INTELLIGENCE BRIEFING
Security Command Center
TLP:CLEAR
2026-05-21 06:58 UTC

TamperedChef Multi-Cluster Campaign: Trojanized Productivity Apps Delivering RATs and Infostealers Since 2023

THREAT CAMPAIGN | **HIGH** | CVSS 7.5

SCC Item ID	SCC-CAM-2026-0347
Type	Threat Campaign
Severity	HIGH
CVSS Base Score	7.5
Affected Products	AppSuite PDF, DocuFlex, Calendaromatic, CrystalPDF, Easy2Convert, PDF-Ezy, JustAskJacky, GoCookMate, RocketPDFPro, ManualReaderPro (trojanized apps); Neutralinojs framework (abused as legitimate runtime); Cortex XDR, Cortex XSIAM, Prisma Browser (detection coverage)
Published	2026-05-20T10:00:46+00:00
Discovery Source	Rss:T1 Threatintel

Executive Summary

Since 2023, a threat actor cluster designated TamperedChef has distributed trojanized productivity applications, PDF readers, converters, and scheduling tools via malvertising, achieving at least 12,000 confirmed installations globally. The campaign delivers remote access trojans, infostealers, and proxy tools capable of stealing credentials, capturing keystrokes, and exfiltrating sensitive data from compromised endpoints. Organizations face compounded risk from credential theft, potential lateral movement, and regulatory exposure if stolen data includes protected information.

Technical Analysis

Unit 42 identified three distinct TamperedChef sub-clusters operating since 2023, distributing trojanized versions of at least ten productivity applications: AppSuite PDF, DocuFlex, Calendaromatic, CrystalPDF, Easy2Convert, PDF-Ezy, JustAskJacky, GoCookMate, RocketPDFPro, and ManualReaderPro. Delivery mechanism is malvertising leading to user-initiated download (MITRE T1204.002, T1566). Payloads include RATs, infostealers, and proxy tools. Key evasion techniques: code-signing certificate abuse across 81 unique organizations (T1553.002, CWE-295); frequent binary rebuilds to defeat hash-based detection (T1027, T1027.003, CWE-506, CWE-494); extended dormancy periods of weeks to months before payload activation; and use of the Neutralinojs cross-platform framework as a legitimate-looking runtime host (T1036, T1036.005).

Post-compromise capabilities include credential dumping (T1003, T1555), keylogging (T1056), screen capture (T1113), JavaScript execution (T1059.007), C2 over HTTP/S (T1071, T1071.001), proxy tunneling (T1090, T1090.002), and exfiltration (T1041). Permissive EULAs are embedded to obscure the legal boundary between adware and malware (CWE-522). The developer ecosystem previously exposed by the Shai-Hulud npm supply chain attack represents an overlapping attack surface (T1195.002). No CVE identifier is assigned. Detection coverage is available via Cortex XDR, Cortex XSIAM, and Prisma Browser log ingestion.

Action Checklist

1. Step 1: Containment. Immediately block the ten identified trojanized application names (AppSuite PDF, DocuFlex, Calendaromatic, CrystalPDF, Easy2Convert, PDF-Ezy, JustAskJacky, GoCookMate, RocketPDFPro, ManualReaderPro) using endpoint application control. Query your asset inventory (CIS 1.1) and software inventory (CIS 2.1) for any installations. Isolate affected hosts from the network pending investigation. Block known malvertising delivery domains at the perimeter firewall (CIS 4.4, CIS 4.5).
2. Step 2: Detection. Search endpoint logs for process execution of the named trojanized binaries and for Neutralinojs runtime instances spawned by unexpected parent processes (NIST SI-4, AU-6). In Cortex XSIAM or XDR, query for code-signed binaries whose signing certificates reference organizations outside your approved vendor list; the campaign abused 81 distinct certificate organizations. Review Prisma Browser logs ingested into Cortex XSIAM for malvertising redirect chains leading to productivity app downloads. Hunt for dormant processes with no network activity at install time followed by delayed C2 connections (T1071, T1071.001). Flag JavaScript execution (T1059.007) from newly installed productivity apps. Apply behavioral analysis to identify unexpected binary modifications consistent with frequent rebuilds.
3. Step 3: Eradication. Remove all identified trojanized applications and their associated Neutralinojs runtime files from affected endpoints. There is no vendor patch; the attack vector is user-installed trojanized software, not a vulnerability in a supported product. Enforce CIS 2.3 (Address Unauthorized Software): remove unauthorized applications and require documented exceptions for any non-inventoried software. Revoke and rotate credentials on any endpoint where these applications were installed (NIST IA controls). Treat all accounts accessible from affected hosts as potentially compromised. Block the 81 identified code-signing certificate organizations at your endpoint protection platform where feasible.
4. Step 4: Recovery. After removing malicious applications and rotating credentials, verify no persistence mechanisms remain: check startup configurations (NIST SI-7), scheduled tasks, registry run keys, and browser extensions on affected hosts (MITRE T1547). Re-image endpoints where full forensic confidence cannot be established. Monitor post-remediation for resumed C2 beacon activity, proxy tunnel establishment (T1090.002), or renewed exfiltration attempts (T1041) using SIEM alerting (NIST AU-6, SI-4). Confirm credential rotation is complete across all services accessible from affected endpoints before restoring to production.
5. Step 5: Post-Incident. Conduct a lessons-learned review against these specific control gaps: software allowlisting (CIS 2.3) to prevent unauthorized application installation; code-signing verification policy (CWE-295 exposure, CIS 4.6); user awareness training targeting malvertising and unsolicited software download prompts (NIST AT controls); and developer environment hardening if your organization overlaps with the npm ecosystem exposure identified in the Shai-Hulud campaign (T1195.002). Evaluate whether your logging posture captured dormant payload activation; extended dormancy is a deliberate evasion of time-bounded detection. Review EULA-based adware classification policies to prevent future misclassification of permissive-EULA malware.

IR / Forensic Enrichment

Triage Priority	IMMEDIATE
Escalation Criteria	Escalate to executive leadership, legal counsel, and your incident response retainer immediately if forensic evidence confirms credential exfiltration from accounts with access to PII, PHI, PCI-scoped systems, or privileged infrastructure — the TamperedChef infostealer's browser credential harvesting capability creates breach notification obligations under GDPR, HIPAA, and state privacy laws, and the 12,000+ confirmed global installations suggest high probability of material data exposure requiring regulatory reporting within mandatory timeframes.
Recovery Notes	Do not restore affected endpoints to production until Autoruns analysis, registry run key inspection, and scheduled task enumeration confirm zero TamperedChef persistence mechanisms remain, AND credential rotation is verified complete across all services authenticated from the affected host — partial rotation is insufficient given the infostealer's documented browser credential and keylogger capabilities. Monitor restored hosts for a minimum of 30 days post-remediation using Sysmon network connection logging and DNS query logging, specifically watching for beacon intervals and proxy tunnel establishment patterns consistent with TamperedChef RAT C2 profiles (T1090.002, T1071.001). Given the campaign's deliberate use of dormancy as a detection evasion technique, any host where the exact installation-to-activation timeline cannot be established forensically should be re-imaged rather than remediated in place.
Forensic Artifacts	Neutralinojs runtime binaries and associated `resources.neu` payload files in trojanized app installation directories under %LOCALAPPDATA% and %APPDATA% — the .neu file contains the malicious JavaScript payload (T1059.007) and will survive application uninstallation if the installer does not clean subdirectories | Browser credential store database files (Chrome/Edge: %LOCALAPPDATA%\Google\Chrome\User Data\Default\Login Data and Cookies; Firefox: %APPDATA%\Mozilla\Firefox\Profiles*.default\key4.db and logins.json) showing access timestamps correlating with trojanized app execution windows — evidence of infostealer credential harvesting activity | Windows Security Event Log entries (Event ID 4688 — Process Creation) and Sysmon Event ID 1 logs recording execution chains of trojanized binary names spawning neutralino.exe, with child process command-line arguments revealing JS payload paths and any embedded C2 configuration parameters | Authenticode signature metadata extracted from trojanized binaries in installation directories — specifically the Subject Organization field of the signing certificate, cross-referenceable against the campaign's 81 known abused certificate organizations, recoverable even from deleted binaries if the MFT record or VSS snapshot is intact | DNS query logs and Sysmon Event ID 22 (DNS Query) records originating from Neutralinojs process PIDs during the post-dormancy activation window, capturing C2 domain resolution events that represent the forensic boundary between dormant installation and active RAT/proxy tool operation

Per-Action IR Details

Step 1: Containment — Immediately block the ten identified trojanized application names (AppSuite PDF, DocuFlex, Calendaromatic, CrystalPDF, Easy2Convert, PDF-Ezy, JustAskJacky, GoCookMate, RocketPDFPro, ManualReaderPro) using endpoint application control. Query your asset inventory (CIS 1.1) and software inventory (CIS 2.1) for any installations. Isolate affected hosts from the network pending investigation. Block known malvertising delivery domains at the perimeter firewall (CIS 4.4, CIS 4.5).

NIST Phase: Containment

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

Controls: NIST IR-4 (Incident Handling), NIST CM-7 (Least Functionality), NIST SC-7 (Boundary Protection), CIS 1.1 (Establish and Maintain Detailed Enterprise Asset Inventory), CIS 2.1 (Establish and Maintain a Software Inventory), CIS 4.4 (Implement and Manage a Firewall on Servers), CIS 4.5 (Implement and Manage a Firewall on End-User Devices)

Compensating: For teams without enterprise EDR: run `Get-WmiObject Win32_Product | Where-Object {$_.Name -match 'AppSuite|DocuFlex|Calendaromatic|CrystalPDF|Easy2Convert|PDF-Ezy|JustAskJacky|GoCookMate|RocketPDF|ManualReader'}` on all Windows endpoints via PSRemoting or scheduled task. On Linux/macOS, use `find /Applications /opt /home -name '*.app' -o -name '*.AppImage' 2>/dev/null | grep -iE 'appsuite|docuflex|calendaromatic|crystalpdf|easy2convert|pdf-ezy|justaskjacky|gocookmate|rocketpdf|manualreader'`. Block delivery domains using host-based firewall rules (`netsh advfirewall` on Windows or `iptables`/`ufw` on Linux) and push DNS sinkholes via your internal resolver for known malvertising domains associated with this campaign.

Evidence: Before isolating hosts, image or snapshot the running process list (`tasklist /v` or `ps aux`), active network connections (`netstat -anob` on Windows, `ss -tulnp` on Linux), and installed software registry hive (`HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall`) to establish the pre-containment state. Capture Neutralinojs runtime presence by checking `%LOCALAPPDATA%`, `%APPDATA%`, and `%TEMP%` for `neutralino.exe` or `neutralino-*` binaries co-located with the trojanized app directories. Document all parent-child process relationships for the named binaries before network isolation destroys in-flight C2 session state.

Step 2: Detection — Search endpoint logs for process execution of the named trojanized binaries and for Neutralinojs runtime instances spawned by unexpected parent processes (NIST SI-4, AU-6). In Cortex XSIAM or XDR, query for code-signed binaries whose signing certificates reference organizations outside your approved vendor list — the campaign abused 81 distinct certificate organizations. Review Prisma Browser logs ingested into Cortex XSIAM for malvertising redirect chains leading to productivity app downloads. Hunt for dormant processes with no network activity at install time followed by delayed C2 connections (T1071, T1071.001). Flag JavaScript execution (T1059.007) from newly installed productivity apps. Apply D3-SFA (System File Analysis) to identify unexpected binary modifications consistent with frequent rebuilds.

NIST Phase: Detection Analysis

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

Controls: NIST SI-4 (System Monitoring), NIST AU-6 (Audit Record Review, Analysis, and Reporting), NIST AU-2 (Event Logging), NIST AU-12 (Audit Record Generation), CIS 8.2 (Collect Audit Logs), CIS 7.1 (Establish and Maintain a Vulnerability Management Process)

Compensating: Deploy Sysmon with a configuration that captures Event ID 1 (Process Create) and Event ID 3 (Network Connect) — filter on `Image` matching `neutralino*.exe` or the ten trojanized binary names, and on `ParentImage` to catch unexpected parent processes (e.g., browser spawning installer). Use this Sigma rule basis: `title: TamperedChef Neutralinojs Spawn | detection: selection: Image|endswith: ['\neutralino.exe'] ParentImage|endswith: ['\chrome.exe','\msedge.exe','\firefox.exe'] condition: selection`. For certificate abuse hunting without EDR, use Sysinternals `sigcheck.exe -tv -c -nobanner * > sigcheck_output.csv` in app installation directories and grep for certificate Subject Organizations not in your approved vendor list. Use osquery `SELECT name, path, publisher FROM programs` to enumerate installed software across the fleet.

Evidence: Query Windows Security Event Log for Event ID 4688 (Process Creation) with `NewProcessName` matching any of the ten trojanized binary names or `neutralino*.exe`, filtered to the past 90 days to account for the campaign's documented dormancy behavior. Extract browser history and download records (`%LOCALAPPDATA%\Google\Chrome\User Data\Default\History`, Edge equivalent, Firefox `places.sqlite`) to reconstruct the malvertising redirect chain that delivered the trojanized installer. Pull Sysmon Event ID 22 (DNS Query) logs for outbound resolution events originating from Neutralinojs processes to identify C2 infrastructure. For certificate analysis, extract Authenticode metadata from binaries in the named app installation directories using `Get-AuthenticodeSignature` and cross-reference Subject CN and Organization fields against the 81 known abused certificate organizations.

Step 3: Eradication — Remove all identified trojanized applications and their associated Neutralinojs runtime files from affected endpoints. There is no vendor patch — the attack vector is user-installed trojanized software, not a vulnerability in a supported product. Enforce CIS 2.3 (Address Unauthorized Software): remove unauthorized applications and require documented exceptions for any non-inventoried software. Revoke and rotate credentials on any endpoint where these applications were installed (D3-CRO, NIST IA controls). Treat all accounts accessible from affected hosts as potentially compromised. Block the 81 identified code-signing certificate organizations at your endpoint protection platform where feasible.

NIST Phase: Eradication

Reference: NIST 800-61r3 §3.4 — Eradication

Controls: NIST IA-4 (Identifier Management), NIST IA-5 (Authenticator Management), NIST CM-7 (Least Functionality), NIST SI-2 (Flaw Remediation), CIS 2.3 (Address Unauthorized Software), CIS 5.3 (Disable Dormant Accounts), CIS 5.4 (Restrict Administrator Privileges to Dedicated Administrator Accounts)

Compensating: Uninstall via `wmic product where name='' call uninstall /nointeractive` for each of the ten named applications, then manually delete residual directories under `%LOCALAPPDATA%`, `%APPDATA%\`, and `%PROGRAMFILES%`. Use `Get-ChildItem -Recurse -Path C:\ -Filter 'neutralino*.exe' -ErrorAction SilentlyContinue` to find orphaned Neutralinojs runtime files not removed by the uninstaller. For credential rotation without a PAM tool, force password resets via Active Directory (`Set-ADAccountPassword`) for all accounts that authenticated on affected hosts, and immediately revoke any long-lived API tokens or browser-saved credentials — the TamperedChef infostealers specifically target browser credential stores (`%LOCALAPPDATA%\Google\Chrome\User Data\Default\Login Data`, Edge and Firefox equivalents). Apply YARA rules targeting Neutralinojs binary signatures to verify removal across the filesystem.

Evidence: Before removing files, collect and preserve full directory listings with hashes (`Get-FileHash -Algorithm SHA256`) for all Neutralinojs runtime components and trojanized app binaries as forensic evidence. Extract the browser credential store files (`Login Data`, `Cookies`, `Web Data` for Chromium-based browsers; `key4.db`, `logins.json` for Firefox) from affected hosts to assess the scope of credential exposure prior to rotation — do not delete these before copying to forensic storage. Document all local and domain accounts that had active sessions on affected hosts using `quser`, `net session`, and Windows Security Event ID 4624 (Successful Logon) logs covering the full suspected compromise window back to the earliest known TamperedChef installation date.

Step 4: Recovery — After removing malicious applications and rotating credentials, verify no persistence mechanisms remain: check startup configurations (D3-SICA), scheduled tasks, registry run keys, and browser extensions on affected hosts (MITRE T1547). Re-image endpoints where full forensic confidence cannot be established. Monitor post-remediation for resumed C2 beacon activity, proxy tunnel establishment (T1090.002), or renewed exfiltration attempts (T1041) using SIEM alerting (NIST AU-6, SI-4). Confirm credential rotation is complete across all services accessible from affected endpoints before restoring to production.

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 CM-6 (Configuration Settings), NIST CP-10 (System Recovery and Reconstitution), CIS 4.6 (Securely Manage Enterprise Assets and Software), CIS 7.2 (Establish and Maintain a Remediation Process)

Compensating: Check persistence locations using Autoruns (Sysinternals) — specifically the `Logon`, `Scheduled Tasks`, `Browser Extensions`, and `Winlogon` tabs — and export results to CSV for comparison against a clean baseline. Query the registry directly for TamperedChef persistence patterns: `HKCU\Software\Microsoft\Windows\CurrentVersion\Run`, `HKLM\Software\Microsoft\Windows\CurrentVersion\Run`, and `HKCU\Software\Microsoft\Windows\CurrentVersion\RunOnce`. For browser extension persistence, enumerate `%LOCALAPPDATA%\Google\Chrome\User Data\Default\Extensions` and compare extension IDs against Chrome Web Store known-malicious lists. Post-remediation, run Wireshark or `tcpdump` for 72 hours on restored hosts to capture any resumed beacon traffic — TamperedChef RATs have exhibited delayed activation, so extended monitoring is warranted. Use Sysmon Event ID 3 (Network Connect) to detect proxy tunnel establishment to known TamperedChef C2 infrastructure.

Evidence: Prior to restoring to production, collect Autoruns output, scheduled task XML exports (`schtasks /query /fo LIST /v`), and a complete browser extension manifest inventory as post-remediation verification evidence. Monitor Windows Security Event ID 4648 (Logon Using Explicit Credentials) and Event ID 4672 (Special Privileges Assigned) on restored hosts for 30 days post-recovery to detect any reuse of credentials that may have been exfiltrated before rotation was completed. Capture a full memory image using WinPmem or LiME on any host where dormancy-to-activation timing is uncertain before returning it to production — the TamperedChef campaign's deliberate dormancy period means active payloads may persist in memory without corresponding disk artifacts.

Step 5: Post-Incident — Conduct a lessons-learned review against these specific control gaps: software allowlisting (CIS 2.3) to prevent unauthorized application installation; code-signing verification policy (CWE-295 exposure — CIS 4.6); user awareness training targeting malvertising and unsolicited software download prompts (NIST AT controls); and developer environment hardening if your organization overlaps with the npm ecosystem exposure identified in the Shai-Hulud campaign (T1195.002). Evaluate whether your logging posture captured dormant payload activation — extended dormancy is a deliberate evasion of time-bounded detection. Review EULA-based adware classification policies to prevent future misclassification of permissive-EULA malware.

NIST Phase: Post Incident

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

Controls: NIST IR-4 (Incident Handling), NIST AT-2 (Literacy Training and Awareness), NIST AT-3 (Role-Based Training), NIST CM-7 (Least Functionality), NIST RA-5 (Vulnerability Monitoring and Scanning), CIS 2.2 (Ensure Authorized Software is Currently Supported), CIS 2.3 (Address Unauthorized Software), CIS 4.6 (Securely Manage Enterprise Assets and Software), CIS 7.1 (Establish and Maintain a Vulnerability Management Process), CIS 7.2 (Establish and Maintain a Remediation Process)

Compensating: Implement software allowlisting without enterprise tooling using Windows AppLocker (available in Windows Pro/Enterprise at no additional cost) — create publisher rules that deny execution of binaries signed by any of the 81 identified TamperedChef certificate organizations, and path rules blocking execution from `%APPDATA%`, `%LOCALAPPDATA%`, and `%TEMP%` where the trojanized apps self-install. Build a YARA rule library targeting Neutralinojs abuse patterns (unusual resource file naming, unexpected JS payloads in `resources.neu`) and schedule weekly scans with ClamAV or the standalone YARA scanner. For logging gap remediation, extend Sysmon log retention to 180 days to capture future dormant-activation events — configure `HKLM\SYSTEM\CurrentControlSet\Services\EventLog\Security` `MaxSize` to at least 1GB. Write a Sigma detection rule for JavaScript execution originating from productivity app process trees and contribute it to the community rule set.

Evidence: Compile a complete post-incident artifact package including: the full timeline of trojanized app installation dates cross-referenced against first observed C2 beacon timestamps to quantify the dormancy window per host; browser download history records documenting the malvertising lure and redirect chain; the complete list of code-signing certificate Subject Organizations observed in this incident for future blocklist maintenance; and redacted credential exposure scope documentation for regulatory notification assessment. Review whether your AV or EDR products classified any of the ten trojanized apps as 'adware' or 'PUA' rather than malware due to permissive EULA language — document classification policy gaps and submit reclassification requests to vendor threat intelligence teams for the specific binary hashes recovered.

Detection Guidance

Primary detection surface is endpoint telemetry and application execution logs. Query for process launches of the ten named trojanized applications; treat any match as high-confidence indicator. Hunt for Neutralinojs runtime instances (neutralino.exe or platform equivalents) launched outside your approved software inventory. In Cortex XDR/XSIAM, create rules for: (1) code-signed binaries whose certificate subject organizations do not appear in your approved vendor list; (2) newly installed productivity apps initiating outbound connections after extended dormancy (days to weeks post-install); (3) JavaScript engine invocations (T1059.007) from PDF or

document utility processes. Apply behavioral analysis to monitor system executables and configuration files for modification consistent with frequent binary rebuilds. For network-layer detection: alert on outbound HTTP/S connections to low-reputation or newly registered domains from productivity application processes (T1071.001); flag proxy tunnel establishment (T1090.002) originating from these process trees. Ingest Prisma Browser logs into Cortex XSIAM per the Palo Alto administrator guide to capture malvertising redirect chains at point of download. Apply Local Account Monitoring on hosts where these applications were found, focusing on credential access events (T1003, T1555) and keylogger artifacts (T1056). Hash-based detection is explicitly insufficient; the campaign uses frequent binary rebuilds (CWE-506). Behavioral and certificate-based detection are required.

Indicators of Compromise

Type	Value	Context	Confidence
DOMAIN	`Not published in available source data`	Unit 42 TamperedChef report references C2 infrastructure — consult the full Unit 42 report at https://unit42.paloaltonetworks.com/tracking-tampered-chef-clusters/ for current IOC lists; specific values not reproduced here to avoid citing unverified specifics	LOW
HASH	`Not published in available source data`	Campaign uses frequent binary rebuilds explicitly to defeat hash-based detection; static hashes are of limited value — behavioral indicators are the recommended detection path	LOW

Framework Mappings

MITRE-ATTACK

- **T1113** — Screen Capture
- **T1027.003** — Steganography
- **T1566** — Phishing
- **T1036** — Masquerading
- **T1059.007** — JavaScript
- **T1105** — Ingress Tool Transfer
- **T1003** — OS Credential Dumping
- **T1195.002** — Compromise Software Supply Chain
- **T1071** — Application Layer Protocol
- **T1204.002** — Malicious File
- **T1553.002** — Code Signing
- **T1027** — Obfuscated Files or Information
- **T1036.005** — Match Legitimate Resource Name or Location

- **T1547** — Boot or Logon Autostart Execution
- **T1056** — Input Capture
- **T1059** — Command and Scripting Interpreter
- **T1090.002** — External Proxy
- **T1071.001** — Web Protocols
- **T1041** — Exfiltration Over C2 Channel
- **T1555** — Credentials from Password Stores
- **T1566.004** — Spearphishing Voice
- **T1090** — Proxy

NIST-800-53R5

- **AT-2** — Literacy Training and Awareness
- **CA-7** — Continuous Monitoring
- **SC-7** — Boundary Protection
- **SI-3** — Malicious Code Protection
- **SI-4** — System Monitoring
- **SI-8** — Spam Protection
- **AC-6** — Least Privilege
- **IA-5** — Authenticator Management
- **CM-7** — Least Functionality
- **SA-9** — External System Services
- **SR-3** — Supply Chain Controls and Processes
- **SI-7** — Software, Firmware, and Information Integrity
- **SC-8** — Transmission Confidentiality and Integrity
- **SC-17** — Public Key Infrastructure Certificates
- **CM-3** — Configuration Change Control
- **SR-2** — Supply Chain Risk Management Plan
- **SC-13** — Cryptographic Protection

OWASP-TOP10-2021

- **A02:2021** — Cryptographic Failures
- **A07:2021** — Identification and Authentication Failures
- **A04:2021** — Insecure Design
- **A08:2021** — Software and Data Integrity Failures

CIS-V8

- **3.10** — Encrypt Sensitive Data in Transit
- **5.2** — Use Unique Passwords
- **2.5** — Allowlist Authorized Software
- **2.6** — Allowlist Authorized Libraries

- **15.1** — Establish and Maintain an Inventory of Service Providers
- **8.2** — Collect Audit Logs

HIPAA-SECURITY

- **164.308(a)(5)(ii)(D)** — Password Management

NIST-CSF-2

- **GV.SC-01** — Cybersecurity supply chain risk management program
- **DE.CM-01** — Networks and network services are monitored

ISO-27001-2022

- **A.5.21** — Managing information security in the ICT supply chain

SOC2-TSC

- **CC9.2** — Manages risks associated with vendors and business partners

MITRE ATT&CK Mapping

Technique ID	Technique Name	Tactic
T1113	Screen Capture	Collection
T1027.003	Steganography	Defense-Evasion
T1566	Phishing	Initial-Access
T1036	Masquerading	Defense-Evasion
T1059.007	JavaScript	Execution
T1105	Ingress Tool Transfer	Command-And-Control
T1003	OS Credential Dumping	Credential-Access
T1195.002	Compromise Software Supply Chain	Initial-Access
T1071	Application Layer Protocol	Command-And-Control
T1204.002	Malicious File	Execution
T1553.002	Code Signing	Defense-Evasion
T1027	Obfuscated Files or Information	Defense-Evasion
T1036.005	Match Legitimate Resource Name or Location	Defense-Evasion
T1547	Boot or Logon Autostart Execution	Persistence
T1056	Input Capture	Collection
T1059	Command and Scripting Interpreter	Execution

Technique ID	Technique Name	Tactic
T1090.002	External Proxy	Command-And-Control
T1071.001	Web Protocols	Command-And-Control
T1041	Exfiltration Over C2 Channel	Exfiltration
T1555	Credentials from Password Stores	Credential-Access
T1566.004	Spearphishing Voice	Initial-Access
T1090	Proxy	Command-And-Control

Sources

Source	URL	Tier
Unit 42	https://unit42.paloaltonetworks.com/tracking-tampered-chef-clusters/	T3
	https://unit42.paloaltonetworks.com/tracking-tampered-chef-clusters/	T3
	https://unit42.paloaltonetworks.com/muddled-libra/	T3
	https://unit42.paloaltonetworks.com/npm-supply-chain-attack/	T3
Ingest Prisma Browser logs into Cortex XSIAM. - Administrator Guide	https://docs-cortex.paloaltonetworks.com/r/Cortex-XSIAM/Cortex-XSIA...	T3

Generated 2026-05-21 06:58 UTC by TJS Security Command Center