Hive Pro

Threat Level

Red

Hiveforce Labs

THREAT ADVISORY

ATTACK REPORT

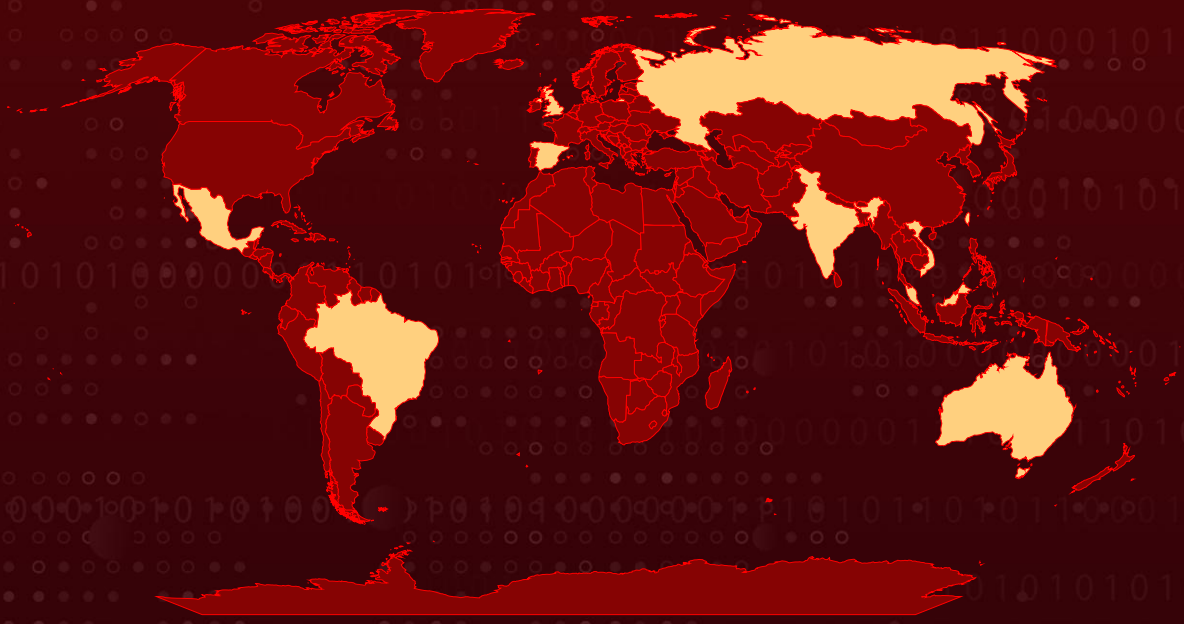
WhatsApp Campaign Turns Victims into Remotely Managed Hosts

Date of Publication	Admiralty Code	TA Number
June 23, 2026	A1	TA2026174

Summary

First Seen: June 2026
Targeted Regions: Malaysia, Brazil, India, Mexico, Singapore, United Kingdom, Spain, Taiwan, Australia, Russia, Vietnam
Targeted Platform: Microsoft Windows
Targeted Products: WhatsApp Desktop, WhatsApp Web (ManageEngine Endpoint Central abused as the delivered remote-access payload)
Attack: An active campaign distributes heavily obfuscated VBScript files through direct messages on compromised WhatsApp accounts, disguised as business and financial documents. When opened on Windows, the script triggers a multi-stage chain that downloads secondary VBScript payloads, attempts to disable User Account Control by modifying the ConsentPromptBehaviorAdmin registry value, and silently installs a preconfigured ManageEngine Endpoint Central (RMM) agent via msiexec. The agent connects to attacker-controlled management servers, granting the operator persistent remote administration over the victim's system.

Attack Regions



Targeted Non-Targeted

Attack Details

#1

An ongoing malware campaign is targeting WhatsApp users in multiple countries with deceptive messages that push VBScript files, leading to remote system access. The operation relies on compromised WhatsApp accounts to distribute malicious attachments to contacts, often without any accompanying message. To increase the chances that recipients will open the files, the attackers disguise them as invoices, account statements, debt notices, payment records, and banking documents. The scripts also include comments and metadata designed to mimic legitimate Microsoft Windows Update components, with several artifacts written in simplified Chinese. Infection requires only two actions from the victim: downloading the attachment and opening it. Depending on whether the target uses WhatsApp Desktop or WhatsApp Web, the script is launched through different parent processes, although the exact method used to compromise the sending accounts remains unclear.

#2

Once executed through Windows Script Host, the first-stage VBScript creates a hidden working directory under C:\Users\Public\Documents\, using randomized names such as Temp_<random> or MSUpdate_<random>. Hidden and system attributes are often applied to reduce visibility. To make analysis more difficult, the malware uses string concatenation, encoded VBScript, randomized variables, and large amounts of junk code, with some samples rebuilding commands and URLs character by character. Several variants copy legitimate utilities such as curl.exe and bitsadmin.exe into the working directory and rename them to resemble DLL files. Others download payloads disguised as PDF or TXT files before renaming them as VBS scripts. Regardless of the variant, the initial script retrieves and launches two additional VBScript payloads, continuing the infection chain.

#3

One of the second-stage scripts focuses on weakening system protections by targeting User Account Control (UAC). It repeatedly attempts to modify the ConsentPromptBehaviorAdmin registry value, using the runas mechanism to request elevated privileges and suppress administrative prompts. The change is performed in a loop with short delays, increasing the likelihood of success once the user approves elevation. Meanwhile, a companion script creates another hidden directory and retrieves a ZIP archive through multiple methods, including curl, bitsadmin, certutil, PowerShell, and direct HTTP requests. The archive is extracted using the Shell.Application COM interface, and some variants remove the Zone.Identifier alternate data stream to eliminate Mark-of-the-Web warnings before executing a script named setup1.vbs.

#4 Rather than immediately stealing data, the final stage gives attackers persistent remote access. The downloaded archive contains a preconfigured ManageEngine Endpoint Central deployment package, including the UEMSAgent installer, configuration files, certificates, and the malicious setup1.vbs launcher. After verifying that the required files are present, the script relaunches itself with administrative privileges and silently installs the agent through msiexec.exe, concealing the installation process from the victim. The embedded configuration connects the system to attacker-controlled Endpoint Central servers, granting operators long-term remote administration capabilities over compromised hosts.

#5 Current analysis suggests that the campaign is opportunistic rather than highly targeted. Its combination of social engineering, heavy obfuscation, abuse of legitimate Windows utilities, and repurposing of trusted remote management software shows how threat actors are increasingly blending malware techniques with legitimate administration tools to establish persistent access while minimizing suspicion.

Recommendations

Block Attacker RMM and Staging Infrastructure: Block the attacker-controlled Endpoint Central management server IPs and the listed staging domains at the network perimeter, proxy, and DNS layers.

Restrict Windows Script Host Execution: Disable or restrict wscript.exe and cscript.exe for standard users and block execution of .vbs, .vbe, and .js files originating from messaging-app download paths and user-writable directories using WDAC or AppLocker.

Hunt for Unauthorized Endpoint Central Agents: Inventory endpoints for unexpected ManageEngine Endpoint Central (UEMSAgent) installations, validate them against your authorized RMM baseline, and isolate and remediate any agent configured to contact the listed servers.

Detect LOLBin and Staging Behavior: Create detections for renamed or copied curl.exe, bitsadmin.exe, and certutil.exe executing from C:\Users\Public\Documents\, for these utilities downloading files, and for creation of hidden or system working directories with randomized names (Temp_ , MSUpdate_ , Sys , Data).

Detect Silent MSI Installs from Script Hosts: Flag msiexec.exe silent installation activity initiated by wscript.exe, which is a strong signal of the setup1.vbs-driven agent deployment.

Harden WhatsApp Attachment Handling: Train users to treat unsolicited WhatsApp attachments as untrusted even when they appear to come from known contacts, and to never open script or executable file types (VBS, VBE, EXE, BAT, CMD, JS, PS1) without independent verification.

Strengthen Messaging-Account Security: Enforce WhatsApp two-step verification and educate users on account-takeover indicators, since compromised accounts are the campaign's distribution vector.

Potential MITRE ATT&CK TTPs

Tactic	Technique	Sub-technique
Resource Development	T1586: Compromise Accounts	T1586.001: Social Media Accounts
Initial Access	T1566: Phishing	T1566.003: Spearphishing via Service
Execution	T1204: User Execution	T1204.002: Malicious File
	T1059: Command and Scripting Interpreter	T1059.005: Visual Basic

Tactic	Technique	Sub-technique
Execution	T1218: System Binary Proxy Execution	T1218.007: Msiexec
Privilege Escalation	T1548: Abuse Elevation Control Mechanism	T1548.002: Bypass User Account Control
Defense Evasion	T1112: Modify Registry	
	T1027: Obfuscated Files or Information	T1027.010: Command Obfuscation
	T1036: Masquerading	T1036.003: Rename System Utilities
		T1036.008: Masquerade File Type
	T1564: Hide Artifacts	T1564.001: Hidden Files and Directories
	T1553: Subvert Trust Controls	T1553.005: Mark-of-the-Web Bypass
	T1197: BITS Jobs	
Command and Control	T1105: Ingress Tool Transfer	
	T1219: Remote Access Software	

Indicators of Compromise (IOCs)

TYPE	VALUE
MD5	c7f38cbb99c8b74fa0465293feeba700, b7cd06c71465038b658a6dc1f273a507, 9f13c7b8ba391b2f597874e54d310648, 993f4c0cadbc769a4b0ed62a918db58d, 7f81c1bc8cfd588e8998968e2621456e, 7403cbcc5a9c32384d431856dc48fcc9, 68c16c46f8afb9e00bbaba0207fb0a46, 66442f2457eca8f47385b1fb2c6fcab8, 6359e6236471cbe434d0ef4c42b7f879, 5b6bbcc06cf08cc99e1afeda486d42fb, 5002eca748205d544618e3bd2dedc223, 4f0593e8e0e8fac49429e9b45ebf7fa1, 4044e4b6471c9de7b0a4ba37d9d9df9a, 20209b3a32769afc6a75694b8d8839dd, 0ba93109757776a44de9d8c88baa4963, 02bb20455cc592a69c080abac770ce90, 6c39900d77dcba158e1d27c7619cb06d, dad708e050632a4280cabf98ac1376b7, 05d188f071d097f5b6bd8138749b4b14, 2c6f05f1f309d89b2236e6c8b59c88f9, 3b1aba44dd3d9b6339b6f56e2f42034b, d43fdaa1f0ee09d7e5f0f94ee9df7b6c, df4fa0369eaca5cec348be293890d4af, 63ac85195b73753333316a889cf5880f, 74fd9f91fc93b6288b4fc253ea5b3e20, d06333c360b51456f427e616c3c5f8bd, 993f4c0cadbc769a4b0ed62a918db58d, 1d94fbe9cab21278cc3f104bea334d08, 9d9ac85765e4a818a3ccabe2cf4fef82, 6fb6a55424adfb61e31f06aef33273e5, f90ed4b2d0b67114aa89ddfed658e5c0, 8c3322009b8982663c0cbecd9492e7eb, 66705384a7ad81d14c34fc6c054a0ecf, 8c6d9fc389ad3f20ccbc71d77eb39bfa, 1a3cc75466ffb1971482f7abf7aabc3f, 1c47c63e5ed25060d95359c57c77b107, 31037a42ca048e06e69a78f55bc2eff5, 7f16449cd0c4862d1eadf8a5742bf09a, 79ecd61b09b0f2d54b34586c916c4ec9, 7849061c536a3efb05a56d504694e7e7, ddaffe9849f7f3c79f8804adb9a6b3d5, d01cad98dd0d01b75e04e784953c5e2b

TYPE	VALUE
Filenames	Financial Reports.vbs, Debt confirmation.vbs, Electronic statement(A).vbs, Financial Reports(s).vbs, Outstanding Payment List.vbs, Statement of debt (4).vbs, Debt Note (2).vbs, Statement of Debt(30K).vbs, Applicationform1.vbs, Extrato de Conciliação.vbs, Statement of Debt(29K).vbs, billing statement (2).vbs, Statement of Debt(A).vbs, Financial Reports(C1).vbs, Le formulaire de demande le plus récent .vbs, Outstanding Balance Sheet(A).vbs, Outstanding Balance Sheet.vbs, Penyata bank.vbs, Account Statement（13K） (2).vbs, Statement of Account.txt, Bitte füllen Sie das Formular für Umsatzsteuer-Nullsatz-Verkäufe aus.vbs, Account Statement.vbs, Statement of Account(O).vbs, Sila semak bil anda.vbs, FinancialReportsS.vbs, Promissory_Note(b).vbs, Debt Statement.vbs, Income Tax Return Form.vbs, dfjieya.vbs, 0lf.vbs, iowepv.vbs, btksfmsi.vbs, home3.vbs, zipats.vbs, 1122.vbs, payload_1.vbs, sac8.vbs, 6oy.vbs, kof.vbs, sleestak_payload_1.vbs

TYPE	VALUE
Domains	temu[.]baskwms[.]top, invoice[.]msopsa[.]top, qse[.]shoppes[.]help, shaaslong[.]one, baoxis[.]cc, baolongwes[.]oss-ap-southeast-1[.]aliyuncs[.]com, sdcwww[.]oss-ap-southeast-1[.]aliyuncs[.]com, baoyuw2s[.]s3[.]ap-southeast-1[.]amazonaws[.]com, hksha3[.]s3[.]ap-southeast-1[.]amazonaws[.]com, sjdkjj23[.]s3[.]ap-southeast-1[.]amazonaws[.]com, xijkwm2[.]s3[.]ap-southeast-1[.]amazonaws[.]com, yifubafu[.]s3[.]ap-southeast-1[.]amazonaws[.]com, caiwuascw[.]s3[.]us-east-005[.]backblazeb2[.]com, facaia[.]s3[.]us-east-005[.]backblazeb2[.]com
IPv4	202[.]61[.]160[.]202, 202[.]61[.]160[.]201, 202[.]61[.]160[.]137, 202[.]61[.]160[.]160, 202[.]61[.]160[.]208, 38[.]55[.]151[.]63
SHA256	1BBB72557FCAA408BFE02EF68DC1C6C4CED901A461BE3F3754B0D2F691EEE032, 4E2C296A386B54B3E8360D899AFB10DA87DE403687754BBA200FBF3AFBB634EA, 586607815075BAFBE7A868C658E0A5A43E959EBACE304DDF3925FA8A6B2D5B6C, 69EFBEA795491BDAC117A299F18977F1E2968A06E7CD3A11F6366169D7214B04, 30DED95156D23EA8911D76B07AC0E4DFC90D9F2ED94545775F355F118A2BEB13, A34B77D553F35517EFBE27D1AFB966FA4E8819ADF5DECEE8B7E496C84AEA4260, 09CFE9DBD75095B17CCEA62466FF128279E54A0D501587EC9C5B992B987B5784, 65662FBFEE31784502F46A4EA3CF58A5146D6F6299B40391CD71C9FC67E3E621, 03402DBFC9CCFE612C37405BBCF072C9C07273FE4F77E82F8238A31D0040094D, B798FCBC54E84C03AC2B7BE97D016D05F04CD754DB36DD5C6CFBF3AEDD0B7DFF, F10DAE1863E89F72ADF8BA913B8A9FA898E6A430430098722E626000A2D4E94A4, 1F92DA4C68B8C88EDF6E055EF75EFD1DCF55296E252545F5782880F6556564D4,

TYPE	VALUE
SHA256	6169AEE26B75B486018E4FD10A2EC8D67DE7D382C9F2900F2B8D78EA0C1CDA33, CCA9C3F98C6552A7B52132B4FB3D969DB5C743B7E663E630D37CE8B2F619C30A, 0D3D531A8FAE455A0676EF4408A683C8AF0671FD589BB6106AFF4637439D73A7, 452259DC297F56CF22C7932E8FBCEFE821EF9C3127134074FAE585F89355D397, A95EE5A8C40C7705F1612335F3E4F4FCD8A28692095C04E0D48F7A6E77CAA42B, 3140C5BEE192B0F125E188451A68B82199EE551DBAB78C92D04711588C400669, 2223CC6687D89A5273041E5410948A852536ED8B63D67A8CEC9E0FDAE884CB64, F37D677AD936D6409E64A3ECC9F3685C455826DB3DABBF21E8C54EB01EBD9128, 01F1EB07125DB5DE0C2362AFC777AA015F136FEABD769628F01D01AC6472646C, 02A7DB29D35CF01ED94B6DFB14A7026BB2906D8FA9A99EF801040C52284CCEB1, D36F50ECFB6A9104F235DF7AEFDBDDAB699495532EDE9C79EF1A577DCE359A90, CFF48752738313B9CB36BB381BBD415AC7D2E8395387B972460B58983AF68FB7, AE44EE4B40C478C109E795C328812D9EBB82750233CF18D0DD3AC1D4518A08C6, 99681A15717AEDB8F3D2DF119D313334442F8505869866F8BFDABD54DD7C8AC3, 69EFBEA795491BDAC117A299F18977F1E2968A06E7CD3A11F6366169D7214B04, 4195EFDEB8833F17E545D1E46BFCBFA634382A5EFE5696CEDC24043C9E116372, 3A18072502C440C51CF8BF42F21FA6FA3216788982892868380C04818FB61291, 1C5E88505728E1B11507FE7D6672EB89DE200BD45C79030FE60EDAE2A17B69CF, 3C9CC5B72FDD0A52FCECAE8C5B952933163527599A15189A01DED39A1A8609E4, 5ADF130842C88D6B732DEF0F5FD1BE2A889A3F7DFBC5AF5FF7438374F3DED233, 27B5CEA842C0ADD3CB0D7A106EE190EDA65201E45CFCFD20F340FD26D1290118, 07F4130E0A52E8C63D8C3DCC989EB185161EA917A9C45900692FDF031AF13AB1,

TYPE	VALUE
SHA256	845D8887EC023255C9896D1644C821168C33B5E8426519228AB3003715FE19DC, 50C74B468C217776B8890B841BAEFEC8B196B14083A7873A9201C838A8E4C90A, 76D351946565AED51B1CB8361097CA5E7D9A6D281300A188CFA8AFF9B6845234, BE532BE5BEAC3C7656654628CC557E546AEA3EE47C0046428A53D23AC58875D1, C30408B75EBC58D15F2766DB15E3789DBF2909B0D71C99A13499E25270C275EE, 28292B9822D83E28C0A5BB3BEFDD5B188BE351314E9B3A1C2740702722999CFA, 4A1B69A8AB51378C1E36C5D9944C4A345E0502CB8CFE2AB7FD9A9496553B02C6

References

https://securelist.com/whatsapp-vbs-rmm-campaign/120290/

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 Demo of **HivePro**.

REPORT GENERATED ON

June 23, 2026 • 08:50 AM

More at www.hivepro.com