Hive Pro

Threat Level

Red

HiveForce Labs

THREAT ADVISORY

ATTACK REPORT

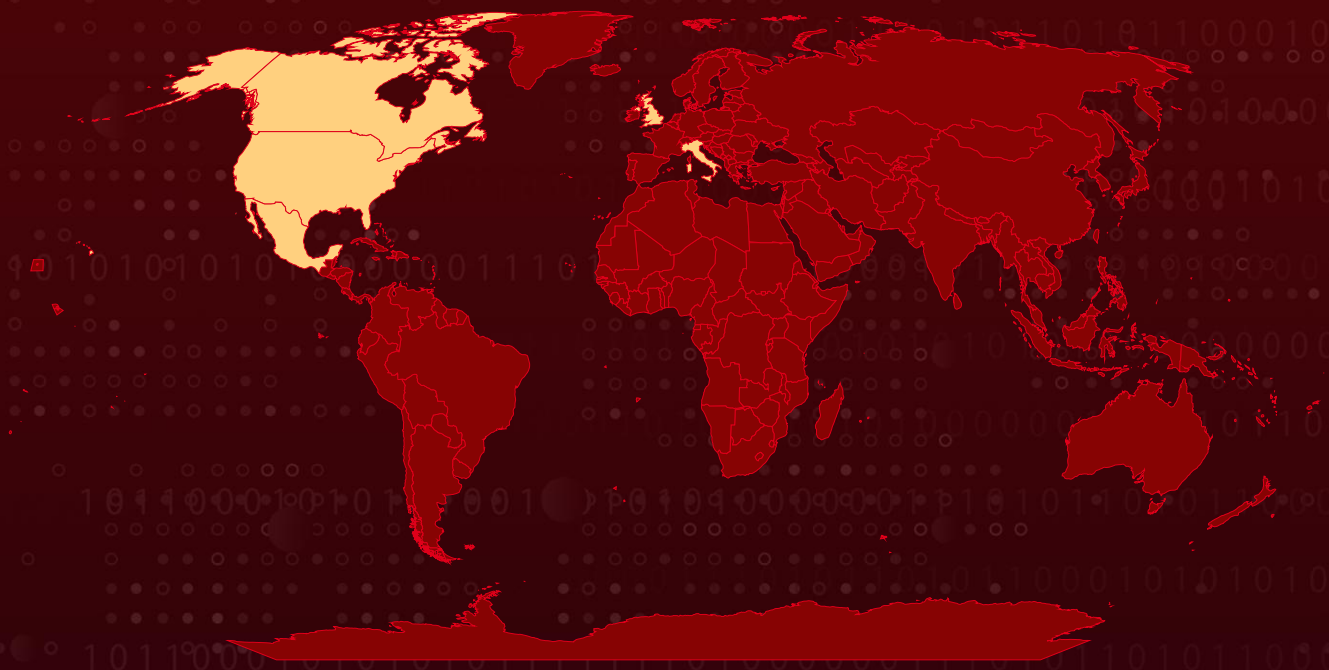
Interlock Ransomware Deploys New PHP RAT via FileFix Phishing

Date of Publication	Admiralty Code	TA Number
July 16, 2025	A1	TA2025221

Summary

First Seen: May 2025
Targeted Countries: United States, Canada, United Kingdom, Mexico, Itay
Malware: Interlock ransomware, Interlock RAT
Targeted Platform: Windows
Targeted Industries: Aerospace, Defense, Business Services & Consulting, Charitable Organizations, Education, Financial Services, Food Service, Government, Healthcare, Legal, Manufacturing, Media, Real Estate, Retail, Technology
Attack: Interlock ransomware has introduced a new PHP-based RAT delivered via the FileFix attack method, tricking users into executing malicious PowerShell commands through fake CAPTCHA prompts. This campaign uses compromised legitimate websites and Cloudflare Tunnel for stealthy C2 communication. The RAT conducts deep system reconnaissance and enables hands-on intrusion activities. It marks a significant escalation in Interlock's tactics, combining advanced social engineering with persistent malware operations.

Attack Regions



Attack Details

#1 The Interlock ransomware group has recently advanced its operations by deploying a new PHP-based Remote Access Trojan (RAT). This latest variant marks a shift from their previous Node.js-based NodeSnake RAT to a stealthier PHP-based implant. The delivery mechanism is built around a refined social engineering method called “FileFix,” which tricks users into executing malicious PowerShell commands by pasting them into the Windows address bar, under the guise of completing security verifications like CAPTCHA tests.

#2 The FileFix method leverages compromised legitimate websites, often through redirect campaigns facilitated by KongTuke (aka LandUpdate808) traffic distribution systems. Once a user is enticed into executing the command, a PowerShell script downloads and installs the RAT into the user's AppData folder, where it operates covertly.

#3 Upon activation, the RAT immediately performs system reconnaissance, gathering details about the host machine, running processes, services, network configurations, and privilege levels. This information is exfiltrated to command-and-control (C2) servers, enabling attackers to map out the network environment efficiently.

#4 One of the standout features of this campaign is the use of Cloudflare Tunnel subdomains for resilient and evasive communications with the C2 infrastructure. Additionally, fallback hardcoded IP addresses are included to ensure persistence even if primary channels are disrupted.

#5 The PHP RAT supports a wide range of attacker operations, from executing shell commands and deploying further payloads to creating persistence through registry modifications and facilitating lateral movement within compromised networks. Targeted industries and countries referenced in this advisory are specifically linked to Interlock ransomware incidents, not to isolated RAT deployments. With this latest evolution, Interlock demonstrates its adaptability and commitment to maintaining a dominant presence in the ransomware landscape.

Recommendations

Restrict access and patch systems: Grant administrative privileges sparingly and keep all security software up to date. Regularly scan for vulnerabilities and ensure endpoint protection can identify or block unknown malware.

Endpoint and Server Hardening: Deploy advanced endpoint detection and response (EDR) or extended detection and response (XDR) tools that can identify and block suspicious behaviors, including command-line flags such as /WIPEMODE and /elevated. Implement application control mechanisms like AppLocker to prevent execution of unauthorized binaries. Monitor for anomalies such as sudden file size reduction or mass file extensions being changed to .interlock.

Network Segmentation and Traffic Control: Segment the internal network to limit lateral movement between endpoints, especially for privileged and critical systems. Apply strict firewall rules and network policies to restrict outbound traffic, particularly to known malicious domains, Tor exit nodes, and suspected command-and-control (C2) infrastructure.

Conduct Regular Data Backups and Test Restoration: Regularly backup critical data and systems, store them securely offline. Test restoration processes to ensure backup integrity and availability. In case of an Interlock ransomware attack, up-to-date backups enable recovery without paying the ransom.

Potential MITRE ATT&CK TTPs

TA0043 Reconnaissance	TA0040 Impact	TA0001 Initial Access	TA0002 Execution
TA0007 Discovery	TA0008 Lateral Movement	TA0009 Collection	TA0011 Command and Control
TA0003 Persistence	TA0004 Privilege Escalation	TA0005 Defense Evasion	TA0006 Credential Access

TA0010 Exfiltration	T1567 Exfiltration Over Web Service	T1486 Data Encrypted for Impact	T1071.001 Web Protocols
T1566.002 Spearphishing Link	T1566 Phishing	T1189 Drive-by Compromise	T1059.001 PowerShell
T1566.001 Spearphishing Attachment	T1059.003 Windows Command Shell	T1059 Command and Scripting Interpreter	T1071 Application Layer Protocol
T1547.001 Registry Run Keys / Startup Folder	T1547 Boot or Logon Autostart Execution	T1027 Obfuscated Files or Information	T1055 Process Injection
T1204 User Execution	T1204.001 Malicious Link	T1082 System Information Discovery	T1083 File and Directory Discovery
T1562 Impair Defenses	T1555 Credentials from Password Stores	T1584 Compromise Infrastructure	T1021 Remote Services
T1021.001 Remote Desktop Protocol	T1219 Remote Access Software	T1005 Data from Local System	

Indicators of Compromise (IOCs)

TYPE	VALUE
SHA256	28a9982cf2b4fc53a1545b6ed0d0c1788ca9369a847750f5652ffa0ca7f7b7d3, 8afd6c0636c5d70ac0622396268786190a428635e9cf28ab23add939377727b0
IPv4	64[.]95[.]12[.]71, 184[.]95[.]51[.]165

TYPE	VALUE
Domains	existed-bunch-balance-councils[.]trycloudflare[.]com, ferrari-rolling-facilities-lounge[.]trycloudflare[.]com, galleries-physicians-psp-wv[.]trycloudflare[.]com, evidence-deleted-procedure-bringing[.]trycloudflare[.]com, nowhere-locked-manor-hs[.]trycloudflare[.]com, ranked-accordingly-ab-hired[.]trycloudflare[.]com

Recent Breaches

https://www.ybconline.com
https://www.wilsonvilletoyota.com
https://positivesolutions.school
https://www.lexrich5.org
https://shscullman.com
https://www.district6.org
https://www.cbasyracuse.org
https://eaglebuilders.ca
https://ketteringhealth.org
https://texasdigestive.com
https://rechlerequity.com
https://intech-ind.com
https://wcsmith.com
https://napergrove.com
https://semplecpa.com

References

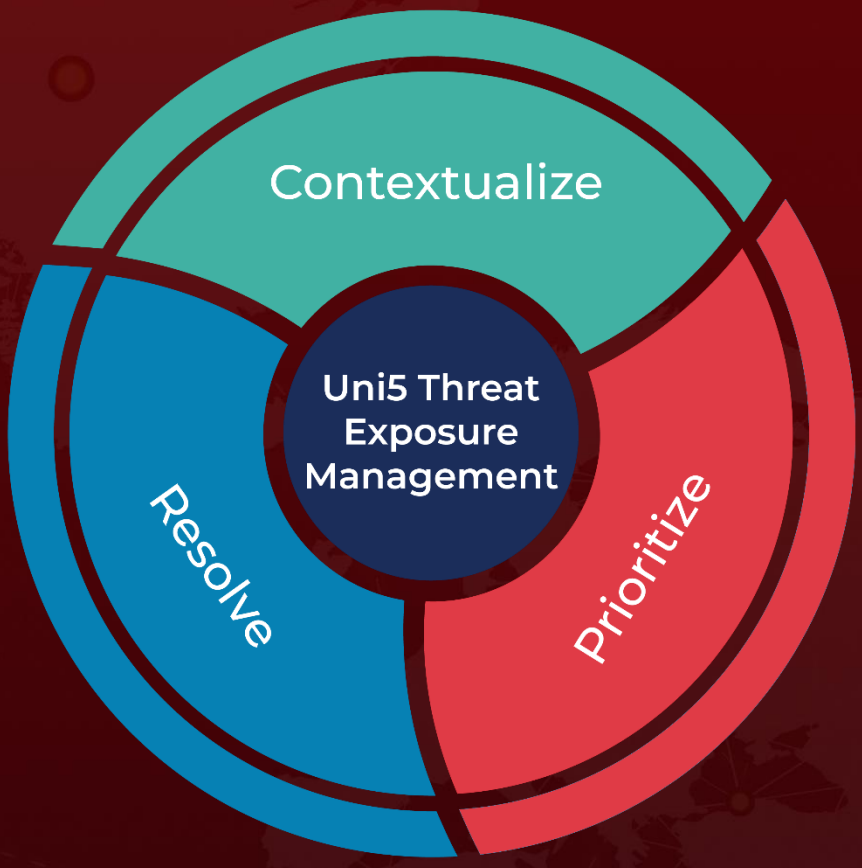
https://thedfirreport.com/2025/07/14/kongtuke-filefix-leads-to-new-interlock-rat-variant/

https://hivepro.com/threat-advisory/interlock-ransomware-blurs-line-between-cybercrime-and-espionage/

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

July 16, 2025 • 11:00 PM

More at www.hivepro.com