Hive Pro

Threat Level

Amber

Hiveforce Labs

THREAT ADVISORY

ATTACK REPORT

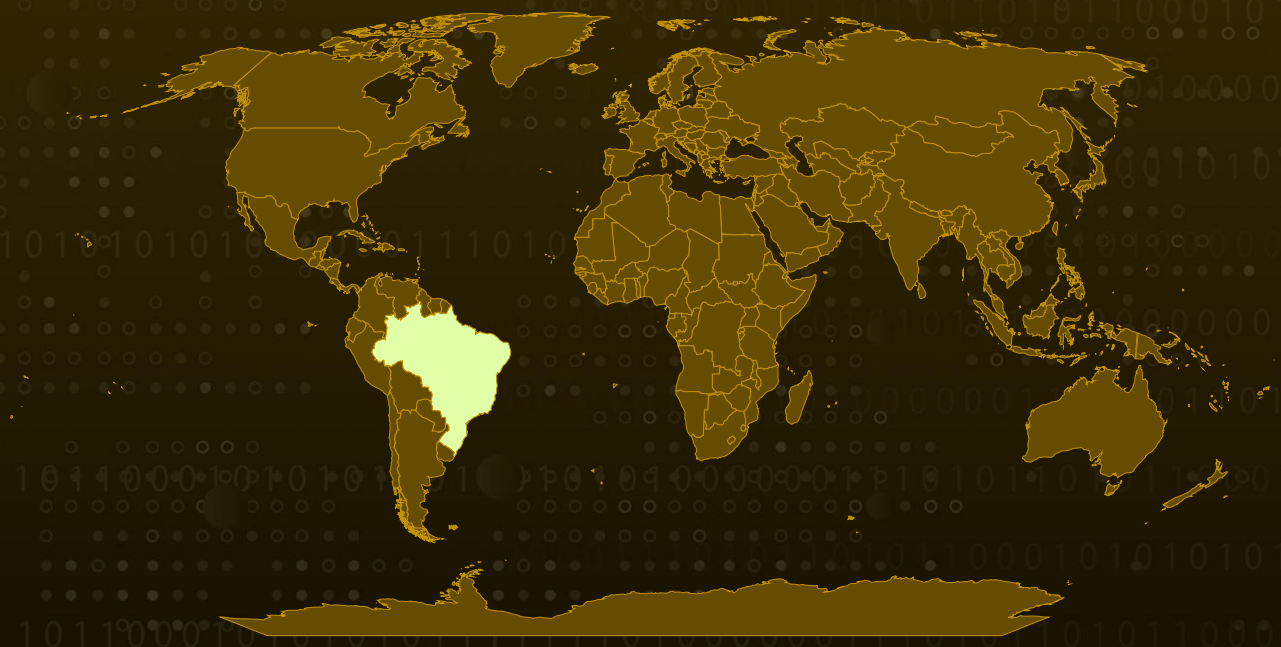
Astaroth Targets Brazil Using GitHub Infrastructure

Date of Publication	Admiralty Code	TA Number
October 14, 2025	A1	TA2025315

Summary

Attack Discovered: 2025
Targeted Country: Brazil
Targeted Industries: Banking, Cryptocurrency
Affected Platform: Windows
Malware: Astaroth
Attack: Astaroth malware is targeting Brazil, using GitHub repositories as backup infrastructure to host its malicious configurations and keep operations running even when primary servers go down. Delivered through phishing emails disguised as DocuSign messages, the attack lures victims into downloading a ZIP file that unleashes an obfuscated JavaScript and AutoIt-based infection chain, loading the Astaroth payload directly into memory. Once active, the malware focuses on stealing banking and cryptocurrency credentials from popular Brazilian financial platforms while employing advanced evasion and anti-analysis techniques to avoid detection. Astaroth continues to evolve, reinforcing its reputation as one of the most adaptive and persistent banking threats.

Attack Regions



Attack Details

#1 The Astaroth malware, first observed in 2017, has resurfaced in a new campaign targeting users in Brazil, marking the return of one of Latin America's most persistent information-stealing threats. In this latest wave, the operators are using GitHub repositories to host malware configurations, allowing them to maintain command-and-control (C2) communication even when their primary servers go offline. This strategic use of GitHub adds both redundancy and a layer of legitimacy, helping the attackers remain undetected for extended periods.

#2 The infection chain begins with phishing emails crafted to appear as DocuSign notifications. These emails lead to a malicious ZIP download, which contains a Windows shortcut (LNK) file embedded with obfuscated JavaScript commands. The URLs used in these phishing emails are geo-restricted, meaning only users in Brazil can access them. Once executed, the JavaScript script downloads several components to the ProgramData directory, including an AutoIt interpreter, a compiled AutoIt script, an encrypted payload, and a malware configuration file. The AutoIt script then runs and injects shellcode directly into memory, initializing the next stage of infection.

#3 The shellcode dynamically loads a Delphi-based DLL, which serves as the core Astaroth payload. It achieves this by resolving Windows APIs and hooking the LocalCompact function in Kernel32.dll before transferring execution to the malware's entry point. Once active, Astaroth carries out extensive anti-analysis checks, terminating execution or even shutting down the system if virtual machines, debuggers, or monitoring tools are detected. The malware specifically monitors browser activity for Brazilian banking and cryptocurrency websites. Stolen credentials and financial data are transmitted to remote servers using a custom binary communication protocol.

#4 To maintain persistence, Astaroth drops a malicious LNK file into the Windows startup folder, ensuring it relaunches after system reboots. The malware also updates its encrypted configuration every two hours, cleverly disguising these updates within image files to avoid detection.

#5 While the current campaign focuses on Brazil, Astaroth has a long history of targeting multiple South American countries, including Mexico, Uruguay, Argentina, Paraguay, Chile, Bolivia, Peru, Ecuador, Colombia, Venezuela, and Panama. Previous campaigns, **Water Makara** in 2024, also relied heavily on phishing to deliver Astaroth payloads. The latest activity reinforces the malware's evolution toward cloud-hosted infrastructure, refined evasion techniques, and modular updates, underscoring its role as one of the most adaptive and enduring banking malware threats.

Recommendations

- **Be Cautious with Unexpected Emails:** Avoid clicking on links or downloading attachments from unsolicited emails, especially those claiming to be from services like DocuSign. Always verify the sender's identity before taking any action.
- **Use Strong Email Filtering:** Enable and regularly update spam and phishing filters to block suspicious or malicious emails before they reach users.
- **Monitor Unusual System Behavior:** Look for signs such as unexpected processes, high CPU usage, or unknown startup entries. These can indicate the presence of hidden malware components.
- **Restrict Script Execution:** Limit the execution of JavaScript, LNK, and AutoIt scripts from untrusted sources to prevent initial infection.
- **Enhance Endpoint Protection:** Deploy next-generation antivirus (NGAV) and endpoint detection & response (EDR) solutions to identify and block malware. Leverage behavioral analysis and machine learning-based detection to spot suspicious activity.

Potential MITRE ATT&CK TTPs

TA0001 Initial Access	**TA0002** Execution	**TA0003** Persistence	**TA0005** Defense Evasion
TA0007 Discovery	**TA0009** Collection	**TA0010** Exfiltration	**TA0011** Command and Control
T1566 Phishing	**T1566.002** Spearphishing Link	**T1204** User Execution	**T1204.002** Malicious File
T1059 Command and Scripting Interpreter	**T1059.007** JavaScript	**T1027** Obfuscated Files or Information	**T1614** System Location Discovery
T1056 Input Capture	**T1056.001** Keylogging	**T1071** Application Layer Protocol	**T1547** Boot or Logon Autostart Execution

T1547.001 Registry Run Keys / Startup Folder	**T1090** Proxy	**T1041** Exfiltration Over C2 Channel	**T1059.010** AutoHotKey & AutoIT
T1055 Process Injection	**T1218** System Binary Proxy Execution	**T1218.005** Mshta	**T1574** Hijack Execution Flow
T1574.001 DLL	**T1027.003** Steganography		

Indicators of Compromise (IOCs)

TYPE	VALUE
SHA256	7418ffa31f8a51a04274fc8f610fa4d5aa5758746617020ee57493546ae35b70, 7609973939b46fe13266eacd1f06b533f8991337d6334c15ab78e28fa3b320be, 11f0d7e18f9a2913d2480b6a6955ebc92e40434ad11bed62d1ff81ddd3dda945, 34207fbffcb38ed51cd469d082c0c518b696bac4eb61e5b191a141b5459669df, 28515ea1ed7befb39f428f046ba034d92d44a075cc7a6f252d6faf681bdba39c, a235d2e44ea87e5764c66247e80a1c518c38a7395291ce7037f877a968c7b42b, db9d00f30e7df4d0cf10cee8c49ee59a6b2e518107fd6504475e99bbcf6cce34, 251cde68c30c7d303221207370c314362f4adccdd5db4533a67bedc2dc1e6195, 049849998f2d4dd1e629d46446699f15332daa54530a5dad5f35cc8904adea43
URLs	hxxps[:]//91[.]220[.]167[.]72[.]host[.]secureserver[.]net/peHg4yDUYgzNeAvm5[.]zip, hxxps[:]//bit[.]ly/49mKne9, hxxps[:]//bit[.]ly/4gf4E7H, hxxps[:]//raw[.]githubusercontent[.]com/dridex2024/razeronline/refs/heads/main/razerlimpa[.]png, hxxps[:]//github[.]com/dridex2024/razeronline, hxxps[:]//github[.]com/Config2023/01atk-83567z, hxxps[:]//github[.]com/S20x/m25, hxxps[:]//github[.]com/Tami1010/base, hxxps[:]//github[.]com/balancinho1/balaco,

TYPE	VALUE
URLs	hxxps[:]//github[.]com/fernandolopes201/675878fvfsv2231im2, hxxps[:]//github[.]com/polarbearfish/fishbom, hxxps[:]//github[.]com/polarbearultra/amendointorrado, hxxps[:]//github[.]com/projetonovo52/master, hxxps[:]//github[.]com/vaicurintha/gol
Domains	clafenval[.]medicarium[.]help, sprudiz[.]medicinatramp[.]click, frecil[.]medicinatramp[.]beauty, stroal[.]medicoassocidos[.]beauty, strosonvaz[.]medicoassocidos[.]help, gluminal188[.]trovaodoceara[.]sbs, scrivinlinfer[.]medicinatramp[.]icu, trisinsil[.]medicesterium[.]help, brusar[.]trovaodoceara[.]autos, gramgunvel[.]medicoassocidos[.]beauty, blojannindor0[.]trovaodoceara[.]motorcycles, 1[.]tcp[.]sa[.]ngrok[.]io[:]20262, 1[.]tcp[.]us-cal-1[.]ngrok[.]io[:]24521, 5[.]tcp[.]ngrok[.]io:22934, 7[.]tcp[.]ngrok[.]io:22426, 9[.]tcp[.]ngrok[.]io:23955, 9[.]tcp[.]ngrok[.]io:24080

References

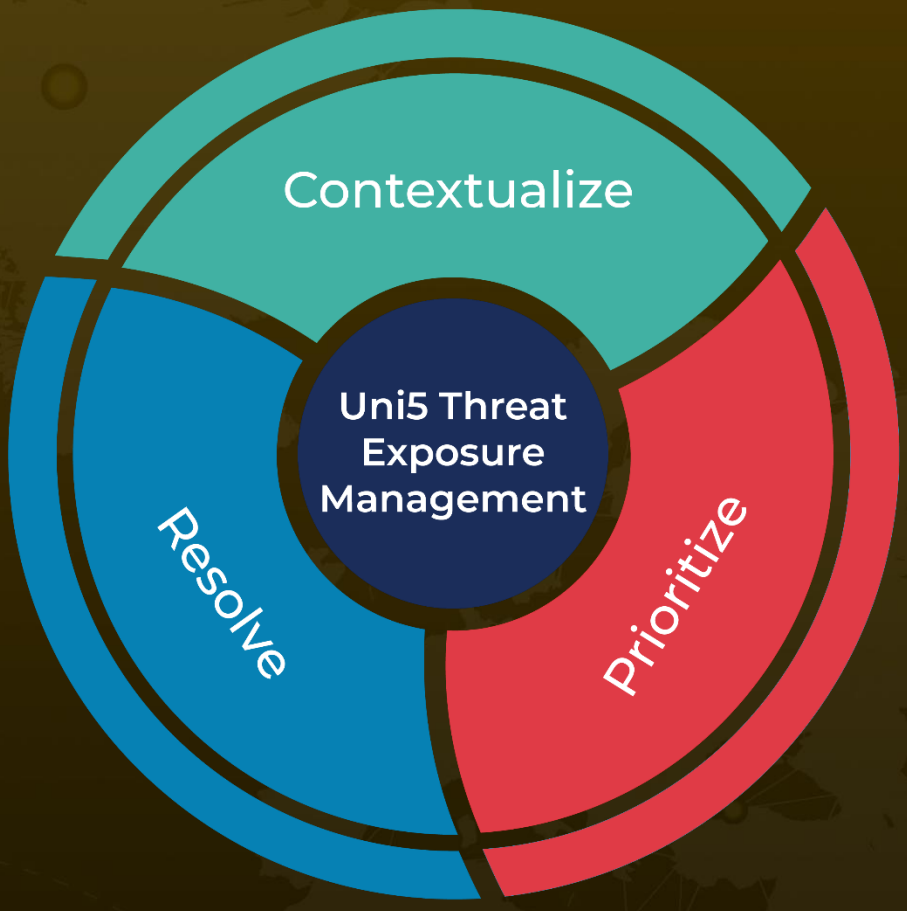
https://www.mcafee.com/blogs/other-blogs/mcafee-labs/astaroth-banking-trojan-abusing-github-for-resilience/

https://hivepro.com/threat-advisory/astaroth-strikes-again-water-makaras-sophisticated-phishing-attacks-targeting-brazil/

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 free demo with **HivePro Uni5**: Threat Exposure Management Platform.



REPORT GENERATED ON

October 14, 2025 . 10:00 AM

More at www.hivepro.com