INTELLIGENCE BRIEFING
Security Command Center
TLP:CLEAR
2026-07-02 07:12 UTC

SEO Poisoning and Signed Binary DLL Side-Loading Drive Global AsyncRAT Distribution Campaign

THREAT CAMPAIGN | **HIGH** | CVSS 7.5

SCC Item ID	SCC-CAM-2026-0610
Type	Threat Campaign
Severity	HIGH
CVSS Base Score	7.5
Affected Products	Windows (targeted platform); users of spoofed software installers impersonating OBS Studio, Bandicam, DS4Windows, DNS Jumper, ScreenConnect (ConnectWise); Microsoft Defender (tampered with via UAC bypass)
Published	2026-07-01T13:53:06
Discovery Source	Rss

Executive Summary

An active, multi-stage campaign is distributing AsyncRAT malware globally by poisoning search engine results to surface fake download sites impersonating widely used Windows software tools including OBS Studio, Bandicam, and ScreenConnect. Victims who download trojanized installers receive a full remote-access implant that gives attackers persistent, privileged control over infected machines, with Defender tampered to suppress detection. Any organization whose employees download software from the internet faces exposure; the infrastructure has been active since at least August 2025 across 90 or more domains, indicating a sustained, well-resourced operation, according to reporting from Securelist.

Technical Analysis

According to Securelist (T1 source), this campaign uses SEO poisoning (MITRE T1608.006) to rank malicious installer pages above legitimate software download sites, targeting users across 10 languages. Trojanized installers abuse DLL side-loading (CWE-426, MITRE T1574.002) via a legitimate signed Microsoft binary to load a malicious DLL without triggering standard signing checks. Initial access established, the installer deploys a ScreenConnect (ConnectWise) remote access client for persistence (MITRE T1219), then injects AsyncRAT via process hollowing (CWE-494, MITRE T1055.012) into a running process. The chain includes: UAC bypass (MITRE T1548.002) for privilege escalation; Microsoft Defender tampering (MITRE T1562.001); obfuscated payloads (MITRE T1027); PowerShell and script-based execution (MITRE T1059, T1059.001, T1059.005);

scheduled task persistence (MITRE T1053.005); and C2 over standard application protocols (MITRE T1071). Infrastructure spans 90-plus domains registered as part of a broader acquisition campaign (MITRE T1583.001). Spoofed software includes OBS Studio, Bandicam, DS4Windows, DNS Jumper, and ScreenConnect. No CVE is assigned to this campaign. CWE-601 (open redirect) is listed in the item data, consistent with redirect chains used to funnel victims from poisoned search results to payload delivery sites. Attribution is open as of 2026-03-04. Source quality score is 0.64 and independent corroboration from CISA or NVD is not confirmed; all claims below are attributed to Securelist and The Hacker News reporting.

Action Checklist

1. Step 1: Containment, Block known malicious domains associated with this campaign at your DNS resolver and web proxy. According to Securelist reporting, the infrastructure spans 90-plus domains; retrieve the IOC list from the Securelist article (https://securelist.com/tr/the-soc-files-screenconnect-campaign-with-asyncrat/120472/) and push domain and IP blocklists to DNS filtering, NGFW, and proxy deny-lists immediately. Isolate any endpoint where a trojanized installer from a spoofed software site was executed.
2. Step 2: Detection, Query endpoint detection logs for: (a) DLL side-loading events where a signed Microsoft binary loads an unsigned or anomalously named DLL from a user-writable path; (b) ScreenConnect client installations not provisioned through your standard software deployment process (NIST AU-2, CIS 8.2); (c) process hollowing indicators, parent-child process anomalies where a hollowed process has a mismatched memory-mapped image; (d) Scheduled task creation (Event ID 4698) by non-administrative users or from temp/download directories; (e) PowerShell or VBScript execution spawned from installer processes. Hunt for AsyncRAT C2 beacon patterns, look for regular outbound connections over non-standard ports to recently registered domains.
3. Step 3: Eradication, On confirmed infected hosts: terminate ScreenConnect client processes not provisioned by IT; remove associated scheduled tasks and registry run keys; delete malicious DLL and dropper files identified in threat intel; run a full AV/EDR scan with updated signatures after verifying Defender has not been tampered with (check Defender service state and policy exclusions, NIST SI-4, CIS 4.4). Re-image hosts where process hollowing or privilege escalation is confirmed rather than attempting manual cleanup.
4. Step 4: Recovery, After re-imaging or eradication: rotate credentials for any accounts that were active on the infected host (MITRE D3-CRO); verify Defender is enabled and no policy exclusions were added (NIST SI-4); confirm no unauthorized ScreenConnect tenants or persistent remote access sessions remain (CIS 5.1, CIS 6.2); restore the host from a known-good backup if available; monitor for re-infection indicators for at least 30 days post-remediation.
5. Step 5: Post-Incident, Review software download policies and enforce allowlisting so employees can only install software from approved repositories (CIS 2.1, CIS 2.3, NIST AC-3). Implement or audit application allowlisting to block unsigned or anomalously side-loaded DLLs (CIS 4.6). Enforce least privilege to limit UAC bypass impact (NIST AC-6, CIS 5.4). Evaluate DNS filtering coverage for newly registered domains. Conduct targeted user awareness training focused on software download hygiene, specifically the risk of searching for software and clicking top-ranked results.

IR / Forensic Enrichment

Triage Priority	IMMEDIATE
Escalation Criteria	Escalate immediately to senior IR leadership and legal/compliance if AsyncRAT persistence is confirmed on hosts processing PII, PHI, or financial data (triggering HIPAA Breach Notification Rule or state breach notification obligations), if the unauthorized ScreenConnect tenant is observed exfiltrating data to campaign C2 infrastructure, or if the team lacks capability to perform memory forensics on a host with confirmed process hollowing before reimaging.
Recovery Notes	Before returning any host to production, verify independently that Defender real-time protection is enabled with no exclusions, no unauthorized ScreenConnect tenant GUID exists in the Services registry, and no scheduled tasks or HKCU run keys matching campaign IOC patterns remain — do not rely solely on AV scan results given this campaign specifically tampers with Defender via UAC bypass. Monitor recovered hosts and DNS resolver logs for at least 30 days post-remediation for re-beacon attempts to the 90-plus campaign domains, as AsyncRAT implants have been observed re-establishing C2 after incomplete cleanup. Re-image any host where privilege escalation or process hollowing was confirmed rather than trusting manual eradication, as fileless or memory-resident components may survive artifact-level cleanup.
Forensic Artifacts	Sysmon Event ID 7 (Image Loaded) records showing a signed Microsoft binary (e.g., legitimate system DLL or executable) loading an unsigned DLL from %TEMP%, %APPDATA%, or %LOCALAPPDATA% — the primary forensic signature of the DLL side-loading delivery mechanism used by this campaign's trojanized OBS Studio, Bandicam, and DS4Windows installers. | Windows Security Event ID 4698 (Scheduled Task Created) log entries where the task action path or working directory resolves to a user-writable temp or download directory, created within the timeframe of the suspected trojanized installer execution — AsyncRAT uses scheduled tasks for persistence in this campaign. | Registry export of HKCU\SOFTWARE\ScreenConnect Client and HKLM\SYSTEM\CurrentControlSet\Services entries containing unauthorized ScreenConnect tenant GUIDs not provisioned by IT, alongside HKCU\Software\Microsoft\Windows\CurrentVersion\Run keys added by the dropper component. | Windows Defender configuration snapshot (output of Get-MpPreference and Get-MpComputerStatus) capturing ExclusionPath, ExclusionProcess, and DisableRealtimeMonitoring values set by the UAC bypass — this directly evidences the tamper technique and the scope of detection suppression during the compromise window. | DNS resolver query logs and proxy access logs showing outbound DNS resolution of spoofed software download domains (e.g., domains impersonating obs-project.com, bandicam.com, ds4windows.com, connectwise.com) and subsequent periodic beacon connections to AsyncRAT C2 infrastructure over non-standard ports, timestamped to establish the initial access and persistence timeline.

Per-Action IR Details

Step 1: Containment — Block known malicious domains associated with this campaign at your DNS resolver and web proxy. According to Securelist reporting, the infrastructure spans 90-plus domains; pull the IOC list from the Securelist article (https://securelist.com/tr/the-soc-files-screenconnect-campaign-with-asyncrat/120472/) and push domain and IP blocklists to DNS filtering, NGFW, and proxy deny-lists immediately. Isolate any endpoint where a trojanized installer from a spoofed software site was executed.

NIST Phase: Containment

Reference: NIST 800-61r3 §3.3 — Containment Strategy: Choose a containment strategy based on criteria such as potential damage, evidence preservation needs, service availability, time and resources required, and effectiveness.

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: Export the Securelist IOC domain list and push via Windows Hosts file or Pi-hole blocklist for DNS sinkholing on a 2-person team budget. At the NGFW, create a deny-all rule for the IP ranges cited in the IOC list using iptables or pfSense. For endpoint isolation without EDR, disable the NIC via `netsh interface set interface 'Ethernet' admin=disabled` or physically unplug; do NOT use graceful shutdown, which would overwrite volatile memory state.

Evidence: Before isolating any endpoint suspected of running a trojanized OBS Studio, Bandicam, DS4Windows, or ScreenConnect installer, capture: (1) full RAM image using WinPmem or Magnet RAM Capture to recover injected AsyncRAT payload from hollowed process memory; (2) live network connections via `netstat -ano` and `Get-NetTCPConnection` to document active AsyncRAT C2 sessions and the non-standard port in use; (3) running process list with parent-child relationships via `Get-Process` or `tasklist /v` to document the signed Microsoft binary performing DLL side-loading; (4) DNS cache via `ipconfig /displaydns` to capture the resolved campaign domain before isolation flushes it. Isolation destroys all of the above.

Step 2: Detection — Query endpoint detection logs for: (a) DLL side-loading events where a signed Microsoft binary loads an unsigned or anomalously named DLL from a user-writable path; (b) ScreenConnect client installations not provisioned through your standard software deployment process (NIST AU-2, CIS 8.2); (c) process hollowing indicators — parent-child process anomalies where a hollowed process has a mismatched memory-mapped image; (d) Scheduled task creation (Event ID 4698) by non-administrative users or from temp/download directories; (e) PowerShell or VBScript execution spawned from installer processes. Hunt for AsyncRAT C2 beacon patterns — look for regular outbound connections over non-standard ports to recently registered domains.

NIST Phase: Detection Analysis

Reference: NIST 800-61r3 §3.2 — Detection and Analysis: Analyze all available precursors and indicators, including network flows, host logs, and endpoint telemetry, and correlate across sources to establish scope and confirm incident criteria.

Controls: NIST AU-2 (Event Logging), NIST AU-6 (Audit Record Review, Analysis, And Reporting), CIS 8.2 (Collect Audit Logs)

Compensating: Without SIEM/EDR: (1) Deploy Sysmon with SwiftOnSecurity config and query Event ID 7 (ImageLoad) for DLLs loaded from %TEMP%, %APPDATA%, or %LOCALAPPDATA% by signed binaries — this directly captures the DLL side-loading vector used in this campaign. (2) Query Windows Security Event Log for Event ID 4698 (Scheduled Task Created) filtered on tasks created from paths containing 'Temp', 'Downloads', or 'AppData'. (3) Use Autoruns (Sysinternals) to surface ScreenConnect persistence entries not matching your approved deployment path. (4) Run the Sigma rule 'proc_creation_win_susp_dllhost_parent' and community Sigma rules for AsyncRAT C2 beacon detection against Sysmon logs using chainsaw or sigma-cli. (5) Use Wireshark with a display filter for DNS queries to domains registered within the past 30 days (correlate with WHOIS) combined with periodic outbound connections on ports outside 80/443.

Evidence: This is an analysis step that does not alter live system state; however, if investigation leads to discovery of an active ScreenConnect session or live AsyncRAT C2 connection during this step, immediately pivot to evidence capture before any action: save Sysmon Event ID 1 (Process Create) logs showing the spoofed installer spawning PowerShell or VBScript; export Windows Event ID 4688 (Process Creation) records for cmd.exe or wscript.exe with parent processes matching installer names (obs-studio-setup.exe, bandicam_setup.exe, ds4windows_setup.exe); capture the loaded DLL path and hash from Sysmon Event ID 7 records for the side-loaded unsigned DLL.

Step 3: Eradication — On confirmed infected hosts: terminate ScreenConnect client processes not provisioned by IT; remove associated scheduled tasks and registry run keys; delete malicious DLL and dropper files identified in threat intel; run a full AV/EDR scan with updated signatures after verifying Defender has not been tampered with (check Defender service state and policy exclusions, NIST SI-4, CIS 4.4). Re-image hosts where process hollowing or privilege escalation is confirmed rather than attempting manual

cleanup.

NIST Phase: Eradication

Reference: NIST 800-61r3 §3.4 — Eradication: After containing the incident, eradicate the threat by removing malware, disabling breached accounts, and mitigating exploited vulnerabilities; verify eradication is complete before moving to recovery.

Controls: CIS 4.4 (Implement and Manage a Firewall on Servers), CIS 2.3 (Address Unauthorized Software)

Compensating: Without EDR: (1) Use Autoruns (Sysinternals) with VirusTotal integration enabled to identify and delete the side-loaded malicious DLL and any registry run keys (HKCU\Software\Microsoft\Windows\CurrentVersion\Run) added by the dropper. (2) Use `schtasks /query /fo LIST /v` to enumerate all scheduled tasks and cross-reference against known-good baselines; delete anomalous tasks with `schtasks /delete /tn '' /f`. (3) Check Defender tamper status with `Get-MpPreference | Select-Object DisableRealtimeMonitoring, ExclusionPath, ExclusionProcess` in PowerShell — any exclusion path pointing to the AsyncRAT dropper or ScreenConnect directory added post-installation is a confirmed tamper indicator. (4) Re-enable Defender with `Set-MpPreference -DisableRealtimeMonitoring $false` and remove exclusions with `Remove-MpPreference -ExclusionPath "` before scanning. For hosts with confirmed process hollowing, reimage from a pre-campaign baseline (prior to the SEO poisoning campaign activity period).

Evidence: Before terminating ScreenConnect processes or deleting files, capture: (1) full memory image of the hollowed process (the signed Microsoft binary with mismatched memory-mapped image) using WinPmem — this is the only opportunity to recover the injected AsyncRAT payload from memory; (2) export current Defender exclusions list and policy state via `Get-MpPreference` output saved to file — this documents the UAC bypass tamper as forensic evidence; (3) copy the malicious DLL, dropper installer file, and any files in %TEMP% or %APPDATA% matching IOC hashes to a write-protected evidence container before deletion; (4) export the full scheduled task XML for anomalous tasks via `schtasks /query /xml` before deleting them; (5) save registry export of HKCU and HKLM run keys (`reg export HKCU\Software\Microsoft\Windows\CurrentVersion\Run evidence_hkcu_run.reg`) before removal.

Step 4: Recovery — After re-imaging or eradication: rotate credentials for any accounts that were active on the infected host (MITRE D3-CRO); verify Defender is enabled and no policy exclusions were added (NIST SI-4); confirm no unauthorized ScreenConnect tenants or persistent remote access sessions remain (CIS 5.1, CIS 6.2); restore the host from a known-good backup if available; monitor for re-infection indicators for at least 30 days post-remediation.

NIST Phase: Recovery

Reference: NIST 800-61r3 §3.5 — Recovery: Restore systems to normal operation, confirm systems are functioning normally, and implement additional monitoring to watch for re-infection or adversary re-entry after eradication.

Controls: NIST AC-2 (Account Management), CIS 5.1 (Establish and Maintain an Inventory of Accounts), CIS 6.2 (Establish an Access Revoking Process), NIST AC-12 (Session Termination)

Compensating: Without enterprise PAM or IDM: (1) Enumerate all ScreenConnect tenants installed on the recovered host by checking `HKLM\SOFTWARE\ScreenConnect Client` registry subtree and Services list for any tenant GUIDs not matching your IT-provisioned instance — remove unauthorized instances via `msiexec /x` with the correct product GUID. (2) Force credential rotation for all accounts logged into the infected host during the compromise window by querying Windows Security Event ID 4624 (Logon) for the infection timeframe and resetting those accounts in Active Directory. (3) Confirm Defender is fully operational with `Get-MpComputerStatus` and verify `RealTimeProtectionEnabled` is True and `AMServiceEnabled` is True before returning host to production. (4) Restore from a backup image dated prior to the first observed campaign IOC DNS query in your DNS resolver logs.

Evidence: Before rotating credentials or terminating remote sessions, document: (1) all active ScreenConnect session IDs and tenant GUIDs from the Services registry key and Windows Security Event ID 4624/4634 logs for the session audit trail; (2) export of all accounts with active sessions on the host during the compromise window from Security Event Log (Event IDs 4624, 4672) as evidence for the credential rotation scope decision; (3) current Defender configuration state snapshot via `Get-MpPreference` and `Get-MpComputerStatus` output to document the post-tamper baseline before remediation. Note: credential rotation itself does not destroy volatile evidence if performed on an already-isolated host, but session termination of any live ScreenConnect C2 session must be preceded by network traffic capture of that session via Wireshark to preserve C2 communication evidence.

Step 5: Post-Incident — Review software download policies and enforce allowlisting so employees can only install software from approved repositories (CIS 2.1, CIS 2.3, NIST AC-3). Implement or audit application allowlisting to block unsigned or anomalously side-loaded DLLs (CIS 4.6). Enforce least privilege to limit UAC bypass impact (NIST AC-6, CIS 5.4). Evaluate DNS filtering coverage for newly registered domains. Conduct targeted user awareness training focused on software download hygiene — specifically the risk of searching for software and clicking top-ranked results.

NIST Phase: Post Incident

Reference: NIST 800-61r3 §4 — Post-Incident Activity: Hold a lessons-learned meeting, update detection and prevention capabilities, and share threat intelligence to reduce recurrence and improve organizational resilience.

Controls: NIST AC-3 (Access Enforcement), NIST AC-6 (Least Privilege), 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 5.4 (Restrict Administrator Privileges to Dedicated Administrator Accounts), CIS 7.1 (Establish and Maintain a Vulnerability Management Process)

Compensating: Without enterprise application control tools: (1) Deploy Windows Software Restriction Policies (SRP) or AppLocker (available on Windows Pro/Enterprise at no additional cost) with a default-deny rule that blocks execution from %TEMP%, %APPDATA%, and %LOCALAPPDATA% — the exact paths this campaign's trojanized OBS Studio, Bandicam, and DS4Windows installers write to. (2) Enable Windows Defender Application Control (WDAC) policy in audit mode first to baseline legitimate side-loading, then enforce to block unsigned DLL loads from user-writable paths. (3) Configure DNS filtering using Quad9 (free, malicious domain blocking) or Pi-hole with a newly-registered-domain blocklist feed to catch future SEO poisoning campaign infrastructure. (4) Create a short internal advisory with screenshots of the spoofed OBS Studio and ScreenConnect download pages (sourced from the Securelist article) for user awareness training — specificity to real campaign pages is significantly more effective than generic phishing training.

Evidence: No live system state is altered in this phase; however, retain and archive all forensic evidence collected during containment, eradication, and recovery for a minimum retention period consistent with your incident records policy: (1) memory images and process dumps from infected hosts; (2) the full IOC list from the Securelist campaign report as the authoritative reference for your post-incident detection rule updates; (3) Sysmon and Windows Event Log exports covering the full compromise window; (4) documentation of the Defender tamper state (exclusions added, service disabled) as evidence of the UAC bypass impact for the lessons-learned report and for any regulatory notification assessment.

Detection Guidance

Detection priority: DLL side-loading via signed Microsoft binaries. Look for Microsoft-signed executables (e.g., binaries from System32 or Program Files) loading DLLs from user-writable directories (AppData, Temp, Downloads). Cross-reference with Sysmon Event ID 7 (Image Loaded) and filter for DLLs loaded by signed binaries where the DLL is unsigned or located outside expected system paths. Hunt for ScreenConnect installations not in your asset inventory (CIS 1.1), query endpoint telemetry for ScreenConnect agent processes and correlate against your authorized remote access tool list. For process hollowing (T1055.012): look for processes where the on-disk image hash does not match the in-memory image; EDR tools that support memory scanning should flag this. For Defender tampering (T1562.001): monitor Windows Security Center state changes, Defender exclusion modifications (Registry path: HKLM\SOFTWARE\Microsoft\Windows Defender\Exclusions), and Defender service stop/disable events (Event ID 7036). For UAC bypass (T1548.002): look for high-integrity processes spawned by medium-integrity parents without a UAC prompt event (Event ID 4703 or absence of expected consent.exe invocation). For C2 (T1071): baseline outbound DNS and HTTP/HTTPS traffic and alert on connections to domains registered within the past 12 months, particularly those impersonating software vendor names. Behavioral indicators: installer processes spawning PowerShell or

WScript; scheduled tasks created from temp paths; ScreenConnect beaconing to non-corporate ScreenConnect tenants. Per Securelist reporting, retrieve published IOCs from the source article for direct blocklist and SIEM rule input.

Indicators of Compromise

Type	Value	Context	Confidence
DOMAIN	`See Securelist IOC list`	Campaign infrastructure spans 90-plus domains impersonating software download sites; full domain list published in Securelist source article. Individual domain values are not reproduced here to avoid transcription error — pull directly from the source.	MEDIUM

Framework Mappings

MITRE-ATTACK

- **T1219** — Remote Access Tools
- **T1583.001** — Domains
- **T1055.012** — Process Hollowing
- **T1562.001** — Disable or Modify Tools
- **T1071** — Application Layer Protocol
- **T1548.002** — Bypass User Account Control
- **T1027** — Obfuscated Files or Information
- **T1059.001** — PowerShell
- **T1059** — Command and Scripting Interpreter
- **T1059.005** — Visual Basic
- **T1053.005** — Scheduled Task
- **T1574.002** — DLL Side-Loading
- **T1195** — Supply Chain Compromise
- **T1608.006** — SEO Poisoning

NIST-800-53R5

- **CA-7** — Continuous Monitoring
- **SC-7** — Boundary Protection
- **SI-4** — System Monitoring
- **SI-3** — Malicious Code Protection
- **CM-7** — Least Functionality
- **SI-7** — Software, Firmware, and Information Integrity
- **SA-9** — External System Services

- **SR-2** — Supply Chain Risk Management Plan
- **SR-3** — Supply Chain Controls and Processes
- **CM-3** — Configuration Change Control
- **AC-6** — Least Privilege

OWASP-TOP10-2021

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

CIS-V8

- **2.5** — Allowlist Authorized Software
- **2.6** — Allowlist Authorized Libraries
- **8.2** — Collect Audit Logs
- **5.4** — Restrict Administrator Privileges to Dedicated Administrator Accounts

NIST-CSF-2

- **DE.CM-01** — Networks and network services are monitored

SOC2-TSC

- **CC6.3** — Authorizes, modifies, or removes access

MITRE ATT&CK Mapping

Technique ID	Technique Name	Tactic
T1219	Remote Access Tools	Command-And-Control
T1583.001	Domains	Resource-Development
T1055.012	Process Hollowing	Defense-Evasion
T1562.001	Disable or Modify Tools	Defense-Evasion
T1071	Application Layer Protocol	Command-And-Control
T1548.002	Bypass User Account Control	Privilege-Escalation
T1027	Obfuscated Files or Information	Defense-Evasion
T1059.001	PowerShell	Execution
T1059	Command and Scripting Interpreter	Execution
T1059.005	Visual Basic	Execution
T1053.005	Scheduled Task	Execution
T1574.002	DLL Side-Loading	Persistence
T1195	Supply Chain Compromise	Initial-Access

Technique ID	Technique Name	Tactic
T1608.006	SEO Poisoning	Resource-Development

Sources

Source	URL	Tier
Security News	https://thehackernews.com/2026/07/seo-poisoned-software-sites-abuse...	T2
How a single ScreenConnect incident exposed a massive ...	https://securelist.com/tr/the-soc-files-screenconnect-campaign-with...	T1
ConnectWise ScreenConnect CVE-2024-1709 & ...	https://www.huntress.com/blog/a-catastrophe-for-control-understandi...	T1
Exploitation of ConnectWise ScreenConnect Vulnerabilities	https://www.darktrace.com/blog/connecting-the-dots-darktraces-detec...	T3

Generated 2026-07-02 07:12 UTC by TJS Security Command Center