Hive Pro

Threat Level

Amber

HiveForce Labs

THREAT ADVISORY

ATTACK REPORT

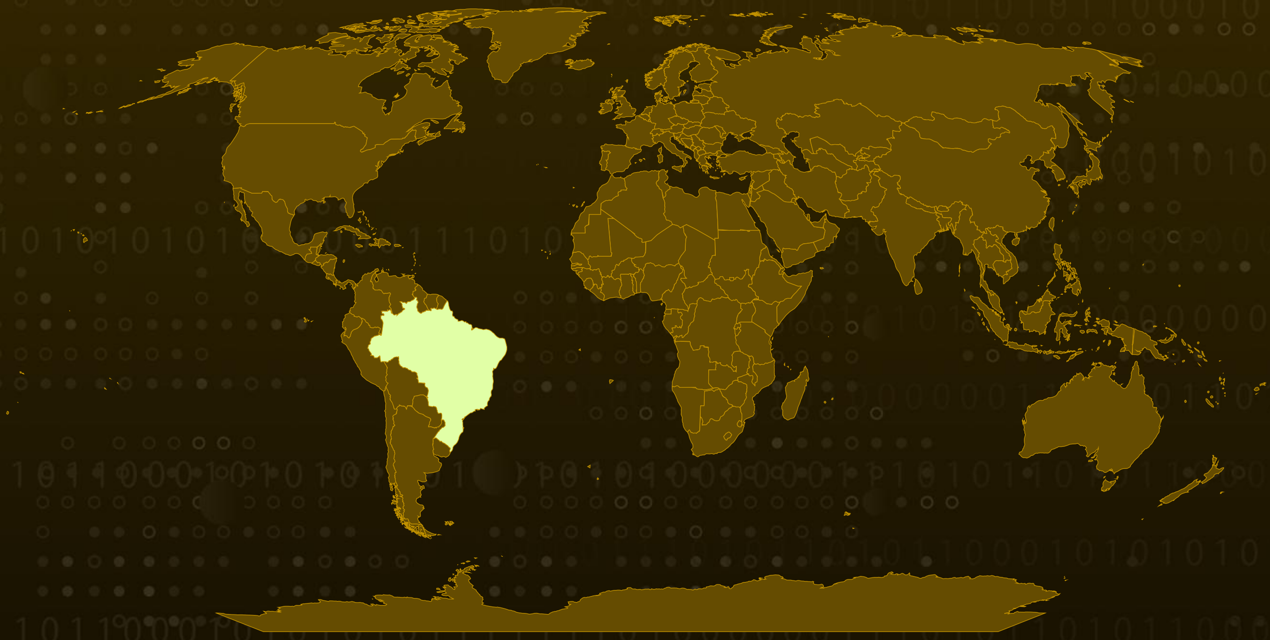
Water Saci: Brazil’s WhatsApp-Borne Malware Storm

Date of Publication	Admiralty Code	TA Number
October 7, 2025	A1	TA2025306

Summary

Attack Discovered: 2025
Targeted Country: Brazil
Targeted Industries: Financial Institutions and Crypto Exchanges
Affected Platform: Windows
Malware: SORVEPOTEL
Campaign: Water Saci
Attack: Water Saci is an aggressive malware campaign that exploits WhatsApp to spread the SORVEPOTEL malware, primarily targeting Windows users in Brazil. It propagates through deceptive messages carrying malicious ZIP attachments that, once opened, execute PowerShell commands to fetch additional payloads in memory. SORVEPOTEL can hijack active WhatsApp Web sessions to automatically send infected files to all contacts and deploy realistic banking overlays to steal credentials from Brazilian institutions. With its multi-stage architecture, stealthy in-memory execution, and regional targeting, Water Saci showcases a sophisticated fusion of automation and social engineering.

Attack Regions



Powered by Bing

© Australian Bureau of Statistics, GeoNames, Microsoft, Navinfo, Open Places, OpenStreetMap, Overture Maps Fundation, TomTom, Zenrin

Attack Details

#1 The Water Saci campaign represents an unusually aggressive malware operation that leverages WhatsApp as its primary infection channel, a shift from conventional phishing and ransomware attacks. The campaign centers on a malware strain dubbed SORVEPOTEL, designed for rapid propagation rather than monetary theft. It capitalizes on user trust, automation, and social familiarity to spread primarily among Windows users in Brazil. Victims receive deceptive WhatsApp messages containing malicious ZIP attachments disguised as legitimate business documents.

#2 Once executed, SORVEPOTEL uses PowerShell commands to communicate with C&C servers, downloading additional payloads that execute directly in memory to evade detection. These payloads enable surveillance of banking activities, sustain self-replication through WhatsApp, and maintain persistent C&C connections for continuous updates. Beyond individual victims, the campaign poses a broader threat to businesses, serving as a template for how messaging platforms can be exploited to launch wide-scale propagation attacks.

#3 The infection process typically begins when victims receive a message from a compromised contact, often impersonating a colleague or friend. These phishing messages, written in Portuguese, include ZIP archives, posing as receipts or invoices. Opening them reveals Windows shortcut (.LNK) files that covertly trigger PowerShell or command-line scripts, fetching the main payload from attacker-controlled domains. These scripts run silently in hidden mode, using Base64 encoding and layered obfuscation to conceal their activity. The malware ensures persistence by copying itself to the Windows Startup directory, guaranteeing execution upon reboot, and maintains multiple C&C connections for receiving updates or additional components.

#4 Once inside a system, it automatically spreads to all available contacts and groups by dispatching the same malicious ZIP file, leading to rapid infection bursts and, in some cases, account suspensions due to automated spam-like behavior. The attack unfolds in multiple stages, from a PowerShell-based loader to .NET DLL modules designed to fetch encrypted shellcode, evade debugging, and execute payloads through reflective loading in memory-only operations. Advanced stages, identified as Maverick.StageTwo and Maverick.Agent, focus on monitoring browser activity.

#5 In its final phase, Water Saci deploys a WhatsApp-focused payload that utilizes Selenium automation and Chromedriver to control browser sessions and automatically send malicious messages. This component ensures continuous spread, verifying active WhatsApp Web sessions before initiating propagation. The malware checks regional settings to confirm its execution environment and terminates if conditions don't match. While the campaign currently prioritizes self-replication and reach over data theft, its architecture suggests potential for future evolution into credential theft or ransomware delivery.

Recommendations

Be Cautious with Unexpected WhatsApp Messages: Avoid opening ZIP files or clicking on links, even if they appear to come from friends or coworkers. Attackers often compromise one account and use it to trick others into downloading malware.

Keep Work and Personal Communication Separate: Refrain from using personal messaging apps like WhatsApp for business-related exchanges. If it's necessary, ensure your organization has clear BYOD (Bring Your Own Device) and messaging policies in place.

Update and Secure Your Systems: Make sure Windows, browsers, and all security tools are regularly updated. This reduces the risk of known vulnerabilities being exploited to install or spread malware.

Disable Automatic Downloads and Previews: Configure WhatsApp Web, email clients, and browsers to block auto-downloads of attachments and images. This adds an extra layer of protection against drive-by infections.

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

TA0042 Resource Development	TA0001 Initial Access	TA0002 Execution	TA0003 Persistence
TA0005 Defense Evasion	TA0007 Discovery	TA0009 Collection	TA0010 Exfiltration
TA0011 Command and Control	T1566 Phishing	T1566.003 Spearphishing via Service	T1059 Command and Scripting Interpreter
T1059.001 PowerShell	T1204 User Execution	T1204.002 Malicious File	T1204.001 Malicious Link

T1547 Boot or Logon Autostart Execution	**T1547.001** Registry Run Keys / Startup Folder	**T1027** Obfuscated Files or Information	**T1140** Deobfuscate/Decode Files or Information
T1574 Hijack Execution Flow	**T1574.001** DLL	**T1057** Process Discovery	**T1614** System Location Discovery
T1497 Virtualization/Sandbox Evasion	**T1124** System Time Discovery	**T1071** Application Layer Protocol	**T1071.001** Web Protocols
T1113 Screen Capture	**T1056** Input Capture	**T1056.001** Keylogging	**T1041** Exfiltration Over C2 Channel
T1105 Ingress Tool Transfer	**T1055** Process Injection	**T1082** System Information Discovery	**T1586** Compromise Accounts
T1036 Masquerading			

Indicators of Compromise (IOCs)

TYPE	VALUE
SHA256	2150f38c436eabebd3a93b3ace1064315153c882ce763991b6d0fb798766e0db, bd62148637152396b757c8b106d5a62982bce9df12f0a6030dda9138e44e7328, 2d83c4d620866f4ae647ed6a70113686bb7b80b1a7bbdcf544fd0ffec105c4a6, 3b68826e4a1d95b1dd58b3bf1095750f31a72d8bddd1dbb35e6547ac0cf4769b, 1a0af26749f5bc21732c53fc12f3a148215c8221cbeffe920411656f1ffe7500, 441a2ad553d166df3cd0ea02482f4b8370e8f9618753e1937a251a6318cb8eba, dcdde53c50aef9531c9f59f341a4e2d59796cdd94a973f2c2a464b2cafed41f5, c50b6ff360e5614d91f80a5e2d616a9d0d1a9984751bf251f065426a63dac0b5

TYPE	VALUE
URL	hxxps[:]//sorvetenopote[.]com/api/itbi/Q77xivT4udoXayYELTwehMD666ovP6DZ
Domains	expansiveuser[.]com, imobiliariaricardoparanhos[.]com, sorvetenopote[.]com, www[.]expansiveuser[.]com, www[.]sorvetenopote[.]com, zapgrande[.]com, sorvetenopoate[.]com, sorvetenoopote[.]com, etenopote[.]com, expahnsiveuser[.]com, sorv[.]etenopote[.]com, sorvetenopotel[.]com, casadecampoamazonas[.]com, expansivebot[.]com, bravexolutions[.]com, adoblesecuryt[.]com, saogeraldoshoping[.]com
IPv4	23[.]227[.]203[.]179, 140[.]99[.]164[.]81, 92[.]246[.]130[.]15

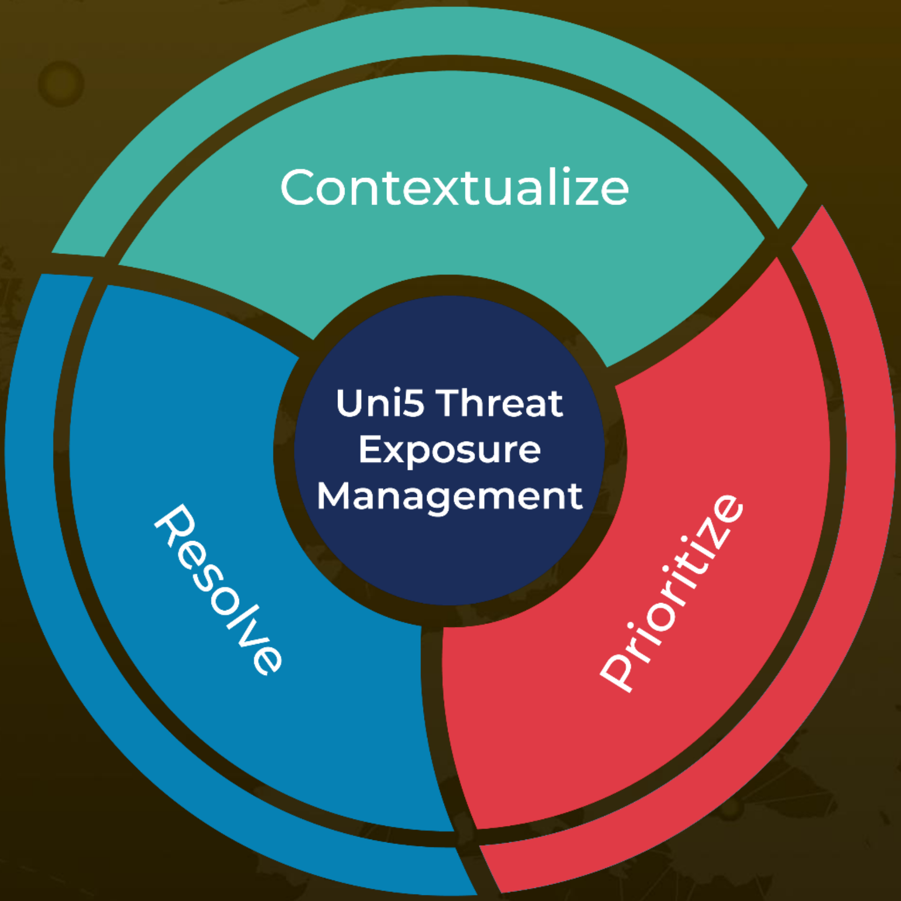
References

https://www.trendmicro.com/en_us/research/25/j/self-propagating-malware-spreads-via-whatsapp.html

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 7, 2025 • 7:30 AM

More at www.hivepro.com