Amuneth CTI

CTI-CRPx0 Ransomware

Erik Westhovens

July 2026

REPORT HEADER

Cyber Threat Intelligence Report

Subject: A modular, cross-platform operation combining cryptocurrency theft, data exfiltration, and double extortion

Audience: SOC, Incident Response, Threat Hunting, Endpoint Security, Security Leadership

Date: July 2026

Author: Erik Westhovens

Management Summary

CRPx0 is an emerging but active cybercrime operation that combines ransomware with cryptocurrency theft, seed-phrase harvesting, modular payload delivery, and data exfiltration. The best-documented infection chain begins with OnlyfansAccounts.zip and a deceptive LNK file. On Windows, the malware builds its own Python environment, installs required libraries, and retrieves additional components. macOS shell scripts and LaunchAgent persistence have also been identified. Linux-compatible code is present, although a complete operational Linux delivery chain has not been publicly confirmed.

The operation is notable because monetization begins before encryption. CRPx0 monitors the clipboard and replaces wallet addresses for multiple cryptocurrencies, searches local files for valid BIP39 seed phrases, and can execute additional Python payloads through remote tasking. Encryption starts only after a command from the C2 infrastructure. Targeted files receive the .crpx0 extension, while the unique Fernet key and host metadata are transmitted to operator-controlled infrastructure.

Public reporting supports an overlap with the DataBreachPlus and TwizAdmin ecosystem and a leak portal used to advertise victims and sell access to stolen data. The operators' identity, organizational structure, and precise affiliate model remain uncertain. Victim totals and claimed exfiltration volumes are actor-controlled and have not been independently verified. Defenders should therefore treat CRPx0 as a capability-driven operation and prioritize its repeatable execution, persistence, C2, collection, and impact behaviors.

Key Takeaways

- CRPx0 is not a standalone locker: cryptocurrency theft, seed-phrase harvesting, remote tasking, exfiltration, and encryption form one modular operation.
- Windows and macOS targeting are confirmed; Linux capability is technically plausible but has not been observed as a complete public infection chain.
- The attack abuses legitimate components such as Python, pip, curl, wscript, and PowerShell, making behavioral detection more valuable than signatures alone.
- Public victim claims indicate continued activity in July 2026, including several healthcare and dental organizations, but leak-site listings are not independently confirmed incidents.

Chapter 1

1. Threat Overview

CRPx0 combines a Python-based loader architecture with several parallel monetization methods.

Aryaka Threat Research Labs documented CRPx0 as a financially motivated, multi-platform campaign. The framework profiles infected hosts, establishes persistence, sends periodic beacons, updates itself, executes additional scripts, replaces cryptocurrency addresses in the clipboard, harvests seed phrases, and ultimately deploys ransomware. This combination makes CRPx0 substantially broader than a conventional encryptor.

In April 2026, Proofpoint Emerging Threats released signatures covering CRPx0 DNS and TLS activity, installation and continuous heartbeats, seed-scan events, victim profiling, and payload delivery. This indicates that several network behaviors were stable enough to support operational detection content.

Activity remained visible in ransomware monitoring during July. Open sources reported several simultaneous claims, including a concentration among US dental practices and other healthcare-related organizations. These entries originate from actor leak sites and aggregators and should not be represented as independently verified breaches.

Analyst Assessment

- Assessment: high potential impact, medium-high confidence in the documented malware chain, and low confidence in actor identity and total operating scale.
- The operation can escalate from opportunistic cryptocurrency theft to large-scale exfiltration and encryption.
- CRPx0 is used both as a ransomware label and as an operational name for the broader DataBreachPlus/TwizAdmin-linked campaign.

Chapter 2

2. Actor and Campaign Profile

Public evidence describes an organized malware and extortion operation but does not support definitive attribution to named individuals.

Aryaka's primary analysis describes an actively managed ecosystem with a kill switch, update functionality, centralized tasking, and a DataBreachPlus leak portal. Breakglass Intelligence separately linked CRPx0 to exposed Malware-as-a-Service infrastructure, the DataBreachPlus Telegram identity, and a later TwizAdmin panel. The overlap points to a broader platform supporting clipper, stealer, RAT, and ransomware capabilities.

Multiple campaigns or customers may be able to use the same backend capabilities. The term 'CRPx0 group' is therefore useful as an operational label, but it is not proof of a stable organization with known members. Public reporting does not establish a country attribution or a confirmed Ransomware-as-a-Service revenue-sharing structure.

During Aryaka's investigation, the leak portal claimed 38 victims, 23 published leaks, and more than 10,000 TB of stolen data. The portal advertised one-time access to current and future leaks for USD 500 in cryptocurrency. These claims demonstrate an additional monetization strategy, but the figures remain operator-controlled.

Attribution Caveats

- Confirmed: financial motivation, centralized C2, modular payloads, and double extortion.
- Probable: overlap with DataBreachPlus/TwizAdmin and a service-oriented operating model.
- Unconfirmed: operator identity, geographic origin, affiliate structure, and the accuracy of leak-site statistics.

Chapter 3

3. Initial Access and Delivery

The documented chain exploits curiosity and risky user behavior to trigger a deceptive LNK loader.

The known Windows chain begins with OnlyfansAccounts.zip. The archive contains Onlyfans Accounts.lnk and decoy content promising free account credentials. The exact distribution method has not been confirmed; researchers assess that victims may encounter the archive while searching for free or leaked access to paid content.

When opened, the LNK launches cmd.exe with caret-obfuscated commands. It creates %APPDATA%\sys32data, downloads launcher.vbs from fanonlyatn.xyz, and starts it with wscript.exe. A decoy accounts.txt file is opened in Notepad while a Python runtime, pip, and libraries such as requests, pyautogui, and pyperclip are installed in the background.

launcher.vbs retrieves call2.py. This orchestrator creates the working directory and downloads last.zip and finderx.zip, which are extracted as sys32.py and finder.py. On Windows, call2.py generates a hidden VBScript and PowerShell execution path. On Unix-like systems, it uses a hidden .sys32data directory.

Early Breakpoints

- Block or inspect ZIP archives containing LNK files when they originate from browsers, email, or untrusted sources.
- Detect wscript.exe or cmd.exe invoking curl, installing Python, or launching payloads from AppData.
- The visible accounts.txt decoy must not be treated as evidence that no background activity occurred.

Chapter 4

4. Execution, Persistence and C2

CRPx0 relies on legitimate scripting tools, redundant persistence, and periodic HTTPS tasking.

sys32.py checks a remote kill switch at databreach.space/cry/control.php. A stop instruction removes Windows Startup or macOS LaunchAgent persistence and terminates the malware. An update instruction retrieves a new script version from fanonlyatn.xyz/get_build.php, overwrites the local code, and starts the replacement.

Windows persistence includes System32.vbs in the Startup folder and the Run value HKCU\Software\Microsoft\Windows\CurrentVersion\Run\WindowsHealthMonitor. The malware also removes StartupApproved records that could disable its autorun entry. On macOS, it writes ~/Library/LaunchAgents/com.cryptoprice.guard.plist.

The initial beacon transmits the hardware ID, operating system, computer name, Python version, build ID, public IP, username, administrative status, and agent ID. Background threads then provide continuous heartbeats and clipboard monitoring. Pending tasks allow the operator to start seed scanning, update scripts, change wallet replacement addresses, deploy additional Python payloads, or initiate encryption.

Execution and Persistence

- Hunt for the combined presence of sys32data, System32.vbs, WindowsHealthMonitor, and com.cryptoprice.guard.plist.
- Correlating Python or pip installation, wscript or PowerShell, and new autorun artifacts provides higher precision than any single IOC.
- HTTPS C2 can resemble ordinary encrypted traffic, making endpoint context and known request patterns essential.

Chapter 5

5. Theft, Exfiltration and Encryption

The malware can steal value before encryption becomes visible and uses C2 tasking to scale impact per host.

The clipper recognizes addresses for Bitcoin, Ethereum, Tron, Dogecoin, Litecoin, Solana, Ripple, and Bitcoin Cash. After detecting a match, it requests an attacker-controlled replacement from api_address_match.php, overwrites the clipboard, and reports the original address, replacement address, cryptocurrency type, host ID, and timestamp to the C2.

The seed scanner launches finder.py and searches local drives for text, log, configuration, and PDF files. It uses a BIP39 wordlist and validation logic to identify valid 12- or 24-word seed phrases. A match is transmitted with host metadata, the source filename, and a base64-encoded copy of the file contents.

After receiving the encryption command, the malware downloads crypter.py, creates a virtual environment when required, and installs the cryptography library. It inventories documents, media, databases, archives, email, source code, and engineering files. A unique Fernet key is sent to C2, and targeted files are encrypted with the .crpx0 extension. System directories are excluded to keep the operating system available for extortion and victim communication.

Impact Chain

- Clipboard manipulation creates direct financial impact and can precede ransomware deployment.
- Seed-phrase harvesting creates an immediate risk of irreversible cryptocurrency theft.
- Containment must stop C2, exfiltration, and key transmission; terminating only the locker process is insufficient.

Chapter 6

6. Platform Coverage and Risk Assessment

Windows is the best-documented platform, macOS support is operational, and Linux remains a credible development direction.

The complete Windows chain from LNK execution to Python loading, persistence, tasking, and ransomware has been documented. For macOS, researchers identified delivery scripts for .app, .pkg, and .dmg packages, LaunchAgent persistence, and use of the same Python orchestrator. This is sufficient to treat macOS as a confirmed target platform.

The code contains Linux paths, exclusions, and platform-independent Python components. Aryaka did not identify a dedicated Linux delivery or initial-access mechanism, however. The most accurate assessment is that Linux capability is technically plausible and partially implemented, but operational deployment has not been publicly confirmed.

Business risk is highest where users can install scripts or runtimes without control, egress to newly registered domains is unrestricted, and endpoint telemetry on macOS or developer systems is weak. The combination of data theft, cryptocurrency theft, and ransomware expands financial, legal, privacy, and operational impact.

Platform Confidence

- Windows: confirmed and fully documented.
- macOS: confirmed through platform-specific delivery and persistence.
- Linux: compatible logic and exclusions are present, but active delivery remains unconfirmed.

Chapter 7

7. Detection and Threat Hunting

The strongest detection opportunities occur during multi-stage setup, autorun creation, network beaconing, and pre-encryption activity.

Begin retrohunting for fanonlyatn.xyz, databreach.space, and the infrastructure listed in the IOC table across DNS, proxy, TLS SNI, firewall, and EDR network telemetry. Proofpoint Emerging Threats published signatures 2068529 through 2068539 for domain activity, heartbeats, seed scanning, victim profiling, and payload delivery.

High-value Windows patterns include an LNK spawning cmd.exe, curl downloading from a script host, wscript.exe executing under %APPDATA%\sys32data, PowerShell downloaders, a private Python runtime in the same directory, silent pip installation, and pythonw.exe referenced from Startup or Run keys. On macOS, .sys32data and com.cryptoprice.guard.plist are important hunt leads.

Pre-impact ransomware hunting should monitor for crypter.py, installation of the Python cryptography library, broad file discovery, enumeration of many targeted extensions, POST activity to /crpx0/notify.php, and mass creation of .crpx0 files. Seed scanning may appear as Python processes rapidly opening large numbers of text, configuration, and PDF files.

Hunt Priorities

- Priority 1: confirmed network IOCs combined with process ancestry.
- Priority 2: persistence artifacts and hidden working directories.
- Priority 3: broad file access, cryptography setup, and .crpx0 extension creation.

Chapter 8

8. Recommendations and Outlook

Break the chain early, restrict script execution, and treat every CRPx0 detection as a potential data and cryptocurrency compromise.

Block known IOCs at DNS, web proxy, firewall, and endpoint controls. Quarantine ZIP and LNK delivery from browser downloads and email, restrict wscript and cscript where they are not required, and monitor Python runtime installation in user-writable directories. Application control for script interpreters and download utilities can prevent the loader from building its environment.

Responders should not wait for the .crpx0 extension. Isolate affected hosts, preserve memory and relevant script files, collect network evidence, assess wallet and seed-phrase exposure, and determine which files were accessed or exfiltrated. Cryptocurrency assets associated with potentially exposed seed material should be moved using a clean, trusted device and newly generated recovery material.

Recover from offline, immutable, and tested backups. Rotate credentials and secrets stored in local configuration, source-code, or document files. Over the near term, expansion through new lures, domains, and platform-specific delivery is more likely than a completely redesigned framework because the current modular architecture already supports operational variation.

Recommended Actions

- Urgent: block IOCs, hunt for persistence, and isolate confirmed hosts.
- Incident response: scope exfiltration, wallet exposure, and seed compromise in addition to ransomware impact.
- Program level: strengthen application control, egress filtering, macOS telemetry, and immutable recovery.

SOC Reference

CRPx0 Indicators of Compromise

Use these indicators as a starting point for retrohunting. Validate matches with process ancestry, DNS or TLS context, and timeline evidence because infrastructure can change or be reused by third parties.

How to use this reference

- Normalize hashes as SHA-256 and deobfuscate domains only inside controlled security tooling.
- Treat payload-hash matches as high confidence; domain matches require additional context.
- After a match, also investigate persistence, seed scanning, clipboard activity, and exfiltration.

Type	Indicator	Context
Domain	fanonlyatn[.]xyz	Primary delivery, builds, and update hosting
Domain	databreach[.]space	Control endpoint and leak ecosystem
Domain	caribb[.]ru	Initial lure hosting and /crpx0/notify.php C2
Domain	mekhovaya-shuba[.]ru	Ransomware notification C2
Domain	beboss34[.]ru	Ransomware notification C2
SHA-256	e1af62979961bc3c4761096dc7ea0ba54c4059fd4a32c296b493324303a7d071	OnlyfansAccounts.zip
SHA-256	1b8c15f17fca23fd9e47be3b07bd34ccc352bc6c3dbbbf940b7652d44fe5ae06	Onlyfans Accounts.lnk
SHA-256	1a489600a433b303e91f859f58b5bc58becbf3f07a1acb7826ed46302326331b	launcher.vbs
SHA-256	596da56de46a85f47fcab615d918d1f5b34f0d4d2e571d762f2249fdc917074c	call2.py
SHA-256	1a623fa9bff1cd560f49e7eb3ddf10e429ee167aaf0a79a5b422dd9468c5efdb	crypter.py
SHA-256	9d9783f57fd543043e0792d125831883259c823a5eaa69211e5254db4db4eaec	finder2.py / seed harvester
SHA-256	d2b135df0f71544de711e4188dd385df0a915894cdaab5228d045d5cc1a14449	sys32.py

Source: Aryaka Threat Research Labs, Appendix A. Domains are safely defanged in this report.

Reference Material

Sources

Aryaka Threat Research Labs - crpx0 Ransomware Operations: Double Extortion, Crypto Theft, and Network Footprint

https://www.aryaka.com/docs/reports/crpx0-ransomware-operations-report.pdf

Primary 2026 technical analysis and main source for the infection chain, persistence, C2, clipper, seed scanner, ransomware, IOCs, and MITRE ATT&CK mapping.

Aryaka Threat Research Lab - crpx0 Ransomware Operations

https://www.aryaka.com/reports-and-guides/crpx0-ransomware-operations-report/

Publication page summarizing the principal findings and defensive context.

SecurityWeek - Free OnlyFans Lure Used to Spread Cross-Platform CRPx0 Malware

https://www.securityweek.com/free-onlyfans-lure-used-to-spread-cross-platform-crpx0-malware/

Published May 12, 2026. Independent reporting on the multi-platform chain and leak-portal claims.

Proofpoint Emerging Threats - Ruleset Update Summary 2026/04/02 v11163

https://community.emergingthreats.net/t/ruleset-update-summary-2026-04-02-v11163/3254

Source for ET signatures 2068529-2068539 covering CRPx0 DNS, TLS, heartbeats, seed scanning, victim profiling, and payload delivery.

Breakglass Intelligence - CRPX0 / DataBreachPlus and TwizAdmin reporting

https://intel.breakglass.tech/

Additional technical reporting on exposed CRPx0/DataBreachPlus and TwizAdmin infrastructure. Used for ecosystem context; attribution remains cautious.

Red Piranha - Threat Intelligence Report July 7 to July 13, 2026

https://redpiranha.net.au/news/threat-intelligence-report-jul-7-jul-13-2026

Recent activity summary reporting CRPx0 impact across six countries during the reporting week.

CTIWATCH - CRPx0 victim listings

https://ctiwatch.com/

Leak-site aggregation used for recent July claims. Listings are not independently verified breaches and are treated only as actor claims.

Partner Profile

About Amuneth

Amuneth provides intelligence-led security operations designed to help organizations detect, investigate, and contain modern threats across identity, endpoint, network, and cloud environments. Our reporting bridges executive decision-making and operational action by combining threat context, analyst judgment, and practical detection guidance.

For CTI consumers, this final page gives reusable context on the operating model behind the report and clarifies how Amuneth supports ongoing monitoring, escalation, and proactive hunting beyond the specific topic covered in the report.

Security Operations Center

- Continuous monitoring across endpoint, identity, cloud, and network telemetry.
- Triage and escalation workflows that prioritize verified risk over raw alert volume.
- Operational coordination with customer stakeholders during incidents, containment, and follow-up investigation.

Threat Hunting Capabilities

- Hypothesis-driven hunting for identity abuse, stealthy persistence, lateral movement, and data exfiltration patterns.
- Targeted hunts based on current CTI findings, campaign tradecraft, and environment-specific risk signals.
- Cross-source correlation between endpoint, Microsoft 365, Entra ID, firewall, proxy, and cloud telemetry to validate or dismiss emerging attacker behavior.

CTI and Reporting Approach

Amuneth reports are built to support both management and frontline defenders. Each report explains why the development matters, how the threat behaves, where detection opportunities exist, and which defensive actions should be prioritized next.

This standardized format keeps reporting visually consistent while making room for actor-specific findings, malware analysis, campaign tradecraft, and strategic risk interpretation.