Hive Pro

Threat Level

Amber

Hiveforce Labs

THREAT ADVISORY

ATTACK REPORT

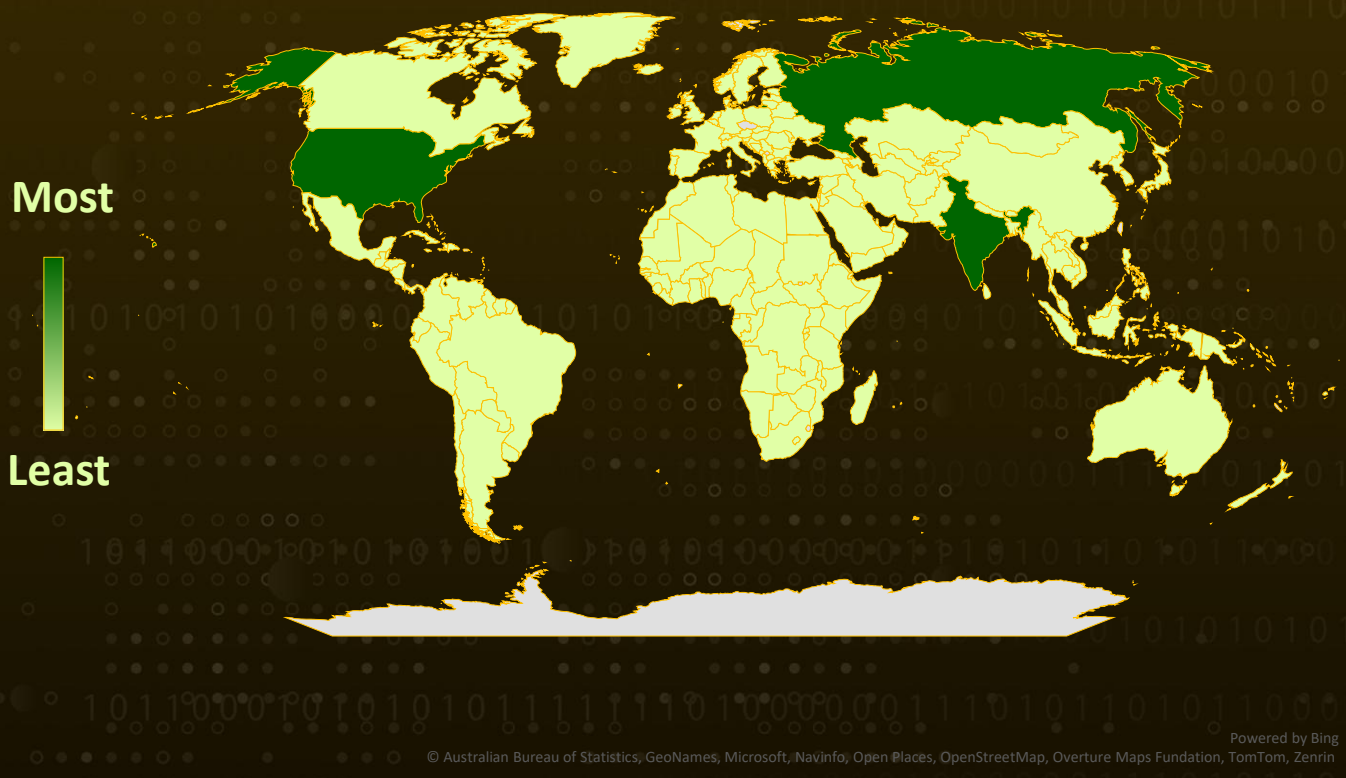
StopAndProtect: Nearly 2,000 Hacked WordPress Sites Weaponized as Criminal Infrastructure

Date of Publication	Admiralty Code	TA Number
August 20, 2026	A1	TA2026239

Summary

First Seen: May 2026
Targeted Regions: Global (compromised hosts concentrated in the United States, Russia, and India)
Targeted Platforms: Windows, WordPress
Targeted Products: WordPress CMS (outdated core versions and vulnerable plugins)
Campaign: StopAndProtect
Malware: SilentDataCollector, NetworkShareScanner, SilentEncryptor
Attack: StopAndProtect is a large-scale cybercrime operation that hijacks nearly 2,000 poorly maintained WordPress sites and turns them into distributed criminal infrastructure for malware delivery, command-and-control, and stolen-data storage. Compromised sites serve fake ClickFix CAPTCHA prompts that trick visitors into running a PowerShell command, kicking off a multi-stage .NET download chain that deploys a modular toolkit, a file-encrypting ransomware, an SMB/USB worm, a VBS spreader, a lock-screen module, a victim-to-operator chat tool, and a credential and data stealer. Rather than always deploying ransomware, the operators most often quietly steal file listings and specific documents. As of late July 2026, the campaign had compromised more than 6,000 unique IP addresses worldwide.

Attack Regions



Attack Details

#1

StopAndProtect is a global cybercrime operation that turns thousands of hacked WordPress websites into working attacker infrastructure for spreading malware, controlling infected machines, and storing stolen documents, screenshots, and activity logs. It preys on outdated WordPress sites running years-old cores and vulnerable plugins. Attackers install a custom plugin via a ZIP-packaged PHP file, uploader-installer.php, which drops a must-use (MU) plugin into the wp-content/mu-plugins directory, letting anyone with valid credentials upload arbitrary files, including PHP, almost anywhere under the web root and enabling remote code execution. The plugin then self-deletes to avoid detection, and the compromised site serves visitors a fake ClickFix-style CAPTCHA that tricks them into running a PowerShell command to start the infection.

#2

That PowerShell command launches a staged .NET chain: a stage-1 downloader reports victim statistics to the command-and-control (C2) server, and a stage-2 loader adds sandbox checks before launching the payloads. Stage 3 unpacks six components: SilentEncryptor (file encryption), NetworkShareScanner (an SMB/USB worm), a VBS spreader, LockScreen (blocks user input and shows a ransom message with a payment QR code), SimpleChatProxy (a victim-to-operator chat tool), and SilentDataCollector (the stealer). Ransomware is not always deployed; in most cases, the operators quietly harvest file lists and then specific documents.

#3

Several components are built to spread. NetworkShareScanner behaves like an SMB/USB worm, while the VBS spreader propagates to hard disks and removable media, scans the network, and moves laterally via Windows Management Instrumentation (WMI). Newer stealer builds can also map and unmap network shares, extending reach across connected systems.

#4

SilentDataCollector enumerates all drives, encrypts the resulting list, and sends it to the C2, after which operators can upload a command file directing it to grab specific files. Newer versions add a keylogger with valid-email detection, WhatsApp data theft, and screenshots taken every 30 seconds. Stolen data is uploaded back to the hacked WordPress sites, more than 700 archives between mid-May and the end of July 2026, and operator security failures exposed those logs, screenshots, and even the attackers' own management tool, fMain.frm, after they apparently infected themselves.

Recommendations

- **Update WordPress Core and Plugins:** Keep WordPress and all installed plugins and themes on their latest supported versions. The campaign specifically preys on sites running years-out-of-date software and known plugin vulnerabilities.
- **Distrust Unexpected CAPTCHA Prompts:** Treat any CAPTCHA or verification page that instructs users to copy, paste, or run commands outside the browser as malicious, and leave the site immediately. This is the ClickFix lure used to trigger infection.
- **Restrict PowerShell Execution:** Constrain PowerShell using Constrained Language Mode, execution policies, and comprehensive logging (script block and module logging) so that pasted commands can be detected and blocked.
- **Audit WordPress for Rogue Plugins and Files:** Review the wp-content/mu-plugins directory and the web root for unauthorized PHP files (such as uploader-installer.php and activator.php), unexpected must-use plugins, and self-deleting "verify" plugins.
- **Harden WordPress Credentials and Access:** Enforce strong, unique administrator passwords and multi-factor authentication, rotate any credentials suspected of exposure, and limit file-upload permissions under the web root.
- **Deploy ClickFix and PowerShell Detections:** Add endpoint detection rules for ClickFix behavior, including clipboard-driven PowerShell launches, staged .NET downloaders, and suspicious child processes spawned from browsers.
- **Maintain Offline, Tested Backups:** Keep segregated, regularly tested backups so that the file-encrypting and lock-screen components cannot force payment.

Potential MITRE ATT&CK TTPs

Tactic	Technique	Sub-technique
Resource Development	T1584: Compromise Infrastructure	T1584.004: Server
Initial Access	T1190: Exploit Public-Facing Application	
	T1189: Drive-by Compromise	
Execution	T1204: User Execution	T1204.004: Malicious Copy and Paste
	T1059: Command and Scripting Interpreter	T1059.001: PowerShell
	T1047: Windows Management Instrumentation	
Persistence	T1505: Server Software Component	T1505.003: Web Shell
Defense Evasion	T1497: Virtualization/Sandbox Evasion	
	T1070: Indicator Removal	T1070.004: File Deletion
Discovery	T1083: File and Directory Discovery	
	T1135: Network Share Discovery	
	T1046: Network Service Discovery	
Lateral Movement	T1021: Remote Services	T1021.002: SMB/Windows Admin Shares
	T1091: Replication Through Removable Media	

Tactic	Technique	Sub-technique
Collection	T1056: Input Capture	T1056.001: Keylogging
	T1113: Screen Capture	
	T1005: Data from Local System	
	T1560: Archive Collected Data	
Command and Control	T1071: Application Layer Protocol	T1071.001: Web Protocols
Exfiltration	T1041: Exfiltration Over C2 Channel	
Impact	T1486: Data Encrypted for Impact	

Indicators of Compromise (IOCs)

TYPE	VALUE
Domains	maximumrock[.]ro, platinumcar[.]ca, norakremer[.]co[.]uk, pharmart[.]ae, ksr-racingparts[.]com, v-k[.]com[.]ua, www[.]lapellelaser[.]pl, www[.]parsrulman[.]com, mectcalcutta[.]com, discherniation[.]com

TYPE	VALUE
SHA256	cab7f141fd6f2c58055b3731ef6a64b8a2d4d88a974770b047da19c0904322f0, cc8aa2bd7bf74ca0bbc5cb03a7b18eae73094b450d11654528c05685fe12e0c9, 99bcb531d6dd3c93d3f28f03d6e4659c865a4ffbd2fb514e809017f3446a940b, 8337bf29100a5871b1275227006dc2a43b21b751e5ce7e2032364fd78af59ac5, 4dee2fe98d4da75ffb259c03b50202212dafc85691429a28641a8068eddea504, 9765b1342cc7eb982a73bb1f94c6c500b63dc817073b76ea926c1097078d3527, 7d3604d0728b242c72bd144b8661ebf63c1042a4f5dd441bc8c8507c701df20c, 976cfa57e1efacbe517b7e3441e9473d275ec1d9ad8ab69ddf8ae3a966aaa153, b79b9b027f76579555069a7506d946648a8cb3126c0dda837dc9fee0e5c79489, 65550f6d0ffec8421f703cdc7273d9c0563b3d480fe6702bad294a18afe72143, 0080d0dd72eda4850a02e51c0e5c6f768423dfe970cafae2ab52ceee75972b40, 8d1e23630a6695fa9c793d73832f59436c98bba30ed81c16d01b549bd17feab4, 10babb15e08f9fbd72cce11713a273b971c910dd5bdb989a3f6ff4d9c8e372c0, f042240c3de00c46dee625916bf246b7e87481e4081a6a97208b091409766e41, 11a635d70444605ede1de0aa227a9fd7cfa4554e75bea93ce18b639ca571a42e, 2adbb2c206be7f23bf77f8f50d1ac0f809511c0b4591421931f81a6eaa42c68c, 38602b76f6c65644b01fa4d81708251c159a883253cda8876396dc7212324ab9, 23cbabfe3ca3a7f1eb365f772d6a4ed8095cb8f7755622cc82e804478259dc70, b3dff910b350ace27d64cbd79405cb154a1967e366d7b88170c3e8303b1d08ad, 3ed8f2cc8da4853fd770ff38f0cbce6d9d4a84e75a828fc0cec3e3ec60db94f9, 3ba161ca7b8dcf389ec3236c9ddfb943e9d1766181b1b81a227649cad46132a8

References

https://research.checkpoint.com/2026/thousands-of-hacked-wordpress-sites-one-operation-unmasking-stopandprotect/

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

August 20, 2026 • 08:00 AM

More at www.hivepro.com