INTELLIGENCE BRIEFING
Security Command Center
TLP:CLEAR
2026-04-05 18:14 UTC

"TrueChaos" Campaign Leverages Zero-Day in TrueConf, Targets Southeast Asian Governments

THREAT CAMPAIGN | **CRITICAL** | CVSS 8.8

SCC Item ID	SCC-CAM-2026-0151
Type	Threat Campaign
Severity	CRITICAL
CVSS Base Score	8.8
Affected Products	TrueConf video conferencing software (specific version unconfirmed, source verification required)
Discovery Source	Gemini

Executive Summary

A threat campaign tracked as 'TrueChaos' is actively exploiting an unpatched zero-day in TrueConf video conferencing software, targeting government and military organizations in Southeast Asia. Attackers have compromised TrueConf's update mechanism to deliver malware, converting a trusted software channel into a distribution vector. CISA KEV inclusion is reported in secondary sources but not confirmed in primary CISA structured data; operators should verify status directly at cisa.gov/known-exploited-vulnerabilities-catalog. Organizations using TrueConf should treat this as an urgent remediation priority regardless of sector.

Technical Analysis

The 'TrueChaos' campaign exploits an unpatched zero-day in TrueConf video conferencing software (specific version unconfirmed; source verification required). The attack vector targets the software's update mechanism: adversaries replace a legitimate update package with a malicious one, weaponizing the trusted update flow as a malware delivery channel. This aligns with CWE-494 (Download of Code Without Integrity Check) and CWE-345 (Insufficient Verification of Data Authenticity); confidence on CWE mapping is medium, inferred from attack description, not vendor disclosure. MITRE ATT&CK techniques applicable: T1195.002 (Compromise Software Supply Chain), T1072 (Software Deployment Tools), T1199 (Trusted Relationship). No CVE identifier was present in source data; assignment status is unconfirmed. CISA KEV listing is asserted in secondary reporting but is not confirmed in structured source data provided; operators should verify directly at cisa.gov/known-exploited-vulnerabilities-catalog. Attribution is unconfirmed. All technical details derive from T3 secondary news sources; direct vendor advisory or CISA KEV entry was not accessed.

Action Checklist

1. Step 1: Containment, Identify all systems running TrueConf across your environment immediately. Disable or block TrueConf's automatic update function at the host and network level until a confirmed patch or vendor advisory is available. If TrueConf is deployed in government, defense, or high-sensitivity segments, disconnect those endpoints from broader network access pending investigation. Verify directly with TrueConf's official vendor portal (trueconf.com) for any published advisory; do not rely solely on third-party reporting for patch status.
2. Step 2: Detection, Audit software deployment and update logs on all TrueConf hosts for unexpected update packages, unsigned binaries, or update requests originating from non-vendor infrastructure. Review endpoint detection logs for process execution chains spawned from TrueConf update processes (look for child processes inconsistent with normal update behavior). Check network logs for outbound connections from TrueConf processes to non-TrueConf IP ranges or domains. No confirmed IOCs were available in source data; treat any anomalous TrueConf update activity as suspicious pending vendor confirmation.
3. Step 3: Eradication, Apply the official TrueConf patch immediately upon vendor release; do not use automated update channels until the update integrity mechanism is confirmed fixed. If compromise is suspected, remove TrueConf from affected systems and re-image hosts where unauthorized code execution may have occurred. Revoke any credentials or tokens accessible to TrueConf processes on compromised hosts.
4. Step 4: Recovery, After patching, validate update package integrity using vendor-published checksums or signatures before re-enabling update functionality. Monitor TrueConf processes post-remediation for 30 days using behavioral detection rules focused on anomalous child process creation and unexpected outbound network activity. Confirm CISA KEV status directly at cisa.gov and align remediation timelines with any active federal directive.
5. Step 5: Post-Incident, Evaluate software update integrity controls across all third-party applications in your environment, particularly those used in sensitive or privileged contexts. This campaign exposes a control gap in CWE-494/CWE-345: absence of cryptographic verification on software update payloads. Map findings to NIST SP 800-53 SI-7 (Software, Firmware, and Information Integrity) and SA-12 (Supply Chain Protection). Update vendor risk assessments for communications and collaboration tools. Require code-signing verification as a procurement requirement for future software acquisitions, particularly for communications and collaboration tools.

IR / Forensic Enrichment

Triage Priority	IMMEDIATE
Escalation Criteria	Escalate to CISO and legal counsel immediately if forensic evidence confirms malware execution from a TrueConf update process on any host with access to classified, PII, PHI, or defense-related data, or if the CISA KEV directive deadline cannot be met — both conditions trigger potential breach notification obligations and mandatory federal reporting requirements.

Recovery Notes	Before returning any TrueConf host to production, validate the installed version matches the vendor-released patch and verify the update server configuration points exclusively to trueconf.com infrastructure — not any alternate endpoint written during the compromise. Maintain Sysmon-based behavioral monitoring scoped to TrueConf process trees for a minimum of 30 days post-remediation, reviewing weekly for anomalous child process creation (Sysmon Event ID 1) or unexpected outbound connections (Sysmon Event ID 3) that could indicate a persistent implant surviving the re-image or patch. If any host shows indicators of persistence — new scheduled tasks, services, or registry run keys created by TrueConf-related processes — treat it as an active compromise and re-initiate containment rather than continuing recovery.
Forensic Artifacts	TrueConf application update logs at `C:\ProgramData\TrueConf\logs\` and `%APPDATA%\TrueConf\` — these will record the update server URL, package filename, and timestamp of any update delivered via the hijacked update mechanism, providing the primary timeline anchor for this campaign's delivery vector. | Windows Prefetch files for TrueConf updater executables at `C:\Windows\Prefetch\TRUECONFUPDATER.EXE-*.pf` — these record execution timestamps and libraries loaded by the update process, revealing whether a malicious payload was staged and executed through the legitimate updater binary. | Sysmon Event ID 1 (Process Create) logs showing the full process tree rooted at TrueConf update processes — the TrueChaos campaign's hallmark is malware delivered through the update channel, so any non-standard child processes (cmd.exe, powershell.exe, rundll32.exe) spawned from TrueConf updater executables are the primary execution-phase artifact. | Network flow records or pcap captures showing outbound DNS queries and TCP/TLS connections initiated by TrueConf process PIDs — connections to non-trueconf.com / non-trueconf.ru domains during or immediately following an update cycle indicate the update mechanism was redirected to attacker-controlled infrastructure. | File system artifacts in `%TEMP%`, `C:\Windows\Temp\`, and the TrueConf installation directory (`C:\Program Files\TrueConf\`) — specifically any PE executables, DLLs, or script files written during the update window whose SHA-256 hashes do not match vendor-published checksums, as these represent the malware payload dropped via the compromised update channel.

Per-Action IR Details

Step 1: Containment — Identify all systems running TrueConf across your environment immediately. Disable or block TrueConf's automatic update function at the host and network level until a vetted patch or vendor advisory is available. If TrueConf is deployed in government, defense, or high-sensitivity segments, isolate those endpoints from broader network access pending investigation. Verify directly with TrueConf's official vendor portal (trueconf.com) for any published advisory; do not rely solely on third-party reporting for patch status.

NIST Phase: Containment

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

Controls: NIST IR-4 (Incident Handling), NIST CM-7 (Least Functionality), NIST SI-7 (Software, Firmware, and Information Integrity), CIS 1.1 (Establish and Maintain Detailed Enterprise Asset Inventory), CIS 4.4 (Implement and Manage a Firewall on Servers)

Compensating: Run `wmic product where 'name like "%TrueConf%"' get name,version,installdate` (Windows) or `dpkg -l | grep -i trueconf` (Linux) across all endpoints using a free RMM tool or PSExec sweep to enumerate TrueConf installations. Block TrueConf update domains and known update infrastructure at the perimeter firewall using a deny-all rule for outbound traffic from TrueConf process paths (default: `C:\Program Files\TrueConf\`). A 2-person team can use osquery with the query `SELECT name, version, install_date FROM programs WHERE name LIKE '%TrueConf%';` deployed via osquery's file carver to enumerate all hosts in under an hour.

Evidence: Before isolating endpoints, capture: (1) a full process list snapshot (`tasklist /v /fo csv > prelist.csv`) to record TrueConf process state and any anomalous child processes at time of discovery; (2) active network connections from TrueConf processes (`netstat -bano | findstr /i trueconf`) to document any live C2 or non-vendor update connections; (3) the TrueConf update configuration file (typically located at `C:\ProgramData\TrueConf\` or equivalent) to establish the configured update endpoint URL before any remediation alters it. Preserve these artifacts to a write-protected network share before blocking network access.

Step 2: Detection — Audit software deployment and update logs on all TrueConf hosts for unexpected update packages, unsigned binaries, or update requests originating from non-vendor infrastructure. Review endpoint detection logs for process execution chains spawned from TrueConf update processes (look for child processes inconsistent with normal update behavior). Check network logs for outbound connections from TrueConf processes to non-TrueConf IP ranges or domains. No confirmed IOCs were available in source data — treat any anomalous TrueConf update activity as suspicious pending vendor confirmation.

NIST Phase: Detection Analysis

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

Controls: NIST IR-5 (Incident Monitoring), NIST AU-6 (Audit Record Review, Analysis, and Reporting), NIST AU-12 (Audit Record Generation), NIST SI-4 (System Monitoring), CIS 8.2 (Collect Audit Logs), CIS 7.1 (Establish and Maintain a Vulnerability Management Process)

Compensating: Deploy Sysmon with a configuration that logs Event ID 1 (Process Create) and Event ID 3 (Network Connection) for TrueConf processes. Query Windows Security Event Log for Event ID 4688 (Process Creation) filtering on parent processes matching TrueConf executable paths (e.g., `TrueConfUpdater.exe`, `TrueConf.exe`) to surface anomalous child processes such as `cmd.exe`, `powershell.exe`, or `mshta.exe`. Use this Sigma-compatible detection logic: `ParentImage|endswith: 'TrueConfUpdater.exe' AND Image|endswith: ('cmd.exe','powershell.exe','wscript.exe','mshta.exe')`. For network detection, run Wireshark or `tcpdump -i any -w trueconf_capture.pcap` filtered on TrueConf process PIDs and inspect for DNS queries or TLS handshakes to non-`trueconf.com` or non-`trueconf.ru` domains during an update cycle.

Evidence: Collect before concluding detection phase: (1) TrueConf application and update logs from `C:\ProgramData\TrueConf\logs\` or `%APPDATA%\TrueConf\` — look for entries referencing non-canonical update server hostnames or IP addresses; (2) Windows Event Log entries (Event ID 4688, 7045 for new service installs, and 4697) from the time window surrounding any TrueConf update event; (3) file system artifacts in the TrueConf installation and temp directories (`%TEMP%`, `C:\Windows\Temp\`) for executables or DLLs written during update operations with creation timestamps correlating to update log entries; (4) DNS query logs from the host or perimeter resolver for domains queried by TrueConf processes that do not resolve to known TrueConf/vendor infrastructure.

Step 3: Eradication — Apply the official TrueConf patch immediately upon vendor release; do not use automated update channels until the update integrity mechanism is confirmed fixed. If compromise is suspected, remove TrueConf from affected systems and re-image hosts where unauthorized code execution may have occurred. Revoke any credentials or tokens accessible to TrueConf processes on compromised hosts.

NIST Phase: Eradication

Reference: NIST 800-61r3 §3.4 — Eradication and Recovery

Controls: NIST IR-4 (Incident Handling), NIST SI-2 (Flaw Remediation), NIST SI-7 (Software, Firmware, and Information Integrity), NIST AC-2 (Account Management), CIS 7.2 (Establish and Maintain a Remediation Process), CIS 7.4 (Perform Automated Application Patch Management)

Compensating: For credential revocation without an enterprise PAM tool: (1) enumerate all service accounts and user tokens that TrueConf processes ran under using `whoami /all` captured pre-eradication, then force password resets via `net user /random` or Active Directory bulk reset; (2) search for credential material in TrueConf configuration files using `findstr /si /r "password\|token\|secret\|api_key" C:\ProgramData\TrueConf\*` and revoke any identified secrets in downstream systems; (3) for hosts requiring re-image, boot from a known-good WinPE environment and image from a gold baseline stored offline — do not trust the running OS to validate its own integrity given the update-channel compromise vector of this campaign.

Evidence: Before re-imaging or removing TrueConf, preserve: (1) a full memory capture using WinPmem (`winpmem_mini_x64.exe output.raw`) from hosts where unauthorized code execution is suspected, as TrueChaos malware delivered via the update mechanism may reside in-memory or inject into TrueConf process space; (2) a forensic image of the TrueConf installation directory and `%APPDATA%\TrueConf\` using a tool such as `robocopy` with timestamp preservation (`/DCOPY:T`) before uninstall destroys artifacts; (3) a copy of any binaries written to disk during update operations — hash each file with `certutil -hashfile SHA256` and compare against vendor-published hashes once available; (4) Windows Prefetch files (`C:\Windows\Prefetch\TRUECONFUPDATER.EXE-*.pf`) which will record execution history and loaded libraries for the update process.

Step 4: Recovery — After patching, validate update package integrity using vendor-published checksums or signatures before re-enabling update functionality. Monitor TrueConf processes post-remediation for 30 days using behavioral detection rules focused on anomalous child process creation and unexpected outbound network activity. Confirm CISA KEV status directly at cisa.gov and align remediation timelines with any active federal directive.

NIST Phase: Recovery

Reference: NIST 800-61r3 §3.5 — Recovery

Controls: NIST IR-4 (Incident Handling), NIST SI-7 (Software, Firmware, and Information Integrity), NIST SI-2 (Flaw Remediation), NIST AU-6 (Audit Record Review, Analysis, and Reporting), CIS 7.3 (Perform Automated Operating System Patch Management), CIS 7.4 (Perform Automated Application Patch Management)

Compensating: Validate patch integrity before deployment using `certutil -hashfile SHA256` and compare output against the checksum published in TrueConf's official advisory on trueconf.com — do not accept checksums from any third-party source. For 30-day behavioral monitoring without EDR, run a persistent Sysmon logging profile capturing Event IDs 1, 3, 7 (Image Load), and 11 (File Created) scoped to TrueConf process paths, and pipe output to a local log aggregator or Windows Event Forwarding (WEF) collector. Write a scheduled PowerShell task that runs nightly: `Get-WinEvent -LogName 'Microsoft-Windows-Sysmon/Operational' | Where-Object {$_.Message -match 'TrueConf' -and $_.Id -in @(1,3,7)} | Export-Csv C:\IRLogs\trueconf_monitor.csv -Append` to build a 30-day behavioral baseline for analyst review.

Evidence: Capture before returning systems to production: (1) the cryptographic hash (SHA-256) of the applied patch installer sourced directly from trueconf.com, recorded in the incident ticket as the verified-clean baseline; (2) a post-patch process tree snapshot (`tasklist /v /fo csv`) and network baseline (`netstat -bano`) from each remediated host to document the expected clean state for comparison during the 30-day monitoring period; (3) confirmation screenshot or export of the CISA KEV catalog entry for this vulnerability from cisa.gov/known-exploited-vulnerabilities-catalog, timestamped, to document regulatory alignment and remediation deadline for after-action records.

Step 5: Post-Incident — Evaluate software update integrity controls across all third-party applications in your environment, particularly those used in sensitive or privileged contexts. This campaign exposes a control gap in CWE-494/CWE-345: absence of cryptographic verification on software update payloads. Map findings to NIST SP 800-53 SI-7 (Software, Firmware, and Information Integrity) and SA-12 (Supply Chain Protection). Update vendor risk assessments for communications and collaboration tools. Consider requiring code-signing verification as a procurement requirement for future software acquisitions.

NIST Phase: Post Incident

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

Controls: NIST IR-4 (Incident Handling), NIST IR-8 (Incident Response Plan), NIST SI-7 (Software, Firmware, and Information Integrity), NIST SA-12 (Supply Chain Protection), NIST RA-3 (Risk Assessment), CIS 2.1 (Establish and Maintain a Software Inventory), CIS 2.2 (Ensure Authorized Software is Currently Supported), CIS 7.1 (Establish and Maintain a Vulnerability Management Process)

Compensating: Audit all third-party applications in your software inventory (CIS 2.1) for update-channel integrity verification using a manual checklist: for each communication or collaboration tool, verify whether the vendor documents code-signing of update packages and whether your deployment enforces signature validation before execution. Create a YARA rule targeting the CWE-494 pattern — unsigned PE executables written to application

installation directories by application-owned processes — and run it weekly via `yara64.exe unsigned_update.yar C:\Program Files\` across managed endpoints. Add a vendor security questionnaire item requiring documented cryptographic update verification (referencing CWE-345 and NIST SI-7) to all future software procurement evaluations, specifically for communications and collaboration tools matching TrueConf's deployment profile.

Evidence: For the lessons-learned record, preserve: (1) the complete timeline of TrueConf update events from application logs and Windows Event Logs across all affected hosts, reconstructed to show when the hijacked update was first delivered; (2) the software inventory state (CIS 2.1) at the time of the incident — specifically which versions of TrueConf were deployed and whether version management controls were in place; (3) any vendor communications from TrueConf received during the incident, archived to the incident case file, to assess vendor notification timeliness and advisory quality for future vendor risk scoring; (4) the MITRE ATT&CK technique mapping for this campaign — specifically T1195.002 (Supply Chain Compromise: Compromise Software Supply Chain) and T1072 (Software Deployment Tools) — documented as detection gaps to drive new Sigma rule development.

Detection Guidance

No confirmed IOCs were present in the source data for this campaign. Detection should focus on behavioral indicators specific to the attack vector: update mechanism hijacking. Key areas to monitor: (1) TrueConf update process spawning unexpected child processes (e.g., cmd.exe, powershell.exe, mshta.exe, or scripting engines); (2) TrueConf update traffic resolving to IP addresses or domains outside TrueConf's documented update infrastructure, compare against official vendor documentation; (3) unsigned or untrusted executables written to disk by TrueConf update processes; (4) outbound network connections from TrueConf processes to newly registered or low-reputation domains. On Windows endpoints, review Sysmon Event ID 1 (Process Create) with ParentImage containing TrueConf paths, and Event ID 3 (Network Connection) for TrueConf processes. EDR telemetry should be queried for execution chains originating from TrueConf installation directories. Given the MITRE mapping to T1195.002 and T1072, also audit software deployment infrastructure for unauthorized package substitution. All detection logic should be treated as hypothetical until confirmed IOCs or a vendor advisory are published.

Indicators of Compromise

Type	Value	Context	Confidence
NOTE	`No confirmed IOCs available`	Source data contained no verified IP addresses, domains, file hashes, or URLs associated with TrueChaos campaign infrastructure. IOC data may be available from TrueConf's official advisory or CISA KEV entry — verify directly. Do not treat absence of IOCs as absence of threat.	LOW

Framework Mappings

MITRE-ATTACK

- **T1199** — Trusted Relationship
- **T1072** — Software Deployment Tools

- **T1195.002** — Compromise Software Supply Chain

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
- **CM-3** — Configuration Change Control
- **IR-5** — Incident Monitoring

OWASP-TOP10-2021

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

CIS-V8

- **2.5** — Allowlist Authorized Software
- **2.6** — Allowlist Authorized Libraries
- **7.3** — Perform Automated Operating System Patch Management
- **7.4** — Perform Automated Application Patch Management

ISO-27001-2022

- **A.8.8** — Management of technical vulnerabilities

NIST-CSF-2

- **DE.AE-08** — Incidents are declared when adverse events meet the defined incident criteria

MITRE ATT&CK Mapping

Technique ID	Technique Name	Tactic
T1199	Trusted Relationship	Initial-Access
T1072	Software Deployment Tools	Execution
T1195.002	Compromise Software Supply Chain	Initial-Access

Sources

Source	URL	Tier
TrueConf Zero-Day Exploited in Attacks on Southeast Asian ...	https://thehackernews.com/2026/03/trueconf-zero-day-exploited-in-at...	T3
Experts find flaw in video conferencing tool used by ... - TechRadar	https://www.techradar.com/pro/security/by-replacing-a-legitimate-up...	T3

Source	URL	Tier
TrueConf Zero-Day Exploited in Asian Government Attacks	https://www.securityweek.com/trueconf-zero-day-exploited-in-asian-g...	T3
CISA gives agencies two weeks to patch video conferencing bug ...	https://therecord.media/trueconf-cyberattack-cisa-hackers	T3
TrueConf zero-day vulnerability exploited to target government ...	https://www.helpnetsecurity.com/2026/04/02/trueconf-zero-day-vulner...	T3

Generated 2026-04-05 18:14 UTC by TJS Security Command Center