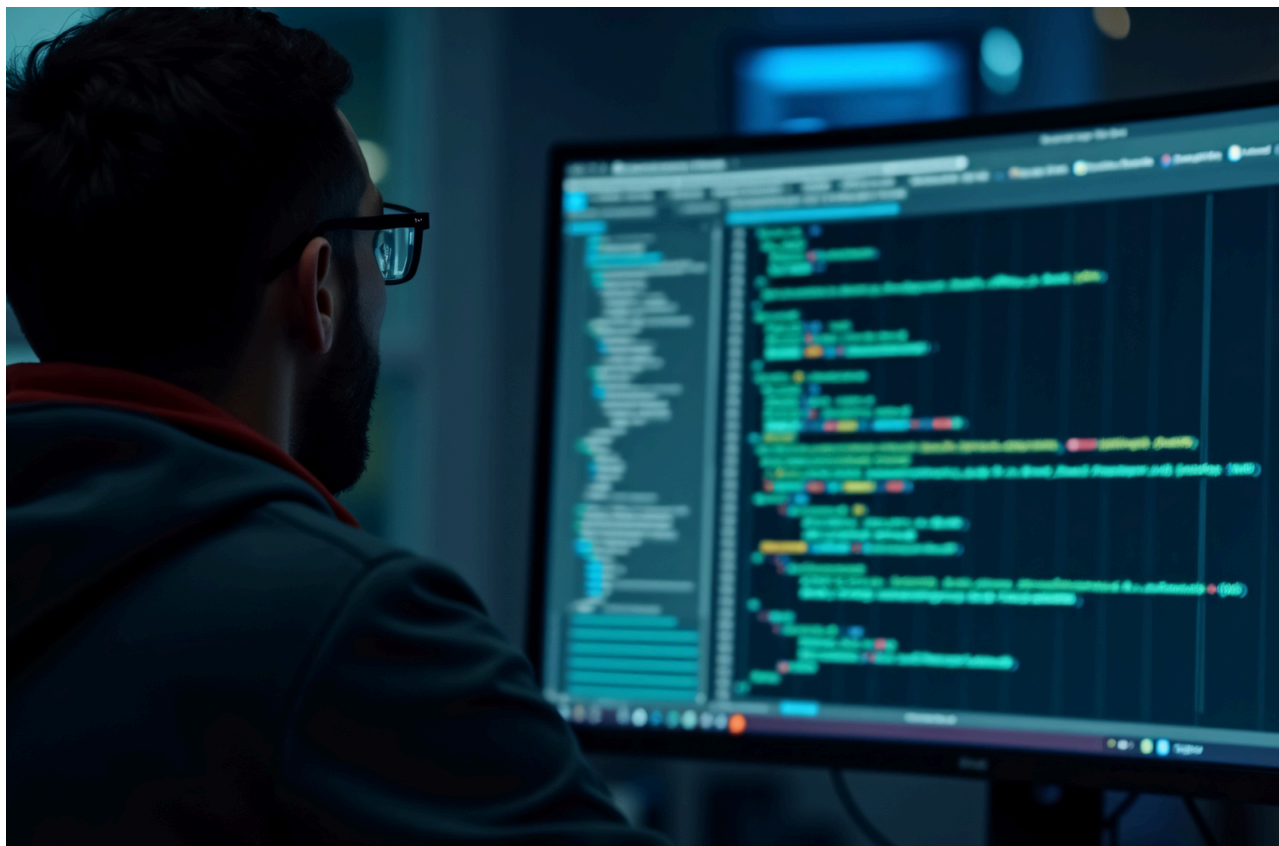


Augmented Marauder's Multi-Pronged Casbaneiro Campaigns

bluevoyant.com/blog/augmented-marauders-multi-pronged-casbaneiro-campaigns

March 31, 2026



These decrypted C2 strings appear to represent a remote configuration command set. They are compared against hardcoded reference values within the binary using an internal Delphi string comparison routine. If a match is found, a corresponding flag at a specific memory offset is flipped (set to 1), enabling that feature or behavior. This modular framework allows operators to adaptively configure the botnet to monitor and hijack webmail providers in real-time, without requiring any direct interaction with the compromised host or the deployment of new binaries.

Linkage to Broader LATAM Ecosystem

BlueVoyant assesses with high confidence the Horabot attack activity detailed in this report is operationally linked to the cybercriminal Augmented Marauder (a.k.a. Water Saci) threat group's Maverick (a.k.a. Sorvepotel) malware campaigns recently documented by [BlueVoyant's TFC](#) as well as [Trend Micro](#). The strongest technical bridge uniting these seemingly distinct toolsets is their shared reliance on the Casbaneiro (a.k.a. Metamorfo) AutoIT execution framework. Because Casbaneiro is widely viewed as an exclusive, proprietary tool operated solely by its Brazil-based developers, its presence in this infection chain serves as a high-confidence attribution anchor.

This report stands alongside recent and foundational Horabot research from [Kaspersky](#), [Fortinet](#), and [Cisco Talos](#), which highlights the use of legitimate AutoIT interpreters to decrypt and reflectively load Delphi banking payloads. In December 2025, Trend Micro [observed](#) Augmented Marauder variants employing this exact same AutoIT delivery mechanism, shortly after the group was observed deploying Maverick [.NET payloads](#) in October 2025—simultaneously identified by BlueVoyant. This highly specific execution chain, coupled with identical cryptographic seeds observed across the various malware families, strongly suggests shared developer resources or tooling for this adversary.

Furthermore, both sets of attack chains exhibit an identical, highly aggressive propagation philosophy that relies heavily on "Living off the Land" (LotL) and fileless execution techniques. Rather than simply stealing credentials and going dormant, both campaigns utilize deeply nested, script-heavy infection chains—transitioning from initial HTA, LNK, or VBS files into obfuscated PowerShell—to turn infected hosts into self-propagating botnets. Whereas this Horabot attack stream weaponizes PowerShell to manipulate Outlook COM objects and the MAPI namespace, the October-described Maverick (a.k.a. Sorvepotel) campaign utilized functionally similar PowerShell and Python scripts to automate WhatsApp Web via Chrome debugging and Selenium. In both models, the core objective is to hijack a victim's active communication session to scrape contacts and distribute malicious payloads, thereby bypassing traditional security perimeters by leveraging trusted sender identities.

Both frameworks also share rigorous anti-analysis routines, utilizing WMI and system queries to evade known antivirus directories, specific debuggers, and sandbox environments. Once resident in memory, both the Horabot and Maverick attack chains utilize continuous window-title monitoring to trigger sophisticated, fake credential overlays when victims navigate to specific Latin American and Iberian banking or cryptocurrency institutions.

Finally, this linkage is reinforced by the parallel targeting and social engineering tactics. Both campaign branches rely on nearly identical initial access lures—such as fake invoices, tax documents, or the judicial summons observed in this draft—packed inside ZIP archives. Augmented Marauder's capacity for continuous evolution is further highlighted by their adoption of "ClickFix" tactics within the Horabot attack path. As recently documented by [Kaspersky](#), the threat actors utilized fake CAPTCHA pages designed to trick victims into manually copying and executing malicious scripts via the Windows Run dialog.

Taken together, the integration of ClickFix social engineering, alongside dynamic PDF generation and WhatsApp automation, demonstrates an agile adversary that is continually innovating and executing diverse attack paths to bypass modern security controls. Ultimately, BlueVoyant assesses this adversary is maintaining a bifurcated, multi-pronged attack infrastructure, dynamically deploying the WhatsApp-centric Maverick chain and concurrently utilizing both ClickFix and email-based Horabot attack paths.

Conclusion

The discovery of this phishing campaign exposes a highly strategic, multi-pronged attack model employed by the Augmented Marauder (a.k.a. Water Saci) threat group. It is now evident that while these Brazil-based operators heavily leverage script-based WhatsApp automation to compromise retail and consumer users in Latin America, they concurrently maintain and deploy an advanced, email-hijacking engine to penetrate enterprise perimeters there and Europe as well. Despite the divergence in initial access vectors, the underlying infection chain remains unified by the Casbaneiro AutoIT execution framework.

What makes this adversary particularly dangerous is its rapid pace of innovation. Its continued use of dynamic payloads, server-side PDF lure generation and programmatic UUID-based ZIP archives allows the attackers to actively engineer methods to defeat hash-based detection and bypass modern Email Security Gateways (SEGs). Coupled with their recent integration of "ClickFix" social engineering tactics, documented WhatsApp automated attack chain and its extension to target Spanish-speaking users in Europe as well, Augmented Marauder has proven to be an agile threat group capable of continually evolving to overcome enterprise security controls.

MITRE ATT&CK Techniques

T1566 (Phishing)

T1566.001 (Spearphishing Attachment)

T1566.002 (Spearphishing Link)

T1534 (Internal Spearphishing)

T1657 (Financial Theft)

T1584 (Compromise Infrastructure)

T1204.001 (User Execution: Malicious Link)

T1059.001 (PowerShell)

T1059.005 (Command and Scripting Interpreter: Visual Basic)

T1059.007 (Command and Scripting Interpreter: JavaScript)

T1027 (Obfuscated Files or Information)

T1140 (Deobfuscate/Decode Files)

T1055 (Process Injection)

T1497 (Virtualization/Sandbox Evasion)

T1218.005 (System Binary Proxy Exectuion: Mshta)

Indicators

hxxps://ge.factu.it[.]com/GZSPEGIJ/YFSBNPQK

hxxps://104.21.19[.]50/GZSPEGIJ/YFSBNPQK

hxxps://ge.factu.it[.]com/g1/ld1/

hxxps://ge.factu.it[.]com/g1/

hxxps://tt.grupobedfs[.]com/.../gera_pdf.php

hxxps://cgf.facturastbs[.]shop/a/08/150822/au

factu.it[.]com

grupobedfs[.]com

facturastbs[.]shop

239cb9232fe01c8b82eb627f66acc6848cb223dfea46d4923844c1fe20f1de49 - PDF Sample

3e4002c7f0909d3c743b3586098e248d413f485c6bb033cafdb322bd8b206ebb - PDF Sample

1af69a3283e28a8cc9a11819ecc2f2cff46dcabbfa78cefc71a02b881a064593 - HTA

69fc15919044fc6a94bb251afd90a0a07204b79df3bc62c49ba6b0febefbc33e - HTA

d1d08f7e44641d921fad22ed175b928c696befd14a55271eb203f8fcaff553d5 - ZIP

b56d00addd6c6a266de3c739dad22aa1de52624066544929754d47332257cba6 - ZIP

1693448804bf1c90ad7317af250bcd6ea021256e33e983b224aea81d4ecc2e20 - staticdata.dll

4e08a1525a62a387595a2e4942b56ec3f3b3259996115ea2e6ea3638ccb87705 - staticdata.dll