INTELLIGENCE BRIEFING
Security Command Center
TLP:CLEAR
2026-04-28 18:49 UTC

VECT 2.0 Ransomware Contains Fatal Encryption Flaw, Operates as Wiper for Files Over 131KB

THREAT CAMPAIGN | **CRITICAL** | CVSS 9.5

SCC Item ID	SCC-CAM-2026-0234
Type	Threat Campaign
Severity	CRITICAL
CVSS Base Score	9.5
Affected Products	Windows, Linux, ESXi (VMware); organizations targeted via BreachForums marketplace and TeamPCP supply chain intrusions
Published	2026-04-28T10:01:00
Discovery Source	Rss

Executive Summary

VECT 2.0 is a Ransomware-as-a-Service operation that contains a fatal cryptographic flaw: it permanently destroys any file larger than 128KB with no possibility of recovery, even if a ransom is paid. Virtually every operationally significant file in an enterprise environment, databases, virtual machine images, document archives, exceeds this threshold, making VECT 2.0 functionally a destructive wiper. Organizations targeted through BreachForums marketplace affiliates and TeamPCP supply chain intrusions face irreversible data loss, not a ransomware recovery scenario.

Technical Analysis

VECT 2.0 is a RaaS operation launched December 2025, targeting Windows, Linux, and ESXi environments. The encryption implementation contains a critical nonce management flaw: per Check Point analysis, of four nonces required to reconstruct a decryption key, three are generated ephemerally, used during encryption, and discarded, neither stored locally nor transmitted to attacker infrastructure. Because nonce recovery is mathematically impossible post-encryption, decryption cannot be performed by any party. Files under 131,072 bytes (128KB) may survive intact; all larger files are permanently destroyed. CWE mappings (inferred from cryptographic implementation flaws): CWE-330 (insufficient randomness in nonce generation), CWE-325 (missing required cryptographic step, nonce persistence). MITRE techniques observed include T1486 (Data Encrypted for Impact), T1485 (Data Destruction), T1195/T1195.002 (Supply Chain Compromise), T1490 (Inhibit System Recovery), T1562.001 (Disable/Modify Security Tools), T1547.001 (Boot/Logon Autostart), T1021.004 (SSH lateral movement), T1071 (Application Layer Protocol C2), T1083 (File and Directory Discovery), T1588.003 and T1588.006 (Acquire capabilities). Distribution is formalized through BreachForums affiliate

partnerships and TeamPCP, a threat actor group conducting multi-stage supply chain attacks against security infrastructure. No CVE has been assigned. No vendor patch exists, this is a threat actor implementation flaw, not a victim-side vulnerability. No decryptor is available or possible.

Action Checklist

1. Containment, Isolate any system exhibiting rapid file I/O activity, shadow copy deletion (vssadmin or wmic calls), or security tool tampering. Block egress paths and associated indicators from BreachForums and TeamPCP threat actors (monitor Check Point and Unit 42 reporting for current IOC lists). Disable unnecessary SSH (T1021.004) and remote access paths on ESXi hosts immediately. Segment backup infrastructure from production networks.
2. Detection, Hunt for: vssadmin delete shadows or wbadmin delete catalog execution (T1490); bcdedit /set recoveryenabled no commands; security tool process termination sequences (T1562.001); registry run key modifications (T1547.001); mass file extension changes across file shares; SSH lateral movement from unexpected internal sources. Query EDR telemetry for file enumeration (T1083) followed by rapid write activity. Alert on any process writing to files with VM, database, or archive extensions at scale.
3. Eradication, No patch or decryptor exists. Remove VECT 2.0 payloads identified by EDR. Audit and harden software supply chain touchpoints exploited by TeamPCP (build pipelines, security tool update mechanisms, third-party integrations). Remove unauthorized persistence mechanisms in registry run keys. Rotate credentials on any system where VECT activity or TeamPCP precursor activity is detected.
4. Recovery, Restore exclusively from offline or air-gapped backups verified to predate any VECT 2.0 activity. Do not trust online or network-connected backup copies, VECT targets backup infrastructure. Validate restored files against known-good checksums before returning systems to production. Confirm shadow copies and system restore points are intact on unaffected systems before relying on them. Do not pay the ransom under any circumstances, the decryption keys are mathematically irrecoverable due to VECT 2.0's nonce management flaw, rendering any ransom payment ineffective.
5. Post-Incident, Assess supply chain exposure: audit all third-party security tool update paths for TeamPCP indicators. Implement offline, immutable backup copies (NIST SP 800-53 CP-9) as a mandatory control. Enforce application allowlisting to prevent unauthorized payload execution. Map detection gaps against T1195.002 (supply chain software compromise) and T1562.001 (security tool tampering) and build or tune detection rules. Brief leadership: this incident category produces permanent data loss, not a recoverable ransomware event.

IR / Forensic Enrichment

Triage Priority	IMMEDIATE
Escalation Criteria	Escalate immediately to senior IR leadership, legal counsel, and executive management if: any VECT 2.0 payload execution is confirmed on production systems (permanent data destruction begins within seconds of execution); backup infrastructure shows signs of compromise (VECT specifically targets backup systems, eliminating recovery options); or regulated data (PII, PHI, PCI) resides on affected systems triggering mandatory breach notification timelines under HIPAA (60 days), GDPR (72 hours), or applicable state laws — note that because decryption is mathematically impossible, any affected regulated data must be treated as permanently lost, not temporarily inaccessible.

Recovery Notes	Restore only from air-gapped, offline backups with cryptographically verified checksums predating the earliest confirmed TeamPCP supply chain intrusion timestamp — not merely the VECT execution timestamp, as TeamPCP precursor access may have corrupted or pre-staged malicious updates in online backup copies weeks prior. After restoration, monitor all restored systems for 30 days for TeamPCP re-intrusion via the original supply chain vector by auditing all security tool update events (Windows EventID 4688 for update installer processes, Linux /var/log/dpkg.log or /var/log/rpm.log) against vendor-signed manifests. Do not return ESXi hosts to production until SSH is disabled or restricted to named administrative IPs and all VM snapshot inventories are validated against pre-incident baselines.
Forensic Artifacts	Windows MFT ($MFT via mftdump or analyzeMFT): records mass file modification timestamps with sub-second granularity, enabling precise identification of VECT 2.0 encryption start time and confirmation of the >131KB file destruction boundary — files exactly at or above this threshold will show modification timestamps within a narrow execution window with no corresponding decryption key material | Sysmon EventID 1 and EventID 23 logs: EventID 1 captures vssadmin.exe and wbadmin.exe process creation with full command-line arguments confirming T1490 shadow copy deletion; EventID 23 (FileDelete) records every file VECT staged for destruction, providing the definitive list of permanently lost assets | ESXi /var/log/shell.log and /var/log/hostd.log: records unauthorized SSH session establishment (T1021.004) used for lateral movement to ESXi hosts, plus vim-cmd and esxcli commands used to delete VM snapshots and unmount datastores prior to VECT payload execution against .vmdk files | CI/CD pipeline build logs (Jenkins build.log, GitHub Actions runner _diag logs, or equivalent): TeamPCP supply chain intrusion (T1195.002) leaves artifact injection timestamps in build system logs — specifically, unexpected package hash mismatches, unsigned artifact warnings, or build steps executing from unauthorized staging paths that predate VECT payload delivery by days to weeks | Windows Security EventID 4698 and 4702 (Scheduled Task Created/Modified) and EventID 7045 (New Service Installed): VECT 2.0 and TeamPCP precursors establish persistence via scheduled tasks or services before payload execution; these event IDs in the Security and System logs provide the persistence mechanism timeline and identify the specific account used to register the task or service

Per-Action IR Details

Containment — Isolate any system exhibiting rapid file I/O activity, shadow copy deletion (vssadmin or wmic calls), or security tool tampering. Block known BreachForums-affiliated egress paths and TeamPCP-associated indicators at perimeter and EDR. Disable unnecessary SSH (T1021.004) and remote access paths on ESXi hosts immediately. Segment backup infrastructure from production networks.

NIST Phase: Containment

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

Controls: NIST IR-4 (Incident Handling), NIST SC-7 (Boundary Protection), CIS 4.4 (Implement and Manage a Firewall on Servers), CIS 4.5 (Implement and Manage a Firewall on End-User Devices)

Compensating: On ESXi hosts without EDR: run 'esxcli network firewall set --enabled true' and 'esxcli network firewall ruleset set --ruleset-id sshServer --enabled false' to disable SSH immediately. On Windows: use 'netsh advfirewall firewall add rule name=VECT_BLOCK dir=out action=block remoteip=' for each known IOC. Deploy Sysmon with a config filtering on EventID 23 (FileDelete) and EventID 11 (FileCreate) with target extensions .vmdk, .vhd, .bak, .mdf to detect VECT file-write activity in real time. For backup segmentation, issue 'net use * /delete' on backup servers to force-disconnect all mapped shares immediately.

Evidence: Before isolating, capture: (1) a full memory image using WinPMEM or LiME (Linux/ESXi) to preserve VECT 2.0 in-memory encryption keys and process context before the payload terminates; (2) Sysmon EventID 1 (Process Create) logs showing vssadmin.exe or wmic.exe execution with parent process identifying the VECT loader; (3)

Windows Security EventID 4688 (Process Creation) filtered on vssadmin.exe with CommandLine containing 'delete shadows /all'; (4) ESXi /var/log/shell.log and /var/log/auth.log for unauthorized SSH sessions originating from internal lateral movement sources; (5) current VSS snapshot inventory via 'vssadmin list shadows' before VECT completes deletion.

Detection — Hunt for: vssadmin delete shadows or wbadmin delete catalog execution (T1490); bcdedit /set recoveryenabled no commands; security tool process termination sequences (T1562.001); registry run key modifications (T1547.001); mass file extension changes across file shares; SSH lateral movement from unexpected internal sources. Query EDR telemetry for file enumeration (T1083) followed by rapid write activity. Alert on any process writing to files with VM, database, or archive extensions at scale.

NIST Phase: Detection Analysis

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

Controls: NIST SI-4 (System Monitoring), NIST AU-6 (Audit Record Review, Analysis, and Reporting), NIST AU-2 (Event Logging), CIS 8.2 (Collect Audit Logs)

Compensating: Without SIEM: deploy the following Sysmon-based hunts manually — (1) EventID 1 targeting Image='vssadmin.exe' OR Image='wbadmin.exe' with CommandLine containing 'delete'; (2) EventID 13 (RegistryValueSet) on HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Run and RunOnce for VECT persistence; (3) EventID 23 (FileDelete) or EventID 11 (FileCreate) on extensions .vmdk, .vhd, .vhdx, .mdf, .bak, .zip, .tar at high velocity (>100 events/min as threshold). Use this PowerShell one-liner for file extension monitoring: 'Get-WinEvent -LogName Microsoft-Windows-Sysmon/Operational | Where-Object {$_.Id -eq 11 -and $_.Message -match "\.vmdk|\.mdf|\.bak"} | Select-Object TimeCreated, Message | Export-Csv vect_filehunt.csv'. For ESXi: grep /var/log/shell.log for 'vim-cmd vmsvc/snapshot.removeall' which VECT uses to delete VM snapshots.

Evidence: Capture before analysis: (1) Windows Security EventID 4688 logs filtered on bcdedit.exe with /set recoveryenabled no — this VECT-specific command disables Windows Recovery Environment to prevent post-encryption rollback; (2) Sysmon EventID 9 (RawAccessRead) showing the VECT process reading file system raw blocks during enumeration prior to encryption; (3) Windows Application EventLog entries from VSS (Source: VSS, EventID 8193 or 8194) confirming shadow copy deletion timestamp; (4) File system MFT ($MFT on NTFS) captured via 'mftdump' or 'analyzeMFT' to establish timeline of mass file modification events consistent with VECT's wiper behavior on files >131KB; (5) registry export of HKLM\SYSTEM\CurrentControlSet\Services for any new service entries created by VECT or TeamPCP supply chain implant.

Eradication — No patch or decryptor exists. Remove VECT 2.0 payloads identified by EDR. Audit and harden software supply chain touchpoints exploited by TeamPCP (build pipelines, security tool update mechanisms, third-party integrations). Remove unauthorized persistence mechanisms in registry run keys. Rotate credentials on any system where VECT activity or TeamPCP precursor activity is detected.

NIST Phase: Eradication

Reference: NIST 800-61r3 §3.4 — Eradication

Controls: NIST SI-2 (Flaw Remediation), NIST SI-7 (Software, Firmware, and Information Integrity), NIST IA-5 (Authenticator Management), CIS 2.2 (Ensure Authorized Software is Currently Supported), CIS 2.3 (Address Unauthorized Software)

Compensating: Without EDR for payload removal: use YARA rules targeting VECT 2.0 binary signatures — scan all running processes and file system with 'yara64.exe vect2_rules.yar C:\' and '/usr/bin/yara vect2_rules.yar /' on Linux. For TeamPCP supply chain audit: compare SHA-256 hashes of all security tool update packages against vendor-published manifests; use 'Get-FileHash -Algorithm SHA256 -Path ' on Windows and 'sha256sum ' on Linux/ESXi. For registry persistence removal: 'reg query HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Run' and 'reg delete' on any entry not matching your baseline. For credential rotation without enterprise PAM: use 'net user /domain' for AD accounts and force logout of all active sessions via 'query session' and 'logoff '.

Evidence: Before eradication, preserve: (1) full forensic disk images of affected systems using 'dd if=/dev/sda of=/mnt/evidence/disk.img bs=4M' (Linux/ESXi) or FTK Imager (Windows) — critical because VECT's wiper behavior on files >131KB means evidence may already be destroyed and remaining artifacts are finite; (2) export of all registry run keys via 'reg export HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Run vect_runkeys.reg'; (3) list of all

security tool processes at time of incident via 'tasklist /svc > processes_snapshot.txt' to identify which tools VECT's T1562.001 kill sequence targeted; (4) TeamPCP-linked artifacts in build pipeline logs — specifically, CI/CD tool logs (Jenkins build.log, GitHub Actions runner logs) for unauthorized package injection timestamps; (5) network connection table captured before eradication via 'netstat -anob > connections.txt' to map active C2 channels.

Recovery — Restore exclusively from offline or air-gapped backups verified to predate any VECT 2.0 activity. Do not trust online or network-connected backup copies — VECT targets backup infrastructure. Validate restored files against known-good checksums before returning systems to production. Confirm shadow copies and system restore points are intact on unaffected systems before relying on them. Do not pay the ransom under any circumstances — decryption is mathematically impossible.

NIST Phase: Recovery

Reference: NIST 800-61r3 §3.5 — Recovery

Controls: NIST CP-9 (System Backup), NIST CP-10 (System Recovery and Reconstitution), NIST SI-7 (Software, Firmware, and Information Integrity), CIS 7.2 (Establish and Maintain a Remediation Process)

Compensating: Without enterprise backup validation tooling: use 'certutil -hashfile SHA256' (Windows) or 'sha256sum ' (Linux) to compare restored file hashes against pre-incident checksums stored in a separate, offline inventory. For ESXi VM image validation: run 'md5sum ' against checksums recorded at last known-good backup and cross-reference VMware's vmkfstools integrity checks. To confirm backup predate: parse backup metadata timestamps against the earliest VECT activity timestamp established from the MFT timeline; use 'mactime' from The Sleuth Kit to generate a timeline: 'mactime -b bodyfile.txt -d > timeline.csv'. Do not restore from any backup copy stored on a network share — mount air-gapped media directly.

Evidence: Before initiating recovery, document: (1) 'vssadmin list shadows' output on all unaffected systems to establish which VSS copies survived VECT's T1490 deletion — these are timestamped and can anchor your recovery point; (2) backup catalog integrity check results from your offline backup system (e.g., Veeam backup job logs, rsync manifest files) confirming the last clean backup timestamp predates the earliest VECT IOC; (3) list of all files confirmed destroyed (>131KB, extension .vmdk/.vhd/.mdf/.bak/.zip etc.) generated from MFT analysis — this is your definitive data loss inventory; (4) ESXi datastore listing via 'esxcli storage filesystem list' to catalog which VM datastores were affected before restoration begins; (5) cryptographic hash of VECT ransom note file (typically dropped in each encrypted directory) to confirm campaign variant and submit to threat intelligence platforms.

Post-Incident — Assess supply chain exposure: audit all third-party security tool update paths for TeamPCP indicators. Implement offline, immutable backup copies (NIST SP 800-53 CP-9) as a mandatory control. Enforce application allowlisting to prevent unauthorized payload execution. Map detection gaps against T1195.002 (supply chain software compromise) and T1562.001 (security tool tampering) and build or tune detection rules. Brief leadership: this incident category produces permanent data loss, not a recoverable ransomware event.

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 CP-9 (System Backup), NIST SI-7 (Software, Firmware, and Information Integrity), CIS 7.1 (Establish and Maintain a Vulnerability Management Process), CIS 4.6 (Securely Manage Enterprise Assets and Software)

Compensating: For application allowlisting without enterprise tooling: enable Windows Software Restriction Policies (SRP) or AppLocker in audit mode first — 'Get-AppLockerPolicy -Effective | Test-AppLockerPolicy -Path ' — then enforce to block unsigned executables in %TEMP%, %APPDATA%, and build pipeline staging directories where TeamPCP injects payloads. For Sigma-based detection gap mapping: download the community Sigma ruleset and deploy via 'sigmac -t splunk sigma/rules/windows/process_creation/proc_creation_win_vssadmin_delete_shadows.yml' or equivalent for your log platform; if no SIEM, convert to PowerShell-based event log queries. For immutable backup enforcement on a budget: configure Windows Server Backup with 'wbadmin enable backup' to write-once network share (set ACL: DENY modify/delete for all service accounts), or use MinIO with S3 Object Lock in COMPLIANCE mode on a dedicated offline host.

Evidence: For post-incident review, preserve and submit: (1) complete TeamPCP intrusion timeline reconstructed from CI/CD pipeline logs, showing initial supply chain injection point — this is critical for vendor notification and potential coordinated disclosure; (2) VECT 2.0 binary sample (if recovered pre-execution from quarantine) for submission to AV vendors and VirusTotal for signature development; (3) full list of ATT&CK techniques observed mapped to detection tool coverage gaps — specifically document which T1195.002 and T1562.001 activity went undetected and why; (4) executive briefing document explicitly stating that VECT 2.0's cryptographic flaw renders ransom payment futile and that affected files >131KB face permanent destruction — this must be documented for insurance, legal, and regulatory notification purposes; (5) lessons-learned report per NIST IR-8 (Incident Response Plan) update requirements, specifically updating supply chain risk sections to reflect TeamPCP TTPs observed.

Detection Guidance

Primary behavioral indicators: (1) vssadmin delete shadows, wbadmin delete catalog, or bcdedit /set recoveryenabled no executed by non-admin or scripted processes, map to T1490; (2) security tool processes (EDR agents, AV services) terminated or modified by parent processes not in your approved management toolchain, map to T1562.001; (3) registry run key writes under HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Run or equivalent from unexpected processes, map to T1547.001; (4) mass file write activity targeting extensions associated with databases (.mdf, .bak, .sql), VM images (.vmdk, .vmx, .vhd), and archives (.zip, .tar, .bak), map to T1486/T1485; (5) SSH connections originating from internal hosts not in your approved jump host inventory, map to T1021.004. Supply chain precursor indicators: unexpected changes to security tool binaries or update packages, unsigned or anomalously signed software updates from vendors in your security stack, map to T1195.002. Query SIEM for file rename events exceeding a threshold (e.g., >500 file renames in 60 seconds) on file servers and ESXi datastores. Cross-reference any detections with BreachForums and TeamPCP IOCs from source reporting (Check Point, Unit 42, Industrial Cyber).

Indicators of Compromise

Type	Value	Context	Confidence
URL	`BreachForums marketplace — affiliate recruitment and payload distribution channel`	VECT 2.0 RaaS operation uses BreachForums as a formalized distribution partner for affiliate recruitment and payload delivery; specific URLs not published in available source reporting	MEDIUM
DOMAIN	`Not yet publicly disclosed`	C2 infrastructure associated with VECT 2.0 and TeamPCP has not been released in the source reporting available at this configuration date; consult Unit 42 and Check Point threat intelligence feeds for current IOC releases	LOW

Framework Mappings

MITRE-ATTACK

- **T1083** — File and Directory Discovery
- **T1490** — Inhibit System Recovery
- **T1195** — Supply Chain Compromise
- **T1588.006** — Vulnerabilities
- **T1588.003** — Code Signing Certificates
- **T1071** — Application Layer Protocol
- **T1485** — Data Destruction
- **T1021.004** — SSH
- **T1547.001** — Registry Run Keys / Startup Folder
- **T1486** — Data Encrypted for Impact
- **T1195.002** — Compromise Software Supply Chain
- **T1562.001** — Disable or Modify Tools

NIST-800-53R5

- **CP-9** — System Backup
- **CP-10** — System Recovery and Reconstitution
- **SA-9** — External System Services
- **SR-2** — Supply Chain Risk Management Plan
- **SR-3** — Supply Chain Controls and Processes
- **SI-7** — Software, Firmware, and Information Integrity
- **CA-7** — Continuous Monitoring
- **SC-7** — Boundary Protection
- **SI-4** — System Monitoring
- **CM-7** — Least Functionality
- **IR-4** — Incident Handling
- **AT-2** — Literacy Training and Awareness
- **SC-13** — Cryptographic Protection

NIST-CSF-2

- **RS.MI-01** — Incidents are contained
- **GV.SC-01** — Cybersecurity supply chain risk management program

HIPAA-SECURITY

- **164.308(a)(7)(ii)(A)** — Data Backup Plan
- **164.312(e)(1)** — Transmission Security

ISO-27001-2022

- **A.5.29** — Information security during disruption
- **A.5.34** — Privacy and protection of personal information
- **A.5.21** — Managing information security in the ICT supply chain
- **A.8.24** — Use of cryptography

CIS-V8

- **14.2** — Train Workforce Members to Recognize Social Engineering Attacks
- **15.1** — Establish and Maintain an Inventory of Service Providers

SOC2-TSC

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

MITRE ATT&CK Mapping

Technique ID	Technique Name	Tactic
T1083	File and Directory Discovery	Discovery
T1490	Inhibit System Recovery	Impact
T1195	Supply Chain Compromise	Initial-Access
T1588.006	Vulnerabilities	Resource-Development
T1588.003	Code Signing Certificates	Resource-Development
T1071	Application Layer Protocol	Command-And-Control
T1485	Data Destruction	Impact
T1021.004	SSH	Lateral-Movement
T1547.001	Registry Run Keys / Startup Folder	Persistence
T1486	Data Encrypted for Impact	Impact
T1195.002	Compromise Software Supply Chain	Initial-Access
T1562.001	Disable or Modify Tools	Defense-Evasion

Sources

Source	URL	Tier
Security News	https://thehackernews.com/2026/04/vect-20-ransomware-irreversibly.html	T3
Vect formalizes BreachForums and TeamPCP alliance to push ...	https://industrialcyber.co/ransomware/vect-formalizes-breachforums-...	T3
VECT Ransomware: Why Paying Won't Get Your Files Back	https://blog.checkpoint.com/security/vect-ransomware-why-paying-won...	T3

Source	URL	Tier
TeamPCP's Multi-Stage Supply Chain Attack on Security Infrastructure	https://unit42.paloaltonetworks.com/teampcp-supply-chain-attacks/	T3
TeamPCP Supply Chain Attack — Executive Briefing	https://www.exposuresecurity.com/briefings/teampcp-supply-chain-att...	T3

Generated 2026-04-28 18:49 UTC by TJS Security Command Center