ZEROFOX INTELLIGENCE

Flash

Campaign to Recruit Cryptocurrency Insiders

F-2026-02-06b

Classification: TLP:CLEAR

Criticality: LOW

Intelligence Requirements: Threat Actor, Cryptocurrency, Insider Threat

February 6, 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 7:00 AM (EST) on February 6, 2026; per cyber hygiene best practices, caution is advised when clicking on any third-party links.

| Flash | Campaign to Recruit Cryptocurrency Insiders

| Key Findings

- A newly registered and untested threat actor known as "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.
- In the post, LocalVulture shared three categories of insider individuals recruitment partners should target. It is likely that the actor has identified these categories in order to exploit financially motivated and inexperienced crypto exchange employees that may be more easily swayed to provide insider knowledge.
- LocalVulture specifies that, after identifying suitable insider targets for recruitment, partners are expected to rely on social engineering techniques to establish and maintain effective communication. ZeroFox assesses this indicates the actor is

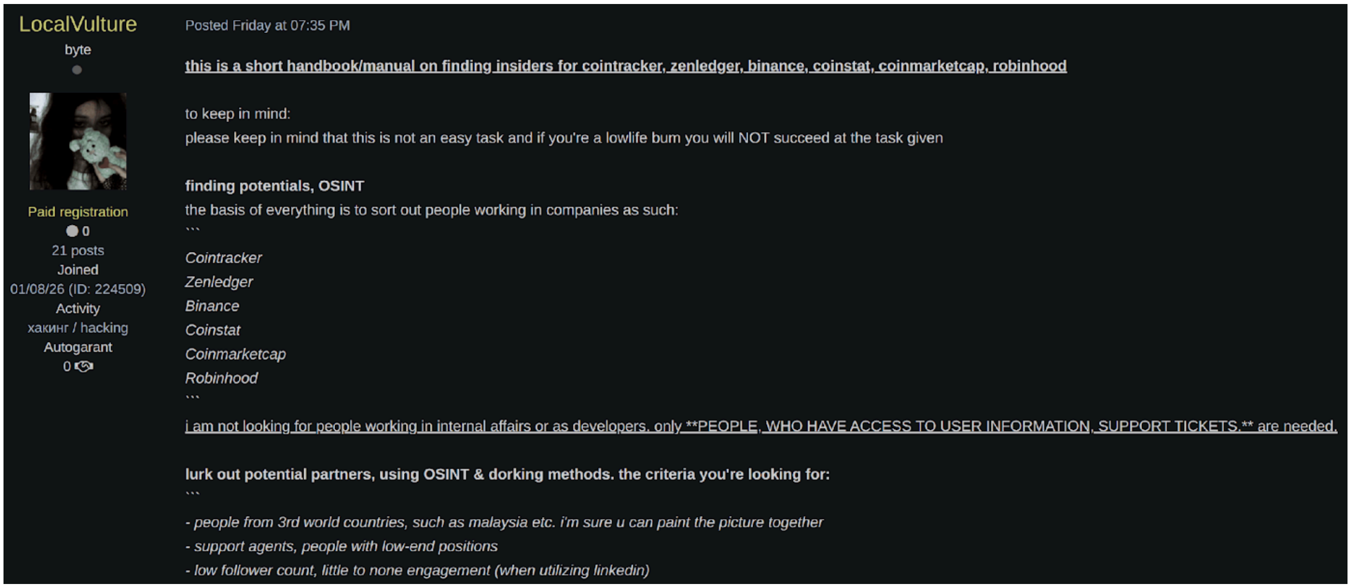
interested in conducting more sophisticated operations beyond financial fraud, such as ransomware deployment, data extortion, and cyber espionage.

Details

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
byte
Paid registration
● 0
21 posts
Joined
01/08/26 (ID: 224509)
Activity
хакинг / hacking
Autogarant
0

Posted Friday at 07:35 PM

this is a short handbook/manual on finding insiders for cointracker, zenledger, binance, coinstat, coinmarketcap, robinhood

to keep in mind:
please keep in mind that this is not an easy task and if you're a lowlife bum you will NOT succeed at the task given

finding potentials, OSINT
the basis of everything is to sort out people working in companies as such:
\`\`\`
Cointracker
Zenledger
Binance
Coinstat
Coinmarketcap
Robinhood
\`\`\`

i am not looking for people working in internal affairs or as developers. only **PEOPLE, WHO HAVE ACCESS TO USER INFORMATION, SUPPORT TICKETS.** are needed.

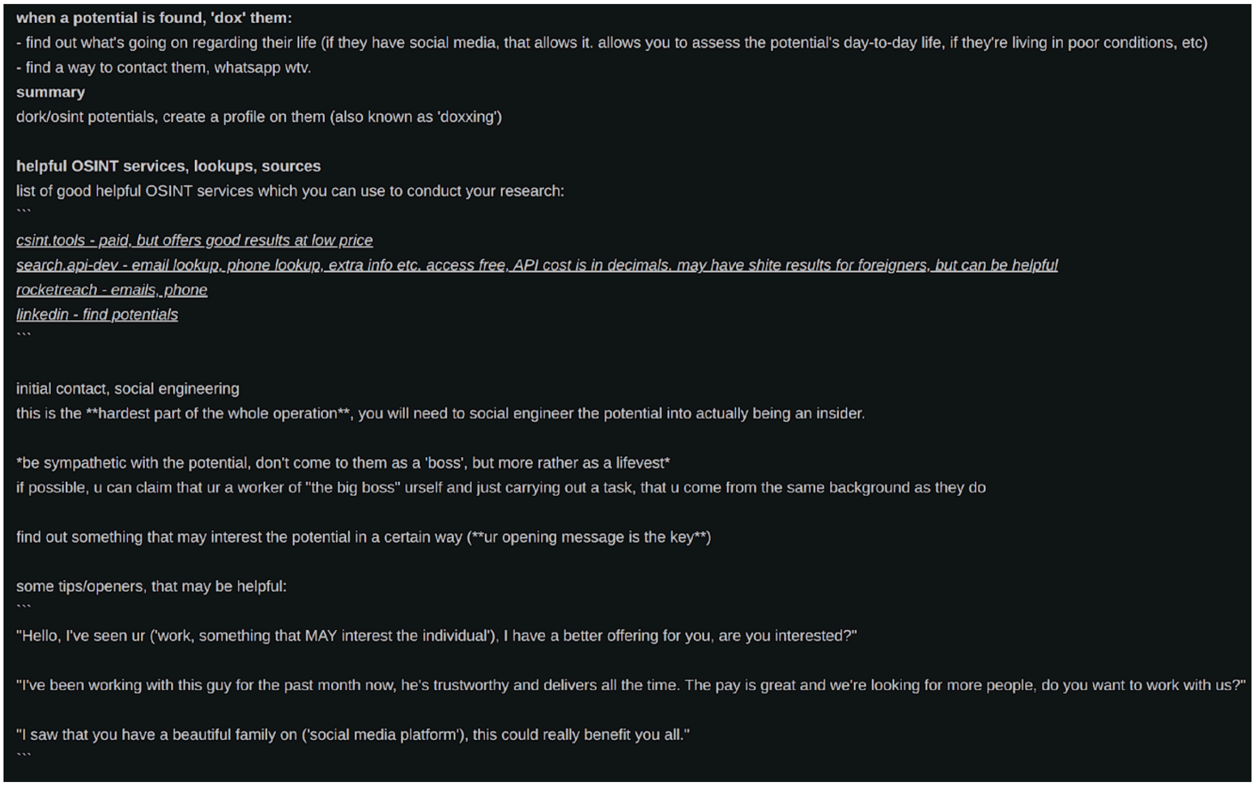
lurk out potential partners, using OSINT & dorking methods. the criteria you're looking for:
\`\`\`
- people from 3rd world countries, such as malaysia etc. i'm sure u can paint the picture together
- support agents, people with low-end positions
- low follower count, little to none engagement (when utilizing linkedin)

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."
```
~~~

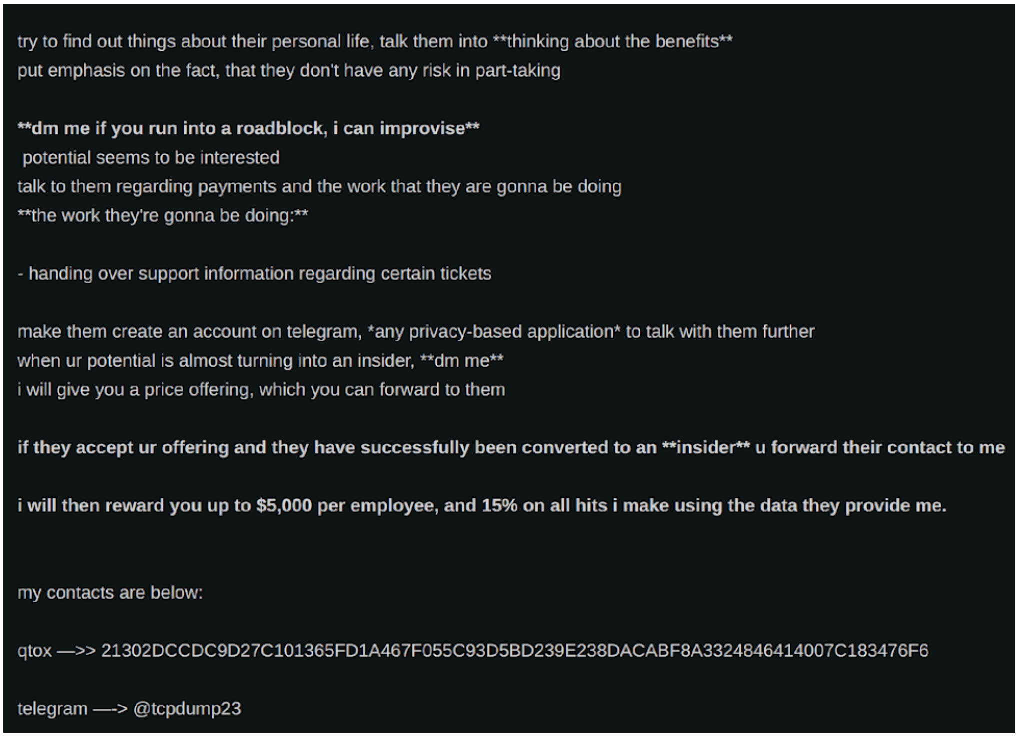
LocalVulture's Exploit post providing specific guidance and techniques

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.



```
try to find out things about their personal life, talk them into **thinking about the benefits**
put emphasis on the fact, that they don't have any risk in part-taking

**dm me if you run into a roadblock, i can improvise**
 potential seems to be interested
talk to them regarding payments and the work that they are gonna be doing
**the work they're gonna be doing:**

- handing over support information regarding certain tickets

make them create an account on telegram, *any privacy-based application* to talk with them further
when ur potential is almost turning into an insider, **dm me**
i will give you a price offering, which you can forward to them

if they accept ur offering and they have successfully been converted to an **insider** u forward their contact to me

i will then reward you up to $5,000 per employee, and 15% on all hits i make using the data they provide me.


my contacts are below:

qtox —>> 21302DCCDC9D27C101365FD1A467F055C93D5BD239E238DACABF8A3324846414007C183476F6

telegram —-> @tcpdump23
```

LocalVulture's Exploit post specifying payment to partners

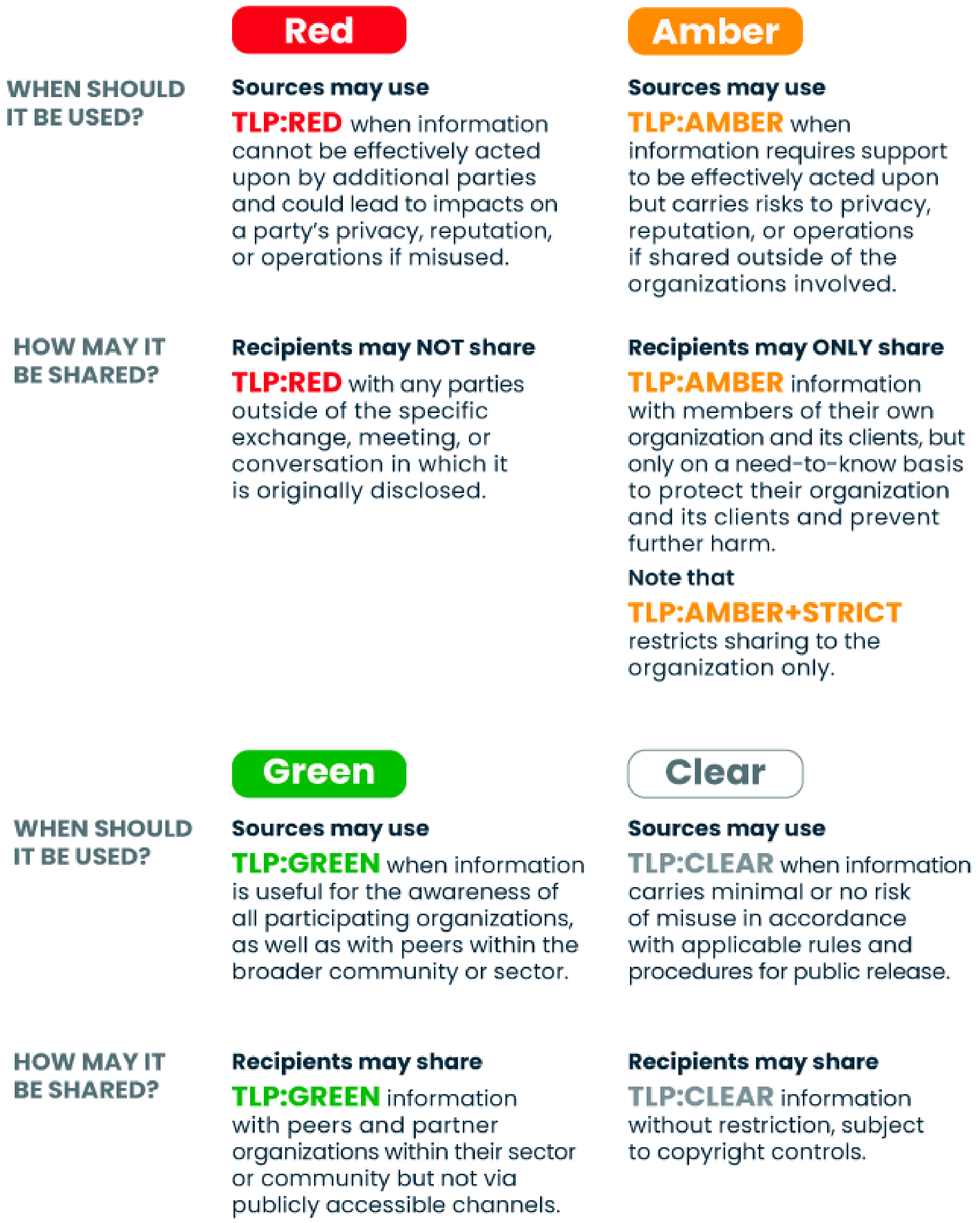
Source: ZeroFox Intelligence

The importance of utilizing insiders in large-scale cybercrime campaigns has often been underestimated. In this case, LocalVulture (or 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

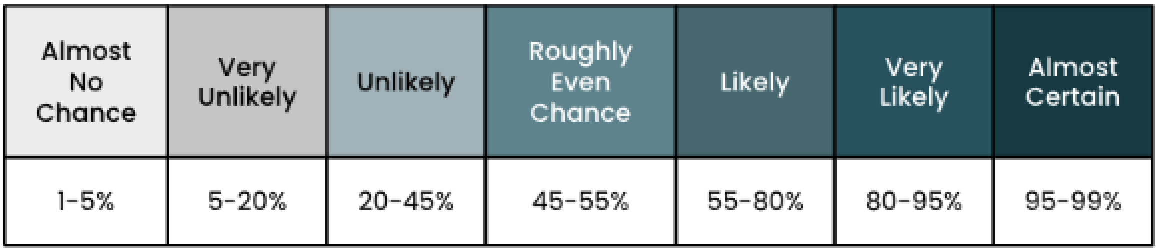


	Red	Amber
WHEN SHOULD IT BE USED?	**Sources may use** **TLP:RED** when information cannot be effectively acted upon by additional parties and could lead to impacts on a party's privacy, reputation, or operations if misused.	**Sources may use** **TLP:AMBER** when information requires support to be effectively 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%