ZEROFOX INTELLIGENCE

Brief

The Underground Economist: Volume 6, Issue 4

B-2026-02-12b

Classification: TLP:CLEAR

Criticality: LOW

Intelligence Requirements: Deep and Dark Web, Threat Actor, Data Breach

February 12, 2026

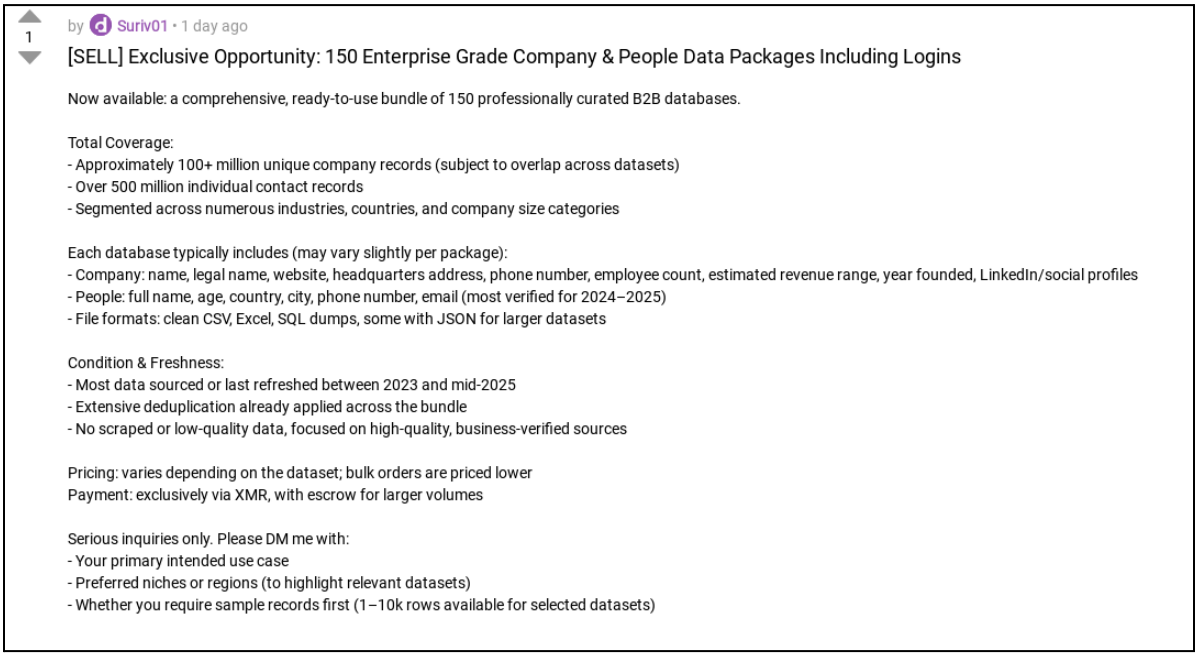
ZeroFox Intelligence is derived from a variety of sources, including—but not limited to—curated open-source accesses, vetted social media, proprietary data sources, and direct access to threat actors and groups through covert communication channels. Information relied upon to complete any report cannot 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 7:00 AM (EST) on February 12, 2026; per cyber hygiene best practices, caution is advised when clicking on any third-party links.

| Brief | The Underground Economist: Volume 6, Issue 4

| Bundle of 150 Databases Advertised on Dark Web Forum

On February 5, 2026, a long-standing actor known as "Suriv01" on the English-language dark web forum Dread advertised an alleged database bundle comprising 150 curated business-to-business (B2B) databases associated with multiple well-known entities, including CNN, Spotify, Coinbase, Apple, and Lockheed Martin. The bundle allegedly contains more than 100 million unique company records and over 500 million personal contact records.

- Each database in the bundle allegedly contains corporate data such as company name, website, headquarters address, contact details, employee count, estimated revenue range, year founded, LinkedIn, and other social media profiles.
- The databases also allegedly contain personal data, including full name, age, country, city, phone number, and email address; the actor claims most of this data was verified between 2024 and 2025.
- Suriv01 has classified the dataset into the following categories: social media data/logins, mail providers, business/crypto, people data, government/military/police/agencies, and large corporate datasets.



Suriv01's advertisement on Dread

Source: ZeroFox Intelligence

The actor did not reveal the exact price of the data but stated pricing is dependent on the type and category of the requested dataset. They also claimed that most of the data, collected between 2023 and mid-2025, was not scraped from publicly accessible sources.

- In the advertisement, Survi01 asked interested buyers to privately communicate their intended use case for the dataset and their "preferred niches or regions."
- There is a roughly even chance that Suriv01's claims about the database bundle are true, considering the large volume of data and the pricing model. The alleged data was likely obtained through botnet logs or compiled from ULP (URL:login:password) records often extracted via infostealer infections.

Suriv01 has been active on Dread on since 2020 and has contributed at least 105 posts to the forum, largely involving scam activities, drug-related crimes, and financial fraud; the actor has garnered at least four negative reactions to their posts. [Analyst Note: The Dread forum is widely used for various topics that range from hobbies to varying degrees of crime—including cybercrime. It is comparable to a dark web social media platform

and is similar in look and function to Reddit, though it has no known association with that company.]

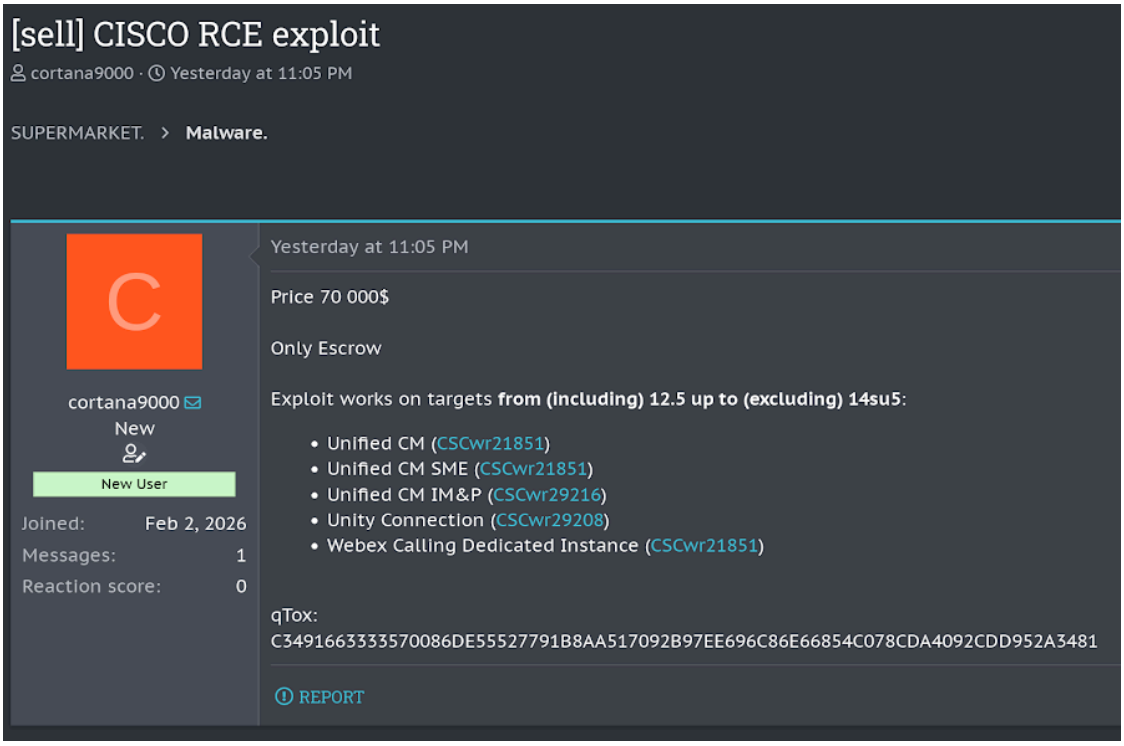
- ZeroFox assesses that Suriv01 is unlikely to be well-regarded by Dread users. While the actor likely has such data, it is most likely outdated—despite the actor's claims.

If Suriv01's claims are true, the bundle will very likely grab the attention of a myriad of threat actors, including state-nexus actors seeking the data categorized under government/military/police/agencies. Additionally, threat actors looking for data to use in social engineering or financial extortion attacks are also likely to be interested in the personal information allegedly included in the bundle.

Threat Actor Advertises Cisco RCE Exploit for USD 70,000

On February 2, 2026, newly registered and untested threat actor "cortana9000" advertised a Cisco remote code execution (RCE) exploit on the predominantly Russian-language dark web forum ReHub. The exploit—listed for a price of USD 70,000—allegedly affects Cisco Unified Communications Manager (Unified CM) products, including:

- Unified CM (CSCwr21851)
- Unified CM SME (CSCwr21851)
- Unified CM IM&P (CSCwr29216)
- Unity Connection (CSCwr29208)
- Webex Calling Dedicated Instance (CSCwr21851)



cortana9000's ReHub post
Source: ZeroFox Intelligence

The actor provided very limited technical details in the post and did not specify whether this exploit is a zero-day—information which is typically observed in other posts of the same nature. As such, ZeroFox assesses there is a roughly even chance that the RCE cortana9000 advertised is leveraging an existing vulnerability in Cisco Unified CM and is not a zero-day.

Exploitation of the flaw likely results in unauthorized user-level access that can be leveraged to escalate privileges to gain complete root-level server access. Cisco Unified CM devices are used by enterprises for voice, video, and messaging services. Compromise of such devices is likely to lead to disruption of services, enable further lateral movement into corporate networks, or result in the theft of sensitive files such as call and messaging logs and user data.

Cryptocurrency Stealer for Sale on Dark Web

On February 2, 2026, ZeroFox observed the 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.

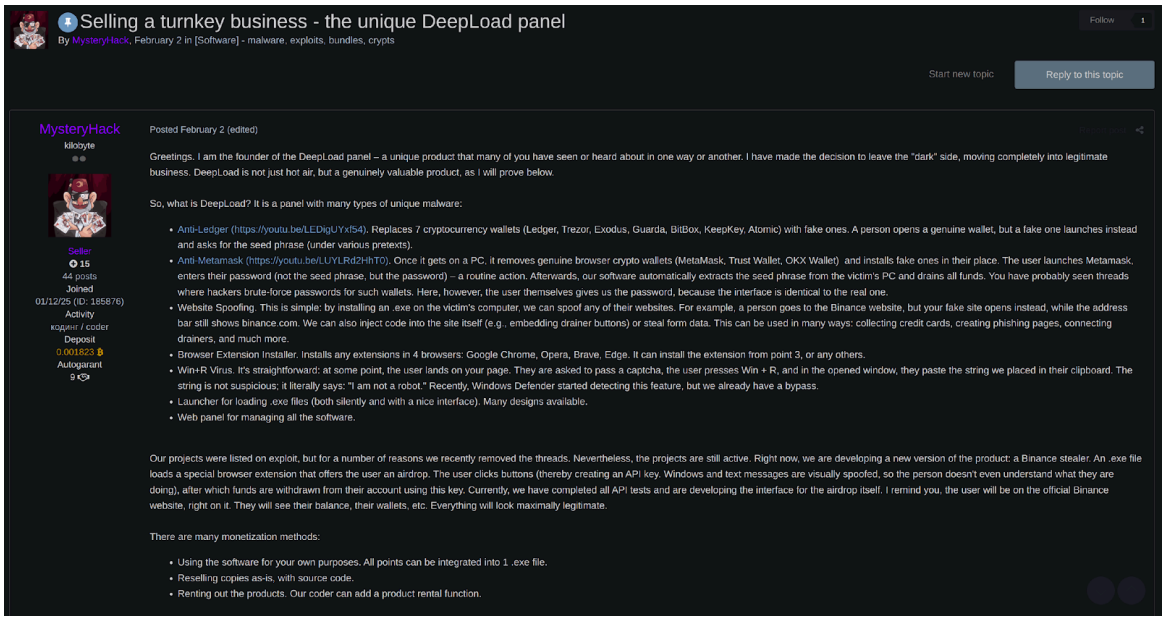
- In this scenario, when a victim attempts to open a legitimate wallet, a fake interface is launched instead, prompting the user to enter their seed phrase.
- MysteryHack has been a member of Exploit since December 2025 and has made 44 posts since that date. ZeroFox assesses they are likely considered 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.

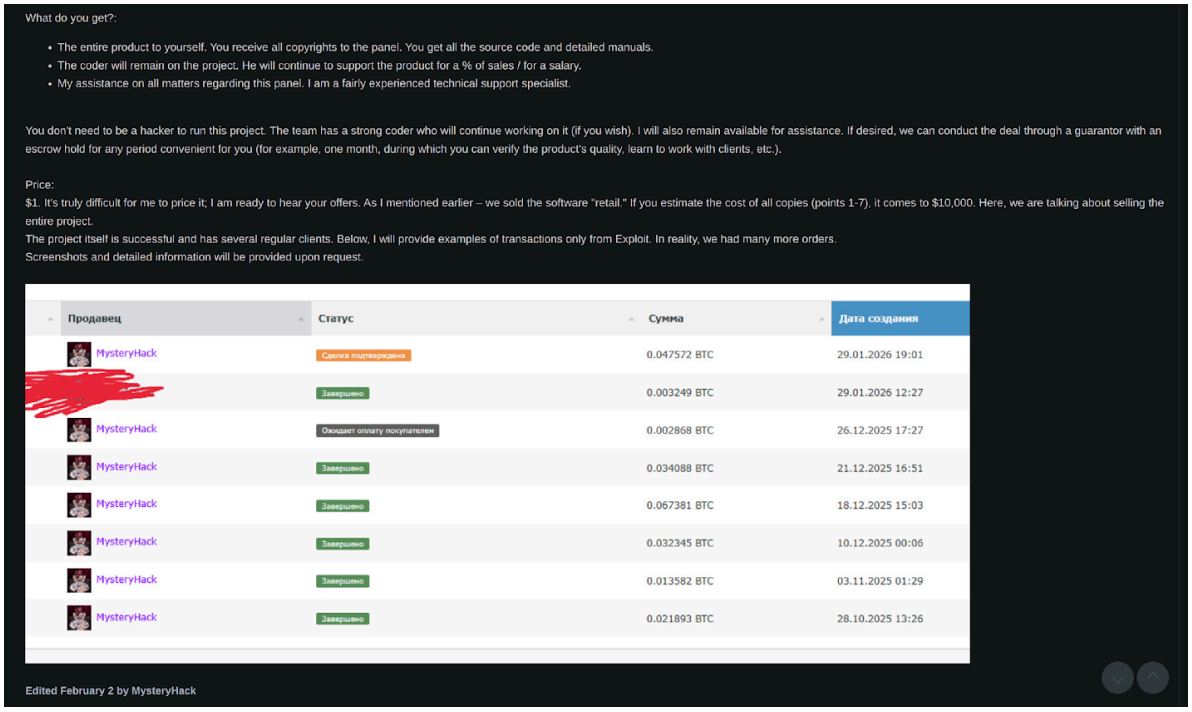
- While this functionality resembles that of traditional infostealers, it is specifically tailored for cryptocurrency-focused attacks.
- The system appears to combine automated phishing techniques with persistent malware infection, enabling attackers to interact with victim data in real time.

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.

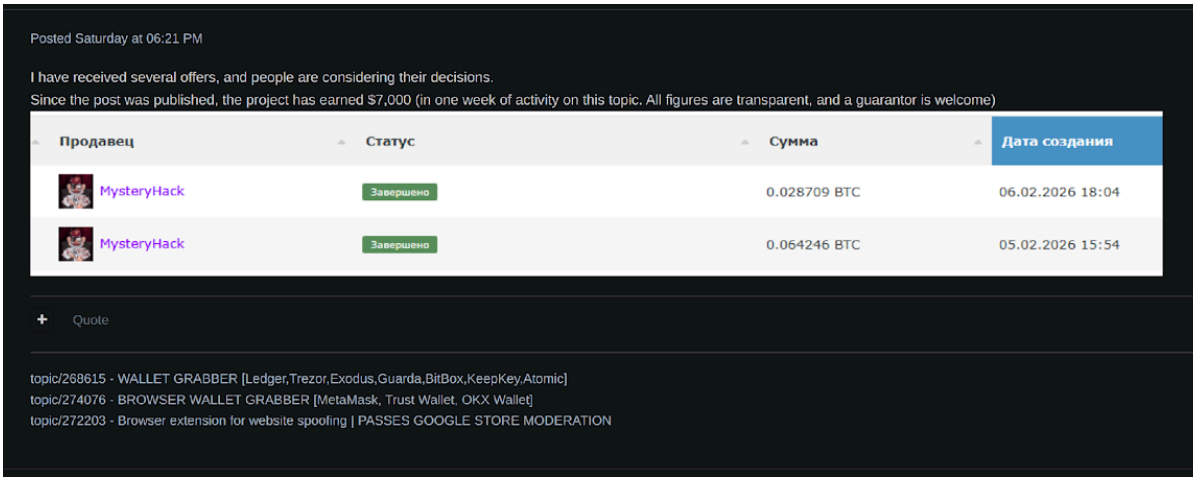


MysteryHack's Exploit Post (Part 1)
Source: ZeroFox Intelligence



MysteryHack's Exploit Post (Part 2)

Source: ZeroFox Intelligence



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.

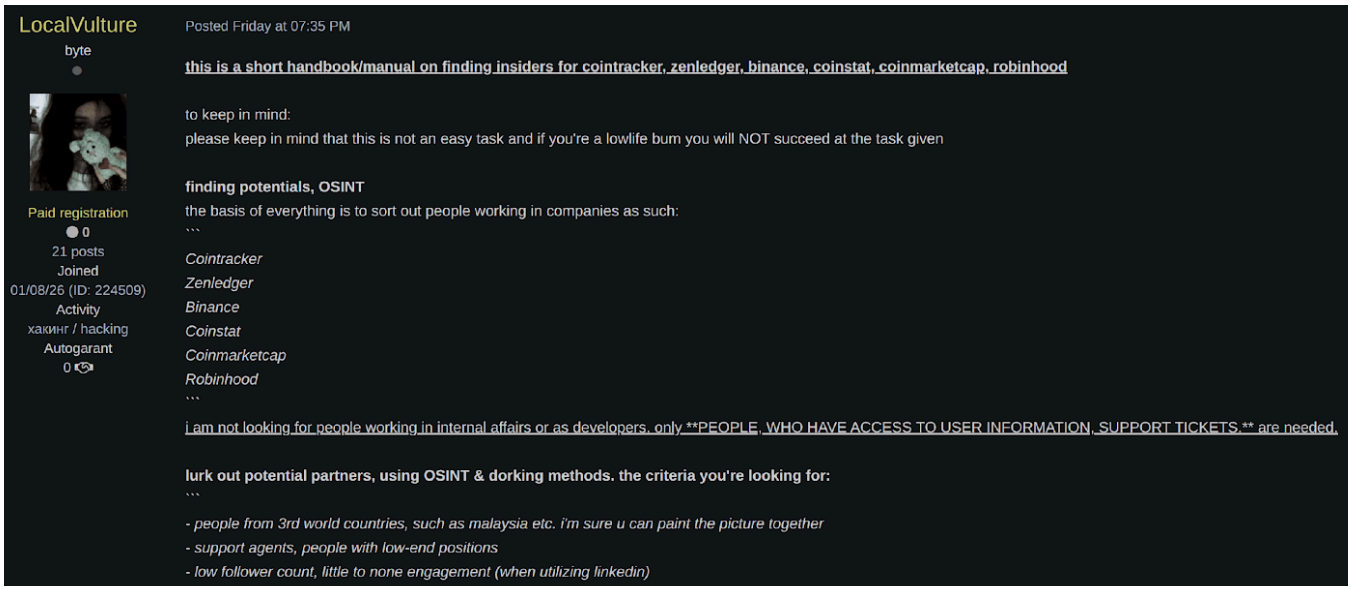
Due to DeepLoad's wallet replacement, phishing automation, and persistent malware capabilities, ZeroFox assesses it is very likely this is a very sophisticated offering. While DeepLoad's malware suite shares similarities with traditional infostealers, its design is explicitly focused on actively facilitating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

Campaign to Recruit Cryptocurrency Insiders

On January 20, 2026, newly registered and untested threat actor "LocalVulture" posted on popular dark web forum Exploit seeking potential partners to recruit insiders within large cryptocurrency exchanges—preferably those from "third-world" countries. Notably, the actor provided a guidance manual and numerous specific suggestions on how to approach and profile prospective insiders. ZeroFox assesses this is a change in previously observed tactics that is likely to reinvigorate long-standing efforts among financially motivated threat actors to infiltrate and target major cryptocurrency exchanges.

The actor explicitly mentioned interest in approaching individuals working for the following platforms:

- CoinTracker
- ZenLedger
- Binance
- CoinStats
- CoinMarketCap
- Robinhood

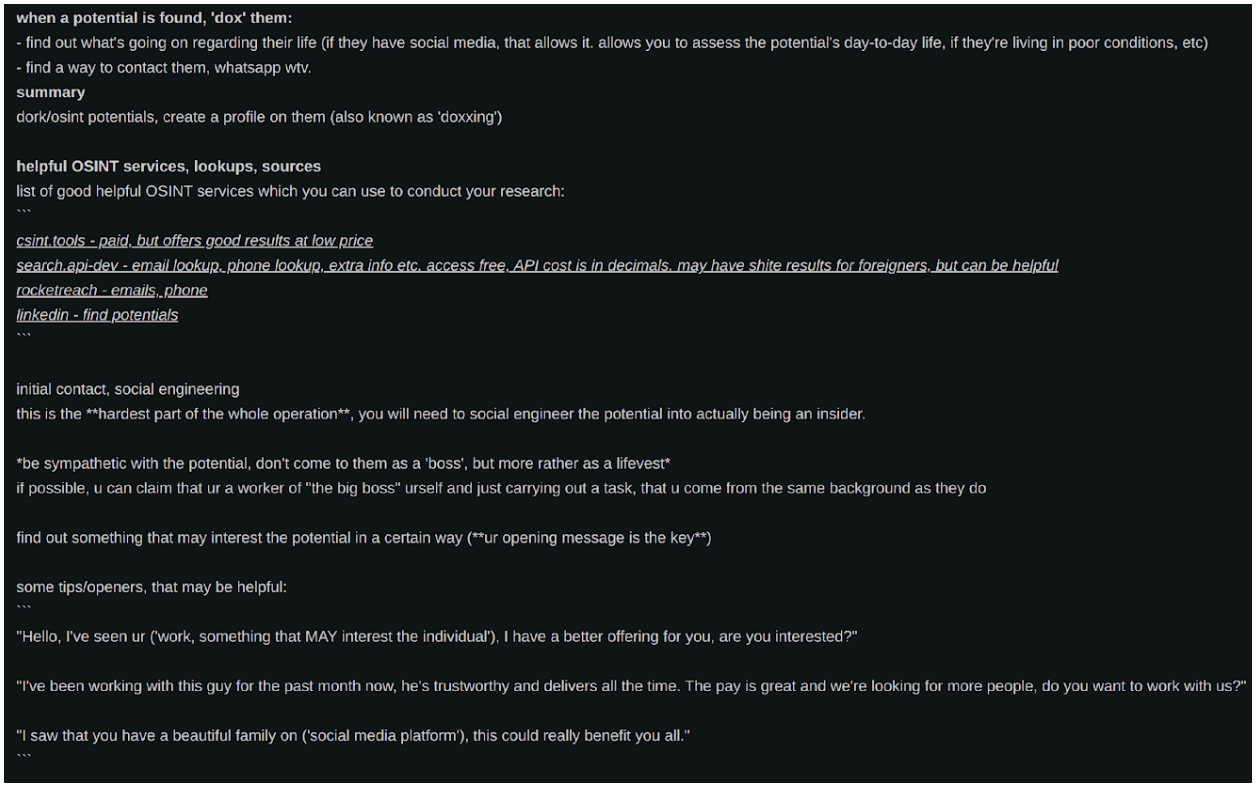


LocalVulture's Exploit post seeking recruitment partners

Source: ZeroFox Intelligence

In the post, LocalVulture shared three categories of insiders potential partners should target for recruitment. It is likely that the actor identified these categories in order to exploit financially motivated and inexperienced crypto exchange employees that may be more easily swayed to provide insider knowledge. These categories are:

- Individuals from third-world countries
- Support agents or employees in low-level positions
- Individuals with a low follower count and little to no online engagement



when a potential is found, 'dox' them:
- find out what's going on regarding their life (if they have social media, that allows it. allows you to assess the potential's day-to-day life, if they're living in poor conditions, etc)
- find a way to contact them, whatsapp wtv.

summary
dork/osint potentials, create a profile on them (also known as 'doxxing')

helpful OSINT services, lookups, sources
list of good helpful OSINT services which you can use to conduct your research:
```
csint.tools - paid, but offers good results at low price
search.api-dev - email lookup, phone lookup, extra info etc, access free, API cost is in decimals, may have shite results for foreigners, but can be helpful
rocketreach - emails, phone
linkedin - find potentials
```

initial contact, social engineering
this is the **hardest part of the whole operation**, you will need to social engineer the potential into actually being an insider.

be sympathetic with the potential, don't come to them as a 'boss', but more rather as a lifevest
if possible, u can claim that ur a worker of "the big boss" urself and just carrying out a task, that u come from the same background as they do

find out something that may interest the potential in a certain way (**ur opening message is the key**)

some tips/openers, that may be helpful:
```
"Hello, I've seen ur ('work, something that MAY interest the individual'), I have a better offering for you, are you interested?"

"I've been working with this guy for the past month now, he's trustworthy and delivers all the time. The pay is great and we're looking for more people, do you want to work with us?"

"I saw that you have a beautiful family on ('social media platform'), this could really benefit you all."
```

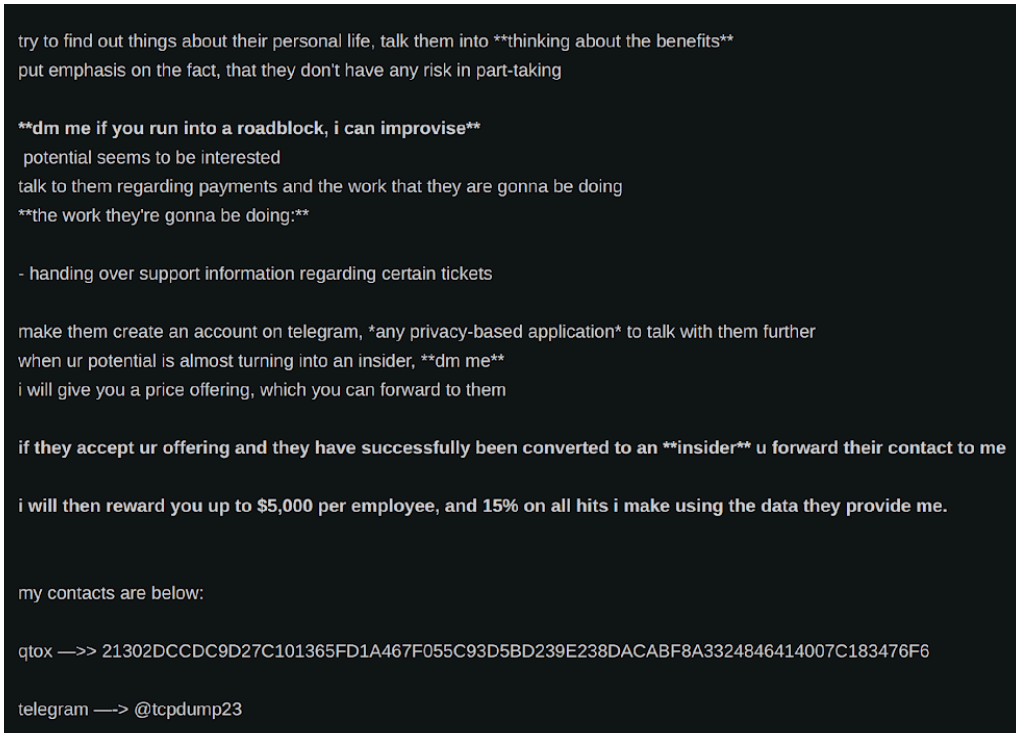
LocalVulture's Exploit post providing specific guidance and techniques

Source: ZeroFox Intelligence

LocalVulture specifies that, after identifying suitable targets for insider recruitment, the partners are expected to rely on social engineering techniques to establish and maintain effective communication. The actor suggests approaching potential insiders with a friendly employment proposal, which would theoretically allow them to earn significantly more than their standard salary from the cryptocurrency company.

- LocalVulture recommended that their partners use open-source intelligence (OSINT) tools such as csint[.]tools, search[.]api-dev, rocketreach[.]co, and LinkedIn to identify and profile potential insiders.
- The actor promised potential partners a reward of USD 5,000 per recruited insider, along with 15 percent of all profits generated via each insider. This payment would be issued once the insider's recruitment is confirmed and their details—likely meaning name, company, and country of employment—are successfully forwarded to LocalVulture.

- LocalVulture joined Exploit on January 8, 2026, and has yet to garner a significant reputation on the forum. As of writing, ZeroFox cannot confirm the actor's credibility.



LocalVulture's Exploit post specifying payment to partners

Source: ZeroFox Intelligence

The importance of utilizing insiders in large-scale cybercrime campaigns has often been underestimated. In this case, LocalVulture (or a group of actors) is motivated to conduct financial fraud; however, they are also seeking to leverage insiders—likely in order to conduct more sophisticated operations, such as ransomware deployment, data extortion, and cyber espionage. It is very likely that this proposed campaign will receive significant traction among financially motivated threat actors, as the majority of the risk lies with the recruited insider rather than the threat actor.

Recommendations

- Develop a comprehensive incident response strategy.
- Deploy a holistic patch management process, and ensure all IT assets are patched with the latest software updates as quickly as possible.
- Adopt a Zero-Trust cybersecurity architecture based upon a principle of least privilege.
- Implement network segmentation to separate resources by sensitivity and/or function.
- Ensure critical, proprietary, or sensitive data is always backed up to secure, off-site, or cloud servers at least once per year—and ideally more frequently.
- Implement secure password policies, phishing-resistant multi-factor authentication (MFA), and unique credentials.
- Configure email servers to block emails with malicious indicators, and deploy authentication protocols to prevent spoofed emails.
- Proactively monitor for compromised accounts and credentials being brokered in deep and dark web (DDW) forums.
- Leverage cyber threat intelligence to inform the detection of relevant cyber threats and associated tactics, techniques, and procedures (TTPs).

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%