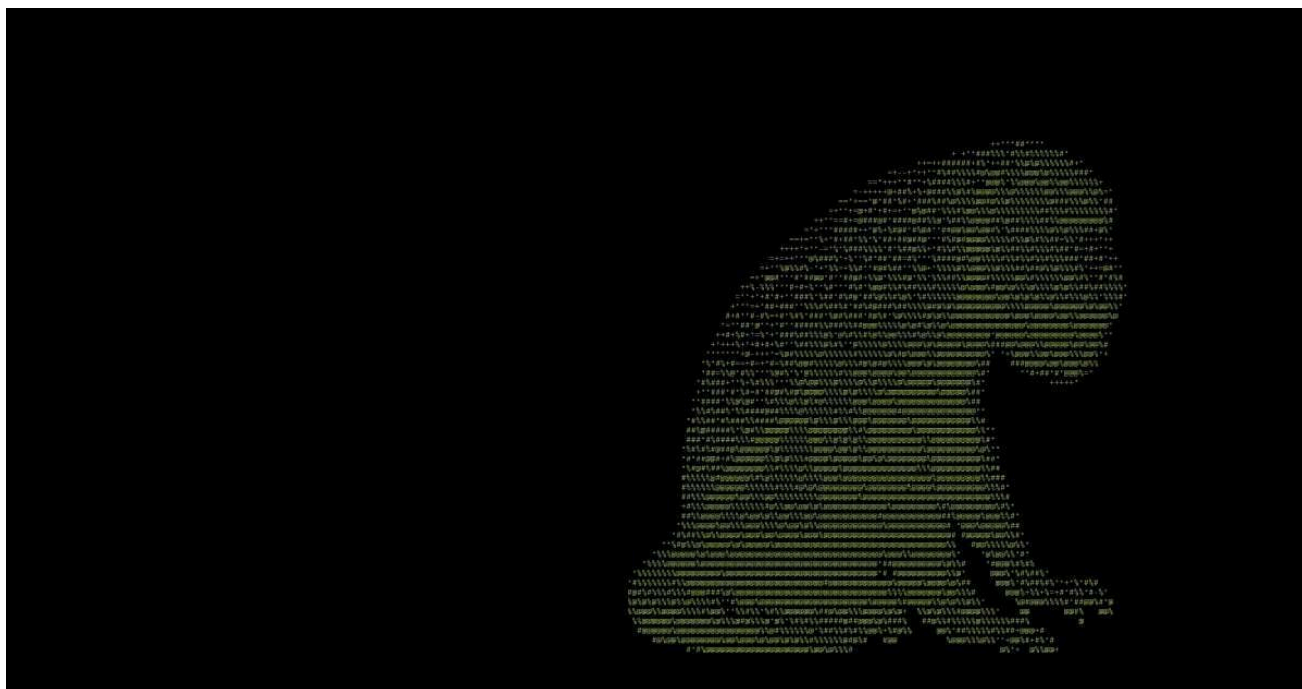


Inside an Active STX RAT Supply Chain Campaign

 cyderes.com/howler-cell/cpuid-hwmonitor-xvpn-dll-sideload-stx-rat

Reegun Jayapaul

June 5, 2026



[Home](#) / [Howler Cell](#) / From Crypto Wallets to a 100M-User VPN: Inside an Active STX RAT Supply Chain Campaign

Key Findings

- **Campaign active after disclosure.** The actor rotated infrastructure and continued delivery rather than going dark.
- **Single delivery mechanism.** All 11 identified packages use CRYPTBASE.dll sideloading into an identical multi-stage unpack chain that loads STX RAT in memory.
- **Centralized staging.** Trojanized bundles distributed from a single Bitbucket repository: amos-trading/dist-internal, attributed to Leda Elacoate (pufferfish11@firemail[.]jcc).
- **Shared C2 infrastructure.** The supp0v3[.]com root domain ties all campaign waves together. Callback subdomain rotated from helloworld to welcome after initial disclosure.
- **Builder-based tooling suspected.** The X-VPN config contains a placeholder referrer value of "changeme," indicating parameters are injected prior to targeted delivery.
- **X-VPN selected as the campaign's highest-value lure.** X-VPN has a reported global user base of over 100 million. The pivot to X-VPN reflects a deliberate expansion toward a privacy-conscious demographic with significant overlap with high-value credential targets.
- **STX RAT confirmed infostealer.** The payload combines remote access with credential and data theft capabilities, confirmed by YARA match and prior analysis.

- **X-VPN service and official installs are not affected.** X-VPN infrastructure, servers, and user accounts were not breached. The risk applies only to users who downloaded the trojanized installer from the attacker distribution channel, not from official sources.
- **X-VPN coordinated disclosure complete.** Howler Cell notified X-VPN on May 18, 2026. X-VPN acknowledged the issue within two business days, shipped a fix in Windows version 77.5.3 on May 28, and is [publishing a coordinated statement alongside this research](#).
- **CWE-427 confirmed.** The X-VPN Windows client contained an uncontrolled search path element (CWE-427) that the threat actor abused. X-VPN has addressed this in version 77.5.3 through stricter DLL loading, startup-time hash verification, and hardened directory permissions.
- **Cyberes clients are protected.** Howler Cell has built and deployed detection coverage for CRYPTBASE.dll sideloading activity and supp0v3[.]com C2 infrastructure.

Summary

A threat actor spent one month building a trojanized software supply chain aimed at a specific type of victim: crypto traders and investors. The lure selection was deliberate: Binance, MEXC, Bybit, Exodus, MetaTrader 5. Each is software used by people likely holding exchange credentials and financial account access.

In 2025, over \$3.4 billion in cryptocurrency was stolen globally, much of it through credential theft and account takeover. Compromised credentials from a machine running crypto trading software are exactly the kind of material that feeds those losses. The actor then pivoted to Steam as a social engineering decoy and to X-VPN, widening the net beyond the crypto-aware user base. Every package used an identical CRYPTBASE.dll sideloading chain to deploy STX RAT in memory. The campaign kept adapting throughout the research period, rotating infrastructure rather than going dark.

Howler Cell Threat Research Team previously documented a supply chain attack targeting [CPUID HWMonitor](#), in which a malicious CRYPTBASE.dll was bundled with a legitimate installer and executed via DLL sideloading to deploy STX RAT. That analysis covered HWMonitor, CPUZ, FileZilla, and LibreOffice packages. Attribution across those packages rests on a convergence of indicators: shared C2 infrastructure under the supp0v3[.]com root domain, an identical STX RAT final payload with code-level similarities across samples, the same DLL sideloading delivery mechanism, and overlapping campaign identifiers in the embedded configurations.

This report expands that scope. Continued monitoring, threat intelligence pivoting, and reverse engineering work identified **seven additional trojanized packages** tied to the same campaign through shared C2 infrastructure. All packages follow the same delivery mechanism. The actor, operating under the alias Leda Elacoate (pufferfish11@firemail[.]cc), built and maintained a Bitbucket repository of trojanized installers over approximately one month, targeting a wide range of user demographics.

Throughout the research period, the campaign kept moving. The actor rotated the C2 callback domain from **helloworld[.]supp0v3[.]com** to **welcome[.]supp0v3[.]com**, updated embedded configurations, and continued staging new packages. The timing of that rotation coincided with the period of active research and public reporting on this campaign. What is clear: this actor was running a deliberate, ongoing credential theft operation, not an opportunistic one-time upload.

The most significant package in this campaign is X-VPN, a consumer VPN with over 100 million reported users. The actor abused a DLL search order condition (CWE-427) in the X-VPN Windows client to load the malicious CRYPTBASE.dll through a repackaged installer.

Howler Cell disclosed this finding to X-VPN on May 18, 2026. X-VPN acknowledged within two business days and shipped a fix in version 77.5.3 on May 28. Ten days from disclosure to patch. X-VPN is publishing a [coordinated statement alongside](#) this research. Users who installed X-VPN from official channels are not affected.

Technical Analysis

What Is STX RAT?

[STX RAT](#) is a remote access trojan with active infostealer capabilities, first documented in 2026. It loads entirely in memory via reflective injection, leaving no file artifacts on disk after the initial sideloaded DLL executes. Confirmed capabilities include:

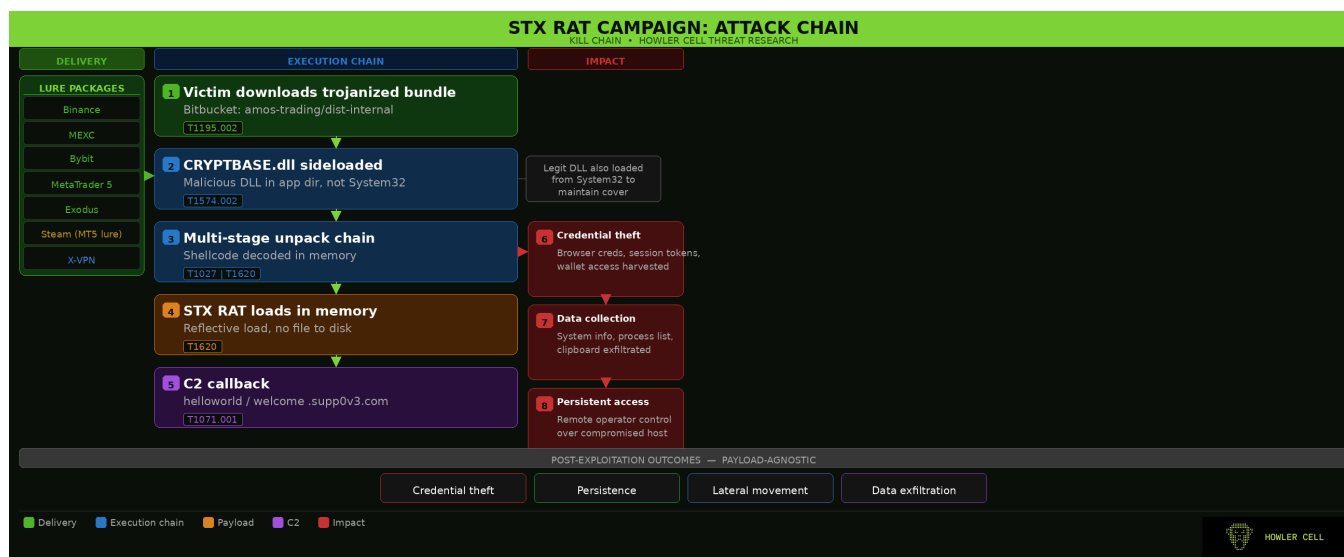
- **Remote access and command execution.** The operator maintains persistent remote control over the compromised host.
- **Credential theft.** Harvests saved browser credentials, session tokens, and system account data.
- **Data collection.** Gathers system information, running process lists, and clipboard content for transmission to the C2 callback.
- **C2 over HTTPS.** All outbound traffic uses standard web protocols, blending with normal browsing activity and avoiding port-based detection.
- **No on-disk persistence.** The RAT operates in memory only. Persistence depends on the installer being re-run or the actor deploying a separate mechanism post-compromise.

For additional technical depth on STX RAT internal structure and capabilities, see: [STX RAT: A New RAT in 2026 with Infostealer Capabilities](#).

Attack Chain Overview

Every package in this campaign follows an identical delivery chain. The diagram below maps the full sequence from trojanized installer to in-memory payload to C2 callback.

Figure 1: STX RAT full attack chain. Post-exploitation outcomes are illustrative. The delivery mechanism and in-memory execution are confirmed across all 11 packages.



Campaign Discovery and Attribution

Following the initial HWMonitor disclosure, pivoting on CRYPTBASE.dll samples surfaced a MEXC cryptocurrency exchange bundle embedding an identical malicious DLL. The bundle traced back to a Bitbucket repository operating under the name **amos-trading** (`https://bitbucket.org/amos-trading/dist-internal/raw/main/vendor/`). All commit history attributes the work to Leda Elacoate, using the address `pufferfish11@firemail[.]cc`. The `firemail[.]cc` domain is an anonymized disposable email service associated with threat actors seeking to minimize attribution risk.

During investigation of the repository, the MEXC package had been removed and replaced with **X-VPN.zip**, last committed **2026-02-26**. This substitution indicated the actor was actively expanding targeting beyond cryptocurrency users to include VPN software consumers.

Figure 2: Bitbucket repository showing X-VPN.zip (229MB) as the active package, last committed 2026-02-26.

amos-trading / Amos / dist-internal

vendor

main Files Filter files

dist-internal / vendor

Name	Size	Last commit
..		
X-VPN.zip	229.48 MB	2026-02-26

Figure 3: Commit metadata confirming author Leda Elacoate (`pufferfish11@firemail[.]cc`), dated January 26, 2026.

```

From bfaaa3027232e548eca9b40d6a1c8aabd747661a Mon Sep 17 00:00:00 2001
From: Leda Elacoate <pufferfish11@firemail.cc>
Date: Mon, 26 Jan 2026 08:14:04 +0000
Subject: [PATCH] Initial commit

```

The HWMonitor, CPUZ, and FileZilla packages were not identified in the Bitbucket repository and appear to have been distributed through separate staging infrastructure. Attribution to the same campaign is based on the same convergence of evidence: identical DLL sideloading technique, code-level similarities in the STX RAT payload, shared supp0v3[.]com C2 infrastructure, and overlapping campaign identifiers. The "tbs" campaign tag appearing across those packages links them to the same operational cluster as the Bitbucket-hosted bundles.

Campaign Timeline and Targeting Evolution

The commit history reveals a methodical, incremental campaign. The actor began with cryptocurrency exchange and trading software as lures, targeting users with likely access to financial accounts, and progressively expanded that lure portfolio across a social engineering decoy and VPN software.

Figure 4: Campaign targeting evolution. Infrastructure rotated post-disclosure rather than going dark.



Table 1: Commit Timeline

Author	Commit Message	Date	Detail
Leda Elacoate	Add WireGuard VPN client	2026-02-26	Trojanized X-VPN installer, CRYPTBASE.dll bundled
Leda Elacoate	Add Steam dist	2026-02-02	steamsetup.exe = renamed MetaTrader 5 installer
Leda Elacoate	Add Exodus dist	2026-02-02	Trojanized Exodus wallet, CRYPTBASE.dll bundled

Author	Commit Message	Date	Detail
Leda Elacoate	Add MetaTrader dist	2026-01-28	Trojanized MT5 installer, CRYPTBASE.dll bundled
Leda Elacoate	Add Bybit dist	2026-01-27	Trojanized Bybit package, CRYPTBASE.dll bundled
Leda Elacoate	Add MEXC dist	2026-01-26	Trojanized MEXC package, CRYPTBASE.dll bundled
Leda Elacoate	Add Binance dist	2026-01-26	Trojanized Binance package, CRYPTBASE.dll bundled
Leda Elacoate	Initial commit	2026-01-26	Repository initialization

Figure 5: Bitbucket diff showing all six packages removed and X-VPN.zip added in the final commit, confirming the deliberate swap.

▼	—	vendor / Binance.zip	📄
		@@ -1,3 +0,0 @@	
1	-	version	https://git-lfs.github.com/spec/v1
2	-	oid	sha256:32b83eeaf6cd645e1b08d8d4633ccdcf6e6f791fc6bab2bec541f88749504f2f
3	-	size	175051373

▼	—	vendor / Bybit.zip	📄
		@@ -1,3 +0,0 @@	
1	-	version	https://git-lfs.github.com/spec/v1
2	-	oid	sha256:c0a8397b2897fe9a7ee120f1914b00a06e493270cc8481b36d193e9f42e7c91b
3	-	size	119142542

▼	—	vendor / Exodus.zip	📄
		@@ -1,3 +0,0 @@	
1	-	version	https://git-lfs.github.com/spec/v1
2	-	oid	sha256:70354be1853eed69825d3c1298029fbd079621697f74250f5099d5e857bb12e0
3	-	size	189838158

▼	—	vendor / mexc.zip	📄
		@@ -1,3 +0,0 @@	
1	-	version	https://git-lfs.github.com/spec/v1
2	-	oid	sha256:e87f9693bfdab6244ca62bb1a2608a9691229515206931639962263014640a33
3	-	size	97156795

▼	—	vendor / mt5setup.zip	📄
		@@ -1,3 +0,0 @@	
1	-	version	https://git-lfs.github.com/spec/v1
2	-	oid	sha256:5d1e31f3952251fbc8671206b56f7a816d7148086cd7e8ed6ce635b2bb0b1920
3	-	size	23159696

▼	—	vendor / Steam.zip	📄
		@@ -1,3 +0,0 @@	
1	-	version	https://git-lfs.github.com/spec/v1
2	-	oid	sha256:aa175f85208e606e26596e6b718a569d47d4052f3c82e88529fb06c662fc8763
3	-	size	22395113

▼	+	vendor / X-VPN.zip	📄
		@@ -0,0 +1,3 @@	
1	+	version	https://git-lfs.github.com/spec/v1
2	+	oid	sha256:ea0ce49a0d7730c6cbcc809ef9c244fb45720c115b3328e8cc293be6bcd7d26c
3	+	size	240628463

The lure selection suggests financial motivation across all phases. Binance, Bybit, MEXC, MetaTrader 5, and Exodus are all platforms whose users are likely to hold exchange accounts, trading credentials, or wallet access: the kind of material that would make credential harvesting from these machines particularly valuable.

The Steam package is notable: on inspection, it contained a renamed MetaTrader 5 installer, suggesting the actor was using the Steam brand to reach a broader population of non-crypto users who would not recognize the MetaTrader 5 name. The pivot to X-VPN in the final commit likely reflects a similar calculation. VPN users frequently overlap with individuals running cryptocurrency infrastructure or handling sensitive communications, making them a logical next target for credential theft.

This level of sustained, incremental campaign management, consistent authorship, a single staging repository, and systematic lure expansion points to one moderately sophisticated actor running a deliberate, broad-spectrum credential theft operation.

X-VPN.zip: Analysis of the Latest Package

X-VPN is a consumer VPN with a reported global user base of over 100 million, and approximately 71 million Google Play downloads at the time of writing. That install base makes this the most significant lure package in the campaign by exposure surface. The threat actor's pivot to X-VPN from crypto-focused software suggests a deliberate calculation: VPN users are privacy-conscious, frequently technically aware, and commonly overlap with individuals handling sensitive credentials or running cryptocurrency infrastructure. That is exactly the victim profile the prior lure packages were targeting.

The team extended analysis to X-VPN.zip (SHA256: ea0ce49a0d7730c6cbcc809ef9c244fb45720c115b3328e8cc293be6bcd7d26c). The bundle contains the same malicious CRYPTBASE.dll alongside legitimate X-VPN and WireGuard client components: X-VPN.exe, WireGuardClient.exe, wireguard.dll, wintun.dll, and associated installer binaries. Despite the commit message referencing a WireGuard VPN client, the bundle is packaged under the X-VPN branding. Both clients are present.

Figure 6: X-VPN.zip file contents. CRYPTBASE.dll (1,213 KB, dated 2026-02-26) is the malicious DLL, timestamped after all legitimate components.

Name	Date modified	Type	Size
bypassConfig	2/26/2026 5:26 AM	File folder	
data	2/26/2026 5:25 AM	File folder	
lib1	2/26/2026 5:26 AM	File folder	
tmp	2/26/2026 5:56 AM	File folder	
app_icon_256.png	1/22/2026 5:51 PM	Portable Network Gra...	32 KB
CRYPTBASE.dll	2/26/2026 6:00 AM	Application extension	1,213 KB
License.rtf	1/22/2026 5:51 PM	Word.RTF.8	28 KB
SensorMonitor.dll	1/22/2026 5:51 PM	Application extension	279 KB
Uninstall X-VPN.exe	2/26/2026 5:25 AM	Application	86 KB
uninstall.exe	1/22/2026 5:51 PM	Application	5,021 KB
wintun.dll	1/22/2026 5:51 PM	Application extension	418 KB
wireguard.dll	1/22/2026 5:51 PM	Application extension	1,310 KB
WireGuardClient.exe	1/22/2026 5:51 PM	Application	4,122 KB
X-VPN.exe	1/22/2026 5:51 PM	Application	69,898 KB
X-VPN.ico	1/22/2026 5:51 PM	Icon File	46 KB
X-VPN_notification.exe	1/22/2026 5:51 PM	Application	4,280 KB
X-VPN_root.exe	1/22/2026 5:51 PM	Application	94,416 KB

On load, CRYPTBASE.dll initiates the multi-stage unpack chain while simultaneously loading the legitimate CRYPTBASE.dll from System32 to maintain normal application functionality. This dual-load pattern is consistent across all samples in the campaign: the legitimate application runs as expected while the malicious chain executes in the background. YARA rule matching confirmed STX RAT as the final in-memory payload, consistent with the [prior HWMonitor analysis](#).

Figure 7: YARA rule output confirming STX RAT attribution across both the HWMonitor and X-VPN samples simultaneously, establishing shared infrastructure.

```
C:\Users\ \Desktop>yara -r STX_RAT.yar .
STX RAT .\HWMonitor\2488654442\stage_4\bottom_00007ffa0884000_00007FFA9B5E4000.bin
STX RAT .\HWMonitor\2488654442\stage_4\bottom_00007ffa0884000_00007FFA9B5E4000.bin.bak
STX RAT .\xvpn\stage_4\stage4_00007ffa99a54000_00007FFA99864000.bin
STX RAT .\xvpn\stage_4\stage4_00007ffa99a54000_00007FFA99864000.bin.bak
```

Campaign Configuration Comparison

The embedded configurations across all packages reveal the campaign's operational structure and a clear infrastructure rotation event. Table 2 maps the full configuration timeline. The X-VPN row is highlighted.

Table 2: Configuration Changes Across Trojanized Packages

Package	Commit Date	Tag	Referrer	Callback
Binance.zip	2026-01-26	click	dll	helloworld[.]supp0v3[.]com
MEXC.zip	2026-01-26	click	dll	helloworld[.]supp0v3[.]com
Bybit.zip	2026-01-27	click	dll	helloworld[.]supp0v3[.]com
mt5setup.zip	2026-01-28	click	dll	helloworld[.]supp0v3[.]com
Exodus.zip	2026-02-02	click	dll	helloworld[.]supp0v3[.]com
Steam.zip	2026-02-02	click	steam	helloworld[.]supp0v3[.]com
X-VPN.zip	2026-02-26	tiktxe	changeme	welcome[.]supp0v3[.]com
FileZilla.zip	N/A	tbs	dll	welcome[.]supp0v3[.]com
HWMonitor.zip	N/A	tbs	monitor3	welcome[.]supp0v3[.]com
CPUZ.zip	N/A	tbs	CPZ	welcome[.]supp0v3[.]com

The consistent use of "click" as the tag and "dll" as the referrer across the first five packages indicates a stable, templated configuration for the initial campaign phase. The referrer value "dll" likely denotes the DLL sideloading delivery mechanism, serving as an internal tracking marker for the infection vector. The "tbs" tag appearing across the HWMonitor, CPUZ, and FileZilla packages is a campaign identifier used by the actor to track and segment infections across different lure packages. It represents a discrete campaign cluster within the same broader operation.

The X-VPN sample marks a clear operational break. The tag shifts to "tiktxe", the referrer is set to the placeholder "changeme", and the callback domain rotates from helloworld[.]supp0v3[.]com to welcome[.]supp0v3[.]com. The "changeme" placeholder is the most significant signal: it indicates this configuration was staged but not finalized at the time of upload, consistent with a **builder-based workflow** where the operator injects campaign tracking parameters prior to each distribution. This points to a semi-commercial or kit-based toolset rather than fully custom infrastructure.

The callback domain rotation from **helloworld[.]supp0v3[.]com** to **welcome[.]supp0v3[.]com** is deliberate infrastructure cycling. Both are subdomains of the same root domain, indicating the actor controls the parent and can spin up new subdomains on demand. Defenders should treat the entire supp0v3[.]com domain family as active C2 infrastructure, not individual indicators.

X-VPN Coordinated Disclosure

Scope: X-VPN's service, infrastructure, servers, and user accounts were not breached or impacted. No user data held by X-VPN was accessed or exposed. Users who installed X-VPN from official channels (the X-VPN website, Microsoft Store, Google Play, or Apple App Store) are not affected. The risk applies only to users who downloaded the trojanized installer from the attacker's distribution channel.

Scope of Impact

The threat actor abused a DLL search order condition in the X-VPN Windows client. CRYPTBASE.dll is a system DLL but is not on Windows' KnownDLLs list, meaning Windows checks the program folder before System32 when loading it by name. By bundling a malicious CRYPTBASE.dll in a repackaged installer and distributing it through the amos-trading Bitbucket repository, the actor caused the malicious DLL to load whenever a victim ran the trojanized bundle. The correct technical classification is **CWE-427: Uncontrolled Search Path Element**. X-VPN did not previously enforce strict path or signature checks when loading DLL dependencies. This is a behavior shared by a broad range of Windows applications, as highlighted by the recent Notepad++ dispute (CVE-2025-56383).

X-VPN classified this issue as High severity, not Critical. Three factors inform that classification: exploitation requires the user to have already run attacker-supplied software from an untrusted source; the official X-VPN client is not affected by the attack path; and X-VPN found no confirmed evidence of in-the-wild exploitation through this specific path.

Disclosure Timeline

- **May 18, 2026.** The Howler Cell Threat Research Team at Cyderes notified X-VPN's security team and shared supporting analysis under coordinated disclosure.
- **May 20, 2026.** X-VPN acknowledged the report within two business days and opened an internal investigation to validate the finding and scope the fix.
- **May 28, 2026.** X-VPN released version 77.5.3 for Windows with the hardening measures described below. X-VPN is publishing a coordinated [public statement](#) alongside this research.

X-VPN's security team shipped a fix within ten days of initial contact. We thank the X-VPN team for their fast and constructive engagement. The full X-VPN official statement is available here: [X-VPN's Response to the Windows DLL Side-Loading Report](#).

The Fix: Version 77.5.3

X-VPN implemented three independent hardening layers in version 77.5.3 to address CWE-427 in the Windows client:

- **Stricter system DLL loading.** CRYPTBASE.dll and other system DLLs are now loaded exclusively from the Windows system folder, regardless of what files exist in the X-VPN program folder.
- **Startup-time hash verification.** Every time X-VPN launches, the client scans every DLL in its program folder and verifies it against a known-good hash list compiled directly into the X-VPN executable. Any DLL not on the whitelist, or with a hash mismatch, causes the client to refuse execution.

- **Per-process DLL load policies.** Each X-VPN process enforces hardened DLL loading rules at startup, restricting which sources are trusted.
- **X-VPN Windows users should update to version 77.5.3 or later.** Download from xvpn.io/download/vpn-win.

Conclusion

The coordinated disclosure with X-VPN produced a concrete outcome: a confirmed fix in version 77.5.3, shipped ten days after initial notification, with X-VPN publishing a [joint statement](#) alongside this research. That is what responsible disclosure looks like in practice.

The broader campaign kept moving after the initial HWMonitor publication. Leda Elacoate rotated infrastructure, updated configurations, and staged new packages rather than abandoning the operation. The consistent CRYPTBASE.dll sideloading mechanism, identical multi-stage unpack chain, and shared supp0v3[.]com C2 root attribute all 11 confirmed packages to a single actor with high confidence.

The builder-based workflow evident in the X-VPN configuration, the deliberate subdomain rotation, and the systematic expansion from crypto-focused lures to VPN software indicate an actor refining their operational process over time. The next wave of packages should be treated as probable. The supp0v3[.]com root domain is an active infrastructure family; any new subdomain appearing in telemetry should be investigated immediately.

Howler Cell will continue monitoring this campaign. All IOCs and detection coverage below are current as of publication.

Detection and Hunting Recommendations

Cyberes clients are protected. Howler Cell has deployed detection coverage for the CRYPTBASE.dll sideloading behavior and supp0v3[.]com C2 infrastructure. The following recommendations apply to all defenders.

- **X-VPN Windows users: update to version 77.5.3 or later.** This version includes stricter DLL loading, startup-time hash verification, and hardened directory permissions that address the CWE-427 condition the threat actor abused.
- **CRYPTBASE.dll load path anomaly.** Alert on any instance of CRYPTBASE.dll loading from a directory other than C:\Windows\System32\ or C:\Windows\SysWOW64\. This is a high-confidence indicator of DLL sideloading and should trigger immediate investigation.
- **Block supp0v3[.]com and all subdomains.** Block the root domain at the perimeter. Alert on any observed connection. Treat any new subdomains as confirmed C2 infrastructure and investigate immediately.
- **YARA-based memory detection for STX RAT.** Apply the STX RAT YARA rule to EDR memory scanning. The rule matched across all samples in this campaign. See the prior HWMonitor post for the rule reference.

- **Behavioral hunting hypothesis.** Hunt for processes that load CRYPTBASE.dll from a non-standard path and subsequently establish outbound HTTPS connections. The legitimate CRYPTBASE.dll is cryptographic base functionality loaded by Windows; any process loading it from an application directory is anomalous.
- **Multi-stage unpack telemetry.** The unpack chain produces in-memory shellcode decode operations detectable via EDR behavioral telemetry. Look for parent processes (legitimate application installers) spawning memory allocation and execution patterns consistent with reflective loading.
- **Software download hygiene.** Enforce policies that restrict software installation to official vendor channels. Third-party hosting platforms, including Bitbucket repositories operated by unknown accounts, should not be approved download sources for production software.

Appendix

File Hashes

Package(s)		SHA-256
Trojanized	Malicious DLL	
Binance, Bybit, Exodus, mt5setup	CRYPTBASE.dll	4b68fcfac8ebe50d5ae489400f33ce01f85de4204eba01a1585fe49002c1582
MEXC	CRYPTBASE.dll	74b5d631cc6802a5790f99a4bfefd9b3dfcfb43007f9fc576f7dfd4eac69d52e
Steam	CRYPTBASE.dll	a2b2fe65819a955b8e2351dd3b75540a9cc38cd0009708a50db2bf9adb8e0657
X-VPN	CRYPTBASE.dll	10f9632491ec37a51d32f41d806e70894f12eed38b74ac2e1f44e9e2226348f

Network Indicators

Indicator	Type	Description
hxtps[://]bitbucket[.]org/amos-trading/dist-internal/raw/main/vendor/	URL	Bitbucket repo hosting all trojanized bundles
helloworld[.]supp0v3[.]com	Domain	C2 callback, initial phase packages

Indicator	Type	Description
welcome[.]supp0v3[.]com	Domain	C2 callback, X-VPN sample post-rotation
supp0v3[.]com	Root Domain	Parent domain of all observed C2 subdomains

Threat Actor Indicators

Indicator	Type	Description
Leda Elacoate	Alias	Author name in Bitbucket commit history
pufferfish11@firemail[.]cc	Email	Disposable email associated with all commits
amos-trading	Repository Name	Bitbucket repo for all trojanized bundles

MITRE ATT&CK

Tactic	Technique ID	Description
Initial Access	T1195.002	Supply Chain Compromise: Compromise Software Supply Chain
Execution	T1204.002	User Execution: Malicious File
Persistence	T1574.002	Hijack Execution Flow: DLL Side-Loading
Defense Evasion	T1574.002	Hijack Execution Flow: DLL Side-Loading
Defense Evasion	T1027	Obfuscated Files or Information
Defense Evasion	T1027.009	Obfuscated Files or Information: Embedded Payloads

Tactic	Technique ID	Description
Defense Evasion	T1620	Reflective Code Loading
Defense Evasion	T1036.005	Masquerading: Match Legitimate Name or Location
Defense Evasion	T1036.008	Masquerading: Masquerade File Type
C2	T1071.001	Application Layer Protocol: Web Protocols

References

1. [Cyderes Howler Cell: CPUID HWMonitor Supply Chain](#)
2. [X-VPN's Response to the Windows DLL Side-Loading Report](#)
3. [eSentire: STX RAT: A New RAT in 2026](#)
4. [Orange Cyberdefense: LibreOffice Fake Installer](#)
5. [Malwarebytes: Fake FileZilla Site Hosts Malicious Download](#)

Stay informed with Howler Cell

Receive the latest Howler Cell news and research directly to your inbox.