



# Vect

Technical Analysis — Cti Report

**REVERSE-ENGINEERED REPORT**

**RansomLook** · [ransomlook.io](https://ransomlook.io)

File last modified: 2026-04-30

Analysis date: 2026-04-29

Sample SHA-256: `01881ad57dec5254c53334a63a6c7216edc3dcf0dce02536856bcff9d66fef5d`

## Executive Summary

<b>Family</b>	VECT 2.0
<b>Platform</b>	Windows x64 (PE32+, MinGW-w64 / C++)
<b>Encryption</b>	ChaCha20 stream cipher, libsodium-derived
<b>Sophistication (Operational)</b>	<b>High</b> — full Active Directory tradecraft, ten distinct PowerShell lateral primitives, Safe Mode persistence, comprehensive killchain
<b>Sophistication (Cryptographic)</b>	<b>Low</b> — hardcoded universal key, lost-nonce bug
<b>Exfiltration</b>	<b>None observed</b> — no socket / HTTP / DNS / SMTP transport in the binary, despite the ransom note's leak threat
<b>Recovery feasibility</b>	Partial — small files trivially decryptable with the extracted key; large files structurally destroyed
<b>Sample SHA-256</b>	01881ad57dec5254c53334a63a6c7216edc3dcf0dce02536856bcff9d66fef5d

## Critical Weaknesses

### 1. Hardcoded universal ChaCha20 key

The 256-bit key used to encrypt every file in this build is statically embedded in `.text` at the crypto-state initializer. A cosmetic randomization gesture XORs an unrelated 64-byte region with a single random byte, but the actual cipher key (offsets 64..95 of the 97-byte state) is never modified at runtime.

```
6A 51 09 57 F1 BF 8E CE D9 AA E3 AA 5E 86 12 15
2D 0A BB F1 11 FC D2 A3 9F 02 FF E6 00 0F 6B E8
```

**Impact:** any victim of this build whose files are smaller than 128 KiB can be decrypted immediately. No cryptanalysis required, no operator cooperation needed.

### 2. Lost-nonce flaw → irreversible destruction of large files

For files > 128 KiB the ransomware encrypts four 32 KiB chunks (at `file_size × {0, ¼, ½, ¾}`) using four independent random 12-byte nonces — but the same stack-local buffer is reused for each call to `RtlGenRandom`. Only the **last** nonce ends up appended as the EOF footer. The first three nonces are not stored on disk, not transmitted, not derivable.

**Impact:** 75 % of every encrypted document, database, virtual disk, or backup archive larger than 128 KiB is **cryptographically unrecoverable**, regardless of payment. VECT 2.0 functions as a wiper on enterprise data sets. The operator cannot honour a "we will decrypt after payment" promise even if they wanted to.

### 3. Ransom-note exfiltration claim is not backed by code

The ransom note threatens public release of stolen data. The binary contains:

- No `socket` / `connect` / `send` / `WSAStartup` / `WinHttp*` / `WinInet*` / `bcrypt` / `crypt32` imports

- No URL outside `.onion` for the chat portal
- No staging directory, no archive, no compression for outbound exfil

The only network-adjacent activity is SMB share mounting ( `MPR.dll!WNetAddConnection2A` ) for local read/write file access during encryption, and `WS2_32` address-string utilities. The leak threat is bluff in this build.

## Sample Fingerprint

SHA-256	<code>01881ad57dec5254c53334a63a6c7216edc3dcf0dce02536856bcff9d66fef5d</code>
MD5	<code>5ccea0d983f04d51d102a91b8353717fa</code>
Size	1,456,128 bytes
Toolchain	MinGW-w64 / GCC libstdc++, Itanium mangling, no PDB
Image base	<code>0x140000000</code>
Encryption library	libsodium-derived (ChaCha20, BLAKE2b, X25519, Poly1305 statically linked)
String obfuscation	per-string 64-bit XOR cycle-of-8, lazy decrypt + atexit re-encrypt
Mutex	none

## Killchain at a Glance

```
[1] Stage gate   C:\ProgramData\.vect must exist (presence-only check)
[2] Privilege   OpenProcessToken + GetTokenInformation(TokenElevation)
[3] Recon      ADSI 'objectCategory=computer' + 192.168.1.0/24 fallback
[4] Weaken     Set-MpPreference (Defender), vssadmin delete shadows /all /quiet,
               wevtutil cl, kill 28 services, kill 8 processes
[5] Persist    Run\<<basename>, SafeBoot\Minimal\<<basename>.exe = "Service",
               SafeBoot\Network\<<basename>.exe = "Service"
[6] Pivot (--gpo) Three parallel std::thread workers iterate 10 PowerShell
               lateral primitives over discovered hosts
[7] Encrypt    For each drive: max(4, n/8) scanner threads + max(12, n - n_scan)
               encryptor threads; producer/consumer queue
[8] Visual stamp Render dvm3_wall.bmp 1920x1080 with VECT 2.0 + victim_id;
               SystemParametersInfoW(SPI_SETDESKWALLPAPER)
[9] Note drop  !!!READ_ME!!!.txt in every visited directory
[10] Self-delete cmd /c ping -n 3 127.0.0.1 > nul & del %0
```

## Lateral Movement (10 PowerShell Primitives)

All ten share the same ADSI domain enumeration preamble and the same staging convention `\<host>\C$\ProgramData\<filename>`. Five require credentials passed via `--creds`, five do not.

#	Technique	Remote primitive
1	SMB stage only	<code>Copy-Item</code> to admin share
2	SMB + cmdkey	<code>Copy-Item</code> + local <code>cmdkey /generic:\$pc /user:\$u /pass:\$p</code>
3	WMI Win32_Process Create	<code>Invoke-WmiMethod -Class Win32_Process -Name Create</code>
4	WMI Win32_Process Create (variant B)	duplicate with reordered init
5	DCOM CIM Win32_Process	<code>New-CimSessionOption -Protocol Dcom</code> + <code>Invoke-CimMethod</code>
6	DCOM MMC20.Application	<code>[activator]::CreateInstance(...).Document.ActiveView.ExecuteShellCommand(..., '7')</code>
7	WinRM Invoke-Command	<code>Invoke-Command -Credential \$cred -ScriptBlock { Start-Process }</code>
8	Service install	<code>sc.exe \\\$pc create \$svc binPath= ... start= auto</code> , then start, then delete
9	schtasks	<code>schtasks /create /s \$pc /ru SYSTEM /f, /run, /delete</code>
10	DCOM scheduled task SYSTEM	CIM session over DCOM + <code>Register-ScheduledTask -Principal SYSTEM RunLevel Highest</code>

Service names follow the pattern `DM[A-Z]{4}` (random uppercase). PowerShell timeouts at 60 seconds via `WaitForSingleObject`.

## Detection & Response

### Priority IOCs

Type	Value
File extension	<code>.vect</code> (appended after original extension)
Ransom note	<code>!!!READ_ME!!!.txt</code> (in every encrypted directory)
Wallpaper artefact	<code>%TEMP%\dvm3_wall.bmp</code> (1920×1080, 24-bit)
Stage gate marker	<code>C:\ProgramData\.vect</code> (zero-byte presence check)
Tor chat	<code>vectordntlcr1mfkcm4alni734tbcrnd5lk44v6sp4lqal6noqrgnbyd.onion</code>
Backup contact	Tox <code>1A51DCBB33FBF603B385D223F599C6D64545E631F7C870FFEA320D84CE5DAF076C1F94100B5B</code>
Campaign ID	<code>5cb9f0f9-e171-403f-bed9-a3cd6ce36d1f</code> (in chat URL <code>/chat/&lt;uuid&gt;</code> )
Encrypted file footer	trailing 12 random bytes (ChaCha20 nonce of last chunk)

### High-signal behaviours

- `bcdedit /set {default} safeboot minimal` from a non-admin-tool process
- `vssadmin delete shadows /all /quiet`
- `Set-MpPreference -DisableRealtimeMonitoring $true ...` from `cmd.exe` parent

- `wevtutil cl Application/Security/System/'Windows PowerShell'`
- Service stop sweep covering CommVault, Veeam, MSSQL, Oracle, MySQL, MongoDB, QuickBooks
- Process kill sweep covering `sql.exe`, `oracle.exe`, `mysqld.exe`, Office (`excel.exe`, `winword.exe`, `outlook.exe`), browsers (`firefox.exe`, `thunderbird.exe`)
- Registry write to `HKLM\SYSTEM\CurrentControlSet\Control\SafeBoot\Minimal\<basename>.exe`
- Registry write to `HKLM\SYSTEM\CurrentControlSet\Control\SafeBoot\Network\<basename>.exe`
- `Copy-Item` to `\\<host>\C$\ProgramData\` from a non-administrative tool
- Scheduled task created with name `DM[A-Z]{4}` and immediately deleted
- Service name pattern `DM[A-Z]{4}` created, started, deleted within seconds
- Self-delete pattern `cmd.exe /c ping -n N 127.0.0.1 > nul & del <path>`

## Hunting queries (Sigma-style sketch)

```

title: VECT 2.0 – Safe Mode Persistence Write
detection:
  selection:
    EventID: 13          # Sysmon RegistryEvent
    TargetObject|contains:
      - '\Control\SafeBoot\Minimal\'
      - '\Control\SafeBoot\Network\'
    Details: 'Service'
condition: selection

```

```

title: VECT 2.0 – Stage Gate Drop
detection:
  selection:
    EventID: 11          # Sysmon FileCreate
    TargetFilename: 'C:\ProgramData\.vect'
condition: selection

```

```

title: VECT 2.0 – Wallpaper Artefact
detection:
  selection:
    EventID: 11
    TargetFilename|endswith: '\dvm3_wall.bmp'
condition: selection

```

## Response priorities

1. Containment: isolate hosts where `\\*\C$\ProgramData\.vect` was created in the last 24 h.
2. Triage encrypted files: anything  $\leq$  128 KiB is decryptable with the universal key extracted from this build. Anything  $>$  128 KiB is structurally non-recoverable — do **not** pay; payment cannot recover the lost-nonce chunks.
3. Hunt for the stage gate marker `C:\ProgramData\.vect` across the estate — its presence indicates pre-execution staging.
4. Audit Safe Mode boot configuration on all reachable hosts (`bcdedit /enum {default}`); Safe Mode persistence is designed to survive standard EDR remediation.
5. Pull all 28 service stops and 8 process terminations from EDR telemetry as a single anomaly cluster — that pattern is highly distinctive.

## Threat Positioning

---

The operational profile reads as a competent red-team operator with strong Active Directory tradecraft: the lateral-movement toolkit (10 distinct primitives covering SMB, WMI, DCOM, WinRM, native scheduled tasks, services, MMC) is broader than the typical commodity ransomware loader, the kill list is curated (CommVault and Veeam alongside MSSQL/Oracle/MySQL/QuickBooks suggests deliberate enterprise targeting), and the persistence chain anticipates Safe Mode boot as an EDR-bypass vector.

The cryptographic engineering, by contrast, reads as work by a developer who has heard of "intermittent encryption" and "ChaCha20" but has not implemented either correctly:

- A static-init helper writes a fixed 32-byte block and treats the surrounding 64 bytes (which the cipher never reads) as the "randomized" portion. This is a misunderstanding of which region of the state the cipher uses.
- A four-chunk encryption loop writes its nonces to a stack local that is overwritten on each iteration, with no awareness that the lost nonces are required for decryption.
- ChaCha20 is used without authentication (no Poly1305) despite Poly1305 being statically linked into the binary.
- A 35-entry analysis-tool exe-name blocklist is compiled into `.data` but referenced by no executable code path.

The mismatch between the two skill sets — operationally sharp, cryptographically incompetent — is the dominant signature of this build. It is consistent with a small operator team where the AD tradecraft is owned by one author and the encryption module by another (or by an LLM-assisted developer with no review).

---

## MITRE ATT&CK

ID	Technique
T1486	Data Encrypted for Impact
T1490	Inhibit System Recovery ( <code>vssadmin delete shadows</code> , <code>wevtutil cl</code> )
T1562.001	Disable Tools ( <code>Set-MpPreference</code> )
T1547.001	Registry Run Keys ( <code>HKLM\...\Run\&lt;basename&gt;</code> )
T1547.001	Safe Mode Persistence ( <code>SafeBoot\Minimal/Network</code> )
T1059.001	PowerShell
T1021.002	SMB / Admin Shares (lateral copy)
T1021.003	DCOM (MMC20.Application, CIM Win32_Process)
T1021.006	WinRM
T1047	WMI (Win32_Process Create)
T1053.005	Scheduled Task / Job ( <code>schtasks</code> , <code>Register-ScheduledTask</code> )
T1543.003	Windows Service ( <code>sc.exe \\\$pc create</code> )
T1087.002	Domain Account Discovery (ADSI)
T1135	Network Share Discovery ( <code>NetShareEnum</code> , <code>WNetEnumResource</code> )
T1491.001	Internal Defacement (wallpaper replacement)
T1070.001	Windows Event Log Clearing ( <code>wevtutil cl</code> )
T1070.003	Clear Command History ( <code>PSReadLine\ConsoleHost_history.txt</code> )
T1070.004	File Deletion (self-delete via <code>ping &amp; del</code> )
T1027	Obfuscated Files or Information (XOR string obfuscation)

## Verdict

Axis	Score
Operational tradecraft	High
Cryptographic engineering	Poor
Exfiltration capability	Absent
Persistence robustness	High (Safe Mode)
Recovery feasibility for the victim	Partial — small files yes, large files no
Threat to enterprise environments	High (despite the broken crypto)

VECT 2.0 should be treated as a **destructive incident**, not a recoverable encryption event. Do not rely on payment as a recovery path: the operator does not possess the means to restore the lost-nonce chunks even with intent. Treat any host carrying `.vect`-suffixed files larger than 128 KiB as having lost that data.