Hive Pro

Threat Level

Amber

HiveForce Labs

THREAT ADVISORY

ATTACK REPORT

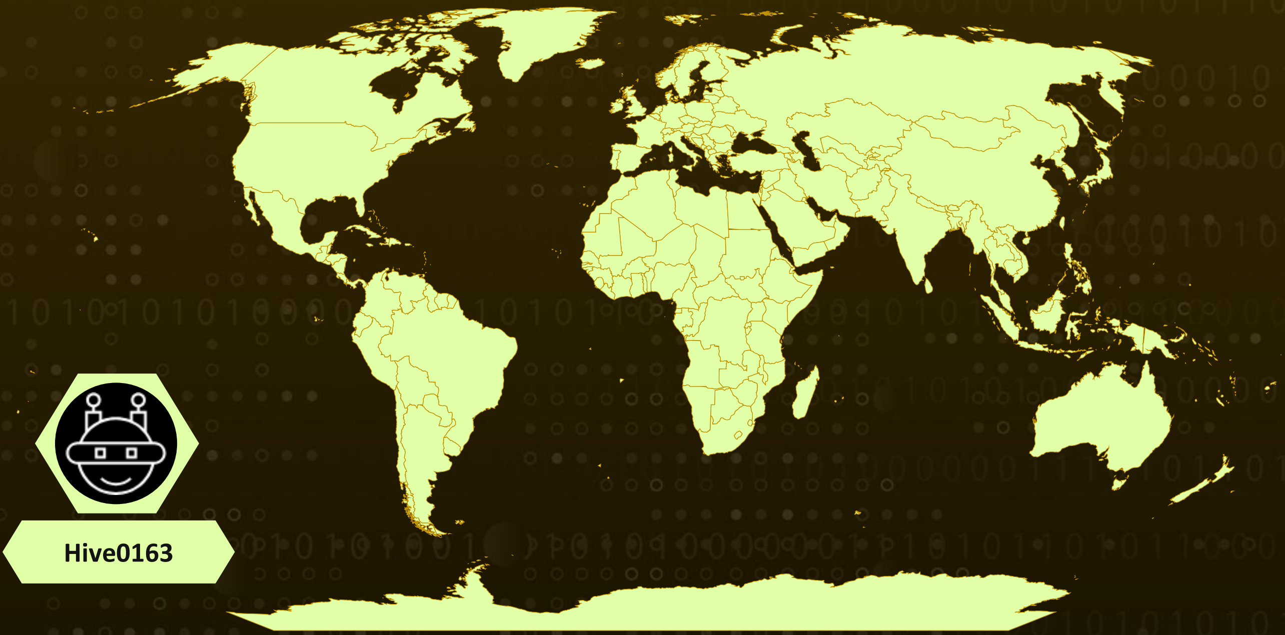
AI-Assisted Slopoly Backdoor Powers Interlock Ransomware Intrusion

Date of Publication	Admiralty Code	TA Number
March 13, 2026	A1	TA2026071

Summary

First Seen: Early 2026
Targeted Regions: Worldwide
Targeted Platforms: Windows, Linux
Targeted Industries: Corporate Enterprises
Threat Actor: Hive0163
Malware: Slopoly, NodeSnake, Interlock ransomware, InterlockRAT
Attack: A recent Interlock ransomware intrusion revealed the use of Slopoly, a suspected AI-assisted PowerShell backdoor that helped attackers maintain access to a compromised server for over a week. The attack began with a ClickFix social engineering trick that lured victims into executing a malicious script, allowing the threat actor Hive0163 to deploy a multi-stage malware chain including NodeSnake and InterlockRAT. Using this access, the attackers conducted reconnaissance and data staging before ultimately deploying Interlock ransomware to encrypt files and demand payment.

Attack Regions



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

🟩 Targeted 🟫 Non-Targeted

Attack Details

#1

A recently uncovered intrusion involving the Interlock ransomware group has revealed the use of a new backdoor called Slopoly, a malware strain that researchers believe may have been developed with the assistance of generative AI. During the incident, the attackers managed to maintain access to a compromised server for more than a week while quietly collecting data. The intrusion began with a ClickFix social engineering tactic, where victims are tricked into executing a malicious PowerShell command. In this case, the victim encountered a fake CAPTCHA-style verification page that secretly copied a malicious script to the clipboard and instructed them to open the Windows Run dialog (Win+R), paste the content, and execute it.

#2

This initial access technique is commonly associated with the threat actor Hive0163, which frequently combines ClickFix with malvertising campaigns and assistance from initial access brokers. Once the victim executed the command, the script deployed NodeSnake, a Node.js based malware that serves as the first stage of the attacker's command-and-control (C2) framework. NodeSnake communicates with its operators through HTTP POST requests and supports multiple capabilities, including downloading and executing payloads, running shell commands, establishing persistence, and updating itself when required.

#3

The attackers then delivered a secondary payload known as InterlockRAT, a JavaScript-based backdoor that significantly expands the attacker's control over the compromised system. InterlockRAT communicates with its operators through web sockets and can create SOCKS5 tunnels, spawn reverse shells, and deliver additional malware. Both NodeSnake and InterlockRAT rely on hardcoded Cloudflare Tunnel infrastructure to conceal their command-and-control servers. With this access established, the attackers deployed Slopoly, a PowerShell-based backdoor placed in the C:\ProgramData\Microsoft\Windows\Runtime directory and configured to run persistently via a scheduled task named "Runtime Broker."

#4

Slopoly acts as a lightweight yet functional backdoor that collects system details such as the public IP address, username, privilege level, and host name. This information is sent as JSON-formatted heartbeat messages to the attacker's C2 server every 30 seconds, while the malware polls for new commands roughly every 50 seconds. Any received commands are executed through cmd.exe, and the results are sent back to the server. The script also maintains a rotating log file named persistence.log. Researchers noted several characteristics suggesting the code may have been generated or assisted by a large language model, including extensive inline comments, structured logging, robust error handling, and unused functions such as a "Jitter" routine.

#5 Throughout the intrusion, Hive0163 also deployed common ransomware operator tools, such as AzCopy for data staging and exfiltration, and Advanced IP Scanner for internal network reconnaissance. The final stage of the attack involved deploying Interlock ransomware, delivered as a 64-bit Windows executable via the JunkFiction loader. The ransomware encrypts files using AES-GCM with RSA-protected keys through a statically linked OpenSSL library, appends extensions such as .!NT3RLOCK or .int3R1Ock to encrypted files, and drops a ransom note named FIRST_READ_ME.txt in affected directories. It also supports several command-line options that allow it to run with SYSTEM privileges, unlock files using the Windows Restart Manager API, and remove itself after execution using a DLL launched via rundll32.exe.

Recommendations

Implement ClickFix Countermeasures: Deploy security measures specifically targeting ClickFix social engineering attacks, such as disabling the "Win+R" keyboard shortcut via Group Policy, monitoring the RunMRU registry key for suspicious entries, and restricting PowerShell execution policies on endpoints to prevent unauthorized script execution.

Prioritize Behavior-Based Detection Over Signatures: Shift detection strategies to focus on behavioral analysis rather than relying solely on signature-based or malware-specific detection mechanisms, as AI-generated malware like Slopoly can be regenerated with different function names and configuration values, evading traditional signatures.

Monitor Scheduled Task Creation: Implement alerting on the creation of new scheduled tasks, particularly those named "Runtime Broker" or similar Windows process names, and any tasks that execute PowerShell scripts or cmd.exe from ProgramData directories.

Restrict PowerShell and Command-Line Execution: Enforce PowerShell Constrained Language Mode and implement application whitelisting to prevent unauthorized PowerShell scripts from executing. Monitor for PowerShell processes making outbound HTTP POST requests at regular intervals, which may indicate C2 beaconing activity.

Monitor for Data Exfiltration Tools: Deploy detection rules for the use of AzCopy and other cloud storage data transfer utilities within the environment, especially when executed outside of sanctioned IT operations, as these tools are commonly abused for large-scale data staging and exfiltration.

Segment Network and Limit Lateral Movement: Implement network segmentation to restrict lateral movement between critical systems. Deploy micro-segmentation for high-value servers to prevent ransomware propagation across network segments.

Implement Robust Backup and Recovery Strategy: Maintain offline, immutable backups that are regularly tested for restoration capability. Ensure backup systems are isolated from the production network to prevent ransomware from encrypting backup data.

Potential MITRE ATT&CK TTPs

Tactic	Technique	Sub-technique
Execution	T1204: User Execution	T1204.004: Malicious Copy and Paste
		T1204.002: Malicious File
	T1059: Command and Scripting Interpreter	T1059.001: PowerShell
		T1059.003: Windows Command Shell
		T1059.007: JavaScript
Persistence	T1053: Scheduled Task/Job	T1053.005: Scheduled Task
	T1574: Hijack Execution Flow	T1574.001: DLL
Discovery	T1016: System Network Configuration Discovery	
	T1082: System Information Discovery	
	T1046: Network Service Discovery	

Tactic	Technique	Sub-technique
Command and Control	T1071: Application Layer Protocol	T1071.001: Web Protocols
	T1572: Protocol Tunneling	
	T1090: Proxy	T1090.001: Internal Proxy
	T1102: Web Service	
Exfiltration	T1567: Exfiltration Over Web Service	
Impact	T1486: Data Encrypted for Impact	
	T1489: Service Stop	

Indicators of Compromise (IOCs)

TYPE	VALUE
SHA256	0884e5590bdf3763f8529453fbd24ee46a3a460bba4c2da5b0141f5ec6a35675
IPv4	94[.]156[.]181[.]89, 77[.]42[.]75[.]119, 23[.]227[.]203[.]123, 172[.]86[.]68[.]64
Domains	plurfestivalgalaxy[.]com, bridal-custody-private-bodies[.]trycloudflare[.]com, corner-teacher-guam-characterization[.]trycloudflare[.]com, yen-hansen-cartoon-aims[.]trycloudflare[.]com, cigarette-assumed-biotechnology-checklist[.]trycloudflare[.]com, meet-noted-tax-qualification[.]trycloudflare[.]com, liverpool-patterns-lanes-specified[.]trycloudflare[.]com, jane-practitioner-lightning-preservation[.]trycloudflare[.]com, misc-elliott-mouth-leading[.]trycloudflare[.]com, playback-attributes-interviews-processing[.]trycloudflare[.]com, postal-ssl-converted-quantity[.]trycloudflare[.]com, forget-canal-chancellor-mas[.]trycloudflare[.]com, chronic-dividend-amendments-das[.]trycloudflare[.]com, planners-mixing-edmonton-endless[.]trycloudflare[.]com,

TYPE	VALUE
Domains	baseline-include-priority-bar[.]trycloudflare[.]com, specials-storm-height-warriors[.]trycloudflare[.]com, safe-accepted-salem-early[.]trycloudflare[.]com, bits-promotions-turned-editions[.]trycloudflare[.]com, logan-practitioners-percent-cartridges[.]trycloudflare[.]com, eugene-examinations-contained-timber[.]trycloudflare[.]com, moore-cgi-pen-drove[.]trycloudflare[.]com, screenshots-executive-joins-hammer[.]trycloudflare[.]com, coffee-lloyd-families-excluded[.]trycloudflare[.]com, communist-flying-provision-calendar[.]trycloudflare[.]com, lamp-voters-biodiversity-phillips[.]trycloudflare[.]com, rpm-chicken-during-staying[.]trycloudflare[.]com, module-source-tree-diverse[.]trycloudflare[.]com, offers-listing-screenshot-alpha[.]trycloudflare[.]com, electrical-protect-molecular-underground[.]trycloudflare[.]com, silk-lift-porter-correctly[.]trycloudflare[.]com, wives-bufing-humans-prot[.]trycloudflare[.]com, describe-absent-operational-seventh[.]trycloudflare[.]com, edinburgh-packaging-sense-idol[.]trycloudflare[.]com, gzip-picked-istanbul-maple[.]trycloudflare[.]com

References

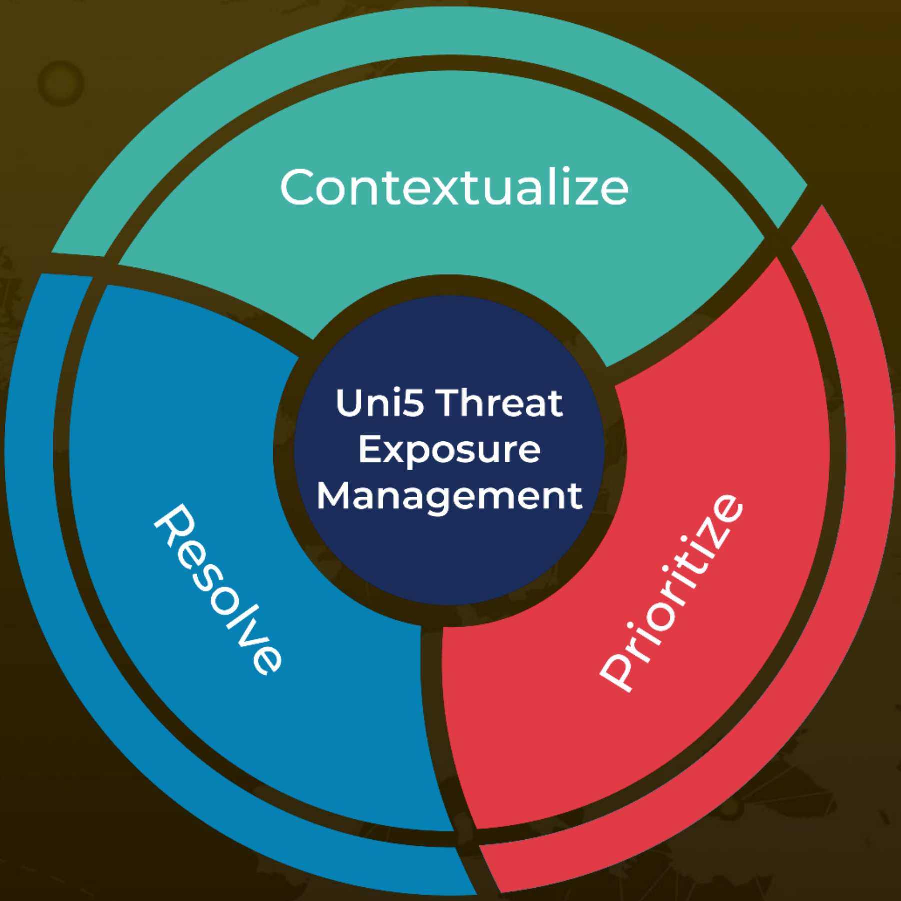
https://www.ibm.com/think/x-force/slopoly-start-ai-enhanced-ransomware-attacks

https://hivepro.com/threat-advisory/interlock-ransomware-deploys-new-php-rat-via-filefix-phishing/

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

March 13, 2026 • 8:10 AM

More at www.hivepro.com