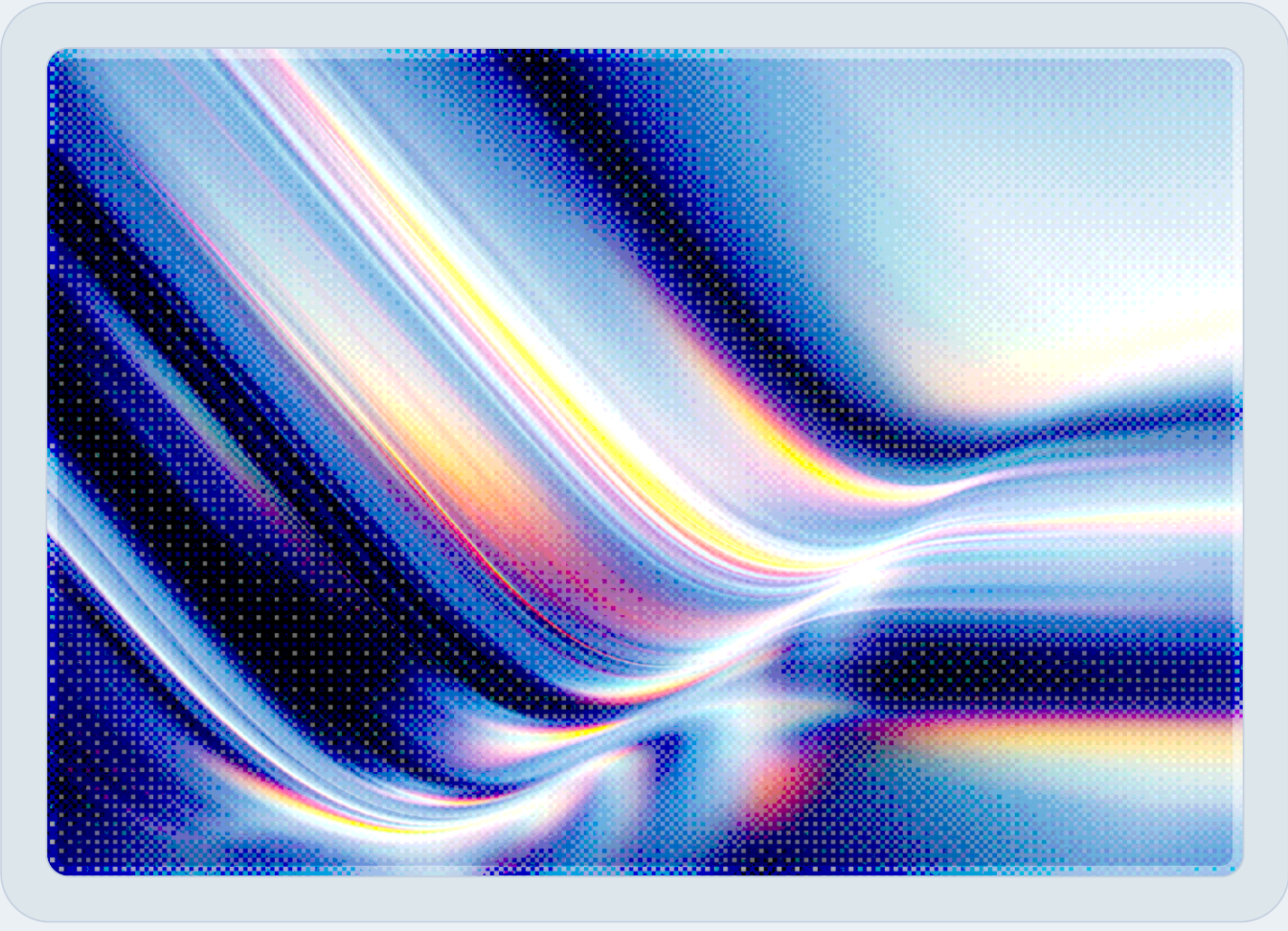
CSAI Foundation | Cloud Security Alliance

VECT 2.0: Paying the Ransom Cannot Recover Enterprise Data

A Flawed Encryption Implementation Turns RaaS Into a Silent, Permanent Wiper

2026-04-29

AI-assisted Rapid Research



CSAI

CSA cloud security alliance®

Key Takeaways

Check Point Research published on April 28, 2026 a technical analysis of VECT 2.0 revealing that all three platform variants — Windows, Linux, and ESXi — share a critical implementation flaw that causes any file larger than 131,072 bytes (128 KB) to be permanently and irrecoverably destroyed rather than encrypted [1]. The flaw lies in how the malware handles the four cryptographic nonces it generates to encrypt large files: it generates a fresh 12-byte nonce for each of four sequential ChaCha20 IETF chunks, but writes only the final nonce to disk, discarding the first three [1][2]. Because ChaCha20 decryption requires the exact nonce used during encryption for each corresponding chunk, the first three-quarters of every large file are mathematically irrecoverable by anyone — including the ransomware operator [3]. Paying the ransom does not restore the data, because no decryptor can exist for keys that were never stored.

The 128 KB threshold is operationally devastating. Database files, virtual machine disk images, backup archives, email stores, financial records, engineering drawings, and the vast majority of documents in active enterprise use all exceed this size. An organization struck by VECT 2.0 is effectively suffering a wiper attack dressed in the extortion framework of ransomware, without the possibility of the recovery that ransomware implicitly promises [4][5].

The threat is compounded by VECT's growing operational alliances. The group formalized partnerships with both BreachForums and TeamPCP in early April 2026, positioning itself to exploit victims already compromised through TeamPCP's March 2026 supply chain attacks on security and AI infrastructure tooling [6][7]. As of late April 2026, VECT's leak site listed 25 organizations, with several among the most recent victims tied to the supply chain campaigns [8]. Security teams should treat any VECT detection as a data-loss event requiring immediate activation of offline backup recovery, independent of any ransom negotiation.

Background

VECT emerged in December 2025 on a Russian-language cybercrime forum as a new Ransomware-as-a-Service (RaaS) offering. The group claimed its first two victims in January 2026 and released VECT version 2.0 in February 2026, expanding platform support from Windows alone to also cover Linux hosts

and VMware ESXi hypervisors [1][9]. The group describes its lockers as custom-built from scratch in C++ — a claim Check Point's reverse engineering broadly corroborated — with separate binaries tailored for each supported environment [1].

VECT's early profile closely resembled several other mid-tier RaaS operations: a leak site on the dark web, tiered affiliate compensation, and targeted intrusions into mid-market enterprises rather than headline-grabbing critical infrastructure. The group's public posture was that of a financially motivated extortion actor with a functional recovery path for paying victims. That profile was contradicted by Check Point's April 28 disclosure, which established that no such recovery path exists for the organization's most valuable data [3].

The RaaS model itself accelerated VECT's reach beyond what its core development team could achieve alone. By licensing their malware and operational infrastructure to external affiliates in exchange for a percentage of collected ransoms, the group distributed both risk and attack surface. This affiliate structure means that the encryption flaw propagated silently to every victim ever struck by any VECT 2.0 affiliate — organizations that may have paid ransoms in the belief they were purchasing data restoration capability [4]. Halcyon researchers separately confirmed that the group targets sectors spanning manufacturing, education, healthcare, technology, and energy, with victims across the United States, Brazil, India, and multiple other countries [9].

Alliance With TeamPCP and BreachForums

The threat profile of VECT shifted materially in March and April 2026 through two formal partnerships. TeamPCP is a threat actor documented by Palo Alto Networks Unit 42 for a series of multi-stage supply chain attacks that injected malware into widely adopted developer tools including Trivy (the container vulnerability scanner), Checkmarx KICS, LiteLLM, and the Telnyx communications SDK [7]. These campaigns compromised downstream consumers of those packages at scale, creating a population of pre-compromised organizations that VECT could then approach with extortion demands [6].

Shortly after the TeamPCP supply chain campaigns made headlines, VECT announced its formal partnership with TeamPCP on BreachForums, explicitly framing the arrangement as an effort to monetize the organizations already affected by those supply chain intrusions [6]. The BreachForums partnership simultaneously elevated the forum from a distribution channel to operational infrastructure, with the platform providing escrow services, affiliate key distribution, and coordination capabilities embedded directly into the ransomware deployment pipeline [8]. On April 15, 2026, VECT claimed two large victims — Guesty and S&P Global — with data exfiltrations reported at 700 GB and 250 GB respectively, which researchers attributed to the TeamPCP compromise pipeline [8].

Security Analysis

The Encryption Flaw: A Cryptographic Dead End

VECT 2.0 divides each file into two categories based on size. Files at or below 131,072 bytes (128 KB) are treated as "small files" and are encrypted as a single unit with a single ChaCha20 IETF nonce that is written to disk alongside the encrypted content [1]. Files above this threshold are treated as "large files" and split into four equal sequential chunks, each encrypted independently using a freshly generated random 12-byte nonce [1][2].

The flaw emerges in how nonces are persisted after use. Across all three platform variants — Windows, Linux, and ESXi — the code generates four nonces, applies each to its corresponding chunk, but writes only the fourth and final nonce to the file on disk [1]. The first three nonces exist only in memory during the encryption pass. Once that memory buffer is overwritten — which occurs before the process exits — the nonces are permanently gone [3]. They are not transmitted to a command-and-control server, not stored in the registry, and not derivable from any information that survives the encryption run [1].

Several published analyses initially described the cipher as ChaCha20-Poly1305 AEAD; Check Point's technical report clarified that all three variants use the raw, unauthenticated ChaCha20 stream cipher in its IETF variant (RFC 8439) via libsodium's `crypto_stream_chacha20_ietf_xor` function [1]. The practical consequence is the same regardless of the label: without the correct nonce for each chunk, the keystream cannot be regenerated and the ciphertext cannot be reversed. The mathematics of the cipher guarantee irrecoverability, not just impracticality.

The boundary of 128 KB matters because it captures essentially every file an enterprise cares about preserving. Virtual machine disk images typically run into gigabytes. Database files — whether SQL Server MDF files, PostgreSQL base tables, or Oracle datafiles — exceed 128 KB from their first substantive record. Corporate email archives, ERP exports, CAD drawings, financial models, backup images, and log archives all fall well above this threshold. The "small file" category protected from permanent destruction is, in enterprise practice, largely confined to configuration snippets, small scripts, and short text documents. Operationally meaningful data is overwhelmingly in the large-file category that VECT 2.0 destroys [5][10].

Why Paying the Ransom Makes No Difference

The extortion model of ransomware rests on a specific economic contract: the operator holds decryption keys and delivers them in exchange for payment, preserving the incentive structure that keeps both parties negotiating in good faith. VECT 2.0 breaks this contract structurally rather than by operator

choice. Even a VECT affiliate who genuinely intends to provide a working decryptor upon payment cannot do so, because the nonces required to produce one were discarded at encryption time [3]. The operator's backend has no record of the first three nonces from any large-file encryption run. There is no key escrow, no deferred transmission, and no side channel by which these values can be reconstructed [1].

This has several downstream implications for incident response that depart significantly from conventional ransomware playbooks. Negotiation cannot be used as a delay tactic to buy recovery time, because there is nothing to recover regardless of the negotiation's outcome. Ransom payment should be excluded from the incident response plan on both policy and practical grounds: it transfers funds to a criminal organization without any prospect of returning data. Insurance coverage contingent on "successful decryption following payment" may not apply, because successful decryption is impossible. Legal obligations around ransom payment notifications — required under some jurisdictions — are triggered by payment, not by recovery outcome, meaning organizations that do pay face both regulatory and financial consequences with no compensating data return [11].

The situation is further complicated for victims who were compromised through the TeamPCP supply chain pipeline. Those organizations may not immediately recognize that their environment was compromised through a software supply chain attack rather than a conventional intrusion, potentially delaying the detection and containment necessary before VECT 2.0 executes [7].

Threat Actor Indicators

VECT 2.0 presents several observable indicators that defenders can use to detect active compromise prior to payload execution or during forensic investigation. The Windows variant deploys a binary named `svc_host_update.exe`, while the Linux and ESXi variant uses `enc_esxi.elf` [9]. Encrypted files receive the `.vect` extension. Check Point's primary analysis identifies the ransom note as `!!!_READ_ME_!!!.txt` [1], though some affiliate deployments have been observed using alternative filenames including `VECT_RECOVERY_GUIDE.txt` and `README_VECT.html` [9]. VECT's data leak site infrastructure has been associated with IP address `158.94.210.11` on port 8000, and the group's email contact in ransom notes uses the address `Qilin[@]exploit[.]im` (distinct from the unrelated Qilin ransomware group) [9]. Desktop wallpaper replacement is also a characteristic behavior of the Windows variant following encryption [9].

These indicators support detection prior to full encryption of the environment. Because the encryption flaw silently discards nonces in memory rather than generating any anomalous disk or network activity specific to destruction, behavioral detection during execution is indistinguishable from legitimate

ransomware. The window for prevention is the intrusion phase — lateral movement, privilege escalation, and staging — before the locker binary runs.

Recommendations

Immediate Actions

Organizations should treat any VECT 2.0 detection as a data-loss incident and activate disaster recovery procedures immediately, without waiting for ransom negotiations to conclude or decryptors to be evaluated. Ransom payment should be excluded from the response plan on both practical and policy grounds; no decryptor exists for files above 128 KB, and payment creates legal, financial, and reputational liability with no compensating benefit.

Security operations teams should search for the known indicators — `svc_host_update.exe`, `enc_esxi.elf`, the `.vect` file extension, and network connections to `158.94.210.11:8000` — across all endpoints, servers, and hypervisor management consoles. ESXi management planes warrant priority attention given VECT 2.0's explicit targeting of VMware infrastructure, where a single successful encryption run can destroy the disk images of an entire virtualized datacenter.

Organizations that use Trivy, Checkmarx KICS, LiteLLM, or Telnyx in their developer toolchains should verify that the versions deployed were not affected by the March 2026 TeamPCP supply chain campaigns and confirm that no unauthorized access resulted from those compromises. The intersection of the TeamPCP victim population and the VECT extortion pipeline means supply chain exposure may be an underappreciated initial access vector in active VECT campaigns.

Short-Term Mitigations

The most direct mitigation against data-destruction outcomes from VECT 2.0 — or from any ransomware-wiper hybrid — is maintaining validated, offline, or air-gapped backups that are provably isolated from the production network and cannot be reached by malware executing on an enterprise host. Backups that are network-accessible from infected systems are at risk of encryption or deletion as part of the same attack. Recovery capability must be verified through periodic restoration tests under realistic conditions; backup existence without restoration validation provides false confidence.

Hypervisor management planes require explicit network segmentation. ESXi management interfaces should not be reachable from general enterprise workstations or from any host that processes email, executes browser sessions, or runs developer toolchains. Management network access should be

restricted to dedicated jump hosts with strong authentication and session recording. WinRM and SMB protocols, which VECT and similar actors use for lateral movement, should be disabled where not operationally required, and SMB signing should be enforced across the environment to reduce east-west traversal opportunities [9][12].

Endpoint detection and response coverage should extend to Linux servers and ESXi hosts, not only to Windows workstations. Many ransomware detection programs remain Windows-centric despite the explicit expansion of groups like VECT to Linux and hypervisor environments. Detection rules that identify rapid file rename operations, mass extension changes, or creation of ransom note filenames should be tuned to fire on Linux and ESXi file systems as well.

Strategic Considerations

VECT 2.0 illustrates a threat category that requires a strategic rethinking of ransomware response playbooks: the ransomware-wiper hybrid, in which a financially motivated extortion framework conceals permanent, irreversible data destruction. Security leaders should review incident response plans specifically for the assumption that ransom payment is an available recovery lever. For VECT 2.0, and potentially for other actors whose encryption implementations share similar defects, that assumption is false. The appropriate strategic posture is to treat ransomware incidents as data loss events by default, reverting to backup recovery rather than decryption as the primary restoration path, and reserving negotiation only for confirmed cases where the actor demonstrably holds functional decryption capability.

The formalization of alliances between ransomware operations, supply chain threat actors, and criminal marketplace infrastructure — exemplified by the VECT-TeamPCP-BreachForums partnership — reflects an industrialization of the attack chain that increases operational scale and reduces the attribution surface. Organizations should monitor threat intelligence feeds for supply chain compromise events affecting developer toolchains as early indicators of downstream ransomware exposure, rather than treating supply chain and ransomware as separate threat categories.

Software supply chain security controls — dependency pinning, artifact integrity verification, and continuous scanning of third-party package repositories — serve double duty as upstream ransomware prevention measures when threat actors like TeamPCP use compromised packages as initial access vectors for subsequent extortion campaigns. The March 2026 supply chain attacks on Trivy, KICS, LiteLLM, and Telnyx demonstrate that security tooling itself is not exempt from being weaponized as an entry point.

CSA Resource Alignment

The VECT 2.0 threat maps directly to several areas of active CSA guidance. The CSA Ransomware in the Healthcare Industry guide establishes foundational principles for backup architecture, incident response escalation, and ransom payment decision frameworks that apply broadly across sectors, though the VECT scenario requires extending those frameworks to account for the possibility that payment yields no technical recovery path [13]. The CSA Cloud Threat Modeling Tabletop Exercise materials specifically include ransomware incident scenarios designed to stress-test cross-functional decision-making under exactly the kind of time pressure that a VECT compromise creates [14].

CSA's Zero Trust Architecture guidance is directly applicable to the lateral movement phase that VECT and its affiliates depend on to reach high-value assets before locker execution. Zero Trust principles — explicit verification of every access request, least-privilege access to hypervisor management planes, microsegmentation of east-west traffic — reduce the blast radius of an initial compromise by constraining how far malware can propagate before detection or containment. The Illumio-eBay microsegmentation case study published through CSA provides concrete implementation evidence for how segmentation at scale can limit ransomware spread in large enterprise environments [16].

The Cloud Controls Matrix (CCM) provides specific control domains relevant to the VECT 2.0 threat: BC-08 through BC-09 address backup and recovery architecture; IR-01 through IR-08 define incident response capability requirements; TVM-07 through TVM-09 establish vulnerability and patch management obligations that would reduce exposure to the supply chain initial access vectors VECT exploits through its TeamPCP partnership. CSA's AI Controls Matrix (AICM), as a superset of the CCM, extends these controls into AI development and deployment environments, which are particularly exposed given TeamPCP's targeting of AI infrastructure tooling such as LiteLLM and KICS.

MAESTRO, CSA's Agentic AI Threat Modeling Framework, surfaces a related risk category: AI development pipelines that rely on compromised open-source tools as dependency inputs can propagate malicious code into production AI systems. MAESTRO's supply chain integrity threat layer and its guidance on validating toolchain provenance apply directly to the TeamPCP attack pattern that feeds the VECT victim pipeline [15].

References

[1] Check Point Research. "VECT: Ransomware by design, Wiper by accident." Check Point Research, April 28, 2026.

[2] The Hacker News. "VECT 2.0 Ransomware Irreversibly Destroys Files Over 131KB on Windows, Linux, ESXi." The Hacker News, April 2026.

[3] Check Point Blog. "VECT Ransomware: Why Paying Won't Get Your Files Back." Check Point, April 2026.

[4] Bleeping Computer. "Broken VECT 2.0 ransomware acts as a data wiper for large files." Bleeping Computer, April 2026.

[5] The Register. "Don't pay VECT a ransom – your big files are likely gone." The Register, April 28, 2026.

[6] Industrial Cyber. "Vect formalizes BreachForums and TeamPCP alliance to push model for industrialized ransomware." Industrial Cyber, April 2026.

[7] Palo Alto Networks Unit 42. "Weaponizing the Protectors: TeamPCP's Multi-Stage Supply Chain Attack on Security Infrastructure." Palo Alto Networks, 2026.

[8] Dataminr. "Cyber Intel Brief: Vect, BreachForums, and TeamPCP Converge." Dataminr, April 2026.

[9] Halcyon. "Emerging Ransomware Group: Vect." Halcyon AI, 2026.

[10] Infosecurity Magazine. "Critical Flaw Turns Vect Ransomware into Data Destroying Wiper." Infosecurity Magazine, April 2026.

[11] SC Media. "TeamPCP-linked VECT 2.0 ransomware unintentionally destroys files larger than 128 KB." SC Media, April 2026.

[12] Cybersecurity News. "New VECT 2.0 Ransomware Destroys Files Over 128 KB Across Windows, Linux, and ESXi." Cybersecurity News, April 2026.

[13] CSA. "Ransomware in the Healthcare Industry." Cloud Security Alliance.

[14] CSA. "Cloud Threat Modeling Tabletop Exercise." Cloud Security Alliance.

[15] CSA. "Agentic AI Threat Modeling Framework: MAESTRO." Cloud Security Alliance, February 2025.

[16] CSA. "How Illumio Simplified eBay's Large-Scale Microsegmentation Project." Cloud Security Alliance.