INTELLIGENCE BRIEFING
Security Command Center
TLP:CLEAR
2026-06-03 19:09 UTC

Triple Convergence: Weedhack, CountLoader, and Unnamed Cryptominer Target Endpoints via Social Engineering and Pirated Content

THREAT CAMPAIGN | **HIGH** | CVSS 7.5

SCC Item ID	SCC-CAM-2026-0402
Type	Threat Campaign
Severity	HIGH
CVSS Base Score	7.5
Affected Products	Minecraft (versions 1.21.0-1.21.11), Microsoft Defender, Windows (mshta.exe/PowerShell), XMRig, Cobalt Strike, AdaptixC2, PureHVNC RAT, Amatera Stealer, PureMiner, SilentCryptoMiner, Discord, Steam, Telegram, 36 web browsers, 56 browser-based crypto wallets, 12 desktop wallet apps
Published	2026-06-03T02:16:54
Discovery Source	Rss

Executive Summary

Three active malware campaigns, Weedhack, CountLoader, and an unnamed cryptomining operation, have collectively compromised over 86,000 endpoints by exploiting consumer trust in gaming content, pirated software, and streaming sites. Weedhack targets Minecraft players with credential-stealing malware capable of draining browser-stored passwords and cryptocurrency wallets; CountLoader establishes persistent remote access footholds via cracked software channels; the third campaign hijacks clipboard data to redirect cryptocurrency transactions while silently mining Monero. Organizations face dual risk: direct endpoint compromise through employee personal device crossover and enterprise network intrusion via CountLoader's Cobalt Strike and AdaptixC2 beacons, which are designed for lateral movement.

Technical Analysis

Three concurrent campaigns share delivery-chain characteristics, YouTube social engineering, pirated content sites, and cracked software distribution, while deploying distinct payloads.

Weedhack: Targets Minecraft Java Edition versions 1.21.0-1.21.11. Trojanized hacked clients (notably Wurst) are distributed via YouTube lure videos. Payload chain delivers PureHVNC RAT and Amatera Stealer. Stealer harvests credentials from 36 browsers, 56 browser-based crypto wallets, and 12 desktop wallet apps. Exfiltration channels: Discord, Steam, and Telegram webhooks/APIs. Persistence via mshta.exe (T1218.005)

and PowerShell (T1059.001). Microsoft Defender evasion confirmed (T1562.001). Relevant CWEs: CWE-829 (inclusion of functionality from untrusted control sphere), CWE-426 (untrusted search path), CWE-494 (download of code without integrity check).

CountLoader: MaaS framework distributed via cracked software sites. Multi-stage loader delivers Cobalt Strike and AdaptixC2 C2 beacons. Establishes persistent remote access via PowerShell (T1059.001) and JavaScript (T1059.007) execution, registry modification (T1112), and boot/logon autostart (T1547). DLL sideloading (T1574.002) and process injection (T1055) observed. Obfuscation (T1027) and code signing abuse (T1553) used to bypass defenses.

Unnamed cryptomining campaign: Delivered via pirated streaming sites. Payloads: PureMiner and SilentCryptoMiner (XMRig-based, T1496). Clipboard hijacking (T1115) redirects outbound cryptocurrency transactions. Proxy-based C2 (T1090) for miner management. Persistence mirrors Weedhack pattern: mshta.exe and PowerShell abuse.

Shared TTPs across all three: T1204.002 (malicious file execution), T1566 (phishing/social engineering lure), T1071.001 (application layer C2 over HTTP/S), T1041 (exfiltration over C2 channel), T1056.001 (keylogging), T1555 (credential store access), T1539 (session token theft), T1113 (screen capture), T1125 (video capture). No CVE identifiers are associated with this campaign set; exploitation is social engineering-driven, not vulnerability-based. No vendor patch is applicable, mitigation is behavioral and policy-driven.

Action Checklist

1. Step 1: Containment. Block known delivery channels at the network perimeter: deny outbound connections to Discord, Steam, and Telegram API endpoints from non-approved endpoints; block pirated streaming site categories via DNS/web proxy filtering. Isolate any endpoint exhibiting mshta.exe or PowerShell spawning from browser or media player processes. Reference: NIST SI-4 (System Monitoring), CIS Benchmark 4.4 (Firewall on Servers), CIS Benchmark 4.5 (Firewall on End-User Devices). Concrete steps: Add firewall rules to block api.telegram.org, cdn.discordapp.com, api.steampowered.com on your perimeter gateway.
2. Step 2: Detection. Search endpoint logs for: (a) mshta.exe or PowerShell child processes spawned by browser, game launcher, or media player executables; (b) PowerShell executing encoded commands (Get-Content, IEX, -EncodedCommand flags); (c) outbound HTTP/S connections to Discord CDN (cdn.discordapp.com), Steam API (api.steampowered.com), or Telegram Bot API (api.telegram.org) from non-approved processes; (d) clipboard monitoring API calls (OpenClipboard/GetClipboardData) from unsigned or newly installed processes; (e) XMRig process signatures or CPU utilization spikes on endpoints not running authorized compute workloads. Event IDs to review: Windows Security 4688 (process creation with command line), Sysmon Event ID 1 (process creation), Sysmon Event ID 3 (network connection). Reference: NIST AU-2 (Event Logging), NIST AU-6 (Audit Record Review), NIST SI-4, CIS Benchmark 8.2 (Collect Audit Logs).
3. Step 3: Eradication. No vendor patch applies; these campaigns are social engineering-driven. Eradication steps: (a) Remove identified malware artifacts (PureHVNC RAT, Amatera Stealer, PureMiner, SilentCryptoMiner, Cobalt Strike/AdaptixC2 beacon files) using EDR tooling; (b) enforce application allowlisting to block unauthorized executables including mshta.exe invocations outside system contexts (reference: NIST CM-7, CIS Benchmark 2.3 Address Unauthorized Software); (c) revoke and rotate all credentials stored in browsers on affected endpoints (reference: D3-CRO Credential Rotation, D3-CH Credential Hardening); (d) audit and remove unauthorized software including game hacking clients and

cracked applications per CIS Benchmark 2.1 and CIS Benchmark 2.3.

4. Step 4: Recovery. Validate remediation by: (a) confirming no mshta.exe or unauthorized PowerShell execution recurs via EDR telemetry for 72 hours post-cleanup; (b) verifying browser credential stores have been cleared and repopulated only with freshly rotated credentials; (c) scanning for XMRig process artifacts or residual scheduled tasks/autostart registry keys (HKCU\Software\Microsoft\Windows\CurrentVersion\Run) created by malware; (d) monitoring cryptocurrency wallet addresses associated with affected users for unauthorized transactions. Reference: NIST IR-4 (Incident Handling), NIST AU-6, D3-LAM (Local Account Monitoring).

5. Step 5: Post-Incident. Control gaps exposed by this campaign set: (a) absence of application allowlisting allowing unsigned executables, remediate via NIST CM-7 (Least Functionality) and CIS Benchmark 2.3; (b) insufficient user awareness around gaming and pirated content risks, address via NIST AT-2 (Awareness Training); (c) browser credential storage in plaintext/accessible stores, enforce enterprise password manager policy and disable browser-native credential storage (reference: NIST IA-5, D3-CH); (d) MFA gaps on accounts whose credentials may have been harvested, enforce MFA on all externally-exposed applications and administrative access (CIS Benchmark 6.3, CIS Benchmark 6.5, D3-MFA); (e) inadequate monitoring of mshta.exe and PowerShell LOLBin abuse, implement Sysmon rules and SIEM detections for living-off-the-land binary abuse (NIST SI-4, AU-12).

IR / Forensic Enrichment

Triage Priority	IMMEDIATE
Escalation Criteria	Escalate to senior IR leadership, legal counsel, and potentially CISA if: (1) Amatera Stealer exfiltration is confirmed from endpoints storing PII, PHI, or financial credentials triggering state breach notification obligations; (2) Cobalt Strike or AdaptixC2 beaconing is detected indicating CountLoader has progressed beyond initial access to active operator-controlled intrusion; (3) more than 10 endpoints show XMRig or clipboard hijacker activity indicating campaign-scale compromise beyond isolated user incidents; or (4) harvested credentials are confirmed used for unauthorized access to corporate systems, cloud accounts, or cryptocurrency wallets holding organizational funds.
Recovery Notes	Post-containment, maintain elevated monitoring of mshta.exe, PowerShell encoding activity, and outbound connections to Discord/Telegram/Steam API endpoints for a minimum of 14 days given that PureHVNC RAT and Cobalt Strike/AdaptixC2 implants may have staged secondary persistence mechanisms not captured in initial eradication. Verify all 36 browser credential stores and 12 desktop wallet application directories on affected endpoints have been cleared and that users have rotated credentials at every service where a stored password was present — prioritize cryptocurrency exchange accounts and any corporate SSO credentials given the Amatera Stealer's confirmed targeting of these asset types. Confirm Minecraft clients on affected systems are sourced exclusively from the official Mojang/Microsoft launcher after incident closure, and validate that no unofficial mod loaders (e.g., unlicensed Forge or Fabric installers sourced from third-party sites) remain installed, as these represent the primary re-infection vector for Weedhack.

Forensic Artifacts	Windows Prefetch files (C:\Windows\Prefetch\MSHTA.EXE-*.pf and POWERSHELL.EXE-*.pf) — these record execution timestamps and file paths for mshta.exe and PowerShell invocations triggered by Weedhack and CountLoader droppers, providing initial execution timeline even if the dropper binary has been deleted | Browser SQLite credential databases before clearance: %LOCALAPPDATA%\Google\Chrome\User Data\Default\Login Data, %APPDATA%\Mozilla\Firefox\Profiles*.default-release\logins.json, and equivalent paths for all targeted browsers — Amatera Stealer specifically targets these files and their timestamps will show last-access time consistent with exfiltration | Desktop crypto wallet keystore and seed files under %APPDATA%\Exodus\exodus.wallet, %APPDATA%\Electrum\wallets*, %APPDATA%\Atomic\Local Storage\leveldb*, and equivalent paths for the 12 targeted wallet apps — presence of recent access timestamps inconsistent with user activity indicates Amatera Stealer collection activity | Sysmon Event ID 10 (ProcessAccess) logs capturing clipboard API access (OpenClipboard/GetClipboardData calls) from unsigned or newly installed processes — these are the direct forensic signature of the clipboard hijacker component within SilentCryptoMiner and Weedhack targeting cryptocurrency wallet address substitution | XMRig configuration file and stratum connection artifacts: search %TEMP%, %APPDATA%, and all user-writable paths for config.json files containing 'pool' and 'wallet' keys, and extract XMR wallet address and pool URL from Sysmon Event ID 3 (NetworkConnect) logs showing outbound TCP 3333/4444/14444 (standard XMRig stratum ports) from xmrig.exe or a renamed variant — these provide attribution data and victim wallet compromise confirmation

Per-Action IR Details

Step 1: Containment — Block known delivery channels at the network perimeter: deny outbound connections to Discord, Steam, and Telegram API endpoints from non-approved endpoints; block pirated streaming site categories via DNS/web proxy filtering. Isolate any endpoint exhibiting mshta.exe or PowerShell spawning from browser or media player processes. Reference: NIST SI-4 (System Monitoring), CIS 4.4 (Firewall on Servers), CIS 4.5 (Firewall on End-User Devices).

NIST Phase: Containment

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

Controls: NIST SI-4 (System Monitoring), NIST AC-4 (Information Flow Enforcement), NIST SC-7 (Boundary Protection), CIS 4.4 (Implement and Manage a Firewall on Servers), CIS 4.5 (Implement and Manage a Firewall on End-User Devices)

Compensating: For teams without NGFW or proxy: deploy Windows Firewall GPO rules blocking outbound TCP 443 to cdn.discordapp.com, api.steampowered.com, and api.telegram.org for all user-tier processes except explicitly approved apps — use 'netsh advfirewall firewall add rule' or PowerShell New-NetFirewallRule targeting by remote address ranges. Use Pi-hole or Windows DNS policy to sinkhole known pirated streaming domains. For mshta.exe isolation, deploy a Sysmon rule (EventID 1) alerting on mshta.exe with ParentImage matching chrome.exe, firefox.exe, vlc.exe, or java.exe; route alert to a local log file monitored via a scheduled Task running a PowerShell log-scan script every 15 minutes.

Evidence: Before isolating the endpoint, capture: full Sysmon Event ID 1 logs showing the parent-child process chain (e.g., chrome.exe or a Minecraft launcher spawning mshta.exe or powershell.exe); Windows Security Event ID 4688 with command-line logging enabled showing encoded PowerShell invocations tied to CountLoader or Weedhack dropper activity; Windows Firewall operational log (Microsoft-Windows-Windows Firewall With Advanced Security/Firewall) for outbound connection attempts to Discord CDN, Telegram Bot API, and Steam API endpoints; network capture (pcap via Wireshark on the gateway) of DNS queries and TCP sessions to cdn.discordapp.com and api.telegram.org from the affected host; memory image (via WinPmem or Magnet RAM Capture) before isolation if Cobalt Strike or AdaptixC2 beacon is suspected resident in-memory.

Step 2: Detection — Search endpoint logs for: (a) mshta.exe or PowerShell child processes spawned by browser, game launcher, or media player executables; (b) PowerShell executing encoded commands (Get-Content, IEX, -EncodedCommand flags); (c) outbound HTTP/S connections to Discord CDN (cdn.discordapp.com), Steam API (api.steampowered.com), or Telegram Bot API (api.telegram.org) from non-approved processes; (d) clipboard monitoring API calls (OpenClipboard/GetClipboardData) from unsigned or newly installed processes; (e) XMRig process signatures or CPU utilization spikes on endpoints not running authorized compute workloads. Event IDs to review: Windows Security 4688 (process creation with command line), Sysmon Event ID 1 (process creation), Sysmon Event ID 3 (network connection). Reference: NIST AU-2 (Event Logging), NIST AU-6 (Audit Record Review), NIST SI-4, CIS 8.2 (Collect Audit Logs).

NIST Phase: Detection Analysis

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

Controls: NIST AU-2 (Event Logging), NIST AU-6 (Audit Record Review, Analysis, and Reporting), NIST SI-4 (System Monitoring), NIST AU-12 (Audit Record Generation), CIS 8.2 (Collect Audit Logs)

Compensating: Without a SIEM, deploy Sysmon with SwiftOnSecurity's config (includes mshta.exe, PowerShell encoding, and network connection rules out of the box); forward Sysmon and Security logs to a central Windows Event Forwarding (WEF) collector at no cost. Run this PowerShell one-liner on each host to surface encoded command execution: Get-WinEvent -LogName Security | Where-Object {$_.Id -eq 4688 -and $_.Message -match 'EncodedCommand|IEX|Get-Content'} | Select-Object TimeCreated, Message | Export-Csv encoded_ps.csv. For clipboard hijacker detection (targeting crypto wallet address substitution by Weedhack/SilentCryptoMiner), use Sysmon Event ID 10 (ProcessAccess) filtering on GrantedAccess 0x1fffff where TargetImage is the calling process; cross-reference with osquery query: SELECT * FROM processes WHERE name LIKE '%xmrig%' OR cmdline LIKE '%stratum%' to detect XMRig pool connections. Use the Sigma rule 'proc_creation_win_mshta_suspicious_parent.yml' from SigmaHQ for mshta parent-process anomalies.

Evidence: Collect before completing analysis: Sysmon Event ID 3 (NetworkConnect) logs filtered for connections from mshta.exe, powershell.exe, or newly created processes to Discord CDN IP ranges (162.159.x.x Cloudflare space used by Discord) and Telegram API (149.154.x.x, 91.108.x.x); Sysmon Event ID 8 (CreateRemoteThread) entries showing potential Cobalt Strike or AdaptixC2 injection into legitimate host processes; Windows Security Event ID 4657 (Registry value modified) or Sysmon Event ID 13 for writes to HKCU\Software\Microsoft\Windows\CurrentVersion\Run by any process other than a known installer; browser credential store files before they are wiped — copy %LOCALAPPDATA%\Google\Chrome\User Data\Default\Login Data, %APPDATA%\Mozilla\Firefox\Profiles*.default\logins.json, and equivalent paths for all 36 targeted browsers; desktop crypto wallet data directories (e.g., %APPDATA%\Exodus, %APPDATA%\Electrum\wallets, %APPDATA%\Atomic) to establish whether Amatera Stealer exfiltrated wallet files.

Step 3: Eradication — No vendor patch applies; these campaigns are social engineering-driven. Eradication steps: (a) Remove identified malware artifacts (PureHVNC RAT, Amatera Stealer, PureMiner, SilentCryptoMiner, Cobalt Strike/AdaptixC2 beacon files) using EDR tooling; (b) enforce application allowlisting to block unauthorized executables including mshta.exe invocations outside system contexts (reference: NIST CM-7, CIS 2.3 Address Unauthorized Software); (c) revoke and rotate all credentials stored in browsers on affected endpoints (reference: D3-CRO Credential Rotation, D3-CH Credential Hardening); (d) audit and remove unauthorized software including game hacking clients and cracked applications per CIS 2.1 and CIS 2.3.

NIST Phase: Eradication

Reference: NIST 800-61r3 §3.4 — Eradication

Controls: NIST CM-7 (Least Functionality), NIST SI-2 (Flaw Remediation), NIST IA-5 (Authenticator Management), NIST AC-2 (Account Management), CIS 2.1 (Establish and Maintain a Software Inventory), CIS 2.3 (Address Unauthorized Software)

Compensating: Without EDR, build YARA rules targeting PureHVNC, PureMiner, and SilentCryptoMiner string signatures (search GitHub for published rules from ANY.RUN or Malpedia entries for these families); run via YARA CLI: yara -r purehvnc_rule.yar C:\ > hits.txt. Use Autoruns (Sysinternals) to enumerate and delete persistence entries written by the malware to HKCU\Software\Microsoft\Windows\CurrentVersion\Run, HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon, and scheduled task XML files under C:\Windows\System32\Tasks. Disable mshta.exe invocation outside trusted installer contexts via Windows AppLocker Publisher or Path rules (available on Windows 10 Pro/Enterprise at no cost): deny mshta.exe execution for all users except SYSTEM in a GPO-linked AppLocker policy. For credential revocation without enterprise tooling, use a browser-exported credentials audit: instruct users to run 'chrome://settings/passwords' export, identify all stored credentials, force password resets at the service level for every stored credential, then clear browser profiles entirely rather than selectively.

Evidence: Before eradication, forensically image or collect: full directory listing and hash inventory of C:\Users\[user]\AppData\Roaming and C:\Users\[user]\AppData\Local\Temp where CountLoader, Weedhack, and PureMiner dropper artifacts are typically staged; hash values (SHA-256) of every executable in the affected user's Downloads, Desktop, and temp folders for submission to VirusTotal and internal IOC tracking; export of all scheduled tasks (schtasks /query /fo CSV /v > tasks_export.csv) and all Run/RunOnce registry keys before removal to document persistence mechanism specifics used by this campaign; collected browser Login Data SQLite files and any crypto wallet seed/keystore files present under the 12 targeted desktop wallet app directories (Exodus, Electrum, Atomic, Coinomi, etc.) to establish scope of potential credential and wallet compromise; a process memory dump of any running instance of xmrig.exe or an unrecognized process with high CPU utilization to extract XMR wallet address and mining pool URL for IOC reporting and victim notification.

Step 4: Recovery — Validate remediation by: (a) confirming no mshta.exe or unauthorized PowerShell execution recurs via EDR telemetry for 72 hours post-cleanup; (b) verifying browser credential stores have been cleared and repopulated only with freshly rotated credentials; (c) scanning for XMRig process artifacts or residual scheduled tasks/autostart registry keys (HKCU\Software\Microsoft\Windows\CurrentVersion\Run) created by malware; (d) monitoring cryptocurrency wallet addresses associated with affected users for unauthorized transactions. Reference: NIST IR-4 (Incident Handling), NIST AU-6, D3-LAM (Local Account Monitoring).

NIST Phase: Recovery

Reference: NIST 800-61r3 §3.5 — Recovery

Controls: NIST IR-4 (Incident Handling), NIST AU-6 (Audit Record Review, Analysis, and Reporting), NIST CM-7 (Least Functionality), NIST AC-2 (Account Management), CIS 7.2 (Establish and Maintain a Remediation Process)

Compensating: Without EDR telemetry, run a recurring scheduled task (every 4 hours for the 72-hour window) executing this PowerShell validation script: Get-WinEvent -LogName Microsoft-Windows-Sysmon/Operational | Where-Object {$_.Id -eq 1 -and ($_.Message -match 'mshta.exe' -or ($_.Message -match 'powershell' -and $_.Message -match 'EncodedCommand'))} | Export-Csv C:\IR\recovery_check.csv -Append — review output daily. Validate credential store clearance by checking Chrome Login Data file size (should be minimal if cleared) and verifying Firefox logins.json is absent or empty in all user profiles. For autorun registry persistence verification, run Autoruns with 'Hide Microsoft Entries' checked and export to CSV baseline; diff against a clean reference system. For XMR wallet monitoring, use a free blockchain explorer (e.g., xmrchain.net) with the extracted wallet address from memory forensics to check for outbound transactions.

Evidence: Evidence to confirm successful recovery: Sysmon Event ID 1 logs for the 72-hour post-cleanup window showing no new instances of mshta.exe, xmrig.exe, pureminer.exe, or powershell.exe with -EncodedCommand flags; Autoruns CSV export post-cleanup showing no entries under HKCU\Software\Microsoft\Windows\CurrentVersion\Run, scheduled tasks, or AppInit_DLLs that were not present on a clean reference baseline; browser profile directory timestamps confirming credential stores were cleared and recreated after the malware removal timestamp; Windows Security Event ID 4720/4726 (account created/deleted) and 4648 (explicit credential use) logs to detect any post-compromise lateral movement or new account creation by PureHVNC RAT before containment was confirmed complete; network flow logs (or Windows Firewall logs) for the recovery period confirming absence of outbound connections to previously identified C2 infrastructure associated with Cobalt Strike, AdaptixC2, or XMRig stratum pool endpoints.

Step 5: Post-Incident — Control gaps exposed by this campaign set: (a) absence of application allowlisting allowing unsigned executables — remediate via NIST CM-7 (Least Functionality) and CIS 2.3; (b) insufficient user awareness around gaming and pirated content risks — address via NIST AT-2 (Awareness Training); (c) browser credential storage in plaintext/accessible stores — enforce enterprise password manager policy and disable browser-native credential storage (reference: NIST IA-5, D3-CH); (d) MFA gaps on accounts whose credentials may have been harvested — enforce MFA on all externally-exposed applications and administrative access (CIS 6.3, CIS 6.5, D3-MFA); (e) inadequate monitoring of mshta.exe and PowerShell LOLBin abuse — implement Sysmon rules and SIEM detections for living-off-the-land binary abuse (NIST SI-4, AU-12).

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 IA-5 (Authenticator Management), NIST SI-4 (System Monitoring), NIST AU-12 (Audit Record Generation), CIS 2.3 (Address Unauthorized Software), CIS 6.3 (Require MFA for Externally-Exposed Applications), CIS 6.5 (Require MFA for Administrative Access)

Compensating: For AppLocker deployment on a zero-budget team: enable AppLocker via GPO (Computer Configuration > Windows Settings > Security Settings > Application Control Policies) with rules denying execution from %TEMP%, %APPDATA%, and user-writable paths — this directly blocks the dropper delivery paths used by Weedhack and CountLoader without any commercial tooling. For awareness training specific to this campaign, build a 10-minute internal briefing using screenshots from the Weedhack Minecraft mod delivery lure and CountLoader cracked software channels; focus on the specific social engineering premise (gaming performance tools, pirated content) rather than generic phishing. For free password manager enforcement, deploy Bitwarden (self-hosted or cloud free tier) and publish a policy prohibiting browser-native credential storage — enforce by GPO setting DisablePasswordReveal and the Chrome policy PasswordManagerEnabled=false via ADM template. For LOLBin detection hardening, add the Sigma ruleset 'windows/process_creation/proc_creation_win_lolbin_*.yml' from SigmaHQ to your WEF/Sysmon pipeline and tune false positives against your environment's legitimate mshta.exe and PowerShell usage baseline.

Evidence: Post-incident artifacts to collect for lessons learned and threat intelligence sharing: final IOC list compiled from all recovered artifacts — XMR wallet addresses, Cobalt Strike/AdaptixC2 C2 IP addresses and domain names, file hashes (SHA-256) of all identified PureHVNC, Amatera Stealer, PureMiner, and SilentCryptoMiner samples for submission to CISA's Malware Next-Gen Analysis platform and sharing via ISAC if applicable; documentation of all 36 browser credential stores and 12 desktop wallet application paths confirmed affected to support user notification and scope reporting; AppLocker or software restriction policy baseline gaps documented — specifically which unsigned executables were found in %TEMP% and %APPDATA% paths that a deny-by-default policy would have blocked; timeline reconstruction mapping the initial Minecraft mod or cracked installer download event (browser download history, Windows Prefetch files under C:\Windows\Prefetch for the dropper binary name) through to first C2 callback for post-incident report and detection rule improvement; gap analysis comparing pre-incident Sysmon configuration against SwiftOnSecurity's recommended baseline to document which LOLBin execution events were not being logged at time of compromise.

Detection Guidance

Behavioral indicators (prioritize these, no CVE-based signatures apply):

1. Process lineage anomalies: mshta.exe or PowerShell spawned as a child of a browser (chrome.exe, firefox.exe, msedge.exe), game launcher (javaw.exe, Minecraft launcher), or media player. This is not normal behavior and should alert immediately.

2. Encoded PowerShell execution: Command lines containing -EncodedCommand, IEX (Invoke-Expression), or DownloadString from non-administrative contexts. Sysmon Event ID 1 with CommandLine field matching these

patterns.

3. Clipboard API abuse: Processes calling OpenClipboard/GetClipboardData at high frequency, particularly unsigned or recently installed binaries. Cross-reference with cryptocurrency wallet address patterns (Ethereum: 0x + 40 hex characters; Bitcoin: 26-35 base58 characters; Monero: 104-110 base58 characters) in clipboard content.

4. C2 exfiltration channels: Outbound HTTPS connections to api.telegram.org, cdn.discordapp.com, or steamcommunity.com from non-browser, non-approved processes. NIST AU-3 requires audit records capturing source process, confirm your logging captures this field.

5. XMRig/cryptominer indicators: CPU utilization sustained above 80% on endpoints during off-hours; process names or hashes matching XMRig, PureMiner, or SilentCryptoMiner; outbound connections to Monero mining pool domains (pool.supportxmr.com, xmrpool.eu, minexmr.com and similar).

6. Persistence mechanisms: New entries in HKCU\Software\Microsoft\Windows\CurrentVersion\Run or HKLM equivalent created by non-system processes; scheduled tasks created by user-context processes; DLL files placed in application directories alongside legitimate executables (DLL sideloading, T1574.002). Use D3-SICA (MITRE ATT&CK Defense System Init Config Analysis) and D3-SFA (System File Analysis) to baseline and monitor these locations.

7. Cobalt Strike/AdaptixC2 beacon patterns: Periodic beaconing at regular intervals (every 60s, 120s, or 300s) to HTTPS endpoints; JA3/JA3S TLS fingerprints matching known Cobalt Strike profiles; large POST requests to pseudo-random URI paths. Reference NIST AU-6 and SI-4 for continuous monitoring requirements.

Log sources to enable if not already active: Windows Security Event Log (4688 with command-line auditing), Sysmon (Events 1, 3, 11, 13), DNS query logs, proxy/web gateway logs with full URL and process attribution, EDR telemetry.

Indicators of Compromise

Type	Value	Context	Confidence
DOMAIN	`api.telegram.org`	Exfiltration channel used by Weedhack/Amatera Stealer for credential and wallet data exfiltration via Telegram Bot API	MEDIUM
DOMAIN	`cdn.discordapp.com`	Exfiltration channel used by Weedhack campaign for stolen credential delivery via Discord webhooks	MEDIUM
DOMAIN	`steamcommunity.com`	Exfiltration channel used by Weedhack campaign via Steam API	MEDIUM
URL	`https://www.youtube.com/watch?v=ssD8jKlb8ws`	YouTube lure video distributing trojanized Wurst hacked client for Minecraft 1.21.11 — confirmed delivery vector per source reporting	MEDIUM

Framework Mappings

MITRE-ATTACK

- **T1113** — Screen Capture
- **T1091** — Replication Through Removable Media
- **T1059.001** — PowerShell
- **T1125** — Video Capture
- **T1041** — Exfiltration Over C2 Channel
- **T1090** — Proxy
- **T1071.001** — Web Protocols
- **T1566** — Phishing
- **T1547** — Boot or Logon Autostart Execution
- **T1059.007** — JavaScript
- **T1056.001** — Keylogging
- **T1055** — Process Injection
- **T1562.001** — Disable or Modify Tools
- **T1218.005** — Mshta
- **T1027** — Obfuscated Files or Information
- **T1553** — Subvert Trust Controls
- **T1496** — Resource Hijacking
- **T1608.001** — Upload Malware
- **T1539** — Steal Web Session Cookie
- **T1112** — Modify Registry
- **T1555** — Credentials from Password Stores
- **T1574.002** — DLL Side-Loading
- **T1204.002** — Malicious File
- **T1071** — Application Layer Protocol
- **T1115** — Clipboard Data

NIST-800-53R5

- **CM-7** — Least Functionality
- **SI-3** — Malicious Code Protection
- **SI-4** — System Monitoring
- **SI-7** — Software, Firmware, and Information Integrity
- **CA-7** — Continuous Monitoring
- **SC-7** — Boundary Protection
- **AT-2** — Literacy Training and Awareness
- **SI-8** — Spam Protection
- **AC-6** — Least Privilege
- **CM-3** — Configuration Change Control

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

HIPAA-SECURITY

- **164.312(d)** — Person or Entity Authentication

SOC2-TSC

- **CC6.1** — Logical access security software, infrastructure, and architectures

MITRE ATT&CK Mapping

Technique ID	Technique Name	Tactic
T1113	Screen Capture	Collection
T1091	Replication Through Removable Media	Lateral-Movement
T1059.001	PowerShell	Execution
T1125	Video Capture	Collection
T1041	Exfiltration Over C2 Channel	Exfiltration
T1090	Proxy	Command-And-Control
T1071.001	Web Protocols	Command-And-Control
T1566	Phishing	Initial-Access
T1547	Boot or Logon Autostart Execution	Persistence
T1059.007	JavaScript	Execution
T1056.001	Keylogging	Collection
T1055	Process Injection	Defense-Evasion
T1562.001	Disable or Modify Tools	Defense-Evasion
T1218.005	Mshta	Defense-Evasion
T1027	Obfuscated Files or Information	Defense-Evasion
T1553	Subvert Trust Controls	Defense-Evasion
T1496	Resource Hijacking	Impact

Technique ID	Technique Name	Tactic
T1608.001	Upload Malware	Resource-Development
T1539	Steal Web Session Cookie	Credential-Access
T1112	Modify Registry	Defense-Evasion
T1555	Credentials from Password Stores	Credential-Access
T1574.002	DLL Side-Loading	Persistence
T1204.002	Malicious File	Execution
T1071	Application Layer Protocol	Command-And-Control
T1115	Clipboard Data	Collection

Sources

Source	URL	Tier
Security News	https://thehackernews.com/2026/06/weedhack-attacks-minecraft-users....	T3
Minecraft 1.21.1 Release Candidate 1 | Critical Exploits Fixed!	https://www.youtube.com/watch?v=QEEPZFkxRF8	T3
Minecraft 1.21 Release Candidate 1	https://www.minecraft.net/en-us/article/minecraft-1-21-release-cand...	T3
Download: Wurst Hacked Client 1.21.11 | Minecraft Java Edition	https://www.youtube.com/watch?v=ssD8jKlb8ws	T3
Minecraft Bedrock 1.21 Update Notes for Creators - Microsoft Learn	https://learn.microsoft.com/sv-se/minecraft/creator/documents/updat...	T1

Generated 2026-06-03 19:09 UTC by TJS Security Command Center