



## | Brief |

# The Underground Economist: Volume 4, Issue 4

B-2024-02-15a

Classification: TLP:CLEAR

Criticality: Medium

Intelligence Requirements: Deep & Dark Web, Ransomware-as-a-Service

**February 15, 2024**

**Scope Note**

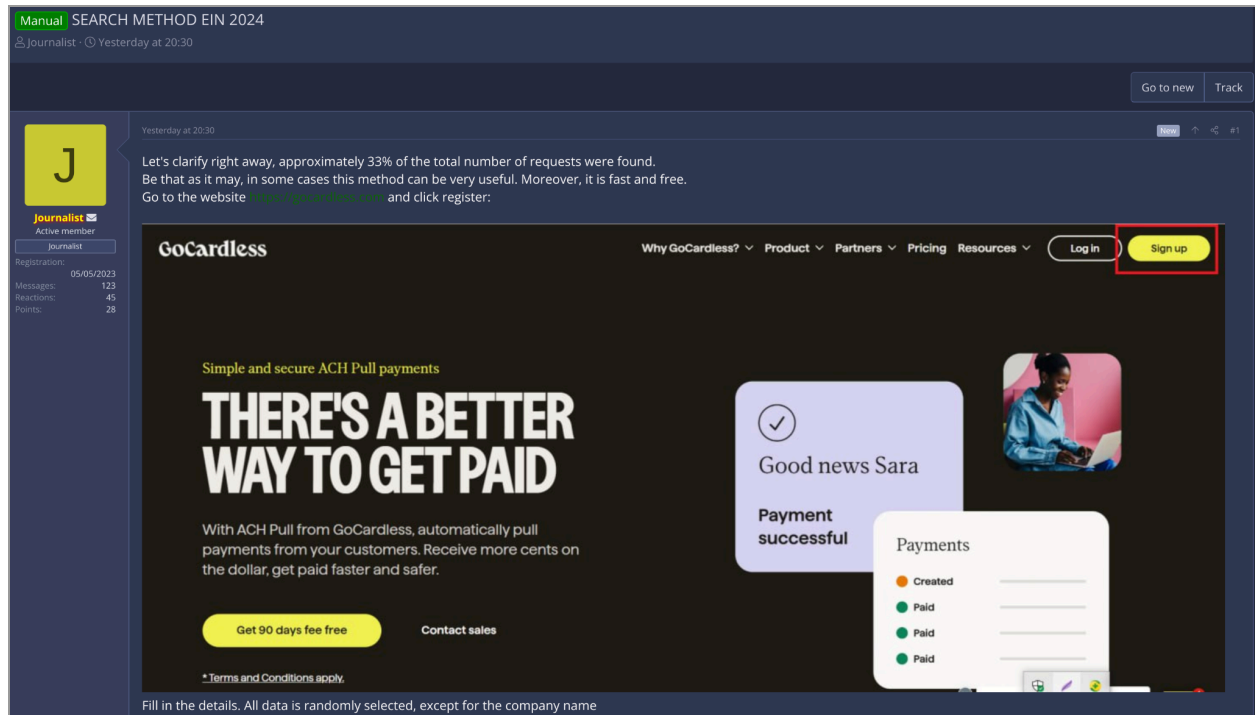
ZeroFox Intelligence is derived from a variety of sources, including—but not limited to—curated open-source accesses, vetted social media, proprietary data sources, and direct access to threat actors and groups through covert communication channels. Information relied upon to complete any report cannot 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 9:00 AM (EST) on February 15, 2024**; per cyber hygiene best practices, caution is advised when clicking on any third-party links.

# **Brief | The Underground Economist: Volume 4, Issue 4**

## **| New Tax Fraud Scheme Leveraging Employee Identification Numbers**

On February 11, 2024, well-regarded Russian-speaking threat actor “Journalist” disclosed a method of leveraging legitimate fintech services to collect information required for performing tax refund scams against U.S. citizens on the Russian-speaking community “Cookie Pro.”

- The method involves leveraging an entity’s Employee Identification Number (EIN) to conduct tax fraud schemes.
- Threat actors can use the EIN to create fake tax documents such as the W-2 form (an Internal Revenue Service tax form used to report wages paid to employees) and raise tax refund claims.
- Journalist advised leveraging gocardless[.]com, a service offered by a financial technology company specializing in online payment solutions, to register an account for free in the name of a targeted company in order to obtain its EIN.

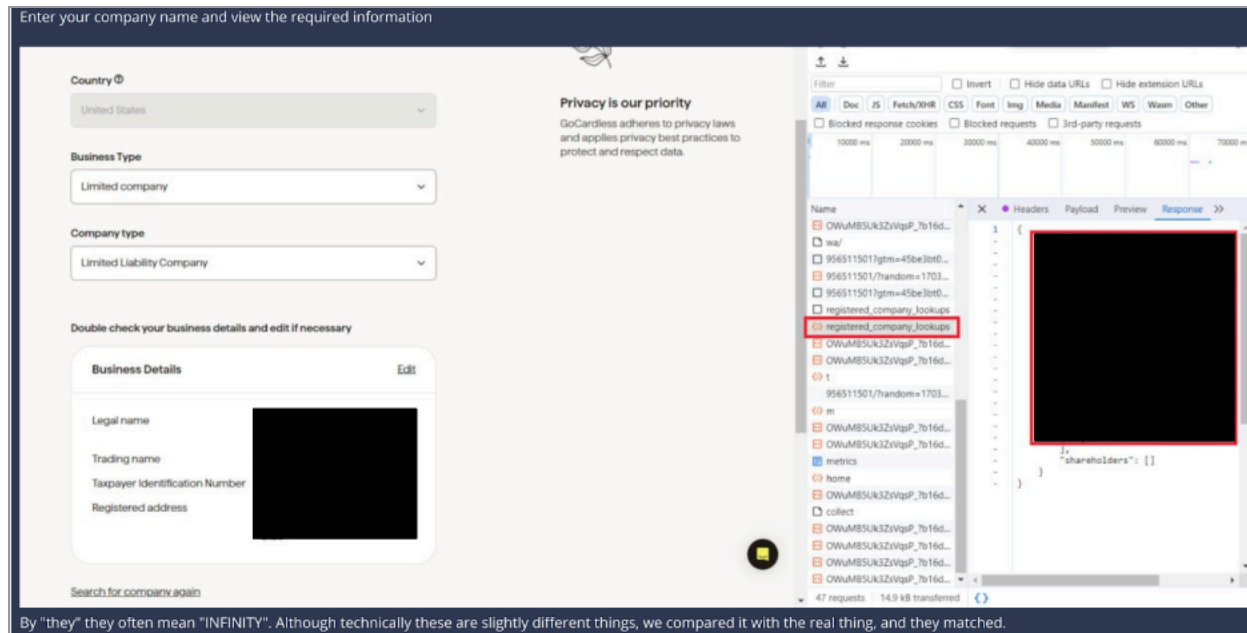


### Translation of Journalist's post outlining how to leverage GoCardless in tax return scams

Source: ZeroFox Intelligence

Journalist provided screenshots of the method in action, seemingly successfully obtaining the EIN for a U.S.-based construction company and confirming the EIN's authenticity by verifying it against another unnamed source.

- Journalist alleges to have obtained the EIN prior to paying for GoCardless' Pro Plan, circumventing any barriers to entry in providing a legitimate payment method that might disclose a threat actor's identity.



## **Translated and redacted screenshot showing the successful obtaining of a U.S.-based construction company's EIN**

*Source: ZeroFox Intelligence*

Tax refund and related schemes surge on the deep and dark web (DDW) in the run up tax season in the United States every year, with Russian-speaking threat actors seeking to leverage innovative methods for financial gain. Journalist's method demonstrates how a legitimate fintech service can be leveraged for performing scams against U.S. citizens. ZeroFox anticipates schemes of this nature will continue to propagate amongst financially-motivated actors ahead of the April 15, 2024, U.S. tax return deadline.

## **Second New Ransomware-as-a-Service of 2024 Announced in Dark Web Forum**

On February 2, 2024, English-speaking threat actor "koley" announced the launch of a Ransomware-as-a-Service (RaaS) project named Ransohub. The announcement, which was made in the Russian-speaking dark web forum RAMP, revealed that affiliates are now being sought. This is the second new RaaS operation that ZeroFox has identified in 2024 and follows the recent discovery of Wing, which was also posted in English.

**[RaaS] 2024 RansomHub**  
koley · Friday at 3:22 AM  
[Reply](#)

Forums > Market \ 市场 > Partners Program \ RaaS \ 合作伙伴计划

**K**  
koley  
May 3, 2023  
Messages 1  
Reaction score 1  
Points 3

Friday at 3:22 AM  
Welcome to join our affiliate raas program RANSOMHUB.  
We considered all the pros and cons of previous affiliate programs and created the next generation of ransomware.  
We have noticed that some affiliates have been seized by the police or have escaped from fraudulent activity causing you to lose your funds. We have adopted a new strategy, You can send your wallet to the chat room and send the decryptor after you confirm the payment. You don't have to worry about your funds security.  
Split is 90/10%, 90% in your direction and you pay us when you receive the money.  
**Locker**  
The Locker is written in golang and c++. The asymmetric algorithm is based on x25519, and the encryption algorithm is adjusted in aes256 chacha20 xchacha20 according to the hardware support, so we have a very fast encryption speed.  
The Locker supports intranet propagation, Safe Mode encryption and disconnected encryption.  
The Locker supports Windows, Linux, ESXi and other arm mips architectures.  
The Locker is obfuscated using AST, built daily.

[New](#) < > #1

[Jump to new](#) [Watch](#)

### RAMP post advertising new Ransomhub Raas project

Source: ZeroFox Intelligence

Koley proclaims Ransomhub to be “the next generation of ransomware”, offering affiliates numerous state-of-the-art features and benefits, including:

- Native architecture with encryption software written in Go Programming (Golang) and C++, which the threat actor claims will create complications for anti-virus (AV) software.
- “Very fast” encryption speeds assisted by an adaptive algorithm change method.
- Supports Windows and Linux-based operating systems, as well as virtual machines.
- Uses an Abstract Syntax Trees (AST) structure to re-encrypt every day, maintaining obfuscation.
- Access to the ransomware’s control panel, which offers affiliates a unique .onion domain. The panel is used to manage targets and log their accesses, use chat rooms, and create private blog pages that can be used for “proofing.”

## **Panel**

Each panel uses a separate onion domain, and the panels can manage targets and chat rooms.  
The panel allows you to view the logs of target accesses and the last access time.  
The panel supports Offline auto-reply for one message  
The panel can create a private blog page, which can be very beneficial for proofing and negotiation.

## **Ticket**

Affiliates who have joined our affiliate program to vouch for you.  
ID of any well-known forums, the longer the registration time or have a certain deal as well as reputation.  
Evidence of cooperation with other RaaS group (including, but not limited to, screenshots of payments received or balances at the receiving address.  
The best and quickest way to join is to pay a deposit(Returned to you after first getting paid.)

## **Rules**

We are not allow to attack CIS as well as Cuba, North Korea, China and Romania.  
Accounts that add false targets or have no activity for a certain period of time will be banned.  
Repeated attacks on paid targets are not allowed, encryption of non-profit hospitals is not allowed but data ransom is allowed.  
After the target pays, you must fulfill all the terms and agreements promised in the negotiations, otherwise you will be banned.  
We do not forbid you to cooperate with other RaaS team at the same time, but you can not disclose our panel address and account password, when we find more than one user logging in and do not explain the situation, we will ban your account.

TOX 4D598799696AD5399FABF7D40C4D1BE9F05D74CFB311047D7391AC0BF64BED47B56EEE66A528

Last edited: Yesterday at 5:09 PM

## **RAMP post advertising new Ransomhub RaaS project**

*Source: ZeroFox Intelligence*

Ransomhub also allegedly includes an innovative feature that enables and encourages efficient communication and cooperation between affiliates. The platform includes tools that enable affiliates to vouch for each other and share evidence of cooperation with other RaaS teams on previous projects.

- Features such as these are very likely an attempt to increase cohesion and trust amongst a fundamentally skeptical user base, particularly amidst numerous recent incidents of disruption and agitation in dark web marketplaces. Koley very likely views the ability to share information and cooperate as a means to increase the project's credibility, stature, and profitability.

As with the vast majority of RaaS operations, Ransomhub declares a host of countries off-limits to attacks under threat of banning from the platform. As expected, this includes countries within the Commonwealth of Independent States (CIS). The project also forbids attacks targeting organizations based in China, North Korea, and Romania.

- The exclusion of CIS likely indicates some affiliation with or loyalty toward the Russian state, though it may instead display intent to conform to the established norms expected when operating within Russian-speaking dark web marketplaces.
- Despite the omission of Iran, the banning of attacks against these states likely indicates geopolitical loyalties to parties seen as anti-Western.

Romania's status as a Western member of both the European Union (EU) and the North Atlantic Treaty Organization (NATO), and its inclusion in this list, indicates the group's likely loyalty, affiliation toward, or residence within the country.

- Romania-based organizations have been targeted in several high-profile ransomware attacks over recent years. In late 2022, the ransomware collective Hive attacked Rompetrol (one of the country's largest petroleum providers), and the Saint Gheorge Recovery Hospital in northeast Romania was held to a ransom of 3 Bitcoin in 2023.<sup>12</sup>
- Romanian National Police assisted in the international 2023 disruption of the prolific Qakbot malware, as well as the 2021 disruption of the REvil ransomware collective.<sup>34</sup> High-profile law enforcement operations have also resulted in the apprehension of Romanian nationals.<sup>5</sup>

The recent increase in new RaaS operations in dark web marketplaces are likely due, in part, to the significant 2023 disruption of prolific ransomware collectives such as ALPHV, NOEscape, and HIVE. While many affiliates from these groups likely associated themselves with existing RaaS operations such as LockBit, others very likely sought to create new services.

- New RaaS operations will likely continue to introduce novel and innovative services in an attempt to attract disenfranchised affiliates from other collectives.
- Due to 2023 seeing the highest number of attacks on record and threat group LockBit conducting more attacks in Q4 than any other quarter, the ransomware

---

<sup>1</sup> [hXXps://www.bleepingcomputer\[.\]com/news/security/rompetrol-gas-station-network-hit-by-hive-ransomware/](https://www.bleepingcomputer.com/news/security/rompetrol-gas-station-network-hit-by-hive-ransomware/)

<sup>2</sup> [hXXps://www.romania-insider\[.\]com/database-romanian-hospital-held-ransom-hackers-jan-2023](https://www.romania-insider.com/database-romanian-hospital-held-ransom-hackers-jan-2023)

<sup>3</sup> [hXXps://www.justice\[.\]gov/opa/pr/qakbot-malware-disrupted-international-cyber-takedown](https://www.justice.gov/opa/pr/qakbot-malware-disrupted-international-cyber-takedown)

<sup>4</sup> [hXXps://www.europol.europa\[.\]eu/media-press/newsroom/news/five-affiliates-to-sodinokibi/revil-unplugged](https://www.europol.europa.eu/media-press/newsroom/news/five-affiliates-to-sodinokibi/revil-unplugged)

<sup>5</sup> [hXXps://www.justice\[.\]gov/usao-sdny/pr/romanian-national-known-virus-extradited-operating-bulletproof-hosting-service](https://www.justice.gov/usao-sdny/pr/romanian-national-known-virus-extradited-operating-bulletproof-hosting-service)

and digital extortion threat landscape is very likely seen as an attractive opportunity by would-be threat actors.<sup>6</sup>

The announcement of Ransomhub in English further supports the recently-observed trend of English-speaking actors being willing to enter the traditionally-Russian dominated ransomware scene, as well as post in Russian-speaking dark web forums.

At the time of writing, ZeroFox has not observed any attacks implicating Ransomhub ransomware, though attacks are very likely to take place in the coming weeks—most likely against North American, Asian, or European-based targets.

## **| Innovative Loader-as-a-Service Announced**

Since its announcement on January 25, 2024, by untested actor “Null14”, an innovative malware loader-as-a-service offering has been gaining traction on the predominantly Russian-speaking dark web community exploit[.]in.

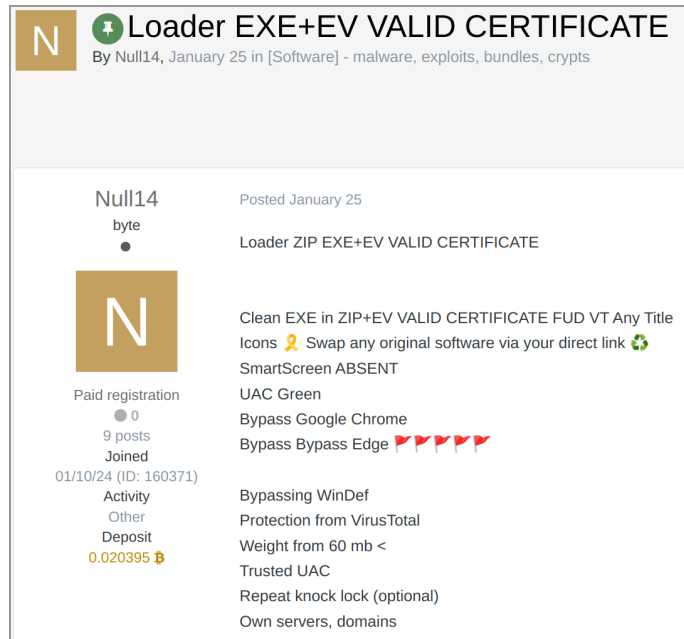
- Loaders are a crucial part of efficient malware-spreading campaigns, as they form the spearhead of actual malware introduction to a targeted system, establishing persistence and enabling follow-on malicious activity.

Null14 claimed the currently unnamed loader targets Windows operating systems and is signed using valid certificates. The actor’s post stated the loader boasts sophisticated detection evasion capabilities as a result of it being signed with valid certificates.

- Null14 alleged that this enables operatives to deploy and execute any weaponized software via a direct link without being detected by Windows SmartScreen, User Account Control, Google Chrome, Windows Defender, and potentially Microsoft Edge. The actor also claimed that use of valid certificates would enable the loader to remain unflagged by VirusTotal.
- The loader is encrypted, with additional re-encryptions possible once per day.
- The offering also included established servers and domains which host the loader and can be used to generate phishing links to target victims.

---

<sup>6</sup> ZeroFox Intelligence



**Loader EXE+EV VALID CERTIFICATE**  
By Null14, January 25 in [Software] - malware, exploits, bundles, crypts

Null14  
byte  
N  
Paid registration  
0  
9 posts  
Joined  
01/10/24 (ID: 160371)  
Activity  
Other  
Deposit  
0.020395 B

Posted January 25  
Loader ZIP EXE+EV VALID CERTIFICATE

Clean EXE in ZIP+EV VALID CERTIFICATE FUD VT Any Title  
Icons Swap any original software via your direct link  
SmartScreen ABSENT  
UAC Green  
Bypass Google Chrome  
Bypass Bypass Edge  
Bypassing WinDef  
Protection from VirusTotal  
Weight from 60 mb <  
Trusted UAC  
Repeat knock lock (optional)  
Own servers, domains

### Translated post announcing the launch of the new loader-as-a-service offering

Source: ZeroFox Intelligence

The loader is offered at a price of USD 490 per week; Null14's post specified that, should the certificate be revoked during this time, the remainder of the purchase period would be refunded.

- Buyers were prohibited from leaking information about the copyright holder of a certificate, as this would allow de-anonymization of the certificate.
- Any buyer caught in the act will have their subscription canceled.

Although ZeroFox can neither independently confirm nor disconfirm the credibility of the service, positive indicators add credence to the legitimacy of this loader service as an innovative malware-spreading technique that moves the burden of bypassing detection from the coding skills of malware developers to relying on valid software-signing certificates.

- On February 5, 2024, vetted exploit[.]in user "boomking" claimed this new loader service is the best solution available for the price requested. The actor also claimed to have successfully bypassed Chromium and Windows Defender using it.

- Null14 posted a screenshot that included a highlighted certificate for the WinRar application, indicating that a certain instance of the WinRar executable was likely weaponized.
- Null14 did not specify the origin of the certificates, but software-signing services and valid certificates have regularly been observed for sale in predominantly Russian-speaking communities since 2021.

Malware distribution based on emulating credible software is likely on an upward trajectory, and this trend is expected to continue in the first half of 2024.

## **| Recommendations**

- Adopt a Zero-Trust cybersecurity architecture based upon a principle of least privilege.
- Implement network segmentation to separate resources by sensitivity and/or function.
- Implement secure password policies with phishing-resistant multi-factor authentication (MFA), complex passwords, and unique credentials.
- Leverage cyber threat intelligence to inform the detection of relevant cyber threats and associated tactics, techniques, and procedures (TTPs).
- 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.
- Develop a comprehensive incident response strategy.
- Configure email servers to block emails with malicious indicators and deploy authentication protocols to prevent spoofed emails.
- Deploy a holistic patch management process and ensure all IT assets are updated with the latest software updates as quickly as possible.
- Proactively monitor for compromised accounts being brokered in deep and dark web forums.
- Configure ongoing monitoring for Compromised Account Credentials.

## | Appendix A: Traffic Light Protocol for Information Dissemination

|                                | <b>Red</b>                                                                                                                                                                                             | <b>Amber</b>                                                                                                                                                                                                                                                                                                                 |
|--------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>WHEN SHOULD IT BE USED?</b> | <b>Sources may use</b><br><b>TLP:RED</b> 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. | <b>Sources may use</b><br><b>TLP:AMBER</b> when information requires support to be effectively acted upon but carries risks to privacy, reputation, or operations if shared outside of the organizations involved.                                                                                                           |
| <b>HOW MAY IT BE SHARED?</b>   | <b>Recipients may NOT share</b><br><b>TLP:RED</b> with any parties outside of the specific exchange, meeting, or conversation in which it is originally disclosed.                                     | <b>Recipients may ONLY share</b><br><b>TLP:AMBER</b> 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.<br><b>Note that</b><br><b>TLP:AMBER+STRICT</b> restricts sharing to the organization only. |
|                                | <b>Green</b>                                                                                                                                                                                           | <b>Clear</b>                                                                                                                                                                                                                                                                                                                 |
| <b>WHEN SHOULD IT BE USED?</b> | <b>Sources may use</b><br><b>TLP:GREEN</b> when information is useful for the awareness of all participating organizations, as well as with peers within the broader community or sector.              | <b>Sources may use</b><br><b>TLP:CLEAR</b> when information carries minimal or no risk of misuse in accordance with applicable rules and procedures for public release.                                                                                                                                                      |
| <b>HOW MAY IT BE SHARED?</b>   | <b>Recipients may share</b><br><b>TLP:GREEN</b> information with peers and partner organizations within their sector or community but not via publicly accessible channels.                            | <b>Recipients may share</b><br><b>TLP:CLEAR</b> 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%         |