Hive Pro

Threat Level

Amber

Hiveforce Labs

THREAT ADVISORY

ATTACK REPORT

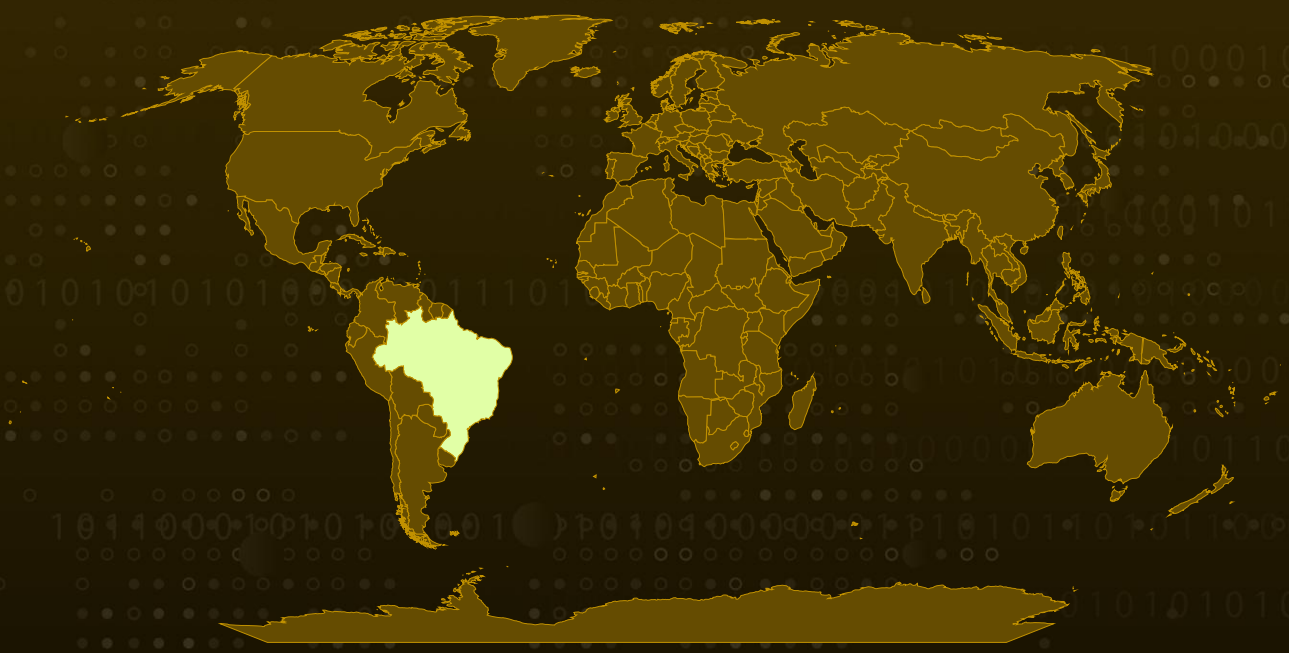
Water Saci Campaign: Multi-Stage Malware Spreading via WhatsApp Web

Date of Publication	Admiralty Code	TA Number
December 4, 2025	A1	TA2025368

Summary

First Seen: 2025
Targeted Country: Brazil
Malware: SORVEPOTEL
Affected Platform: Windows
Targeted Industries: Finance, Banking, Cryptocurrency
Campaign: Water Saci
Attack: Water Saci is a rapidly evolving malware campaign spreading through malicious files delivered over WhatsApp and WhatsApp Web, using multi-stage scripted loaders to deploy a banking-focused backdoor. It conducts system reconnaissance, injects into legitimate processes, and propagates worm-style by hijacking victims' WhatsApp sessions. The latest wave is more advanced than the October attack, shifting from MSI/PowerShell loaders to more evasive Python-based and multi-format delivery. Overall, it represents a highly adaptive threat combining social engineering, stealth, and automated financial credential theft.

Attack Regions



Attack Details

#1

The Water Saci campaign is a financially motivated malware operation primarily targeting users in Brazil. It spreads mainly through WhatsApp and WhatsApp Web, where victims receive malicious files such as ZIP archives, PDFs, or HTA documents disguised as invoices, receipts, or business communications. Once opened, these files execute a multi-stage script chain that downloads additional components and installs the main payload, typically the SORVEPOTEL backdoor, a trojan built to steal banking information and maintain remote access to the infected system.

#2

The attack chain is notable for its multi-format delivery and heavy obfuscation. The malware uses layered scripts (HTA -> script -> downloader -> automation loader) to evade detection and avoid dropping easily-scannable executables. The payload conducts reconnaissance on the victim's system, checking for banking activity, browser history, and installed security products. When sensitive activity is detected, Water Saci injects itself into legitimate processes to hide its presence and intercept credentials, session data, or financial information.

#3

One of the most dangerous aspects of Water Saci is its worm-like propagation. After infection, the malware hijacks the victim's WhatsApp Web session and automatically forwards the same malicious files to all contacts and groups, exploiting trust relationships to spread rapidly. Combined with anti-sandbox checks and stealthy persistence mechanisms, the campaign is both fast-moving and difficult to analyze.

#4

Compared to the October attack, the new Water Saci campaign shows clear evolution. Earlier attacks relied primarily on MSI installers and PowerShell-based loaders, making the infection chain more traditional and easier to detect. The current wave replaces these components with Python-based scripts, more diverse file formats (including HTA), improved automation, and more sophisticated obfuscation. The shift suggests rapid development by the operators, possibly aided by automated code-conversion tools or AI, resulting in a more flexible, evasive, and scalable infection method.

#5

Water Saci represents a modern hybrid of social engineering, automation, and stealth. By abusing a widely trusted platform like WhatsApp, using multi-stage scripting to hide activity, and adapting quickly between campaigns, the operators behind Water Saci continue to refine a highly effective financial-theft ecosystem.

Recommendations

Strengthen user awareness and training: Warn users to be cautious with any file received over WhatsApp or WhatsApp Web, even if it appears to come from a known contact. Emphasize that ZIP, PDF, HTA, LNK, or other unexpected attachments should never be opened without verification. Encourage employees to verify suspicious messages via a secondary channel (phone call, SMS, email).

Implement stricter controls on script execution: Restrict or disable execution of HTA, VBS, PowerShell, and Python scripts for regular users whenever possible. Enforce PowerShell Constrained Language Mode and block high-risk file types at the endpoint or email/web gateway (ZIP, ISO, HTA, MSI, etc.). Deploy application allowlisting (AppLocker or Windows Defender Application Control) to limit unauthorized scripts.

Harden endpoints and browsers: Ensure Windows systems are fully patched and that reputable endpoint protection (EDR or next-gen AV) is enabled. Block or alert on suspicious process behavior such as process hollowing, script spawning, or non-browser processes making network calls. Configure browsers to block unauthorized extensions and clear session cookies after high-risk activity.

Monitor messaging platforms and automate detection: Raise monitoring on WhatsApp Web usage within corporate environments, especially for large bursts of outbound ZIP/PDF file transfers. Set alerts for unusual automation patterns (e.g., browser automation tools, repetitive outbound messaging traffic).If feasible, isolate messaging applications in sandboxed browser profiles or dedicated virtual containers.

Protect financial transactions and sensitive accounts: Encourage the use of 2FA or hardware tokens for banking and internal systems. Require financial users or high-privilege staff to operate from hardened, secured workstations. Monitor for access to Brazilian banking sites or finance platforms initiated from unusual or newly installed processes.

Potential MITRE ATT&CK TTPs

TA0010 Exfiltration	TA0042 Resource Development	TA0001 Initial Access	TA0002 Execution
TA0005 Defense Evasion	TA0008 Lateral Movement	TA0009 Collection	TA0011 Command and Control
TA0007 Discovery	TA0003 Persistence	T1588.007 Artificial Intelligence	T1041 Exfiltration Over C2 Channel
T1056.003 Web Portal Capture	T1056 Input Capture	T1105 Ingress Tool Transfer	T1588 Obtain Capabilities
T1566 Phishing	T1204 User Execution	T1059 Command and Scripting Interpreter	T1566.001 Spearphishing Attachment
T1059.005 Visual Basic	T1204.002 Malicious File	T1059.001 PowerShell	T1547 Boot or Logon Autostart Execution
T1620 Reflective Code Loading	T1055 Process Injection	T1036 Masquerading	T1027 Obfuscated Files or Information
T1082 System Information Discovery	T1217 Browser Bookmark Discovery	T1071 Application Layer Protocol	T1573 Encrypted Channel
T1059.006 Python	T1059.010 AutoHotKey & AutoIT	T1614 System Location Discovery	T1518 Software Discovery
T1140 Deobfuscate/Decode Files or Information	T1055.012 Process Hollowing	T1614.001 System Language Discovery	T1518.001 Security Software Discovery
T1574 Hijack Execution Flow	T1574.001 DLL	T1497 Virtualization/Sandbox Evasion	T1547.001 Registry Run Keys / Startup Folder
T1083 File and Directory Discovery	T1113 Screen Capture		

Indicators of Compromise (IOCs)

TYPE	VALUE
SHA256	12f2e7e997480a3ea3150614664d6de4e6e229dacd6e8ff0ed74cd22207e753d, 15e8f315901ea12639665f1adb9d18a9ace1074a33d70e47ad43203eb8ebfba4, 2d95769a016b397333ba90fdc2f668f883c64774a2c0aaaf6b2d942bebaee9e0, 495697717be4a80c9db9fe2dbb40c57d4811ffe5ebceb9375666066b3dda73c3, 5db59a8a8c2ca54615a6079fa9035d2886c1ec2270ee508efbb0ff98c98b90be, 6745bb11b8c692be78ec7ade285094beef907ecb3a99f475afa284ccbe7565f2, 67ad7a950257cc5920b2119539049bcea3863bb2002f7118fcef57788f7eca59, 6ee5355b786282a6904806a4f55e59e9aad8067ae01b37afaf0009527e5c0205, 9b0996380c61060ed3bfec25962c56131ea0eac42c7f373216aab72fdb7b8ac7, a416cad095a6e77857f8fba4552ddc8ece41ce997b5086a4fbea5ac0fdfc4860, c03fecbf52c38cf363bbc4f94bbe183e394f921af756442b674f4fe5f2b2090c, de07516f39845fb91d9b4f78abeb32933f39282540f8920fe6508057eedcbbea, ebe37505fa162461515d50bd86cb0fd983a000d418f0be0f9098e087170909bd, ec69a53fd3ff11327aa98248bf55572f4ea8c1b40a12f49f5669f3df1f598353, f262434276f3fa09915479277f696585d0b0e4e72e72cbc924c658d7bb07a3ff
SHA1	a1c88a022e55d73a2894ddfb8b7bf5381d9f13dd
MD5	5bcb9f187320893d1b1c36fa0c18e094
Domains	centrogauchodabahia123[.]com, storeshomeestusfluworkss[.]online
URLs	hxxp[:]//centrogauchodabahia123[.]com/altor/installer[.]msi, hxxp[:]//centrogauchodabahia123[.]com/altor/whatsz[.]py

References

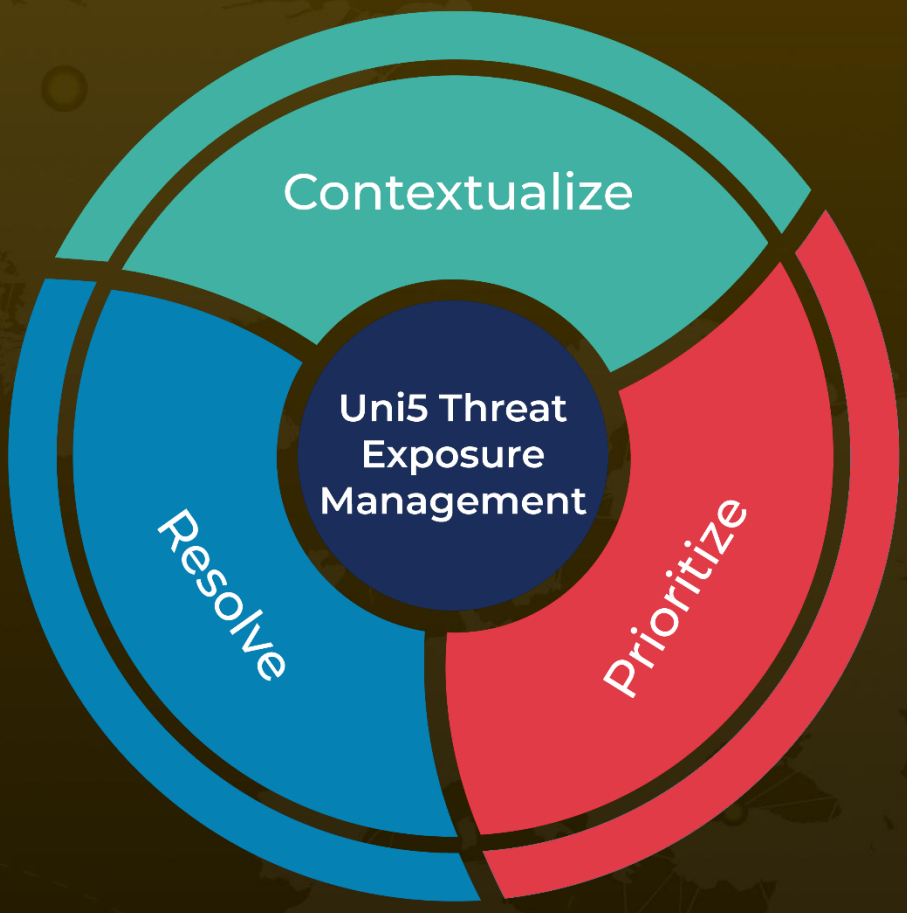
https://www.trendmicro.com/en_us/research/25/l/water-saci.html

https://hivepro.com/threat-advisory/water-saci-brazils-whatsapp-borne-malware-storm/

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

December 4, 2025 • 10:00 AM

More at www.hivepro.com