Hive Pro

Threat Level

Amber

Hiveforce Labs

THREAT ADVISORY

ATTACK REPORT

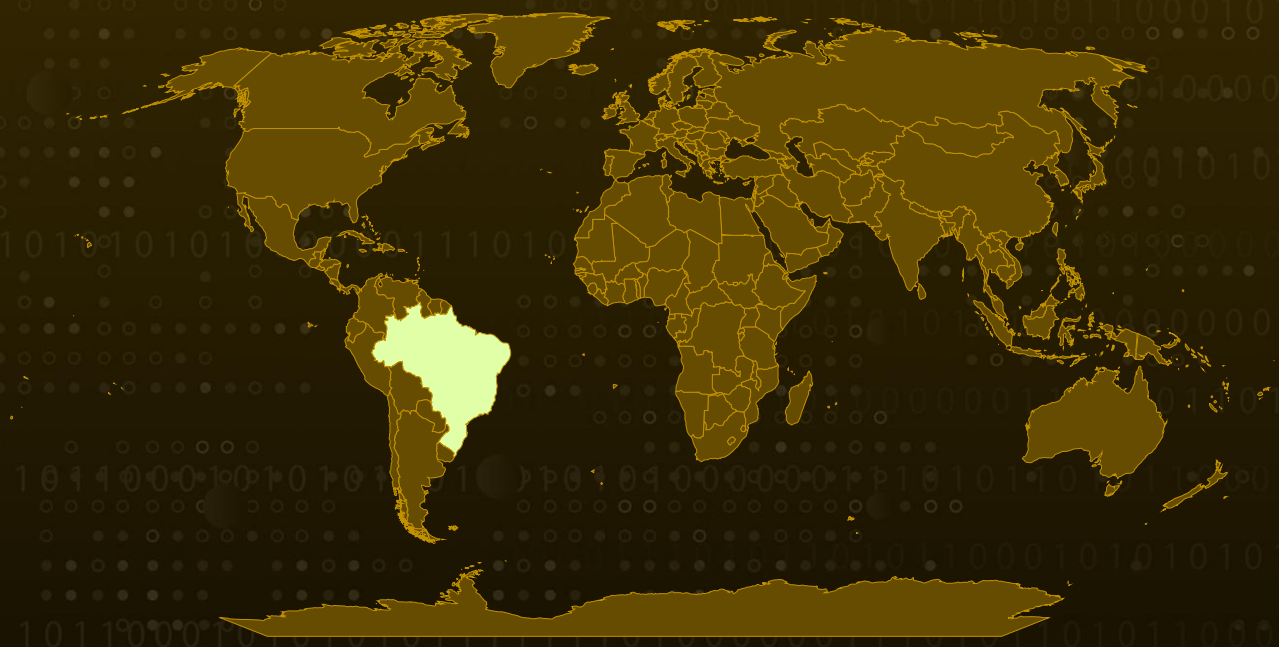
Astaroth Reimagined: Weaponizing WhatsApp for Scalable Banking Fraud

Date of Publication	Admiralty Code	TA Number
January 9, 2026	A1	TA2026008

Summary

First Seen: April 2025
Targeted Region: Brazil
Targeted Industries: Financial Services, Banking
Malware: Astaroth (aka Guildma)
Affected Platform: WhatsApp
Campaign: Boto Cor-de-Rosa
Attack: The Boto Cor-de-Rosa campaign represents a significant evolution in the Astaroth banking malware family, introducing WhatsApp-based worm propagation capabilities. This campaign leverages WhatsApp Web to automatically harvest victim contact lists and distribute malicious ZIP archives containing obfuscated Visual Basic Script downloaders. The malware operates with dual functionality: a propagation module that sustains self-reinforcing infection loops through social engineering, and a banking module that silently monitors browsing activity to steal financial credentials when victims access banking URLs. The campaign exclusively targets Brazilian victims using Portuguese-language lures and culturally appropriate social engineering tactics, including time-of-day aware greetings.

Attack Regions



Attack Details

#1

Astaroth is a well-established Brazilian banking trojan written in Delphi that has steadily evolved since its first appearance, adapting its tooling and delivery methods to stay effective. The Boto Cor-de-Rosa campaign marks a notable shift in this evolution by introducing a WhatsApp-based worm written entirely in Python. This move highlights the threat actors' adoption of a multi-language, modular architecture and a deeper reliance on social engineering. By abusing a trusted messaging platform and impersonating known contacts, the malware significantly lowers victims' suspicion while blending traditional credential theft with modern, relationship-driven infection techniques.

#2

The infection process begins with a seemingly harmless WhatsApp message carrying a malicious ZIP archive named with randomized alphanumeric strings. Once extracted, the archive reveals a heavily obfuscated Visual Basic Script masquerading as a legitimate file. Executing this script silently launches a two-track infection chain. On one side, the VBS downloader fetches an MSI installer that deploys the core Astaroth payload into a hidden directory under. The malware leverages a legitimate AutoIt interpreter paired with an encoded loader to decrypt and execute its primary components in memory, helping it evade traditional security controls.

#3

In parallel, the script installs a Python runtime and drops the zapbiu.py module responsible for WhatsApp-based propagation. This component systematically harvests the victim's WhatsApp contacts and sends out malicious ZIP files to each one, using Portuguese-language messages tailored to the time of day, such as "Bom dia," "Boa tarde," or "Boa noite." The messages are crafted to appear routine and cooperative, often claiming to share a requested file and offering further assistance if needed. Behind the scenes, the spreader closely monitors its own activity, logging delivery statistics after every 50 messages and exfiltrating contact lists and propagation data to remote command-and-control servers.

#4

The impact of this campaign is particularly severe within Brazil, where it primarily targets individual banking customers and organizations in the financial services sector. The worm-like behavior creates exponential growth potential, as each newly infected system immediately attempts to compromise every contact in its address book. This dual-module design allows Astaroth to spread laterally through personal networks while simultaneously stealing banking credentials, greatly expanding both its reach and its capacity for financial fraud. Any user accessing banking or financial portals from an infected system is exposed to a high risk of credential theft.

#5

From a risk perspective, the Boto Cor-de-Rosa campaign stands out as a high-priority threat. The abuse of WhatsApp, a platform users inherently trust, dramatically increases infection success compared to email-based attacks. Combined with culturally and regionally tailored social engineering, these factors make the campaign particularly dangerous for organizations with Brazilian operations or customer bases, warranting immediate attention and defensive action.

Recommendations

- **Be Cautious With WhatsApp Attachments:** Avoid opening unexpected ZIP files or installers received via WhatsApp, even if they appear to come from known contacts. Always verify the request through a separate message or call before interacting with shared files.
- **Disable Automatic File Downloads:** Turn off automatic media and file downloads in WhatsApp and other messaging apps. This reduces the risk of accidentally executing malicious files without deliberate user action.
- **Restrict Script and Installer Execution:** Organizations should limit the execution of scripting engines such as VBScript, AutoIt, and Python, especially from user-writable directories. Blocking unsigned scripts can break the infection chain at an early stage.
- **Strengthen Banking and Account Security:** Do not store banking credentials in browsers and enable multi-factor authentication wherever possible. Regularly monitor bank accounts for unusual login activity or unauthorized transactions.
- **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	**TA0005** Defense Evasion	**TA0007** Discovery
TA0009 Collection	**TA0010** Exfiltration	**TA0011** Command and Control	**T1566** Phishing
T1566.001 Spearphishing Attachment	**T1059** Command and Scripting Interpreter	**T1059.005** Visual Basic	**T1059.006** Python
T1204 User Execution	**T1204.002** Malicious File	**T1218** System Binary Proxy Execution	**T1218.007** Msiexec

T1036 Masquerading	**T1087** Account Discovery	**T1005** Data from Local System	**T1071** Application Layer Protocol
T1071.001 Web Protocols	**T1041** Exfiltration Over C2 Channel	**T1059.010** AutoHotKey & AutoIT	**T1027** Obfuscated Files or Information
T1105 Ingress Tool Transfer			

Indicators of Compromise (IOCs)

TYPE	VALUE
SHA256	098630efe3374ca9ec4dc5dd358554e69cb4734a0aa456d7e850f873408a3553, 073d3c77c86b627a742601b28e2a88d1a3ae54e255f0f69d7a1fb05cc1a8b1e4, bb0f0be3a690b61297984fc01befb8417f72e74b7026c69ef262d82956df471e, c185a36317300a67dc998629da41b1db2946ff35dba314db1a580c8a25c83ea4, 5d929876190a0bab69aea3f87988b9d73713960969b193386ff50c1b5ffeadd6, 9081b50af5430c1bf5e84049709840c40fc5fdd4bb3e21eca433739c260018b2e, 3b9397493d76998d7c34cb6ae23e3243c75011514b1391d1c303529326cde6d5, 1e101fbc3f679d9d6bef887e1fc75f5810cf414f17e8ad553dc653eb052e1761, 01d1ca91d1fec05528c4e3902cc9468ba44fc3f9b0a4538080455d7b5407adcd, 025dccd4701275d99ab78d7c7fbd31042abbed9d44109b31e3fd29b32642e202, 19ff02105bbe1f7cede7c92ade9cb264339a454ca5de14b53942fa8fbe429464, 1fc9dc27a7a6da52b64592e3ef6f8135ef986fc829d647ee9c12f7cea8e84645, 3bd6a6b24b41ba7f58938e6eb48345119bbaf38cd89123906869fab179f27433,

TYPE	VALUE
SHA256	4a6db7ffbc67c307bc36c4ade4fd244802cc9d6a9d335d98657f9663ebab900f, 4b20b8a87a0cceac3173f2adbf186c2670f43ce68a57372a10ae8876bb230832, 4bc87764729cbc82701e0ed0276cdb43f0864bfaf86a2a2f0dc799ec0d55ef37, 6168d63fad22a4e5e45547ca6116ef68bb5173e17e25fd1714f7cc1e4f7b41e1, 7c54d4ef6e4fe1c5446414eb209843c082eab8188cf7bdc14d9955bdd2b5496d, a48ce2407164c5c0312623c1cde73f9f5518b620b79f24e7285d8744936afb84, f262434276f3fa09915479277f696585d0b0e4e72e72cbc924c658d7bb07a3ff
Domains	centrogauchodabahia123[.]com, coffe-estilo[.]com, empautlipa[.]com, miportuarios[.]com, varegjopeaks[.]com

References

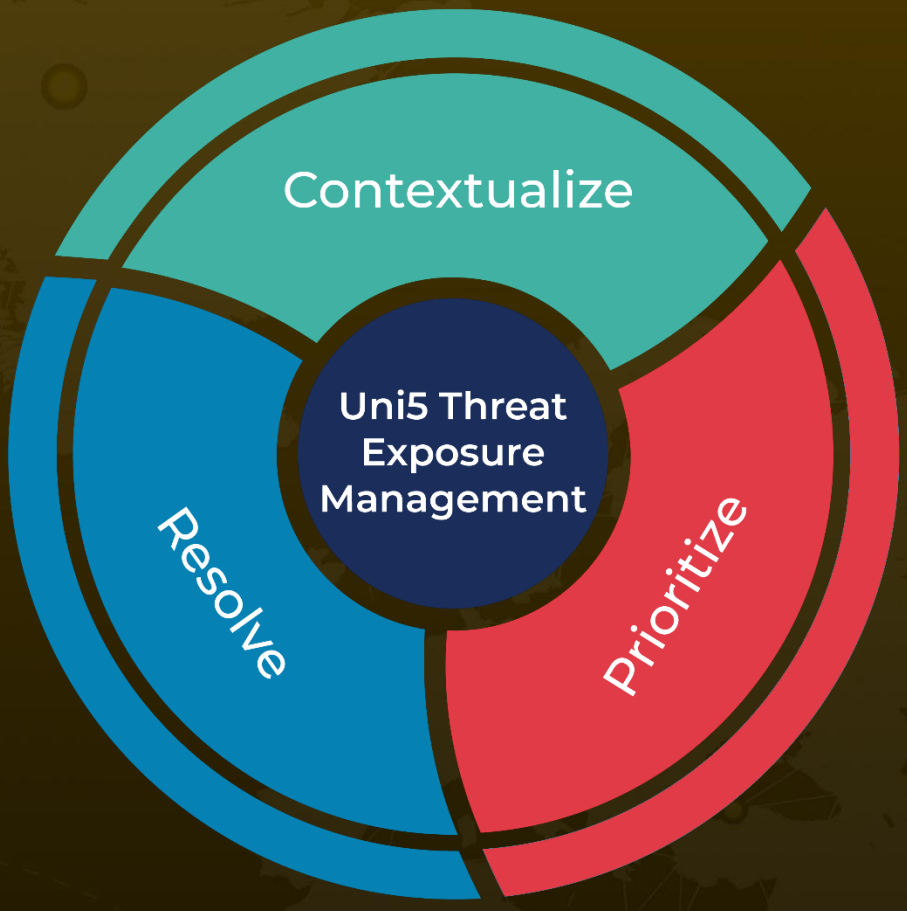
https://www.acronis.com/en/tru/posts/boto-cor-de-rosa-campaign-reveals-astaroth-whatsapp-based-worm-activity-in-brazil/

https://hivepro.com/threat-advisory/astaroth-targets-brazil-using-github-infrastructure/

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

January 9, 2026 • 8:00 AM

More at www.hivepro.com