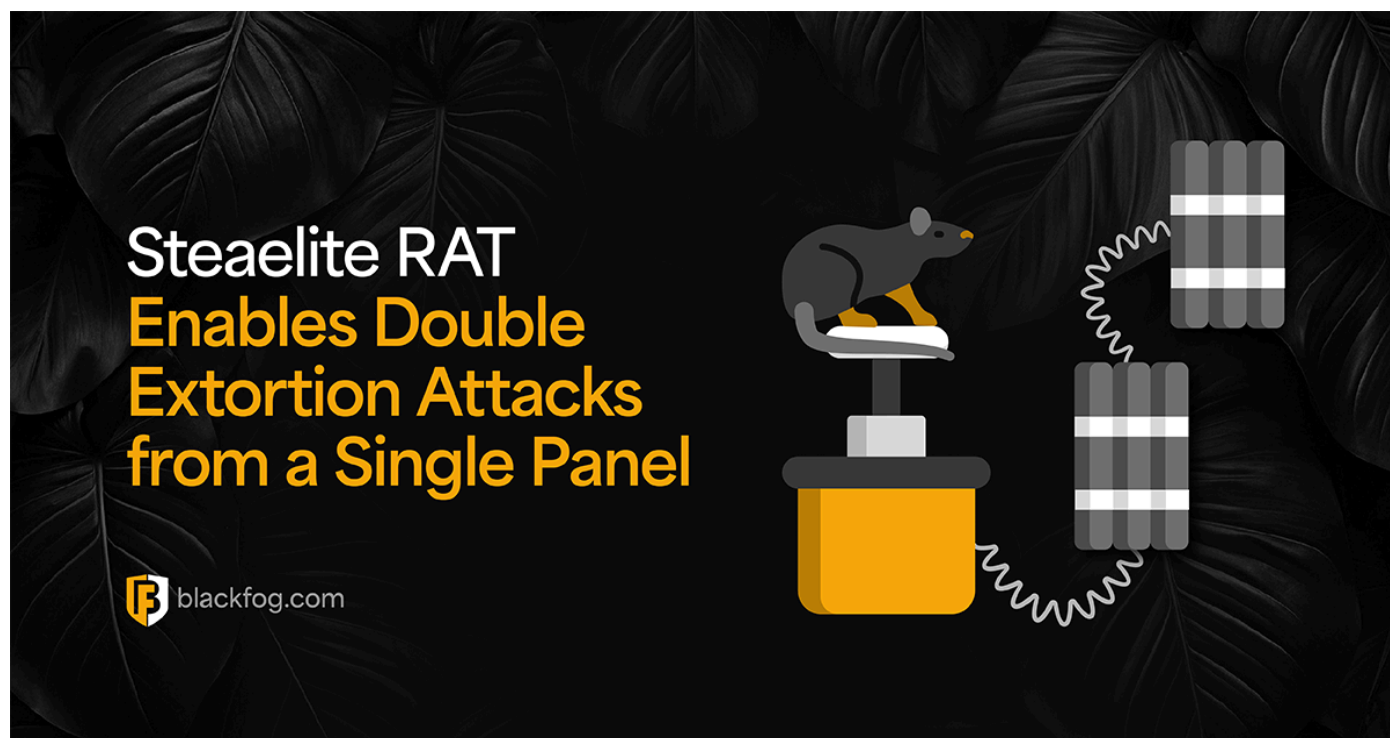


Steelite RAT Enables Double Extortion Attacks from a Single Panel

 blackfog.com/steelite-rat-double-extortion-from-single-panel

Wendy McCague

February 25, 2026



|Last Updated: February 24th, 2026|6 min read|Categories: [Ransomware](#), [Data Exfiltration](#), [Exploits](#)

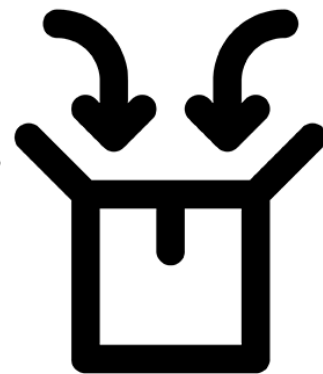
Contents

A new remote access trojan called Steelite is being sold on underground cybercrime networks. The tool gives operators browser-based control over infected Windows machines, covering remote code execution, credential theft, live surveillance, file exfiltration, and ransomware deployment from a single dashboard.

What makes Steelite notable is what it bundles together: data theft and ransomware, traditionally separate parts of the cybercrime toolchain, are packaged into one web panel, with an Android ransomware module already in development.



What makes **Steelite** notable is what it bundles together: **data theft and ransomware**, traditionally separate parts of the cybercrime toolchain, are packaged into one web panel, with an Android ransomware module already in development.”



Distribution and Market Presence

Steelite first appeared on underground cybercrime networks in November 2025, describing itself as a “best Windows RAT” with “fully undetectable” (FUD) capabilities. The seller advertises Windows 10 and 11 compatibility, stabilised HVNC monitoring, and banking application bypass.

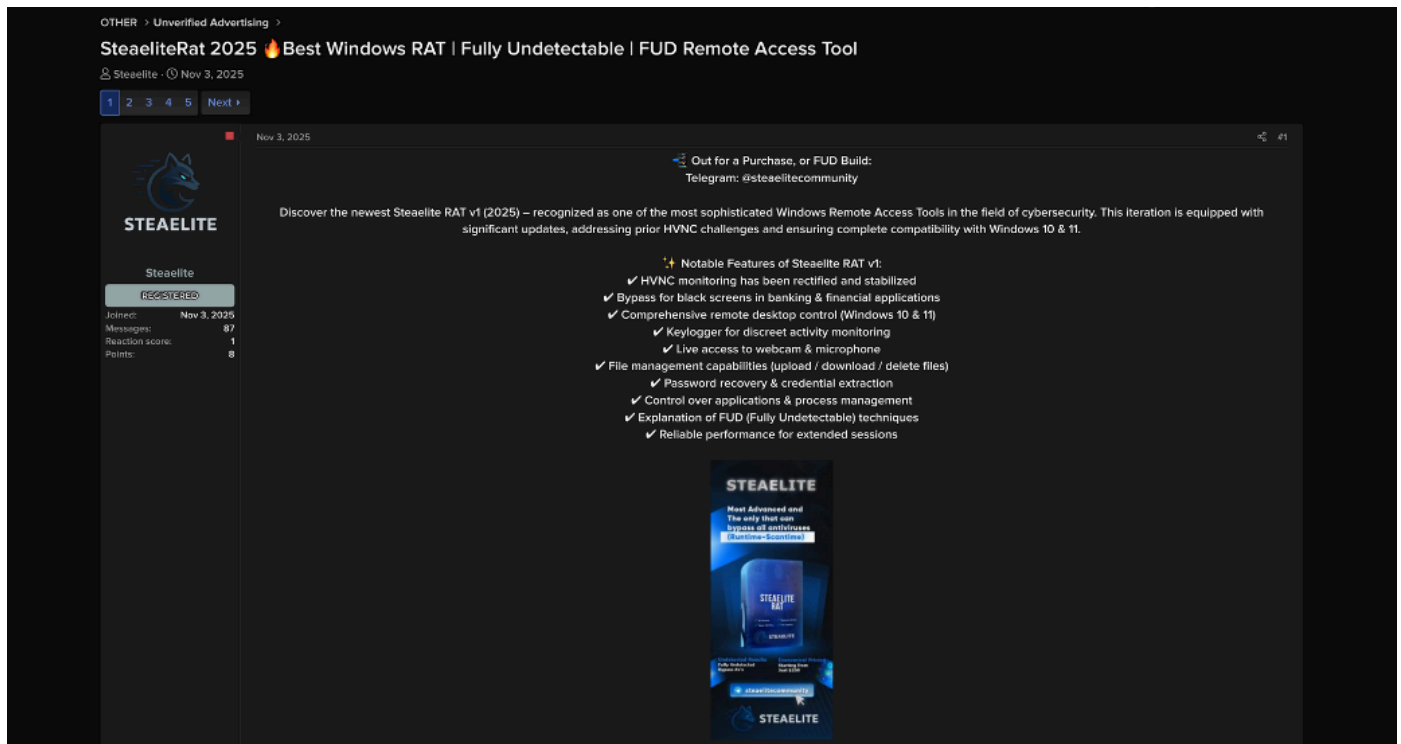


Figure 1. One of the Steelite forum listings.

The listing has been bumped consistently across multiple forum threads with 87 messages at the time of writing, and a promotional video demonstrating the tool's capabilities has been published on YouTube, a common distribution tactic for commercial remote access trojans looking to reach buyers outside of traditional forum ecosystems.

Inside the Steelite Control Panel

Steelite's operator interface runs entirely in the browser. The dashboard displays connected victims with their computer name, hardware ID, CPU and RAM usage, and operating system version in real-time.

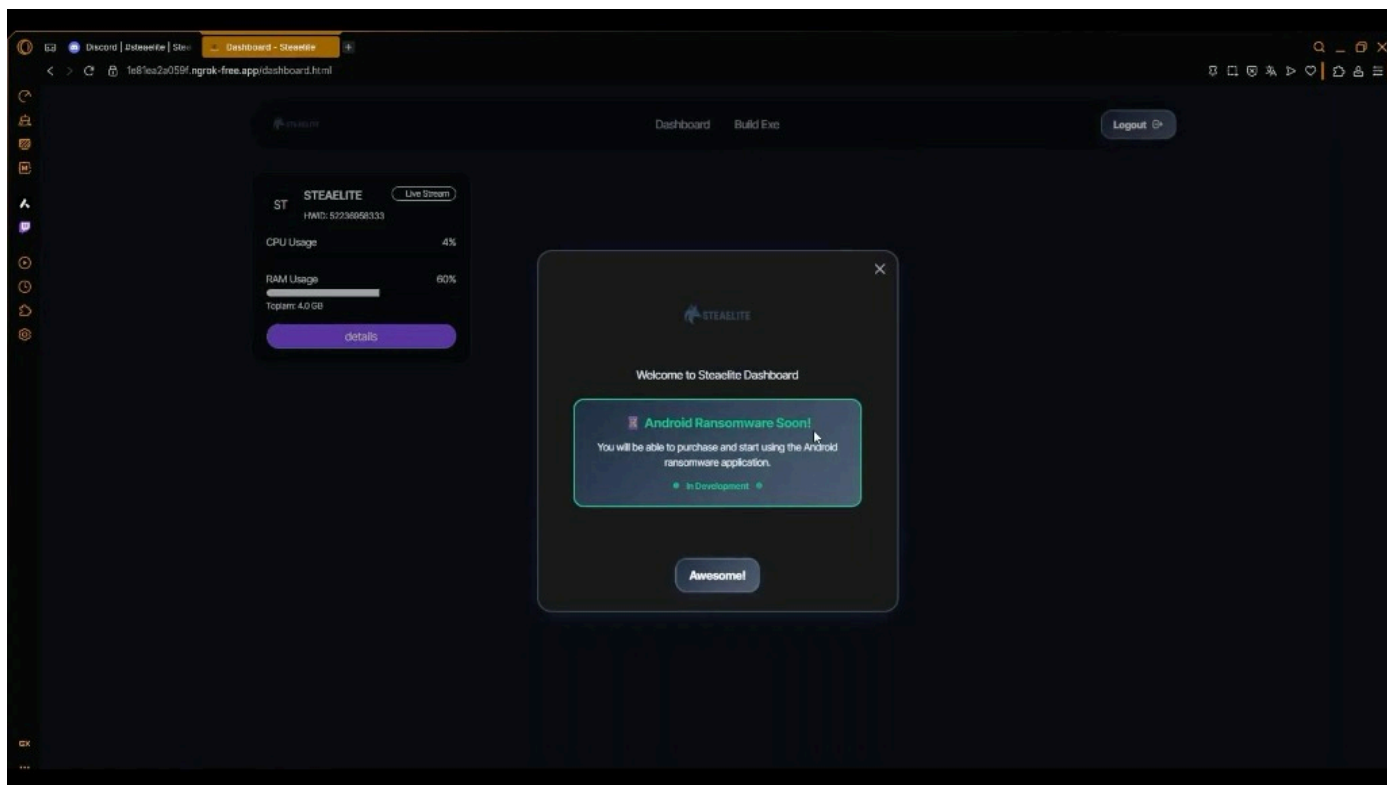


Figure 2. The dashboard advertising the upcoming Android ransomware module.

The welcome popup that greets operators on first login advertises an “Android ransomware” module marked “in development,” signalling expansion into mobile extortion.

The primary toolbar includes modules for remote code execution, file management, live streaming, webcam and microphone access, process management, clipboard monitoring, password recovery, installed program enumeration, location tracking, arbitrary file execution, URL opening, DDoS attacks, and VB.NET payload compilation.

Below the primary toolbar, operators can expand two additional sections. The “advanced tools” panel exposes ransomware deployment, hidden RDP, Windows Defender disabling and exclusion management, and persistence installation.

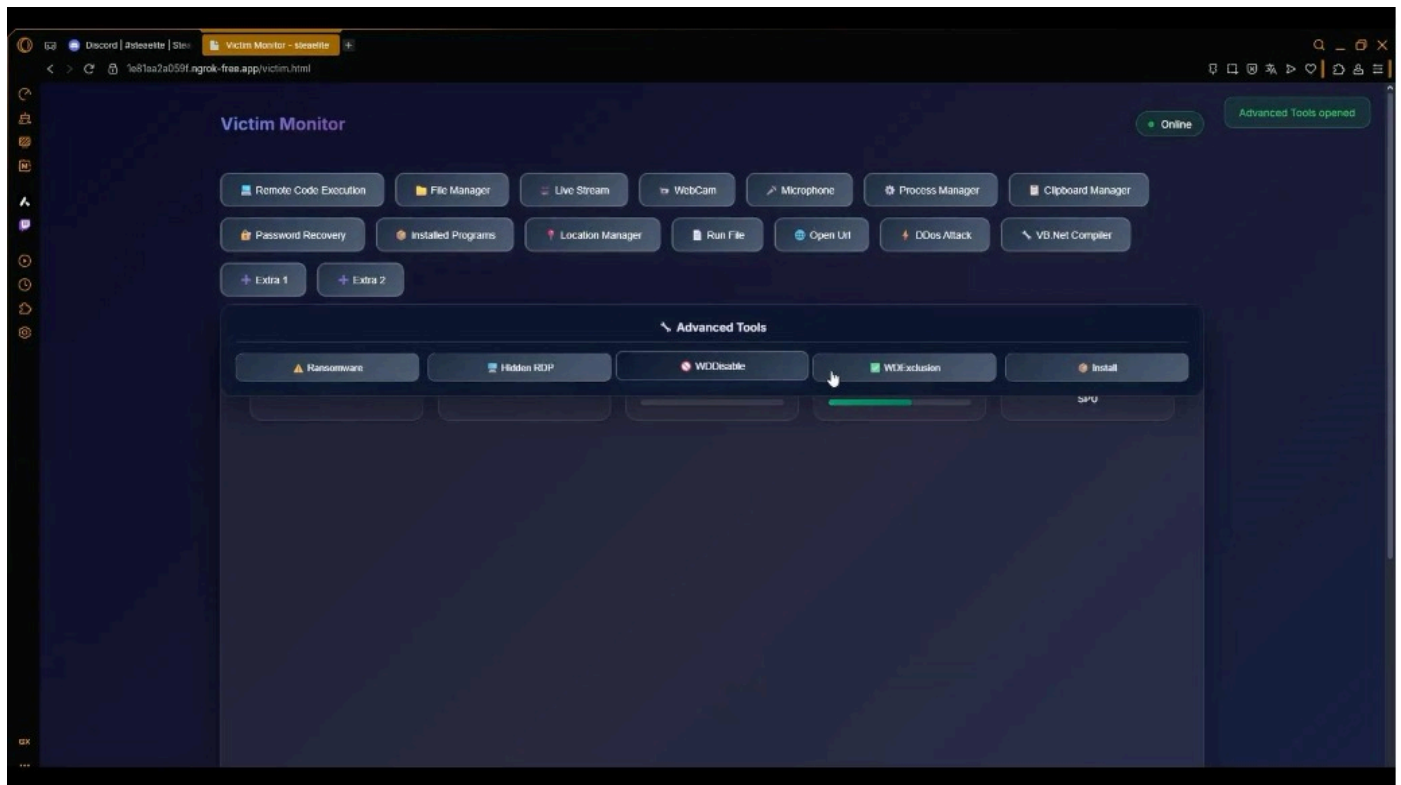


Figure 3. The advanced tools section.

The “developer tools” panel adds keylogging, client-to-victim chat, file searching, USB spreading, bot killing (removing competing malware), message box delivery, wallpaper modification, UAC bypass, and a clipper that swaps cryptocurrency wallet addresses during copy-paste operations.

The clipper silently monitors the victim’s clipboard for wallet addresses and replaces them with an attacker-controlled address before the paste completes, redirecting funds without the victim realizing the swap.

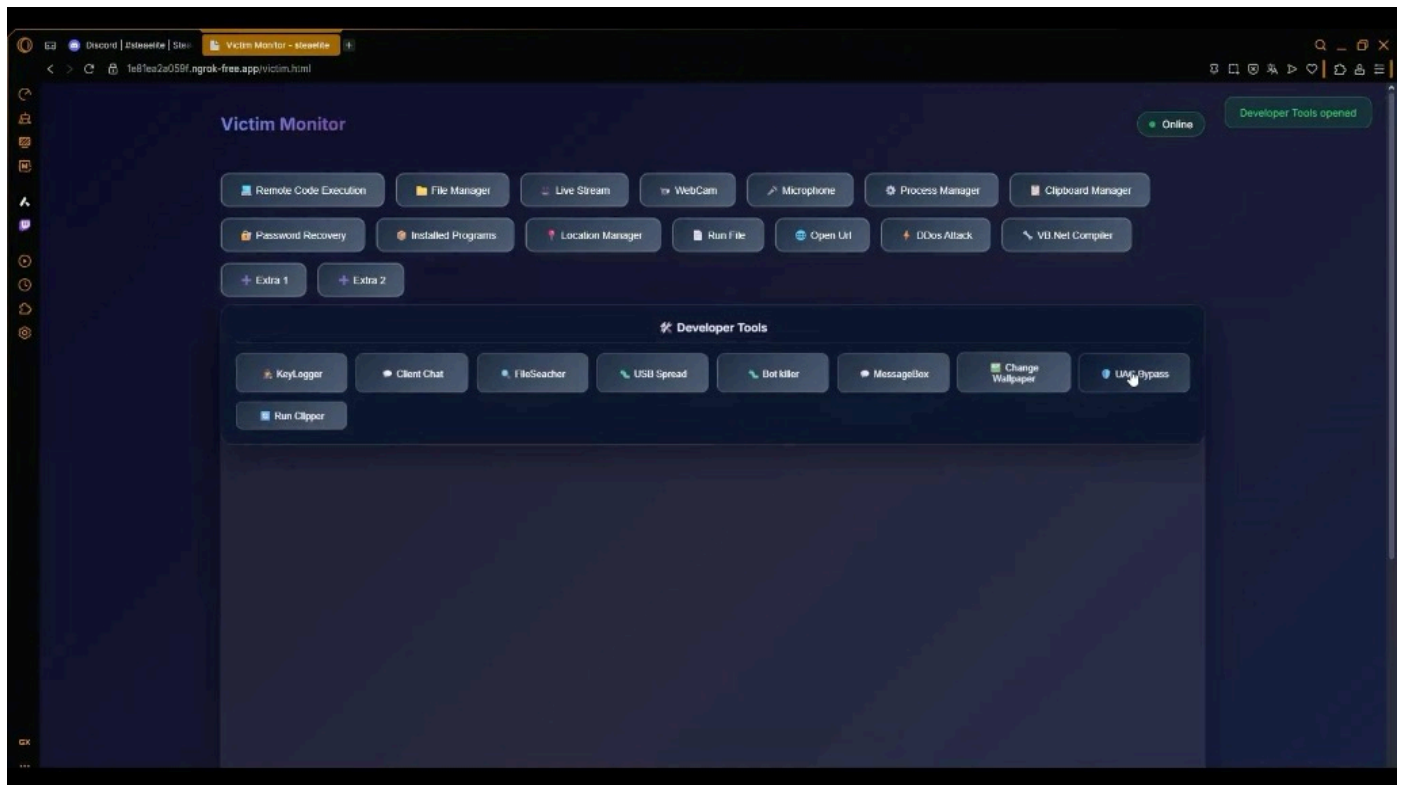


Figure 4. The developer tools section.

The remote code execution module provides a command prompt interface where operators type commands, execute them, and receive output directly in the browser. Combined with the UAC bypass module, this provides arbitrary command execution at administrative privilege levels.

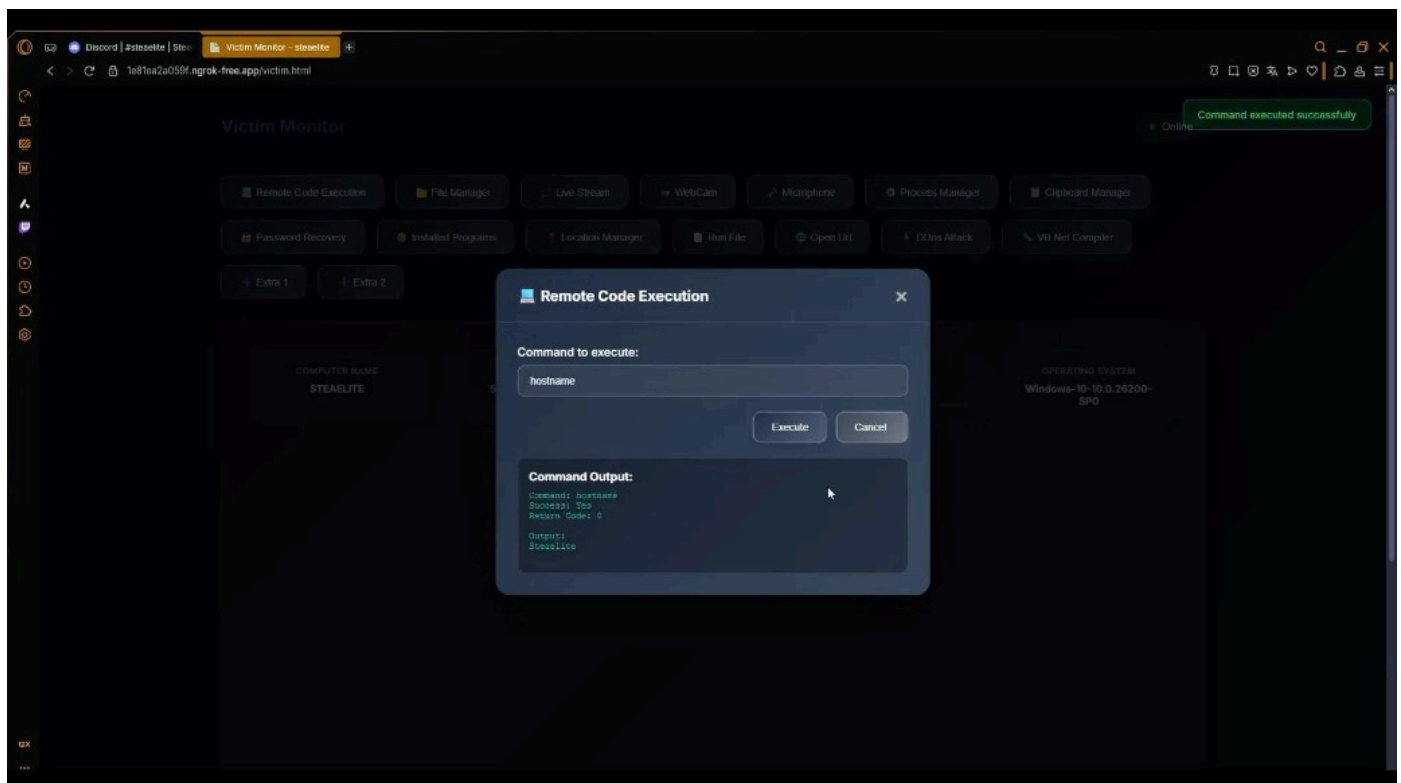


Figure 5. Remote code execution showing a successful 'hostname' command.

The file manager provides full directory browsing with one-click download. Operators traverse the victim's file system and exfiltrate any file without writing scripts or configuring separate exfiltration channels.

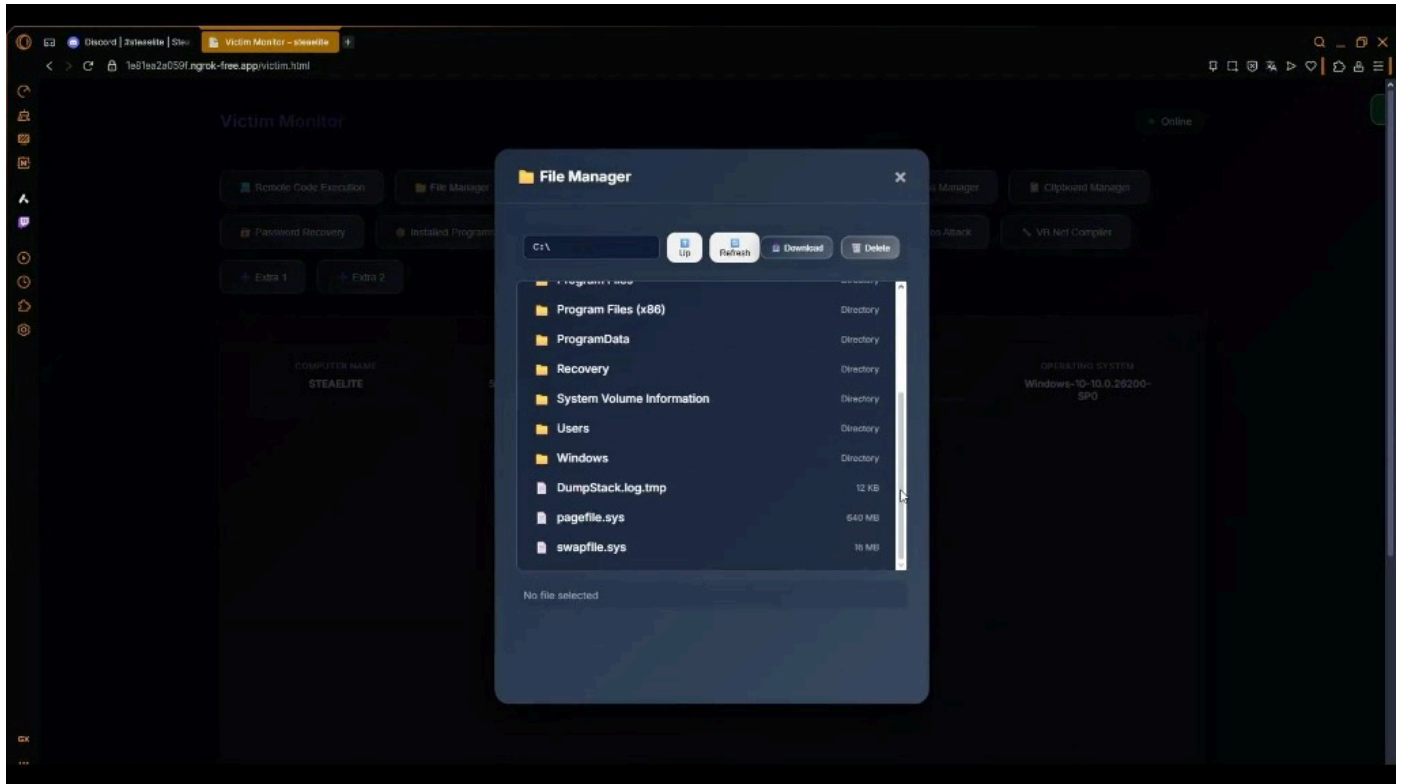


Figure 6. The file manager browsing the C:\ drive.

Real-time screen streaming shows the victim's desktop with a "LIVE STREAM" indicator. Combined with webcam and microphone modules, this turns Stealite into a persistent surveillance platform for as long as the victim remains connected.

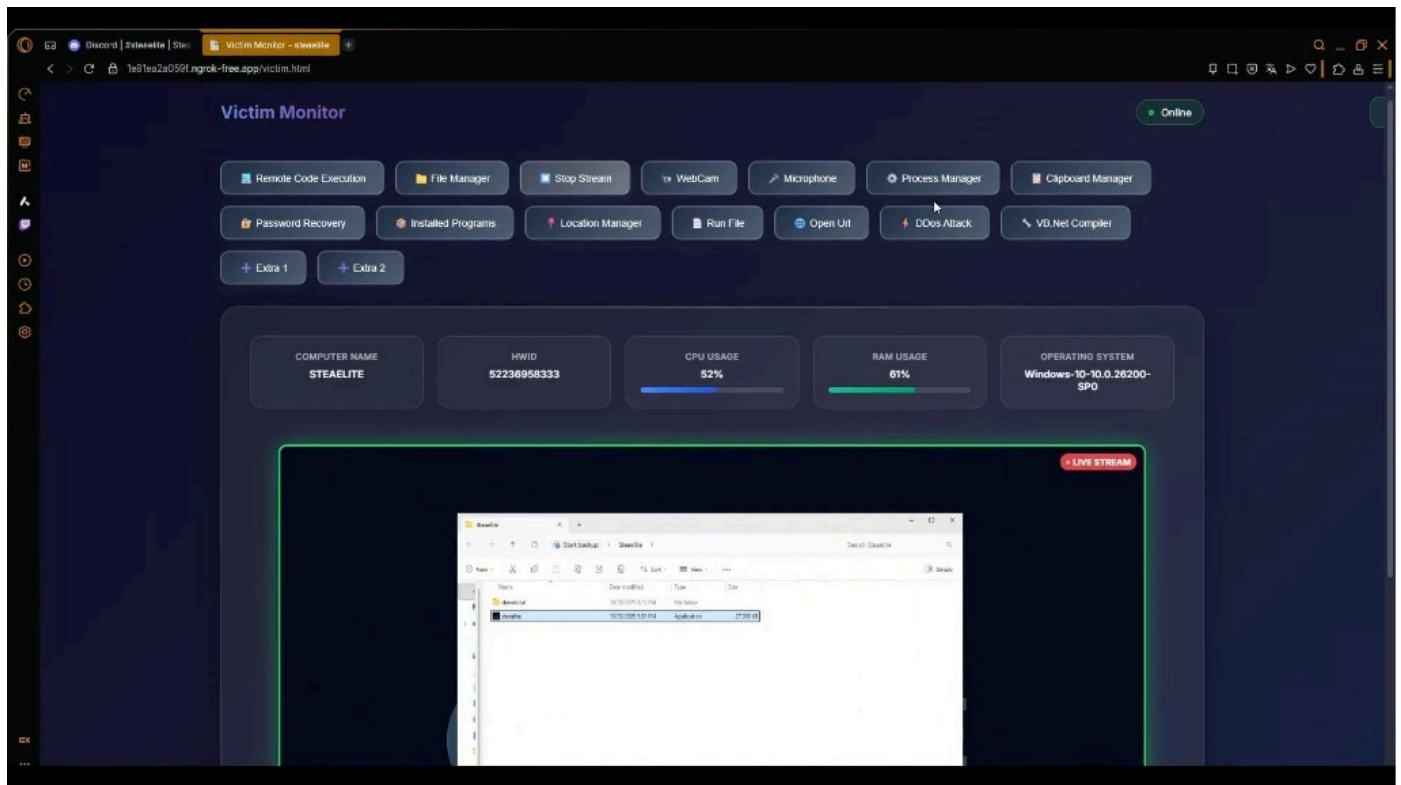


Figure 7. Live stream of the victim's desktop.

The messagebox module displays custom dialog boxes on the victim's screen, configurable by content, title, and type. This enables social engineering directly on the endpoint: fake update prompts, fabricated security warnings, or credential harvesting dialogs that originate from the victim's own machine rather than an external email or website.

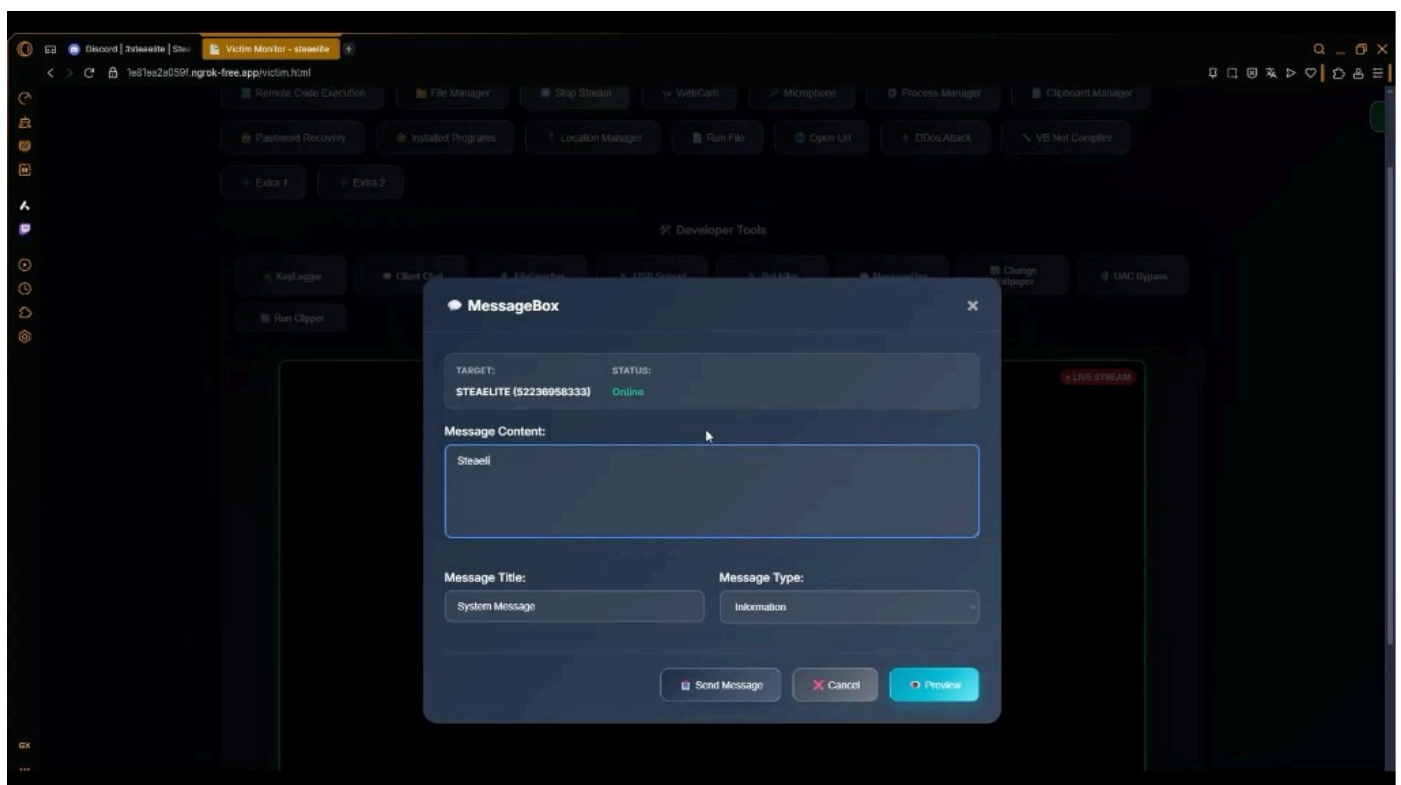


Figure 8. The message box module.

When a new victim connects, Steelite automatically harvests browser-stored passwords, session cookies, and application tokens before the operator issues any commands. Data theft begins at the moment of connection. Even if the operator never opens the dashboard, the initial exfiltration has already completed.

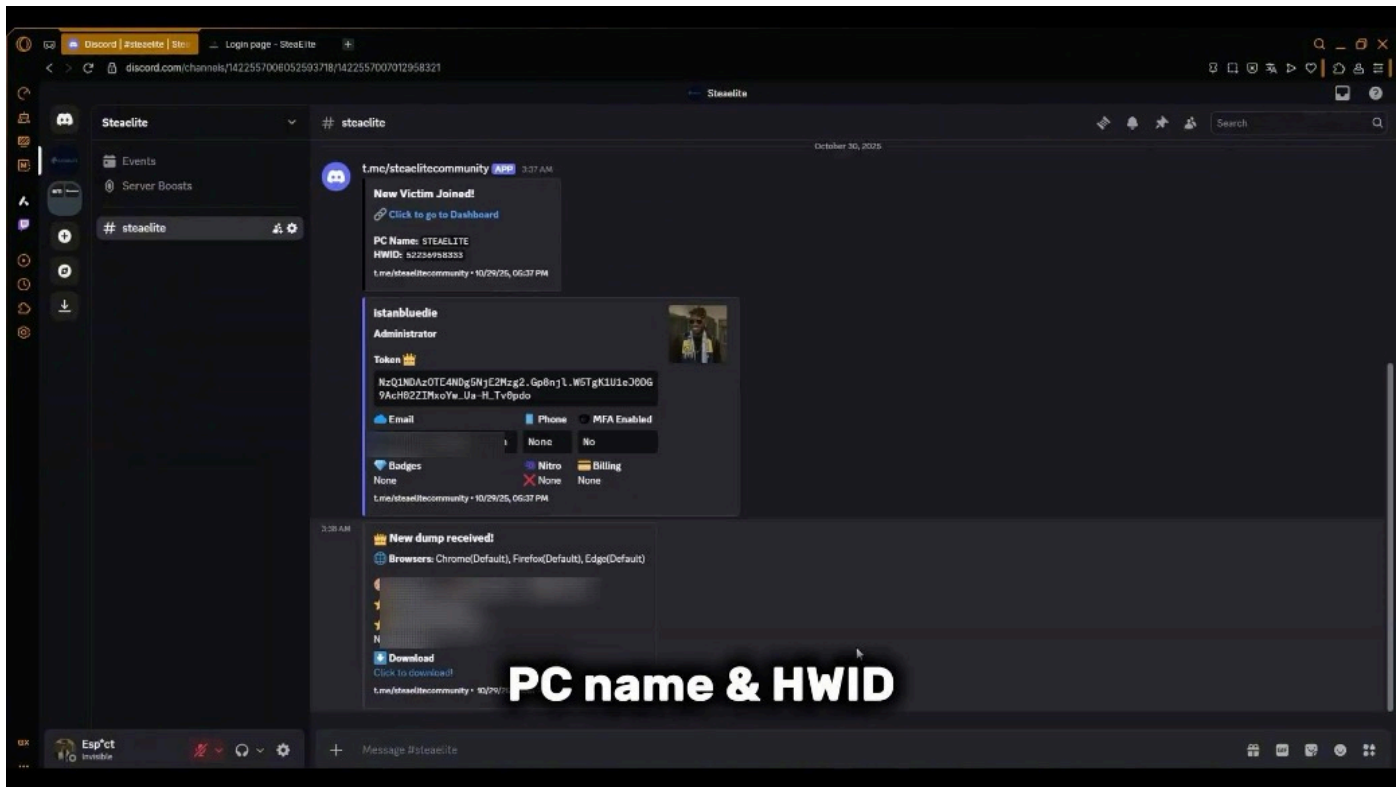


Figure 9. Automated credential dump notification.

What Steelite Means for Security Teams

A single threat actor can browse files, exfiltrate documents, harvest credentials, and deploy ransomware from the same dashboard. This enables complete [double extortion](#) from one tool.

Previously, double extortion required malware for initial access and exfiltration, then a separate ransomware payload for encryption, often involving coordination between initial access brokers and [ransomware affiliates](#). Steelite puts both in the same interface, and the automated credential harvesting means data theft fires before the operator even interacts with the dashboard.

The Android ransomware module on the roadmap extends this further. If the developer delivers, a single Steelite licence could cover corporate Windows endpoints, and the mobile devices employees use for authentication and messaging.

For organizations, the line between data theft and ransomware is disappearing at the tooling level. Stopping ransomware at the point of encryption is too late if the data has already left through the same tool’s exfiltration modules.

How BlackFog Disrupts Double Extortion

BlackFog’s [anti data exfiltration \(ADX\)](#) technology addresses exactly this convergence. By monitoring and blocking unauthorized outbound data transfers in real-time, ADX can prevent the credential dumps, file theft, and clipboard-based cryptocurrency redirection that tools like Steaelite rely on, cutting off the exfiltration half of a double extortion attack before the ransomware ever detonates.

Indicators of Compromise

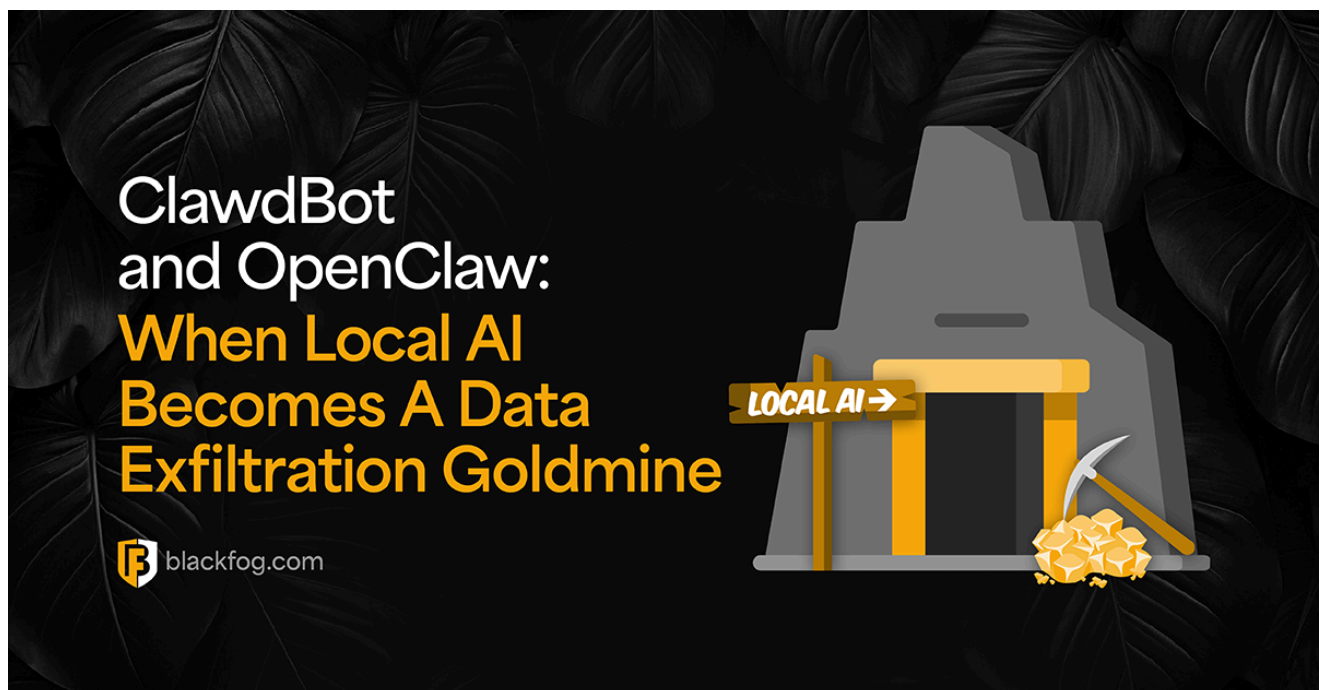
SHA-256:	b2a8d97da2a653de75d3d1be583910233a81a3794364e19ee4bc352b06b48f36 (shared by @solostalking on X)
Username:	Steaelite
First Observed:	November 2025
C2:	1e81ea2a059f.ngrok-free.app (changes per session, observed in demo)
Associated Paths:	/dashboard.html, /victim.html

Share This Story, Choose Your Platform!



[Steelite RAT Enables Double Extortion Attacks from a Single Panel](#)

Steelite is a newly emerging RAT that unifies credential theft, data exfiltration, and ransomware in a single web panel, accelerating double extortion attacks.



[ClawdBot and OpenClaw: When Local AI Becomes A Data Exfiltration Goldmine](#)

ClawdBot stores API keys, chat histories, and user memories in plaintext files, and infostealers like RedLine, Lumma, and Vidar are already targeting it.



[West Harlem Group Assistance Stops Ransomware and Cryptojacking with BlackFog ADX](#)

West Harlem Group Assistance secures its community mission by preventing ransomware and cryptojacking with BlackFog ADX.

Why Traditional Security Fails To Deal With Advanced Persistent Threats



[Why Traditional Security Fails To Deal With Advanced Persistent Threats](#)

Learn why advanced persistent threats remain a growing cybersecurity risk in 2026 and where organizations must focus to address them.

What Does Advanced Threat Protection Really Mean In 2026?



[What Does Advanced Threat Protection Really Mean In 2026?](#)

Find out why businesses need advanced threat protection to cope with the new era of sophisticated, persistent cyber risks.



[How Can You Prevent Viruses And Malicious Code Today?](#)

Preventing viruses and malicious code is harder than ever in a landscape where APTs are a growing threat. Here's what you need to know to stay safe.