ZEROFOX INTELLIGENCE

| Flash |

Cryptocurrency Stealer for Sale on Dark Web

F-2026-02-12a

Classification: TLP:CLEAR

Criticality: LOW

Intelligence Requirements: Malware, Threat Actor, Cryptocurrency

February 12, 2026

Scope Note

ZeroFox Intelligence is derived from a variety of sources, including—but not limited to—curated open-source accesses, vetted social media, proprietary data sources, and direct access to threat actors and groups through covert communication channels. Information relied upon to complete any report cannot always be independently verified. As such, ZeroFox applies rigorous analytic standards and tradecraft in accordance with best practices and includes caveat language and source citations to clearly identify the veracity of our Intelligence reporting and substantiate our assessments and recommendations. All sources used in this particular Intelligence product were identified prior to 10:00 AM (EST) on February 12, 2026; per cyber hygiene best practices, caution is advised when clicking on any third-party links.

| Flash | Cryptocurrency Stealer for Sale on Dark Web

| Key Findings

- On February 2, 2026, ZeroFox observed an actor using the alias “MysteryHack” advertising a malware suite called DeepLoad on the dark web forum Exploit. The actor described DeepLoad as a centralized panel for multiple types of malware; its primary function is to replace seven cryptocurrency wallet applications with counterfeit versions.

- The actor claimed that a second DeepLoad feature, called Anti-Metamask, is designed to remove legitimate browser-based cryptocurrency wallets and replace them with fraudulent versions.

- MysteryHack further claimed that they are developing a future DeepLoad module, which they described as an executable file that installs an unspecified browser extension offering fraudulent airdrops.

- Due to DeepLoad’s wallet replacement, phishing automation, and persistent malware capabilities, ZeroFox assesses it is very likely a very sophisticated offering. DeepLoad’s design is explicitly focused on actively facilitating real-time cryptocurrency theft, which almost certainly makes it an attractive malware suite in the cybercrime-as-a-service (CaaS) environment.

Details

On February 2, 2026, ZeroFox observed actor MysteryHack advertising a malware suite called DeepLoad on the dark web forum Exploit. The actor described DeepLoad as a centralized panel for multiple types of malware; its function is to replace seven cryptocurrency wallet applications (Ledger, Trezor, Exodus, Guarda, BitBox, KeepKey, and Atomic) with counterfeit versions.

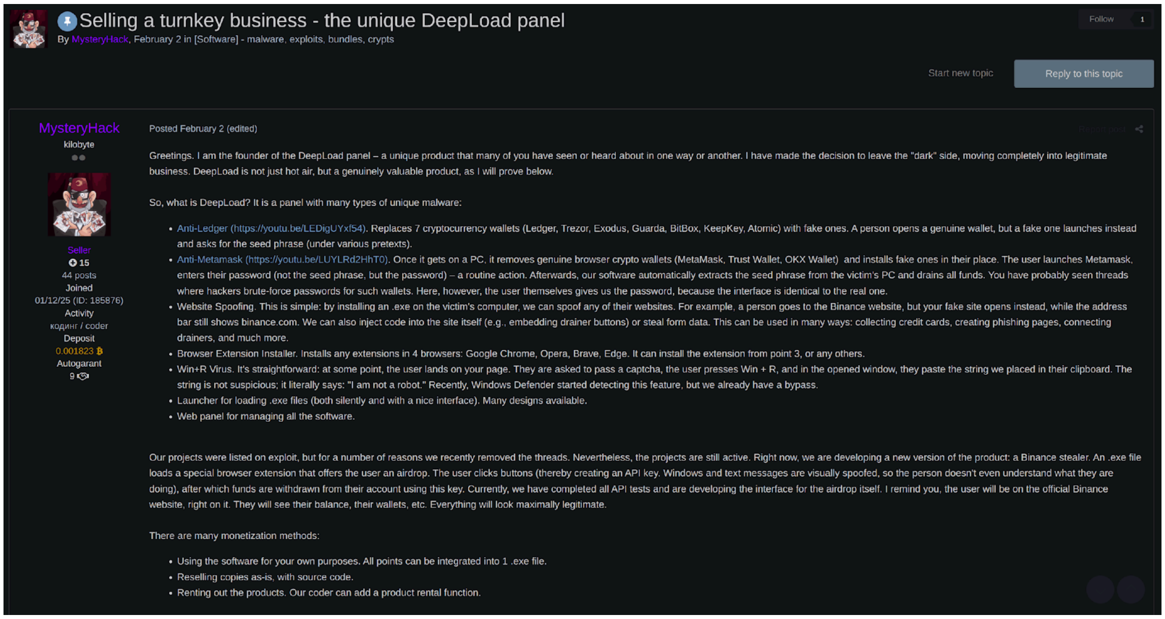
- In this scenario, when a victim attempts to open a legitimate wallet, a fake interface is launched instead, prompting the user to enter their seed phrase.
- MysteryHack has been a member of Exploit since December 2025 and has made 44 posts since that date. ZeroFox assesses they are likely considered very active by other forum users, given the timeframe. The threat actor has a favorable reputation on the forum, meaning they are very likely to be taken seriously by potential customers and will almost certainly receive attention from cybercriminals seeking solutions for attacking cryptocurrency platforms.

The actor claimed a second feature of DeepLoad, called Anti-Metamask, is designed to remove legitimate browser-based cryptocurrency wallets (such as MetaMask, Trust Wallet, and OKX Wallet) and replace them with fraudulent versions. The malware is capable of transmitting harvested credentials from infected victims' devices to the operator's control panel.

- While this functionality resembles that of traditional infostealers, it is specifically tailored for cryptocurrency-focused attacks.
- The system appears to combine automated phishing techniques with persistent malware infection, enabling attackers to interact with victim data in real time.

MysteryHack further claimed that they are developing a future DeepLoad module, referred to as a "Binance stealer." The actor described the component as an executable file that installs an unspecified browser extension offering fraudulent airdrops. The stealer is likely to be integrated into the DeepLoad panel in a future update.

- MysteryHack did not specify a price for the product and indicated that they are open to private offers. Given their claim that the product generated USD 7,000 in profit within a single week, it is very likely that the final price will be substantial.
- Notably, the sale of the project will allegedly include support from the original coder, who can additionally be paid a percentage of earnings or a salary to continue longer-term technical support, if the buyer is interested.



Selling a turnkey business - the unique DeepLoad panel

By MysteryHack, February 2 in [Software] - malware, exploits, bundles, crypts

Posted February 2 (edited)

Greetings. I am the founder of the DeepLoad panel – a unique product that many of you have seen or heard about in one way or another. I have made the decision to leave the "dark" side, moving completely into legitimate business. DeepLoad is not just hot air, but a genuinely valuable product, as I will prove below.

So, what is DeepLoad? It is a panel with many types of unique malware:

- Anti-Ledger (https://youtu.be/LEDigUYxf54). Replaces 7 cryptocurrency wallets (Ledger, Trezor, Exodus, Guarda, BitBox, KeepKey, Atomic) with fake ones. A person opens a genuine wallet, but a fake one launches instead and asks for the seed phrase (under various pretexts).
- Anti-Metamask (https://youtu.be/LUYLRd2HhT0). Once it gets on a PC, it removes genuine browser crypto wallets (MetaMask, Trust Wallet, OKX Wallet) and installs fake ones in their place. The user launches Metamask, enters their password (not the seed phrase, but the password) – a routine action. Afterwards, our software automatically extracts the seed phrase from the victim's PC and drains all funds. You have probably seen threads where hackers brute-force passwords for such wallets. Here, however, the user themselves gives us the password, because the interface is identical to the real one.
- Website Spoofing. This is simple: by installing an .exe on the victim's computer, we can spoof any of their websites. For example, a person goes to the Binance website, but your fake site opens instead, while the address bar still shows binance.com. We can also inject code into the site itself (e.g., embedding drainer buttons) or steal form data. This can be used in many ways: collecting credit cards, creating phishing pages, connecting drainers, and much more.
- Browser Extension Installer. Installs any extensions in 4 browsers: Google Chrome, Opera, Brave, Edge. It can install the extension from point 3, or any others.
- Win+R Virus. It's straightforward: at some point, the user lands on your page. They are asked to pass a captcha, the user presses Win + R, and in the opened window, they paste the string we placed in their clipboard. The string is not suspicious; it literally says: "I am not a robot." Recently, Windows Defender started detecting this feature, but we already have a bypass.
- Launcher for loading .exe files (both silently and with a nice interface). Many designs available.
- Web panel for managing all the software.

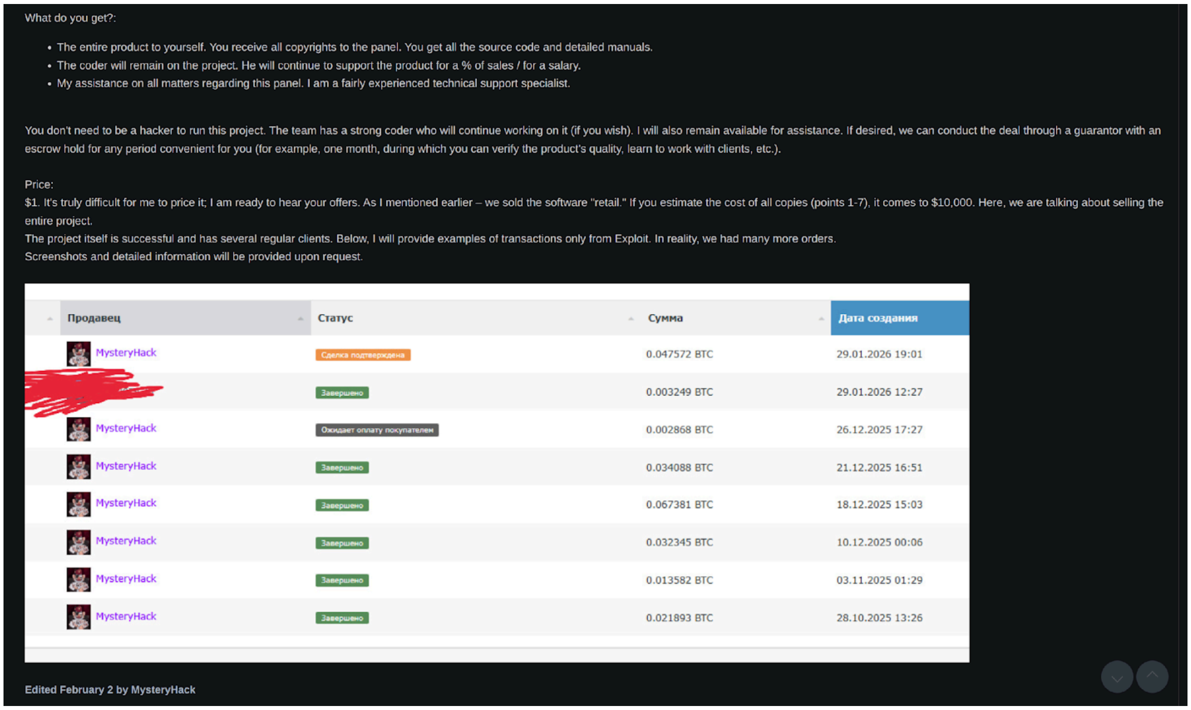
Our projects were listed on exploit, but for a number of reasons we recently removed the threads. Nevertheless, the projects are still active. Right now, we are developing a new version of the product: a Binance stealer. An .exe file loads a special browser extension that offers the user an airdrop. The user clicks buttons (thereby creating an API key. Windows and text messages are visually spoofed, so the person doesn't even understand what they are doing), after which funds are withdrawn from their account using this key. Currently, we have completed all API tests and are developing the interface for the airdrop itself. I remind you, the user will be on the official Binance website, right on it. They will see their balance, their wallets, etc. Everything will look maximally legitimate.

There are many monetization methods:

- Using the software for your own purposes. All points can be integrated into 1 .exe file.
- Reselling copies as-is, with source code.
- Renting out the products. Our coder can add a product rental function.

MysteryHack's Exploit Post (Part 1)

Source: ZeroFox Intelligence



What do you get?:

- The entire product to yourself. You receive all copyrights to the panel. You get all the source code and detailed manuals.
- The coder will remain on the project. He will continue to support the product for a % of sales / for a salary.
- My assistance on all matters regarding this panel. I am a fairly experienced technical support specialist.

You don't need to be a hacker to run this project. The team has a strong coder who will continue working on it (if you wish). I will also remain available for assistance. If desired, we can conduct the deal through a guarantor with an escrow hold for any period convenient for you (for example, one month, during which you can verify the product's quality, learn to work with clients, etc.).

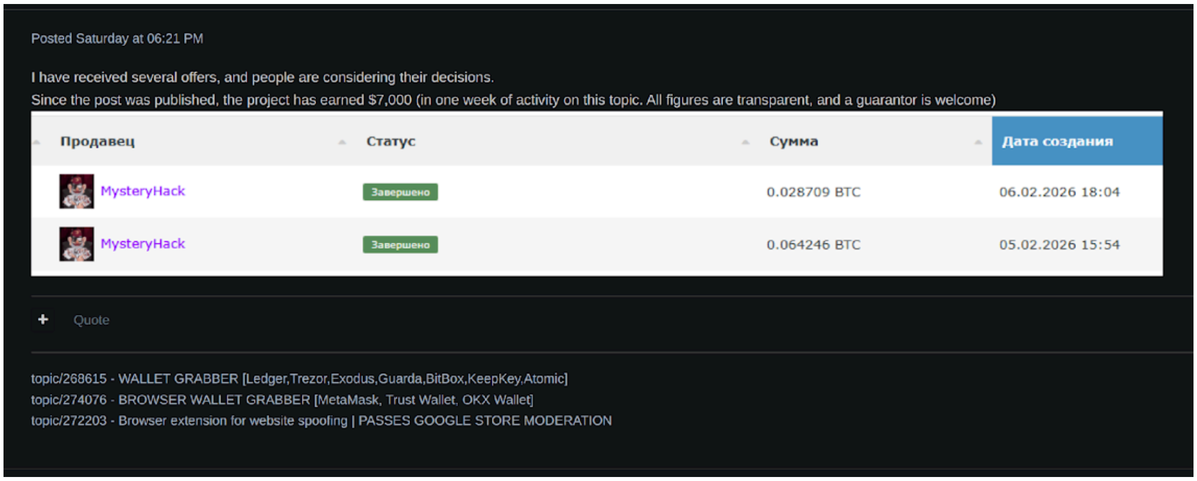
Price:
$1. It's truly difficult for me to price it; I am ready to hear your offers. As I mentioned earlier – we sold the software "retail." If you estimate the cost of all copies (points 1-7), it comes to $10,000. Here, we are talking about selling the entire project.
The project itself is successful and has several regular clients. Below, I will provide examples of transactions only from Exploit. In reality, we had many more orders.
Screenshots and detailed information will be provided upon request.

Продавец	Статус	Сумма	Дата создания
MysteryHack	Сделка подтверждена	0.047572 BTC	29.01.2026 19:01
[redacted]	Завершено	0.003249 BTC	29.01.2026 12:27
MysteryHack	Ожидает оплату покупателем	0.002868 BTC	26.12.2025 17:27
MysteryHack	Завершено	0.034088 BTC	21.12.2025 16:51
MysteryHack	Завершено	0.067381 BTC	18.12.2025 15:03
MysteryHack	Завершено	0.032345 BTC	10.12.2025 00:06
MysteryHack	Завершено	0.013582 BTC	03.11.2025 01:29
MysteryHack	Завершено	0.021893 BTC	28.10.2025 13:26

Edited February 2 by MysteryHack

MysteryHack's Exploit Post (Part 2)

Source: ZeroFox Intelligence



Posted Saturday at 06:21 PM

I have received several offers, and people are considering their decisions.
Since the post was published, the project has earned $7,000 (in one week of activity on this topic. All figures are transparent, and a guarantor is welcome)

Продавец	Статус	Сумма	Дата создания
MysteryHack	Завершено	0.028709 BTC	06.02.2026 18:04
MysteryHack	Завершено	0.064246 BTC	05.02.2026 15:54

topic/268615 - WALLET GRABBER [Ledger,Trezor,Exodus,Guarda,BitBox,KeepKey,Atomic]
topic/274076 - BROWSER WALLET GRABBER [MetaMask, Trust Wallet, OKX Wallet]
topic/272203 - Browser extension for website spoofing | PASSES GOOGLE STORE MODERATION

MysteryHack's Exploit Post (Part 3)

Source: ZeroFox Intelligence

ZeroFox observed no information about how the malware would be delivered or how threat actors would generate traffic and infections at scale. The service appears to rely heavily on customized phishing techniques to achieve initial compromise; however, if a more persistent initial access method is developed, DeepLoad would likely represent a significant threat to the cryptocurrency marketplace.

Due to DeepLoad's wallet replacement, phishing automation, and persistent malware capabilities, ZeroFox assesses it is very likely this is a very sophisticated offering. While DeepLoad's malware suite shares similarities with traditional infostealers, its design is explicitly focused on actively facilitating real-time cryptocurrency theft, which almost certainly makes it an attractive offering in the CaaS environment.

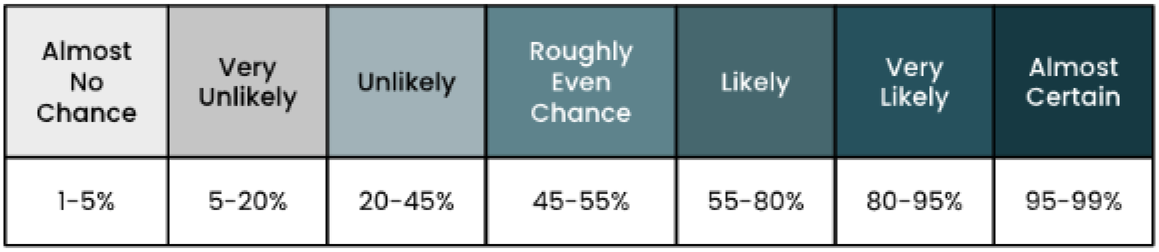
Appendix A: Traffic Light Protocol for Information Dissemination

	Red	Amber
WHEN SHOULD IT BE USED?	**Sources may use** **TLP:RED** when information cannot be effectively acted upon by additional parties and could lead to impacts on a party's privacy, reputation, or operations if misused.	**Sources may use** **TLP:AMBER** when information requires support to be effectively acted upon but carries risks to privacy, reputation, or operations if shared outside of the organizations involved.
HOW MAY IT BE SHARED?	**Recipients may NOT share** **TLP:RED** with any parties outside of the specific exchange, meeting, or conversation in which it is originally disclosed.	**Recipients may ONLY share** **TLP:AMBER** information with members of their own organization and its clients, but only on a need-to-know basis to protect their organization and its clients and prevent further harm. **Note that** **TLP:AMBER+STRICT** restricts sharing to the organization only.

	Green	Clear
WHEN SHOULD IT BE USED?	**Sources may use** **TLP:GREEN** when information is useful for the awareness of all participating organizations, as well as with peers within the broader community or sector.	**Sources may use** **TLP:CLEAR** when information carries minimal or no risk of misuse in accordance with applicable rules and procedures for public release.
HOW MAY IT BE SHARED?	**Recipients may share** **TLP:GREEN** information with peers and partner organizations within their sector or community but not via publicly accessible channels.	**Recipients may share** **TLP:CLEAR** information without restriction, subject to copyright controls.

Appendix B: ZeroFox Intelligence Probability Scale

All ZeroFox intelligence products leverage probabilistic assessment language in analytic judgments. Qualitative statements used in these judgments refer to associated probability ranges, which state the likelihood of occurrence of an event or development. Ranges are used to avoid a false impression of accuracy. This scale is a standard that aligns with how readers should interpret such terms.



Almost No Chance	Very Unlikely	Unlikely	Roughly Even Chance	Likely	Very Likely	Almost Certain
1-5%	5-20%	20-45%	45-55%	55-80%	80-95%	95-99%