INTELLIGENCE BRIEFING
Security Command Center
TLP:CLEAR
2026-06-03 06:52 UTC

WeedHack MaaS Infostealer Exploits Gaming Communities to Harvest Credentials at Scale

THREAT CAMPAIGN | **HIGH** | CVSS 5.0

SCC Item ID	SCC-CAM-2026-0399
Type	Threat Campaign
Severity	HIGH
CVSS Base Score	5.0
Affected Products	Minecraft (versions 1.21.0-1.21.10), 36 browsers (unspecified), 12 desktop cryptocurrency wallet applications, Discord, Steam, Telegram
Published	2026-06-02T17:54:49
Discovery Source	Rss

Executive Summary

WeedHack is an active Malware-as-a-Service infostealer campaign that has infected over 116,000 systems since January 2026, spreading through trojanized Minecraft mod files promoted via YouTube and search engine manipulation. According to BleepingComputer reporting, the malware harvests credentials from 36 browsers, 12 cryptocurrency wallets, Discord, Steam, and Telegram at an estimated rate of 2,000-3,000 new infections daily. Enterprise risk centers on credential reuse: employees who game on personal devices may carry compromised credentials into corporate systems.

Technical Analysis

WeedHack operates as a tiered MaaS platform. The free tier provides credential harvesting; the premium tier (under $25) adds full remote access capability (T1021). Distribution relies on SEO poisoning (T1608.004) and YouTube video description lures (T1608.006) pointing to trojanized Minecraft mod files for versions 1.21.0-1.21.10. Execution is user-initiated via malicious file download (T1204.002, T1566). Once running, the stealer performs keylogging (T1056.001), browser credential extraction (T1555.003), session cookie theft (T1539), and screen capture (T1113). Command-and-control uses HTTP/S (T1071.001). Adversary infrastructure includes web services staged for lure delivery (T1583.006) and spear-phishing resource staging (T1598). Relevant CWEs: CWE-494 (Download of Code Without Integrity Check, no signature validation on mod files), CWE-312 (Cleartext Storage of Sensitive Information, credentials stored unencrypted), CWE-306 (Missing Authentication for Critical Function, premium remote access). No CVE assigned; this is a campaign, not a discrete software vulnerability. No vendor patch exists; the attack exploits user behavior and social engineering rather than a patchable code flaw in Minecraft. Primary reporting via BleepingComputer (T3 source). CVSS

does not apply to threat campaigns; severity is set editorially based on attack scope, target criticality, and operational impact.

Action Checklist

1. Step 1: Containment. Block known WeedHack distribution vectors at the perimeter: configure DNS and web proxies to block YouTube redirect chains leading to external file hosting (Mediafire, MEGA, Discord CDN links in video descriptions). Alert on downloads of .jar and .zip files from non-sanctioned sources on managed endpoints. Enforce host-based firewall rules consistent with CIS Control 6 (Access Control) and NIST SC-7 (Boundary Protection) to restrict unexpected outbound connections from gaming-adjacent processes.
2. Step 2: Detection. Query endpoint logs for execution of unsigned .jar files or PowerShell launched from browser or download manager processes. Hunt for MITRE T1555.003 indicators: access to browser credential store paths (e.g., Login Data, cookies databases) by non-browser processes. Check for T1539 session cookie harvesting: unusual reads of browser profile directories. Review SIEM for outbound HTTP/S beaconing to low-reputation domains from endpoints with Minecraft or Java Runtime installed (T1071.001). Cross-reference AU-6 audit log review against known WeedHack C2 patterns reported by BleepingComputer. Apply D3 (Detection Maturity Model) logic: D3-LAM (Local Account Monitoring) to flag new local account creation, and D3-SFA (System File Analysis) to flag abnormal credential store access by non-application processes.
3. Step 3: Eradication. For confirmed infections: isolate the endpoint and revoke all browser-saved credentials and session tokens from the affected user's accounts immediately. Reset credentials for any corporate SSO, VPN, or SaaS applications accessible from the compromised device per NIST AC-2 (Account Management). Enforce D3-CRO (Credential Rotation) for all accounts associated with affected users. Remove malicious mod files and scan with updated AV/EDR signatures. Disable or remove Java Runtime Environment on endpoints where it is not business-required, consistent with NIST CM (Configuration Management) and CIS Control 2 (unauthorized software removal).
4. Step 4: Recovery. Validate that rotated credentials are active and old sessions are invalidated across all corporate systems. Confirm MFA enrollment is in place for all affected accounts before restoring normal access, per CIS Control 6 (Access Control); require MFA on all externally exposed applications. Monitor AU-6 audit logs for 30 days post-remediation for residual beaconing or anomalous login patterns. Apply D3-MFA (Multi-Factor Authentication maturity) controls to all applications the affected user could access from external networks. Verify no persistence mechanisms (scheduled tasks, registry run keys) remain on remediated endpoints.
5. Step 5: Post-Incident. This campaign exploits credential reuse between personal and corporate devices, a control gap that CIS Control 5 (Account Management - unique passwords) and CIS Control 6 (MFA for externally exposed applications) directly address. Conduct a review of BYOD and personal device policies per NIST AC-19 and AC-20. Evaluate whether corporate credential vaults or SSO providers show any access anomalies from the infection window (January 2026 onward). Brief employees on SEO poisoning and social engineering lures targeting gaming communities, consistent with NIST AT-2 (Awareness Training). Consider D3-CH (Credential Hardening) controls such as hardware security keys for high-privilege accounts.

IR / Forensic Enrichment

Triage Priority	URGENT
Escalation Criteria	Escalate to immediate and engage legal/privacy counsel if SSO or IdP audit logs confirm any corporate account was accessed using WeedHack-harvested credentials during the January 2026–present infection window, as this constitutes a confirmed breach triggering GDPR Article 33, CCPA, or state breach notification obligations depending on jurisdiction and data classification of accessible systems.
Recovery Notes	After credential rotation and MFA enrollment, monitor IdP/SSO audit logs and VPN authentication logs daily for the first 14 days and weekly through 30 days post-remediation, specifically for the affected users' accounts, looking for successful authentications from unfamiliar IP geolocation, ASN, or device fingerprint — WeedHack-harvested session cookies may have a validity window that extends beyond password reset if active sessions were not explicitly invalidated at the token level. Verify that all 36 browser credential stores were cleared and not merely the primary browser, as WeedHack targets a broad browser set and residual stored credentials in secondary browsers (e.g., Opera, Brave, Vivaldi) on the same endpoint represent continued exposure. Confirm cryptocurrency wallet application reinstallation from official sources only, as wallet seed phrase exposure from the 12 targeted desktop wallets is irreversible and affected users should be advised to transfer funds to new wallets with freshly generated keys.
Forensic Artifacts	%APPDATA%\.minecraft\mods\ directory — SHA-256 hash each .jar file present; WeedHack is distributed as a trojanized mod file so any unsigned or recently added .jar not matching known CurseForge or Modrinth official mod hashes is a primary malware sample | Browser SQLite credential databases on the affected endpoint — %LOCALAPPDATA%\Google\Chrome\User Data\Default\Login Data, Cookies, and Web Data; %APPDATA%\Mozilla\Firefox\Profiles*.default\logins.json and cookies.sqlite — read-only VSS copies taken before wipe to establish which credentials were stored and available for harvest at time of infection | Sysmon Event ID 10 (ProcessAccess) log entries where the source process is javaw.exe or a child process thereof and the target process path matches any browser executable or the target object is a browser profile directory — this is the specific telemetry signature of WeedHack's T1555.003 credential store access behavior | Windows Prefetch files at C:\Windows\Prefetch\JAVAW.EXE-*.pf and any associated PowerShell prefetch entries — parse with WinPrefetchView to establish exact execution timestamps and file paths accessed by the trojanized mod at runtime, providing the attack execution timeline | Network flow records or Wireshark PCAP showing outbound HTTPS connections from javaw.exe to non-Minecraft-infrastructure domains during or after mod file execution — WeedHack exfiltrates harvested credentials over HTTP/S (T1071.001), so these flows represent the exfiltration artifact and the destination IPs/domains are your C2 IOCs for perimeter blocking and threat intel sharing

Per-Action IR Details

Step 1: Containment — Block known WeedHack distribution vectors at the perimeter: configure DNS and web proxies to block YouTube redirect chains leading to external file hosting (Mediafire, MEGA, Discord CDN links in video descriptions). Alert on downloads of .jar and .zip files from non-sanctioned sources on managed endpoints. Enforce CIS 4.4 and CIS 4.5 host-based firewall rules to restrict unexpected outbound connections from gaming-adjacent processes.

NIST Phase: Containment

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

Controls: NIST AC-4 (Information Flow Enforcement), NIST SC-7 (Boundary Protection), NIST SI-3 (Malicious Code Protection), CIS 4.4 (Implement and Manage a Firewall on Servers), CIS 4.5 (Implement and Manage a Firewall on

End-User Devices), CIS 7.1 (Establish and Maintain a Vulnerability Management Process)

Compensating: On endpoints without enterprise proxy: deploy a local hosts-file blocklist for known WeedHack distribution domains (cdn.discordapp.com paths used as drop sites, mediafire.com, mega.nz) via a pushed PowerShell script: `Add-Content C:\Windows\System32\drivers\etc\hosts '0.0.0.0 www.mediafire.com'`. For .jar download alerting, configure Sysmon Event ID 11 (FileCreate) with a target filename filter on `*.jar` and `*.zip` in user Download and Temp directories. Use Windows Firewall with Advanced Security (netsh advfirewall) to block outbound connections from javaw.exe and java.exe to non-whitelisted IPs.

Evidence: Before blocking, capture DNS query logs from your resolver (Windows DNS debug log or Pi-hole query log) to document the full redirect chain from YouTube description links through to the final Mediafire/MEGA payload URL — this establishes the distribution chain for your incident report. Export proxy or firewall logs showing which managed endpoints already retrieved .jar or .zip files from Discord CDN (cdn.discordapp.com), Mediafire, or MEGA during the January 2026–present window.

Step 2: Detection — Query endpoint logs for execution of unsigned .jar files or PowerShell launched from browser or download manager processes. Hunt for MITRE T1555.003 indicators: access to browser credential store paths (e.g., Login Data, cookies databases) by non-browser processes. Check for T1539 session cookie harvesting: unusual reads of browser profile directories. Review SIEM for outbound HTTP/S beaconing to low-reputation domains from endpoints with Minecraft or Java Runtime installed (T1071.001). Cross-reference AU-6 audit log review against known WeedHack C2 patterns reported by BleepingComputer. Apply D3-LAM (Local Account Monitoring) and D3-SFA (System File Analysis) to flag abnormal credential store access.

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 AU-12 (Audit Record Generation), NIST SI-4 (System Monitoring), CIS 8.2 (Collect Audit Logs)

Compensating: Without SIEM, run the following targeted queries manually: (1) Sysmon Event ID 1 (Process Create) — filter for parent process of chrome.exe, firefox.exe, or any browser spawning javaw.exe or powershell.exe. (2) Sysmon Event ID 10 (ProcessAccess) — filter for any process other than the browser executable itself accessing `%LOCALAPPDATA%\Google\Chrome\User Data\Default\Login Data` or equivalent Firefox/Edge paths. (3) Use Sysinternals Autoruns to detect persistence in scheduled tasks or run keys dropped by the trojanized mod. Run this osquery query on all endpoints with Java installed: `SELECT pid, name, path FROM processes WHERE name IN ('java.exe','javaw.exe');` then cross-reference those PIDs against open network connections via `SELECT * FROM process_open_sockets WHERE pid IN ();`

Evidence: Capture the following before any remediation action: full Sysmon event log (Events 1, 10, 11, 13) from the suspected infection timeframe; the contents of `%LOCALAPPDATA%\Temp` and `%APPDATA%\Roaming` directories for .jar files or unfamiliar subdirectories created by javaw.exe; browser SQLite credential databases (`Login Data`, `Cookies`, `Web Data`) with read-only copies taken via VSS shadow copy to preserve pre-wipe state; Windows Prefetch files for javaw.exe and any PowerShell invocations (C:\Windows\Prefetch\JAVAW.EXE-*.pf) to establish execution timeline; network capture (Wireshark on the endpoint or a TAP) of any active outbound connections from java.exe to document C2 beacon patterns.

Step 3: Eradication — For confirmed infections: isolate the endpoint, revoke all browser-saved credentials and session tokens from the affected user's accounts immediately. Reset credentials for any corporate SSO, VPN, or SaaS applications accessible from the compromised device (NIST AC-2 account management). Enforce D3-CRO (Credential Rotation) for all accounts associated with affected users. Remove malicious mod files and scan with updated AV/EDR signatures. Disable or remove Java Runtime Environment on endpoints where it is not business-required (NIST CM control family; CIS 2.3 unauthorized software removal).

NIST Phase: Eradication

Reference: NIST 800-61r3 §3.4 — Eradication

Controls: NIST AC-2 (Account Management), NIST CM-7 (Least Functionality), NIST CM-11 (User-Installed Software), NIST SI-2 (Flaw Remediation), CIS 2.3 (Address Unauthorized Software), CIS 5.3 (Disable Dormant

Accounts), CIS 5.4 (Restrict Administrator Privileges to Dedicated Administrator Accounts)

Compensating: For credential revocation without an enterprise IdP dashboard: (1) Force-invalidate all active browser sessions by navigating to each affected SaaS provider's security settings and revoking all active sessions (Google: myaccount.google.com/security → 'Manage all devices'; Microsoft: mysignins.microsoft.com). (2) To identify and remove WeedHack mod files specifically: scan `%APPDATA%\.minecraft\mods\` and the user's Downloads folder with ClamAV using an updated signature database (`clamscan -r --remove=yes %APPDATA%\.minecraft\mods\`). (3) Disable JRE on non-business endpoints via: `wmic product where "name like 'Java%'" call uninstall` or GPO Software Restriction Policy targeting java.exe and javaw.exe.

Evidence: Before wiping the endpoint, image the `%APPDATA%\.minecraft\mods\` directory and compute SHA-256 hashes of all .jar files present — these are your primary malware samples for AV submission and IOC extraction. Export the Windows Security Event Log filtering for Event ID 4663 (Object Access) on `Login Data` and `Cookies` SQLite files to establish exactly which accounts' credentials were accessed and when. Capture a memory image (WinPmem or Magnet RAM Capture) if the infection is active, to extract in-memory credential buffers or C2 communication state before process termination.

Step 4: Recovery — Validate that rotated credentials are active and old sessions are invalidated across all corporate systems. Confirm MFA enrollment is in place for all affected accounts before restoring normal access (CIS 6.3, CIS 6.5; NIST AC-7). Monitor AU-6 audit logs for 30 days post-remediation for any residual beaconing or anomalous login patterns. Apply D3-MFA to all externally exposed applications the affected user could access. Verify no persistence mechanisms (scheduled tasks, registry run keys) remain on remediated endpoints.

NIST Phase: Recovery

Reference: NIST 800-61r3 §3.5 — Recovery

Controls: NIST AC-7 (Unsuccessful Logon Attempts), NIST AC-17 (Remote Access), NIST AU-6 (Audit Record Review, Analysis, and Reporting), NIST AU-11 (Audit Record Retention), CIS 6.3 (Require MFA for Externally-Exposed Applications), CIS 6.5 (Require MFA for Administrative Access)

Compensating: Without an enterprise SIEM for 30-day monitoring: configure Windows Event Forwarding (WEF) to a central Windows Event Collector to aggregate Security Event ID 4624 (Successful Logon) and 4648 (Explicit Credential Use) from remediated endpoints. Use a free Sigma rule converted to a PowerShell scheduled task that runs nightly, parsing the forwarded event logs for logons from new geolocations or outside business hours for the affected user accounts. For persistence verification, run Sysinternals Autoruns with the `/accepteula /a /c` flags to export a baseline of all autorun locations and diff against a known-clean reference from an unaffected peer endpoint.

Evidence: Before returning the endpoint to service, collect: output of `schtasks /query /fo LIST /v > schtasks_output.txt` to document all scheduled tasks and identify any WeedHack-planted persistence (look for tasks executing .jar files or PowerShell from Temp/AppData paths); a full export of `HKCU\Software\Microsoft\Windows\CurrentVersion\Run` and `HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Run` registry keys; and IdP/SSO audit logs covering the full infection window (January 2026 to present) for the affected user, specifically filtering for impossible-travel login events or API token issuances that may indicate harvested session cookies were already used against corporate resources.

Step 5: Post-Incident — This campaign exploits credential reuse between personal and corporate devices — a control gap CIS 5.2 (Unique Passwords) and CIS 6.3 (MFA for externally exposed applications) directly address. Conduct a review of BYOD and personal device policies (NIST AC-19, AC-20). Evaluate whether corporate credential vaults or SSO providers show any access anomalies from the infection window (January 2026 onward). Brief employees on SEO poisoning and social engineering lures targeting gaming communities (NIST AT-2 awareness training). Consider D3-CH (Credential Hardening) controls such as hardware security keys for high-privilege accounts.

NIST Phase: Post Incident

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

Controls: NIST AC-19 (Access Control for Mobile Devices), NIST AC-20 (Use of External Systems), NIST AT-2 (Literacy Training and Awareness), NIST IR-4 (Incident Handling), NIST RA-3 (Risk Assessment), CIS 5.2 (Use Unique Passwords), CIS 6.3 (Require MFA for Externally-Exposed Applications), CIS 6.5 (Require MFA for Administrative Access)

Compensating: For awareness training without an LMS: produce a one-page internal advisory specifically describing the WeedHack YouTube-to-Mediafire/MEGA lure chain, with screenshots of the social engineering pattern (gaming mod promised in video description linking to an external file host), and distribute via email with a mandatory read-receipt. For BYOD policy enforcement without MDM: add a clause to acceptable-use policy requiring employees to attest that personal devices used to access corporate resources do not have unauthorized gaming mods or software installed, and use this incident as the documented basis for that policy update per NIST AC-20.

Evidence: For the lessons-learned record, assemble: a timeline of the infection window correlated against SSO/IdP access logs to determine whether any corporate account was accessed using credentials harvested by WeedHack during January 2026 onward (this is your breach scope determination artifact); a list of all affected users cross-referenced against their corporate application access entitlements to assess data exposure; and the SHA-256 hashes and file paths of all malicious .jar mod files recovered, submitted to VirusTotal and your AV vendor for signature development and shared with sector ISACs if applicable.

Detection Guidance

Primary behavioral indicators: (1) Non-browser processes reading from browser credential store paths, such as Windows paths %APPDATA%\Local\Google\Chrome\User Data\Default\Login Data or equivalent Firefox/Edge paths. (2) Java processes (javaw.exe, java.exe) spawning cmd.exe, PowerShell, or network connections to external IPs not associated with Mojang/Microsoft infrastructure. (3) Outbound HTTPS connections to newly registered or low-reputation domains from endpoints with Minecraft installed (T1071.001). (4) Access to Discord, Steam, or Telegram local data directories by processes other than those applications. (5) .jar or .zip files downloaded via browser to non-standard paths and immediately executed. SIEM query focus: correlate file download events with immediate process execution and subsequent credential store access within a short time window. Apply D3-SFA (System File Analysis) logic to flag reads of authentication databases outside normal application context. D3-LAM (Local Account Monitoring): alert on new local account creation or privilege escalation on endpoints following .jar execution. IOC enrichment: cross-reference outbound IPs and domains against threat intel feeds. Specific C2 infrastructure IOCs should be sourced from the full BleepingComputer technical report; request details from the threat source analyst before operational deployment.

Indicators of Compromise

Type	Value	Context	Confidence
URL	`YouTube video description links pointing to external mod file hosting`	Distribution vector — trojanized Minecraft mod files promoted via YouTube video descriptions using SEO poisoning; specific URLs not confirmed in available sources	LOW

Framework Mappings

MITRE-ATTACK

- **T1583.006** — Web Services

- **T1056.001** — Keylogging
- **T1598** — Phishing for Information
- **T1608.006** — SEO Poisoning
- **T1555.003** — Credentials from Web Browsers
- **T1204.002** — Malicious File
- **T1566** — Phishing
- **T1608.004** — Drive-by Target
- **T1021** — Remote Services
- **T1539** — Steal Web Session Cookie
- **T1071.001** — Web Protocols
- **T1113** — Screen Capture

NIST-800-53R5

- **AT-2** — Literacy Training and Awareness
- **CA-7** — Continuous Monitoring
- **SC-7** — Boundary Protection
- **SI-3** — Malicious Code Protection
- **SI-4** — System Monitoring
- **SI-8** — Spam Protection
- **AC-17** — Remote Access
- **AC-3** — Access Enforcement
- **CM-7** — Least Functionality
- **IA-2** — Identification and Authentication (Organizational Users)
- **SI-7** — Software, Firmware, and Information Integrity
- **CM-3** — Configuration Change Control

OWASP-TOP10-2021

- **A08:2021** — Software and Data Integrity Failures
- **A07:2021** — Identification and Authentication Failures

CIS-V8

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

HIPAA-SECURITY

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

SOC2-TSC

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

ISO-27001-2022

- **A.8.8** — Management of technical vulnerabilities

MITRE ATT&CK Mapping

Technique ID	Technique Name	Tactic
T1583.006	Web Services	Resource-Development
T1056.001	Keylogging	Collection
T1598	Phishing for Information	Reconnaissance
T1608.006	SEO Poisoning	Resource-Development
T1555.003	Credentials from Web Browsers	Credential-Access
T1204.002	Malicious File	Execution
T1566	Phishing	Initial-Access
T1608.004	Drive-by Target	Resource-Development
T1021	Remote Services	Lateral-Movement
T1539	Steal Web Session Cookie	Credential-Access
T1071.001	Web Protocols	Command-And-Control
T1113	Screen Capture	Collection

Sources

Source	URL	Tier
Security News	https://www.bleepingcomputer.com/news/security/over-116-000-mincraf...	T3
News in Minecraft 1.21.10 Release Candidate 1! - YouTube	https://www.youtube.com/watch?v=v7Mh6kj828k	T3
Minecraft 1.21.10 Release Candidate 1	https://www.minecraft.net/en-us/article/minecraft-1-21-10-release-c...	T3
All the News in the Minecraft 1.21.10 Hotfix! - YouTube	https://www.youtube.com/watch?v=IwOBOQydWD0	T3
ISSUES WITH 1.21.9 UPDATE · Issue #711 · PepperCode1/Continuity	https://github.com/PepperCode1/Continuity/issues/711	T3

DISCLAIMER

This intelligence report is produced by Tech Jacks Solutions Security Command Center (SCC) for informational purposes only. It does not constitute professional security advice, legal counsel, or an incident response engagement. The information herein is derived from publicly available sources and AI-assisted analysis; while every effort is made to ensure accuracy, Tech Jacks Solutions makes no warranties regarding completeness or timeliness. Organizations should conduct their own validation and consult qualified security professionals before taking action based on this report. Tech Jacks Solutions is not liable for any damages resulting from the use of this information.

Generated 2026-06-03 06:52 UTC by TJS Security Command Center