INTELLIGENCE BRIEFING
Security Command Center
TLP:CLEAR
2026-03-29 18:34 UTC

Red Menshen’s BPFDoor Evolution: Kernel-Level Sleeper Cells Inside Telecom Backbone Infrastructure

THREAT CAMPAIGN | **HIGH** | CVSS 9.5

SCC Item ID	SCC-CAM-2026-0107
Type	Threat Campaign
Severity	HIGH
CVSS Base Score	9.5
Affected Products	Linux-based telecom and enterprise systems; initial access via Ivanti VPN appliances, Cisco, Juniper Networks, Fortinet, VMware, Palo Alto Networks, Apache Struts
Published	2026-03-26
Discovery Source	Rss

Executive Summary

Red Menshen (Earth Bluecrow), a China-nexus APT group, has deployed an advanced variant of the BPFDoor kernel-level backdoor against telecom backbone infrastructure across the Middle East and Asia, with government entities assessed as the primary collection target. The implant operates below the visibility of standard security tools, embedding activation triggers inside HTTPS traffic and conducting lateral movement over ICMP, making it invisible to userspace monitoring tools (ps, netstat) but detectable via kernel-level auditing (bpftool, eBPF probes). New support for SCTP, a telecom signaling protocol, elevates the threat beyond network espionage to potential subscriber-level surveillance, with serious implications for any organization operating or relying on regional telecom infrastructure.

Technical Analysis

BPFDoor is a passive backdoor that attaches to the Linux kernel via eBPF, intercepting network packets before they reach userspace. This eliminates the need for open listening ports and makes the implant invisible to standard process enumeration (ps, netstat, ss). The latest variant, attributed to Red Menshen / Earth Bluecrow (MITRE G0112), replaces earlier magic-packet activation with triggers embedded in HTTPS traffic (T1071.001), substantially reducing the detection surface for network-layer tools. Lateral movement is conducted over ICMP (T1095), minimizing socket and process artifacts visible to EDR platforms. Newly documented SCTP support (T1095) indicates positioning within telecom signaling stacks adjacent to SS7 and Diameter, raising the risk of subscriber data interception. Persistence is achieved through kernel-resident mechanisms (T1547, T1543),

consistent with CWE-912 (Hidden Functionality) and CWE-284 (Improper Access Control). The implant also employs masquerading (T1036, T1036.005), obfuscation (T1027), and abuse of elevation control (T1548) to resist removal. Initial access vectors are assessed to include perimeter appliance exploitation (T1190, T1133) targeting Ivanti Connect Secure, Cisco, Juniper, Fortinet, VMware, Palo Alto Networks, and Apache Struts, consistent with this group's documented TTPs. No CVE is directly tied to this BPFDoor variant. CWE references: CWE-284 (Improper Access Control), CWE-693 (Protection Mechanism Failure; reflects kernel security model bypass via eBPF injection), CWE-912 (Hidden Functionality). Source confidence: high on campaign activity; primary threat intelligence research via The Hacker News (March 2026), pending CISA or MITRE ATT&CK group-level corroboration.

Action Checklist

1. Step 1: Containment, Audit all Linux-based systems in telecom and network backbone roles for unexpected kernel modules and eBPF programs. Immediately isolate systems that cannot be confirmed clean. Verify patch status on all perimeter appliances (Ivanti Connect Secure, Cisco ASA/FTD, Juniper SRX, Fortinet FortiGate, VMware ESXi/NSX, Palo Alto PAN-OS, Apache Struts deployments) and apply any outstanding security updates from vendor advisories. Restrict inbound ICMP and SCTP where not operationally required.
2. Step 2: Detection, Run 'bpftool prog list' and 'bpftool map list' on all Linux hosts to enumerate active eBPF programs; any unexpected entries warrant immediate investigation. Audit loaded kernel modules via 'lsmod' and cross-reference against known-good baselines. Search SIEM for anomalous ICMP traffic between internal hosts (lateral movement indicator) and unexpected SCTP session establishment. Review perimeter appliance logs for exploitation attempts against CVEs associated with Ivanti, Fortinet, Cisco, Juniper, VMware, Palo Alto, and Apache Struts from 2021 onward. Identify process masquerading (T1036.005): compare running process names against expected binary paths using EDR telemetry.
3. Step 3: Eradication, For confirmed BPFDoor infections, full OS reinstallation from verified clean media is recommended; kernel-level implants resist standard malware removal. Before reinstalling, preserve forensic images for analysis. Revoke and rotate all credentials (SSH keys, API tokens, application passwords) that may have been accessible to or used on compromised hosts, prioritizing service accounts and privileged administrative users. Apply all available patches to identified initial access vectors; consult vendor-specific advisories for Ivanti (https://www.ivanti.com/security), Fortinet (https://fortiguard.fortinet.com), Cisco (https://tools.cisco.com/security/center), Juniper (https://supportportal.juniper.net), Palo Alto (https://security.paloaltonetworks.com), VMware (https://www.vmware.com/security), and Apache (https://httpd.apache.org/security). Remove unauthorized SSH keys and review sudoers and cron configurations for persistence artifacts.
4. Step 4: Recovery, Before returning systems to production, validate eBPF program lists, kernel module inventories, and network socket states against clean baselines. Deploy continuous eBPF monitoring (e.g., Falco with eBPF probe, Tetragon, or equivalent) to detect future kernel-level anomalies. Monitor for reinfection indicators: anomalous ICMP inter-host traffic, unexpected SCTP sessions, and HTTPS traffic patterns inconsistent with application baselines. Confirm perimeter appliance firmware integrity via vendor-provided hash verification where available.
5. Step 5: Post-Incident, This campaign exposes three control gaps: insufficient kernel-level visibility on Linux systems, over-reliance on userspace detection tools (netstat, ps) that BPFDoor bypasses by design, and delayed patching cycles on perimeter appliances. Remediation priorities: deploy eBPF-aware runtime security on all Linux production hosts; implement network segmentation to limit host-to-host ICMP;

establish a 30-day SLA for critical perimeter appliance patches; and map existing controls to MITRE ATT&CK T1014 (Rootkit), T1205 (Traffic Signaling), and T1095 (Non-Application Layer Protocol) to identify remaining detection gaps.

IR / Forensic Enrichment

Triage Priority	IMMEDIATE
Escalation Criteria	Escalate immediately to CISO and legal counsel if any compromised host is confirmed to have processed, stored, or transmitted subscriber PII, call detail records, or government communications metadata — Red Menshen's assessed collection target of government entities via telecom backbone infrastructure creates high-probability regulatory notification obligations under applicable telecommunications and data protection frameworks (e.g., FCC breach notification rules, GDPR Article 33, or regional equivalents).
Recovery Notes	Do not return any Linux telecom backbone host to production without a cryptographically verified clean OS installation and a confirmed-empty 'bpftool prog list' output compared against a known-good baseline — BPFDoor's kernel persistence survives service restarts and standard malware removal, making partial remediation indistinguishable from active infection. Post-recovery monitoring must include continuous capture and analysis of internal ICMP traffic (specifically payload sizes exceeding standard echo request format) and SCTP session logs for a minimum of 90 days, given Red Menshen's documented capability for long-dwell reinfection via re-exploitation of unpatched perimeter appliances. Perimeter appliance firmware integrity must be re-verified weekly for the first month post-recovery using vendor-published hashes, as re-exploitation of residual unpatched Ivanti, Fortinet, or Cisco vulnerabilities represents the most likely reinfection vector.
Forensic Artifacts	/proc/net/packet and /proc/net/raw — BPFDoor attaches a socket-filter eBPF program at the raw socket layer; entries in these proc files with PIDs belonging to processes that no longer appear in /proc (indicating the parent binary was deleted post-execution) are definitive BPFDoor indicators that netstat and ss will not surface | auditd logs filtered on syscall=321 (bpf()) — captures the exact timestamp, UID, and parent process of the BPFDoor eBPF program load event; if auditd was not running, absence of this log is itself a finding documenting the kernel-visibility gap exploited by Red Menshen | LiME memory image (/proc/kcore or lime.ko dump) analyzed for BPFDoor eBPF bytecode and associated map data — in-memory forensics is mandatory for this implant class because BPFDoor deletes its on-disk binary after loading, leaving no file artifact for traditional AV or hash-based detection | Perimeter appliance authentication and session logs (Ivanti ICS /var/log/runtime-logs/, Fortinet FortiGate traffic logs, Cisco ASA syslog) covering the 2021-to-present window for the specific CVEs exploited by Red Menshen as initial access vectors — these logs establish the intrusion timeline and patient-zero host identification critical to scoping the full blast radius across telecom backbone infrastructure | tcpdump pcap captures of internal network segments filtered on 'proto 1' (ICMP) with payload length greater than 8 bytes — BPFDoor lateral movement uses ICMP as a covert channel with magic-byte activation sequences embedded in the data field, a pattern invisible to flow-based monitoring but recoverable from full-packet capture retained on backbone network taps or span ports

Per-Action IR Details

Step 1: Containment — Audit all Linux-based systems in telecom and network backbone roles for unexpected kernel modules and eBPF programs. Immediately isolate systems that cannot be confirmed clean. Verify patch status on all perimeter appliances (Ivanti Connect Secure, Cisco ASA/FTD, Juniper SRX, Fortinet

FortiGate, VMware ESXi/NSX, Palo Alto PAN-OS, Apache Struts deployments) and apply any outstanding security updates from vendor advisories. Restrict inbound ICMP and SCTP where not operationally required.

NIST Phase: Containment

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

Controls: NIST IR-4 (Incident Handling), NIST SI-4 (System Monitoring), NIST CM-7 (Least Functionality), CIS 4.4 (Implement and Manage a Firewall on Servers), CIS 7.1 (Establish and Maintain a Vulnerability Management Process)

Compensating: On each Linux telecom host, run: 'sudo bpftool prog list' and 'sudo bpftool map list' — any program of type 'socket_filter' or 'xdp' with an unrecognized name or pinned path outside /sys/fs/bpf/ warrants immediate isolation. Block ICMP at the perimeter using iptables: 'iptables -A INPUT -p icmp --icmp-type echo-request -j DROP' and block SCTP with 'iptables -A INPUT -p sctp -j DROP'. For Ivanti Connect Secure patch verification without a SIEM, pull the running version via the admin UI and cross-reference against Ivanti's published advisory page for ICS vulnerabilities from 2021 onward.

Evidence: Before isolating any host, capture: (1) full output of 'bpftool prog list --json' and 'bpftool map list --json' saved to timestamped files — BPFDoor registers socket-filter eBPF programs that will not appear in standard network socket listings; (2) 'lsmod' output and '/proc/modules' contents for comparison against a known-good kernel module baseline, focusing on modules with generic or misspelled names; (3) full network socket state via 'ss -anp' and 'cat /proc/net/raw' — BPFDoor bypasses netstat but raw socket entries in /proc/net/raw will reflect its socket_filter attachment; (4) perimeter appliance authentication and VPN session logs from the 2021-onward window covering Ivanti CVEs (e.g., CVE-2023-46805, CVE-2024-21887) and Fortinet CVEs (e.g., CVE-2022-40684) for source IPs that subsequently appear in internal ICMP lateral movement traffic.

Step 2: Detection — Run 'bpftool prog list' and 'bpftool map list' on all Linux hosts to enumerate active eBPF programs; any unexpected entries warrant immediate investigation. Audit loaded kernel modules via 'lsmod' and cross-reference against known-good baselines. Search SIEM for anomalous ICMP traffic between internal hosts (lateral movement indicator) and unexpected SCTP session establishment. Review perimeter appliance logs for exploitation attempts against CVEs associated with Ivanti, Fortinet, Cisco, Juniper, VMware, Palo Alto, and Apache Struts from 2021 onward. Hunt for process masquerading (T1036.005): compare running process names against expected binary paths using EDR telemetry.

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-12 (Audit Record Generation), NIST IR-5 (Incident Monitoring), CIS 8.2 (Collect Audit Logs), CIS 7.1 (Establish and Maintain a Vulnerability Management Process)

Compensating: Without SIEM/EDR: (1) Deploy Sysmon on any Linux hosts running systemd with the sysmon-for-linux build, capturing process creation events to detect processes whose executable path does not match their name (T1036.005 — BPFDoor variants masquerade as legitimate daemons such as 'kdmtmpflush' or 'avahi-daemon'). (2) Use Wireshark or tcpdump on a tap port or span: 'tcpdump -i eth0 -w capture.pcap proto 1 or proto 132' to capture all ICMP (proto 1) and SCTP (proto 132) for offline analysis — BPFDoor's magic-byte activation trigger arrives embedded in ICMP or SCTP payloads, so filter for ICMP packets with payloads exceeding 8 bytes. (3) Deploy the public YARA rule set for BPFDoor (available from Trend Micro's BPFDoor disclosure) against all ELF binaries in /tmp, /dev/shm, and /var/tmp. (4) Use osquery with: 'SELECT name, path, cmdline FROM processes WHERE path NOT LIKE /usr/%' to surface process masquerading without EDR.

Evidence: Before concluding detection scope: (1) Capture /proc/[pid]/maps and /proc/[pid]/exe symlink resolution for all suspicious processes — BPFDoor deletes its binary on disk post-execution so the exe link will point to a deleted inode, visible as '/path/to/binary (deleted)'; (2) Extract /proc/net/packet entries which will show BPFDoor's raw socket registration at protocol layer with an unexpected PID owner; (3) Pull kernel audit logs from auditd (if enabled) filtering on syscall 321 (bpf()) to identify when the malicious eBPF program was loaded and the originating process; (4) Collect pcap evidence of internal host-to-host ICMP traffic with payload sizes inconsistent with standard ping (BPFDoor magic bytes vary by variant but are typically 4-byte sequences embedded in the ICMP data field); (5) Pull VPN authentication logs from Ivanti Connect Secure (/var/log/ on the appliance or syslog forwarding destination) for the initial access

window to establish patient-zero timing.

Step 3: Eradication — For confirmed BPFDoor infections, full OS reinstallation from verified clean media is recommended; kernel-level implants resist standard malware removal. Before reinstalling, preserve forensic images for analysis. Revoke and rotate all credentials accessible from compromised hosts. Apply all available patches to identified initial access vectors; consult vendor-specific advisories for Ivanti (ivanti.com/security), Fortinet (fortiguard.fortinet.com), Cisco (tools.cisco.com/security/center), Juniper (supportportal.juniper.net), Palo Alto (security.paloaltonetworks.com), VMware (vmware.com/security), and Apache (httpd.apache.org/security). Remove unauthorized SSH keys and review sudoers and cron configurations for persistence artifacts.

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 IA-5 (Authenticator Management), CIS 5.1 (Establish and Maintain an Inventory of Accounts), CIS 7.3 (Perform Automated Operating System Patch Management), CIS 7.4 (Perform Automated Application Patch Management)

Compensating: Before wiping: acquire a full disk image using 'dd if=/dev/sda | gzip > /mnt/external/host-forensic-$(hostname)-$(date +%Y%m%d).img.gz' over a network mount to preserve evidence. For credential rotation without a PAM/vault: use 'passwd -l [username]' to immediately lock all local accounts on compromised hosts, then audit '/etc/ssh/authorized_keys' and all user '~/.ssh/authorized_keys' files with 'find / -name authorized_keys -exec cat {} \;' — Red Menshen has been observed planting SSH keys for persistent re-entry. Audit cron with 'crontab -l' for all users and check '/etc/cron.d/', '/etc/cron.daily/', and '/var/spool/cron/' for entries referencing paths in /tmp or /dev/shm, which BPFDoor variants use as staging directories. For Ivanti ICS, follow Ivanti's factory reset and reimaging procedure specifically (not just patch application) given confirmed exploitation of CVE-2023-46805/CVE-2024-21887.

Evidence: Before beginning eradication: (1) Image all volatile memory using LiME (Linux Memory Extractor) kernel module to capture the live BPFDoor eBPF bytecode, associated maps, and any in-memory command-and-control parameters that will be lost on reboot — 'insmod lime.ko path=/mnt/external/mem.lime format=lime'; (2) Extract /sys/fs/bpf/ directory tree in full — BPFDoor variants that use pinned eBPF maps will leave map files here that survive process termination and contain C2 configuration data; (3) Collect all authorized_keys files and /etc/sudoers.d/ entries added after the assessed initial access date; (4) Preserve full cron directories and systemd unit files in /etc/systemd/system/ and /usr/lib/systemd/system/ for any units with ExecStart paths pointing to non-standard directories; (5) Capture perimeter appliance running configs and firmware version strings via CLI before patching, to document the exploited state for the incident record.

Step 4: Recovery — Before returning systems to production, validate eBPF program lists, kernel module inventories, and network socket states against clean baselines. Deploy continuous eBPF monitoring (e.g., Falco with eBPF probe, Tetragon, or equivalent) to detect future kernel-level anomalies. Monitor for reinfection indicators: anomalous ICMP inter-host traffic, unexpected SCTP sessions, and HTTPS traffic patterns inconsistent with application baselines. Confirm perimeter appliance firmware integrity via vendor-provided hash verification where available.

NIST Phase: Recovery

Reference: NIST 800-61r3 §3.5 — Recovery

Controls: NIST IR-4 (Incident Handling), NIST SI-4 (System Monitoring), NIST SI-7 (Software, Firmware, and Information Integrity), NIST CP-10 (System Recovery and Reconstitution), CIS 4.2 (Establish and Maintain a Secure Configuration Process for Network Infrastructure), CIS 7.2 (Establish and Maintain a Remediation Process)

Compensating: For teams without commercial eBPF runtime security: deploy Falco (free, CNCF project) with the eBPF probe enabled — create a custom Falco rule to alert on any process invoking the bpf() syscall that is not in an approved list (e.g., only 'bpftool', 'falco', 'tetragon' should call bpf()). Establish a clean-state baseline by running 'bpftool prog list --json > /etc/security/baselines/ebpf-baseline-$(date +%Y%m%d).json' immediately after OS reinstallation and

before any application deployment. For firmware integrity verification of Ivanti ICS without automated tooling, download the vendor-published SHA-256 hash from the Ivanti security portal and compare against the installed image hash computed on-appliance via the admin CLI 'system diagnostics' or equivalent. Use tcpdump with a persistent capture job: 'tcpdump -i any -s 0 proto 1 -w /var/log/icmp-monitor.pcap &' to maintain a rolling capture of all ICMP for reinfection detection.

Evidence: During recovery validation, collect and retain: (1) Post-reinstall 'bpftool prog list --json' and 'bpftool map list --json' outputs as signed baselines — any future deviation is a reinfection indicator; (2) Network flow data (NetFlow/IPFIX from backbone routers or tcpdump captures) covering the 30 days post-recovery specifically for ICMP type 8 (echo request) traffic between internal telecom backbone hosts with payload sizes greater than 8 bytes, which indicates BPFDoor magic-byte signaling; (3) Perimeter appliance firmware hash verification outputs with timestamps, retained as integrity attestation records; (4) Falco alert logs or equivalent eBPF monitoring output from the first 72 hours post-recovery to establish normal eBPF activity baseline and detect re-establishment of Red Menshen's socket-filter programs.

Step 5: Post-Incident — This campaign exposes three control gaps: insufficient kernel-level visibility on Linux systems, over-reliance on userspace detection tools (netstat, ps) that BPFDoor bypasses by design, and delayed patching cycles on perimeter appliances. Remediation priorities: deploy eBPF-aware runtime security on all Linux production hosts; implement network segmentation to limit host-to-host ICMP; establish a 30-day SLA for critical perimeter appliance patches; and map existing controls to MITRE ATT&CK T1014 (Rootkit), T1205 (Traffic Signaling), and T1095 (Non-Application Layer Protocol) to identify remaining detection gaps.

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-2 (Flaw Remediation), NIST SI-4 (System Monitoring), NIST AU-6 (Audit Record Review, Analysis, and Reporting), CIS 7.1 (Establish and Maintain a Vulnerability Management Process), CIS 7.2 (Establish and Maintain a Remediation Process), CIS 8.2 (Collect Audit Logs)

Compensating: For the lessons-learned process without a dedicated threat intel platform: (1) Build a Sigma rule set targeting BPFDoor TTPs — specifically rules for T1205 (traffic signaling via ICMP magic bytes) and T1095 (SCTP C2) — and publish internally for use with any log aggregator; the MITRE ATT&CK Navigator layer for Red Menshen/Earth Bluecrow (if available from Trend Micro's public disclosure) provides the starting ATT&CK mapping. (2) Formalize the 30-day patch SLA as a written policy change referencing the specific perimeter appliances exploited in this campaign (Ivanti ICS, Fortinet FortiGate, Cisco ASA/FTD) and assign ownership to named individuals. (3) Conduct a tabletop exercise specifically simulating BPFDoor-style kernel backdoor deployment to validate that the new Falco/Tetragon controls would have detected this intrusion at the initial access or lateral movement phase. (4) Submit IOCs (BPFDoor ELF hashes, magic byte sequences, C2 IP addresses) to sector ISACs (e.g., Communications ISAC for telecom) per NIST IR-6 (Incident Reporting) obligations.

Evidence: For the post-incident report and future detection improvement, retain: (1) All forensic images, memory captures, and eBPF artifact dumps collected during the incident — these are the ground truth for developing BPFDoor-specific YARA and Sigma signatures; (2) Timeline reconstruction correlating Ivanti/Fortinet/Cisco exploitation events (from perimeter logs) to first observed BPFDoor eBPF program load (from auditd bpf() syscall logs) to first observed internal ICMP lateral movement — this dwell time calculation is critical for breach notification SLA assessment; (3) Complete inventory of all credentials, SSH keys, and service accounts present on confirmed-compromised hosts at time of discovery — this scopes the credential rotation requirement and feeds identity risk assessment; (4) Documentation of all userspace tool outputs (netstat, ps, lsmod) collected during the incident that failed to surface BPFDoor artifacts, retained as evidence for the control gap finding and the case for eBPF-aware tooling investment.

Detection Guidance

Primary detection surface is the kernel and network layers, not process lists. Run 'bpftool prog list' and 'bpftool map list' on all Linux systems; BPFDoor attaches eBPF programs that will not appear in standard ps or netstat output. Cross-reference loaded kernel modules ('lsmod') against a known-good baseline. Network-layer indicators: hunt for ICMP traffic between internal hosts that lacks a corresponding ping utility process, and any SCTP session establishment on systems that have no legitimate signaling function. HTTPS traffic behavioral anomalies (unusual source/destination pairs, odd packet sizes consistent with covert triggers) may indicate activation traffic, but are difficult to distinguish without deep packet inspection and baseline profiling. EDR behavioral indicators: look for processes with names matching legitimate system binaries but executing from unexpected paths (T1036.005), and for privilege escalation events (T1548) on hosts with no corresponding administrative activity. SIEM correlation: alert on any bpftool or eBPF-related commands executed interactively on production Linux hosts; legitimate administrative use is rare and should be investigated. Threat intelligence: no public IOC hashes, domains, or IP addresses have been published by primary threat researchers or CISA as of this item's publication date; treat any IOCs released by CISA or primary researchers as high-confidence when available.

Indicators of Compromise

Type	Value	Context	Confidence
DOMAIN	`No confirmed IOCs available in source data`	Primary threat intelligence research has not publicly released confirmed file hashes, IP addresses, or domains as of the item date (March 2026). Monitor CISA alerts, MITRE ATT&CK G0112 updates, and the originating research publication for IOC releases. Do not treat unverified community-sourced IOCs as high-confidence without corroboration.	LOW

Framework Mappings

MITRE-ATTACK

- **T1071** — Application Layer Protocol
- **T1021** — Remote Services
- **T1057** — Process Discovery
- **T1133** — External Remote Services
- **T1095** — Non-Application Layer Protocol
- **T1071.001** — Web Protocols
- **T1572** — Protocol Tunneling
- **T1190** — Exploit Public-Facing Application
- **T1049** — System Network Connections Discovery
- **T1205** — Traffic Signaling
- **T1547** — Boot or Logon Autostart Execution

- **T1059** — Command and Scripting Interpreter
- **T1543** — Create or Modify System Process
- **T1036.005** — Match Legitimate Resource Name or Location
- **T1036** — Masquerading
- **T1056.001** — Keylogging
- **T1016** — System Network Configuration Discovery
- **T1110** — Brute Force
- **T1027** — Obfuscated Files or Information
- **T1548** — Abuse Elevation Control Mechanism
- **T1205.002** — Socket Filters
- **T1082** — System Information Discovery
- **T1014** — Rootkit

NIST-800-53R5

- **CA-7** — Continuous Monitoring
- **SC-7** — Boundary Protection
- **SI-4** — System Monitoring
- **AC-17** — Remote Access
- **AC-3** — Access Enforcement
- **CM-7** — Least Functionality
- **IA-2** — Identification and Authentication (Organizational Users)
- **AC-20** — Use of External Systems
- **IA-5** — Authenticator Management
- **CA-8** — Penetration Testing
- **RA-5** — Vulnerability Monitoring and Scanning
- **SI-2** — Flaw Remediation
- **SI-7** — Software, Firmware, and Information Integrity
- **SI-3** — Malicious Code Protection
- **AC-7** — Unsuccessful Logon Attempts
- **AC-6** — Least Privilege
- **CM-6** — Configuration Settings

OWASP-TOP10-2021

- **A01:2021** — Broken Access Control

CIS-V8

- **6.1**
- **6.2**
- **8.2** — Collect Audit Logs

SOC2-TSC

- **CC6.1** — The entity implements logical access security software, infrastructure, and architectures over protected information assets

HIPAA-SECURITY

- **164.312(a)(1)** — Access Control

NIST-CSF-2

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

MITRE ATT&CK Mapping

Technique ID	Technique Name	Tactic
T1071	Application Layer Protocol	Command-And-Control
T1021	Remote Services	Lateral-Movement
T1057	Process Discovery	Discovery
T1133	External Remote Services	Persistence
T1095	Non-Application Layer Protocol	Command-And-Control
T1071.001	Web Protocols	Command-And-Control
T1572	Protocol Tunneling	Command-And-Control
T1190	Exploit Public-Facing Application	Initial-Access
T1049	System Network Connections Discovery	Discovery
T1205	Traffic Signaling	Defense-Evasion
T1547	Boot or Logon Autostart Execution	Persistence
T1059	Command and Scripting Interpreter	Execution
T1543	Create or Modify System Process	Persistence
T1036.005	Match Legitimate Resource Name or Location	Defense-Evasion
T1036	Masquerading	Defense-Evasion
T1056.001	Keylogging	Collection
T1016	System Network Configuration Discovery	Discovery
T1110	Brute Force	Credential-Access
T1027	Obfuscated Files or Information	Defense-Evasion
T1548	Abuse Elevation Control Mechanism	Privilege-Escalation

Technique ID	Technique Name	Tactic
T1205.002	Socket Filters	Defense-Evasion
T1082	System Information Discovery	Discovery
T1014	Rootkit	Defense-Evasion

Sources

Source	URL	Tier
Security News	https://thehackernews.com/2026/03/china-linked-red-menshen-uses-ste...	T3
Ivanti VPN Vulnerability: What You Need to Know - Palo Alto Networks	https://www.paloaltonetworks.com/cyberpedia/ivanti-VPN-vulnerabilit...	T3
Why Enterprise VPN and Gateway Products Are Perpetually Broken	https://hivesecurity.gitlab.io/blog/why-enterprise-vpn-gateways-alw...	T3
Critical Ivanti Connect Secure Vulnerability	https://kudelskisecurity.com/research/critical-ivanti-connect-secur...	T3
Ivanti Connect Secure VPN Targeted in New Zero-Day Exploitation	https://cloud.google.com/blog/topics/threat-intelligence/ivanti-con...	T3

Generated 2026-03-29 18:34 UTC by TJS Security Command Center