



| Brief |

The Underground Economist: Volume 4, Issue 3

B-2024-02-01a

Classification: TLP:CLEAR

Criticality: Medium

Intelligence Requirements: Deep & Dark Web, Threat Actors, Geopolitical
Threats, Ransomware, Business Email Compromise

February 1, 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 1, 2024**; per cyber hygiene best practices, caution is advised when clicking on any third-party links.

Brief | The Underground Economist: Volume 4, Issue 3

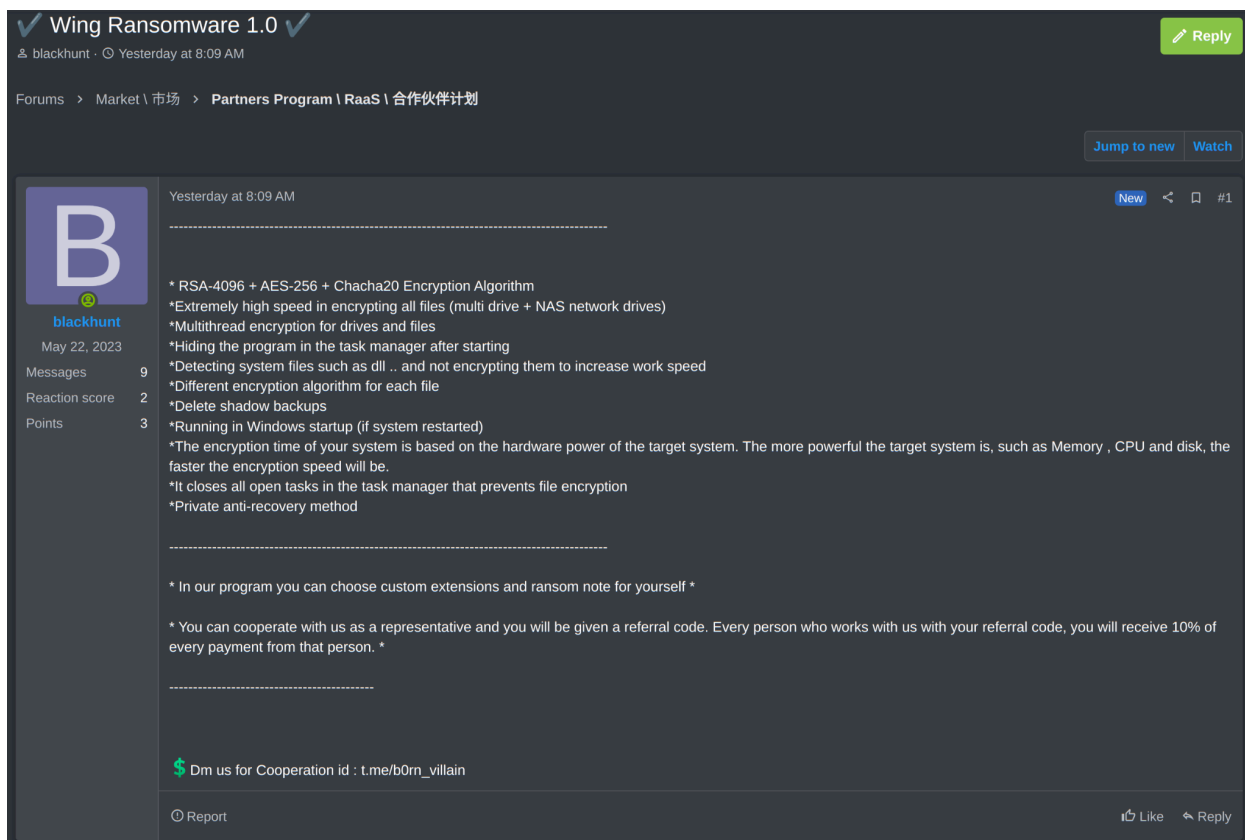
| Introducing Wing, New Ransomware-as-a-Service

On January 28, 2024, positive-reputation English-speaking actor “blackhunt” announced a new Ransomware-as-a-Service (RaaS) operation known as Wing on the predominantly Russian-speaking dark web forum RAMP. This is the first RaaS operation launched on RAMP in 2024, following seven such operations launched in 2023. (Several additional operations were announced in 2023 implicitly under the call for affiliates or pentesters.)

Wing is touted as a state-of-the art ransomware tool with multiple features designed to facilitate effective deployment and defense evasion, including:

- Three modes of encryption (and a changing encryption algorithm for each file)
- Multithreading
- Lateral propagation
- Persistence mechanisms
- Destruction of backups
- A “private” anti-recovery implementation

The post also states that affiliates can customize their copy and their ransom note and can refer other affiliates to receive 10 percent of the profits of their successful extortions.



Post announcing the launch of the Wing RaaS operation

Source: ZeroFox Intelligence

At the time of writing, ZeroFox has observed no instances of active deployment of the Wing ransomware strain, although victims are likely to emerge in coming weeks. The post indicates that 2024 will see continued diversification across the ransomware and digital extortion (R&DE) threat landscape with new operations emerging frequently, continuing the trend seen in 2023.

However, the announcement of the RaaS operation in English only—suggesting the threat actor is unable to speak Russian—indicates a continuation of the trend observed in Q4 2023 of English-speaking actors entering the ransomware scene, which has traditionally been dominated by Russian-speaking operatives.

| New BEC Campaign Set to Target Western Countries

On January 22, 2024, ZeroFox observed the announcement of a potential new BEC campaign in the dark web forum exploit[.]in. The declaration was made by well-regarded English-speaking threat actor “general7”, who is seeking partners that have “first hand” access to email accounts belonging to corporate entities based in Canada, the United States, the United Kingdom, and specific European Union countries.

- BEC is a type of cyberattack that enables the threat actor to gain unauthorized access to a personal or organizational email account before socially engineering victims. Threat actors—who are usually financially-motivated—leverage threat vectors such as account compromise and CEO or vendor impersonation to elicit fraudulent payment or data theft from unsuspecting victims.

General7 claimed to have significant experience in conducting BEC attacks and also alluded to their extensive network of contacts that assist in attack facilitation.

- An established network of affiliates very likely confirms general7’s consolidated ability to conduct successful BEC campaigns. The role of affiliates very likely differs depending upon the campaign specifics but could include specialists proficient in ransomware deployment, data encryption, or various social engineering methods.

The announcement claims that the campaign is set to generate substantial monetary profit, starting at “100k” and reaching as high as “5kk” (very likely USD 100,000 – 5,000,000). It is not made clear how such profit would be divided amongst associates.

- These figures are likely unrealistic and an attempt to attract attention from credible potential affiliates. However, the threat actor’s forum reputation (and their claim that proof of previous successes can be shown privately) indicate a small probability that such financial success is possible.

- BEC attacks are very likely becoming an increasingly lucrative attack vector for threat actors, with the median transaction observed during attacks reported to have almost tripled over the past five years to approximately USD 50,000.¹
- BEC attacks are also becoming increasingly common, reportedly making up the majority of cyberattacks.²

**Partnership with Business Email compromise - Professional work - Proof**
By general7, 7 hours ago in [Spam] - mailings, databases, responses, mail-dumps, software

**general7**
megabyte
●●●
Paid registration
7
86 posts
Joined
10/27/20 (ID: 110072)
Activity
вирусология / malware

Posted 7 hours ago
I need people who have first hand corporate email access, from networks/spam etc does not matter.
Countries: ca/usa/some eu/gb - and we can look at anything else you have as long as it meets our criteria.

I have been doing this for a very long time. I have success because i have a good network that i can trust.

Amounts that are done will start from 100k and go to amounts that are over 5kk and much higher.

I can show proof if i think you are serious. You can pm me your please TG if you want to discuss.

i can buy boxes as well from 1\$

Exploit[.]in post advertising new BEC campaign

Source: ZeroFox Intelligence

In the absence of the mention of malware, it is likely that the campaign will leverage traditional BEC tactics, techniques, and procedures (TTPs) such as using credential recycling and account takeovers to gain initial access to corporate email accounts. The threat actor can then proceed with numerous social engineering methods to accomplish predetermined, financially-motivated ends.

- During 2023, BEC attackers almost certainly adopted progressively more diverse TTPs. Threat actors increasingly used spoofed email addresses or stolen credentials to target supply chain entities associated with their primary target.

¹ [hXXps://www.tripwire\[.\]com/state-of-security/business-email-compromise-statistics](https://www.tripwire.com/state-of-security/business-email-compromise-statistics)

² [hXXps://www.verizon\[.\]com/business/resources/Te34/reports/2023-data-breach-investigations-report-dbir.pdf](https://www.verizon.com/business/resources/Te34/reports/2023-data-breach-investigations-report-dbir.pdf)

This enables them to leverage sensitive information to enhance credibility prior to conducting an impersonation attack, such as seeking payment for an outstanding legitimate invoice.

Despite advertisements seeking BEC associates being relatively rare in dark web forums, this is the second instance ZeroFox has observed in 2024. On January 8, untested threat actor “ke56” posted in three languages (English, Russian, and Chinese) in the RAMP forum seeking an associate with malware experience for a BEC campaign.

- This is not typical for such advertisements but coincides with ke56’s claim that the campaign will involve infecting victims’ networks with malware.

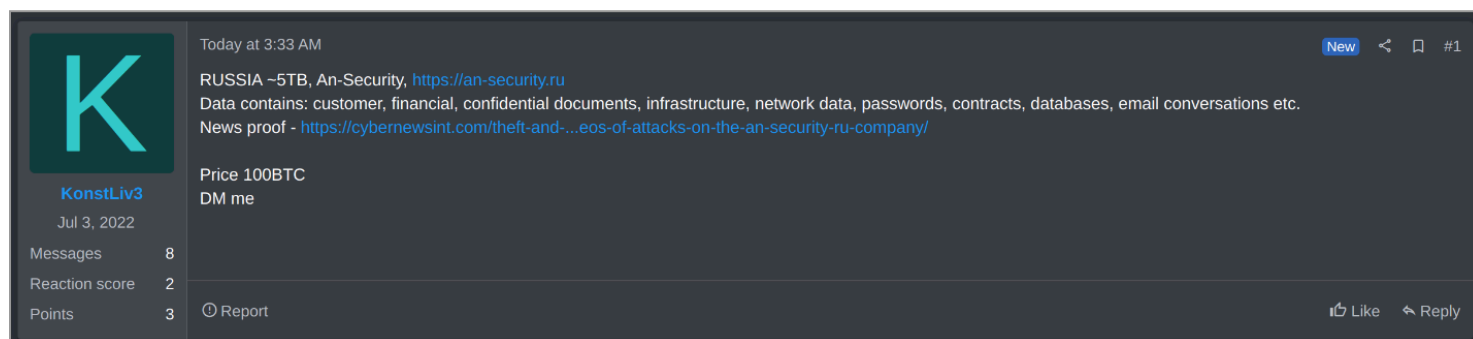
There is a roughly even chance that organizations will face an increased threat from BEC attacks in 2024, reflected by the upward trajectory in the number of attacks and financial impacts. Threat actors will very likely continue to enhance and diversify their social engineering TTPs, leveraging topical lures to target unsuspected aspects of an organization or its supply chain.

| LockBit Denies Attack Against Russian Entity

On January 26, 2024, LockBit representatives posted several statements in the predominantly Russian-speaking forum RAMP denying their involvement in an alleged extortion attack against the Russia-based security company An-Security—targeting that would violate the unwritten rules about using the strain to attack entities in Russia and other Commonwealth of Independent States (CIS) countries. The denial followed claims made on January 22, 2024, by threat actor “KonstLiv3”, who allegedly used LockBit ransomware in the extortion.

- KonstLiv3, an actor with a positive—albeit limited—reputation in the forum, sought to sell digital property amounting to 5 TB of customer and financial documents, network infrastructure access data, employee passwords, contract information, email correspondence, and various databases.

- KonstLiv3 included an asking price of BTC 100, equivalent to approximately USD 3,951,000 at the time the post was published. Given the nature of both the stolen information and the target, this is almost certainly deliberately exorbitant.

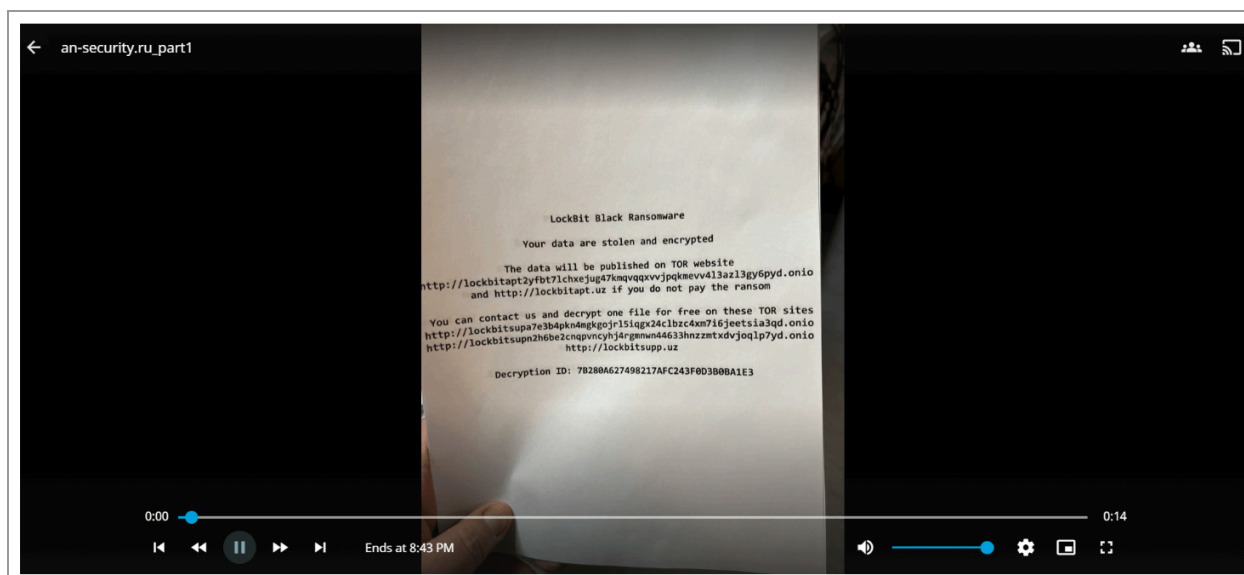


RAMP post advertising information stolen from An-Security

Source: ZeroFox Intelligence

The post included additional information intended to serve as proof the data has been obtained. This “News proof” consists of a URL directing to an information security magazine, which itself reported on the alleged attack. The magazine also provided screenshots of a video that suggests the prominent ransomware strain LockBit was leveraged in the attack.

- ZeroFox cannot confirm or deny the authenticity of this screenshot, where it occurred, or why the text is written in English rather than Russian.
- During extortion, LockBit typically conveys instructions to the victim electronically via the malware program.
- Using this link as “News proof” likely lowers the chance that the intent of the poster was a successful sale, as the unorthodox and low-quality approach would deter some interested buyers.
- A series of URLs pertaining to LockBit were present within both the post and the video screenshot. ZeroFox verified the authenticity of a link to a LockBit blog, while others such as Decryption ID URL—which promises to decrypt one stolen file for free—were confirmed invalid. Also, all are public data available via the open source.



Screenshot of a video containing a LockBit ransom note

Source:

[hXXps://cybernews\[.\]com/theft-and-disclosure-of-confidential-information-cybercriminals-share-videos-of-attacks-on-the-an-security-ru-company/](https://cybernews[.]com/theft-and-disclosure-of-confidential-information-cybercriminals-share-videos-of-attacks-on-the-an-security-ru-company/)

KonstLiv3's post violates a widely-held understanding within Russian-speaking dark web communities that it is prohibited to target victims in the CIS. The post sparked an almost-immediate backlash, with well-regarded Russian-speaking actor "Bratislava" responding, "You crazy or what? CIS is forbidden." KonstLiv3 was quickly banned by the RAMP moderator, and the post was locked (preventing a sale taking place).

- The CIS is an economic, political, and military intergovernmental organization that was formed in 1991 following the dissolution of the Soviet Union.

KonstLiv3's post triggered widespread speculation in separate deep and dark web (DDW) forum xss about the RAMP post and the potential implication of LockBit. Bratislava asserted that the LockBit collective was not involved, suggesting instead that "kids" had used the LockBit "builder."

- Several months after its detection in June 2022, the source code of LockBit's most recent malware strain (LockBit 3.0) was widely reported to have leaked, allowing other threat actors to leverage their own, customized version of the malware.

- Although this gave rise to an increase in the use of LockBit 3.0, threat actors seeking to create their own version would need to possess a level of proficiency not dispersed amongst all extortion collectives.
- “Kids” likely refers to unknown actors that were able to leverage the leaked LockBit 3.0 source code.



Братислава
HDD-drive
Пользователь
Joined: Jul 24, 2023
Messages: 21
Reaction score: 10

Today at 9:57 AM

<http://rampjcdlqvqko5oywutpo6ggl7g6tvddysustfl6qzhr5osr24xxqqd.onion/threads/russia-5tb-an-security-https-an-security-ru.1706/>

кажется это не **LockBitSupp** а может быть дети, которые используют биулдером локбита

Report



Братислава
Jul 27, 2023
Messages: 16
Reaction score: 18
Points: 3

Today at 8:35 AM

ты сумасшедший или что ?

CHГ запрещено
@vAz

Contant Tox: 5700F2F2B10F590AAEEEE1C6FA0410CA40A6CD08852B7A1FA26A37A6A06E1A40C6AAB43B8AD0D

"Они меня называют теперь сумасшедшим"

Report

New < > #2

Like Reply

Posted URLs allegedly pertaining to LockBit infrastructure

Source: ZeroFox Intelligence

LockBit’s series of denial posts is very likely reflective of the gravity of the claims and the concern the group has for its potential implication in the attack. LockBit stated that the attack had leveraged malware based upon the leaked (LockBit) builder and accused “Signature”—likely a threat actor pseudonym—of conducting the attack. LockBit further claimed that Signature is the “owner of the Clop affiliate programme” and offered a reward of USD 10,000,000 for information helping to identify the accused.

- ZeroFox cannot confirm if Signature is associated with the Clop extortion collective, and the reasoning behind LockBit’s accusation is unknown.
- The offering of such a large reward is very likely intended to serve as commitment to uncovering the attacker’s identity and to absolve LockBit of responsibility.

Another post from a LockBit representative alluded to a note allegedly received from an employee of the victim company, confirming contact between the two parties.

- The intent, channels, or reasoning behind these communications is unknown, but there is a roughly even chance that LockBit had intended to discover information that would aid in identifying the attacker.
- It is unknown whether LockBit intended or was able to return the victims' stolen data.

It is likely the attack took place, and threat actor KonstLiv3 is in possession of the stolen data. It is likely that LockBit malware was used by a threat actor able to leverage it against a Russia-based target—almost certainly violating any terms of use associated with LockBit malware.

- The attack was very likely conducted in this fashion to discredit the LockBit collective, either to satisfy a personal rivalry between extortion operatives or to exploit the general paranoia present amongst cybercriminals to sow confusion.
- It is unlikely to have been conducted knowingly by an established LockBit affiliate, as posting such an attack in RAMP—and at such an exorbitant price—would have either been a significant misjudgment by an inexperienced threat actor or indicative of very little intent to conduct a successful sale. LockBit generally does not advertise the sale of its stolen data in DDW forums.
- ZeroFox notes the unlikely possibility that the attack did not take place; the sale was illegitimate; and the post was an attempt to sow confusion, conduct general trolling activity, or carry out a financial scam. The exorbitant asking price would likely be an attempt to increase perceived authenticity for an actor with a limited reputation.

This event is reflective of the dynamic and likely paranoid environment found in DDW forums fueled by ongoing law enforcement evasion, the internal politics of threat collectives and their affiliates, and the ever-changing norms to which participants must abide in the pursuit and retention of a credible reputation that aids in lucrative sales. The quick banning of KonstLiv3 from RAMP and the prevention of the sale reinforces the low tolerance for targeting of CIS-based organizations within Russian-speaking threat actor forums.

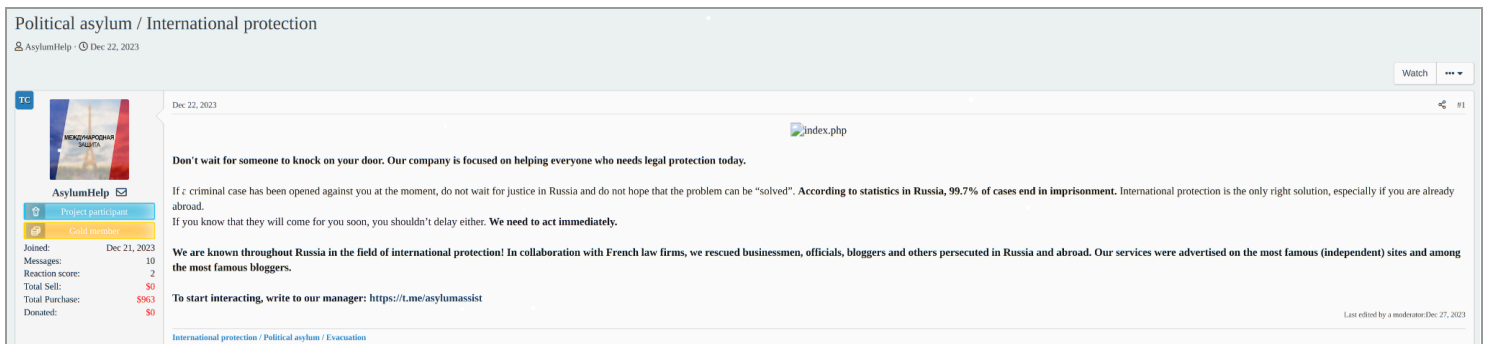
The threat posed by LockBit, Clop, or the wider R&DE threat landscape to Western organizations is almost certainly unchanged. LockBit, which conducted more attacks in Q4 2023 than any other quarter observed by ZeroFox, will continue to primarily target organizations based in North America and Europe, with particular emphasis on those in the manufacturing, retail, and construction sectors.

| Political Asylum Service to Assist Russians Fleeing to France

Since its announcement on December 22, 2023, a “political asylum” service claiming to assist Russians with fleeing to France has been gaining traction on the Russian-language deep web community WWH-Club. “AsylumHelp”, a positive-reputation actor, started the “Political Asylum/International protection” thread in December 2023, claiming that the process is entirely legal.

This latest post likely follows rumors of a new, large-scale mobilization looming in Russia. Following Russia’s invasion of Ukraine, ZeroFox has observed numerous posts in Russian-language DDW communities by threat actors seeking to avoid being implicated in mass mobilization.

- The service is not overtly advertised as a means to avoid forced conscription into the Russian army but rather as “helping everyone who needs legal protection today.”
- The post claims to help Russian citizens against whom a criminal case has been opened as, according to the actor, 99.7 percent of these cases end with imprisonment.
- The actor claims that the only way to avoid this is to receive asylum by moving abroad.



Political asylum / International protection

AsylumHelp · Dec 22, 2023

Dec 22, 2023

Don't wait for someone to knock on your door. Our company is focused on helping everyone who needs legal protection today.

If a criminal case has been opened against you at the moment, do not wait for justice in Russia and do not hope that the problem can be "solved". According to statistics in Russia, 99.7% of cases end in imprisonment. International protection is the only right solution, especially if you are already abroad.

If you know that they will come for you soon, you shouldn't delay either. We need to act immediately.

We are known throughout Russia in the field of international protection! In collaboration with French law firms, we rescued businessmen, officials, bloggers and others persecuted in Russia and abroad. Our services were advertised on the most famous (independent) sites and among the most famous bloggers.

To start interacting, write to our manager: <https://t.me/asylumassist>

International protection / Political asylum / Evacuation

AsylumHelp

Project participant

Gold member

Joined: Dec 21, 2023

Messages: 10

Reaction score: 2

Total Sell: \$0

Total Purchase: \$963

Donated: \$0

WWH-Club post advertising the political asylum service

Source: ZeroFox Intelligence

The post offers numerous incentives to threat actors seeking to purchase the services, with AsylumHelp claiming that the fees an asylum seeker needs to pay will be nullified by the benefits attained.

- AsylumHelp did not specify a price in the post, claiming instead that the exact price would follow a consultation. The actor claimed to accept escrow.
- The actor claimed that, if successful, Russian asylum seekers will be entitled to EUR 1,200 per month in addition to "real estate provided to our wards." Additionally, buyers could expect social privileges, such as free insurance and free travel.
- AsylumHelp is likely based in France, given they promote themselves as a group of "renowned advocates" who are easy to find in databases and legal registers in France.

Since the original post, AsylumHelp has added additional services to the offering.

- The actor recently claimed the service also operates in Ukraine, likely to enable males of conscription age to leave the country.
- On January 19, 2024, AsylumHelp announced additional legal services, such as procuring a talent visa for France, which is usually issued to exceptionally-skilled individuals and grants the recipient a permit to reside in France.
- On January 28, 2024, the actor offered an evacuation service in problematic cases, such those with debts or of conscription age in Russia, Ukraine, and

Kazakhstan. This likely means the threat actor has contacts in these countries able to provide emergency transport and a means to leave these countries.

TC


МЕЖДУНАРОДНАЯ ЗАЩИТА

AsylumHelp

Project participant

Gold member

Joined: Dec 21, 2023

Messages: 10

Reaction score: 2

Total Sell: \$0

Total Purchase: \$963

Donated: \$0

Jan 19, 2024

Additional services:
1) Assistance in obtaining a Talent visa (France).
2) Assistance in obtaining a French residence permit.
3) Assistance in relocation (renting - purchasing housing, assistance in integrating the whole family).
4) Assistance in obtaining visas to France.
5) Assistance in selecting French lawyers of any specialization.
6) Assistance in opening and maintaining a business in France.
7) Assistance in resolving commercial issues and disputes.
8) Breaking through the Interpol line

International protection / Political asylum / Evacuation

Report

TC


МЕЖДУНАРОДНАЯ ЗАЩИТА

AsylumHelp

Project participant

Gold member

Joined: Dec 21, 2023

Messages: 10

Reaction score: 2

Total Sell: \$0

Total Purchase: \$963

Donated: \$0

Yesterday at 5:09 PM

Additionally :
Evacuation with any problems
(ang. Business, Debts, Conscriptio age. and TD).
Russia, Ukraine, Kazakhstan.
Write: <https://t.me/asylumassist>

International protection / Political asylum / Evacuation

Report

**Updated post offering additional services,
including talent visa procurement and evacuation**

Source: ZeroFox Intelligence

ZeroFox can neither confirm nor deny the authenticity of the service or the claims made by the actor. If credible, the service has significant implications for the streamlining of immigration from Russia to Europe by finding and utilizing recognized legal mechanisms, such as asylum-seeking and talent visa procurement. There are factors that support its credibility, including:

- AsylumHelp has a positive reputation.
- The actor deposited the sum required to start doing business on the forum—in this case, USD 1,000.
- AsylumHelp has been regularly adding information to the thread and answering questions posted by interested actors.

However, it remains plausible AsylumHelp is seeking to scam or unmask citizens in Russia, Ukraine, and Kazakhstan that are attempting to dodge mobilization drafts. No successful deals have been recorded, and no public evidence was presented to affirm that the alleged “group of advocates” is authentic.

| 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 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

	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%