



| Brief |

The Underground Economist: Volume 5, Issue 3

B-2025-02-14a

Classification: TLP:CLEAR

Criticality: Medium

Intelligence Requirements: Deep and Dark Web, Threat Actor

February 14, 2025

Scope Note

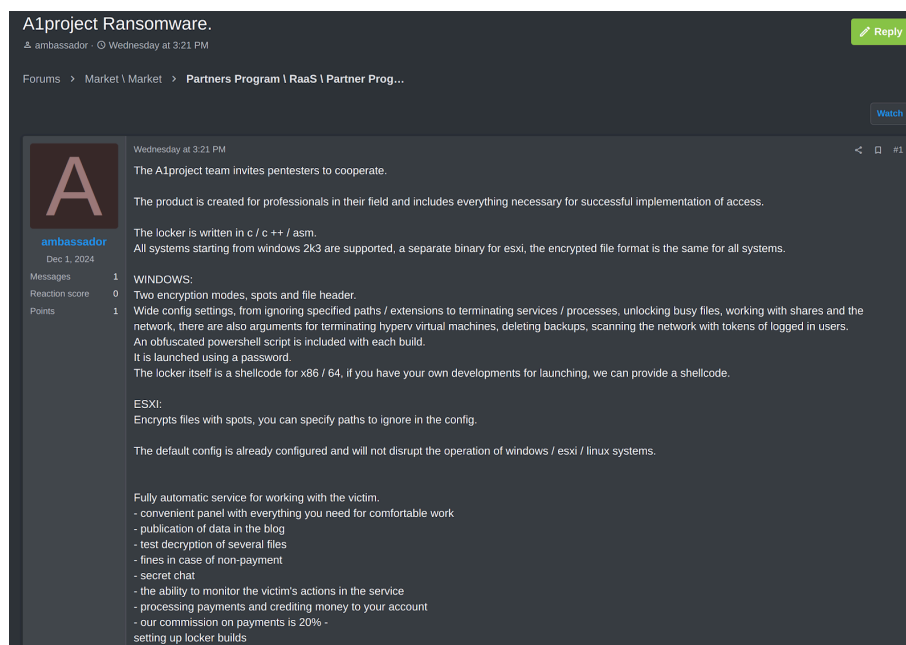
ZeroFox Intelligence is derived from a variety of sources, including—but not limited to—curated open-source accesses, vetted social media, proprietary data sources, and direct access to threat actors and groups through covert communication channels. Information relied upon to complete any report cannot 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 14, 2025**; per cyber hygiene best practices, caution is advised when clicking on any third-party links.

Brief | The Underground Economist: Volume 5, Issue 3

| New Ransomware-as-a-Service Project Advertised on RAMP

On January 29, 2025, untested Russian-speaking threat actor “ambassador” announced the launch of a new ransomware-as-a-service (RaaS) project called “AI Project Ransomware” on the predominantly Russian-speaking dark web forum RAMP. Ambassador claimed to have developed a fully functional product designed for “professionals” who can convert initial access into successful ransomware operations.

- ZeroFox has observed a high tempo of new ransomware & digital extortion (R&DE) collectives in recent months, with 45 new collectives identified in 2024, compared to 35 in 2023.
- Many of these commenced operations, demonstrated consistency, and posed a prominent threat faster than that observed in previous years.
- Law enforcement disruption to prominent threat collectives including LockBit and ALPHV has driven significant diversification of the R&DE threat landscape. This has paved the way for new collectives to increase their operational tempo.



Translated Post announcing the launch of the A1 Project Ransomware from RAMP

Source: ZeroFox Intelligence

A1 Project Ransomware is very likely still in its development phase. Although it is marketed as having advanced capabilities for efficient deployment and stealth, ambassador shared limited detail about the capabilities of the ransomware. The actor agreed to provide raw shellcode, upon being asked, and indicated that affiliates would be able to use their own tools for deployment. This would likely enable more capable affiliates to run the code in memory or for evading security controls to run a stealthier operation. Ambassador also stated that they were actively seeking penetration testers (pentesters) to collaborate on the tool. This continues the growing trend of R&DE collectives seeking collaborators to secure their product and infrastructure, particularly in the wake of high profile law enforcement activity.

A1 Project Ransomware does not currently operate a data leak site, but this is very likely to change as the service evolves. The actor stated that there would be an 80/20 split, with the collective's leadership charging a 20 percent commission on earnings from every successful ransom.

- This 80/20 split between leadership and affiliate is identical to the fee structure used by LockBit and many other ransomware collectives for their affiliates.

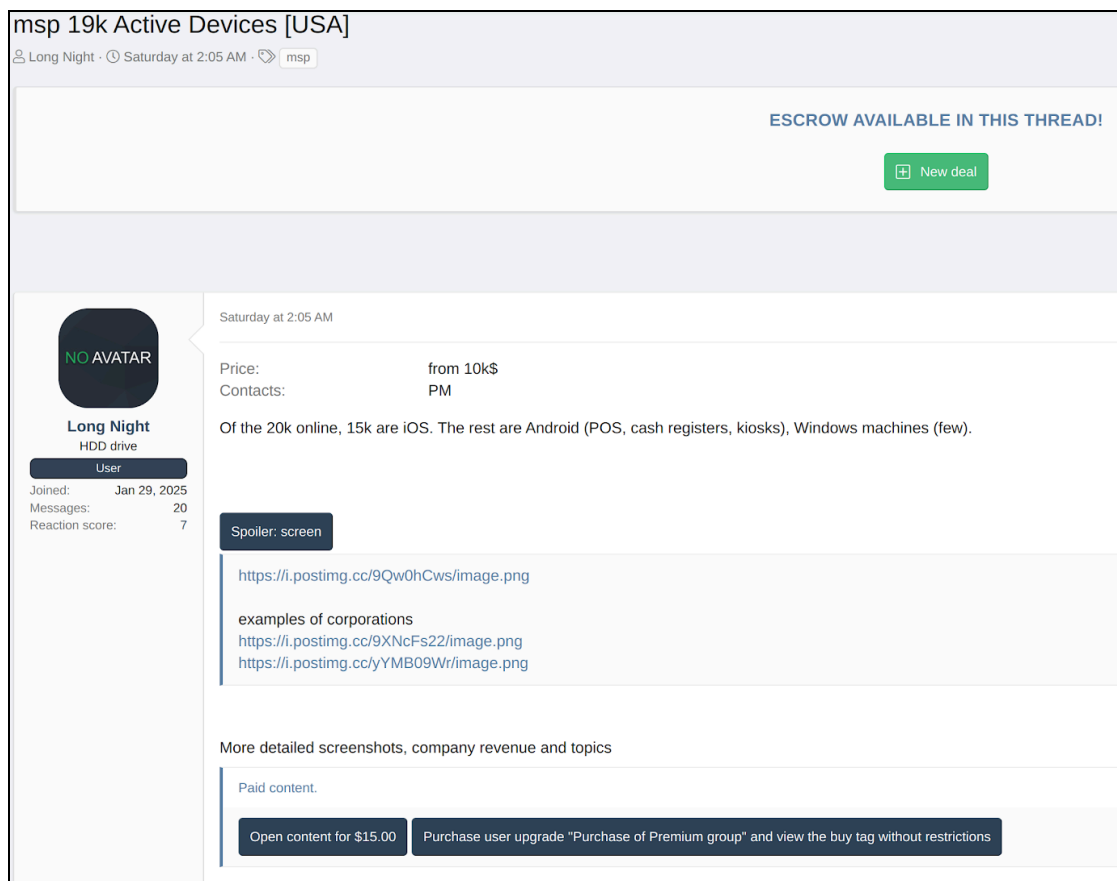
- This project is likely built upon an already established ransomware operation, although this cannot be independently verified at this time.
- The 20 percent commission charged is higher than some other prominent RaaS operations, including RansomHub who charge 15 percent commission on successful ransom negotiations. This is likely to dissuade some actors from joining AI Project Ransomware.

At the time of writing, the post has garnered very little traction on RAMP and ZeroFox has observed no evidence that the strain is being actively deployed. Prospective affiliates are likely exercising extreme caution, given the unknown credibility of the actor and the apparent alignment with other prolific RaaS operations like LockBit. This lack of engagement is likely to change if AI Project Ransomware begins to increase its operational tempo and can demonstrate its credibility and sophistication as a vector for financial gain.

| Threat Actor Advertises Network Access to likely U.S.-Based Managed Service Provider (MSP)

On February 8, 2025, Russian-speaking threat actor "Long Night" advertised network access to 19,000 active MSP devices on the predominantly Russian-language deep web forum xss. While the source of this access remains unknown, the actor stated that the 19,000 devices are U.S.-based, indicating the victim organization is very likely a United States-based MSP. Long Night stated that the MSP in question has 20,000 devices online, with the compromised devices including:

- 15,000 devices running iOS—an exclusive Apple operating system. These are likely primarily mobile devices, such as mobile phones, laptops and tablets.
- Various Android devices, allegedly including Point-of-Sale (POS) systems, cash registers, and kiosks. It is not specified whether mobile telephone devices are also included.
- A smaller number of devices running Windows operating systems. The type of devices were not specified.



Long Night advertising access to an unnamed U.S.-based MSP

Source: ZeroFox Intelligence

The actor stated that access could be purchased from USD 10,000. As alleged proof of the breach, Long Night shared three images purportedly from the MSP's management panel. They also offered additional details—such as screenshots, company revenue figures, and specifics about the breach—for an additional USD 15, payable on the forum to unlock the exclusive content.

- The USD 10,000 price for purchasing the access is notably lower than expected, particularly when considering the potential impact on multiple downstream organizations.
- This pricing may reflect the threat actor's desire to sell quickly or a lack of understanding of the full value of the data.

- The reason for the discrepancy between the 20,000 devices the actor claims the MSP has online and the 19,000 active devices the access affects is unclear.

It is likely that any unauthorized access to an MSP's network would enable threat actors to deploy malicious payloads, steal sensitive data, and compromise multiple clients by exploiting the provider's centralized management systems. The breach could also lead to financial losses for affected businesses due to ransom demands, downtime, or the theft of sensitive financial data.

| Pro-Palestine Actor Claims to Target Israeli Hospital

On February 6, 2025, English-speaking hacking group "blackfield" posted in the dark web forum RAMP—where they have a positive reputation, stating that they had compromised the networks of an Israel-based financial institution. According to the advertisement, the breach enabled blackfield to obtain data pertaining to the bank accounts of Israeli Defence Force (IDF) personnel, as well as the personal computer of a senior officer.

- Blackfield detailed that their previous activity targeting IDF personnel had only provided access to personally identifiable information (PII) such as phone numbers and email addresses, but following the latest breach they are able to provide access to "live bank accounts".

Blackfield did not advertise a price for the access, which will very likely be negotiated in private messaging channels. Also provided is alleged proof of access, composed of blurred images displaying what appears to be a banking login portal with username and password fields already populated. A live view of the compromised accounts is also allegedly available, but prospective buyers are required to deposit at least BTC 1 to the forum.

- At the time of writing, BTC 1 is the equivalent of approximately USD 97,000—a significant sum which many interested parties would be unable or unwilling to provide. Blackfield's reputation in the forum is very positive, however, largely owing to their history of attacks targeting Israeli targets. This almost certainly increases the likelihood of a successful negotiation.

Bank Leumi Israel & IDF bank accounts
blackfield · Thursday at 9:29 AM

Forums > Market \ 市场 > Access (SSH/RDP/VNC/Shell) \ 访问

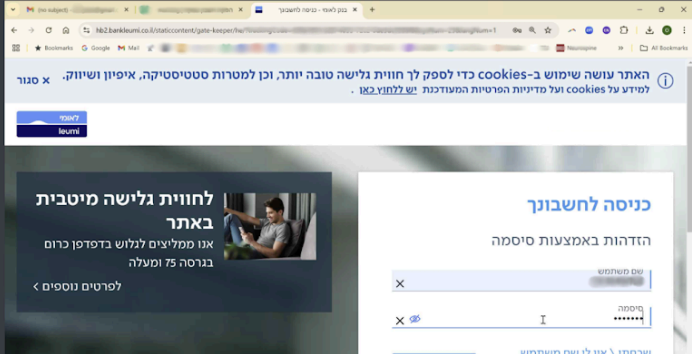
Thursday at 9:29 AM

Hey ! 🤖

The samples below related to Senior IDF officer , and we have more like him !!
In the past sales it's was just phone & emails & other data , now we can provide Live bank accounts
any members in ramp from israel and want to be rich contact us with bank account but say free Palestine first 😊

Note : IF anyone interesting we can provide Live View Into the accounts , But First you need to deposit into ramp at least 1 BTC

Freeccs



RAMP post by Blackfield, advertising compromise of IDF personnel

Source: ZeroFox Intelligence

If the offering available is as-advertised, it is very likely to appeal to a wide range of threat actors.

- Financially-motivated actors can use the access to initiate unauthorized fund transfers, though security challenges such as multi-factor authentication (MFA) are almost certain to hinder this process. The data can also be used to attempt credential stuffing attacks, in order to establish access to a victim's other accounts.
- Politically-motivated actors, particularly opposing nation states, will almost certainly deem this offering as a means of gathering information pertaining to high-profile members of the IDF. While significant government-classified

information is unlikely to be present on personal networks, PII can be used to access other personal accounts—leading to malicious activity such as extortion.

- Ideologically-motivated hackers, such as other cyber threat groups with an aversion to Israel, almost certainly deem this data as a means by which to conduct malicious activity such as doxxing, extortion, or physical attacks.

| 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 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 forums.
- Leverage cyber threat intelligence to inform the detection of relevant cyber threats and associated TTPs.

| Appendix A: Traffic Light Protocol for Information Dissemination

WHEN SHOULD IT BE USED?

Red

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.

Amber

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

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.

Clear

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%