



| Flash |

Second New RaaS of 2024 Announced in Dark Web Forum

F-2024-02-07a

Classification: TLP:CLEAR

Criticality: High

Intelligence Requirements: Deep and Dark Web, Ransomware, Threat
Actor

February 7, 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 12:00 PM (EST) on February 7, 2024**; per cyber hygiene best practices, caution is advised when clicking on any third-party links.

| Flash | Second New RaaS of 2024 Announced in Dark Web Forum

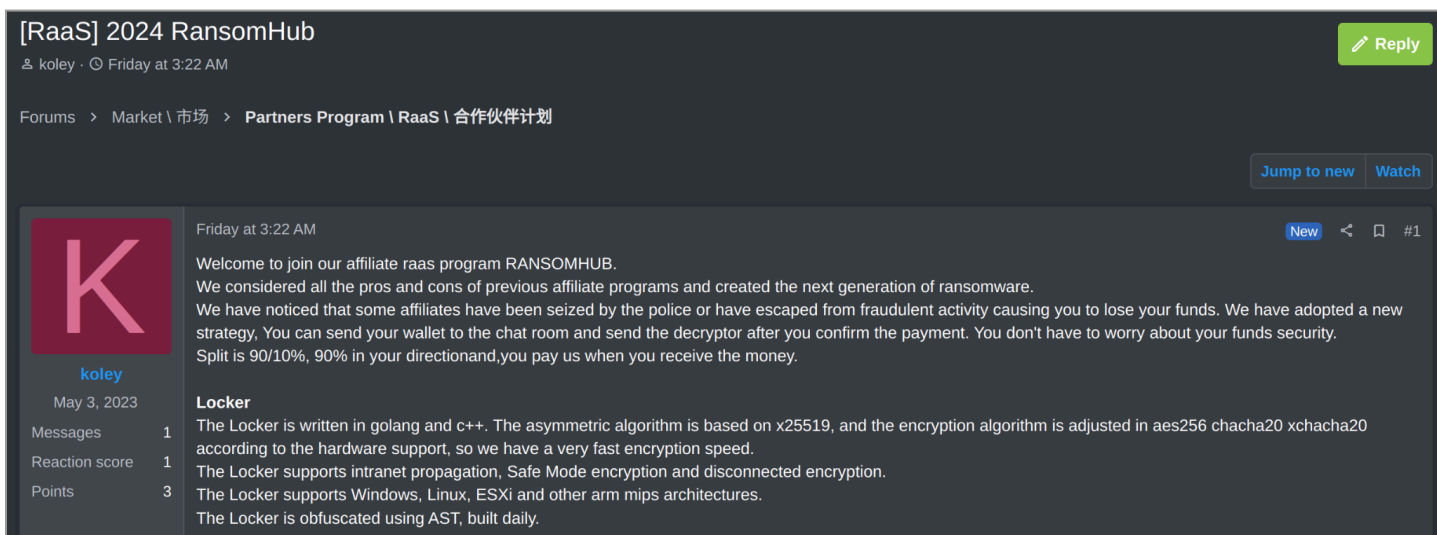
› Key Findings

- On February 2, 2024, English-speaking threat actor “koley” announced the launch of a Ransomware-as-a-Service (RaaS) project named Ransomhub. The announcement, which was made in the Russian-speaking dark web forum “RAMP”, revealed that affiliates are now being sought.
- Ransomhub allegedly offers affiliates a host of new features, such as daily re-encryption and access to a control panel comprising a unique .onion domain address.
- The announcement about Ransomhub in English aligns with 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.
- The recent increase in new RaaS operations observed by ZeroFox is likely contributed to by the recent disruption of several prolific ransomware and digital extortion (R&DE) threat collectives.

Details

On February 2, 2024, English-speaking threat actor koley announced the launch of a RaaS project named Ransomhub. 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.

- On January 28, 2024, positive-reputation English-speaking actor “blackhunt” announced a new RaaS operation known as Wing on the RAMP forum.
- In the post, Wing is touted as a state-of-the art ransomware tool with multiple features designed to facilitate effective deployment and defense evasion.



The screenshot shows a forum post on a dark-themed website. The title is "[RaaS] 2024 RansomHub" and the user is "koley". The post is dated "Friday at 3:22 AM". The forum path is "Forums > Market \ 市场 > Partners Program \ RaaS \ 合作伙伴计划". The post content includes a welcome message to affiliates, a description of the RANSOMHUB program, and a section titled "Locker" detailing its features and supported architectures. The post has 1 message, 1 reaction score, and 3 points.

[RaaS] 2024 RansomHub
koley · Friday at 3:22 AM

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

Jump to new Watch

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.

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

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 2023.¹²
- 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.³⁴ High-profile law enforcement operations have also resulted in the apprehension of Romanian nationals.⁵

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

¹ [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/)

² [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)

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

⁴ [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)

⁵

[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)

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 R&DE threat landscape is very likely seen as an attractive opportunity by would-be threat actors.⁶

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.

| Recommendations

- Implement secure password policies with phishing-resistant multi-factor authentication, complex passwords, and unique credentials.
- Configure ongoing monitoring for Compromised Account Credentials.
- Proactively monitor for compromised accounts being brokered in deep and dark web forums.
- Leverage cyber threat intelligence to inform the detection of R&DE threats; their associated tactics, techniques, and procedures (TTPs); and Indicators of Compromise (IOCs).
- 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.
- Adopt a Zero-Trust cybersecurity posture based upon a principle of least privilege.
- Implement network segmentation to separate resources.
- Develop a comprehensive incident response strategy.
- Configure email servers to block emails with malicious indicators, and deploy

⁶ ZeroFox Intelligence

authentication protocols to prevent spoofed emails.

- Deploy a holistic patch management system, and ensure all business IT assets are updated with the latest software as quickly as possible.
- Should your organization be impacted by a data breach, utilize ZeroFox Incident Response Services to swiftly deploy IDX data breach products and services to mitigate the impact to you and your customers.

| 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%