INTELLIGENCE BRIEFING
Security Command Center
TLP:CLEAR
2026-06-16 19:18 UTC

Steam Workshop Weaponized: Multi-Actor Campaign Turns Wallpaper Engine Into Malware Delivery Platform

THREAT CAMPAIGN | **HIGH** | CVSS 7.5

SCC Item ID	SCC-CAM-2026-0486
Type	Threat Campaign
Severity	HIGH
CVSS Base Score	7.5
Affected Products	Steam Workshop (Valve), Wallpaper Engine (Krzysztof Jedrzejewski / BEEFEATER Technology), Windows
Published	2026-06-16T14:27:55
Discovery Source	Rss

Executive Summary

Threat actors have abused Steam Workshop, Valve's user-content distribution platform, to deliver malware through Wallpaper Engine, a widely used Windows desktop customization application. Malicious packages disguised as wallpapers executed credential-stealing tools, ransomware, and cryptominers automatically upon installation, reaching a significant number of downloads before removal. Organizations face elevated risk where employees use personal gaming accounts on work devices or where Steam credentials overlap with corporate identity systems.

Technical Analysis

The campaign exploits Wallpaper Engine's legitimate 'application wallpaper' feature, which allows wallpaper packages to execute arbitrary binaries on the host system. This is not a software vulnerability, it is an abuse of documented, intended functionality (CWE-829: Inclusion of Functionality from Untrusted Control Sphere; CWE-693: Protection Mechanism Failure; CWE-494: Download of Code Without Integrity Check). No CVE has been assigned. Payload families observed include DarkKomet RAT (T1059, T1543), Lumma Stealer and Vidar Stealer (T1555, T1555.003, T1539), cryptominers (T1496), and ransomware (T1486). The delivery chain follows a trusted-platform abuse pattern: attacker uploads malicious package to Steam Workshop → user installs via Wallpaper Engine → application wallpaper feature executes embedded payload without additional user confirmation. MITRE ATT&CK techniques span initial access (T1195, T1195.002, T1566, T1204.002), execution (T1059, T1059.003), credential access (T1555, T1555.003, T1539, T1056), persistence (T1543), defense

evasion (T1553, T1036.005, T1574.002), and impact (T1486, T1496). The campaign is multi-actor; attribution is unresolved. Source quality is moderate (primary reporting from BleepingComputer). No vendor patch exists; the attack surface is the feature itself. Wallpaper Engine does not currently enforce code-signing or integrity verification on workshop package executables.

Action Checklist

1. Step 1: Containment, Identify all Windows endpoints where Wallpaper Engine (Steam App ID 431960) is installed. Evaluate disabling or removing the 'application wallpaper' feature on managed devices pending a formal policy decision. If Steam Workshop sync is active on any endpoint, isolate that device for triage. Block outbound Steam Workshop content download domains at the perimeter for managed assets where gaming software is unauthorized. Apply NIST AC-4 (Information Flow Enforcement) to restrict workshop content ingestion from unclassified external sources.
2. Step 2: Detection, Query EDR telemetry for processes spawned by Wallpaper Engine's runtime (wallpaper_engine.exe or wallpaper32.exe / wallpaper64.exe) that are not image rendering or audio processes. Look for child processes including cmd.exe, powershell.exe, wscript.exe, mshta.exe, or unknown binaries launched from %APPDATA%\Wallpaper Engine or Steam Workshop cache directories. Review Windows Event Log (Security event ID 4688, process creation with command line logging enabled) and Sysmon Event ID 1 for these parent-child relationships. Hunt for DarkKomet RAT indicators (persistent services, outbound IRC or custom C2 traffic), Lumma and Vidar Stealer indicators (browser credential store access, exfil to known stealer C2s), and cryptominer indicators (sustained high CPU on wallpaper_engine child processes). Apply NIST AU-6 (Audit Record Review, Analysis, and Reporting) and AU-12 (Audit Record Generation) to ensure process creation logging is active across affected endpoints. CIS 8.2 (Collect Audit Logs) should be validated as enabled.
3. Step 3: Eradication, Remove Wallpaper Engine from all managed endpoints where it is not business-justified. If removal is not immediately possible, disable the application wallpaper feature type in Wallpaper Engine settings (restrict to video/web/scene types only, which do not execute arbitrary binaries). Unsubscribe from all Steam Workshop packages on affected accounts and delete cached workshop content from disk. On any endpoint where malicious execution is confirmed: terminate and quarantine identified payload processes, remove persistence mechanisms (scheduled tasks, registry run keys, installed services added by payloads), rotate all credentials stored in browsers on that device. Apply D3-CRO (Credential Rotation) and D3-UAP (User Account Permissions) immediately for affected users.
4. Step 4: Recovery, After remediation, validate that no payload persistence remains by re-scanning with EDR and running a second-pass review of startup items (NIST SI-4 equivalent; D3-SICA, System Init Config Analysis). Confirm browser credential stores have been cleared and users have rotated passwords for accounts accessed from affected endpoints. Monitor outbound network traffic from remediated endpoints for 14 days for signs of lingering C2 communication. Verify audit logging continuity was not disrupted during the infection period (NIST AU-5, Response to Audit Logging Process Failures). Re-image endpoints where full remediation confidence cannot be established.
5. Step 5: Post-Incident, This campaign exposes a control gap in personal software governance on managed or BYOD endpoints. Conduct a policy review under NIST AC-20 (Use of External Systems) to address personal gaming platforms on corporate assets. Implement application allowlisting or execution control to prevent unapproved software from launching child processes (CIS 2.3, Address Unauthorized Software). Evaluate whether credential isolation controls (NIST AC-5, Separation of Duties; AC-6, Least Privilege) prevent personal account credentials from overlapping with corporate identity. Brief users on

trusted-platform abuse patterns, content from legitimate storefronts is not automatically safe. Update the acceptable use policy to explicitly address gaming clients and workshop/mod content on work devices.

IR / Forensic Enrichment

Triage Priority	URGENT
Escalation Criteria	Escalate to CISO and legal counsel immediately if forensic analysis confirms Lumma or Vidar Stealer successfully exfiltrated browser credential stores or session cookies from endpoints where users accessed corporate SaaS applications or stored PII, triggering breach notification obligations under applicable state privacy laws or GDPR Article 33.
Recovery Notes	After eradication, prioritize re-imaging over in-place remediation for any endpoint where DarkKomet RAT persistence is confirmed, as RAT implants may have deployed secondary backdoors or modified system binaries not detectable by signature scans alone. Monitor remediated endpoints for 14 days using outbound traffic analysis focused on IRC ports (6667/6697), sustained HTTPS POST to low-reputation or newly registered domains, and anomalous CPU utilization consistent with residual cryptomining processes. Verify that all user credentials accessed from affected endpoints — including corporate SSO, email, and SaaS applications — have been rotated and that active session tokens have been invalidated, as Lumma and Vidar are known to harvest cookies enabling session hijacking independent of password rotation.
Forensic Artifacts	Steam Workshop content cache directory at %LOCALAPPDATA%\Steam\steamapps\workshop\content\431960\ — contains the malicious wallpaper packages as delivered; PE binaries, scripts, or HTA files within subdirectories are primary payload artifacts specific to this campaign's delivery mechanism. | Windows Security Event Log Event ID 4688 and Sysmon Event ID 1 records with ParentImage matching wallpaper_engine.exe, wallpaper32.exe, or wallpaper64.exe — documents the exact process chain from Wallpaper Engine runtime to credential-stealer or RAT execution, which is the defining forensic signature of this attack vector. | Browser credential SQLite databases (Chrome/Edge: %LOCALAPPDATA%\Google\Chrome\User Data\Default\Login Data; Firefox: %APPDATA%\Mozilla\Firefox\Profiles*.default\logins.json) — access timestamps and process handle records (Sysmon Event ID 10) will show whether Lumma or Vidar accessed these stores from a non-browser process spawned within the Workshop content directory. | Windows Registry Run keys (HKCU\Software\Microsoft\Windows\CurrentVersion\Run and HKLM equivalent) and Scheduled Tasks exported via `schtasks /query /fo XML` — DarkKomet RAT and cryptominer payloads delivered through this campaign establish persistence via these mechanisms, and artifact timestamps will correlate to the Workshop package installation window. | Network capture or Sysmon Event ID 3 logs filtered for outbound connections on TCP 6667/6697 (DarkKomet IRC C2) and HTTPS POST traffic to domains registered within 30 days of the incident (Lumma/Vidar C2 infrastructure) originating from wallpaper_engine.exe child process PIDs — these network artifacts tie the host-level execution directly to confirmed C2 communication for this specific malware family cluster.

Per-Action IR Details

Step 1: Containment — Identify all Windows endpoints where Wallpaper Engine (Steam App ID 431960) is installed. Suspend use of the 'application wallpaper' feature immediately on managed devices. If Steam Workshop sync is active on any endpoint, isolate that device for triage. Block outbound Steam Workshop content download domains at the perimeter for managed assets where gaming software is unauthorized. Apply NIST AC-4 (Information Flow Enforcement) to restrict workshop content ingestion from unclassified

external sources.

NIST Phase: Containment

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

Controls: NIST AC-4 (Information Flow Enforcement), CIS 4.4 (Implement and Manage a Firewall on Servers), CIS 4.5 (Implement and Manage a Firewall on End-User Devices)

Compensating: Use PowerShell inventory across managed endpoints: `Get-ItemProperty HKLM:\Software\Microsoft\Windows\CurrentVersion\Uninstall\* | Where-Object {$_.DisplayName -like '*Wallpaper Engine*'}`. Block Steam Workshop CDN domains (steamuserimages-a.akamaihd.net, steamworkshopdownloader.io, and *.steampowered.com/workshop) via Windows Firewall GPO or pfSense/OPNsense ACL rules. For host isolation on a budget, use the Windows Firewall `netsh advfirewall set allprofiles firewallpolicy blockinbound,blockoutbound` to sever Workshop sync before triage begins.

Evidence: Before isolating any endpoint with active Wallpaper Engine sync, capture: full RAM image using WinPmem or Magnet RAM Capture to preserve in-memory C2 beacons or injected shellcode from Workshop payloads; run `netstat -ano` and `Get-NetTCPConnection` to document live outbound connections from wallpaper_engine.exe or its child processes; export the Steam Workshop subscription cache manifest at `%LOCALAPPDATA%\Steam\steamapps\workshop\` and log active process list with parent-child relationships via `wmic process get ProcessId,ParentProcessId,Name,CommandLine`. These artifacts are destroyed the moment network isolation or process termination occurs.

Step 2: Detection — Query EDR telemetry for processes spawned by Wallpaper Engine's runtime (wallpaper_engine.exe or wallpaper32.exe / wallpaper64.exe) that are not image rendering or audio processes. Look for child processes including cmd.exe, powershell.exe, wscript.exe, mshta.exe, or unknown binaries launched from %APPDATA%\Wallpaper Engine or Steam Workshop cache directories. Review Windows Event Log (Security event ID 4688 — process creation with command line logging enabled) and Sysmon Event ID 1 for these parent-child relationships. Hunt for DarkKomet RAT indicators (persistent services, outbound IRC or custom C2 traffic), Lumma and Vidar Stealer indicators (browser credential store access, exfil to known stealer C2s), and cryptominer indicators (sustained high CPU on wallpaper_engine child processes). Apply NIST AU-6 (Audit Record Review, Analysis, and Reporting) and AU-12 (Audit Record Generation) to ensure process creation logging is active across affected endpoints. CIS 8.2 (Collect Audit Logs) should be validated as enabled.

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), CIS 8.2 (Collect Audit Logs)

Compensating: Deploy Sysmon with SwiftOnSecurity config to capture Event ID 1 (process create) and Event ID 3 (network connect) filtering on parent image paths containing `wallpaper_engine.exe`, `wallpaper32.exe`, or `wallpaper64.exe`. Use this PowerShell query against Windows Security logs: `Get-WinEvent -LogName Security | Where-Object {$_.Id -eq 4688 -and $_.Message -match 'wallpaper'}`. For Lumma/Vidar browser credential access, monitor Sysmon Event ID 10 (process access) for any wallpaper_engine child process opening handles to `Login Data` or `Cookies` files under Chrome/Edge/Firefox profile directories. Use Wireshark with display filter `tcp.port == 6667 || tcp.port == 6697` to catch DarkKomet IRC C2 traffic in real time.

Evidence: All detection steps are read-only and do not alter live state — no volatile pre-capture is required before querying logs or EDR telemetry. However, if active C2 communication is confirmed during analysis (live IRC connection or active Lumma exfil session), immediately snapshot RAM and `netstat -ano` output before any blocking action. Key artifacts to examine: Windows Security Event ID 4688 with `ParentProcessName` matching wallpaper_engine runtime paths; Sysmon Event ID 1 command-line arguments for scripts launched from `%LOCALAPPDATA%\Steam\steamapps\workshop\content\431960\`; browser SQLite `Login Data` files for timestamp anomalies indicating unauthorized access by a non-browser process; `%APPDATA%\Microsoft\Windows\Recent` LNK files pointing to Workshop payload directories.

Step 3: Eradication — Remove Wallpaper Engine from all managed endpoints where it is not business-justified. If removal is not immediately possible, disable the application wallpaper feature type in Wallpaper Engine settings (restrict to video/web/scene types only, which do not execute arbitrary binaries). Unsubscribe from all Steam Workshop packages on affected accounts and delete cached workshop content from disk. On any endpoint where malicious execution is confirmed: terminate and quarantine identified payload processes, remove persistence mechanisms (scheduled tasks, registry run keys, installed services added by payloads), rotate all credentials stored in browsers on that device. Apply D3-CRO (Credential Rotation) and D3-UAP (User Account Permissions) immediately for affected users.

NIST Phase: Eradication

Reference: NIST 800-61r3 §3.4 — Eradication

Controls: NIST AC-6 (Least Privilege), CIS 2.3 (Address Unauthorized Software), CIS 5.1 (Establish and Maintain an Inventory of Accounts)

Compensating: Use `schtasks /query /fo LIST /v | findstr /i "wallpaper\|steam"` and `Get-ScheduledTask | Where-Object {$_.TaskPath -match 'wallpaper|steam'}` to enumerate persistence via scheduled tasks. Query Run/RunOnce keys: `reg query HKCU\Software\Microsoft\Windows\CurrentVersion\Run` and `HKLM` equivalent, filtering for Steam or Workshop paths. Delete Workshop content cache directory `%LOCALAPPDATA%\Steam\steamapps\workshop\content\431960\` after hashing and preserving a forensic copy. For credential rotation without enterprise tooling, force browser password store invalidation by deleting `Login Data` and `Cookies` from all Chromium-based profile directories after notifying users to reset passwords via an out-of-band channel (phone or secondary email).

Evidence: CRITICAL — volatile capture is mandatory before terminating any confirmed malicious process. Acquire RAM image before killing DarkKomet, Lumma, or Vidar processes to preserve in-memory decryption keys and C2 configuration. Run `netstat -ano` and map PIDs to processes via `tasklist /svc` before process termination. Export the full registry hive `HKCU\Software\Microsoft\Windows\CurrentVersion\Run` and `HKLM\SYSTEM\CurrentControlSet\Services` before removing persistence entries. Preserve a forensic copy of Workshop content directories under `%LOCALAPPDATA%\Steam\steamapps\workshop\content\431960\` including all PE binaries and scripts before deletion. Hash all collected artifacts with SHA-256 before eradication proceeds.

Step 4: Recovery — After remediation, validate that no payload persistence remains by re-scanning with EDR and running a second-pass review of startup items (NIST SI-4 equivalent; D3-SICA — System Init Config Analysis). Confirm browser credential stores have been cleared and users have rotated passwords for accounts accessed from affected endpoints. Monitor outbound network traffic from remediated endpoints for 14 days for signs of lingering C2 communication. Verify audit logging continuity was not disrupted during the infection period (NIST AU-5 — Response to Audit Logging Process Failures). Re-image endpoints where full remediation confidence cannot be established.

NIST Phase: Recovery

Reference: NIST 800-61r3 §3.5 — Recovery

Controls: NIST AU-5 (Response To Audit Logging Process Failures), NIST AU-9 (Protection Of Audit Information), CIS 4.6 (Securely Manage Enterprise Assets and Software)

Compensating: Without EDR, use Autoruns (Sysinternals) configured to check VirusTotal hashes — scan all startup locations including scheduled tasks, services, and browser extensions for residual Workshop payload artifacts under Steam-related paths. For 14-day C2 monitoring without a SIEM, deploy a Zeek or Suricata instance on the network segment with rules triggering on outbound IRC (port 6667/6697), connections to known Lumma and Vidar C2 IP ranges (pull current IOCs from abuse.ch URLhaus), and sustained outbound HTTPS to newly registered domains from wallpaper_engine process descendants. Validate audit log continuity by checking the earliest event timestamp in Security and Sysmon logs post-infection — a gap indicates potential log tampering by the payload.

Evidence: Recovery actions (reimaging, credential store clearing) alter live state — before reimaging a confirmed-compromised endpoint, ensure full RAM capture, disk image (using FTK Imager or `dd`), and browser artifact copies (`Login Data`, `Cookies`, browser history DBs) have been preserved for post-incident forensics. Verify the integrity of audit logs collected during the infection window: check AU-9 protections were intact and that Security

Event Log records are contiguous (no gaps in Event Record IDs that would indicate log clearing by a DarkKomet or stealer payload). Post-recovery, monitor Sysmon Event ID 3 (network connection) for outbound traffic to Steam Workshop CDN domains or IRC ports from any process other than a legitimately reinstalled Steam client.

Step 5: Post-Incident — This campaign exposes a control gap in personal software governance on managed or BYOD endpoints. Conduct a policy review under NIST AC-20 (Use of External Systems) to address personal gaming platforms on corporate assets. Implement application allowlisting or execution control to prevent unapproved software from launching child processes (CIS 2.3 — Address Unauthorized Software). Evaluate whether credential isolation controls (NIST AC-5 — Separation of Duties; AC-6 — Least Privilege) prevent personal account credentials from overlapping with corporate identity. Brief users on trusted-platform abuse patterns — content from legitimate storefronts is not automatically safe. Update the acceptable use policy to explicitly address gaming clients and workshop/mod content on work devices.

NIST Phase: Post Incident

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

Controls: NIST AC-20 (Use Of External Systems), NIST AC-5 (Separation Of Duties), NIST AC-6 (Least Privilege), CIS 2.1 (Establish and Maintain a Software Inventory), CIS 2.2 (Ensure Authorized Software is Currently Supported), CIS 2.3 (Address Unauthorized Software)

Compensating: For application execution control without an enterprise solution, deploy Windows Software Restriction Policies (SRP) or AppLocker rules blocking execution from `%LOCALAPPDATA%\Steam\steamapps\workshop\` and `%APPDATA%\Wallpaper Engine\` directories. Author a YARA rule targeting Wallpaper Engine child-process execution patterns and schedule nightly scans via ClamAV with the custom rule on managed endpoints. For user awareness, prepare a one-page brief with sanitized IOCs from this campaign — specifically the trusted-platform abuse pattern where Steam Workshop served as the delivery vector — to counter the assumption that Valve-hosted content is inherently safe.

Evidence: No volatile evidence capture is required for post-incident policy and procedural actions, as these steps do not alter live system state on compromised hosts. However, the lessons-learned process should incorporate the forensic artifacts collected during the incident: specifically, the process tree showing wallpaper_engine.exe spawning credential-stealing child processes, and the Workshop content package metadata (Steam package IDs, subscriber counts, upload timestamps) to document the blast radius and inform the policy gap analysis. Preserve all IOC lists, affected endpoint inventories, and timeline reconstructions for regulatory reporting if PII was exfiltrated by Lumma or Vidar stealers.

Detection Guidance

Primary detection target: Wallpaper Engine runtime processes spawning unexpected child processes. In Sysmon or EDR, alert on Event ID 1 (process creation) where ParentImage matches wallpaper_engine.exe, wallpaper32.exe, or wallpaper64.exe and ChildImage is cmd.exe, powershell.exe, wscript.exe, mshta.exe, certutil.exe, or any binary executing from %APPDATA%, %TEMP%, or Steam Workshop cache paths (typically C:\Program Files (x86)\Steam\steamapps\workshop\content\431960\). Secondary detection: monitor for DarkKomet RAT behavioral indicators, persistent registry entries associated with DarkKomet RAT persistence, and outbound connections on non-standard ports. For Lumma and Vidar Stealer: watch for reads against browser credential stores (Login Data, Cookies files under Chrome/Edge/Firefox profiles) by non-browser processes, followed by outbound HTTPS to newly registered or low-reputation domains. For cryptominers: sustained CPU utilization from Wallpaper Engine child processes with no corresponding render activity. For ransomware: mass file rename or extension change events originating from Wallpaper Engine process tree. Windows Security Event ID 4688 with command line auditing enabled is the minimum logging baseline required; Sysmon with process creation and network connection logging is preferred. Apply D3-SFA (System File Analysis) for monitoring of browser credential stores and startup configuration changes. D3-LAM (Local Account

Monitoring) should be active to detect new local accounts or privilege escalation following initial compromise.

Indicators of Compromise

Type	Value	Context	Confidence
URL	`https://steamcommunity.com/workshop/about/?appid=431960`	Steam Workshop hub for Wallpaper Engine — source of malicious package distribution; monitor for new subscriptions from managed endpoints	LOW

Framework Mappings

MITRE-ATTACK

- **T1555** — Credentials from Password Stores
- **T1496** — Resource Hijacking
- **T1566** — Phishing
- **T1059** — Command and Scripting Interpreter
- **T1539** — Steal Web Session Cookie
- **T1486** — Data Encrypted for Impact
- **T1204.002** — Malicious File
- **T1574.002** — DLL Side-Loading
- **T1056** — Input Capture
- **T1059.003** — Windows Command Shell
- **T1195** — Supply Chain Compromise
- **T1553** — Subvert Trust Controls
- **T1195.002** — Compromise Software Supply Chain
- **T1543** — Create or Modify System Process
- **T1555.003** — Credentials from Web Browsers
- **T1036.005** — Match Legitimate Resource Name or Location

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
- **CM-7** — Least Functionality
- **SI-7** — Software, Firmware, and Information Integrity
- **CP-9** — System Backup

- **CP-10** — System Recovery and Reconstitution
- **SA-9** — External System Services
- **SR-2** — Supply Chain Risk Management Plan
- **SR-3** — Supply Chain Controls and Processes
- **CM-3** — Configuration Change Control
- **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

NIST-CSF-2

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

HIPAA-SECURITY

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

ISO-27001-2022

- **A.5.29** — Information security during disruption
- **A.8.8** — Management of technical vulnerabilities

SOC2-TSC

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

MITRE ATT&CK Mapping

Technique ID	Technique Name	Tactic
T1555	Credentials from Password Stores	Credential-Access
T1496	Resource Hijacking	Impact
T1566	Phishing	Initial-Access
T1059	Command and Scripting Interpreter	Execution
T1539	Steal Web Session Cookie	Credential-Access
T1486	Data Encrypted for Impact	Impact
T1204.002	Malicious File	Execution

Technique ID	Technique Name	Tactic
T1574.002	DLL Side-Loading	Persistence
T1056	Input Capture	Collection
T1059.003	Windows Command Shell	Execution
T1195	Supply Chain Compromise	Initial-Access
T1553	Subvert Trust Controls	Defense-Evasion
T1195.002	Compromise Software Supply Chain	Initial-Access
T1543	Create or Modify System Process	Persistence
T1555.003	Credentials from Web Browsers	Credential-Access
T1036.005	Match Legitimate Resource Name or Location	Defense-Evasion

Sources

Source	URL	Tier
Security News	https://www.bleepingcomputer.com/news/security/steam-workshop-abuse...	T3
If you use Wallpaper Engine on Steam, feel free to check out my ...	https://www.facebook.com/groups/5279785325430642/posts/886134806394...	T3
The Steam Workshop for Wallpaper Engine	https://steamcommunity.com/workshop/about/?appid=431960	T3
Coaxed into Wallpaper Engine's steam workshop : r/coaxedintoasnafu	https://www.reddit.com/r/coaxedintoasnafu/comments/1lkr7vu/coaxed_i...	T3
Steam Community :: Wallpaper Engine - Pinterest	https://www.pinterest.com/pin/627689266813159078/	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 2026-06-16 19:18 UTC by TJS Security Command Center