

Astaroth's Boto Cor-de-Rosa campaign targets Brazil with new WhatsApp malware technique

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



Authors: Jozsef Gegeny, Jonathan Micael

Summary

Astaroth is a Brazilian banking malware previously covered in our analysis [Astaroth Unleashed](#), where we detailed its evolution and capabilities.

In a newly identified campaign, internally referred to as [Boto Cor-de-Rosa](#), our researchers discovered that Astaroth now exploits WhatsApp Web as part of its propagation strategy. The malware retrieves the victim's WhatsApp contact list and automatically sends malicious messages to each contact to further spread the infection.

While the core Astaroth payload remains written in Delphi and its installer relies on Visual Basic script, the newly added WhatsApp-based worm module is implemented entirely in Python, highlighting the threat actors' growing use of multilanguage modular components.

This campaign continues Astaroth's long-standing pattern of focusing almost exclusively on Brazilian victims, leveraging region-specific lures, local ecosystem knowledge and culturally familiar communication channels to maximize infection success.

Infection chain overview

The infection sequence begins when the victim receives a message on WhatsApp containing a malicious ZIP archive. The file name varies per infection but consistently follows a pattern of digits and hexadecimal characters separated by underscores and dashes (for example: 552_516107-a9af16a8-552.zip).

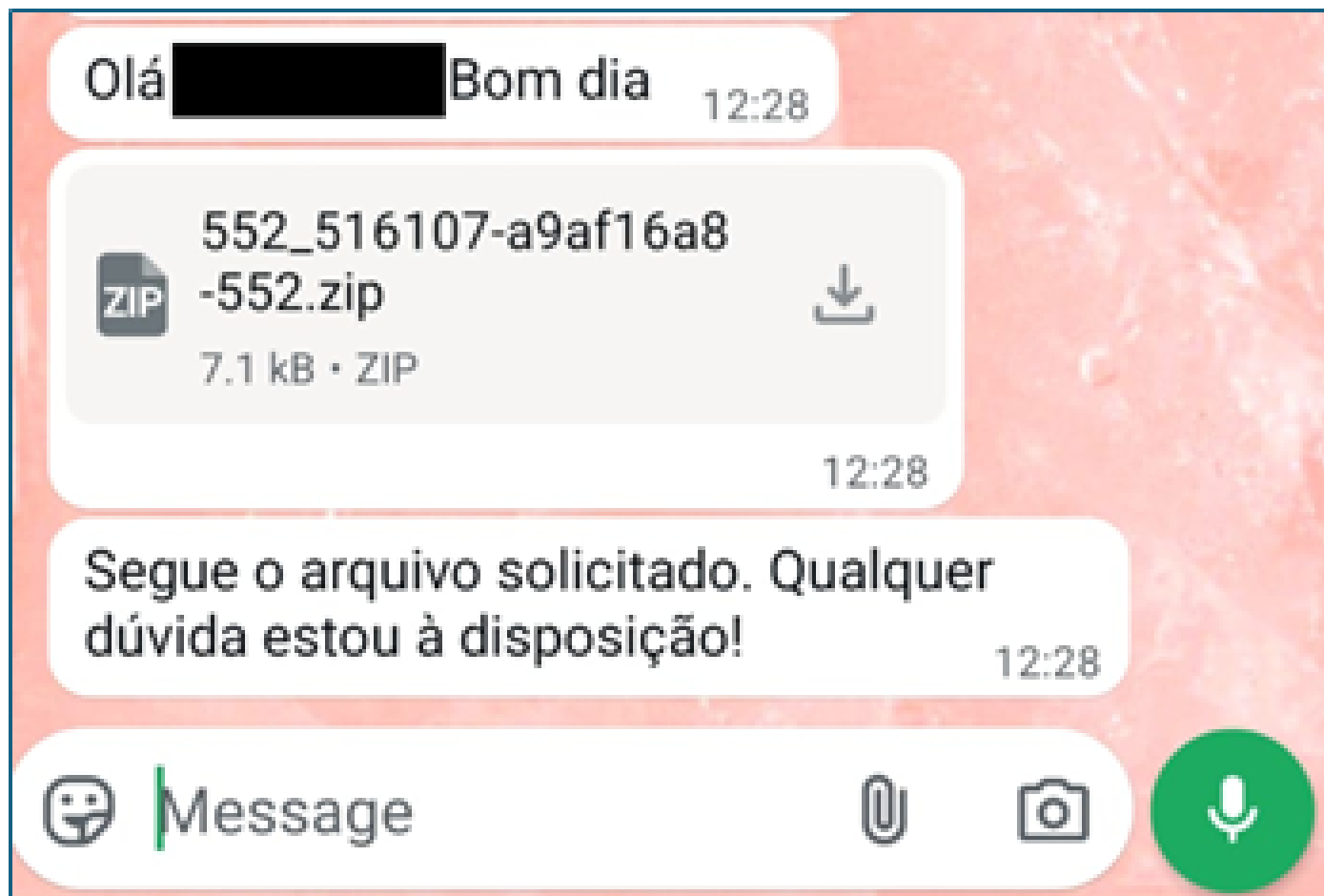


Figure 1: Message received on WhatsApp

When the victim extracts and opens the archive, they encounter a Visual Basic script disguised as a benign file. Executing this script triggers the download of the next-stage components and marks the beginning of the compromise.

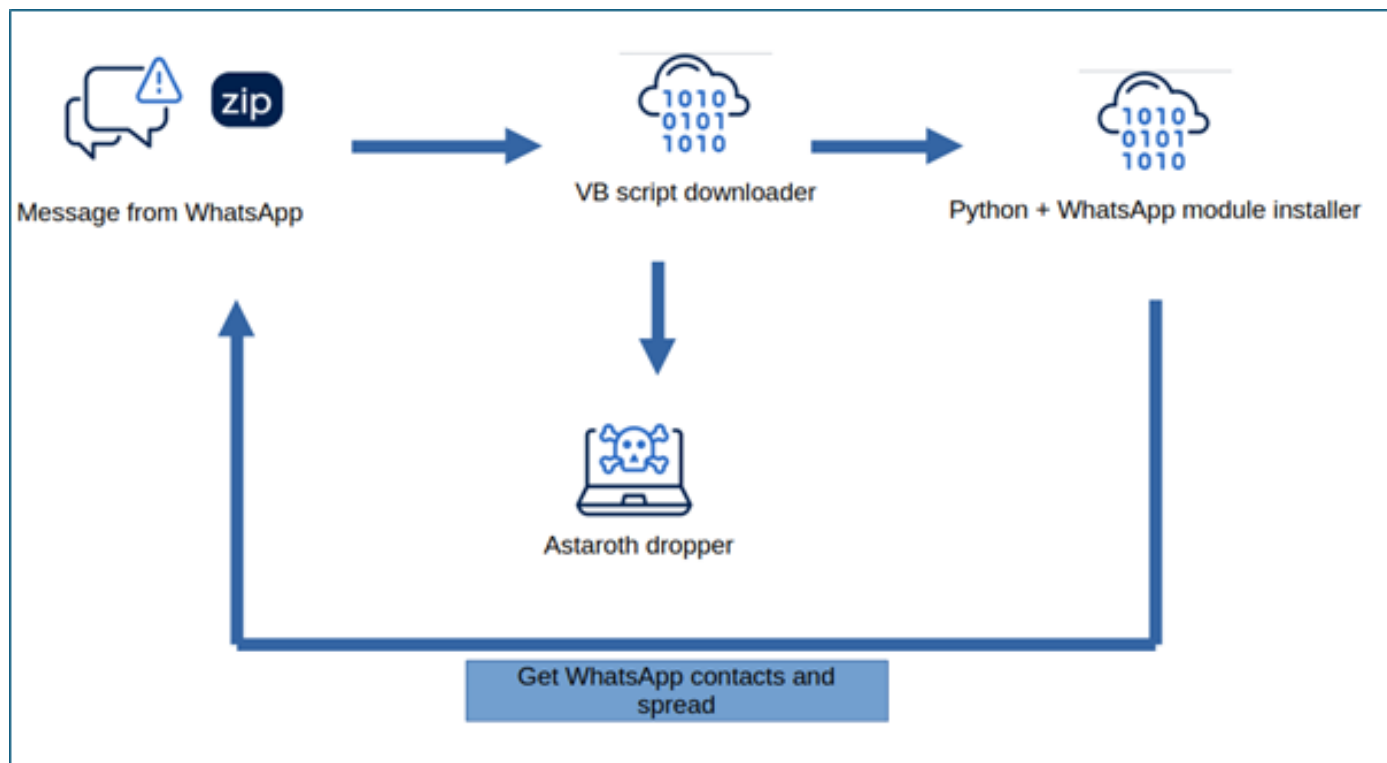


Figure 2: Infection chain

Once the payloads are delivered, the malware branches into two parallel modules:

Propagation module: This component harvests the victim's WhatsApp contacts and automatically sends each of them a new malicious ZIP file, sustaining a continuous and self-reinforcing propagation loop.

Banking module: Operating silently in the background, this component monitors the victim's browsing activity. When banking-related URLs are accessed, it activates credential-stealing functionality and other fraudulent behaviors aimed at financial gain.

Together, these modules allow the campaign to simultaneously expand its footprint and perform targeted banking fraud on infected systems.

Technical analysis

VBS downloader

The infection chain is driven by an obfuscated VBS downloader embedded inside the malicious WhatsApp ZIP archive. Although the file name varies, the script is typically around 50 to 100 KB and heavily obfuscated to hinder analysis.

Once deobfuscated, its role becomes straightforward: the VBS script retrieves and executes two additional components — the core Astaroth banking payload and the Python-based WhatsApp spreader. These downloads lay the groundwork for the multistage attack, enabling both lateral

propagation and credential-harvesting capabilities immediately after execution.

Figure 3: Initial downloader

MSI Dropper of Astaroth

The downloaded MSI package (installer.msi) deploys a collection of files into the directory: C:\Public\MicrosoftEdgeCache_6.60.2.9313:

Figure 4: Dropped files

Astaroth is well known for this deployment pattern: a legitimate Autolt interpreter is bundled alongside an encoded loader, which dynamically decrypts and loads the main Astaroth payload from disk. This modular structure helps the malware evade static detection and analysis. You can read more about this technique in our earlier in-depth write-up: [Astaroth Unleashed](#).

WhatsApp spreader

The propagation component is introduced by the initial downloader, which is responsible for installing a bundled copy of Python along with the malicious Python module zapbiu.py, enabling the new WhatsApp-based worming functionality.

Figure 5: Python installation

Figure 6: Installation of WhatsApp spreader

Once executed, this module handles the WhatsApp-based spreading mechanism, enabling the malware to harvest contact lists and dispatch new malicious ZIP archives — effectively continuing the infection loop.

A closer look at zapbiu.py source code reveals the exact message template used by the malware to initiate the fraudulent conversation:

Figure 7: Template for crafted messages

The message, originally written in Portuguese, translates to: “Here is the requested file. If you have any questions, I’m available!” This phrasing is intentionally casual and familiar, mirroring everyday interactions on WhatsApp and increasing the likelihood that recipients will trust the attachment and open it without suspicion.

What makes this implementation particularly noteworthy is the attention to social-engineering detail. Before sending the malicious ZIP file, the spreader script automatically initiates the conversation with a context-appropriate greeting. The author implemented logic to detect the local time of day and select the correct salutation: “Bom dia” (good morning), “Boa tarde” (good afternoon) or “Boa noite” (good evening).

Figure 8: Choosing the right salutation

The malware author also implemented a built-in mechanism to track and report propagation metrics in real time. The code periodically logs statistics such as the number of messages successfully delivered, the number of failed attempts, and the sending rate measured in messages per minute. For example, after every 50 messages, the script calculates the percentage of contacts processed and the current throughput, then prints a progress update:

Figure 9: Progress update

In addition to propagating itself, the component also exfiltrates the victim's contact list to a remote server:

Figure 10: Contact list exfiltration

Conclusion

The latest Astaroth campaign demonstrates the continued evolution of banking malware, combining traditional credential-stealing techniques with sophisticated social engineering and multiplatform propagation. By leveraging WhatsApp as a distribution channel, the malware not only accelerates its spread but also exploits trust-based communication patterns to increase the likelihood of victim interaction.

This campaign underscores the importance of user vigilance, particularly when receiving unsolicited files through messaging platforms, and highlights the need for organizations to deploy layered defenses that monitor both traditional attack vectors and emerging social-engineering techniques. Astaroth's integration of messaging-based propagation with financial credential theft represents a concerning trend in malware evolution, illustrating how attackers continue to blend technical innovation with psychological manipulation to maximize their impact.

Detection by Acronis

This threat has been detected and blocked by Acronis EDR / XDR:

Figure 11: Threat detection

Indicators of Compromise

ZIP files

098630efe3374ca9ec4dc5dd358554e69cb4734a0aa456d7e850f873408a3553
073d3c77c86b627a742601b28e2a88d1a3ae54e255f0f69d7a1fb05cc1a8b1e4
bb0f0be3a690b61297984fc01befb8417f72e74b7026c69ef262d82956df471e Astaroth MSI
Installers

c185a36317300a67dc998629da41b1db2946ff35dba314db1a580c8a25c83ea4
5d929876190a0bab69aea3f87988b9d73713960969b193386ff50c1b5ffeadd6
9081b50af5430c1bf5e84049709840c40fc5fdd4bb3e21eca433739c26018b2e
3b9397493d76998d7c34cb6ae23e3243c75011514b1391d1c303529326cde6d5
1e101fbc3f679d9d6bef887e1fc75f5810cf414f17e8ad553dc653eb052e1761 WhatsApp Spreaders
(Python)

01d1ca91d1fec05528c4e3902cc9468ba44fc3f9b0a4538080455d7b5407adcd
025dccd4701275d99ab78d7c7fbd31042abbed9d44109b31e3fd29b32642e202
19ff02105bbe1f7cede7c92ade9cb264339a454ca5de14b53942fa8fbe429464
1fc9dc27a7a6da52b64592e3ef6f8135ef986fc829d647ee9c12f7cea8e84645
3bd6a6b24b41ba7f58938e6eb48345119bbaf38cd89123906869fab179f27433
4a6db7ffbc67c307bc36c4ade4fd244802cc9d6a9d335d98657f9663ebab900f
4b20b8a87a0cceac3173f2adbf186c2670f43ce68a57372a10ae8876bb230832
4bc87764729cbc82701e0ed0276cdb43f0864bfaf86a2a2f0dc799ec0d55ef37
6168d63fad22a4e5e45547ca6116ef68bb5173e17e25fd1714f7cc1e4f7b41e1
7c54d4ef6e4fe1c5446414eb209843c082eab8188cf7bdc14d9955bdd2b5496d
a48ce2407164c5c0312623c1cde73f9f5518b620b79f24e7285d8744936afb84
f262434276f3fa09915479277f696585d0b0e4e72e72cbc924c658d7bb07a3ff

Contacted domains

centrogauchodabahia123[.]com

coffe-estilo[.]com

empautlipa[.]com

miportuarios[.]com

varegjopeaks[.]com