Hive Pro

Threat Level

Red

HiveForce Labs

THREAT ADVISORY

ACTOR REPORT

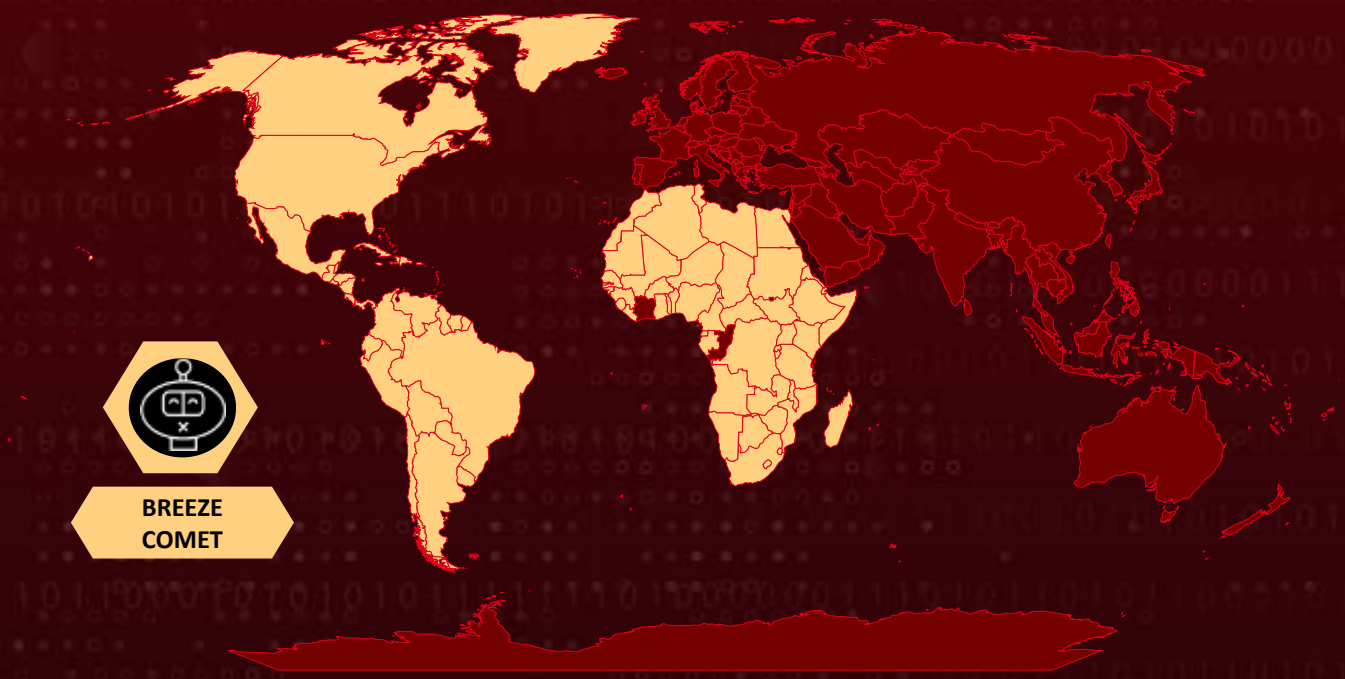
BREEZE COMET Turns Brazil's Instant Payment Rails into a Cash-Out Channel

Date of Publication	Admiralty Code	TA Number
September 07, 2026	A1	TA2026259

Summary

First Seen: September 2023
Targeted Regions: Brazil, Argentina, Bolivia, Chile, Colombia, Ecuador, French Guiana, Guyana, Peru, Suriname, Uruguay, United States, Mexico, Canada, Guatemala, Haiti, Cuba, Dominican Republic, Honduras, El Salvador, Nicaragua, Costa Rica, Panama, Jamaica, Puerto Rico, Trinidad and Tobago, Belize, Guadeloupe, Bahamas, Martinique, Barbados, Saint Lucia, Grenada, United States Virgin Islands, Antigua and Barbuda, Dominica, Bermuda, Greenland, Saint Kitts and Nevis, Saint Maarten, Anguilla, Nigeria, Paraguay, Venezuela, Ethiopia, Egypt, DR Congo, Tanzania, South Africa, Kenya, Sudan, Uganda, Algeria, Angola, Morocco, Mozambique, Ghana, Madagascar, Cameroon, Niger, Mali, Burkina Faso, Malawi, Zambia, Chad, Senegal, Zimbabwe, Guinea, Benin, Rwanda, Burundi, Tunisia, Togo, Sierra Leone, Libya, Liberia, Central African Republic, Mauritania, Namibia, Gabon, Botswana, Lesotho, Guinea-Bissau, Equatorial Guinea, Mauritius, Djibouti, Comoros, Seychelles.
Targeted Platforms: Windows, Linux, Active Directory, Cloud environments, Kubernetes, CI/CD pipelines, Java Virtual Machine (JVM) process space.
Targeted Industries: Financial Services, Fintech, Banking Software Providers, Payment Processors, Banks, Retail, Point-Of-Sale, E-Commerce, Exchanges, Government
Threat Actor: BREEZE COMET (aka UNC5669, PLUMP SPIDER, SHADOW-AETHER-064, CL-CRI-1163)
Malware: COBALTSPIN, REALBREEZE, MILDFROST, BOATBEAM, LIGHTPAINT, KICKPLATE, XWORM

Actor Map



Actor Details

#1

BREEZE COMET is a financially motivated eCrime group operating out of Brazil, formerly tracked as UNC5669 and also reported as PLUMP SPIDER, SHADOW-AETHER-064, and CL-CRI-1163. It targets Brazilian financial services, fintech, retail, and eCommerce organizations, monetizing intrusions by reaching internal payment systems and executing fraudulent transfers. Doing so requires access to the National Financial System Network (RSFN), mTLS credentials that can send authenticated transactional orders to Pix, STR, or another transactional listener, persistent access across the target's Active Directory and cloud estate, and a working understanding of the organization's transfer approval and anti-fraud controls.

#2

Activity dates back to at least September 2023; early tradecraft was simple: password spraying and voice calls impersonating IT support to get users to install RMM tools such as AnyDesk, which then served as the group's access mechanism. In 2025, both the entry points and the toolkit changed. Operators connected rogue hardware directly into retail store networks, exploited JBoss AS servers to plant web shells, and from mid-2025 staged payloads on compromised small Brazilian government websites, using trusted domains to carry delivery and C2 past reputation filters.

#3

Persistence moved from commercial RMM to malicious Kubernetes pods that stole cloud secrets and exfiltrated them to public notepad sites, then to a redundant multi-language backdoor set: LIGHTPAINT (Java, installs SoftEther VPN), MILDFROST (Java JAR, DNS tunneling fallback C2), KICKPLATE (Nim, impersonates Windows Update Health Tools), and BOATBEAM (Go, fake IIS HTTPS server on port 443). Backdoors such as XWORM persist via automated startup shortcut modifications.PowerShell disables Defender real-time monitoring to keep them running.

#4

A mature intrusion follows a consistent sequence. Reconnaissance uses Impacket, ADRecon, and ADVipscan executed in memory via PowerShell. REALBREEZE brute-forces LDAP while custom scripts mine CI/CD pipelines and host files for credentials, API keys, and the mTLS certificates needed to authenticate against core banking systems. Lateral movement runs through hijacked service accounts over RDP and SMB, after which COBALTSPIN, a Rust tunneler opening a reverse SOCKS5 proxy over WebSocket, crosses segmented financial networks. With that access, the group executes hundreds of fraudulent transactions within 24 to 48 hours, moving Brazilian Real equivalent to tens of thousands of US dollars in one observed case, then clears event logs and deletes the directories it created.

Actor Group

NAME	ORIGIN	TARGET REGIONS	TARGET INDUSTRIES
BREEZE COMET (aka UNC5669, PLUMP SPIDER, SHADOW-AETHER-064, CL-CRI-1163)	Brazil **MOTIVE** Financial Gain	Brazil, Argentina, Bolivia, Chile, Colombia, Ecuador, French Guiana, Guyana, Peru, Suriname, Uruguay, United States, Mexico, Canada, Guatemala, Haiti, Cuba, Dominican Republic, Honduras, El Salvador, Nicaragua, Costa Rica, Panama, Jamaica, Puerto Rico, Trinidad and Tobago, Belize, Guadeloupe, Bahamas, Martinique, Barbados, Saint Lucia, Grenada, United States Virgin Islands, Antigua and Barbuda, Dominica, Bermuda, Greenland, Saint Kitts and Nevis, Saint Maarten, Anguilla, Nigeria, Paraguay, Venezuela, Ethiopia, Egypt, DR Congo, Tanzania, South Africa, Kenya, Sudan, Uganda, Algeria, Angola, Morocco, Mozambique, Ghana, Madagascar, Cameroon, Niger, Mali, Burkina Faso, Malawi, Zambia, Chad, Senegal, Zimbabwe, Guinea, Benin, Rwanda, Burundi, Tunisia, Togo, Sierra Leone, Libya, Liberia, Central African Republic, Mauritania, Namibia, Gabon, Botswana, Lesotho, Guinea-Bissau, Equatorial Guinea, Mauritius, Djibouti, Comoros, Seychelles	Financial Services, Fintech, Banking Software Providers, Payment Processors, Banks, Retail, Point-Of-Sale, Ecommerce, Exchanges, Government

Recommendations

Enforce Application Control in User-Writable Paths: Apply Windows WDAC, macOS Gatekeeper or MDM, and Linux fapolicyd to block execution from user-writable directories including %APPDATA%, ~/Downloads, /tmp, and /var/tmp. Mount /tmp and /home with the noexec flag on Linux hosts.

Harden Physical Network Access at Branches and Retail Sites: Deploy 802.1X Network Access Control across physical Ethernet switch ports at branch and retail locations so unauthorized hardware cannot obtain an IP address or reach internal subnets. Disable unused switch ports, enforce port security through MAC limiting on critical drops, and physically restrict networking closets and public-facing jacks.

Restrict and Log PowerShell Execution: Enforce PowerShell Constrained Language Mode, enable Script Block Logging via Event ID 4104, and keep the Antimalware Scan Interface enabled to catch in-memory execution of reconnaissance scripts pulled from GitHub.

Inspect Outbound Traffic Instead of Trusting Reputation: Perform SSL/TLS decryption and deep packet inspection on outbound web traffic rather than relying on domain reputation scoring or .gov top-level domain allowlists. This group's core evasion advantage was staging payloads on legitimate compromised government sites.

Monitor DNS for Tunneling and Delegated Subdomain Abuse: Baseline outbound DNS volume and query patterns per host and alert on slow, high-entropy, or delegated-subdomain query chains. MILDFROST uses DNS as a covert fallback channel that survives HTTP-layer blocking.

Centralize Secrets and Eliminate Hard-Coded Credentials: Mandate a centralized secrets manager such as HashiCorp Vault with full access logging, and remove plaintext keys from code and CI/CD pipeline configuration. This group specifically mines CI/CD environments for pipeline credentials, API keys, and cloud access tokens.

Potential MITRE ATT&CK TTPs

Tactic	Technique	Sub-technique
Resource Development	T1584: Compromise Infrastructure	T1584.004: Server
	T1608: Stage Capabilities	T1608.001: Upload Malware
	T1588: Obtain Capabilities	T1588.001: Malware
		T1588.002: Tool
		T1588.007: Artificial Intelligence
Initial Access	T1566: Phishing	T1566.004: Spearphishing Voice
	T1190: Exploit Public-Facing Application	
	T1200: Hardware Additions	
	T1219: Remote Access Tools	T1219.002: Remote Desktop Software
Execution	T1059: Command and Scripting Interpreter	T1059.001: PowerShell
		T1059.004: Unix Shell

Tactic	Technique	Sub-technique
Execution	T1204: User Execution	T1204.002: Malicious File
	T1610: Deploy Container	
Persistence	T1505: Server Software Component	T1505.003: Web Shell
	T1547: Boot or Logon Autostart Execution	T1547.001: Registry Run Keys / Startup Folder
	T1543: Create or Modify System Process	T1543.003: Windows Service
	T1053: Scheduled Task/Job	T1053.005: Scheduled Task
Privilege Escalation	T1078: Valid Accounts	T1078.002: Domain Accounts
Credential Access	T1110: Brute Force	T1110.003: Password Spraying
	T1552: Unsecured Credentials	T1552.001: Credentials In Files
		T1552.007: Container API
	T1528: Steal Application Access Token	
Discovery	T1087: Account Discovery	T1087.002: Domain Account

Tactic	Technique	Sub-technique
Discovery	T1046: Network Service Discovery	
	T1083: File and Directory Discovery	
Defense Evasion	T1562: Impair Defenses	T1562.001: Disable or Modify Tools
		T1562.004: Disable or Modify System Firewall
	T1036: Masquerading	T1036.005: Match Legitimate Name or Location
	T1070: Indicator Removal	T1070.001: Clear Windows Event Logs
		T1070.004: File Deletion
	T1620: Reflective Code Loading	
Lateral Movement	T1021: Remote Services	T1021.001: Remote Desktop Protocol
		T1021.002: SMB/Windows Admin Shares
Collection	T1119: Automated Collection	
Command and Control	T1572: Protocol Tunneling	

Tactic	Technique	Sub-technique
Command and Control	T1090: Proxy	T1090.001: Internal Proxy
	T1071: Application Layer Protocol	T1071.001: Web Protocols
		T1071.004: DNS
	T1568: Dynamic Resolution	
	T1105: Ingress Tool Transfer	
Exfiltration	T1567: Exfiltration Over Web Service	
Impact	T1657: Financial Theft	

Indicators of Compromise (IOCs)

TYPE	VALUE
SHA256	3b22605244dbace8f0c07c2c599f88c4b831bb07e9998b869a5da2759d27ceec, 2214907e696bad85bde1d90c943ef66e413d7a5c6d7596ced25b74441200439a, c0db6ddd6222d02ad7490399d33c61ded0076f0037409dc8498924458646d78a, 6d4012e0dd3b56a3e52857734fa0d582cdf3c56f0e5decc8005c882d1d1c6ceb, f139b4ca15feffb7a6633ec1a431c5c604b397576b56b5c863ae8fe4fa14db4f, 51fdd83b3737add7f3832bd0ad0b56863c0a8f7cf9bcc16fd787d1ae4b403ce6, d2aa40cc53b40c6e76ac0677c4a54387b3f27ee94c85d9b2c3a3d66aeef92a66, 447e3a131e62bd33b1297739a7b959a92358a97f58554469044636a3c4f244e8

TYPE	VALUE
URLs	hxxps[:]//procon[.]go[.]gov[.]br/ComprovantePDF[.]exe, hxxps[:]//cmgovernadorluizrocha[.]ma[.]gov[.]br/Comprovantepdf[.]exe, hxxp[:]//gcm[.]setelagoas[.]mg[.]gov[.]br/files/ti[.]zip, hxxp[:]//gcm[.]setelagoas[.]mg[.]gov[.]br/files/notepadd[.]exe, hxxp[:]//gcm[.]setelagoas[.]mg[.]gov[.]br/files/tes[.]exe, hxxps[:]//minacu[.]go[.]gov[.]br/ComprovantePDF[.]exe, hxxps[:]//conseg[.]ssp[.]go[.]gov[.]br/COAF-POLICIAFEDERAL[.]exe, hxxps[:]//conseg[.]ssp[.]go[.]gov[.]br/ComprovanteBBpix[.]exe, hxxps[:]//suporte[.]camaratunapolis[.]sc[.]gov[.]br/ti/attvpn[.]zip, hxxps[:]//suporte[.]camaratunapolis[.]sc[.]gov[.]br/ti/1[.]exe, hxxps[:]//tisup[.]camaratunapolis[.]sc[.]gov[.]br/SoftEther[.]exe, hxxp[:]//suporte[.]ourinhos[.]sp[.]gov[.]br/files/s[.]zip, hxxp[:]//suporte[.]ourinhos[.]sp[.]gov[.]br[:]443/files/s[.]exe, hxxp[:]//suporte[.]ourinhos[.]sp[.]gov[.]br/files/a[.]exe, hxxps[:]//servicos[.]salto[.]sp[.]gov[.]br/j[.]jar, hxxps[:]//www[.]mrtb[.]gov[.]ng/apps/attvpn[.]vip, hxxp[:]//credeb[.]gov[.]gn/r[.]zip, hxxps[:]//sit[.]baer[.]gob[.]ve/r[.]exe, hxxps[:]//jmcov[.]gov[.]py/cxv[.]exe
Filenames	ComprovantePDF.exe, Comprovantepdf.exe, COAF-POLICIAFEDERAL.exe, ComprovanteBBpix.exe, SoftEther.exe, notepadd.exe, tes.exe, ti.zip, attvpn.zip, attvpn.vip, 1.exe, s.zip, s.exe, a.exe, j.jar, r.zip, r.exe, cxv.exe, DnsCommandBeacon.class

References

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

https://www.crowdstrike.com/en-us/adversaries/plump-spider/

What Next?

At **Hive Pro**, it is our mission to detect the most likely threats to your organization and to help you prevent them from happening.

Book a Demo of **HivePro**.

REPORT GENERATED ON

September 07, 2026 • 07:00 AM

More at www.hivepro.com