INTELLIGENCE BRIEFING
Security Command Center
TLP:CLEAR
2026-06-08 13:47 UTC

VerdantBamboo (Clay Typhoon/UNC5221) Deploys BSD BRICKSTORM, PLENET, and AGENTPSD Against Unmonitored Appliances via MSP Pivot

THREAT CAMPAIGN | **HIGH** | CVSS 9.5

SCC Item ID	SCC-CAM-2026-0424
Type	Threat Campaign
CVE ID	CVE-2026-22769
Severity	HIGH
CVSS Base Score	9.5
EPSS Score	0.2289 (96th percentile)
Affected Products	Egnyte Storage Sync (patched v13.13), Synology NAS appliances, pfSense firewalls, Dell RecoverPoint for Virtual Machines, Microsoft 365
Published	2026-06-08T06:27:32
Discovery Source	Rss

Executive Summary

A China-linked espionage group tracked as VerdantBamboo conducted an 18-month undetected intrusion by compromising a managed services provider's network infrastructure, then pivoting into downstream victim environments hosting Egnyte Storage Sync, Synology NAS, and Microsoft 365. The attackers deployed three purpose-built malware families engineered specifically for network appliances and storage devices that fall outside standard endpoint detection coverage. Organizations using MSPs to manage network infrastructure, or running NAS and appliance stacks without EDR visibility, face elevated risk of long-term, silent data exfiltration.

Technical Analysis

VerdantBamboo (Clay Typhoon/UNC5221/Warp Panda) deployed three novel implants: a BSD-compiled BRICKSTORM variant targeting non-EDR appliances, PLENET (also tracked as GRIMBOLT), a cross-platform .NET Core backdoor, and AGENTPSD, a Python fallback shell. The intrusion entered through a managed services provider's pfSense firewall (T1199, Trusted Relationship) before reaching Egnyte Storage Sync (vulnerable before v13.13), Synology NAS, and Microsoft 365. CVE-2026-22769 affects Dell RecoverPoint for

Virtual Machines with a CVSS base score of 9.5 and an EPSS score of 0.229 (96th percentile). Associated weaknesses include CWE-269 (Improper Privilege Management), CWE-284 (Improper Access Control), and CWE-522 (Insufficiently Protected Credentials). MITRE ATT&CK techniques observed span initial access via T1190 (Exploit Public-Facing Application) and T1199 (Trusted Relationship), persistence via T1543 (Create or Modify System Process) and T1505.003 (Web Shell), defense evasion via T1562.001 (Impair Defenses) and T1027 (Obfuscated Files), lateral movement via T1021.004 (SSH) and T1078/T1078.002 (Valid Accounts/Domain Accounts), and exfiltration via T1560 (Archive Collected Data). The toolchain demonstrates deliberate targeting of BSD and Linux appliance environments where EDR agents are typically absent. Dell advisory DSA-2026-079 covers the RecoverPoint vulnerability; Egnyte Storage Sync v13.13 or later is the patched release. CVE-2026-22769 is not currently listed on the CISA KEV catalog.

Action Checklist

1. Step 1: Containment, Immediately isolate any pfSense, Synology NAS, or Dell RecoverPoint for Virtual Machines appliances managed by or accessible to third-party MSPs. Revoke MSP remote access credentials pending review (NIST AC-17; CIS 6.2). Segment Egnyte Storage Sync hosts from lateral-movement paths until patched to v13.13.
2. Step 2: Detection, Query firewall and VPN logs for SSH lateral movement (T1021.004) originating from MSP IP ranges. Hunt for unexpected .NET Core or Python processes on NAS and appliance hosts (AU-6; CIS 8.2). Search for web shell artifacts aligned with T1505.003 on pfSense and Synology. Review Microsoft 365 Unified Audit Logs for anomalous account activity (T1078) and archive/exfiltration events (T1560). Check for BRICKSTORM, PLENET, and AGENTPSD file hashes and process names in available log sources.
3. Step 3: Eradication, Apply Dell DSA-2026-079 to all Dell RecoverPoint for Virtual Machines instances to remediate CVE-2026-22769. Upgrade Egnyte Storage Sync to v13.13 or later. Audit and rotate all credentials stored on or accessible from compromised appliances, including MSP-held service accounts (NIST AC-2; CIS 5.2; D3-CRO). Remove any identified web shells, unauthorized scheduled tasks, or persistence mechanisms on appliance hosts.
4. Step 4: Recovery, Validate patch application on all affected appliances using vendor-provided verification steps from DSA-2026-079. Re-enable MSP access only after implementing least-privilege, time-limited, monitored remote access sessions (NIST AC-6; AC-17). Monitor Microsoft 365 audit logs and NAS access logs continuously for 30 days post-remediation for signs of persistent access or re-compromise. Verify no unauthorized accounts remain in M365 (NIST AC-2; CIS 5.1).
5. Step 5: Post-Incident, Conduct a coverage gap review for all network appliances, NAS devices, and perimeter infrastructure outside EDR visibility (CIS 1.1). Formalize MSP access governance: require MFA for all MSP administrative sessions (CIS 6.5; NIST AC-17), enforce session logging (NIST AU-14), and establish contractual security requirements. Map all third-party trust relationships and assess supply chain adjacency risk (NIST AC-20). Document findings against NIST CSF Detect and Respond functions for board reporting.

IR / Forensic Enrichment

Triage Priority	IMMEDIATE

Escalation Criteria	Escalate to executive leadership, legal counsel, and your relevant sector ISAC immediately if any of the following are confirmed: (1) BRICKSTORM, PLENET, or AGENTPSD artifacts are found on appliances storing PII, PHI, or regulated financial data triggering breach notification obligations; (2) the compromised MSP manages appliances for other downstream clients who have not yet been notified, creating third-party duty-to-warn exposure; (3) Dell RecoverPoint or Synology NAS appliances with backup data are confirmed exfiltrated, indicating ransomware pre-positioning or IP theft at a scale requiring executive crisis response.
Recovery Notes	Before restoring MSP access to any appliance, validate that CVE-2026-22769 is remediated via Dell DSA-2026-079 by confirming the RecoverPoint management interface version string matches the patched build — do not rely solely on the patch installer's success message, as VerdantBamboo campaigns have historically involved tampering with update verification mechanisms on targeted appliances. Monitor Synology NAS and Egnyte Storage Sync outbound traffic baselines for 30 days using pfSense's built-in Bandwidth Monitoring (Status > Traffic Graph) or ntopng community edition, specifically watching for resumed periodic beaconing to non-corporate external IPs that would indicate a PLENET or AGENTPSD implant survived eradication on an unimaged appliance. Conduct a formal re-scan of all in-scope appliances at day 7, day 14, and day 30 post-remediation using the YARA rules and osquery queries established during detection, treating any detection as a full incident re-declaration rather than a routine finding.
Forensic Artifacts	pfSense /var/log/filter.log and system.log entries showing TCP/22 and TCP/443 connections from MSP IP ranges to internal NAS and RecoverPoint management interfaces — these establish VerdantBamboo's lateral movement path from MSP pivot into victim environments over the 18-month intrusion window | Synology DSM /root/.ssh/authorized_keys and /home/*/.ssh/authorized_keys files — AGENTPSD and similar appliance-targeting implants commonly plant SSH public keys for persistent backdoor access that survives DSM reboots and software updates | Dell RecoverPoint management audit log (accessible via 'get_audit_log' CLI or the RecoverPoint management console) showing all API calls and CLI commands executed during MSP-authenticated sessions — CVE-2026-22769 exploitation would appear as anomalous unauthenticated or privilege-escalated API calls in this log | Microsoft 365 Unified Audit Log entries for ContentSearch, eDiscovery case creation, New-InboxRule, and MailboxExport operations during MSP access windows — VerdantBamboo's T1560 data staging and T1114.003 email collection activity against M365 would be captured here and is typically absent from standard alert configurations | Egnyte Storage Sync %ProgramData%\Egnyte\Logs\EgnyteDrive*.log files on Windows sync client hosts showing file access and upload events during the pre-patch period — these logs capture which files were synced to the Egnyte cloud during the intrusion, establishing the data exfiltration scope for breach notification assessment

Per-Action IR Details

Step 1: Containment — Immediately isolate any pfSense, Synology NAS, or Dell RecoverPoint for Virtual Machines appliances managed by or accessible to third-party MSPs. Revoke MSP remote access credentials pending review (NIST AC-17; CIS 6.2). Segment Egnyte Storage Sync hosts from lateral-movement paths until patched to v13.13.

NIST Phase: Containment

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

Controls: NIST AC-17 (Remote Access), NIST AC-4 (Information Flow Enforcement), CIS 6.2 (Establish an Access Revoking Process)

Compensating: On pfSense, immediately add a floating firewall rule blocking all traffic from known MSP IP ranges (Firewall > Rules > Floating, action: Block, source: MSP_subnet, log: enabled). On Synology DSM, navigate to Control

Panel > Terminal & SNMP > disable SSH, and Control Panel > File Services > disable SMB/AFP/NFS. For Dell RecoverPoint, use the boxmgmt CLI to disable remote management interfaces: 'boxmgmt network disable-remote-access'. Document all MSP VPN gateway IPs from your firewall connection logs before revoking access so you have the full MSP network footprint for threat hunting.

Evidence: Before revoking MSP credentials, capture: (1) pfSense firewall state table dump (Diagnostics > States > Download) to preserve active sessions from MSP IP ranges at time of isolation; (2) Synology DSM connection logs at /var/log/messages and /var/log/synolog/ for SSH session records showing MSP source IPs and timestamps; (3) Dell RecoverPoint management audit logs via 'get_audit_log' CLI command documenting all administrative actions taken from MSP accounts; (4) Egnyte Storage Sync access logs showing file sync events and authenticated session tokens prior to credential revocation — these may reveal pre-positioned data staging by VerdantBamboo.

Step 2: Detection — Query firewall and VPN logs for SSH lateral movement (T1021.004) originating from MSP IP ranges. Hunt for unexpected .NET Core or Python processes on NAS and appliance hosts (AU-6; CIS 8.2). Search for web shell artifacts aligned with T1505.003 on pfSense and Synology. Review Microsoft 365 Unified Audit Logs for anomalous account activity (T1078) and archive/exfiltration events (T1560). Check for BRICKSTORM, PLENET, and AGENTPSD file hashes and process names in available log sources.

NIST Phase: Detection Analysis

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

Controls: NIST AU-6 (Audit Record Review, Analysis, And Reporting), CIS 8.2 (Collect Audit Logs)

Compensating: For pfSense web shell hunting, run: 'find /usr/local/www/ /var/www/ -name "*.php" -newer /etc/version -ls' to identify PHP files modified after the OS baseline, then grep for BRICKSTORM indicators: 'grep -r "base64_decode\|eval\|system\|passthru" /usr/local/www/ 2>/dev/null'. On Synology, check for unexpected .NET Core or Python processes: 'ps aux | grep -E "dotnet|python3|python" | grep -v "synology"' and examine /volume1/@tmp/ and /tmp/ for PLENET or AGENTPSD staging files. For M365 without a SIEM, use the free Microsoft 365 Management Activity API or export Unified Audit Logs via PowerShell: 'Search-UnifiedAuditLog -StartDate (Get-Date).AddDays(-90) -EndDate (Get-Date) -Operations "MailItemsAccessed,FileDownloaded,SearchQueryInitiatedExchange" -ResultSize 5000 | Export-Csv UAL_export.csv'. Write a YARA rule targeting BRICKSTORM's BSD-targeting characteristics and scan NAS mounted volumes using 'yara -r brickstorm.yar /volume1/'.

Evidence: Capture before analysis is complete: (1) pfSense /var/log/system.log and /var/log/filter.log in raw form — VerdantBamboo's SSH lateral movement from MSP pivot IPs will appear here as repeated TCP/22 connections across internal segments; (2) Synology /var/log/auth.log for SSH authentication events and /var/log/messages for process execution records showing unexpected .NET Core or Python interpreter launches indicative of PLENET deployment; (3) Dell RecoverPoint /var/log/esrs/ ESRS (remote support) logs and /var/log/secure for authentication attempts using MSP service accounts post-compromise; (4) Microsoft 365 Unified Audit Logs scoped to MailItemsAccessed, FileDownloaded, and New-InboxRule operations over the full 18-month suspected intrusion window — VerdantBamboo's T1560 archiving activity will appear as bulk download or PST export events; (5) Egnyte Storage Sync application logs at %ProgramData%\Egnyte\Logs\ on Windows hosts for file sync events from sensitive directories during MSP access windows.

Step 3: Eradication — Apply Dell DSA-2026-079 to all Dell RecoverPoint for Virtual Machines instances to remediate CVE-2026-22769. Upgrade Egnyte Storage Sync to v13.13 or later. Audit and rotate all credentials stored on or accessible from compromised appliances, including MSP-held service accounts (NIST AC-2; CIS 5.2; D3-CRO). Remove any identified web shells, unauthorized scheduled tasks, or persistence mechanisms on appliance hosts.

NIST Phase: Eradication

Reference: NIST 800-61r3 §3.4 — Eradication

Controls: NIST AC-2 (Account Management), CIS 5.2 (Use Unique Passwords)

Compensating: For web shell removal on pfSense, after identifying malicious PHP files via the find command above, do not simply delete — first copy to an evidence partition: 'cp -p /usr/local/www/malicious.php /mnt/evidence/webshells/' then remove. Audit pfSense cron persistence: 'crontab -l -u root' and inspect /etc/cron.d/ and /var/cron/tabs/. On Synology, check DSM task scheduler for unauthorized entries at Control Panel > Task Scheduler,

and inspect /etc/cron.d/ and /var/spool/cron/crontabs/root for AGENTPSD persistence mechanisms. For credential rotation, generate a full list of service accounts with access to compromised appliances using PowerShell against Active Directory: 'Get-ADServiceAccount -Filter * | Select-Object Name,Description | Export-Csv sa_audit.csv' — rotate all passwords for accounts that authenticated to MSP-managed devices in the 18-month window. Apply Dell DSA-2026-079 following the vendor's offline update procedure to avoid re-exposing the CVE-2026-22769 attack surface during patching.

Evidence: Before eradication actions, preserve: (1) Full forensic image of pfSense /var/ and /usr/local/www/ directories using 'tar czf /mnt/evidence/pfsense_webroot_$(date +%Y%m%d).tar.gz /usr/local/www/' — captures BRICKSTORM web shell artifacts in their installed state before removal; (2) Synology memory dump if possible using the 'avmcore' utility or third-party memory acquisition, as PLENET and AGENTPSD are reported to operate as in-memory implants on appliance targets; (3) Export all pfSense and Synology system configuration backups (config.xml on pfSense, DSM config backup on Synology) to capture any VerdantBamboo-modified configuration values such as added admin accounts or modified SSH authorized_keys at /root/.ssh/authorized_keys; (4) Screenshot and export the Dell RecoverPoint audit log before applying DSA-2026-079, documenting the full timeline of administrative actions taken via CVE-2026-22769 exploitation.

Step 4: Recovery — Validate patch application on all affected appliances using vendor-provided verification steps from DSA-2026-079. Re-enable MSP access only after implementing least-privilege, time-limited, monitored remote access sessions (NIST AC-6; AC-17). Monitor Microsoft 365 audit logs and NAS access logs continuously for 30 days post-remediation for signs of persistent access or re-compromise. Verify no unauthorized accounts remain in M365 (NIST AC-2; CIS 5.1).

NIST Phase: Recovery

Reference: NIST 800-61r3 §3.5 — Recovery

Controls: NIST AC-6 (Least Privilege), NIST AC-17 (Remote Access), NIST AC-2 (Account Management), CIS 5.1 (Establish and Maintain an Inventory of Accounts)

Compensating: For M365 unauthorized account verification without a commercial CASB, run PowerShell: 'Get-MsolUser -All | Where-Object {$_.IsLicensed -eq $true} | Select-Object DisplayName,UserPrincipalName,LastDirSyncTime | Export-Csv m365_accounts.csv' and cross-reference against your known-good HR roster. Check for guest account abuse: 'Get-MsolUser -All | Where-Object {$_.UserType -eq "Guest"}'. For monitored MSP re-access, configure pfSense to log all MSP VPN sessions to a remote syslog server outside MSP administrative control: System > Advanced > Notifications > Syslog, ensuring VerdantBamboo cannot tamper with session evidence. On Synology DSM, enable IP auto-block (Control Panel > Security > Auto Block) with threshold 5 failures / 5 minutes and enable login notifications. Validate Egnyte Storage Sync v13.13 by running the installer's built-in version check and confirming the build hash matches the vendor's published checksum from the DSA-2026-079 advisory.

Evidence: During the 30-day monitoring window, continuously collect: (1) Microsoft 365 Unified Audit Logs filtered on New-InboxRule, Set-Mailbox, and Add-MailboxPermission operations — VerdantBamboo commonly establishes email forwarding rules (T1114.003) as a post-remediation persistence fallback; (2) Synology DSM /var/log/auth.log for any SSH authentication attempts from IP ranges outside the newly-allowlisted MSP CIDR blocks, which would indicate use of a secondary C2 channel planted before eradication; (3) pfSense firewall logs for outbound connections from internal NAS or appliance IPs to known BRICKSTORM C2 infrastructure — even post-patch, an undetected implant on a different appliance could resume beaconing; (4) Egnyte Storage Sync sync event logs for resumption of large-volume outbound sync operations to non-corporate cloud destinations, which would indicate an unrotated credential still in use.

Step 5: Post-Incident — Conduct a coverage gap review for all network appliances, NAS devices, and perimeter infrastructure outside EDR visibility (CIS 1.1). Formalize MSP access governance: require MFA for all MSP administrative sessions (CIS 6.5; NIST AC-17), enforce session logging (NIST AU-14), and establish contractual security requirements. Map all third-party trust relationships and assess supply chain adjacency risk (NIST AC-20). Document findings against NIST CSF Detect and Respond functions for board reporting.

NIST Phase: Post Incident

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

Controls: CIS 1.1 (Establish and Maintain Detailed Enterprise Asset Inventory), CIS 6.5 (Require MFA for Administrative Access), NIST AC-17 (Remote Access), NIST AU-14 (Session Audit), NIST AC-20 (Use Of External Systems)

Compensating: For the appliance coverage gap review, export your asset inventory and flag all devices where the OS is BSD-based, Linux-based embedded firmware, or vendor-locked (not supporting agent installation) — these are the exact device classes VerdantBamboo's BRICKSTORM and PLENET were engineered to exploit. Deploy osquery on any appliances that support package installation (Synology supports osquery via SynoCommunity packages) using the query: 'SELECT pid, name, path, cmdline FROM processes WHERE name IN ("python3","dotnet","sh") AND path NOT LIKE "/usr/syno/%";' scheduled every 15 minutes. For MSP session logging where AU-14 tooling is unavailable, require MSP technicians to conduct all work via a jump host you control running OpenSSH with ForceCommand and full session logging to /var/log/msp_sessions/ with append-only permissions. Map each MSP contractual relationship against the NIST AC-20 control requirements and document which MSPs have been granted network-level access versus application-level access — VerdantBamboo's 18-month dwell time was enabled by overly broad MSP network trust that lacked this segmentation.

Evidence: For lessons-learned documentation, preserve: (1) The complete MSP access log timeline showing the original credential compromise date through the 18-month dwell period — this establishes the detection gap baseline for board reporting and future detection SLA targets; (2) The full list of pfSense, Synology, and Dell RecoverPoint appliances identified during the coverage gap review with their EDR/monitoring status — this becomes the remediation backlog driving detection engineering for BSD and embedded Linux targets; (3) All BRICKSTORM, PLENET, and AGENTPSD IOCs (file hashes, C2 IPs, process names, file paths) compiled from eradication findings, formatted as STIX 2.1 for sharing with your ISAC and peer organizations who share the same MSP; (4) M365 Unified Audit Log export covering the full suspected intrusion window, retained per NIST AU-11 (Audit Record Retention) requirements for regulatory and legal review.

Detection Guidance

Primary detection focus is on EDR-blind surfaces: pfSense, Synology NAS, and Dell RecoverPoint appliances. Log sources to prioritize: pfSense syslog (authentication events, outbound connections), Synology NAS access and security logs, Microsoft 365 Unified Audit Log (SharePoint, Exchange, and Azure AD sign-in events), and VPN/firewall NetFlow or session logs. Behavioral indicators to hunt: (1) SSH sessions originating from MSP IP ranges to internal appliances outside business hours (T1021.004); (2) .NET Core or Python interpreter spawned by appliance processes not in baseline (PLENET/AGENTPSD); (3) New or modified startup configurations on BSD/Linux appliances (T1543; D3-SICA); (4) Web shell files in web-accessible directories on pfSense or Synology (T1505.003); (5) Large archive creation or staged data in temporary directories on NAS (T1560); (6) M365 account logins from unusual IPs or with legacy authentication protocols (T1078); (7) Proxy or tunneling traffic patterns indicating C2 over HTTP/S (T1090; T1071.001). Reference NIST AU-6 for audit review cadence and CIS 8.2 for log collection baseline. File integrity monitoring on appliance system directories (D3-SFA) and local account monitoring (D3-LAM) should be enabled where the platform supports it. When BRICKSTORM, PLENET, or AGENTPSD IOCs are published by Volexity or eSentire, cross-reference against available SIEM telemetry immediately.

Indicators of Compromise

Type	Value	Context	Confidence
HASH	`not yet published`	BRICKSTORM BSD variant — Volexity IOCs pending public release; monitor Volexity and eSentire threat intelligence feeds for file hashes	LOW
HASH	`not yet published`	PLENET/GRIMBOLT .NET Core backdoor — IOCs not yet publicly released as of this item's sourcing; subscribe to Volexity public advisories	LOW
HASH	`not yet published`	AGENTPSD Python fallback shell — no public hash available; watch for Python interpreter processes on NAS/appliance hosts outside baseline	LOW

Framework Mappings

MITRE-ATTACK

- **T1543** — Create or Modify System Process
- **T1083** — File and Directory Discovery
- **T1021.004** — SSH
- **T1027** — Obfuscated Files or Information
- **T1055** — Process Injection
- **T1133** — External Remote Services
- **T1059.006** — Python
- **T1090** — Proxy
- **T1078** — Valid Accounts
- **T1560** — Archive Collected Data
- **T1190** — Exploit Public-Facing Application
- **T1098** — Account Manipulation
- **T1071.001** — Web Protocols
- **T1059.004** — Unix Shell
- **T1199** — Trusted Relationship
- **T1078.002** — Domain Accounts
- **T1505.003** — Web Shell
- **T1562.001** — Disable or Modify Tools

NIST-800-53R5

- **SI-3** — Malicious Code Protection
- **SI-4** — System Monitoring
- **AC-6** — Least Privilege
- **SC-7** — Boundary Protection

- **AC-17** — Remote Access
- **AC-20** — Use of External Systems
- **IA-2** — Identification and Authentication (Organizational Users)
- **IA-5** — Authenticator Management
- **AC-2** — Account Management
- **CA-8** — Penetration Testing
- **RA-5** — Vulnerability Monitoring and Scanning
- **SI-2** — Flaw Remediation
- **SI-7** — Software, Firmware, and Information Integrity
- **CM-7** — Least Functionality
- **CM-2** — Baseline Configuration
- **AC-3** — Access Enforcement
- **SR-2** — Supply Chain Risk Management Plan

OWASP-TOP10-2021

- **A04:2021** — Insecure Design
- **A07:2021** — Identification and Authentication Failures
- **A01:2021** — Broken Access Control

CIS-V8

- **5.2** — Use Unique Passwords
- **6.1** — Establish an Access Granting Process
- **6.2** — Establish an Access Revoking Process
- **5.4** — Restrict Administrator Privileges to Dedicated Administrator Accounts
- **6.8** — Define and Maintain Role-Based Access Control
- **6.3** — Require MFA for Externally-Exposed Applications
- **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(a)(1)** — Access Control
- **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
- **CC6.3** — Authorizes, modifies, or removes access

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
T1543	Create or Modify System Process	Persistence
T1083	File and Directory Discovery	Discovery
T1021.004	SSH	Lateral-Movement
T1027	Obfuscated Files or Information	Defense-Evasion
T1055	Process Injection	Defense-Evasion
T1133	External Remote Services	Persistence
T1059.006	Python	Execution
T1090	Proxy	Command-And-Control
T1078	Valid Accounts	Defense-Evasion
T1560	Archive Collected Data	Collection
T1190	Exploit Public-Facing Application	Initial-Access
T1098	Account Manipulation	Persistence
T1071.001	Web Protocols	Command-And-Control
T1059.004	Unix Shell	Execution
T1199	Trusted Relationship	Initial-Access
T1078.002	Domain Accounts	Defense-Evasion
T1505.003	Web Shell	Persistence
T1562.001	Disable or Modify Tools	Defense-Evasion

Sources

Source	URL	Tier
Security News	https://thehackernews.com/2026/06/verdantbamboo-deploys-bsd-variant...	T3

Source	URL	Tier
CVE-2026-22769 Detail - NVD	https://nvd.nist.gov/vuln/detail/CVE-2026-22769	T1
CVE-2026-22769 - CVE Record	https://www.cve.org/CVERecord?id=CVE-2026-22769	T3
DSA-2026-079: Security Update for RecoverPoint for Virtual ... - Dell	https://www.dell.com/support/kbdoc/en-us/000426773/dsa-2026-079	T3
Dell RecoverPoint Vulnerability Exploited for Two Years (CVE-2026 ...	https://www.esentire.com/security-advisories/dell-recoverpoint-vuln...	T3
Microsoft Security Advisory	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-22769	T1

DISCLAIMER

This intelligence report is produced by Tech Jacks Solutions Security Command Center (SCC) for informational purposes only. It does not constitute professional security advice, legal counsel, or an incident response engagement. The information herein is derived from publicly available sources and AI-assisted analysis; while every effort is made to ensure accuracy, Tech Jacks Solutions makes no warranties regarding completeness or timeliness. Organizations should conduct their own validation and consult qualified security professionals before taking action based on this report. Tech Jacks Solutions is not liable for any damages resulting from the use of this information.

Generated 2026-06-08 13:47 UTC by TJS Security Command Center