INTELLIGENCE BRIEFING
Security Command Center
TLP:CLEAR
2026-03-29 18:42 UTC

Typosquatting Campaign Weaponizes 7-Zip Brand to Deploy Proxy Malware on Enterprise Systems

THREAT CAMPAIGN | **MEDIUM** | CVSS 5.0

SCC Item ID	SCC-CAM-2026-0025
Type	Threat Campaign
Severity	MEDIUM
CVSS Base Score	5.0
Affected Products	7-Zip (trojanized installer targeting Windows users; legitimate 7-Zip versions unaffected)
Published	2026-03-14

Executive Summary

A threat actor created a fake website impersonating the official 7-Zip project to distribute a trojanized installer that silently deploys proxyware on Windows machines. Any employee who downloaded 7-Zip outside of approved channels may have enrolled their workstation into a covert proxy network, exposing corporate traffic to interception or enabling attacker-controlled tunneling through your network perimeter. The attack requires no software vulnerability, only a user search and a manual download, making shadow IT and unmanaged endpoints the primary exposure surface.

Technical Analysis

Attack vector: typosquatting domain mimicking the legitimate 7-Zip distribution site (7-zip.org). The malicious installer bundles the expected 7-Zip application alongside proxyware, silencing user suspicion. No CVE is associated, the attack chain exploits social engineering and brand impersonation, not a vulnerability in 7-Zip itself. Relevant CWEs: CWE-1021 (Improper Restriction of Rendered UI Layers, brand impersonation via spoofed site), CWE-494 (Download of Code Without Integrity Check, no signature validation on the installer), CWE-345 (Insufficient Verification of Data Authenticity). MITRE ATT&CK coverage: T1583.001 (Acquire Infrastructure: Domains), T1608.001 (Stage Capabilities: Upload Malware), T1566.002 (Phishing: Spearphishing Link), T1204.002 (User Execution: Malicious File), T1036.005 (Masquerading: Match Legitimate Name or Location), T1090 / T1090.002 (Proxy / External Proxy), T1071.001 (Application Layer Protocol: Web Protocols), T1195.002 (Supply Chain Compromise: Compromise Software Supply Chain, social-engineering variant). Payload behavior is consistent with residential proxy enrollment or covert network tunneling; immediate credential theft or data exfiltration has not been confirmed in available source material. Legitimate 7-Zip versions

obtained from the official 7-zip.org site are unaffected. Source quality: T3 sources only (Malwarebytes Threat Intel, BleepingComputer); no primary vendor advisory available at time of writing.

Action Checklist

1. Step 1, Immediate: Identify any 7-Zip installers downloaded from sources other than 7-zip.org or your approved software repository; quarantine and do not execute.
2. Step 2, Detection: Search endpoint logs and EDR telemetry for proxyware process execution, unexpected outbound connections on proxy-associated ports (e.g., SOCKS5, HTTP CONNECT), and installer file hashes not matching official 7-Zip releases, cross-reference against Malwarebytes threat intel report for specific indicators.
3. Step 3, Assessment: Inventory all Windows endpoints for installed 7-Zip instances; flag any installed outside of centralized patch management or software deployment tools; prioritize unmanaged and shadow IT endpoints.
4. Step 4, Communication: Notify IT helpdesk and end-user population to avoid manual software downloads and report any recent 7-Zip installations; brief SOC on detection signatures and escalation path for confirmed proxy activity.
5. Step 5, Long-term: Enforce application allowlisting or software installation controls to block unapproved installer execution; add DNS/web proxy blocking for known typosquatting domains; review and update acceptable use and software procurement policy to require centralized distribution for all utilities.

IR / Forensic Enrichment

Triage Priority	URGENT
Escalation Criteria	Escalate to C-level management and external DFIR firm if: (1) more than 5% of endpoints are confirmed infected, (2) evidence of lateral movement or persistent backdoor installation is found, (3) exfiltrated sensitive data is confirmed through network forensics, or (4) the organization cannot isolate and remediate affected systems within 72 hours.
Recovery Notes	Post-containment: (1) Rebuild or restore affected endpoints from clean backup images dated before the campaign start (validate backup integrity with hash verification). (2) Re-deploy 7-Zip from your centralized repository using SCCM/WSUS with signature verification enabled. (3) Conduct 30-day post-recovery monitoring of re-infected endpoints (check for port 1080/8080 outbound activity, unsigned 7z.exe execution, and anomalous process creation). Document all findings in post-incident report per NIST 800-61r3 §3.4.3.
Forensic Artifacts	Windows Event Log 4688 (Process Creation) and 4689 (Process Termination) — captures trojanized installer and proxy process execution | Browser Download History ($LOCALAPPDATA\Google\Chrome\User Data\Default\History, $LOCALAPPDATA\Microsoft\Edge\User Data\Default\History) — establishes source of malicious installer (typosquatting domain vs. legitimate 7-zip.org) \| NTFS MFT ($MFT) and $LogFile — recovers deleted installer artifacts and file activity timeline | Network Traffic Capture (.pcapng) on proxy-associated ports (1080 SOCKS5, 8080 HTTP) — demonstrates covert proxy tunnel establishment and potential data exfiltration | Windows Registry (HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services, HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run) — identifies persistence mechanisms and auto-start execution

Per-Action IR Details

Step 1, Immediate: Identify any 7-Zip installers downloaded from sources other than 7-zip.org or your approved software repository; quarantine and do not execute.

NIST Phase: Preparation

Reference: NIST 800-61r3 §2.1 (Preparation phase: tools and resources)

Controls: NIST 800-53 SI-7 (Software, Firmware, and Information Integrity), CIS 2.1 (Address Unauthorized Software)

Compensating: Search Windows file system using PowerShell: Get-ChildItem -Path C:\Users -Recurse -Filter *7zip* -ErrorAction SilentlyContinue | Select-Object FullName,CreationTime. Export results to CSV. Cross-reference download locations against browser history in AppData\Local\Google\Chrome\User Data\Default\History (SQLite) or Edge equivalent. For offline inspection, use autopsy or FTK to recover deleted installer artifacts from $Recycle.Bin and unallocated space.

Evidence: Before quarantining: (1) Capture file hash (SHA-256) of all discovered installers using Get-FileHash; (2) preserve browser download history and cache ($LOCALAPPDATA\Google\Chrome\User Data\Default\History, $LOCALAPPDATA\Microsoft\Edge\User Data\Default\History); (3) snapshot file system metadata (creation, modification, access times) and owner from Properties or fsutil fsinfo volumeinfo; (4) preserve MFT ($MFT) and $LogFile from NTFS for deleted installer recovery.

Step 2, Detection: Search endpoint logs and EDR telemetry for proxyware process execution, unexpected outbound connections on proxy-associated ports (e.g., SOCKS5, HTTP CONNECT), and installer file hashes not matching official 7-Zip releases, cross-reference against Malwarebytes threat intel report for specific indicators.

NIST Phase: Detection Analysis

Reference: NIST 800-61r3 §3.2 (Detection and Analysis phase: determining if an incident occurred)

Controls: NIST 800-53 SI-4 (Information System Monitoring), NIST 800-53 CA-7 (Continuous Monitoring), CIS 8.2 (Configure Data Protection)

Compensating: Query Windows Event Log 4688 (Process Creation) for parent-child process chains using wevtutil qe Security /q:*[System[(EventID=4688)]] /f:text. Search for outbound port 1080 (SOCKS5) or port 8080 (HTTP proxy) in netstat -ano and established connections via Get-NetTCPConnection -State Established. Use Wireshark to capture and filter network traffic (tcp.dstport==1080 or tcp.dstport==8080) on suspect endpoints. Cross-validate file hashes against public 7-Zip release hashes (available at 7-zip.org/download.html) using certutil -hashfile SHA256.

Evidence: Preserve: (1) Windows Event Log 4688 and 4689 (process termination) for 72 hours prior to detection; (2) netstat output and Get-NetTCPConnection snapshots at detection time and hourly thereafter; (3) raw network traffic capture (.pcapng) for all suspect endpoints, filtered to include DNS queries, TCP handshakes, and data exfiltration; (4) Registry HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services and HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run for persistence mechanisms; (5) Process memory dumps (procdump -ma) of suspected proxy processes before termination.

Step 3, Assessment: Inventory all Windows endpoints for installed 7-Zip instances; flag any installed outside of centralized patch management or software deployment tools; prioritize unmanaged and shadow IT endpoints.

NIST Phase: Detection Analysis

Reference: NIST 800-61r3 §3.2.2 (Scope determination and prioritization)

Controls: NIST 800-53 CM-8 (Information System Component Inventory), CIS 1.1 (Inventory and Control of Enterprise Assets)

Compensating: Query WMI to enumerate 7-Zip installations: wmic product list brief | findstr /i 7zip. Export to CSV with endpoint hostname and install date. Cross-reference against centralized deployment logs (WSUS, SCCM logs in C:\Program Files\Microsoft Configuration Manager\Logs or WSUS AdminUI database). For unmanaged endpoints, manually execute remote PowerShell: Invoke-Command -ComputerName -ScriptBlock {Get-ItemProperty

HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Uninstall* | Where-Object {$_.DisplayName -like "*7-Zip*"}. Maintain spreadsheet ranking by: (1) installed via unofficial channel, (2) installation date post-campaign start, (3) absence from SCCM/WSUS logs, (4) shadow IT/unmanaged status.

Evidence: Preserve: (1) snapshots of HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Uninstall (Registry key export); (2) C:\Program Files\7-Zip\7z.exe file metadata (hash, timestamps, digital signature verification); (3) WMI product inventory output with date/time stamp; (4) WSUS/SCCM deployment logs (C:\Program Files\Microsoft Configuration Manager\Logs or SQL database backup if available); (5) BITS Job history (Get-BitsTransfer -AllUsers) to identify unofficial download sources.

Step 4, Communication: Notify IT helpdesk and end-user population to avoid manual software downloads and report any recent 7-Zip installations; brief SOC on detection signatures and escalation path for confirmed proxy activity.

NIST Phase: Containment

Reference: NIST 800-61r3 §3.3 (Containment phase: stakeholder coordination)

Controls: NIST 800-53 IR-4 (Incident Handling), CIS 17.1 (Incident Response Program)

Compensating: Draft and distribute: (1) user alert via email with installation check procedure (native Windows: Control Panel > Programs and Features > search '7-Zip'); (2) helpdesk ticket template with 5 required fields (endpoint hostname, 7-Zip version, installation date, download source, user who installed); (3) SOC detection runbook with Yara rule for trojanized 7-Zip hashes and SIEM alert query for ports 1080/8080. Brief SOC verbally with this escalation path: suspicious process/network activity → run verification scripts (hash and port scan) → if confirmed malicious → isolate endpoint from network → escalate to CIRT lead.

Evidence: Preserve: (1) timestamp and distribution log of user alert (delivery records); (2) SOC alert telemetry for 30 days pre-communication to detect early signals missed during initial detection sweep; (3) helpdesk ticket submission logs to track user-reported 7-Zip installations; (4) communications team log documenting awareness campaign reach and response rate.

Step 5, Long-term: Enforce application allowlisting or software installation controls to block unapproved installer execution; add DNS/web proxy blocking for known typosquatting domains; review and update acceptable use and software procurement policy to require centralized distribution for all utilities.

NIST Phase: Recovery

Reference: NIST 800-61r3 §3.4 (Post-Incident Activities phase: lessons learned and control updates)

Controls: NIST 800-53 CM-11 (User-Installed Software), NIST 800-53 AC-3 (Access Enforcement), CIS 2.1 (Address Unauthorized Software), CIS 13.5 (Restrict and Remediate Unauthorized Network Services)

Compensating: Deploy group policy application allowlist via gpedit.msc (User Configuration > Administrative Templates > System > Don't Run Specified Windows Applications) or AppLocker (Computer Configuration > Windows Settings > Security Settings > Application Control Policies > AppLocker). Create allowlist rule: allow only signed executables from C:\Program Files\7-Zip\ with publisher CN=Igor Pavlov. Block all other 7z.exe variants. For DNS filtering without enterprise appliances: configure Windows Hosts file (C:\Windows\System32\drivers\etc\hosts) with known typosquatting domains (obtain from Malwarebytes, PhishTank) mapped to 127.0.0.1. Document policy in Employee Handbook with escalation path for exceptions (requires CISO sign-off + business justification). Train procurement on centralized vendor approval process.

Evidence: Preserve: (1) baseline AppLocker policy export (XML) before implementation; (2) DNS/web proxy deny list with IOC source and capture date; (3) policy document version control (approved date, reviewer sign-off); (4) training attendance logs and competency assessments.

Detection Guidance

Behavioral indicators: unexpected outbound proxy connections (SOCKS4/5, port 1080; HTTP CONNECT tunneling) from endpoints shortly after a 7-Zip install event; proxyware process names or services not consistent

with approved software inventory; installer execution from user download directories (e.g., %USERPROFILE%\Downloads) rather than a managed deployment path. Log sources to query: EDR process creation logs (parent-child relationship of installer spawning a secondary process), Windows Event Log (Event ID 4688 for process creation, Event ID 7045 for new service installation), DNS query logs for typosquatting domains resembling '7-zip.org' (e.g., 7zip[.]org variants, 7-zip[.]com, 7ziip[.]org), proxy/firewall logs for sustained low-volume outbound connections to residential proxy infrastructure. File integrity check: compare SHA-256 hash of any installed 7-Zip binary against official hashes published at 7-zip.org. Specific IOC values (domain names, hashes, IPs) were not independently verified in available source material at this time, consult primary threat intelligence sources directly for confirmed indicators before deploying as detection rules.

Indicators of Compromise

Type	Value	Context	Confidence
DOMAIN	`typosquatting domain mimicking 7-zip.org — specific domain not independently verified in available source material`	Fake distribution site serving trojanized 7-Zip installer bundled with proxyware. Consult Malwarebytes report for confirmed domain value before blocking.	LOW
URL	`https://www.malwarebytes.com/blog/threat-intel/2026/02/fake-7-zip-downloads-are-turning-home-pcs-into-proxy-nodes`	Primary source report containing confirmed IOCs including domain names and file hashes — retrieve directly for operationalization.	HIGH

Framework Mappings

MITRE-ATTACK

- **T1071.001** — Web Protocols
- **T1608.001** — Upload Malware
- **T1204.002** — Malicious File
- **T1036.005** — Match Legitimate Resource Name or Location
- **T1195.002** — Compromise Software Supply Chain
- **T1583.001** — Domains
- **T1566.002** — Spearphishing Link
- **T1090.002** — External Proxy
- **T1090** — Proxy

NIST-800-53R5

- **CM-7** — Least Functionality
- **SA-9** — External System Services
- **SR-3** — Supply Chain Controls and Processes
- **SI-7** — Software, Firmware, and Information Integrity
- **AT-2** — Literacy Training and Awareness

- **SC-7** — Boundary Protection
- **SI-3** — Malicious Code Protection
- **SI-4** — System Monitoring
- **SI-8** — Spam Protection
- **CM-3** — Configuration Change Control

OWASP-TOP10-2021

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

CIS-V8

- **2.5**
- **2.6**
- **6.3** — Require MFA for Externally-Exposed Applications
- **7.3** — Perform Automated Operating System Patch Management
- **7.4** — Perform Automated Application Patch Management
- **14.2** — Train Workforce Members to Recognize Social Engineering Attacks

HIPAA-SECURITY

- **164.312(d)** — Person or Entity Authentication
- **164.308(a)(6)(ii)** — Response and Reporting

SOC2-TSC

- **CC6.1** — Logical access security software, infrastructure, and architectures
- **CC7.4** — Responds to identified security incidents

ISO-27001-2022

- **A.8.8** — Management of technical vulnerabilities
- **A.5.34** — Privacy and protection of personal information

MITRE ATT&CK Mapping

Technique ID	Technique Name	Tactic
T1071.001	Web Protocols	Command-And-Control
T1608.001	Upload Malware	Resource-Development
T1204.002	Malicious File	Execution
T1036.005	Match Legitimate Resource Name or Location	Defense-Evasion
T1195.002	Compromise Software Supply Chain	Initial-Access
T1583.001	Domains	Resource-Development
T1566.002	Spearphishing Link	Initial-Access

Technique ID	Technique Name	Tactic
T1090.002	External Proxy	Command-And-Control
T1090	Proxy	Command-And-Control

Sources

Source	URL	Tier
Security News	https://www.bleepingcomputer.com	T3
Fake 7-Zip downloads are turning home PCs into proxy nodes	https://www.malwarebytes.com/blog/threat-intel/2026/02/fake-7-zip-d...	T3
7-Zip: A Trusted Tool Being Used for Malware - SD Solutions	https://www.sdsolutionsllc.com/7-zip-a-trusted-tool-being-used-for-...	T3
Fake 7-Zip Installer Drops Proxyware Trojan | Threat Intel Reports	https://www.smarttech247.com/threat-intel-reports/fake-7-zip-instal...	T3
Malicious 7-Zip site distributes installer laced with proxy tool	https://www.bleepingcomputer.com/news/security/malicious-7-zip-site...	T3

Generated 2026-03-29 18:42 UTC by TJS Security Command Center