INTELLIGENCE BRIEFING
Security Command Center
TLP:CLEAR
2026-03-29 18:33 UTC

Hive0163 Weaponizes AI-Generated Backdoor in Interlock Ransomware Campaign: Slopoly Signals Shifting Malware Development Norms

THREAT CAMPAIGN | **HIGH** | CVSS 7.5

SCC Item ID	SCC-CAM-2026-0081
Type	Threat Campaign
Severity	HIGH
CVSS Base Score	7.5
Affected Products	Windows (64-bit); Microsoft Windows Restart Manager API; organizations including Texas Tech University System, DaVita, Kettering Health, City of Saint Paul MN
Published	2026-03-22
Discovery Source	Rss

Executive Summary

IBM X-Force confirmed that threat group Hive0163 deployed an AI-generated PowerShell backdoor, Slopoly, during an Interlock ransomware intrusion that resulted in data exfiltration over more than one week before detection. The attack used ClickFix social engineering to gain initial access, layered multiple backdoors to maintain persistence, and deployed ransomware via the JunkFiction loader. Organizations in healthcare, education, and public sector are among confirmed victims, and this campaign establishes that LLM-assisted malware development is now an active operational tactic, not a theoretical concern.

Technical Analysis

Hive0163 conducted a multi-stage intrusion on Windows 64-bit systems using a documented attack chain: ClickFix social engineering (T1566) delivered initial access, followed by sequential backdoor staging with NodeSnake, InterlockRAT, and the AI-generated PowerShell backdoor Slopoly (T1059.001, T1547, T1027). Slopoly maintained persistence on a compromised server for over one week while data was exfiltrated via T1041. The JunkFiction loader delivered the Interlock ransomware payload (T1105, T1486). Lateral movement and masquerading techniques are associated with T1036.004 and T1078. Slopoly is assessed as technically shallow but functional; its significance is confirmed operational deployment in a live financially motivated campaign. Associated weaknesses: CWE-494 (Download of Code Without Integrity Check) and CWE-78 (OS Command Injection). No CVE is assigned to this campaign. C2 communication observed over T1071.001 (Application Layer Protocol: Web Protocols). Scheduled tasks (T1053.005) were used for persistence. No CISA

KEV entry exists for this campaign as of the configuration date. Source: IBM X-Force (primary T1 source); reported by BleepingComputer (T3 coverage).

Action Checklist

1. Step 1, Immediate: Block known Interlock ransomware and Hive0163 IOCs at perimeter and endpoint controls; consult IBM X-Force's full campaign report (if available to your organization) for current indicators before deploying blocks.
2. Step 2, Detection: Hunt for anomalous PowerShell execution (T1059.001) on Windows servers, specifically encoded or obfuscated scripts making outbound HTTP/HTTPS connections; review scheduled task creation events (Event ID 4698) for unauthorized entries (T1053.005, T1547).
3. Step 3, Assessment: Audit internet-facing Windows systems for evidence of ClickFix-style browser-based social engineering delivery; review access logs for use of valid accounts (T1078) outside normal patterns, particularly service and admin accounts.
4. Step 4, Communication: Notify SOC leadership and IR stakeholders if any indicators are found; organizations in healthcare, education, or public sector with externally accessible Windows infrastructure should treat this as elevated priority given confirmed victim profile.
5. Step 5, Long-term: Update detection rules to flag LLM-characteristic PowerShell patterns (verbose commenting, structured error handling in scripts from unknown origins); review and restrict PowerShell execution policy via AppLocker or WDAC; incorporate Interlock TTPs into tabletop exercises and purple team scenarios mapped to the MITRE ATT&CK techniques listed.

IR / Forensic Enrichment

Triage Priority	URGENT
Escalation Criteria	Escalate immediately to IR firm or law enforcement (FBI, CISA) if any confirmed Interlock ransomware payload is detected, ransomware encryption activity is observed, or if the victim organization is in healthcare/critical infrastructure; threat actor Hive0163 has demonstrated rapid-to-deployment timelines (7+ day dwell time before detection in this campaign).
Recovery Notes	Post-containment: (1) Do not bring affected systems back online until forensic imaging and analysis are complete and eradication is confirmed (rebuild from clean backups if available, date-verified as pre-intrusion). (2) Rotate all administrative credentials, service account passwords, and API keys; audit privileged account usage across all systems for the 30 days prior to initial compromise. (3) Conduct full network segmentation review: isolate internet-facing Windows systems from internal infrastructure using DMZ, network ACLs, and zero-trust architecture; disable legacy protocols (SMBv1, RDP over internet).

Forensic Artifacts	Windows Event Log Security channel (Event IDs 4688, 4698, 4624, 4625, 4648, 4720) | PowerShell Operational and Script Block Logs (Microsoft-Windows-PowerShell/Operational) | Sysmon logs (Event IDs 3 network connection, 11 file created, 12/13 registry modification) | Registry hives: HKLM\SYSTEM\CurrentControlSet\Services, HKCU\Software\Microsoft\Windows\CurrentVersion\Run*, HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System | IIS access logs (W3C format) from C:\inetpub\logs\LogFiles\; browser history/cache from C:\Users*/AppData/Local/; MFT (Master File Table) for file timestamps; memory dump (if ransomware payload detected); network packet capture (pcap) for outbound C2 communications

Per-Action IR Details

Step 1 — Immediate: Block known Interlock ransomware and Hive0163 IOCs at perimeter and endpoint controls; consult IBM X-Force's full campaign report for current indicators before deploying blocks.

NIST Phase: Preparation

Reference: NIST 800-61r3 §2.1 (Preparation phase: tools and resources)

Controls: NIST 800-53 SI-4 (Information System Monitoring), NIST 800-53 AC-3 (Access Enforcement), CIS 6.1 (Deny and dont-monitor access to application services)

Compensating: Without enterprise EDR/SIEM: (1) Extract IOC hashes from IBM X-Force report; (2) populate Windows Defender antimalware signatures via PowerShell: `Update-MpSignature -UpdateSource MER`; (3) manually add file hashes to Defender exclusion blocklist via Group Policy or Registry: `HKLM\SOFTWARE\Microsoft\Windows Defender\Exclusions\Paths`; (4) configure Windows Firewall outbound rules for known C2 domains using `netsh advfirewall firewall add rule name="Block Interlock C2" dir=out action=block remoteip=`.

Evidence: Before blocking: (1) capture network baseline for 24 hours using netsh: `netsh trace start capture=yes tracefile=C:\baseline.etl`; (2) export current Defender threat history via `Get-MpPreference | Select-Object -ExpandProperty ThreatTrackingPath`; (3) preserve current firewall rules: `netsh advfirewall firewall show rule name=all > firewall_baseline.txt`; (4) document existing scheduled tasks: `schtasks /query /v > scheduled_tasks_baseline.txt`.

Step 2 — Detection: Hunt for anomalous PowerShell execution (T1059.001) on Windows servers, specifically encoded or obfuscated scripts making outbound HTTP/HTTPS connections; review scheduled task creation events (Event ID 4698) for unauthorized entries (T1053.005, T1547).

NIST Phase: Detection Analysis

Reference: NIST 800-61r3 §3.2 (Detection and analysis); NIST 800-61r3 §3.2.4 (log archival and preservation)

Controls: NIST 800-53 AU-2 (Audit Events), NIST 800-53 AU-12 (Audit Generation), CIS 8.1 (Collect detailed audit logs for user logons), CIS 8.4 (Collect detailed audit logs for administrative activities)

Compensating: On systems without centralized logging: (1) Enable PowerShell Module Logging and Script Block Logging via Group Policy: `HKLM\SOFTWARE\Policies\Microsoft\Windows\PowerShell\ModuleLogging` and `ScriptBlockLogging` (set EnableModuleLogging=1, EnableScriptBlockLogging=1); (2) Export 7-day PowerShell Operational logs: `wevtutil qe Microsoft-Windows-PowerShell/Operational /f:text > ps_logs.txt`; (3) Query Event ID 4698 (scheduled task created) via `wevtutil qe Security /q:"*[System[(EventID=4698)]]" /f:text > task_creation.txt`; (4) Monitor Network Connections with Process: `Get-NetTCPConnection -State Established | Select-Object LocalAddress,LocalPort,RemoteAddress,RemotePort,@{Name="ProcessName";Expression={(Get-Process -Id $_.OwningProcess).Name}} | Export-Csv active_connections.csv`.

Evidence: Capture: (1) Windows Event Log Security channel (Event IDs 4688 process creation, 4698 scheduled task, 4720 user account creation); (2) PowerShell Operational and Analytic logs (Microsoft-Windows-PowerShell/Operational); (3) Sysmon logs if available (Event ID 3 network connection, Event ID 11 file created); (4) network traffic pcap for outbound HTTPS: `netsh trace start capture=yes tracefile=C:\network.etl maxsize=500`; (5) Registry hives: `HKLM\SYSTEM\CurrentControlSet\Services\` and `HKCU\Software\Microsoft\Windows\CurrentVersion\RunOnce`.

Step 3 — Assessment: Audit internet-facing Windows systems for evidence of ClickFix-style browser-based social engineering delivery; review access logs for use of valid accounts (T1078) outside normal patterns, particularly service and admin accounts.

NIST Phase: Detection Analysis

Reference: NIST 800-61r3 §3.2.3 (Correlation); NIST 800-61r3 §3.3.2 (Target analysis)

Controls: NIST 800-53 AC-2 (Account Management), NIST 800-53 AU-6 (Audit Review, Analysis, and Reporting), CIS 5.3 (Disable administrative accounts), CIS 8.5 (Collect information about logon/logoff events)

Compensating: Without SIEM: (1) Export browser download history from all user profiles: search `C:\Users\*/AppData\Local/*/Download History` and `C:\Users\*/AppData/Local/Google/Chrome/Default/History`; (2) query RDP logon events (Event ID 4624, 4625, 4648) via `wevtutil qe Security /q:"*[System[(EventID=4624 or EventID=4625 or EventID=4648)]]" /f:text > rdp_logons.txt`; (3) extract service account logon anomalies: `Get-EventLog Security -InstanceId 4624 | Where-Object {$_.Message -match 'SYSTEM|Administrator|service'} | Export-Csv service_logons.csv`; (4) review IIS logs (if present): `%SYSTEMROOT%\System32\LogFiles\HTTP*` for suspicious User-Agent strings and .exe downloads.

Evidence: Collect: (1) IIS access logs (W3C format) from `C:\inetpub\logs\LogFiles\`; (2) Windows Event Log Security channel (Event IDs 4624 logon, 4625 failed logon, 4648 logon using explicit credentials); (3) Browser history and cache from `C:\Users\*/AppData/Local/` for all profiles; (4) DNS query logs if available via `ipconfig /displaydns > dns_cache.txt`; (5) temporary internet files and download history; (6) file modification times on web-facing directories via `Get-ChildItem -Path C:\inetpub -Recurse | Select-Object FullName,LastWriteTime`.

Step 4 — Communication: Notify SOC leadership and IR stakeholders if any indicators are found; organizations in healthcare, education, or public sector with externally accessible Windows infrastructure should treat this as elevated priority given confirmed victim profile.

NIST Phase: Containment

Reference: NIST 800-61r3 §3.4 (Containment, eradication, and recovery); NIST 800-61r3 §2.2.3 (Communication plan)

Controls: NIST 800-53 IR-4 (Incident Handling), NIST 800-53 CP-2 (Contingency Planning), CIS 19.1 (Establish a process for incident response)

Compensating: If no formal IR program exists: (1) immediately create a written incident declaration with timestamp, discoverer name, and affected system scope; (2) notify executive stakeholder (CISO, CEO) and legal department via signed email with subject line "INCIDENT: [CVSS Level] — [Threat Name] Detected"; (3) isolate affected system from network immediately (disconnect Ethernet or disable NIC) if ransomware indicators are present; (4) document chain of custody: record who accessed affected systems and at what time; (5) if a third-party IR firm contract exists, invoke it before modifying any systems.

Evidence: Preserve before communication: (1) create a complete forensic image of affected system using dd or imaging tool: `dd if=/dev/sda of=forensic_image.dd status=progress`; (2) capture live memory if available: `psexec -s -d C:\temp\dumpit.exe` or use Volatility toolkit; (3) document network configuration: routing tables, ARP cache, active connections; (4) lock down the system to prevent further modification: change local admin passwords, disable remote access.

Step 5 — Long-term: Update detection rules to flag LLM-characteristic PowerShell patterns (verbose commenting, structured error handling in scripts from unknown origins); review and restrict PowerShell execution policy via AppLocker or WDAC; incorporate Interlock TTPs into tabletop exercises and purple team scenarios mapped to the MITRE ATT&CK techniques listed.

NIST Phase: Post Incident

Reference: NIST 800-61r3 §3.4.3 (Post-incident activities); NIST 800-61r3 §2.1.3 (Detection tools and rules)

Controls: NIST 800-53 SI-4 (Information System Monitoring), NIST 800-53 CA-7 (Continuous Monitoring), NIST 800-53 IR-6 (Incident Reporting), CIS 6.1 (Application Whitelisting/Blacklisting), CIS 17.4 (Implement Secure Development Practices)

Compensating: Without endpoint EDR: (1) Deploy AppLocker via Group Policy to block unsigned PowerShell scripts: `Set-AppLockerPolicy -XmlPolicy C:\AppLocker_policy.xml`; set execution policy to RemoteSigned or Restricted: `Set-ExecutionPolicy -ExecutionPolicy RemoteSigned -Scope LocalMachine`; (2) Create detection rule for obfuscated PowerShell indicators via scheduled task: search for keywords like `-enc`, `-nop`, `FromBase64String`, `IEX` in PowerShell logs; (3) Conduct tabletop using MITRE ATT&CK techniques T1059.001, T1053.005, T1547, T1078, and document response procedures in a playbook; (4) train administrators on ClickFix social engineering (fake support calls, fake Windows Update prompts).

Evidence: Document for future hunts: (1) preserved baseline PowerShell scripts from known-good sources for comparison; (2) snapshot of current AppLocker and execution policy settings; (3) exported detection rule signatures in YARA or Sigma format; (4) captured network IOCs (C2 domains, IP addresses, file hashes) for threat intel feeds.

Detection Guidance

Focus detection on the following behavioral patterns derived from confirmed campaign TTPs. PowerShell: alert on Base64-encoded PowerShell launching from browser child processes or Office applications; flag scripts executing Invoke-Expression or downloading remote content (CWE-494, T1105). Scheduled Tasks: query Windows Security Event Log for Event ID 4698 (scheduled task created) by non-standard accounts; cross-reference with Task Scheduler operational log. Outbound C2: monitor for sustained low-volume HTTP/HTTPS beaconing from server-class systems to newly registered or low-reputation domains (T1071.001). Data staging and exfiltration: alert on large file compression or transfer activity from servers not normally involved in data movement (T1041). Masquerading: review process names and paths for known Interlock masquerade patterns (T1036.004); compare running process hashes against baseline. ClickFix delivery: review browser proxy or DNS logs for access to domains associated with fake CAPTCHA or browser-update lure pages. Note: specific IOC values (hashes, IPs, domains) from IBM X-Force's report should be ingested directly from the primary source; the item data provided does not include confirmed hash or network IOC values.

Indicators of Compromise

Type	Value	Context	Confidence
MALWARE-FAMILY	`Slopoly`	AI-generated PowerShell backdoor used for persistence; deployed by Hive0163 in confirmed Interlock ransomware intrusion	HIGH
MALWARE-FAMILY	`NodeSnake`	Backdoor staged prior to Slopoly in the Hive0163 attack chain	HIGH
MALWARE-FAMILY	`InterlockRAT`	Remote access trojan staged as part of layered persistence in this campaign	HIGH
MALWARE-FAMILY	`JunkFiction`	Loader used to deliver Interlock ransomware payload in final stage of attack chain	HIGH

Type	Value	Context	Confidence
THREAT-ACTOR	`Hive0163`	IBM X-Force attributed threat group; operator of this Interlock ransomware campaign	HIGH
TECHNIQUE	`ClickFix social engineering`	Initial access vector; browser-based lure used to execute malicious PowerShell	HIGH

Framework Mappings

MITRE-ATTACK

- **T1071.001** — Web Protocols
- **T1486** — Data Encrypted for Impact
- **T1078** — Valid Accounts
- **T1036.004** — Masquerade Task or Service
- **T1547** — Boot or Logon Autostart Execution
- **T1041** — Exfiltration Over C2 Channel
- **T1059.001** — PowerShell
- **T1105** — Ingress Tool Transfer
- **T1566** — Phishing
- **T1053.005** — Scheduled Task
- **T1027** — Obfuscated Files or Information

NIST-800-53R5

- **CP-9** — System Backup
- **CP-10** — System Recovery and Reconstitution
- **AC-2** — Account Management
- **AC-6** — Least Privilege
- **IA-2** — Identification and Authentication (Organizational Users)
- **IA-5** — Authenticator Management
- **CM-7** — Least Functionality
- **SI-3** — Malicious Code Protection
- **SI-4** — System Monitoring
- **CA-7** — Continuous Monitoring
- **SC-7** — Boundary Protection
- **SI-7** — Software, Firmware, and Information Integrity
- **AT-2** — Literacy Training and Awareness
- **SI-8** — Spam Protection
- **SI-10** — Information Input Validation
- **CM-3** — Configuration Change Control

- **IR-4** — Incident Handling

OWASP-TOP10-2021

- **A03:2021** — Injection
- **A08:2021** — Software and Data Integrity Failures

CIS-V8

- **2.5**
- **16.10**
- **2.6**
- **14.2** — Train Workforce Members to Recognize Social Engineering Attacks

NIST-CSF-2

- **RS.MI-01** — Incidents are contained

HIPAA-SECURITY

- **164.308(a)(7)(ii)(A)** — Data Backup Plan

ISO-27001-2022

- **A.5.29** — Information security during disruption

MITRE ATT&CK Mapping

Technique ID	Technique Name	Tactic
T1071.001	Web Protocols	Command-And-Control
T1486	Data Encrypted for Impact	Impact
T1078	Valid Accounts	Defense-Evasion
T1036.004	Masquerade Task or Service	Defense-Evasion
T1547	Boot or Logon Autostart Execution	Persistence
T1041	Exfiltration Over C2 Channel	Exfiltration
T1059.001	PowerShell	Execution
T1105	Ingress Tool Transfer	Command-And-Control
T1566	Phishing	Initial-Access
T1053.005	Scheduled Task	Execution
T1027	Obfuscated Files or Information	Defense-Evasion

Sources

Source	URL	Tier
Security News	https://www.bleepingcomputer.com/news/security/ai-generated-slopoly...	T3
October 23, 2025—KB5070882 (OS Build 14393.8524) Out-of-band	https://support.microsoft.com/en-us/topic/october-23-2025-kb5070882...	T1
Satine Sentinel: March 13, 2026	https://satinetech.com/2026/03/13/satine-sentinel-march-13-2026/	T3
Microsoft Fixes 63 Security Flaws, Including a Windows Kernel Zero ...	https://thehackernews.com/2025/11/microsoft-fixes-63-security-flaws...	T3
Researchers Identify AI-Generated Slopoly Malware In Ransomware ...	https://the420.in/slopoly-ai-generated-malware-interlock-ransomware...	T3

Generated 2026-03-29 18:33 UTC by TJS Security Command Center