

Financially Motivated Threat Actor BREEZE COMET Targets Brazil

By GoogleCloudIntel

Published: 2026-09-01 · Archived: 2026-09-03 02:00:25 UTC



Google Cloud

Threat Intelligence

BREEZE COMET is a financially motivated threat actor that targets Brazilian financial services, retail, and eCommerce organizations by abusing compromised websites, custom malware, and stolen credentials to manipulate payment systems and fraudulent transfers. The group has also used generative AI to accelerate malware and script development, while expanding its infrastructure and tactics across Latin America and Africa. [#BREEZECOMET](#) [#COBALTSPIN](#) [#REALBREEZE](#) [#MILDFROST](#) [#KICKPLATE](#) [#BOATBEAM](#) [#XWORM](#) [#ANYDESK](#)

Keypoints

- BREEZE COMET (formerly UNC5669) is a financially motivated threat actor focused on fraudulent transfers through Brazilian banking and payment systems.
- The group targets organizations with access to Pix, STR, Boleto, RSFN, mTLS credentials, and financial APIs, including banks, fintechs, retailers, and payment processors.
- Initial access has included password spraying, voice phishing impersonating IT support, RMM tools like AnyDesk, compromised government websites, and rogue hardware devices placed in retail networks.
- BREEZE COMET uses custom tools such as REALBREEZE, COBALTSPIN, KICKPLATE, MILDFROST, LIGHTPAINT, and BOATBEAM to support reconnaissance, lateral movement, persistence, tunneling, and stealth.
- The group abuses Windows, Active Directory, cloud, CI/CD, SMB, RDP, and Kubernetes environments to steal credentials, deploy backdoors, and maintain redundant access.

- Mandiant observed the actor clearing logs, deleting directories, and disabling Windows Defender real-time monitoring to hide activity and preserve access.
- Forensic evidence shows BREEZE COMET executed waves of fraudulent transactions within 24-48 hours of compromise and has likely stolen tens of thousands of USD in assets.

MITRE Techniques

- [T1110.003] Password Spraying – Used during early compromises to gain access by attempting many passwords against accounts ('use password spraying').
- [T1204.004] User Execution: Malicious Copy and Paste – Social engineering encouraged users to install RMM tools after voice calls impersonating IT support ('convince users to install Remote Monitoring and Management (RMM) tools').
- [T1566.004] Phishing: Voice Phishing – Threat actors impersonated IT support over voice calls to trick users into installing tools ('voice calls impersonating IT support teams').
- [T1021.001] Remote Services: Remote Desktop Protocol – Hijacked service accounts were used to initiate unauthorized RDP sessions ('initiate unauthorized Remote Desktop Protocol (RDP) sessions').
- [T1021.002] Remote Services: SMB/Windows Admin Shares – Commands were executed via SMB network file shares and internal scanning focused on SMB pathways ('execute commands via SMB network file shares').
- [T1057] Process Discovery – Recon utilities and scripts were used to identify systems and available resources within compromised environments ('reconnaissance utilities such as Impacket, ADRecon and ADVipscan').
- [T1082] System Information Discovery – Custom scripts searched host files and environment variables for credentials and system details ('search internal host files and environmental variables').
- [T1555] Credentials from Password Stores – The actor stole hard-coded pipeline credentials, API keys, and cloud access tokens from CI/CD environments ('steal hard-coded pipeline credentials').
- [T1003.002] OS Credential Dumping: Security Account Manager – REALBREEZE brute-forced LDAP and the group harvested credentials from internal systems ('custom LDAP brute-forcing utility REALBREEZE').
- [T1068] Exploitation for Privilege Escalation – Trend Micro reported exploitation of JBoss AS servers to gain initial access ('exploited vulnerabilities in JBoss AS servers').
- [T1018] Remote System Discovery – Network scanning across internal subnets was used to enumerate hosts and SMB pathways ('executing network scanning tools across internal subnets').
- [T1021.004] Remote Services: SSH – Scripts included scanning for SSH ports on Linux systems ('STEP 1: ENUM ALL LINUX (SSH PORT 22)').
- [T1090.001] Proxy: Internal Proxy – COBALTSPIN created a reverse SOCKS5 proxy over WebSocket to route traffic and maintain access ('reverse SOCKS5 proxy over a WebSocket connection').
- [T1090.003] Proxy: Multi-hop Proxy – Specialized tunneling was used to move traffic through boundary firewalls and segmented networks ('communicate and maintain persistent network access').
- [T1095] Non-Application Layer Protocol – COBALTSPIN used network tunneling and DNS-based channels to communicate with C2 ('establish slow, covert DNS tunnels').
- [T1090.002] Proxy: External Proxy – Compromised trusted websites were used as staging and C2 infrastructure ('compromised, trusted websites').

- [T1190] Exploit Public-Facing Application – Rogue hardware and compromised websites, plus reported JBoss exploitation, were used to reach internal environments (‘exploit vulnerabilities in JBoss AS servers’).
- [T1059.001] Command and Scripting Interpreter: PowerShell – PowerShell was used for in-memory execution, downloads, and Defender tampering (‘executed in memory via PowerShell’).
- [T1105] Ingress Tool Transfer – Malware, RMM tools, and scripts were downloaded from GitHub, open directories, and compromised sites (‘downloaded the Netcat utility’).
- [T1074.001] Data Staged: Local Data Staging – Files and payloads were staged on compromised government and municipal websites for delivery (‘used compromised Brazilian small government websites to stage RMM tools’).
- [T1071.001] Application Layer Protocol: Web Protocols – C2 and exfiltration used web infrastructure such as paste sites and HTTPS servers (‘fake IIS HTTPS server on port 443’).
- [T1041] Exfiltration Over C2 Channel – Cloud secrets were exfiltrated to public notepad sites (‘exfiltrating them to public facing notepad websites’).
- [T1562.001] Impair Defenses: Disable or Modify Tools – Windows Defender real-time monitoring was disabled to keep malware operational (‘DisableRealtimeMonitoring \$true’).
- [T1562.006] Impair Defenses: Indicator Blocking – Event logs were cleared to erase forensic evidence (‘cleared event logs across compromised hosts’).
- [T1070.001] Indicator Removal on Host: Clear Windows Event Logs – The actor cleared event logs after activity to hide movement and API use (‘cleared event logs across compromised hosts’).
- [T1070.004] Indicator Removal on Host: File Deletion – Directories created during the compromise were deleted (‘deleted directories they had created during the compromise’).
- [T1053.005] Scheduled Task/Job: Scheduled Task – Malicious scheduled tasks were used for persistence via schtasks.exe (‘abusing native scheduled tasks (schtasks.exe running as SYSTEM)’).
- [T1547.001] Boot or Logon Autostart Execution: Registry Run Keys / Startup Folder – KICKPLATE and shortcut changes were used to persist through startup mechanisms (‘modify Windows services’ and ‘shortcut (.lnk) modifications in user startup folders’).
- [T1136.001] Create Account: Local Account – Compromised accounts across AD and cloud environments were maintained to preserve access (‘persistent access to multiple accounts’).
- [T1203] Exploitation for Client Execution – Malicious documents and staged payloads were used to trigger execution on victim systems (‘infostealers disguised as legitimate tax or receipt documents’).
- [T1584.001] Compromise Infrastructure: Domains – Trusted municipal and government domains were compromised for staging and delivery (‘compromised Brazilian small government websites’).
- [T1584.006] Compromise Infrastructure: Web Services – Paste services and cloud-hosted web resources were used for exfiltration and staging (‘dntpad[.]com’).

Indicators of Compromise

- [File hashes] Malware samples for custom tooling –
3b22605244dbace8f0c07c2c599f88c4b831bb07e9998b869a5da2759d27ceec,
2214907e696bad85bde1d90c943ef66e413d7a5c6d7596ced25b74441200439a, and other 6 items
- [File names] Staged or deployed payloads and loaders – ComprovantePDF.exe, Comprovantepdf.exe, and other 6 items

- [Domains / URLs] Compromised staging and delivery sites – dontpad[.]com, procon[.]go[.]gov[.]br/ComprovantePDF[.]exe, and other 16 items
- [File names] Custom backdoors and tooling referenced in detections – COBALTSPIN, REALBREEZE, MILDFROST, BOATBEAM, KICKPLATE, XWORM
- [Network indicators] Paste site used for data exfiltration and payload hosting – dontpad[.]com, hxxps://procon[.]go[.]gov[.]br/ComprovantePDF[.]exe

Read more: <https://cloud.google.com/blog/topics/threat-intelligence/financially-motivated-threat-actor-breeze-comet-targets-brazil/>

SHARE THIS STORY

Post navigation

Source: <https://www.hendryadrian.com/financially-motivated-threat-actor-breeze-comet-targets-brazil/>