INTELLIGENCE BRIEFING
Security Command Center
TLP:CLEAR
2026-06-01 18:42 UTC

SmartApeSG ClickFix Chain Delivers NetSupport RAT via Unidentified Dropper with Encoded C2 Traffic

THREAT CAMPAIGN | **HIGH** | CVSS 7.5

SCC Item ID	SCC-CAM-2026-0388
Type	Threat Campaign
Severity	HIGH
CVSS Base Score	7.5
Affected Products	Windows endpoints targeted via browser-based social engineering; NetSupport Manager abused as post-exploitation RAT (no specific vulnerable product version identified)
Published	2026-05-31T20:02:30
Discovery Source	Rss

Executive Summary

SmartApeSG, an active threat group, is running a two-stage attack campaign that compromises Windows endpoints through browser-based deception, tricking users into executing malicious commands themselves. Once inside, attackers deploy a legitimate remote administration tool (NetSupport Manager) as a backdoor, giving them persistent access to affected systems. Organizations with Windows endpoints and standard web browsing access face risk of sustained, covert remote access that can lead to data theft, lateral movement, or ransomware staging.

Technical Analysis

Campaign documented by SANS Internet Storm Center (May 27, 2026) and attributed to SmartApeSG, a ClickFix threat cluster. Attack chain: Stage 1, a browser-delivered ClickFix lure social-engineers users into manually executing commands via the Windows Run dialog or PowerShell (T1204.002, T1059.001, T1059.003, T1566). An unidentified dropper RAT establishes C2 using encoded, non-TLS traffic (T1001, T1571, T1573), an intentional design choice to bypass TLS inspection while simultaneously obscuring payload structure. Stage 2, the dropper fetches and installs a malicious NetSupport Manager package (T1105, T1219), abusing the legitimate, signed remote administration tool as a persistent RAT (T1036.004). Persistence established via T1547 (boot/logon autostart). C2 uses HTTP application-layer protocol (T1071.001). Relevant CWEs: CWE-693 (Protection Mechanism Failure, encoded C2 bypasses TLS inspection), CWE-494 (Download of Code Without Integrity Check, dropper payload delivery), CWE-77 (Command Injection, user-executed command lure). No

CVE assigned; no specific vulnerable product version identified. No patch available, this is a social engineering and tool-abuse campaign, not a software vulnerability. Corroborating NetSupport RAT abuse context available from Red Canary, Corelight, Talos, and Darktrace, though those sources predate this specific campaign instance.

Action Checklist

1. Step 1: Containment, Identify any Windows endpoints that have recently launched PowerShell or cmd.exe from browser-spawned processes (parent process: chrome.exe, msedge.exe, firefox.exe, iexplore.exe). Isolate those endpoints from the network immediately. Block outbound connections to known NetSupport Manager C2 ports (TCP 5405 and 443 where NetSupport is not authorized) at the perimeter firewall per CIS 4.4 and NIST AC-4 (Information Flow Enforcement).
2. Step 2: Detection, Query EDR and SIEM for: (a) PowerShell or cmd.exe processes with parent process matching a browser executable; (b) msiexec.exe or regsvr32.exe loading from user-writable directories (AppData, Temp); (c) NetSupport Manager client binary (client32.exe) executing outside approved software inventory, cross-reference CIS 2.1 (Software Inventory) and CIS 2.3 (Unauthorized Software). Monitor network logs for encoded, non-TLS outbound traffic on non-standard ports (NIST AU-6, AU-12). Alert on any new NetSupport Manager installation not present in CIS 1.1 (Asset Inventory). Use local account monitoring to flag unexpected privilege changes post-infection.
3. Step 3: Eradication, Remove unauthorized NetSupport Manager installations using endpoint management tooling; verify against CIS 2.1 software inventory. Kill and remove dropper artifacts from user-writable directories. Revoke any local or domain credentials used on compromised endpoints. Reset browser session tokens and cached credentials on affected systems. Document all removed artifacts for forensic retention per NIST AU-11.
4. Step 4: Recovery, Re-image confirmed compromised endpoints where forensic analysis is complete. Validate that NetSupport Manager is absent from all endpoints not in the approved software inventory (CIS 2.3). Confirm outbound encoded C2 traffic is no longer present in network logs (NIST SI-4, AU-6). Restore endpoints from known-good backups only after confirming dropper persistence mechanisms (T1547 autostart entries: registry Run keys, Startup folder) have been removed. Monitor for re-infection attempts over 30 days post-remediation.
5. Step 5: Post-Incident, Conduct a targeted review of browser process execution policies; implement application control rules to block browser-spawned script interpreters (PowerShell, cmd.exe) where not operationally required (NIST AC-6, Least Privilege; CIS 4.6). Enforce NIST AC-3 (Access Enforcement) to restrict NetSupport Manager installation rights to IT administration accounts only (CIS 5.4). Review and strengthen user security awareness training focused on ClickFix and Run-dialog lure patterns. Assess whether TLS inspection gaps exposed non-TLS encoded C2 channels, if so, remediate per NIST SC controls. Apply system file analysis monitoring rules for future dropper-stage detection.

IR / Forensic Enrichment

Triage Priority	IMMEDIATE

Escalation Criteria	Escalate to senior IR leadership, legal, and privacy counsel immediately if forensic evidence shows NetSupport Manager C2 sessions exported files from sensitive directories (Documents, Desktop, browser credential stores), if domain administrator credentials were present on any compromised endpoint, or if more than 5 endpoints show confirmed client32.exe execution — indicating a broad lateral spread that may trigger organizational breach notification obligations under applicable data protection regulations.
Recovery Notes	Prior to restoring any endpoint, confirm via Autoruns and registry export that all SmartApeSG dropper persistence mechanisms under HKCU/HKLM Run keys and the Startup folder have been removed, and verify client32.exe is absent from all user-writable directories and %ProgramFiles%. Restore exclusively from pre-infection system images or backups taken before the earliest confirmed SmartApeSG activity timestamp established during forensic timeline analysis. Maintain elevated network monitoring for outbound TCP 5405 and anomalous non-TLS 443 traffic for a minimum of 30 days post-recovery, as SmartApeSG campaigns have demonstrated re-targeting of previously compromised environments.
Forensic Artifacts	Sysmon Event ID 1 (Process Create) logs — browser parent process (chrome.exe, msedge.exe, firefox.exe) spawning powershell.exe or cmd.exe with encoded or obfuscated command-line arguments containing the SmartApeSG dropper URI; found in Microsoft-Windows-Sysmon/Operational event log | NetSupport Manager client32.exe and associated DLLs (PCICAPI.DLL, HTCTL32.DLL) in anomalous paths outside %ProgramFiles%\NetSupport — typically written to %AppData%\Roaming or %Temp% by the unidentified dropper stage; hash these for IOC extraction | Windows Prefetch files at C:\Windows\Prefetch\CLIENT32.EXE-*.pf and MSIEXEC.EXE-*.pf — confirm execution of NetSupport client and msiexec-based dropper delivery even after binary removal, with embedded timestamps establishing the initial compromise window | Registry keys HKCU\Software\Microsoft\Windows\CurrentVersion\Run and HKCU\Software\NetSupport — SmartApeSG's dropper establishes T1547.001 persistence for client32.exe here; export full hive with 'reg export HKCU C:\IR\HKCU_run.reg' before eradication | Network firewall or proxy logs showing outbound TCP 5405 sessions or non-TLS application-layer traffic on 443 with non-browser User-Agent strings — NetSupport Manager's encoded C2 protocol produces a distinctive non-HTTP framing pattern distinguishable from legitimate HTTPS, confirmable via Wireshark protocol dissection

Per-Action IR Details

Step 1: Containment — Identify any Windows endpoints that have recently launched PowerShell or cmd.exe from browser-spawned processes (parent process: chrome.exe, msedge.exe, firefox.exe, iexplore.exe). Isolate those endpoints from the network immediately. Block outbound connections to known NetSupport Manager C2 ports (TCP 5405 and 443 where NetSupport is not authorized) at the perimeter firewall per CIS 4.4 and NIST AC-4 (Information Flow Enforcement).

NIST Phase: Containment

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

Controls: NIST AC-4 (Information Flow Enforcement), NIST IR-4 (Incident Handling), CIS 4.4 (Implement and Manage a Firewall on Servers)

Compensating: Without EDR, deploy Sysmon with SwiftOnSecurity config and query Event ID 1 (Process Create) filtering where ParentImage contains 'chrome.exe', 'msedge.exe', 'firefox.exe', or 'iexplore.exe' AND Image ends in 'powershell.exe' or 'cmd.exe': Get-WinEvent -LogName 'Microsoft-Windows-Sysmon/Operational' | Where-Object {$_.Id -eq 1} | Where-Object {$_.Message -match 'chrome|msedge|firefox' -and $_.Message -match 'powershell|cmd.exe'}. Block TCP 5405 outbound immediately on perimeter firewall and on Windows host firewall via: netsh advfirewall firewall add rule name='Block NetSupport C2' dir=out protocol=TCP remoteport=5405 action=block.

Evidence: Capture BEFORE isolating: (1) Sysmon Event ID 1 logs showing browser parent-to-PowerShell/cmd.exe process chain with full command-line arguments — the ClickFix lure causes the user to paste a Run-dialog or PowerShell command, so the command line will contain encoded or obfuscated strings characteristic of SmartApeSG's dropper stage; (2) Windows Security Event Log Event ID 4688 (Process Creation) with command-line auditing enabled, filtering on parent PID matching browser processes; (3) Active network connections at time of isolation via 'netstat -anob > C:\IR\netstat_$(hostname)_$(Get-Date -f yyyyMMddHHmm).txt' to capture live C2 session on TCP 5405 or 443 to non-browser destinations; (4) Browser history and clipboard contents from affected user profile (AppData\Local\Google\Chrome\User Data\Default\History) to recover the SmartApeSG lure page URL that delivered the ClickFix prompt.

Step 2: Detection — Query EDR and SIEM for: (a) PowerShell or cmd.exe processes with parent process matching a browser executable; (b) msiexec.exe or regsvr32.exe loading from user-writable directories (AppData, Temp); (c) NetSupport Manager client binary (client32.exe) executing outside approved software inventory — cross-reference CIS 2.1 (Software Inventory) and CIS 2.3 (Unauthorized Software). Monitor network logs for encoded, non-TLS outbound traffic on non-standard ports (NIST AU-6, AU-12). Alert on any new NetSupport Manager installation not present in CIS 1.1 (Asset Inventory). Use D3-LAM (Local Account Monitoring) to flag unexpected privilege changes post-infection.

NIST Phase: Detection Analysis

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

Controls: NIST AU-6 (Audit Record Review, Analysis, And Reporting), NIST AU-12 (Audit Record Generation), NIST SI-4 (System Monitoring), CIS 2.1 (Establish and Maintain a Software Inventory), CIS 2.3 (Address Unauthorized Software), CIS 1.1 (Establish and Maintain Detailed Enterprise Asset Inventory), CIS 8.2 (Collect Audit Logs)

Compensating: Without SIEM/EDR: (1) Use Sysmon Event ID 1 to hunt browser-spawned interpreters and Event ID 7 (Image Load) to catch regsvr32.exe or msiexec.exe loading DLLs from %AppData% or %Temp% — apply the Sigma rule 'proc_creation_win_susp_cmd_spawn_from_browser.yml' from SigmaHQ; (2) Scan all endpoints for client32.exe using: Get-ChildItem -Path C:\ -Recurse -Filter 'client32.exe' -ErrorAction SilentlyContinue | Select FullName, LastWriteTime; (3) Use Wireshark or tcpdump to capture and inspect outbound traffic on TCP 5405 and flag non-TLS sessions on 443 that do not present a valid TLS handshake — NetSupport's encoded C2 protocol is identifiable by its non-standard application-layer framing; (4) Run osquery: SELECT name, path, pid FROM processes WHERE name IN ('client32.exe', 'powershell.exe', 'cmd.exe');

Evidence: Capture BEFORE proceeding: (1) Full Sysmon Event ID 1 log entries with command-line arguments for any PowerShell execution originating from browser parent — SmartApeSG's ClickFix stage typically pastes a msiexec.exe or PowerShell one-liner with a remote URI pointing to the dropper; (2) %AppData%\Local\Temp and %AppData%\Roaming directory listings with timestamps (dir /T:C /O:D) to identify dropper artifacts written during infection window; (3) Windows Security Event ID 4697 (Service Installed) or 7045 for any NetSupport Manager service registration; (4) Prefetch files at C:\Windows\Prefetch\CLIENT32.EXE-*.pf to confirm client32.exe execution history even if the binary has been removed; (5) Network flow logs (NetFlow or Windows Firewall logs at C:\Windows\System32\LogFiles\Firewall\pfirewall.log) showing outbound TCP 5405 connections with destination IP for threat intel enrichment against known SmartApeSG infrastructure.

Step 3: Eradication — Remove unauthorized NetSupport Manager installations using endpoint management tooling; verify against CIS 2.1 software inventory. Kill and remove dropper artifacts from user-writable directories. Revoke any local or domain credentials used on compromised endpoints (D3-CRO, Credential Rotation). Reset browser session tokens and cached credentials on affected systems. Document all removed artifacts for forensic retention per NIST AU-11.

NIST Phase: Eradication

Reference: NIST 800-61r3 §3.4 — Eradication

Controls: NIST AU-11 (Audit Record Retention), NIST CM-7 (Least Functionality), NIST IA-4 (Identifier Management), CIS 2.1 (Establish and Maintain a Software Inventory), CIS 5.3 (Disable Dormant Accounts), CIS 6.2 (Establish an Access Revoking Process)

Compensating: Without endpoint management tooling: (1) Remove NetSupport Manager via: wmic product where 'name like "%NetSupport%"' call uninstall /nointeractive, then verify with Get-ChildItem 'C:\Program Files*\NetSupport' and 'C:\ProgramData\NetSupport'; (2) Delete dropper artifacts from user-writable paths: Remove-Item -Recurse -Force $env:APPDATA*.msi, $env:TEMP*.msi — capture SHA-256 hashes first via Get-FileHash before deletion; (3) Revoke local credentials: net user and force AD password reset for domain accounts via: Set-ADAccountPassword -Identity -Reset; (4) Export and archive all collected evidence to a write-protected network share or external drive before deletion to satisfy NIST AU-11 retention requirements — retain for minimum 1 year or per organizational policy.

Evidence: Capture BEFORE eradication: (1) Full forensic image or at minimum a KAPE triage collection (AppData, Temp, Prefetch, registry hives, event logs) from each compromised endpoint before any removal; (2) Registry export of HKCU\Software\Microsoft\Windows\CurrentVersion\Run, HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Run, and HKCU\Software\NetSupport — SmartApeSG's dropper may establish NetSupport persistence via Run keys; (3) SHA-256 hashes of client32.exe and any associated NetSupport DLLs (PCICAPI.DLL, HTCTL32.DLL) found outside %ProgramFiles% for IOC submission; (4) Browser credential stores — Chrome: %AppData%\Local\Google\Chrome\User Data\Default\Login Data (SQLite), Edge: %AppData%\Local\Microsoft\Edge\User Data\Default\Login Data — to assess scope of credential exposure; (5) Windows Credential Manager dump via: cmdkey /list to identify any harvested credentials stored post-RAT deployment.

Step 4: Recovery — Re-image confirmed compromised endpoints where forensic analysis is complete. Validate that NetSupport Manager is absent from all endpoints not in the approved software inventory (CIS 2.3). Confirm outbound encoded C2 traffic is no longer present in network logs (NIST SI-4, AU-6). Restore endpoints from known-good backups only after confirming dropper persistence mechanisms (T1547 autostart entries: registry Run keys, Startup folder) have been removed. Monitor for re-infection attempts over 30 days post-remediation.

NIST Phase: Recovery

Reference: NIST 800-61r3 §3.5 — Recovery

Controls: NIST SI-4 (System Monitoring), NIST AU-6 (Audit Record Review, Analysis, And Reporting), NIST CP-10 (System Recovery and Reconstitution), CIS 2.3 (Address Unauthorized Software), CIS 1.1 (Establish and Maintain Detailed Enterprise Asset Inventory), CIS 7.3 (Perform Automated Operating System Patch Management)

Compensating: Without enterprise imaging infrastructure: (1) Verify clean state by running Get-ChildItem -Recurse -Filter 'client32.exe' across all drives and checking Autoruns (Sysinternals) output for any NetSupport or dropper entries in Run keys, Startup folder (C:\Users\%username%\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup), and scheduled tasks; (2) Confirm C2 cessation by monitoring Windows Firewall logs and running Wireshark on a network tap for 72 hours post-remediation, filtering on TCP 5405 and any connections to IPs flagged during investigation; (3) For re-infection monitoring, deploy a Sysmon rule or Sigma detection (sigma/rules/windows/process_creation/proc_creation_win_susp_regsvr32_anomalies.yml) and schedule a weekly osquery scan for client32.exe presence across the fleet.

Evidence: Capture BEFORE restoring from backup: (1) Autoruns (Sysinternals) HTML export showing all T1547 autostart locations — specifically HKCU and HKLM Run keys, Startup folder entries, and scheduled tasks created during the infection window — to confirm all dropper persistence is cleared; (2) Windows Security Event ID 4698 (Scheduled Task Created) and 4702 (Scheduled Task Updated) logs covering the infection timeframe to identify any task-based persistence SmartApeSG's dropper may have established alongside Run key persistence; (3) Final network flow logs post-eradication confirming no outbound TCP 5405 or encoded non-TLS 443 traffic to previously identified C2 IPs, establishing a clean-baseline timestamp for the 30-day monitoring window.

Step 5: Post-Incident — Conduct a targeted review of browser process execution policies; implement application control rules to block browser-spawned script interpreters (PowerShell, cmd.exe) where not operationally required (NIST AC-6, Least Privilege; CIS 4.6). Enforce NIST AC-3 (Access Enforcement) to restrict NetSupport Manager installation rights to IT administration accounts only (CIS 5.4). Review and strengthen user security awareness training focused on ClickFix and Run-dialog lure patterns. Assess whether TLS inspection gaps exposed non-TLS encoded C2 channels — if so, remediate per NIST SC

controls. Apply D3-SFA (System File Analysis) monitoring rules for future dropper-stage detection.

NIST Phase: Post Incident

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

Controls: NIST AC-3 (Access Enforcement), NIST AC-6 (Least Privilege), NIST SC-7 (Boundary Protection), NIST SC-8 (Transmission Confidentiality and Integrity), NIST IR-4 (Incident Handling), NIST AT-2 (Literacy Training and Awareness), CIS 4.6 (Securely Manage Enterprise Assets and Software), CIS 5.4 (Restrict Administrator Privileges to Dedicated Administrator Accounts)

Compensating: Without enterprise application control (AppLocker/WDAC): (1) Block browser-to-interpreter chains via Software Restriction Policies (SRP) — create a Disallowed rule for powershell.exe and cmd.exe under HKLM\SOFTWARE\Policies\Microsoft\Windows\Safer\CodeIdentifiers when invoked from browser process context; alternatively deploy the free Sigma rule 'proc_creation_win_susp_powershell_parent_combo.yml' into Sysmon for detection; (2) Restrict NetSupport Manager installation via GPO — set 'Prevent users from installing software' under Computer Configuration > Administrative Templates > Windows Components > Windows Installer; (3) Deliver targeted ClickFix awareness using free SANS Security Awareness materials; specifically train users to recognize Run-dialog and PowerShell-paste lures, which are the specific social engineering vectors SmartApeSG uses to initiate this chain; (4) Add a YARA rule scanning %AppData% and %Temp% for NetSupport client32.exe PE characteristics and dropper MSI artifacts as a scheduled weekly scan via ClamAV or Windows Defender CLI: 'MpCmdRun.exe -Scan -ScanType 2'.

Evidence: Collect for lessons-learned and future detection hardening: (1) Full timeline reconstruction from Sysmon, Windows Security, and firewall logs covering the initial ClickFix lure interaction through NetSupport C2 establishment — this timeline should anchor the detection gap analysis showing where existing controls failed to alert on the browser-to-PowerShell execution chain; (2) The specific SmartApeSG lure page URL and ClickFix prompt text recovered from browser history and clipboard artifacts, to create organization-specific phishing awareness training examples and to share with threat intelligence communities (ISACs); (3) IOCs extracted during investigation (client32.exe hash, C2 IP/domain, dropper MSI hash, encoded C2 traffic pattern/signature) formatted as STIX 2.1 for ingestion into future detection tooling and sharing per NIST IR-4 requirements.

Detection Guidance

Primary detection opportunity is the encoded, non-TLS C2 channel in Stage 1. Network monitoring teams should alert on: (1) outbound traffic with non-standard encoding patterns on ports not associated with known application profiles, specifically look for high-entropy, non-HTTP-structured payloads on TCP ports outside your approved egress list; (2) DNS queries or connections to newly registered or low-reputation domains initiated by browser processes or short-lived child processes. EDR detection focus: (a) process tree anomalies, browser spawning PowerShell, cmd.exe, mshta.exe, or wscript.exe (maps to T1059.001, T1059.003, T1204.002); (b) msiexec.exe or rundll32.exe loading from AppData or Temp paths; (c) client32.exe (NetSupport Manager client) appearing on endpoints not in software inventory (CIS 2.1, CIS 2.3); (d) new autostart registry entries (HKCU\Software\Microsoft\Windows\CurrentVersion\Run) created by non-administrative users (T1547). SIEM correlation rule: browser process → script interpreter spawn → outbound connection to new external host within 60-second window. Cross-reference with system file analysis and local account monitoring for post-compromise indicators. Log sources required: Windows Security Event Log (Event ID 4688, process creation with command line), Sysmon (Event IDs 1, 3, 7, 10), EDR telemetry, firewall/proxy egress logs, DNS query logs (per NIST AU-2, AU-12). Note: no confirmed public IOCs (IPs, domains, hashes) are available for this specific campaign instance from the documented sources. Treat any client32.exe installation outside approved inventory as a high-confidence indicator.

Indicators of Compromise

Type	Value	Context	Confidence
URL	`https://isc.sans.edu/diaryimages/images/2026-06-01-ISC-diary-image-01a.png`	SANS ISC diary image documenting the May 27, 2026 SmartApeSG infection chain — reference artifact, not a threat IOC	HIGH

Framework Mappings

MITRE-ATTACK

- **T1219** — Remote Access Tools
- **T1571** — Non-Standard Port
- **T1059.003** — Windows Command Shell
- **T1036.004** — Masquerade Task or Service
- **T1105** — Ingress Tool Transfer
- **T1547** — Boot or Logon Autostart Execution
- **T1071.001** — Web Protocols
- **T1001** — Data Obfuscation
- **T1059.001** — PowerShell
- **T1204.002** — Malicious File
- **T1566** — Phishing
- **T1573** — Encrypted Channel

NIST-800-53R5

- **CM-7** — Least Functionality
- **SI-3** — Malicious Code Protection
- **SI-4** — System Monitoring
- **CA-7** — Continuous Monitoring
- **SC-7** — Boundary Protection
- **SI-7** — Software, Firmware, and Information Integrity
- **AT-2** — Literacy Training and Awareness
- **SI-8** — Spam Protection
- **CM-3** — Configuration Change Control
- **SI-10** — Information Input Validation
- **SC-13** — Cryptographic Protection

OWASP-TOP10-2021

- **A08:2021** — Software and Data Integrity Failures
- **A03:2021** — Injection

CIS-V8

- **2.5** — Allowlist Authorized Software
- **2.6** — Allowlist Authorized Libraries
- **16.10** — Apply Secure Design Principles in Application Architectures
- **14.2** — Train Workforce Members to Recognize Social Engineering Attacks
- **8.2** — Collect Audit Logs

HIPAA-SECURITY

- **164.312(e)(1)** — Transmission Security

NIST-CSF-2

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

MITRE ATT&CK Mapping

Technique ID	Technique Name	Tactic
T1219	Remote Access Tools	Command-And-Control
T1571	Non-Standard Port	Command-And-Control
T1059.003	Windows Command Shell	Execution
T1036.004	Masquerade Task or Service	Defense-Evasion
T1105	Ingress Tool Transfer	Command-And-Control
T1547	Boot or Logon Autostart Execution	Persistence
T1071.001	Web Protocols	Command-And-Control
T1001	Data Obfuscation	Command-And-Control
T1059.001	PowerShell	Execution
T1204.002	Malicious File	Execution
T1566	Phishing	Initial-Access
T1573	Encrypted Channel	Command-And-Control

Sources

Source	URL	Tier
Security News	https://isc.sans.edu/diaryimages/images/2026-06-01-ISC-diary-image-...	T1
NetSupport Manager | Red Canary Threat Detection Report	https://redcanary.com/threat-detection-report/threats/netsupport-ma...	T3

Source	URL	Tier
Detecting NetSupport Manager Abuse - Corelight	https://corelight.com/blog/detecting-netsupport-manager-abuse	T3
NetSupport RAT: Why Legitimate Tools Are as Damaging as Malware	https://www.darktrace.com/blog/netsupport-rat-how-legitimate-tools-...	T3
Detecting evolving threats: NetSupport RAT campaign	https://blog.talosintelligence.com/detecting-evolving-threats-netsu...	T3

Generated 2026-06-01 18:42 UTC by TJS Security Command Center