INTELLIGENCE BRIEFING
Security Command Center
TLP:CLEAR
2026-05-27 06:37 UTC

GPU-Targeted Cryptojacking Campaign Extends SEO Poisoning to AI Chatbots, Deploys Persistent ScreenConnect Backdoors

THREAT CAMPAIGN | **HIGH** | CVSS 7.5

SCC Item ID	SCC-CAM-2026-0369
Type	Threat Campaign
Severity	HIGH
CVSS Base Score	7.5
Affected Products	Windows endpoints (PC enthusiasts / hardware hobbyists); ScreenConnect (ConnectWise Control), used as persistent backdoor; Microsoft .NET LOLBins (InstallUtil.exe, RegAsm.exe, RegSvcs.exe, MSBuild.exe, AppLaunch.exe, AddInProcess.exe, aspnet_compiler.exe), used as process-hollowing targets; Impersonated legitimate utilities: CrystalDiskInfo, HWMonitor, Display Driver Uninstaller, FurMark, K-Lite Codec Pack, PDFgear; Dynu dynamic DNS infrastructure, used for C2
Published	2026-05-26T21:35:34+00:00
Discovery Source	Rss:T1 Threatintel

Executive Summary

An active cryptojacking campaign, documented by Microsoft Defender Experts on May 26, 2026, targets PC enthusiasts and hardware hobbyists by poisoning search engine results and manipulating AI chatbot responses to distribute trojanized versions of popular utilities such as CrystalDiskInfo, HWMonitor, FurMark, and PDFgear. Once installed, the malware silently deploys ScreenConnect (ConnectWise Control) for persistent remote access and injects a GPU cryptocurrency miner into legitimate Windows processes to evade detection. The ScreenConnect backdoor extends the risk far beyond resource theft, creating an established foothold for lateral movement, credential harvesting, data exfiltration, and ransomware staging across any endpoint where the software was executed.

Technical Analysis

This unattributed campaign, active since at least March 2026, chains multiple evasion techniques to achieve persistent access and GPU mining on Windows endpoints. Initial access occurs via SEO-poisoned search results and AI chatbot response manipulation (MITRE T1598, T1608.006) that redirect users to lookalike download sites impersonating legitimate utilities. Downloaded ZIP payloads (CWE-494) contain a DLL

sideloading chain (T1574.002, CWE-426) where a malicious autorun.dll is loaded by a legitimate utility binary. The loader installs ScreenConnect silently (T1219) and establishes persistence via three scheduled tasks (T1053.005), Registry Run keys (T1547.001), and a Startup folder LNK. A process-hollowing loader (T1055.012) injects a GPU miner into trusted Microsoft .NET LOLBins including InstallUtil.exe, RegAsm.exe, RegSvcs.exe, MSBuild.exe, AppLaunch.exe, AddInProcess.exe, and aspnet_compiler.exe. Windows Defender exclusions are abused (T1562.001, CWE-693) to suppress AV alerts on the install directory. C2 communication uses Dynu dynamic DNS infrastructure (T1568) over application-layer protocols (T1071). Masquerading techniques (T1036) include naming the install folder and tasks to resemble legitimate system components. No CVE is associated; no patch applies. Mitigation is behavioral. CVSS base score reported at 7.5 (High).

Action Checklist

1. Containment: Block ScreenConnect (ConnectWise Control) binaries on endpoints where it is not an authorized remote access tool; add Dynu dynamic DNS domains (*.dynu.com, *.dynu.net) and associated C2 infrastructure to DNS/proxy blocklists immediately. Reference Microsoft's May 26, 2026 advisory for specific IOC lists.
2. Detection: Hunt for process-hollowing activity: parent-child relationships where InstallUtil.exe, RegAsm.exe, RegSvcs.exe, MSBuild.exe, AppLaunch.exe, AddInProcess.exe, or aspnet_compiler.exe spawn unexpected child processes or exhibit unusual network connections. Query endpoint logs (NIST AU-6) for ScreenConnect installation events outside approved change windows. Check for scheduled tasks with names mimicking system components and Registry Run keys under HKCU\Software\Microsoft\Windows\CurrentVersion\Run referencing WinSysCache or similar. Audit Windows Defender exclusion lists for user-writable directories (T1562.001).
3. Eradication: Remove trojanized utility packages; terminate and uninstall unauthorized ScreenConnect instances; delete malicious scheduled tasks, Run keys, and Startup LNK entries; purge Windows Defender exclusions added by the malware; remove hidden/system-attributed install folders. Re-image endpoints where process hollowing into .NET LOLBins is confirmed.
4. Recovery: Validate that all three persistence mechanisms (scheduled tasks, Run keys, Startup LNK) are absent post-remediation; confirm Defender exclusion lists reflect only approved entries (CIS 4.6); monitor .NET LOLBin processes for anomalous GPU utilization and outbound connections to dynamic DNS infrastructure for a minimum of 30 days (NIST SI-4); rotate credentials for any accounts active on confirmed-compromised endpoints (D3-CRO).
5. Post-Incident: Address the control gaps this campaign exposed: enforce application allowlisting to block unapproved LOLBin abuse (NIST CM-7, CIS 2.3); implement software inventory controls to detect unauthorized installs (CIS 2.1); deploy endpoint controls that alert on Defender exclusion modifications (NIST SI-4); and establish user awareness training specifically covering AI chatbot referral risks and software download verification (NIST AT-2). Review remote access tool policy and enforce an approved-tools list (CIS 4.6, NIST AC-17).

IR / Forensic Enrichment

Triage Priority	IMMEDIATE

Escalation Criteria	Escalate to senior IR leadership and legal/compliance if ScreenConnect telemetry confirms the attacker exercised interactive remote access (indicated by ScreenConnect session logs showing keyboard/mouse input or file transfer events), if more than 10 endpoints are confirmed compromised suggesting a domain-wide exposure, or if any compromised endpoint is found to have processed payment card data, PII, or PHI — triggering breach notification assessment under applicable regulations.
Recovery Notes	After eradicating ScreenConnect and persistence mechanisms, restore affected endpoints only from verified clean images or known-good snapshots taken prior to the trojanized installer execution date; do not restore from backups made after the earliest confirmed infection timestamp. Monitor all remediated endpoints for 30 days using Sysmon Event ID 3 and GPU utilization counters specifically for the seven named LOLBin processes, as the malware's process-hollowing technique may survive incomplete memory-only cleanup if the host process was not terminated and re-imaged. Validate that Dynu DNS resolution fails from all endpoints and network egress points before declaring recovery complete, using 'Resolve-DnsName *.dynu.com' as a lightweight post-containment verification check.
Forensic Artifacts	Trojanized installer binaries (fake CrystalDiskInfo, HWMonitor, FurMark, PDFgear, Display Driver Uninstaller, K-Lite Codec Pack, PDFgear executables): SHA-256 hash each file and preserve originals in write-protected evidence storage — these are the initial access payload and the primary artifact linking victim to the SEO/AI-poisoning delivery chain. | Memory dumps of hollowed .NET LOLBin processes (InstallUtil.exe, RegAsm.exe, MSBuild.exe, AppLaunch.exe, AddInProcess.exe, aspnet_compiler.exe, RegSvcs.exe) captured via ProcDump at time of detection: these contain the injected GPU miner shellcode or PE image in unpacked form, enabling YARA rule development and miner wallet address extraction for blockchain tracing. | ScreenConnect client configuration and session logs (typically in %ProgramData%\ScreenConnect Client \ including relay server hostname, access code, and if accessible, session history logs): the relay server hostname identifies the attacker-controlled ConnectWise infrastructure and is the primary network IOC for enterprise-wide threat hunting. | Windows Registry export of HKCU\Software\Microsoft\Windows\CurrentVersion\Run and malicious scheduled task XML exports: these document the three persistence mechanisms (Run keys, scheduled tasks, Startup LNK) specific to this campaign, including the exact file paths used for WinSysCache-named entries that distinguish this campaign's artifacts from legitimate software. | DNS query logs (Sysmon Event ID 22 or DNS debug log) showing resolution of *.dynu.com and *.dynu.net domains with resolved IP addresses and timestamps: these establish the C2 communication timeline and provide network-layer IOCs for upstream firewall and ISP-level blocking, and may reveal additional dynamic DNS subdomains beyond those listed in the Microsoft advisory.

Per-Action IR Details

Containment — Block ScreenConnect (ConnectWise Control) binaries on endpoints where it is not an authorized remote access tool; add Dynu dynamic DNS domains (*.dynu.com, *.dynu.net) and associated C2 infrastructure to DNS/proxy blocklists immediately. Reference Microsoft's May 26, 2026 advisory for specific IOC lists.

NIST Phase: Containment

Reference: NIST 800-61r3 §3.3 — Containment Strategy

Controls: NIST IR-4 (Incident Handling), NIST SC-7 (Boundary Protection), NIST AC-3 (Access Enforcement), CIS 4.4 (Implement and Manage a Firewall on Servers), CIS 4.5 (Implement and Manage a Firewall on End-User Devices)

Compensating: On endpoints without EDR, use Windows Firewall with Advanced Security (wf.msc) to block outbound connections from ScreenConnect binaries: 'New-NetFirewallRule -DisplayName "Block ScreenConnect" -Direction Outbound -Program "%ProgramFiles(x86)%\ScreenConnect Client*\ScreenConnect.ClientService.exe" -Action Block'.

For Dynu DNS blocking without a corporate DNS gateway, push a hosts file entry via GPO or a local PowerShell script appending '0.0.0.0 *.dynu.com' and '0.0.0.0 *.dynu.net' to C:\Windows\System32\drivers\etc\hosts. Verify block effectiveness with Wireshark filtering on 'dns.qry.name contains dynu'.

Evidence: Before blocking, capture: (1) active ScreenConnect client process list via 'Get-Process | Where-Object {$_.Name -like "*ScreenConnect*"}' and note PIDs, parent PIDs, and full executable paths; (2) netstat -ano output showing established connections to Dynu-resolved IPs to document C2 channel state; (3) DNS cache snapshot via 'Get-DnsClientCache | Where-Object {$_.Entry -like "*dynu*"}' to preserve resolved C2 IP addresses before cache flush; (4) ScreenConnect installation directory contents (typically %ProgramData%\ScreenConnect Client* or %APPDATA%\ScreenConnect*) including configuration files that contain the attacker-controlled relay server address.

Detection — Hunt for process-hollowing activity: parent-child relationships where InstallUtil.exe, RegAsm.exe, RegSvcs.exe, MSBuild.exe, AppLaunch.exe, AddInProcess.exe, or aspnet_compiler.exe spawn unexpected child processes or exhibit unusual network connections. Query endpoint logs (NIST AU-6) for ScreenConnect installation events outside approved change windows. Check for scheduled tasks with names mimicking system components and Registry Run keys under HKCU\Software\Microsoft\Windows\CurrentVersion\Run referencing WinSysCache or similar. Audit Windows Defender exclusion listings for user-writable directories (T1562.001).

NIST Phase: Detection Analysis

Reference: NIST 800-61r3 §3.2 — Detection and Analysis

Controls: NIST AU-6 (Audit Record Review, Analysis, and Reporting), NIST AU-12 (Audit Record Generation), NIST SI-4 (System Monitoring), CIS 8.2 (Collect Audit Logs)

Compensating: Deploy Sysmon with SwiftOnSecurity config to capture Event ID 1 (Process Create) and Event ID 3 (Network Connection). Hunt LOLBin parent-child abuse with this PowerShell query against Sysmon operational log: 'Get-WinEvent -LogName "Microsoft-Windows-Sysmon/Operational" | Where-Object {$_.Message -match "InstallUtil|RegAsm|RegSvcs|MSBuild|AppLaunch|AddInProcess|aspnet_compiler"} | Select-Object TimeCreated, Message | Format-List'. For scheduled task enumeration: 'Get-ScheduledTask | Where-Object {$_.TaskPath -notlike "\Microsoft*"} | Select TaskName, TaskPath, @{N="Actions";E={$_.Actions.Execute}}'. For Defender exclusion audit: 'Get-MpPreference | Select-Object ExclusionPath, ExclusionProcess'. Apply the Sigma rule 'proc_creation_win_lolbin_installutil' from SigmaHQ as a manual grep pattern against Windows Security Event Log Event ID 4688 (Process Creation) exports.

Evidence: Collect before analysis concludes: (1) Sysmon Event ID 1 logs showing InstallUtil.exe, RegAsm.exe, MSBuild.exe, or AppLaunch.exe with ParentImage paths pointing to the trojanized utility installer (e.g., CrystalDiskInfo_setup.exe or HWMonitor_setup.exe) — this chain directly evidences the process-hollowing injection sequence; (2) Windows Security Event Log Event ID 4688 records for the seven named LOLBins filtered to the 24-hour window following trojanized installer execution; (3) full contents of HKCU\Software\Microsoft\Windows\CurrentVersion\Run and HKLM\Software\Microsoft\Windows\CurrentVersion\Run exported via 'reg export' before any remediation; (4) 'schtasks /query /fo LIST /v' full output saved to file, specifically looking for tasks with actions pointing into %APPDATA% or %TEMP% directories; (5) Windows Defender exclusion list exported via 'Get-MpPreference | ConvertTo-Json' to document which user-writable directories were whitelisted by the malware to evade on-access scanning.

Eradication — Remove trojanized utility packages; terminate and uninstall unauthorized ScreenConnect instances; delete malicious scheduled tasks, Run keys, and Startup LNK entries; purge Windows Defender exclusions added by the malware; remove hidden/system-attributed install folders. Re-image endpoints where process hollowing into .NET LOLBins is confirmed.

NIST Phase: Eradication

Reference: NIST 800-61r3 §3.4 — Eradication

Controls: NIST IR-4 (Incident Handling), NIST SI-2 (Flaw Remediation), NIST CM-7 (Least Functionality), CIS 2.3 (Address Unauthorized Software), CIS 7.2 (Establish and Maintain a Remediation Process)

Compensating: For ScreenConnect removal without an MDM/RMM tool: 'Get-WmiObject -Class Win32_Product | Where-Object {$_.Name -like "*ScreenConnect*"} | ForEach-Object {$_.Uninstall()}'. Remove malicious scheduled

tasks: 'Get-ScheduledTask | Where-Object {$_.Actions.Execute -match "AppData|Temp|WinSysCache"} | Unregister-ScheduledTask -Confirm:$false'. Remove Run key entries: 'Remove-ItemProperty -Path "HKCU:\Software\Microsoft\Windows\CurrentVersion\Run" -Name "WinSysCache"' (replace name with discovered variant). Purge Defender exclusions: 'Remove-MpPreference -ExclusionPath ""' for each malware-added entry. For hidden/system-attributed folders use 'attrib -s -h ' then 'Remove-Item -Recurse -Force'. Trigger a full Defender scan post-cleanup: 'Start-MpScan -ScanType FullScan'. Re-image any endpoint where Sysmon Event ID 8 (CreateRemoteThread) or memory injection into a LOLBin is confirmed — do not attempt in-place cleanup of confirmed hollow-injected processes.

Evidence: Before executing eradication: (1) acquire a full memory image of any process confirmed or suspected as a hollowing target (InstallUtil.exe, MSBuild.exe, etc.) using ProcDump ('procdump -ma output.dmp') to preserve the injected GPU miner payload for YARA signature development and threat intel sharing; (2) copy the trojanized installer binary (e.g., the fake CrystalDiskInfo or FurMark executable) to an isolated evidence share before deletion — compute SHA-256 hash and submit to VirusTotal for community correlation; (3) export full registry hive (HKCU and HKLM) via 'reg save HKCU hkcu_evidence.hiv' before removing Run keys; (4) copy the malicious scheduled task XML export ('schtasks /query /xml /tn "" > task_evidence.xml') for each identified malicious task; (5) export the ScreenConnect client configuration file (typically ScreenConnect.ClientService.exe.config or relay.json in the install directory) which contains the attacker's relay server hostname — critical for IOC extraction and blocking.

Recovery — Validate that all three persistence mechanisms (scheduled tasks, Run keys, Startup LNK) are absent post-remediation; confirm Defender exclusion lists reflect only approved entries (CIS 4.6); monitor .NET LOLBin processes for anomalous GPU utilization and outbound connections to dynamic DNS infrastructure for a minimum of 30 days (NIST SI-4); rotate credentials for any accounts active on confirmed-compromised endpoints (D3-CRO).

NIST Phase: Recovery

Reference: NIST 800-61r3 §3.5 — Recovery

Controls: NIST SI-4 (System Monitoring), NIST AC-2 (Account Management), NIST CP-10 (System Recovery and Reconstitution), CIS 4.6 (Securely Manage Enterprise Assets and Software), CIS 5.3 (Disable Dormant Accounts)

Compensating: Validate persistence removal with a post-remediation checklist script: (1) scheduled tasks: 'Get-ScheduledTask | Where-Object {$_.Actions.Execute -match "AppData|Temp|Roaming"}'; (2) Run keys: 'Get-ItemProperty HKCU:\Software\Microsoft\Windows\CurrentVersion\Run' and 'Get-ItemProperty HKLM:\Software\Microsoft\Windows\CurrentVersion\Run'; (3) Startup LNK: 'Get-ChildItem "$env:APPDATA\Microsoft\Windows\Start Menu\Programs\Startup"'. For GPU utilization monitoring without EDR, schedule a recurring task running 'nvidia-smi --query-compute-apps=pid,process_name,used_memory --format=csv' or 'Get-Counter "\GPU Engine(*)\Utilization 3D"' every 15 minutes and log to a CSV — alert on LOLBin processes (InstallUtil.exe, MSBuild.exe) appearing in GPU compute process lists. For dynamic DNS monitoring, run a daily PowerShell job checking Sysmon Event ID 22 (DNS Query) for any *.dynu.com or *.dynu.net resolution. Credential rotation without a PAM tool: force password reset via 'Set-ADAccountPassword' for all domain accounts whose last interactive logon (Event ID 4624) occurred on confirmed-compromised endpoints.

Evidence: During the 30-day monitoring window, preserve: (1) weekly GPU utilization logs from nvidia-smi or WMI counter exports for any endpoint that hosted the miner — baseline normal utilization to distinguish legitimate GPU workloads from resumed cryptomining; (2) Sysmon Event ID 3 (Network Connection) and Event ID 22 (DNS Query) logs for the seven LOLBin processes, capturing any outbound connections to dynamic DNS infrastructure that would indicate re-infection or a missed persistence mechanism; (3) Windows Security Event ID 4624/4625 (logon success/failure) and Event ID 4648 (explicit credential use) for rotated accounts for the full 30-day window to detect credential reuse from attacker-cached credentials.

Post-Incident — Address the control gaps this campaign exposed: enforce application allowlisting to block unapproved LOLBin abuse (NIST CM-7, CIS 2.3); implement software inventory controls to detect unauthorized installs (CIS 2.1); deploy endpoint controls that alert on Defender exclusion modifications (NIST SI-4); and establish user awareness training specifically covering AI chatbot referral risks and software download verification (NIST AT-2). Review remote access tool policy and enforce an approved-tools list (CIS

4.6, NIST AC-17).

NIST Phase: Post Incident

Reference: NIST 800-61r3 §4 — Post-Incident Activity

Controls: NIST CM-7 (Least Functionality), NIST AT-2 (Literacy Training and Awareness), NIST AC-17 (Remote Access), NIST SI-4 (System Monitoring), CIS 2.1 (Establish and Maintain a Software Inventory), CIS 2.3 (Address Unauthorized Software), CIS 4.6 (Securely Manage Enterprise Assets and Software), CIS 7.1 (Establish and Maintain a Vulnerability Management Process)

Compensating: Application allowlisting without enterprise tooling: configure Windows Defender Application Control (WDAC) policy in audit mode first using 'New-CIPolicy -Level Publisher -FilePath baseline.xml -UserPEs' then enforce after baselining — this natively restricts LOLBin abuse by publisher and path rules without additional cost. For software inventory, deploy osquery with the query 'SELECT name, version, install_date, install_location FROM programs' on a weekly scheduled task and diff output against an approved software list stored in a CSV. For Defender exclusion change alerting, create a Sysmon rule monitoring registry writes to 'HKLM\SOFTWARE\Microsoft\Windows Defender\Exclusions\Paths' (Sysmon Event ID 13, Registry Value Set) and forward to a log aggregator or email alert. For AI chatbot awareness training, create a one-page quick-reference card showing the legitimate download URLs for CrystalDiskInfo (crystalmark.info), HWMonitor (cpuid.com), FurMark (geeks3d.com), and PDFgear (pdfgear.com) — distribute to all hardware hobbyist user populations and include a section on verifying software hashes before execution. For remote access tool governance, maintain an approved-tools registry in a SharePoint or wiki listing authorized RAT/RMM tools with their approved relay servers, and configure AppLocker rules to block ScreenConnect client binaries on endpoints where it is not approved.

Evidence: For the lessons-learned report, compile: (1) timeline reconstruction from Sysmon and Windows Security logs showing the full attack chain from trojanized installer execution through ScreenConnect installation to LOLBin hollowing — this quantifies attacker dwell time; (2) list of all endpoints where the trojanized utilities were installed (sourced from Windows Installer Event Log, Application Event Log Event ID 11707/11724) to establish the full blast radius; (3) documented Defender exclusion paths added by the malware to support the control gap narrative for CM-7 remediation; (4) any AI chatbot conversation artifacts (browser history, cached pages) demonstrating how users were referred to the poisoned download sites — this directly supports the AT-2 training content development.

Detection Guidance

Primary behavioral indicators: (1) .NET LOLBins (InstallUtil.exe, RegAsm.exe, RegSvcs.exe, MSBuild.exe, AppLaunch.exe, AddInProcess.exe, aspnet_compiler.exe) exhibiting sustained high GPU utilization or initiating outbound network connections to dynamic DNS domains. (2) ScreenConnect client installation events (ScreenConnect.ClientService.exe) outside approved change windows, cross-reference against NIST AC-2 authorized software lists. (3) New scheduled tasks or Run key entries referencing 'WinSysCache' or similarly named system-lookalike strings. (4) Windows Defender exclusion additions targeting user-writable directories (check Microsoft-Windows-Windows Defender/Operational Event ID 5007 for exclusion changes). (5) DLL loads of autorun.dll or similarly named files from non-standard directories co-located with legitimate utility executables (CIS 8.2, audit log collection required). (6) Outbound DNS queries or connections to *.dynu.com or *.dynu.net from workstation-class endpoints. (7) Download of ZIP archives from domains impersonating CrystalDiskInfo, HWMonitor, Display Driver Uninstaller, FurMark, K-Lite Codec Pack, or PDFgear; verify download source URLs against official vendor domains before execution. NIST AU-6 (audit record review) and NIST SI-4 (system monitoring) are the primary control anchors for detection operations. D3-LAM (Local Account Monitoring) and D3-SFA (System File Analysis) are applicable D3FEND countermeasures.

Indicators of Compromise

Type	Value	Context	Confidence
DOMAIN	`*.dynu.com`	Dynu dynamic DNS used for C2 infrastructure and payload hosting	HIGH
DOMAIN	`*.dynu.net`	Dynu dynamic DNS used for C2 infrastructure and payload hosting	HIGH
URL	`https://www.microsoft.com/en-us/security/blog/2026/05/26/poisoned-search-results-gpu-mining-cryptojacking-campaign-abusing-screenconnect-microsoft-net-utilities/`	Primary Microsoft Defender Experts advisory — contains full IOC list including specific domains, hashes, and file paths. Retrieve current IOC table directly from this source.	HIGH

Framework Mappings

MITRE-ATTACK

- **T1568** — Dynamic Resolution
- **T1598** — Phishing for Information
- **T1562.001** — Disable or Modify Tools
- **T1071** — Application Layer Protocol
- **T1496** — Resource Hijacking
- **T1195** — Supply Chain Compromise
- **T1055.012** — Process Hollowing
- **T1059** — Command and Scripting Interpreter
- **T1218** — System Binary Proxy Execution
- **T1036** — Masquerading
- **T1219** — Remote Access Tools
- **T1583.001** — Domains
- **T1027** — Obfuscated Files or Information
- **T1078** — Valid Accounts
- **T1053.005** — Scheduled Task
- **T1543** — Create or Modify System Process
- **T1608.006** — SEO Poisoning
- **T1021.005** — VNC
- **T1574.002** — DLL Side-Loading
- **T1547.001** — Registry Run Keys / Startup Folder

NIST-800-53R5

- **CA-7** — Continuous Monitoring
- **SC-7** — Boundary Protection
- **SI-4** — System Monitoring

- **SA-9** — External System Services
- **SR-2** — Supply Chain Risk Management Plan
- **SR-3** — Supply Chain Controls and Processes
- **SI-7** — Software, Firmware, and Information Integrity
- **CM-7** — Least Functionality
- **SI-3** — Malicious Code Protection
- **AC-2** — Account Management
- **AC-6** — Least Privilege
- **IA-2** — Identification and Authentication (Organizational Users)
- **IA-5** — Authenticator Management
- **CM-3** — Configuration Change Control
- **CP-9** — System Backup
- **IR-4** — Incident Handling

OWASP-TOP10-2021

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

CIS-V8

- **2.5** — Allowlist Authorized Software
- **2.6** — Allowlist Authorized Libraries
- **6.3** — Require MFA for Externally-Exposed Applications
- **8.2** — Collect Audit Logs

NIST-CSF-2

- **RS.MI-01** — Incidents are contained
- **DE.CM-01** — Networks and network services are monitored

HIPAA-SECURITY

- **164.308(a)(7)(ii)(A)** — Data Backup Plan
- **164.312(d)** — Person or Entity Authentication
- **164.308(a)(6)(ii)** — Response and Reporting

ISO-27001-2022

- **A.5.29** — Information security during disruption
- **A.5.34** — Privacy and protection of personal information

SOC2-TSC

- **CC6.1** — Logical access security software, infrastructure, and architectures
- **CC7.4** — Responds to identified security incidents

MITRE ATT&CK Mapping

Technique ID	Technique Name	Tactic
T1568	Dynamic Resolution	Command-And-Control
T1598	Phishing for Information	Reconnaissance
T1562.001	Disable or Modify Tools	Defense-Evasion
T1071	Application Layer Protocol	Command-And-Control
T1496	Resource Hijacking	Impact
T1195	Supply Chain Compromise	Initial-Access
T1055.012	Process Hollowing	Defense-Evasion
T1059	Command and Scripting Interpreter	Execution
T1218	System Binary Proxy Execution	Defense-Evasion
T1036	Masquerading	Defense-Evasion
T1219	Remote Access Tools	Command-And-Control
T1583.001	Domains	Resource-Development
T1027	Obfuscated Files or Information	Defense-Evasion
T1078	Valid Accounts	Defense-Evasion
T1053.005	Scheduled Task	Execution
T1543	Create or Modify System Process	Persistence
T1608.006	SEO Poisoning	Resource-Development
T1021.005	VNC	Lateral-Movement
T1574.002	DLL Side-Loading	Persistence
T1547.001	Registry Run Keys / Startup Folder	Persistence

Sources

Source	URL	Tier
Microsoft Security Blog	https://www.microsoft.com/en-us/security/blog/2026/05/26/poisoned-s...	T1
	https://www.microsoft.com/en-us/security/blog/2026/05/26/poisoned-s...	T1
Microsoft Cryptojacking Campaign Uses AI Links and Fake Utilities ...	https://windowsforum.com/threads/microsoft-cryptojacking-campaign-u...	T3

Source	URL	Tier
ScreenConnect™ Extensions & Integrations	https://www.screenconnect.com/features/extensions	T3
ScreenConnect Product Forum / ScreenConnect	https://screenconnect.product.connectwise.com/	T3

Generated 2026-05-27 06:37 UTC by TJS Security Command Center