



Brief

The Underground Economist: Volume 4, Issue 1

B-2024-01-05a

Classification: TLP:CLEAR

Criticality: Medium

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

January 5, 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 January 4, 2024**; per cyber hygiene best practices, caution is advised when clicking on any third-party links.

Brief | The Underground Economist: Volume 4, Issue 1

| Stolen marinetraffic[.]com Data Available for Sale

On December 27, 2023, threat actor “APTlord” announced on the dark web forum RAMP that they were selling source code and other information owned by marinetraffic[.]com, which was allegedly obtained by the theft of backup data from web-based Git repository GitLab. Marinetraffic[.]com is an open-source analytics platform that provides real-time information on maritime vessels and activity around the globe. Some of the information available includes:

- The geographic positions of vessels (accuracy and update frequencies vary between vessels)
- Vessel details (such as photographs, country of operation, speed, design, and other physical attributes)
- Journey details (such as originating locations and destinations and expected arrival times)
- Information relating to maritime infrastructure (such as port locations, capacity, traffic statistics, and weather conditions)

SELL: Marinetrtraffic.com gitlab backup data{ source code}

& APTlord · Wednesday at 5:05 PM Reply

Forums > Main \ 主要内容 > Data base & leakage \ 数据库和泄露

Jump to new Watch



APTlord
Oct 29, 2023

Messages 1
Reaction score 0
Points 1

Wednesday at 5:05 PM New < □ #1

The MarineTraffic website has derived from a community-driven project that was based on research collaboration among global academics and the development of existing Information & Communication Technology (ICT). It has always been (and still is) dedicated to collecting and presenting data which can be exploited in research areas such as, but not limited to, the following:

- Study of marine telecommunications in respect of efficiency and propagation parameters
- Simulation of vessel movements in order to contribute to the safety of navigation and to cope with critical incidents
- Interactive information systems design
- Design of databases providing real-time information
- Statistical processing of ports' traffic with applications in operational research
- Design of models for the spotting of the origin of pollution-related incidents
- Design of efficient algorithms for sea path evaluation and for determining the estimated time of ship arrivals
- Correlation of the collected information with weather data
- Cooperation with Institutes dedicated to the protection of the environment

MarineTraffic provides a provides information about current geographical positions of ships as well as other related information, whenever available, such as ships' details, their destination, estimated time of arrival, photographs, port traffic statistics, weather conditions, points of interest, etc.
MarineTraffic is a global pioneer in AIS vessel tracking.

Gitlab backup file will be sold to a single person.

Note:I agree to work with escrow!

Price:8k\$

RAMP post advertising the sale of source code owned by marinetrtraffic[.]com

Source: ZeroFox Intelligence

The price requested for the data is USD 8,000, and the threat actor claims that the information will only be sold to a single buyer. APTlord also explicitly agrees to using escrow (a third-party mediator able to facilitate the sale). This is likely indicative of a credible threat actor and sale.

APTlord asserts that some of the website's research areas—such as interactive information systems design, design of databases providing real-time information, and correlation of the collected information with weather data—can be exploited. It is unclear, however, how this information could be directly leveraged to facilitate attacks against maritime targets, especially given the abundance of detail already publicly available. There is a roughly even chance that the original purpose of the stolen data was the facilitation of extortion, which either failed or never took place.

This announcement comes at a time of uncertainty for many maritime organizations, with high levels of regional unrest influencing military, economic, and political maritime

operations in the Mediterranean Sea, the Red Sea, the Suez Canal, the Indian Ocean, and the South China Sea. In addition to financially motivated threat groups seeking to conduct extortion attacks, it is likely that this advertisement is seeking to attract the attention of actors interested in geopolitical affairs. This likely includes government entities and politically/ideologically-driven threat groups—both of which have been observed targeting maritime assets in recent weeks.

| New “Prank” Service Offered to Organizations in Dark Web Marketplace

On December 26, 2023, untested Russian-speaking threat actor “PrankService” announced a new global “prank” service on dark web forum exploit[.]in. The service offers to help clients deal with competition or enemies and turn the target’s “life into a nightmare.”

- Services on the dark web offering direct harassment and intimidation of third parties are relatively rare, particularly those involving physical or non-cyber techniques.

P

Prank service. Let's turn life into a nightmare!

By PrankService, 1 hour ago in [Other] - everything else

Follow 1

Start new topic

Reply to this topic

PrankService

byte

●

P

Paid registration

● 0

1 post

Joined

12/25/23 (ID: 159475)

Activity

Other

Posted 1 hour ago

Report post

Do you want to take revenge on the scammer who cheated you? To distract a competitor from business, or just to take revenge on a moron neighbor? - Then you should come to us, we are the ones you need. Expensive, high-quality, effective!

We are a full-fledged service, our specialty is to turn the life of your enemy into a real nightmare. Make the victim change addresses, numbers, and contacts, lose what they had, and don't get what they could. So that life before our intervention would be considered a dream.

We have a whole range of offline and online measures that we are ready to fully use against your enemy.

If you do not have complete information about the victim, then you will only need primary information, the rest we will try in agreement with you and work in order to get the most effective result.

We do not ask for prepayment AT ALL, you pay 100% of the payment to the guarantor. In case we failed to complete the work, but we undertook, we compensate the guarantor's commission. Or pay directly in BTC / Monero.

We work EVERYWHERE, in ANY city, ANY country.

We take on almost everything, it is not important the status of a person, where and who he is, we are not afraid of difficulties.

We work 100% anonymously and confidentially.

Exploit[.]in post advertising new “prank” service (translated)

Source: ZeroFox Intelligence

The actor claims that their actions can cause the target to change address, telephone numbers, and contacts; incur financial losses; and lose business opportunities. This can be achieved using both “online and offline measures,” which very likely alludes to the leveraging of both cyber and physical (non-cyber) disruption techniques such as systematic harassment, threats, and spam communications.

- The actor further claims that they can study intended targets to facilitate results, which likely relates to a service offering a more tailored or bespoke disruption approach.
- A client is only required to provide the target’s “primary information” in order to ensure the legitimacy of the target.
- The service is allegedly available in every city and country. It is unclear how this may impact the actor’s ability to conduct physical measures against the target.

How are we different from others? - We are really working. If you have previously searched for these services, then you have faced the fact that EVERYONE refused the guarantor, took 100/50% of the prepayment in advance and then merged, or a complete frost in contacts / the matter never went beyond a conversation.

To understand how we work - you write to us by contacts, tell us what you need, we offer our options that we can fulfill, negotiate the terms and payment, then you make a payment to the guarantor, and we get to work. + - this is the scheme of work.

Prices: from \$1000 and more, depending on how much time it takes us to complete and how much complexity it takes.

For more detailed information about the services provided, please write to the contacts.

Telegram: <https://t.me/PrankService>

Jabber: PrankService@exploit.im

TOX – leave yours, I’ll add you

If necessary, I can make a deposit.

Exploit[.]in post advertising “Prank” payment and contact details (*translated*)

Source: ZeroFox Intelligence

Services start at USD 1,000 and increase requisite with the time and complexity associated with the job. Although payment is said to not be required until the job is complete, it is unclear what conditions determine a “complete” attack. Payment is made to exploit[.]in’s escrow service, which—given the lack of the actor’s reputation and sales history/vouches—is the only element indicative of likely credibility.

The nature of the service is very likely to appeal to a vast array of individuals and organizations that are seeking to take punitive, disruptive, or vengeful measures against

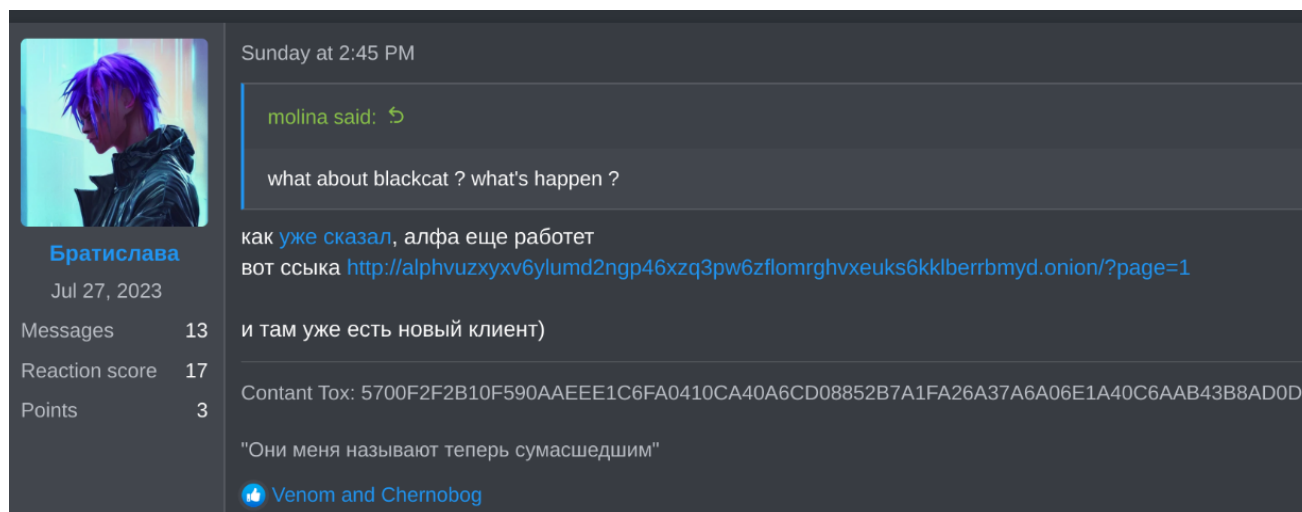
an opposition. Should the actor establish a credible reputation on exploit[.]in and keep the price relatively low, the service will likely attract a high volume of clients from across the globe. A similar service was observed in 2019 in dark web marketplaces, though it was restricted to “prank call” type communications. “PrankService” appears to be significantly more comprehensive in techniques leveraged, seemingly aiming to inflict actual reputational, financial, and psychological damage on the target.

- The service was announced solely in Russian, indicating the demographic/location of its target audience. The intended targets are, therefore, very likely to be Russian-speaking, particularly relating to the unspecified “offline measures.”

| Threat Collective ALPHV Continues a Reduced Attack Tempo

Evidence observed by ZeroFox indicates that Ransomware & Digital Extortion (R&DE) threat collective ALPHV (also known as BlackCat) is still operational following the Federal Bureau of Investigation’s (FBI) disruption and seizure of their dark web infrastructure and release of a free decryption tool on December 19, 2023. ALPHV representatives quickly disputed the extent of the disruption caused, claiming sufficient contingency to continue operations on alternative infrastructure.

- In the most recent instance, on December 23, 2023, well-regarded threat actor “Братислава” (“Bratislava”) once again affirmed via a post on dark web forum RAMP that ALPHV is still operational. Bratislava referred to a functioning darknet blog belonging to the threat collective and noted that a new victim had been added very recently.
- ZeroFox Intelligence has observed 14 attacks conducted by ALPHV in the 17 days since December 19, 2023. This is roughly equal to the number of attacks in the 17 days prior to the FBI disruption.



Post translating to “As I have already said, alpha (ALPHV) is still working. Here is the link (...) and there is already a new client”

Source: ZeroFox Intelligence

- The restored darknet blog indicated that “clients” (victims) were added by ALPHV on December 22, 23, and 24, soon after the FBI’s initial statements relating to the operation.

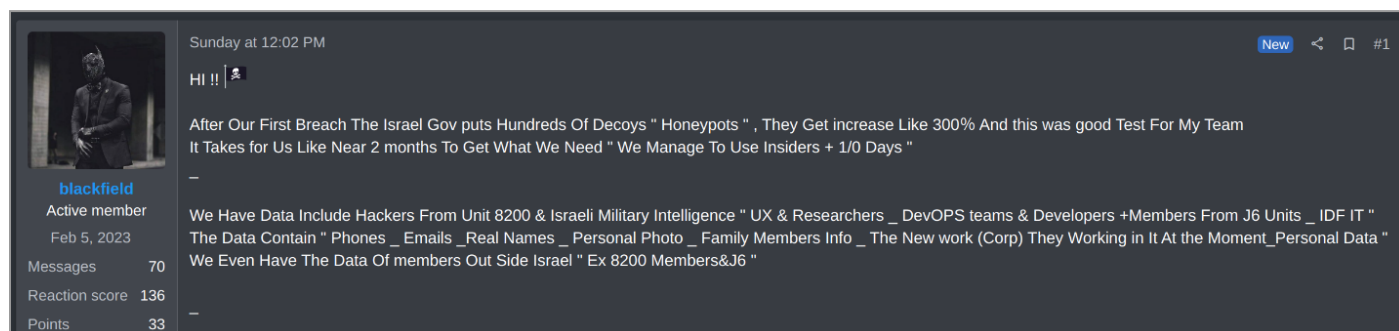
| Threat Actor Seeks to Profit from Israel–Hammas War

On December 24, 2023, threat actor “Blackfield” posted on the dark web forum RAMP announcing a data breach targeting the Israeli Defense Force (IDF). Blackfield is a well-regarded threat actor and was among the first RAMP actors to announce the sale of stolen information relating to the IDF and Shin Bet (Israel’s Internal Security Agency), as reported by ZeroFox on October 11, 2023.

The most recent breach reportedly affects members from the military intelligence capability Unit 8200, which is subordinate to the IDF’s Military Intelligence Directorate. The data is alleged to include personal information pertaining to both current and ex-members, such as:

- Email addresses
- Phone numbers
- Personal photographs
- Data relating to family members

The actor indicated that the breach took a long time (two months in total) due to numerous “Honeypots” set up by the Israeli government and the leveraging of “Insiders.”



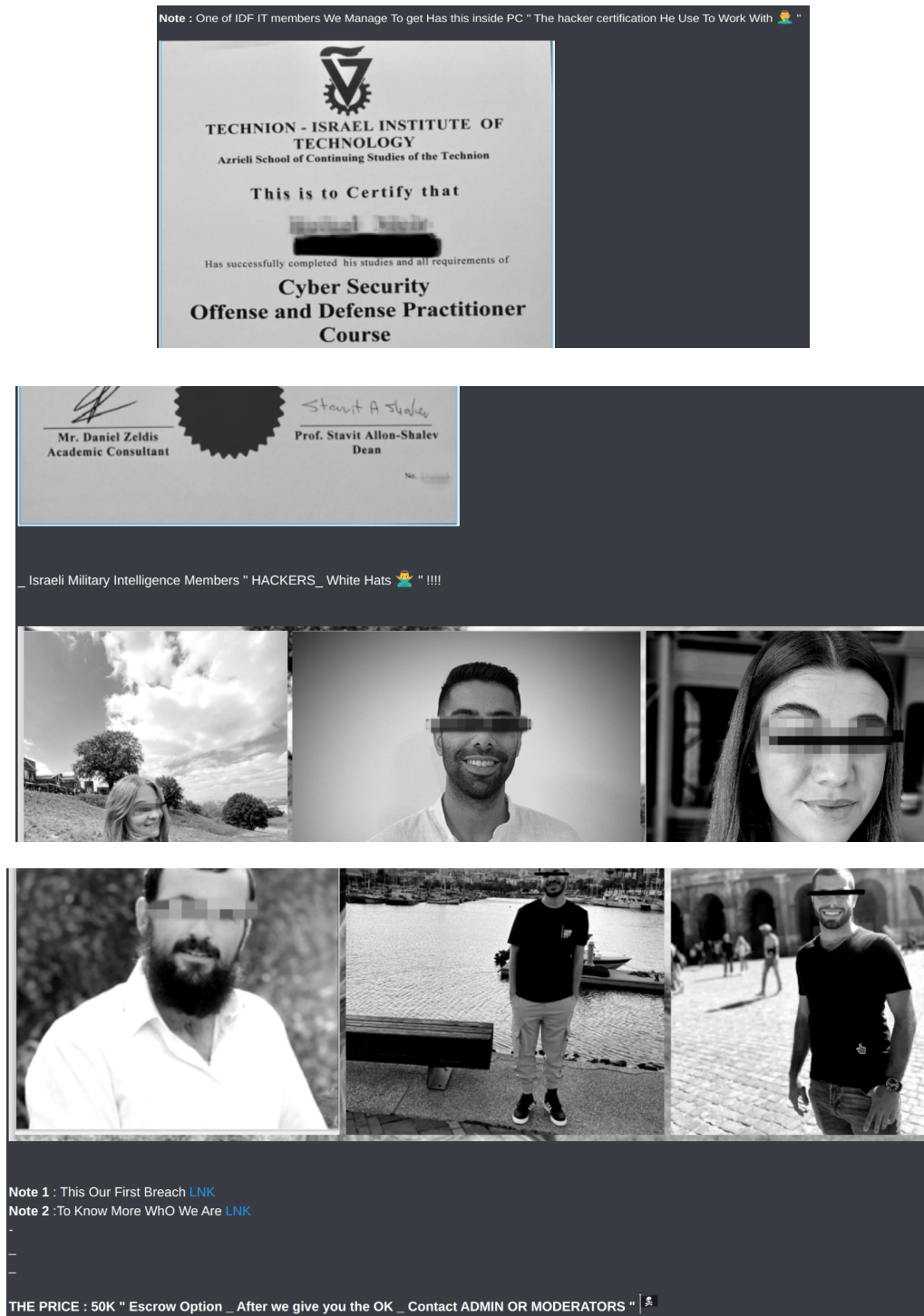
RAMP post claiming Unit 8200 data breach

Source: ZeroFox Intelligence

The actor announced a price of USD 50,000 for the breached data. The steep price is likely indicative of the actor’s intent to advertise the information to politically and ideologically motivated threat actors deemed able to afford it, such as nation-states and affiliated groups.

- The willingness to use escrow, longstanding forum reputation, and the offer of alleged samples are all positive indicators and behaviors consistent with a reputable actor.

The thread gained significant traction on the forum, garnering positive feedback and congratulations by likely ideologically incentivized actors. A skeptical minority questioned whether the data originated from an already-known breach, such as the Israeli Technion breach in February 2023, and doubted the credibility of the alleged samples.



Embedded "Samples" serving as a proof of life

Source: ZeroFox Intelligence

Notwithstanding these uncertainties, this post confirms the continued targeting of Israeli government entities in data theft attacks by high-profile threat actors that likely seek clients of nation state-level capabilities. Depending on the threat actor's credibility, it may also attest to the ongoing employing and leveraging of insiders within the Israeli military that are used to extract sensitive, very likely classified information.

The intended use of this information is unclear; however, such information is likely appealing to the governments and intelligence services of states opposing Israel and its role in the ongoing Israel-Hamas War. Militant groups in the region and the numerous cyber threat collectives that have been observed conducting attacks against Israeli targets in recent weeks would also likely deem such information valuable to the pursuit of their geopolitical ends.

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

	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%