Hive Pro

Threat Level

Amber

HiveForce Labs

THREAT ADVISORY

ATTACK REPORT

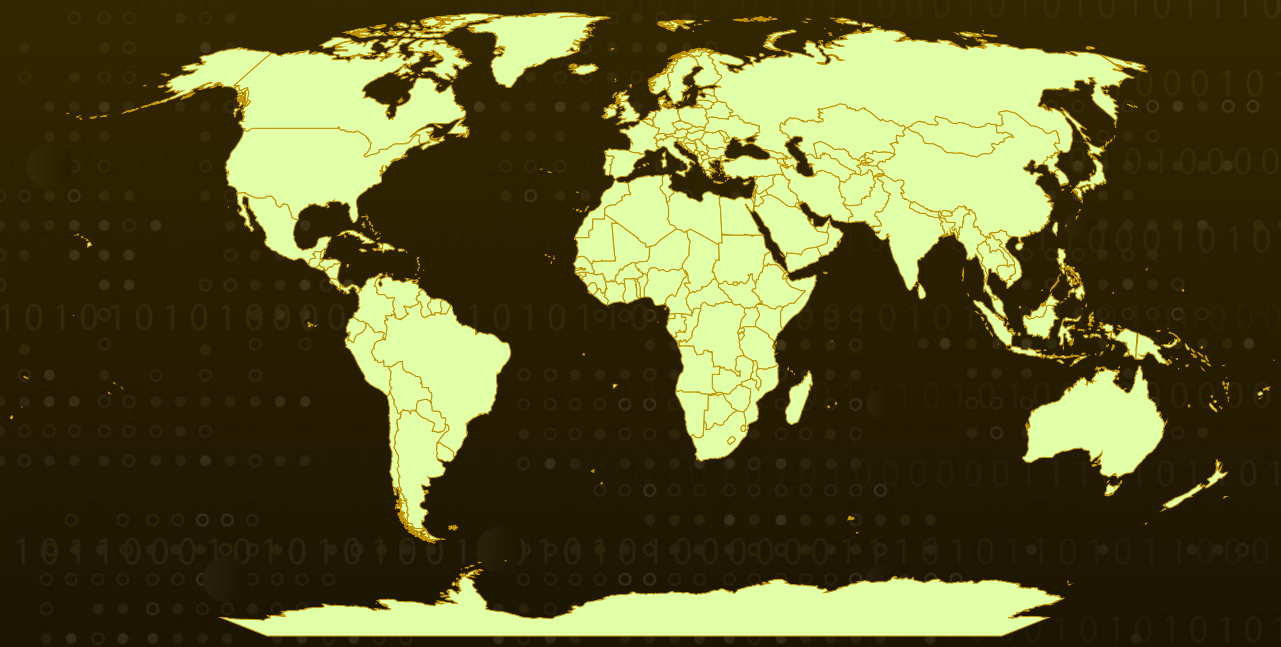
ClipXDaemon Clipboard Attack: Linux Malware Targeting Crypto Payments

Date of Publication	Admiralty Code	TA Number
March 06, 2026	A1	TA2026062

Summary

First Seen: February 2026
Targeted Region: Worldwide
Targeted Platform: Linux (X11 Desktop Environments)
Targeted Products: Cryptocurrency Wallets - Bitcoin, Ethereum, Litecoin, Monero, Tron, Dogecoin, Ripple, TON
Targeted Industry: Cryptocurrency
Malware: ClipXDaemon
Attack: ClipXDaemon is an autonomous Linux clipboard hijacker that targets cryptocurrency users operating in X11 desktop environments. Delivered through a bincrypter-based encrypted loader, the malware monitors clipboard contents every 200 milliseconds and replaces copied cryptocurrency wallet addresses with attacker-controlled alternatives. It operates entirely without command-and-control infrastructure, monetizing victims directly through manipulated wallet addresses during cryptocurrency transactions.

Attack Regions



Attack Details

#1

In early February 2026, a new Linux malware strain named ClipXDaemon. It spreads through a multi-stage infection chain that begins with an encrypted shell-script loader created using bincrypter, an open-source tool for protecting shell scripts. The loader contains an encrypted payload hidden inside the script. During execution, the payload is decoded from base64, decrypted with AES-256-CBC, decompressed with gzip, and executed directly from memory. Because the decrypted components never touch the disk, traditional static inspection becomes difficult. The loader's structure resembles one used in earlier ShadowHS campaigns, though no confirmed link connects the two.

#2

After running, the in-memory dropper prints a harmless-looking message to appear legitimate. It then decodes an embedded ELF binary and writes it to disk using a random filename made of several characters followed by numbers. The file is placed in a normal user directory, avoiding the need for administrator privileges and blending in with ordinary programs. The dropper marks the file as executable, launches it quietly in the background, and adds a command that ensures the program runs again during future user login sessions.

#3

The installed payload is a 64-bit Linux program linked to X11 libraries. It first checks whether the system is using Wayland. If Wayland is detected, the program stops immediately because Wayland prevents global clipboard monitoring. On systems using X11, the malware detaches itself and disguises its process name to resemble a kernel worker thread, making it less noticeable in process lists.

#4

Once active, the program repeatedly checks the system clipboard every 200 milliseconds using X11 selection APIs. Clipboard text is scanned with encrypted patterns designed to recognize cryptocurrency wallet addresses, including Bitcoin, Ethereum, Litecoin, Monero, Tron, Dogecoin, Ripple, and TON.

#5

When a matching wallet address appears, the malware replaces the clipboard contents with an attacker-controlled address. It quietly takes ownership of the clipboard through a hidden window and returns the substituted address when the user pastes the data. The program contains no command-and-control communication, sends no network requests, and holds no hardcoded servers. Profit occurs only if a victim unknowingly pastes the altered address and completes a cryptocurrency transfer. Because the malware operates without an external infrastructure, detection depends primarily on analyzing behavior on the infected system rather than monitoring network activity.

Recommendations

Restrict Execution from User-Writable Directories: Implement application control policies that prevent or alert on execution of binaries from user-writable paths such as ~/.local/bin/. This disrupts the malware's deployment strategy of dropping payloads into userland directories that blend with legitimate binaries.

Audit User-Level Persistence Mechanisms: Continuously monitor modifications to ~/.profile, ~/.bashrc, and other user-level autostart files. Establish baselines for these files and alert security teams on any unauthorized changes, as ClipXDaemon persists by appending execution lines to ~/.profile.

Detect Kernel Thread Process Masquerading: Deploy endpoint detection rules that identify processes with kernel-thread naming conventions (e.g., kworker/) running under non-root user contexts. Correlate prctl(PR_SET_NAME) system call modifications with suspicious execution ancestry to detect process masquerading techniques used by this malware.

Deploy Host-Based Behavioral Detection: Since ClipXDaemon operates without network communication, traditional network security controls are ineffective. Prioritize endpoint detection and response (EDR) solutions capable of behavioral analysis, focusing on clipboard access patterns, process genealogy anomalies, and unauthorized file creation in user directories.

Implement File Integrity Monitoring on Login Scripts: Deploy file integrity monitoring (FIM) solutions that track changes to user shell initialization files such as ~/.profile and ~/.bashrc. Unauthorized modifications to these files should generate high-priority alerts for investigation.

Potential MITRE ATT&CK TTPs

Tactic	Technique	Sub-technique
Execution	T1059: Command and Scripting Interpreter	T1059.004: Unix Shell
	T1106: Native API	
Persistence	T1547: Boot or Logon Autostart Execution	
	T1546: Event Triggered Execution	T1546.004: Unix Shell Configuration Modification
Defense Evasion	T1036: Masquerading	T1036.004: Masquerade Task or Service
	T1027: Obfuscated Files or Information	T1027.013: Encrypted/Encoded File
	T1620: Reflective Code Loading	
	T1497: Virtualization/Sandbox Evasion	
	T1140: Deobfuscate/Decode Files or Information	
Discovery	T1082: System Information Discovery	
Collection	T1115: Clipboard Data	
Impact	T1565: Data Manipulation	T1565.001: Stored Data Manipulation

Indicators of Compromise (IOCs)

TYPE	VALUE
Ethereum Wallet Address	0x502010513bf2d2B908A3C33DE5B65314831646e7
Monero Wallet Address	424bEKfpB6C9LkdfNmg61pMEnAitjde8YWFsCP1JXRYhfu4Tp5EdbUBjCYf9kRBYGzWoZqRYMhWfGAm1N5h6wSPg8bSrbB9
Bitcoin Wallet Address	bc1qe8g2rgac5rssdf5jxcyytrs769359ltle3ekle
Dogecoin Wallet Address	DTkSZNdtYDGndq1kRv5Z2SuTxJZ2Ddacjk
Litecoin Wallet Address	ltc1q7d2d39ur47rz7mca4ajzam2ep74ccdwvqre6ej
Tron Wallet Address	TBupDdRjUscZhsDWjSvuwdevnj8eBrE1ht
File Paths	~/.local/bin/<random_name>, ~/.profile
SHA256	87ab42a2a58479cf17e5ce1b2a2e8f915d539899993848e5db679c218f0e7287, 23099eea9c4f85ff62a4f43634d431bbed0bf6b039a3f228b1c047f1c2f0cd11, b6bb28160532400eafad532842e4ba9add6d6bbba4f7e7c85e3dbb650369eb00

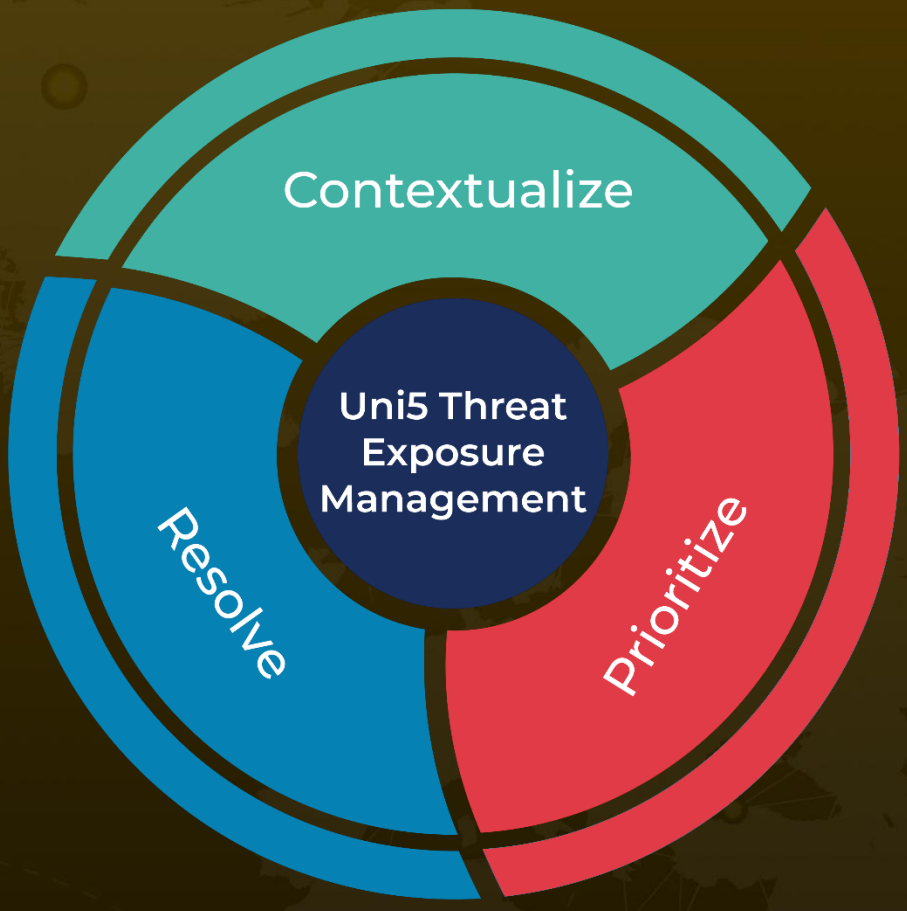
References

https://cyble.com/blog/clipxdaemon-autonomous-x11-clipboard-hijacker/

What Next?

At **Hive Pro**, it is our mission to detect the most likely threats to your organization and to help you prevent them from happening.

Book a free demo with **HivePro Uni5**: Threat Exposure Management Platform.



REPORT GENERATED ON

March 06, 2026 • 2:00 AM

More at www.hivepro.com