INTELLIGENCE BRIEFING
Security Command Center
TLP:CLEAR
2026-06-06 06:28 UTC

UNC5221 Sustains 18-Month Footholds Across MSP Supply Chains Using Brickstorm, Plenet, and AgentPSD

THREAT CAMPAIGN | **HIGH** | CVSS 9.5

SCC Item ID	SCC-CAM-2026-0418
Type	Threat Campaign
Severity	HIGH
CVSS Base Score	9.5
Affected Products	Microsoft 365, VMware vSphere, Dell RecoverPoint for Virtual Machines, Egnyte Storage Sync, Synology NAS, pfSense, Linux GroupWise
Published	2026-06-05T14:09:47
Discovery Source	Rss

Executive Summary

Chinese espionage group UNC5221 (also tracked as VerdantBamboo) maintained undetected access to a victim organization and its managed services provider for at least 18 months, deploying three backdoors, including two previously undocumented malware families, across edge devices, NAS appliances, and legacy servers. The attackers deliberately targeted infrastructure incapable of running endpoint detection tools, survived an initial remediation attempt by re-compromising the environment, and leveraged the MSP relationship to propagate access downstream. Organizations using MSPs for infrastructure management, or running VMware vSphere, Synology NAS, Dell RecoverPoint, pfSense, or legacy Linux environments, face elevated risk of long-duration, undetected compromise.

Technical Analysis

UNC5221 deployed three backdoor families across a victim environment and its MSP over an 18-month period: the previously documented Brickstorm implant and two newly identified families, Plenet and AgentPSD. Attack surface deliberately excluded EDR-capable hosts, focusing instead on VMware vSphere hypervisors, Dell RecoverPoint for Virtual Machines appliances, Synology NAS devices, pfSense edge routers, and legacy Linux servers running Novell GroupWise. Relevant CWEs include CWE-287 (improper authentication), CWE-522 (insufficiently protected credentials), and CWE-912 (hidden functionality/backdoor). Dell DSA-2024-369 is cited in associated threat intelligence reporting as a plausible initial access vector for the RecoverPoint appliance; direct exploitation linkage has not been confirmed by Dell's own advisory and should be treated as suspected,

not confirmed. MITRE ATT&CK techniques observed include T1190 (exploit public-facing application), T1195.002 (compromise software supply chain), T1505.003 (web shell), T1078 (valid accounts), T1133 (external remote services), T1021 (remote services), T1003 (credential dumping), T1550.001 (pass the hash), T1560 (archive collected data), T1090 (proxy), T1571 (non-standard port), T1027 (obfuscated files), T1036 (masquerading), T1095 (non-application layer protocol), T1071 (application layer protocol), T1083 (file and directory discovery), T1059 (command and scripting interpreter), T1105 (ingress tool transfer), T1199 (trusted relationship). No CVE identifier is associated with this campaign item. No CVSS or EPSS scores are available for the campaign as a whole; severity is qualitatively assessed as High.

Action Checklist

1. Step 1: Containment. Immediately audit MSP access paths into your environment; suspend or segment any MSP remote access sessions (T1199, T1133) until verified clean. Isolate VMware vSphere hosts, Dell RecoverPoint appliances, Synology NAS devices, and pfSense edge routers from lateral movement paths. Block non-standard outbound ports consistent with T1571 at the perimeter firewall (CIS 4.4, CIS 4.5).
2. Step 2: Detection. Query available log sources for indicators of Brickstorm, Plenet, and AgentPSD: look for anomalous processes on ESXi hosts, unexpected cron jobs or init scripts on Linux-based appliances (NIST AU-6, NIST AU-2), NAS admin interface access outside business hours, and outbound connections on non-standard ports from appliance management IPs. Review Dell RecoverPoint logs for exploitation attempts consistent with DSA-2024-369 (suspected initial access vector, not confirmed). Enable NIST AU-12 audit record generation on any appliance that supports it. Apply system file analysis and system init config analysis to edge and NAS devices. Threat hunt for T1550.001 (pass-the-hash) and T1003 (credential dumping) artifacts in authentication logs (NIST AU-3).
3. Step 3: Eradication. Apply Dell DSA-2024-369 patches per the Dell support advisory (https://www.dell.com/support/kbdoc/en-us/000228154/dsa-2024-369-security-update-for-dell-recoverpoint-for-virtual-machines-multiple-vulnerabilities). Rotate all credentials on affected systems and any accounts with MSP-delegated access (NIST AC-2). Disable or harden default accounts on all appliances (CIS 4.7). Audit and remove unauthorized web shells on ESXi and Linux hosts (T1505.003). Remove or reimage any host where Plenet or AgentPSD artifacts are found; reimaging is preferred given confirmed re-compromise after prior remediation.
4. Step 4: Recovery. After reimaging, validate no persistence mechanisms remain: check init configs, scheduled tasks, and startup scripts. Confirm MSP access is re-established only through MFA-enforced, logged channels (CIS 6.3, CIS 6.4, NIST AC-17). Monitor for re-compromise indicators for a minimum of 90 days given UNC5221's documented re-entry after remediation. Verify audit logging is active and shipping to a protected, centralized store not accessible from managed appliances (NIST AU-9, NIST AU-4). Apply continuous local account monitoring post-recovery.
5. Step 5: Post-Incident. This campaign exposed three structural gaps: (1) absence of EDR coverage on edge/appliance infrastructure - evaluate agent-less behavioral monitoring or network-based detection for EDR-blind devices; (2) insufficient segmentation between MSP access paths and production environments - enforce least-privilege and separation of duties for all third-party access (NIST AC-5, NIST AC-6, CIS 5.4); (3) credential reuse across MSP-managed and downstream environments - enforce unique credentials per environment and rotate on a defined schedule (CIS 5.2). Conduct a formal supply-chain risk review of all active MSP relationships against NIST AC-20 (use of external systems).

IR / Forensic Enrichment

Triage Priority	IMMEDIATE
Escalation Criteria	Escalate immediately to senior leadership, legal counsel, and potentially CISA if: UNC5221 artifacts are confirmed on systems processing PII, PHI, or regulated data requiring breach notification; if MSP downstream customer environments show evidence of lateral movement beyond the initially identified victim; if re-compromise is detected post-remediation (consistent with UNC5221's documented behavior); or if the incident response team lacks the forensic capability to analyze ESXi-resident malware or appliance firmware-level persistence without external support.
Recovery Notes	Given UNC5221's confirmed re-compromise of this environment after an initial remediation attempt, recovery cannot be declared complete without validating that MSP access paths — not just the directly compromised appliances — have been fully restructured with MFA, least-privilege scoping, and independent logging not accessible from MSP-managed infrastructure. Monitor all appliance management interfaces and outbound connections continuously for a minimum of 90 days post-recovery, with weekly review of the file integrity baseline and syslog anomaly reports, since Brickstorm and Plenet are specifically engineered for long-term undetected persistence on EDR-blind devices. Treat any unexplained outbound connection from a previously compromised appliance management IP as a confirmed re-compromise indicator and re-initiate containment immediately rather than investigating in place.
Forensic Artifacts	ESXi /var/log/shell.log and /var/log/hostd.log: capture all shell commands and vSphere API calls made during UNC5221's access window — Brickstorm's ESXi implant would generate API calls for VM enumeration and potential snapshot manipulation that appear in hostd.log with associated timestamps and source IPs | Synology NAS /var/packages/ directory and /var/log/synology.log: AgentPSD artifacts on Synology systems may be disguised as installed packages with plausible names; the packages directory preserves installation timestamps and file manifests that can be compared against Synology's official package catalog to identify unauthorized implants | Linux appliance cron and init directories (/etc/cron.d/, /etc/cron.daily/, /etc/rc.local, /etc/systemd/system/, /etc/init.d/): Plenet and Brickstorm achieve persistence via startup scripts and scheduled tasks on Linux-based appliances — file creation timestamps in these directories predating the confirmed discovery date are primary persistence evidence | Dell RecoverPoint management interface HTTP access logs (appliance-local log path /opt/brs/log/ or equivalent): exploitation attempts consistent with DSA-2024-369 would appear as anomalous POST requests to management API endpoints, HTTP 500 error responses, or unusual URI patterns — these logs are time-critical as they may be overwritten on appliance reboot and should be exported before any patching activity | Network capture from appliance management VLAN covering all outbound connections: Brickstorm's C2 beaconing on non-standard ports (T1571) produces a characteristic periodic connection pattern to fixed destination IPs — a minimum 24-hour full packet capture from this segment preserved as evidence will reveal C2 infrastructure, data exfiltration volumes, and beaconing intervals usable for IOC development and attribution corroboration

Per-Action IR Details

Step 1: Containment — Immediately audit MSP access paths into your environment; suspend or segment any MSP remote access sessions (T1199, T1133) until verified clean. Isolate VMware vSphere hosts, Dell RecoverPoint appliances, Synology NAS devices, and pfSense edge routers from lateral movement paths. Block non-standard outbound ports consistent with T1571 at the perimeter firewall (CIS 4.4, CIS 4.5).

NIST Phase: Containment

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

Controls: NIST AC-17 (Remote Access), NIST AC-4 (Information Flow Enforcement), NIST AC-20 (Use Of External Systems), CIS 4.4 (Implement and Manage a Firewall on Servers), CIS 4.5 (Implement and Manage a Firewall on End-User Devices)

Compensating: Pull all active MSP sessions immediately: on pfSense, navigate to Diagnostics > States and filter by MSP source IP ranges, then kill matching state table entries via 'pfctl -k '. On ESXi, run 'esxcli network connection list' and kill suspicious sessions with 'esxcli network connection kill'. Use Wireshark or tcpdump on a span port to capture all traffic from MSP VLANs before termination — 'tcpdump -i eth0 -w msp_capture_$(date +%F).pcap host ' — preserving lateral movement evidence. Apply pfSense block rules on the MSP-facing interface to drop all non-port-443/22 outbound from appliance management IPs, targeting T1571 non-standard port usage documented in Brickstorm C2 behavior.

Evidence: BEFORE suspending MSP sessions, capture: (1) pfSense firewall state table export ('pfctl -ss > pf_states_$(date +%F).txt') showing active MSP-originated connections and destination IPs; (2) ESXi active session list ('vim-cmd vmsvc/getallvms' and 'esxcli network connection list > esxi_connections.txt'); (3) Synology NAS admin interface access logs at /var/log/synology.log and connection logs at /var/log/messages filtered for DSM web interface authentication events; (4) pfSense syslog for outbound connection attempts on ports outside 80/443 from appliance management segment IPs, specifically looking for Brickstorm's use of non-standard ports for tunneled C2; (5) Dell RecoverPoint management console session logs for any active or recently terminated remote sessions tied to MSP accounts.

Step 2: Detection — Query available log sources for indicators of Brickstorm, Plenet, and AgentPSD: look for anomalous processes on ESXi hosts, unexpected cron jobs or init scripts on Linux-based appliances (NIST AU-6, NIST AU-2), NAS admin interface access outside business hours, and outbound connections on non-standard ports from appliance management IPs. Review Dell RecoverPoint logs for exploitation attempts consistent with DSA-2024-369 (suspected initial access vector — not confirmed). Enable NIST AU-12 audit record generation on any appliance that supports it. Apply D3-SFA (System File Analysis) and D3-SICA (System Init Config Analysis) to edge and NAS devices. Threat hunt for T1550.001 (pass-the-hash) and T1003 (credential dumping) artifacts in authentication logs (NIST AU-3).

NIST Phase: Detection Analysis

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

Controls: NIST AU-6 (Audit Record Review, Analysis, And Reporting), NIST AU-2 (Event Logging), NIST AU-12 (Audit Record Generation), NIST AU-3 (Content Of Audit Records)

Compensating: On ESXi hosts, enumerate suspicious processes and backdoor artifacts: 'ps aux | grep -Ev "(hostd|vpxa|vmkiscsid|sfcbd|slpd)"' to surface non-standard daemons consistent with Brickstorm or Plenet implants. Check for unexpected cron entries across all Linux-based appliances: 'for f in /etc/cron* /var/spool/cron/crontabs/*; do echo "=== $f ==="; cat $f 2>/dev/null; done'. On Synology NAS, examine /etc/rc.local, /usr/local/etc/rc.d/, and /var/packages/ for unauthorized startup scripts consistent with AgentPSD persistence. Build a YARA rule targeting Plenet and Brickstorm string patterns (C2 URI formats, hardcoded IPs, known function names from threat reporting) and scan ESXi VMFS datastores and NAS shares: 'yara -r brickstorm_plenet.yar /vmfs/volumes/'. Use osquery on any Linux host that can run it: 'SELECT * FROM process_open_sockets WHERE remote_port NOT IN (80,443,22)' to surface T1571 non-standard port C2 connections.

Evidence: BEFORE remediation, collect: (1) ESXi /var/log/shell.log and /var/log/auth.log for authentication events and shell commands executed — UNC5221 shell activity will appear here if interactive access was used; (2) ESXi /var/log/hostd.log for API calls and management plane events that could indicate Brickstorm's use of vSphere APIs for persistence; (3) Synology NAS /var/log/synology.log filtered for admin logins outside business hours and DSM package installation events that could indicate AgentPSD deployment; (4) Dell RecoverPoint /opt/brs/log/ directory (or equivalent appliance log path) for any HTTP requests to management interfaces consistent with DSA-2024-369 exploitation attempts — look for unusual URI patterns, large POST bodies, or HTTP 500 responses indicating exploitation; (5) pfSense /var/log/filter.log for outbound connection attempts from appliance management IPs, specifically recording destination IPs, ports, and byte counts to identify Brickstorm C2 beaconing intervals and T1571

non-standard port usage.

Step 3: Eradication — Apply Dell DSA-2024-369 patches per the Dell support advisory (https://www.dell.com/support/kbdoc/en-us/000228154/dsa-2024-369-security-update-for-dell-recoverpoint-for-virtual-machines-multiple-vulnerabilities — note: URL is from provided source data; validate before use). Rotate all credentials on affected systems and any accounts with MSP-delegated access (D3-CRO, NIST AC-2). Disable or harden default accounts on all appliances (CIS 4.7). Audit and remove unauthorized web shells on ESXi and Linux hosts (T1505.003). Remove or reimage any host where Plenet or AgentPSD artifacts are found — reimaging is preferred given confirmed re-compromise after prior remediation.

NIST Phase: Eradication

Reference: NIST 800-61r3 §3.4 — Eradication

Controls: NIST AC-2 (Account Management), NIST SI-2 (Flaw Remediation), CIS 4.7 (Manage Default Accounts on Enterprise Assets and Software), CIS 7.3 (Perform Automated Operating System Patch Management), CIS 7.4 (Perform Automated Application Patch Management)

Compensating: Web shell hunting on ESXi: 'find /vmfs/volumes /etc /tmp -name "*.php" -o -name "*.jsp" -o -name "*.py" -newer /etc/passwd 2>/dev/null' — UNC5221 has deployed T1505.003 web shells on edge appliances; compare file hashes against known-good ESXi installation manifests using 'md5sum'. For credential rotation without enterprise tooling, generate a complete account list on each appliance before rotation: on Synology, 'cat /etc/passwd'; on ESXi, 'esxcli system account list'; on pfSense, review System > User Manager — document all MSP-delegated accounts and rotate to environment-unique passwords of 20+ characters. For reimaging ESXi hosts, use VMware's documented ESXi reinstall procedure and restore VMs only from snapshots predating the earliest confirmed UNC5221 intrusion date (work backward 18 months minimum from discovery). Do not restore from backups managed by the compromised RecoverPoint appliance without first validating backup integrity from an out-of-band source, given UNC5221's documented survival of prior remediation.

Evidence: BEFORE patching or reimaging, preserve: (1) Full memory dump of any ESXi host where Brickstorm or Plenet is suspected — use 'vm-support -n' on ESXi to collect a support bundle including memory artifacts; (2) Complete copy of /etc, /var, /tmp, and all cron directories from Synology NAS and Linux appliances to an isolated forensic store before any changes; (3) Hash inventory of all files in ESXi /bin, /sbin, /usr/lib/vmware, and web-accessible directories (compare against VMware's published file manifests for the installed ESXi build); (4) Export of all Synology NAS package installation records and timestamps from /var/packages/ — AgentPSD may be disguised as a legitimate Synology package; (5) Network capture from the RecoverPoint management interface covering at least 24 hours prior to patching, to preserve exploitation traffic patterns consistent with DSA-2024-369 for post-incident analysis and potential law enforcement referral.

Step 4: Recovery — After reimaging, validate no persistence mechanisms remain: check init configs, scheduled tasks, and startup scripts (D3-SICA). Confirm MSP access is re-established only through MFA-enforced, logged channels (CIS 6.3, CIS 6.4, NIST AC-17). Monitor for re-compromise indicators for a minimum of 90 days given UNC5221's documented re-entry after remediation. Verify audit logging is active and shipping to a protected, centralized store not accessible from managed appliances (NIST AU-9, NIST AU-4).

NIST Phase: Recovery

Reference: NIST 800-61r3 §3.5 — Recovery

Controls: NIST AC-17 (Remote Access), NIST AU-9 (Protection Of Audit Information), NIST AU-4 (Audit Storage Capacity), CIS 6.3 (Require MFA for Externally-Exposed Applications), CIS 6.4 (Require MFA for Remote Network Access)

Compensating: Validate persistence-free state post-reimaging with a structured checklist executed by two analysts independently: (1) 'systemctl list-units --type=service --state=running' and 'ls -la /etc/systemd/system/' on Linux appliances to verify no unauthorized services; (2) 'crontab -l' for all users including root, plus 'ls -la /etc/cron.d/ /etc/cron.daily/ /etc/cron.hourly/'; (3) on ESXi, 'cat /etc/rc.local.d/local.sh' and 'find /etc/vmware -name "*.sh" -newer /etc/passwd' — Plenet and Brickstorm have used these paths for ESXi persistence. For log centralization without a

commercial SIEM, configure rsyslog on all appliances to forward to an isolated syslog receiver (rsyslog on a hardened Linux VM not managed by the MSP): 'echo "*.* @@:514" >> /etc/rsyslog.conf'. MSP re-access must traverse a jump host with PAM (Privileged Access Management) logging — use free OpenSSH with AllowUsers restriction and ForceCommand logging as minimum viable control.

Evidence: BEFORE declaring recovery complete, document: (1) Baseline file integrity snapshot of all reimaged appliances using 'sha256sum -r /bin /sbin /usr/bin /usr/sbin /etc > baseline_$(hostname)_$(date +%F).sha256' — store off-appliance and off-MSP-network; (2) Verified syslog forwarding confirmation: generate a test authentication event and confirm receipt at the centralized syslog server within 60 seconds; (3) MSP access log review for the first 72 hours post-recovery, capturing all commands executed under MSP accounts on all appliances — compare against a documented change request for that period; (4) Outbound connection baseline from all appliances post-recovery using 'ss -tnp' or 'netstat -tnp' snapshots every 15 minutes for the first 48 hours, establishing a clean-state connection profile to detect Brickstorm re-establishment of C2 on non-standard ports; (5) Screenshot and export of pfSense firewall rules post-recovery confirming MSP access restrictions remain in place and no rules were modified during the recovery window.

Step 5: Post-Incident — This campaign exposed three structural gaps: (1) absence of EDR coverage on edge/appliance infrastructure — evaluate agent-less behavioral monitoring or network-based detection for EDR-blind devices (NIST SI-4 equivalent behavior: no mapped control in provided knowledge base for agentless EDR); (2) insufficient segmentation between MSP access paths and production environments — enforce least-privilege and separation of duties for all third-party access (NIST AC-5, NIST AC-6, CIS 5.4); (3) credential reuse across MSP-managed and downstream environments — enforce unique credentials per environment and rotate on a defined schedule (CIS 5.2, D3-CH). Conduct a formal supply-chain risk review of all active MSP relationships against NIST AC-20 (use of external systems).

NIST Phase: Post Incident

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

Controls: NIST AC-5 (Separation Of Duties), NIST AC-6 (Least Privilege), NIST AC-20 (Use Of External Systems), CIS 5.2 (Use Unique Passwords), CIS 5.4 (Restrict Administrator Privileges to Dedicated Administrator Accounts), CIS 7.1 (Establish and Maintain a Vulnerability Management Process), CIS 7.2 (Establish and Maintain a Remediation Process)

Compensating: Address the EDR-blind appliance gap with network-based behavioral detection: deploy Zeek (formerly Bro) on a network tap or span port covering the appliance management VLAN — write custom Zeek scripts to alert on beaconing behavior (periodic outbound connections at fixed intervals) characteristic of Brickstorm and Plenet C2. Publish community Sigma rules for Brickstorm and Plenet IOCs to your centralized syslog receiver and parse with grep-based alerting as a minimum viable SIEM: 'tail -f /var/log/remote/*.log | grep -E "(|)"'. For supply-chain risk formalization, create a one-page MSP access inventory documenting: each MSP's access scope, authentication method, logging state, and last access review date — review quarterly. Enforce credential uniqueness by generating a per-environment password matrix stored in an offline password manager (KeePassXC), eliminating the MSP-to-downstream credential reuse that enabled UNC5221's lateral movement.

Evidence: For the post-incident lessons-learned record, preserve and reference: (1) Timeline reconstruction document mapping UNC5221's first confirmed access date, failed remediation date, and re-compromise date — this 18-month dwell timeline is required evidence for any regulatory notification assessment; (2) Inventory of all EDR-blind devices (ESXi hosts, RecoverPoint, Synology NAS, pfSense) with documented detection gap rationale — this justifies investment in network-based controls to leadership; (3) Credential reuse map showing which MSP-held credentials also had access to downstream customer environments — document scope of potential credential-based lateral movement beyond the directly compromised systems; (4) Complete IOC set (file hashes, C2 IPs, non-standard ports, persistence file paths) for Brickstorm, Plenet, and AgentPSD contributed to an ISAC or shared via STIX/TAXII for sector-wide defense; (5) MSP contractual review findings documenting whether the MSP's security obligations (logging, MFA, segmentation) were met per the service agreement — relevant to both internal accountability and potential legal or regulatory obligations.

Detection Guidance

Detection is difficult by design; UNC5221 deliberately avoided EDR-capable hosts. Focus detection on network telemetry and appliance-native logs. Key indicators: (1) Outbound connections from NAS, ESXi, or edge device management IPs to unfamiliar external addresses, especially on non-standard ports (T1571) or using proxied channels (T1090); (2) New or modified files in ESXi /init.d/, /etc/rc.local, or equivalent startup paths on Linux appliances (NIST SI-2, D3-SICA); (3) Unexpected admin interface logins to Synology DSM, pfSense, or Dell RecoverPoint consoles, particularly outside business hours or from unusual source IPs (NIST AU-6, NIST AU-3); (4) Use of pass-the-hash or pass-the-ticket techniques in Windows authentication logs, Event ID 4624 with logon type 3 and NTLM auth from appliance IPs (T1550.001); (5) Archive creation or staging activity on file servers or NAS devices inconsistent with backup schedules (T1560); (6) Non-interactive command execution (T1059) on legacy Linux servers running GroupWise; (7) MSP remote access sessions initiating lateral movement to internal systems (T1021, T1199). Apply local account monitoring for account anomalies on all appliance types that support account logging. Before deploying detection rules, consult primary threat intelligence reporting for confirmed IOC lists. IOCs available in public threat intelligence reflect currently available data only.

Indicators of Compromise

Type	Value	Context	Confidence
HASH	`not available`	Brickstorm, Plenet, and AgentPSD file hashes are not present in provided source data. Consult primary technical reporting (Mandiant/NVISO) for confirmed malware hashes.	LOW
DOMAIN	`not available`	C2 domains associated with UNC5221 infrastructure in this campaign are not present in provided source data. Primary reporting is required for confirmed C2 indicators.	LOW
IP	`not available`	C2 IP addresses for this campaign are not present in provided source data. Do not populate IOC blocklists from memory — obtain from primary vendor reporting.	LOW

Framework Mappings

MITRE-ATTACK

- **T1036** — Masquerading
- **T1095** — Non-Application Layer Protocol
- **T1071** — Application Layer Protocol
- **T1133** — External Remote Services
- **T1021** — Remote Services

- **T1505.003** — Web Shell
- **T1560** — Archive Collected Data
- **T1190** — Exploit Public-Facing Application
- **T1003** — OS Credential Dumping
- **T1078** — Valid Accounts
- **T1195.002** — Compromise Software Supply Chain
- **T1059** — Command and Scripting Interpreter
- **T1083** — File and Directory Discovery
- **T1550.001** — Application Access Token
- **T1027** — Obfuscated Files or Information
- **T1199** — Trusted Relationship
- **T1571** — Non-Standard Port
- **T1090** — Proxy
- **T1105** — Ingress Tool Transfer

NIST-800-53R5

- **CA-7** — Continuous Monitoring
- **SC-7** — Boundary Protection
- **SI-4** — System Monitoring
- **AC-17** — Remote Access
- **AC-20** — Use of External Systems
- **IA-2** — Identification and Authentication (Organizational Users)
- **IA-5** — Authenticator Management
- **AC-3** — Access Enforcement
- **CM-7** — Least Functionality
- **CM-2** — Baseline Configuration
- **SI-3** — Malicious Code Protection
- **SI-7** — Software, Firmware, and Information Integrity
- **CA-8** — Penetration Testing
- **RA-5** — Vulnerability Monitoring and Scanning
- **SI-2** — Flaw Remediation
- **AC-6** — Least Privilege
- **AC-2** — Account Management
- **SA-9** — External System Services
- **SR-3** — Supply Chain Controls and Processes
- **IA-8** — Identification and Authentication (Non-Organizational Users)
- **SR-2** — Supply Chain Risk Management Plan

OWASP-TOP10-2021

- **A04:2021** — Insecure Design

- **A07:2021** — Identification and Authentication Failures

CIS-V8

- **5.2** — Use Unique Passwords
- **6.3** — Require MFA for Externally-Exposed Applications
- **6.4** — Require MFA for Remote Network Access
- **6.5** — Require MFA for Administrative Access
- **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
- **164.312(d)** — Person or Entity Authentication

SOC2-TSC

- **CC6.1** — The entity implements logical access security software, infrastructure, and architectures over protected information assets
- **CC9.2** — Manages risks associated with vendors and business partners

ISO-27001-2022

- **A.8.8** — Management of technical vulnerabilities
- **A.5.21** — Managing information security in the ICT supply chain

NIST-CSF-2

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

MITRE ATT&CK Mapping

Technique ID	Technique Name	Tactic
T1036	Masquerading	Defense-Evasion
T1095	Non-Application Layer Protocol	Command-And-Control
T1071	Application Layer Protocol	Command-And-Control
T1133	External Remote Services	Persistence
T1021	Remote Services	Lateral-Movement
T1505.003	Web Shell	Persistence
T1560	Archive Collected Data	Collection
T1190	Exploit Public-Facing Application	Initial-Access

Technique ID	Technique Name	Tactic
T1003	OS Credential Dumping	Credential-Access
T1078	Valid Accounts	Defense-Evasion
T1195.002	Compromise Software Supply Chain	Initial-Access
T1059	Command and Scripting Interpreter	Execution
T1083	File and Directory Discovery	Discovery
T1550.001	Application Access Token	Defense-Evasion
T1027	Obfuscated Files or Information	Defense-Evasion
T1199	Trusted Relationship	Initial-Access
T1571	Non-Standard Port	Command-And-Control
T1090	Proxy	Command-And-Control
T1105	Ingress Tool Transfer	Command-And-Control

Sources

Source	URL	Tier
Security News	https://www.bleepingcomputer.com/news/security/chinese-apt-deploys-...	T3
Virtual machine protection and recovery | Synology Inc.	https://www.synology.com/en-us/backup/solution/virtual-machines	T3
A Vulnerability in Dell RecoverPoint for Virtual Machines Could ...	https://www.cisecurity.org/advisory/a-vulnerability-in-dell-recover...	T3
DSA-2024-369: Security Update for Dell RecoverPoint for Virtual ...	https://www.dell.com/support/kbdoc/en-us/000228154/dsa-2024-369-sec...	T3
Snapshot consolidation errors or VM restarts on 6.x protected VMs	https://www.dell.com/support/kbdoc/en-ae/000423284/recoverpoint-for...	T3

Solutions is not liable for any damages resulting from the use of this information.

Generated 2026-06-06 06:28 UTC by TJS Security Command Center