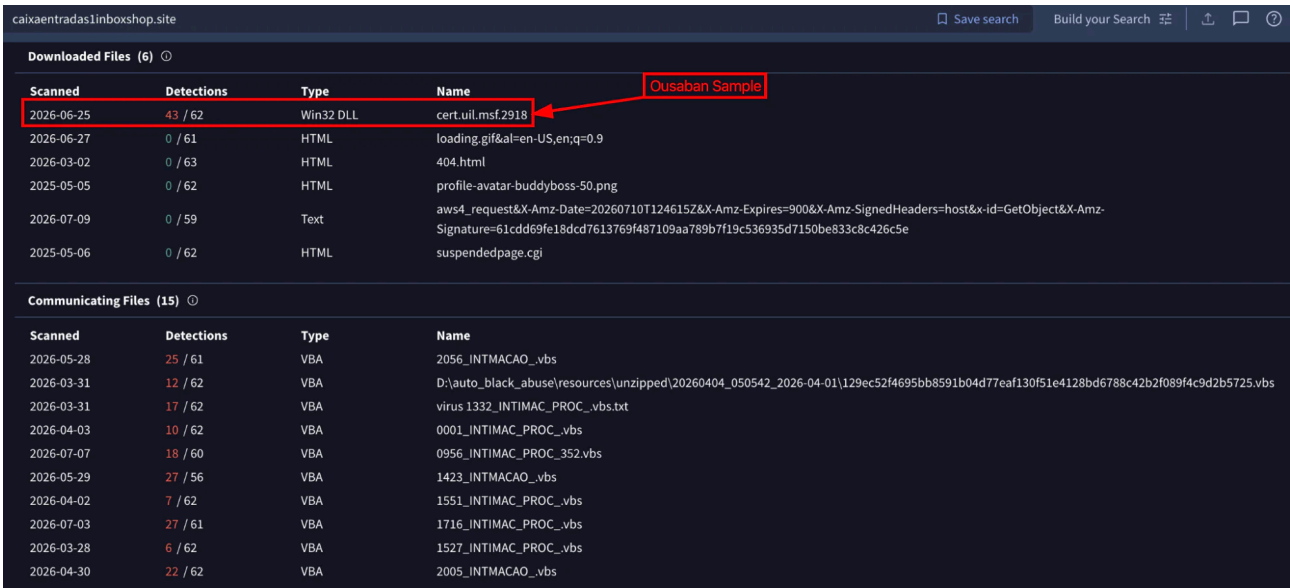


Figure 6. Certain files associated with the caixaentradas1boxshop[.]site domain.

You can hide the logic, but not your intentions

Logging messages interpretations

Group-IB assesses with moderate confidence that the developers are likely native Portuguese speakers. This assessment is supported by the malware's Portuguese-language strings, which use natural syntax and idiomatic phrasing rather than the awkward constructions, literal translations, or grammatical inconsistencies commonly seen in false-flag attempts. While linguistic artifacts alone are insufficient for attribution, they provide a supporting indicator when considered alongside technical, operational, and contextual evidence. Several examples of these operational logging messages are detailed below.

```
"Buscando configuração em: "  
"Configuração OK: "  
"Varredura finalizada. "  
" arquivos detectados."  
"Comando finalizado (sem saída de texto)."  
"Executando em segundo plano..."  
"[*] Executando comando remoto: "  
"[+++] Agente Online: "  
"[*] Softwares/Tags Detectados: "  
"[*] Qualidade alterada para HD"  
"[*] Qualidade alterada para SD"  
"[*] Analisando Navegador: "  
" [+] Perfil detectado: '"  
"[*] Encontrado em subpasta: "  
"Iniciando varredura de histórico..."  
"[🔑] Iniciando busca profunda de certificados..."  
"Busca certificados PFX de forma RECURSIVA no perfil do usuário e OneDrive."  
"[🚀] Enviando Dossiê e Certificados..."  
"[*] Identidade Detectada: "  
"Iniciando varredura estável por dossiê financeiro..."  
"\n[🔍] INICIANDO VARREDURA DE INTELIGÊNCIA EM TODOS OS PERFIS..."  
"Busca profunda e recursiva por arquivos CNAB.  
\n LIMITADO PARA EVITAR QUEDA DE CONEXÃO.\n "  
"Busca profunda e atualizada por softwares bancários, segurança (Topaz/Warsaw),  
\n ERPs e Inteligência de Negócio. Versão V12 (Ultra High Precision).\n "  
"\n[📊] RESULTADO CONSOLIDADO:"
```

Extensive logging messages, paired with the use of emojis, are a well-known signature of code generated by Large Language Models (LLMs), suggesting that the creators of BraZetsu relied on generative AI tools throughout development.

The extent of AI use across the entire attack lifecycle remains unknown. However, embedded log messages explicitly reference an artificial intelligence engine operating on the BraZetsu Command and Control (C2)

backend to process, triage, and interpret stolen data. Notable strings include:

- “Coleta metadados de hardware e porte da máquina para a IA do servidor.” (*Collects hardware and machine port metadata for server AI.*)
- “Define se o arquivo é um alvo prioritário para a IA.” (*Defines whether the file is a priority target for AI.*)

Intelligence Gathering capabilities

BraZetsu’s primary goal is intelligence gathering. This can be inferred from the logging messages and the naming conventions of its internal functions. This latest version contains 27 distinct functions, most of which relate to automated enumeration and reconnaissance capabilities. It also allows operators to execute commands and take screenshots on the compromised machine.

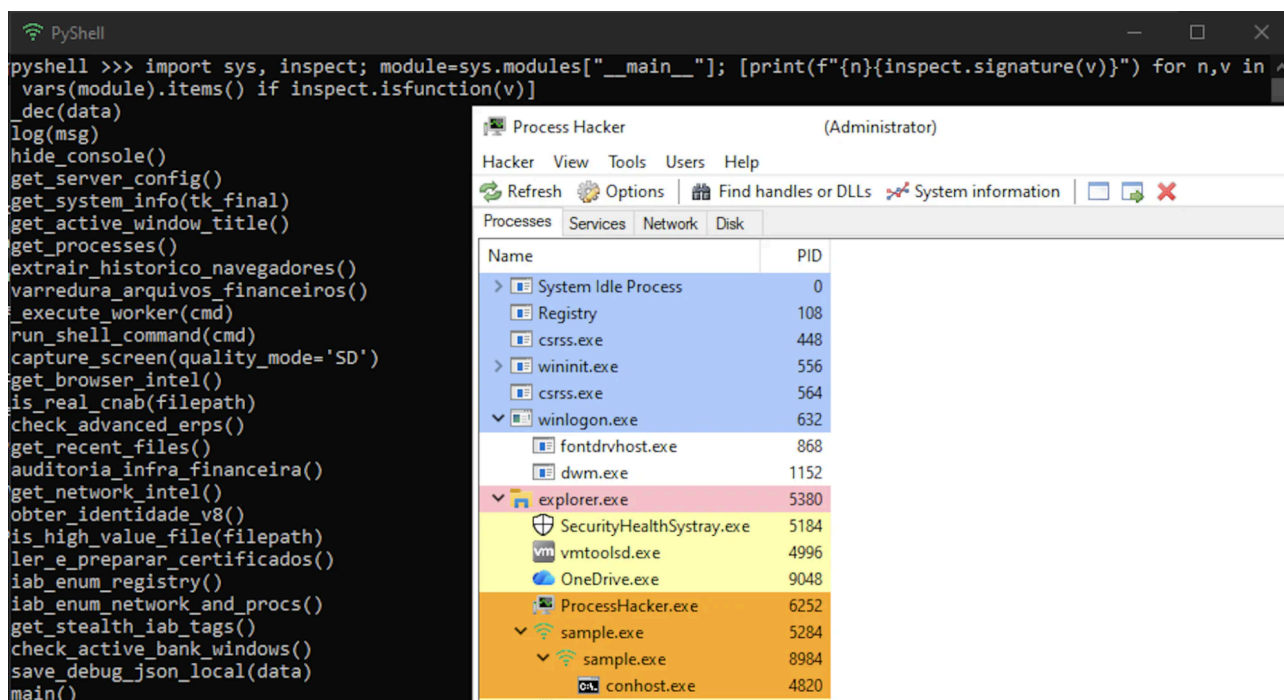


Figure 7. Extraction of BraZetsu malware’s internal functions.

Notable features of this malicious framework are described in more detail below.

get_server_config & _dec

To establish a connection, the `get_server_config()` function retrieves the encrypted and base64-encoded C2 configuration from a specified Pastebin URL. After retrieval, `_dec()` decodes and XOR decrypts it with a very clever key (p4st3s3cr3t_k3y). The resulting configuration string is then split on the “|” character to isolate `<c2_domain>|<port>|<auth_token>`.

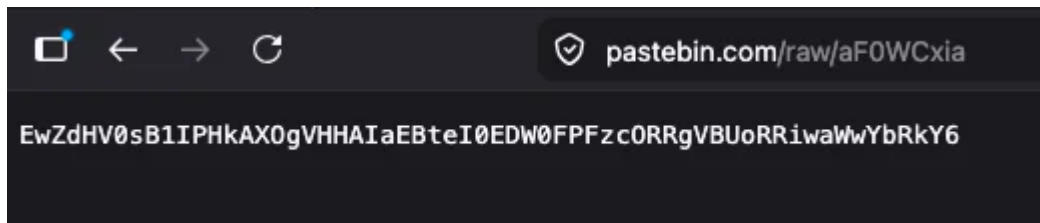


Figure 8. Pastebin URL containing the base64-encoded BraZetsu C2 configuration.

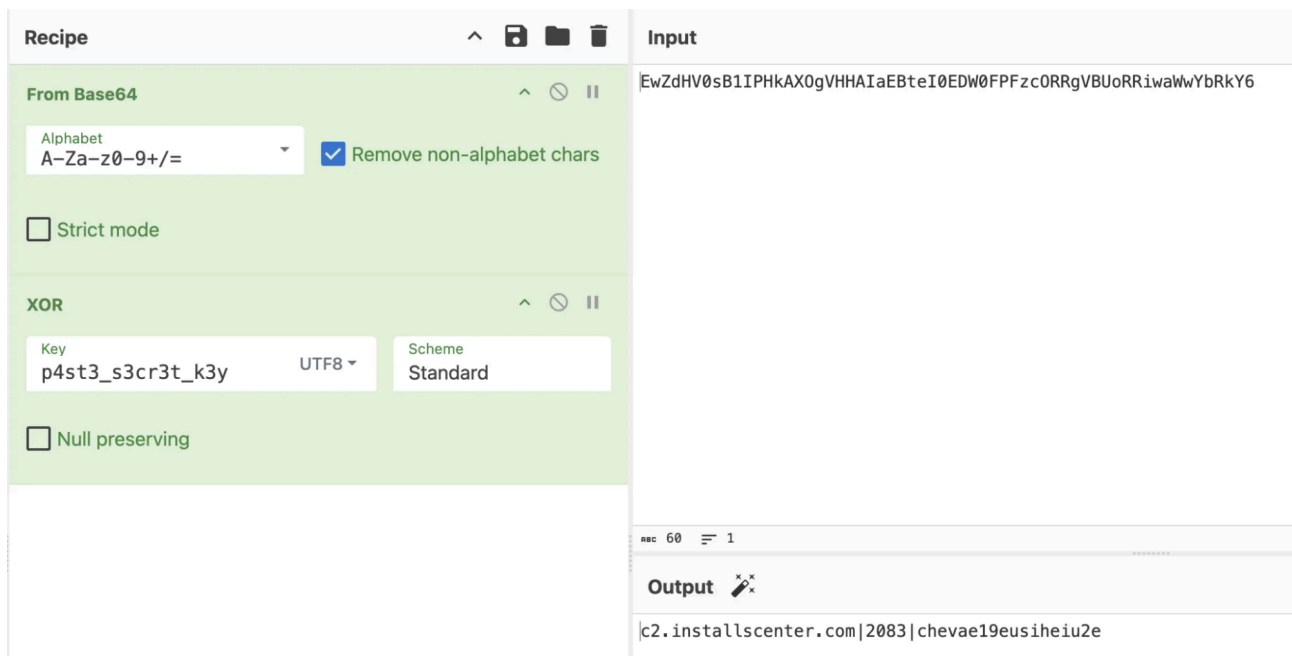


Figure 9. BraZetsu c2[.]installcenter[.]com configuration

get_active_window_title & check_active_bank_windows

The function `get_active_window_title()` retrieves the title of the compromised user's active application window. In contrast, the `check_active_bank_windows()` function scans for common banking keywords in window titles, a standard behavioral trait typically associated with banking Trojans. The image below shows the common keywords monitored by BraZetsu.

```
922     "get_active_window_title",
923     {
924         "BANCO ITAÚ": "BANK:Itau_Aberto",
925         "BANCO ITAU": "BANK:Itau_Aberto",
926         "BANCO BRADESCO": "BANK:Bradesco_Aberto",
927         "BANCO DO BRASIL": "BANK:BB_Aberto",
928         "CAIXA": "BANK:Caixa_Aberto",
929         "SICOOB": "BANK:Sicoob_Aberto",
930         "SANTANDER": "BANK:Santander_Aberto",
931         "SICREDI": "BANK:Sicredi_Aberto",
932         "SAFRA": "BANK:Safra_Aberto",
933         "BANRISUL": "BANK:Banrisul_Aberto"
934     },
935     {
936         "INTERNET BANKING": "BANK:Acesso_Bancario_Ativo",
937         "_BANKING_": "BANK:Caixa_Embaralhado",
938         "_CAI": "BANK:Caixa_Embaralhado",
939         "GERENCIADOR FINANCEIRO": "BANK:Gestao_PJ_Ativa",
940         "ACESSO SEGURO": "BANK:Login_Bancario",
941         "NET EMPRESA": "BANK:Bradesco_PJ_Ativo",
942         "AUTOATENDIMENTO": "BANK:BB_Acesso_Ativo"
943     },
944     "Detecta atividade bancária por títulos específicos e genéricos.",
```

Figure 10. Examples of banking window keywords monitored by BraZetsu.

get_browser_intel & extrair_historico_navegadores

To profile its targets, BraZetsu uses the *get_browser_intel()* function to scan for all user profiles across Chromium-based web browsers, specifically targeting Google Chrome, Microsoft Edge, Brave, Vivaldi, and Opera.

After identifying these browsers and profiles on an infected host, the malware extracts browser history rather than collecting credentials or cookies, distinguishing it from typical info-stealers and highlighting its specific objective of mapping the victim's activities. A user's browser history reveals significantly more about them than they might realize. In fact, it serves as an ideal source for intelligence gathering.

The framework performs this victim profiling by executing the SQLite query *"SELECT url, title, visit_count FROM urls WHERE url LIKE ?"* to cross-reference the extracted history with its TARGET_DOMAINS global variable. This global variable is a Python list containing nearly 230 distinct domains and URL paths that span a wide array of sectors.

```

pyshell >>> len(TARGET_DOMAINS)
228
pyshell >>> print(TARGET_DOMAINS)
['bradesco.com.br', 'banco.bradesco', 'bradesconetempresa.com.br', 'bradesconetempresa.b.br', 'ne2.bradesconetempresa.b.br', 'ne12.bradesconetempresa.b.br', 'ibpjlogin/login.jsf', 'pj.bradesco', 'itau.com.br', 'itaubusiness.com.br', 'empresas.itau.com.br', 'personalite.itau.com.br', 'itaucustody.com.br', 'itauconretora.com.br', 'bankline.itau.com.br', 'bb.com.br', 'bancobrasil.com.br', 'acesso.bb.com.br', 'ww2.bb.com.br', 'autoatendimento.bb.com.br', 'apj.bb.com.br', 'gerenciador.bb.com.br', 'origemlogin-bbdigital', 'caixa.gov.br', 'acessosseguro.sso.caixa.gov.br', 'caixaprepagos.com.br', 'sincb/#/login', 'conectividade.caixa.gov.br', 'pj.caixa.gov.br', 'v3.conectividade.caixa.gov.br', 'mercadolivre.com.br', 'mercadopago.com.br', 'mercadolivre.com', 'vendedores.mercadolivre.com.br', 'developers.mercadopago.com', 'mercadopago.com.br/developers/panel/credentials', 'mercadopago.com.br/activities', 'stripe.com', 'dashboard.stripe.com/apikeys', 'dashboard.stripe.com/webhooks', 'pagar.me', 'dash.pagar.me/settings/keys', 'dashboard.pagar.me/#/settings/api-keys', 'asaas.com', 'asaas.com/customer/apikeys', 'asaas.com/customerConfigIntegrations', 'iugu.com', 'app.iugu.com/settings/api_tokens', 'gerencianet.com.br', 'sejaefi.com.br', 'app.sejaefi.com.br/api/aplicacoes', 'paypal.com', 'developer.paypal.com/dashboard/applications', 'pagseguro.uol.com.br', 'minhaconta.pagseguro.uol.com.br/configuracoes/integracoes', 'appmax.com.br', 'admin.appmax.com.br', 'ticto.com.br', 'perfactpay.com.br', 'recapay.com.br', 'paghiper.com', 'transfeera.com', 'paggue.io', 'santander.com.br', 'pj.santander.com.br', 'coretara.santander.com.br', 'safracom.br', 'safrapay.com.br', 'banrisul.com.br', 'sicoob.com.br', 'ib.sicoobnet.com.br', 'sicredi.com.br', 'ib.sicredi.com.br', 'safracom.br', 'internettbanking.safracom.br', 'safrapay.com.br', 'safracom.br/pj', 'corporate.safracom.br', 'banrisul.com.br', 'ww8.banrisul.com.br', 'banrisul.com.br/office', 'banrisul.com.br/pessoaJuridica', 'sicoob.com.br', 'ib.sicoobnet.com.br', 'sicoobnet.com.br', 'sicredi.com.br', 'ib.sicredi.com.br', 'sicredi.com.br/pj', 'bancodonordeste.gov.br', 'bancoamazonia.com.br', 'bancobs2.com.br', 'daycoval.com.br', 'btgpactual.com', 'btgpactual.com/empresas', 'xpi.com.br', 'portal.xpi.com.br', 'clear.com.br', 'rico.com.br', 'nubank.com.br', 'nubank.com.br/pj', 'inter.co', 'inter.co/empresas', 'cora.com.br', 'app.cora.com.br', 'cobank.com.br', 'neon.com.br', 'btgpactual.com', 'btgpactual.com/empresas', 'original.com.br', 'modais.com.br', 'digio.com.br', 'superdigital.com.br', 'contasimplis.com.br', 'linkabanking.com.br', 'banco.bradesco', 'picpay.com', 'recar.gapay.com.br', 'shopify.com', 'admin.shopify.com', 'myshopify.com/admin', 'nuvemshop.com.br', 'tiendanube.com/admin', 'nuvemshop.com.br/admin', 'yampi.com.br', 'app.yampi.com.br', 'cartpanda.com', 'account.ts.cartpanda.com', 'lojaintegrada.com.br', 'lojaintegrada.com.br/painel', 'tray.com.br', 'bit.tray.com.br', 'bagy.com.br', 'vtex.com', 'vtexcommercestable.com.br', 'woocommerce', 'dooca.com.br', 'lojavirtual.com.br', 'venda.com.br', 'kiwify.com.br', 'dashboard.kiwify.com.br', 'hotmart.com', 'app-vlc.hotmart.com', 'hotmart.com/membership', 'eduzz.com', 'orbita.eduzz.com', 'braip.com', 'ev.braip.com', 'monetizze.com.br', 'kivirano.com', 'app.kivirano.com', 'dopopus.com', 'lastlink.com', 'herospark.com', 'ticto.com.br/checkout', 'guru.com.br', 'seller.shopee.com.br', 'ads.shopee.com.br', 'sellercentral.amazon.com.br', 'integra.magaluu.com.br', 'marketplace.magaluu.com.br', 'painelexpo.com.br', 'portal.americanasmarketplace.com.br', 'portal.ifood.com.br', 'gestorder.ifood.com.br', 'entregador.ifood.com.br', 'ads.google.com', 'ads.google.com/aw/overview', 'business.facebook.com', 'adsmanager.facebook.com', 'facebook.com/ads/library', 'ads.tiktok.com', 'ads.tiktok.com/i18n/dashboard', 'ads.kwai.com', 'taboola.com', 'taboola.com/backstage', 'outbrain.com', 'ads.pinterest.com', 'rdstation.com.br', 'activecampaign.com', 'mailchimp.com', 'bling.com.br', 'bling.com.br/vendas', 'tiny.com.br', 'tiny.com.br/app', 'omie.com.br', 'app.omie.com.br', 'contaazul.com', 'app.contaazul.com', 'sankhya.com.br', 'totvs.com.br', 'senior.com.br', 'alterdata.com.br', 'nfe.fazenda.gov.br', 'nfe.prefeitura', 'enotas.com.br', 'arquivel.com.br', 'cav.receita.fazenda.gov.br/ccac', 'ww8.receita.fazenda.gov.br/SimplesNacional', 'gov.br/mel', 'portaldoempreendedor.gov.br', 'binance.com', 'binance.com/pt-BR/my/dashboard', 'okx.com', 'bybit.com', 'metamask.io', 'tradingview.com', 'xpi.com.br', 'portal.xpi.com.br', 'clear.com.br', 'rico.com.br', 'nuinvest.com.br', 'neologica.com.br', 'iqoption.com', 'stake.com', 'blaze.com', 'bet365.com', 'melhorenvio.com.br', 'frenet.com.br', 'kangu.com.br', 'intelipost.com.br', 'correios.com.br', 'jadlog.com.br', 'wise.com', 'revolut.com', 'payoneer.com', 'nomadglobal.com', 'westernunion.com']
pyshell >>>

```

Figure 11. Global list variable containing nearly 230 cross-sector domains and URLs.

get_stealth_iab_tags

This function performs about 20 initial access broker checks by enumerating environment variables, network ports, running processes, and common keywords. Once it identifies these characteristics on an infected system, BraZetsu adds a tag for those indicators.

Group-IB research team reconstructed this content to provide a formatted JSON representation of BraZetsu's raw object constants; however, it does not reflect the malware's original source-code configuration.

Based on the reconstructed object, BraZetsu conducts explicit Initial Access Broker (IAB) verifications across various systems:

- Administrative endpoints in e-commerce utilizing VTEX or Magento.
- Enterprise security systems, specifically Endpoint Detection and Response (EDR) solutions.
- Police and law enforcement environments (identifiable via hostname prefixes like PC-, PM-, DP-, or SSP-).
- Financial and ERP configurations, including SAP, Warsaw, TOTVS/Protheus, Topaz, and Diebold.
- Industrial SCADA networks running FactoryTalk, RSLogix, or WinCC.
- Development and DevOps environments.
- Helpdesk and IT support environments.
- Human resources management workstations.
- Fleet logistics networks running Autotrac or Sascar platforms.
- Insurance brokerage services.
- Internet Service Providers (ISPs) utilize Winbox as their primary utility for MikroTik router administration.
- Hospital Information Systems (HIS) executing Tasy ERP solutions.
- Database services include Oracle, PostgreSQL, SQL Server, and MySQL.
- Data backup instances running Veritas Backup Exec or Veeam Backup & Replication.

```

{
  "[DOMAIN_ADMIN]": {
    "environment_variables": [
      "USERDOMAIN"
    ]
  },

```

```
"[DEVOPS_CLOUD]": {
  "environment_variables": [
    "AWS_ACCESS_KEY_ID",
    "AZURE_CONFIG_DIR",
    "KUBECONFIG"
  ],
  "processes": [
    "docker.exe"
  ]
},
"[FINANCE_ERP]": {
  "process_keywords": [
    "sap",
    "warsaw",
    "diebold",
    "topaz",
    "totvs",
    "protheus"
  ]
},
"[IT_SUPPORT]": {
  "process_keywords": [
    "putty",
    "wireshark",
    "anydesk"
  ],
  "ports": [
    3389 // RDP network port
  ]
},
"[SCADA_INDUSTRIAL]": {
  "process_keywords": [
    "wincc",
    "rslogix",
    "factorytalk"
  ]
},
"[HR_MANAGER]": {
  "process_keywords": [
    "senior"
  ],
  "keywords": [
    "folha",
    "salario",
    "holerite"
  ]
},
```

```
"[LEGAL_DEPT]": {
  "keywords": [
    "projuris",
    "cpj",
    "contrato"
  ]
},
"[DEVELOPER]": {
  "processes": [
    "code.exe"
  ],
  "files": [
    ".gitconfig"
  ]
},
"[GOV_ACCESS]": {
  "keywords": [
    "safenet",
    "token"
  ]
},
"[ECOMMERCE_ADMIN]": {
  "keywords": [
    "magento",
    "vtex"
  ]
},
"[CRYPTO_EXCHANGE]": {
  "paths": [
    "AppData\\Roaming\\Exodus"
  ]
},
"[BACKUP_SERVER]": {
  "processes": [
    "veeam.exe",
    "bengine.exe"
  ]
},
"[SECURITY_EDR]": {
  "processes": {
    "csfalconservice.exe": "CrowdStrike",
    "sentinelagent.exe": "SentinelOne",
    "msmpeng.exe": "Defender"
  }
},
"[VPN_CONFIG]": {
  "processes": [
```

```

        "openvpn.exe",
        "vpnuui.exe"
    ]
},
"[HEALTHCARE_HIS]": {
    "process_keywords": [
        "tasy"
    ],
    "ports": [
        104 // DICOM (Digital Imaging and Communications in Medicine) network port
    ]
},
"[LOGISTICS_FLEET]": {
    "process_keywords": [
        "sascar",
        "autotrac"
    ]
},
"[INSURANCE_BROKER]": {
    "keywords": [
        "apolice",
        "seguro"
    ]
},
"[LAW_ENFORCEMENT]": {
    "hostname_prefixes": [
        "PC-", // Polícia Civil
        "PM-", // Polícia Militar
        "DP-", // Departamento de Polícia
        "SSP-" // Secretaria de Segurança Pública
    ]
},
"[ISP_ADMIN]": {
    "processes": [
        "winbox.exe"
    ],
    "keywords": [
        "winbox"
    ]
}
}

```

Other functionalities

Function name	Description
---------------	-------------

log	Logs timestamped operations if the global variable SHOW_LOG is enabled. Otherwise, logging is disabled.
hide_console	Hides all console window operations during BraZetsu execution.
get_system_info	Gather details regarding the compromised machine, including the username, hostname, and operating system version.
get_processes	Retrieves a comprehensive list of all active processes executing on the compromised system.
_execute_worker	This function launches an additional worker instance as a module or separate payload.
run_shell_commands	Executes arbitrary shell commands via the Windows Command Shell (cmd.exe), allowing remote operators hands-on control.
capture_screen	Captures a screenshot of the compromised system in either SD or HD quality, converting it into a base64-encoded string.
is_real_cnab	Although the internal mechanics of this function remain unknown, its name suggests it verifies the CNAB file's validity.
check_advanced_erps	Although its internal workings are unclear, log messages suggest this function enumerates the compromised machine to find common ERP installation directories.
get_recent_files	Retrieves recently opened files on the compromised machine to support automated reconnaissance and intelligence gathering.
auditoria_infra_financeira	Although its internal workings are unclear, log messages suggest this function enumerates the compromised machine to search for common internet banking applications.
get_network_intel	While its internal workings are unclear, the name suggests it enumerates common network services.
obter_identidade_v8	Although its internal workings are not fully understood, operational logs and specific regex patterns for detecting CPF and CNPJ numbers suggest this function primarily extracts legal identifiers.
ler_e_preparar_certificados	Though its internal mechanics are unclear, operational logs indicate that this function collects “.PFX” or “.P12” digital certificates by scanning the file system and OneDrive shares (“Iniciando busca profunda de certificados...”). Once gathered, it bundles them with a machine data dossier and exfiltrates them to the C2 server (“Enviando Dossiê e Certificados...”).

save_debug_json_local	Stores debugging details locally in a JSON file named “debug_payload_sent.json”.
iab_enum_registry	Identifies applications currently installed on the compromised system by reading the “SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall” and “SOFTWARE\WOW6432Node\Microsoft\Windows\CurrentVersion\Uninstall” registry keys
iab_enum_network_and_procs	Conducts an enumeration of active network services and running processes on the compromised system.

BraZetsu Constant Evolution

With the discovery of BraZetsu, several questions arise regarding the operational history and whether earlier iterations of this malware family existed. Through extensive threat hunting and differential analysis, Group-IB successfully identified five distinct versions of BraZetsu and traced their origins back to February 2026. Our team established this internal versioning system to accurately track the malware’s lifecycle and technical progression.

The framework’s timeline demonstrates a steady advance in functionality, transitioning from a basic tool into a highly specialized intelligence-gathering framework:

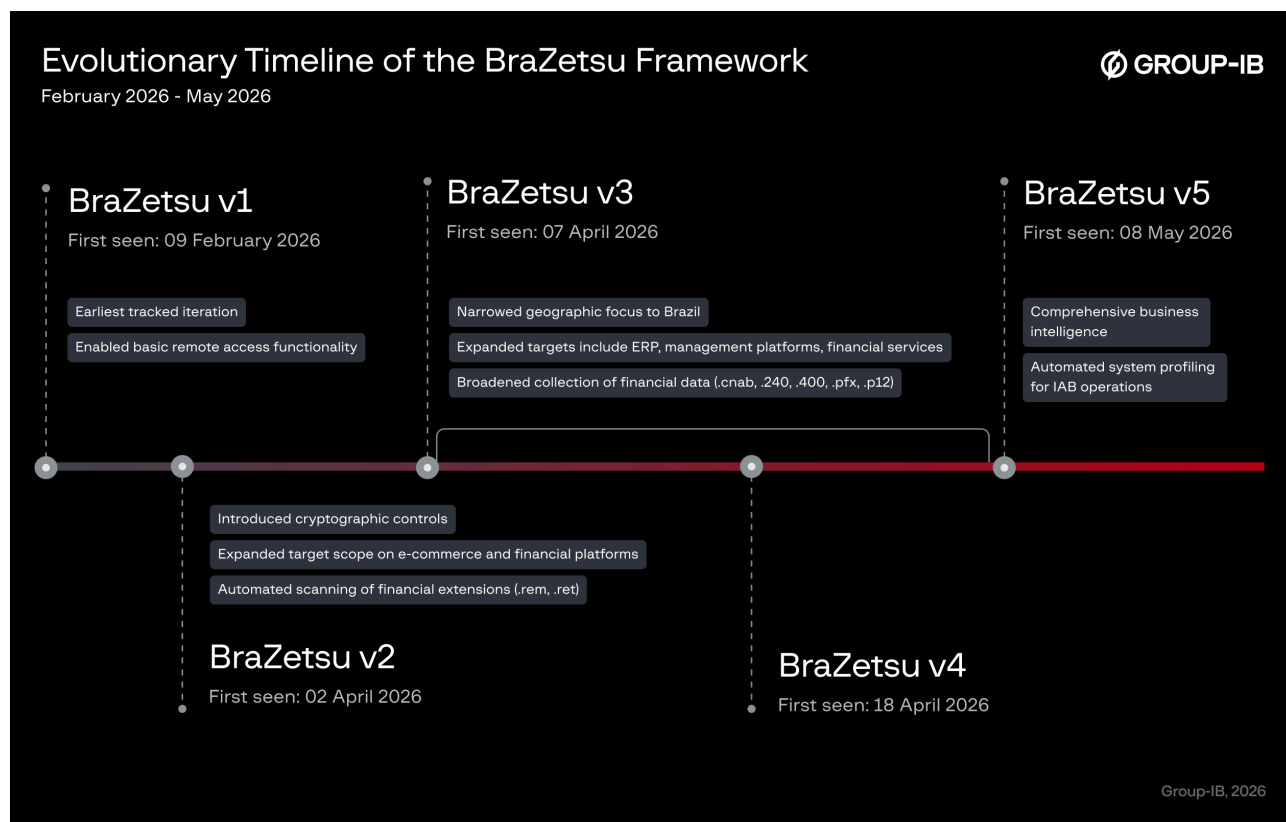


Figure 12. Evolutionary timeline of the BraZetsu framework from February to May 2026.

- **BraZetsu v1:** The earliest tracked iteration primarily focused on enabling basic remote access to compromised systems. It featured a simpler configuration with parameters such as PASTEBIN_URL and

AUTH_TOKEN and established persistence on host machines by creating a registry run key named “MonitorSystem”.

- **BraZetsu v2:** This version introduced cryptographic controls, utilizing a hardcoded SECRET_KEY (‘p4st3_s3cr3t_k3y’) to handle obfuscated Command and Control (C2) configurations. Strategically, its target scope expanded to focus on prominent e-commerce and financial platforms across multiple Latin American regions, specifically targeting Mercado Libre and Mercado Pago domains in Brazil, Argentina, Mexico, and Chile. It also initiated basic automated scanning for financial extensions like .rem and .ret.
- **BraZetsu v3 & v4:** In these versions, the developers implemented a refined strategic pivot, narrowing their geographical focus to corporate targets in Brazil while significantly deepening reconnaissance. The list of targeted web domains was significantly expanded to include local Enterprise Resource Planning (ERP) providers, management platforms, and financial services, such as Conta Azul, Omie, Bling, Tiny, Sankhya, and TOTVS. Furthermore, the framework began explicitly searching for specific installation paths (e.g., SAP, Senior, Alterdata, Nasajon). It broadened its collection criteria to exfiltrate a wider array of financial data and digital certificates, adding extensions such as .cnab, .240, .400, .pfx, and .p12.
- **BraZetsu v5:** Representing the latest step in its development, this version integrates comprehensive business intelligence and automated system profiling features designed to facilitate Initial Access Broker (IAB) operations.

This ongoing technical progression is marked by a shift to newer compilers and updated Python versions, along with more complex evasion tactics. The ongoing development of advanced features, such as deep browser profile parsing and financial dossier scanning, reflects a calculated effort by the threat actors to maximize the commercial value of initial access within the regional cybercriminal ecosystem.

The image below illustrates the breakdown of features and capabilities extracted for each framework version.

1 BraZetsu v1:	1 BraZetsu v2:	1 BraZetsu v3:	1 BraZetsu v4:	1 BraZetsu v5:
2 log	2 _dec	2 _dec	2 _dec	2 _dec
3 hide_console	3 log	3 log	3 log	3 log
4 get_server_config	4 hide_console	4 hide_console	4 hide_console	4 hide_console
5 add_to_startup	5 get_server_config	5 get_server_config	5 get_server_config	5 get_server_config
6 get_system_info	6 get_system_info	6 get_system_info	6 get_system_info	6 get_system_info
7 get_active_window_title	7 get_active_window_title	7 get_active_window_title	7 get_active_window_title	7 get_active_window_title
8 get_processes	8 get_processes	8 get_processes	8 get_processes	8 get_processes
9 run_shell_command	9 extrair_historico_navegadores	9 extrair_historico_navegadores	9 extrair_historico_navegadores	9 extrair_historico_navegadores
10 capture_screen	10 varredura_arquivos_financeiros	10 varredura_arquivos_financeiros	10 varredura_arquivos_financeiros	10 varredura_arquivos_financeiros
11 main	11 run_shell_command	11 run_shell_command	11 run_shell_command	11 _execute_worker
12 TOTAL = 10 functions	12 capture_screen	12 capture_screen	12 capture_screen	12 run_shell_command
13	13 get_browser_intel	13 get_browser_intel	13 get_browser_intel	13 capture_screen
	14 varredura_financeira_rapida	14 varredura_financeira_rapida	14 varredura_financeira_rapida	14 get_browser_intel
	15 is_real_cnab	15 is_real_cnab	15 is_real_cnab	15 is_real_cnab
	16 check_erp_software	16 check_erp_software	16 check_advanced_erps	16 check_advanced_erps
	17 main	17 calculador_score_tesouraria	17 get_recent_files	17 get_recent_files
	18 TOTAL = 16 functions	18 main	18 auditoria_infra_financeira	18 auditoria_infra_financeira
	19	19 TOTAL = 17 functions	19 main	19 get_network_intel
		20	20 TOTAL = 18 functions	20 obter_identidade_v8
			21	21 is_high_value_file
				22 ler_e_preparar_certificados
				23 iab_enum_registry
				24 iab_enum_network_and_procs
				25 get_stealth_iab_tags
				26 check_active_bank_windows
				27 save_debug_json_local
				28 main
				29 TOTAL = 27 functions
				30

Figure 13. Ongoing technical evolution and upgrades across BraZetsu framework versions.

Marketplace & Threat Actors

Active since February 2026, the Brazilian cybercriminal known as “Exilware” has operated a commercial platform through the infect[.]online domain, where it sells compromised systems as tradable assets. Access is

available for an initial deposit of approximately \$5.80, equivalent to a cup of coffee, establishing a low financial barrier for customers to begin using the platform within the first 24 hours.



Figure 14. Marketplace advertisement.

During the analysis of the BraZetsu malware, the Group-IB Threat Intelligence Team identified the domain `c2[.]installcenter[.]com`, and further analysis of the associated infrastructure revealed that it resolves to the same marketplace previously attributed to Exilware, establishing a direct link between BraZetsu and the Infect Marketplace. This connection was later corroborated by statements made by Exilware himself.

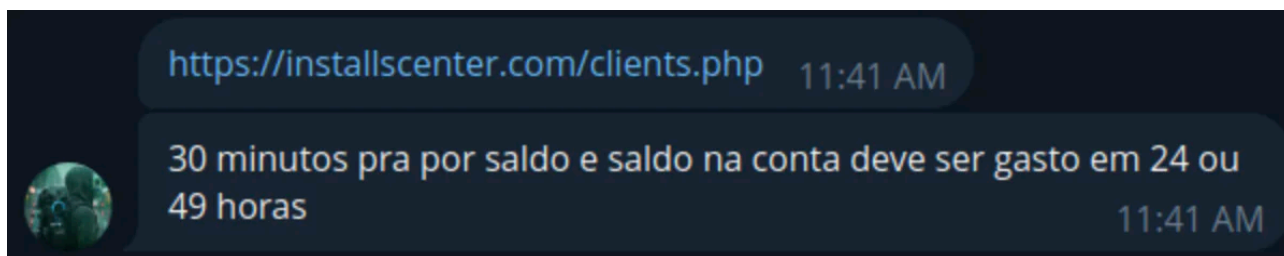


Figure 15. Exilware confirming the new marketplace domain & informing new rules requiring payment within 24-49 hours.

Based on these findings, Group-IB assesses with high confidence that BraZetsu functions as the primary malware framework supporting Exilware’s Initial Access Broker (IAB) operation by establishing initial footholds and continuously replenishing the Infect Marketplace inventory. The figure below illustrates the complete attack and monetization workflow.

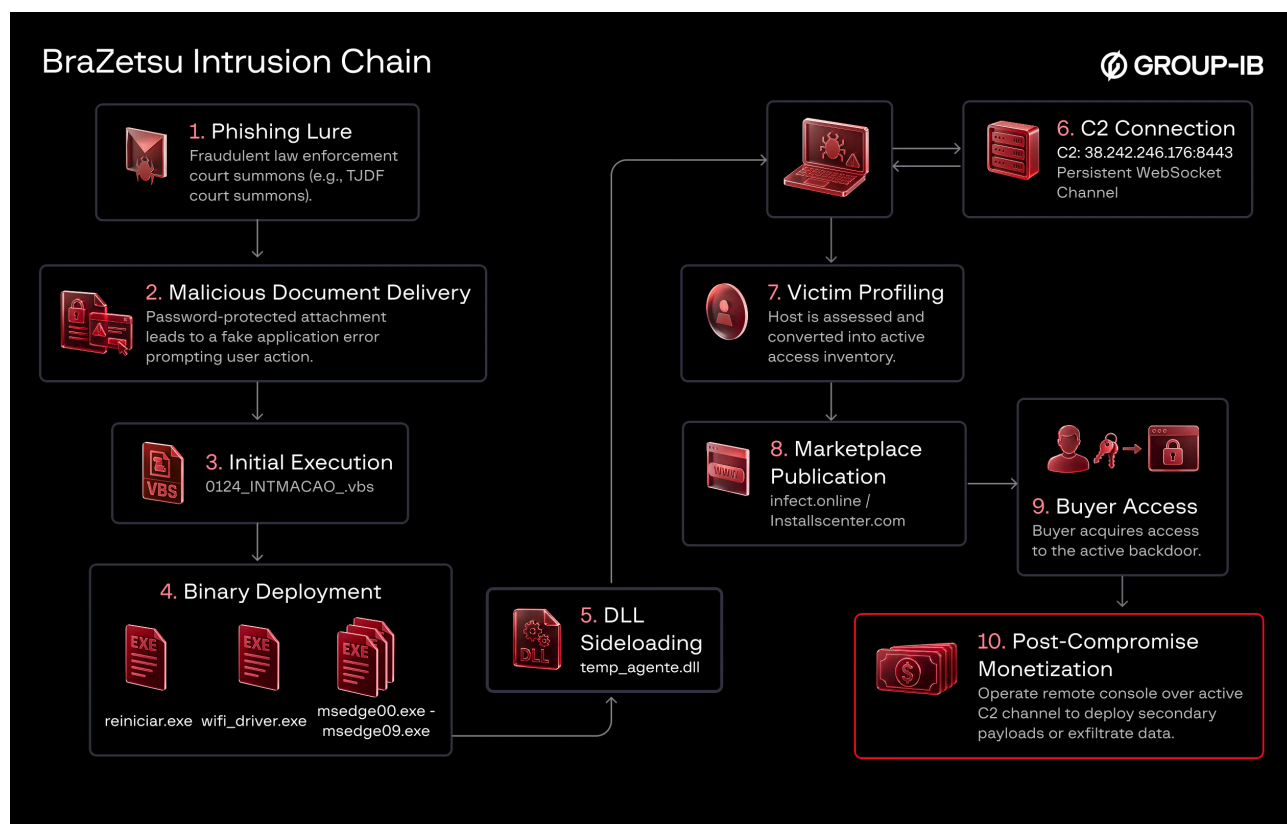


Figure 16. Intrusion & Monetization Flow.

Over time, Exilware shifted toward a more discreet operational model. Unlike many financially motivated cybercriminals that rely on broad marketplace exposure to expand their customer base, Exilware intentionally limited access to its services and imposed rules requiring any account to spend the money within 24 hours on days with a high volume of newly compromised machines or 49 hours on “normal” days. This controlled approach likely reduced operational risk while allowing the operators to maintain a smaller, trusted network of customers.

This cautious approach is likely intended to reduce operational risk and limit visibility to law enforcement and security researchers.

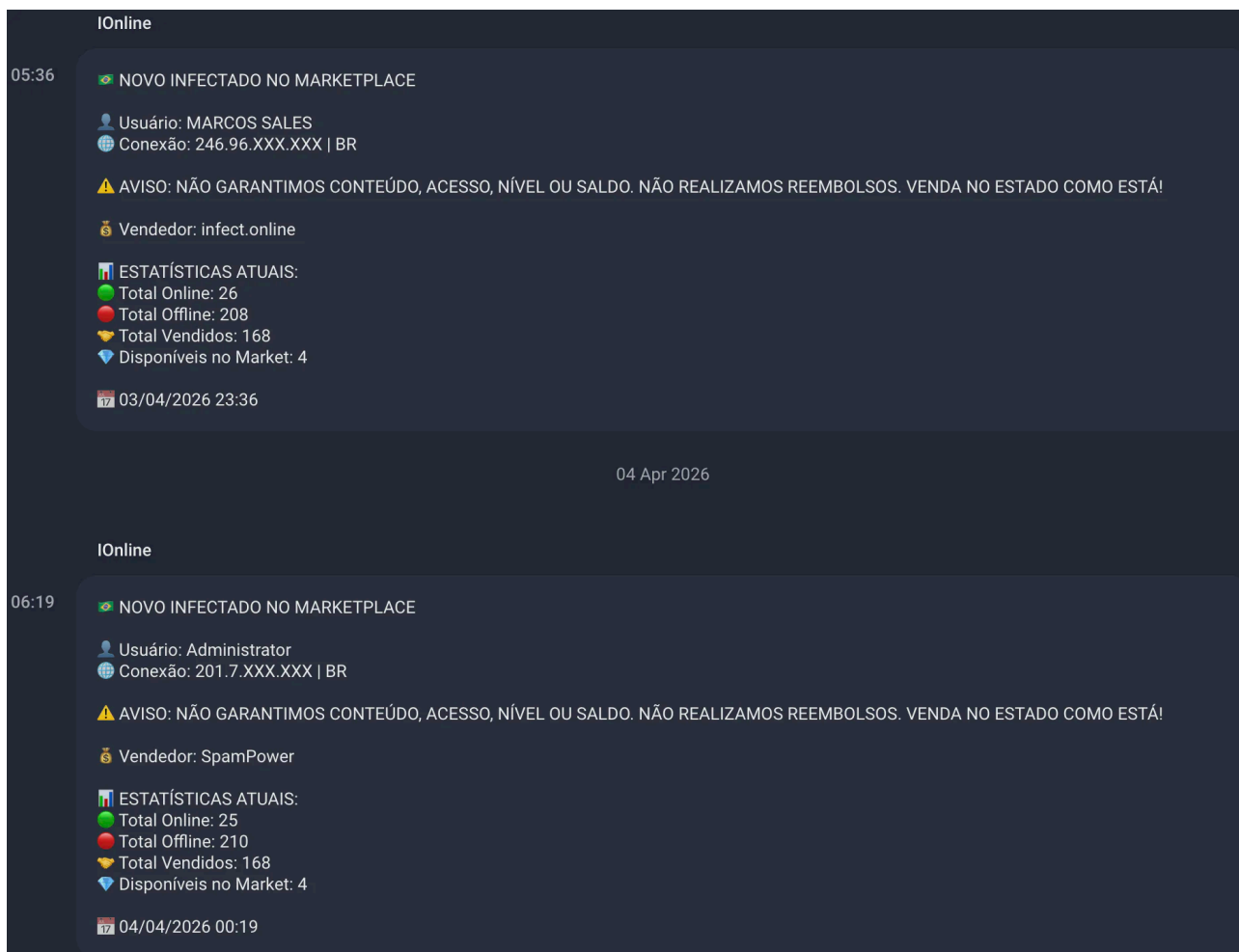


Figure 18. SpamPower Seller.

In the course of this investigation, we observed two primary vendors operating within the marketplace under the aliases “infect.online” and “SpamPower”. Although the relationship between these vendors remains unclear, Exilware’s public statements suggest that its operation is not conducted independently.

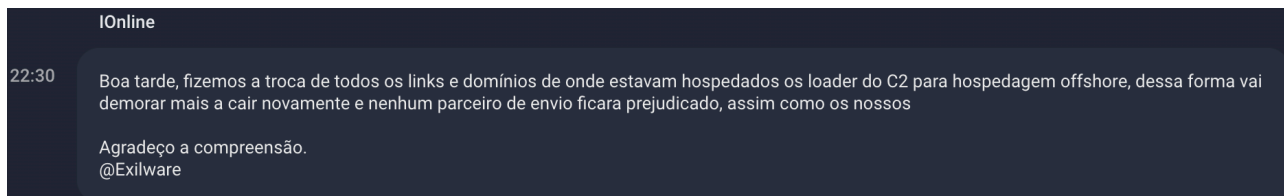


Figure 19. Exilware alerting the change of C2 domains to offshore.

The commercial arrangements between these actors, including revenue-sharing mechanisms, commission structures, and operational responsibilities, remain unknown. However, given the volume of daily infections and the scale of the operation, Group-IB assesses with moderate confidence that the cybercriminal relies on a restricted network of partners to distribute BraZetsu and continuously supply the marketplace with newly compromised assets.

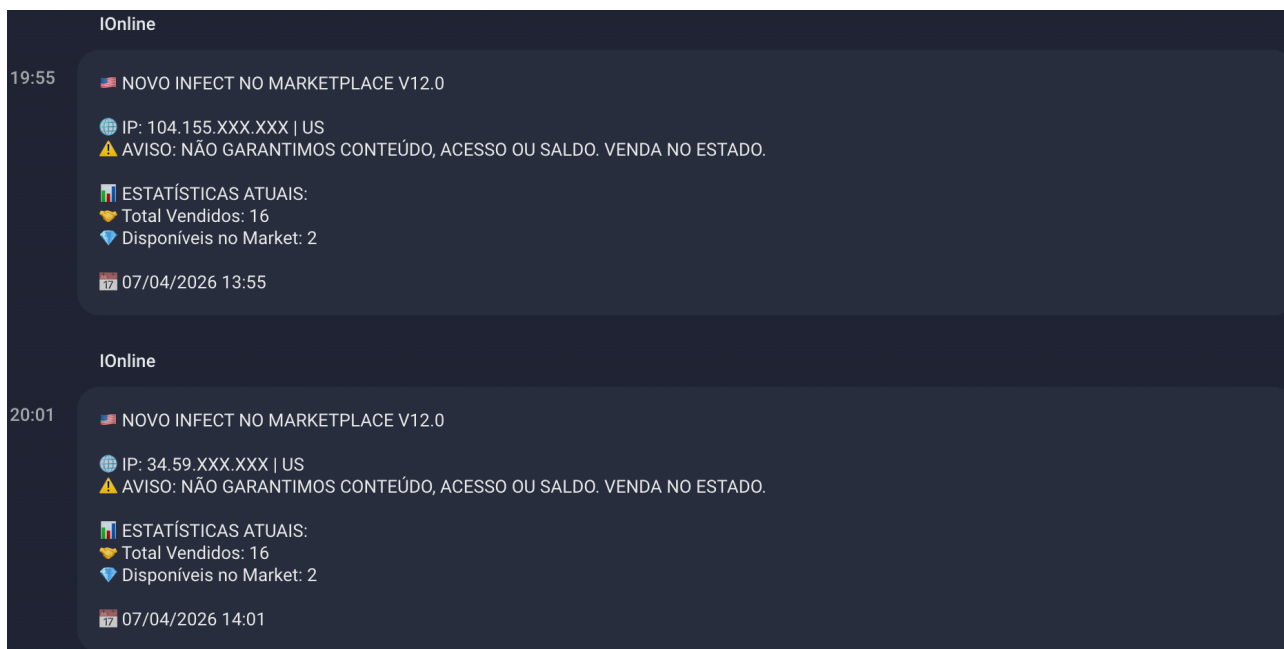


Figure 20. U.S compromised machines for sale.

Finally, although the ecosystem has historically focused on Spanish and Portuguese-speaking countries, our analysis identified two compromised hosts located in the United States that were advertised in April 2026. While this observation alone is insufficient to establish a sustained shift in targeting, it suggests a new partner or a possible expansion of the cybercriminal operation’s footprint beyond its traditional geographic focus.

Infrastructure

The Group-IB Threat Intelligence Team conducted a hunt across open and private sources on the file convention used by BraZetsu, “msedge.exe”, which led us to a previously observed IP address, **38[.]242[.]246[.]176**, revealing old infrastructure (“infect[.]online”) for the Infect Marketplace.

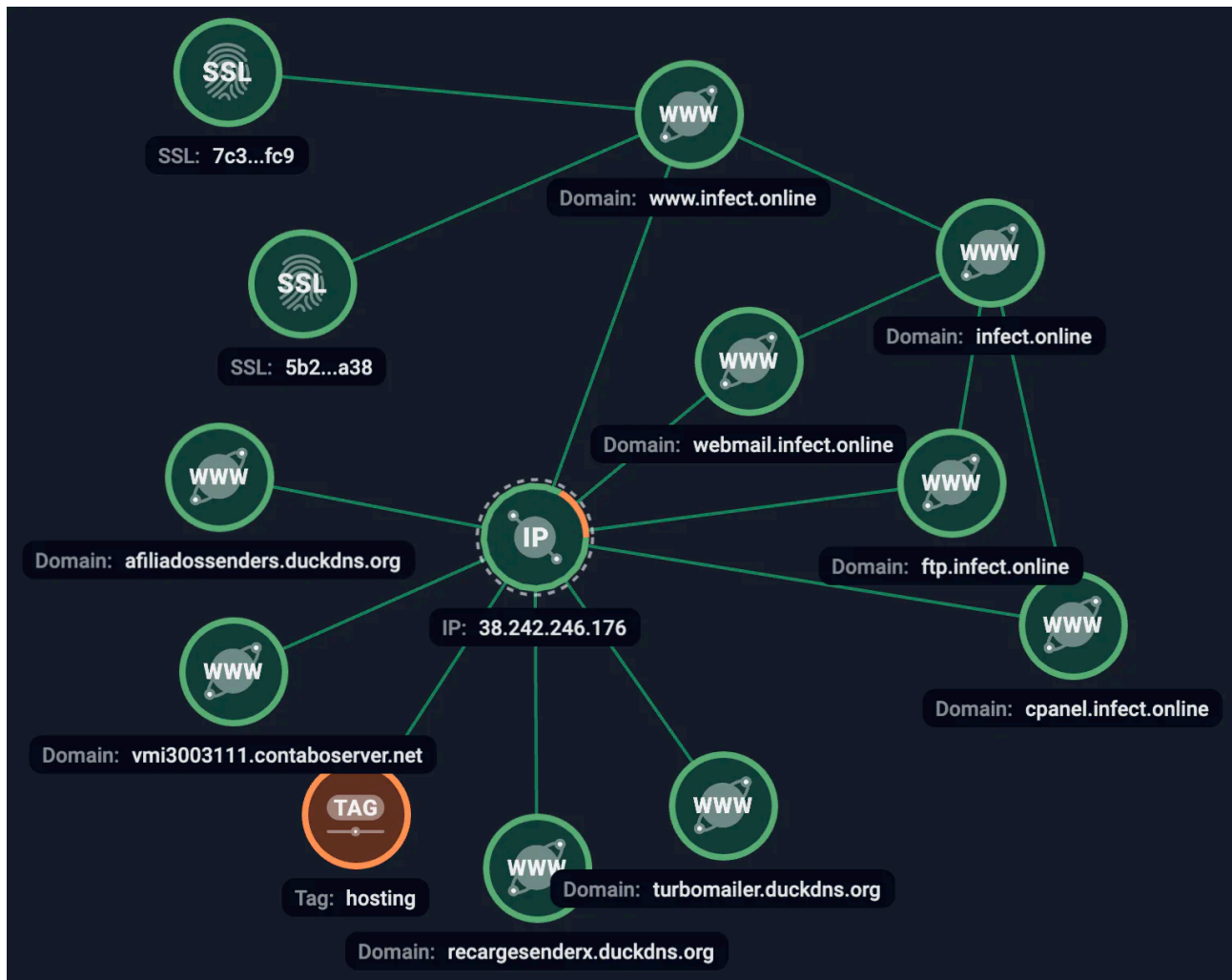


Figure 21. Old infrastructure to host infect[.]online domain.

Graph Intelligence identified that the IP address had previously been associated with an AgenteV2 investigation documented by [ANY.RUN](#), as shown in the figure below.

Network diagram showing the infrastructure for infect[.]online domains. The central node is IP: 38.242.246.176. Connected nodes include:

- Domain: www.infect.online
- Domain: infect.online
- Domain: webmail.infect.online
- Domain: ftp.infect.online
- Domain: cpanel.infect.online
- Domain: afiliadossenders.duckdns.org
- Domain: vmi3003111.contaboserver.net
- Domain: turbomailer.duckdns.org
- Domain: recargesenderx.duckdns.org
- SSL: 7c3...fc9
- SSL: 5b2...a38
- Tag: hosting

PTR record: vmi3003111.contaboserver.net
 Hostnames: www.infect.online · cpanel.infect.online · webmail.infect.online · ftp.infect.online · vmi3003111.contaboserver.net
 Show all 8

ISP	Contabo GmbH	Country	France
ASN	AS174	City	Lauterbourg
Netname	Contabo GmbH	Organization	Contabo GmbH

Google search results

Inside agenteV2: How Brazilian Attackers Use Fake Court Summons to Steal Banking Credentials in Real Time | by ANY.RUN
<https://medium.com/@anyrun/inside-agentev2-how-brazilian-attackers-use-fake-court-summons-to-steal-banking-credential-s-in-30394867eb6a>
 A new phishing campaign targeting Brazilian users demonstrates how modern financial malware has evolved from simple credential theft into full-...Read more

Inside agenteV2: How Brazilian Attackers Use Fake Court Summons to Steal Banking Credentials in Real Time
<https://any.run/cybersecurity-blog/brazilian-banking-phishing-campaign/>
 Apr 24, 2026 — Brazilian phishing delivers agenteV2: a Nutika-compiled banking stealer targeting major banks with live screen streaming via WebSocket

Figure 22. Articles linking 38[.]242[.]246[.]176 infrastructure to “AgenteV2”.

This discovery prompted a deeper comparative analysis, which revealed multiple technical overlaps between BraZetsu and AgenteV2. The key analytical evidence supporting this assessment is presented below.

Unified Nomenclature and Payload Equivalency

- The initial loader filenames, `wifi_driver.exe` and `msedge04.exe`, are consistent across both campaigns.
- The core payload documented by ANY.RUN, `agenteV2_historico_detect.dll`, is functionally equivalent to the `temp_agente.dll` payload identified by the Group-IB Threat Intelligence Team during the BraZetsu investigation.

Shared Codebase and Build Methodology

- Both malware variants are developed in Python 3 and compiled with Nuitka into native PE executables.
- Both deploy an identical runtime environment, including Python 3.13, OpenSSL libraries, and mypyc auxiliary components.
- Both retain the same development artifacts, including unstripped Portuguese debug messages and descriptive string variables embedded in the `.rdata` section.

Shared Tradecraft and Functional Capabilities

- Both use `shutil.copyfile` to copy Chrome and Microsoft Edge databases to `%TEMP%`, bypassing SQLite file locks while the browsers remain open.
- Both establish an interactive WebSocket backdoor over TLS port 8443, enabling bidirectional communications, screen capture using the PIL and mss libraries, and remote shell execution through `subprocess.Popen`.
- Both explicitly check for the presence of Diebold Warsaw and GbPlugin security software prior to or during execution.

Shared Infrastructure

- Both communicate with infrastructure hosted at `38[.]242[.]246[.]176`, a Contabo VPS.
- Both retrieve their C2 configuration through Pastebin dead-drop resolvers containing Base64-encoded, XOR-encrypted configuration data.

We assess with **high confidence** that **AgenteV2** and **BraZetsu** refer to the same initial access malware framework. This assessment is supported by their shared codebase, identical build methodology, overlapping functionality, common infrastructure, and equivalent payload architecture, and further reinforces our assessment that the Brazilian threat actor Exilware develops and maintains the framework.

Victimology

The BraZetsu victimology demonstrates a sophisticated understanding of target-value optimization, with comprehensive reconnaissance across 20+ categories, including banking systems, ERP platforms (TOTVS, SAP, Sankhya, Senior), SCADA infrastructure, government systems, cryptocurrency platforms, and other sectors. The malware's AI-driven assessment capabilities automatically evaluate compromised machines' commercial potential

through hardware profiling, software environment analysis, and network infrastructure mapping, enabling Exilware to categorize automatically and price marketplace access based on victim value.

Recent versions show an exclusive focus on Brazilian infrastructure while maintaining multi-language capabilities for regional expansion, indicating deep operational knowledge of the domestic threat landscape and strategic positioning for broader Latin American operations targeting critical infrastructure and high-value commercial sectors.

Ultimately, although Exilware's primary motivation and broader criminal operations appear to be financially driven, its activity extends beyond opportunistic cybercrime. The operation reflects a coordinated effort to establish and maintain persistent access across interconnected sectors that underpin national economic activity and critical services. This access almost certainly facilitates lower-impact, financially motivated intrusions and enables more capable threat actors by providing access that can be leveraged in higher-impact operations, thereby strengthening the regional cybercriminal ecosystem.

Attribution

The analysis definitively establishes that BraZetsu serves as Exilware's primary operational tool through several critical connections:

- **C2 Infrastructure Overlap:** BraZetsu's Command and Control infrastructure `installcenter[.]com` directly connects to a customer login panel that Group-IB attributes with high confidence to the "Infect Marketplace" operated by Exilware.
- **Marketplace Integration:** The malware framework includes specific functionality for remote payload execution that directly enables the marketplace's core service offering, allowing customers to execute malicious code on purchased access.
- **Geographic Targeting Alignment:** BraZetsu's evolution shows a refined focus exclusively on Brazil in recent versions (v3 & v4), perfectly matching Exilware's primary target market while maintaining capabilities for Portuguese and Spanish-speaking countries.

Group-IB assesses with high confidence that the Exilware threat actor uses BraZetsu malware as the primary technical mechanism to achieve initial access to victim environments and subsequently monetize these compromises through the "Infect Marketplace." This connection represents a sophisticated Initial Access Broker (IAB) operation that transforms compromised systems into commercial assets through automated intelligence gathering and AI-enhanced target prioritization.

This assessment draws on technical artifacts, operational tradecraft, and behavioral patterns observed throughout the investigation.

Conclusion

BraZetsu represents a significant shift in the Latin American cybercriminal landscape, evolving from a standard RAT into an advanced, modular malicious IAB framework. By automating reconnaissance across corporate, financial, and industrial systems and integrating with AI-driven triage mechanisms, the framework identifies and prioritizes high-value targets, feeding an underground marketplace that commercializes access to compromised

hosts. This platform allows cybercriminals to leverage pre-prepared access to install their own malicious tools, a convenience that significantly complicates defenders' efforts to track and attribute these mixed malicious activities.

Recommendations

Based on these findings, Group-IB recommends that organizations strengthen endpoint visibility, proactively monitor for abuse of trusted services, and continuously validate their security controls against similar attack techniques.

- **Strengthen Endpoint Visibility:** Since BraZetsu targets specific ERP (e.g., TOTVS, SAP, Sankhya, Senior) and financial infrastructure, ensure all endpoints associated with these applications have robust, proactive monitoring and logging enabled.
- **Implement Layered Defenses:** Adopt a defense-in-depth strategy by enforcing network segmentation to isolate critical assets and minimize the attack surface, reducing opportunities for unauthorized access and lateral movement. Implement advanced threat monitoring solutions such as the [Group-IB Threat Intelligence Platform](#) and [Managed XDR](#) to identify malicious activity early, disrupt intrusion attempts, and prevent follow-on attacks.
- **File Naming and Patterns:** Look for filenames and distribution patterns identified in the report, such as those masquerading as legitimate software (e.g., *msedge[0-9].exe*, *wifi_driver.exe*, *temp_agente.dll*).
- **Reconnaissance Patterns:** Detect attempts to query registry keys, enumerate software, and scan for financial files (like .cnab, .240, .400, .pfx, .p12).
- **Unusual Network Activity:** BraZetsu uses WebSocket C2 communication; monitor for anomalous outbound traffic on non-standard ports to unknown external domains and IP addresses.
- **Proxy rules:** Block Pastebin and similar sites unless necessary. This stops BraZetsu from accessing the C2 configuration.

Frequently Asked Questions (FAQ)

1. What are Initial Access Brokers?

arrow_drop_down

Initial Access Brokers (IABs) are specialized threat actors who focus on gaining unauthorized entry into corporate or organizational networks. Once an IAB establishes a foothold—typically through methods such as credential theft, vulnerability exploitation, or the deployment of malware like BraZetsu—they sell this access on underground marketplaces. This allows other cybercriminal groups, such as ransomware operators or financial threat actors, to purchase the entry points and conduct their own high-impact malicious operations.

2. How does BraZetsu monetize infections?

arrow_drop_down

BraZetsu monetizes infections by functioning as the technical engine for the “Infected Marketplace”, which operates on an access-as-a-service model. These compromised systems are then listed on the marketplace as

tradable assets for criminal customers, allowing them to deploy secondary malicious payloads without needing initial access.

3. Who are the main targets of BraZetsu?

arrow_drop_down

BraZetsu targets organizations across Iberian and Latin American countries, specifically Brazil, Portugal, Spain, Argentina, and Paraguay. The malware operates across over 20 sectors, including Financial and Banking Systems, Industrial Infrastructure, Government, Law Enforcement, Cryptocurrency Platforms, Healthcare Systems, Insurance Brokerage, Logistics, E-commerce, and IT and ERP Platforms.

4. How much does it cost to access the Infect Marketplace?

arrow_drop_down

To access the Infect Marketplace, users must make a minimum deposit of BRL 30.00 using cryptocurrency via the NowPayments platform.

Mitre ATT&CK

Tactic	Technique ID	Technique
Execution	T1204.002	User Execution: Malicious File
Execution	T1059.001	Command and Scripting Interpreter: PowerShell
Execution	T1059.003	Command and Scripting Interpreter: Windows Command Shell
Defense Evasion	T1027.002	Obfuscated Files or Information: Software Packing
Defense Evasion	T1564.003	Hide Artifacts: Hidden Window
Discovery	T1012	Query Registry
Discovery	T1518	Software Discovery
Discovery	T1082	System Information Discovery
Discovery	T1016	System Network Configuration Discovery
Discovery	T1046	Network Service Discovery
Discovery	T1083	File and Directory Discovery
Discovery	T1010	Application Window Discovery
Discovery	T1217	Browser Information Discovery
Collection	T1113	Screen Capture

Command and Control	T1071.001	Application Layer Protocol: Web Protocols
---------------------	-----------	---

Indicators of Compromise (IOCs)

Network IOCs

- [hxxps://pastebin\[.\]com/raw/aF0WCxia](https://pastebin.com/raw/aF0WCxia)
- [hxxps://pastebin\[.\]com/raw/hM0nXNBP](https://pastebin.com/raw/hM0nXNBP)
- [hxxps://pastebin\[.\]com/raw/9ChwVzzw](https://pastebin.com/raw/9ChwVzzw)
- [c2\[.\]installcenter\[.\]com](https://c2[.]installcenter[.]com)
- [infectonline\[.\]store](https://infectonline[.]store)
- [infect\[.\]online](https://infect[.]online)
- [38\[.\]242\[.\]246\[.\]176](https://38[.]242[.]246[.]176)

File Hashes

- f775fe06a4c2563cb03e1aa42eb4e9532840cce9dc168ea2ca97cee7972e6b17
- 54e313434a7f3fa349e439857e23ab536a95c9927cf62f8358b5cdd9fabf2700
- 91f225dcc7a01f926b03e8540d8b5e2d6c8e3763cc30f57381d702ce638fa6b0
- cd8fc8effea20d28e76c53f3386c783e55dcb309e1525b27f7a141d51b6f6c78
- d881a60ccd03b5417a1eed184143a18a333e7e9e9e351596a7a765843643af99
- 0fa785bb9f95b113539bb909da88e6cac9a433a07935571d9bcd2d85746fc5bf
- 1510823e7c80b4db5333dd18cd5992881496da30032d6d69b2a82e1c5cf30246
- 96960409b6e1abf20eeb689d9e0a170008a15096de6a06ca5ae0d5aa56579042
- 0cd0cc49ea4ff48c675368f725e183608494f22fefa92d2f33577f70bb6c0d5d
- 30af2ec2437af0f4910d528440715540dbec6a5587f86f327316a7a781c1e2fe
- 10de6185e31539cf01c8b05d9559e65e8693efd695f315de54667ef8c04de39c
- bc91f90a5677404cf9c8f4bed7b36c22027b1549ffefee129b41fab3db3108b8
- 93bb4a4812e77ddc17c2722340d915bd5c8387316bbdbc394c201a28cb9b7c88
- 67fcfbdaab397ad1273135a3c6aa1d220ab76491cf945df081503401cc9732d2
- c4dd46e5b450349fd9fbf686a5a22f55f8371123b098104db663a3980646e138
- 3f2f48525cf082672e38808480e214775e03dd943ff2df86172665aad96a5eaa

DISCLAIMER: All technical information, including malware analysis, indicators of compromise and infrastructure details provided in this publication, is shared solely for defensive cybersecurity and research purposes. Group-IB does not endorse or permit any unauthorized or offensive use of the information contained herein. The data and conclusions represent Group-IB's analytical assessment based on available evidence and are intended to help organizations detect, prevent, and respond to cyber threats.

Group-IB expressly disclaims liability for any misuse of the information provided. Organizations and readers are encouraged to apply this intelligence responsibly and in compliance with all applicable laws and regulations.

This blog may reference legitimate third-party services such as Telegram and others, solely to illustrate cases where threat actors have abused or misused these platforms.

This material is provided for informational purposes, prepared by Group-IB as part of its own analytical investigation, and reflects recently identified threat activity.

All trademarks referenced herein are the property of their respective owners and are used solely for informational purposes, without any implication of affiliation or sponsorship.

Source: <https://www.group-ib.com/blog/brazetsu-ai-enhanced-iab-marketplace/>