



| Brief |

The Underground Economist: Volume 4, Issue 17

B-2024-09-05b

Classification: TLP:CLEAR

Criticality: Medium

Intelligence Requirements: Deep and Dark Web

September 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 (EDT) on September 5, 2024**; per cyber hygiene best practices, caution is advised when clicking on any third-party links.

Brief | The Underground Economist: Volume 4, Issue 17

Threat Actor Returns with Sales of Government Email Addresses

On August 22, 2024, threat actor “Pwnstar” announced that they are selling “high quality” .gov email addresses for use in espionage, social engineering, and data extortion activities. Pwnstar has previously been observed conducting similar activity as early as October 2023, when they advertised details associated with the governments of developing nations. However, in this most recent announcement, Pwnstar specified the availability of data pertaining to Five-Eyes countries, alongside others such as Italy, Belgium, and “many more.” The announcement further specifies that no email addresses associated with “CIS Countrys” will be available.

- Five-Eyes countries refers to the intelligence-sharing alliance and agreement between the United Kingdom (UK), the United States, Canada, Australia and New Zealand.
- CIS refers to the Commonwealth of Independent States, an international association composed of sovereign states that were once part of the Soviet Union. As of the writing of this report, the CIS is composed of nine states.
- A multitude of governments use .gov domains; the majority also include their country code top level domain, such as .gov.uk in the UK and .gov.au in Australia.

- These .gov email addresses are not ordinarily associated with government networks that contain highly classified information, such as those used by the military. However, it is very likely that they are regularly used to communicate sensitive, official, or proprietary information.

Pwnstar's alleged government email access almost certainly originates from parsed logs derived from stealer malware previously deployed to the compromised systems. According to the advertisement, various types of session cookies are also available, which threat actors can leverage to obtain access to accounts and bypass multi-factor authentication (MFA) security protocols. Pwnstar advises that the email accounts and cookies can be exploited alongside stolen subpoena documents to impersonate various legal authorities. Finally, Pwnstar offers access to various "law enforcement panels", which can allegedly be used to search for various types of personal information.

On September 1, 2024, the positive reputation actor "gulak" posed on the thread to inform Pwnstar that they had sent a direct message enquiring about the service. Gulak has previously been observed conducting initial network access brokerage activities, and their interest is likely indicative of the level of interest financially motivated extortion collectives will have in the offerings.



RAMP post advertising .gov email addresses

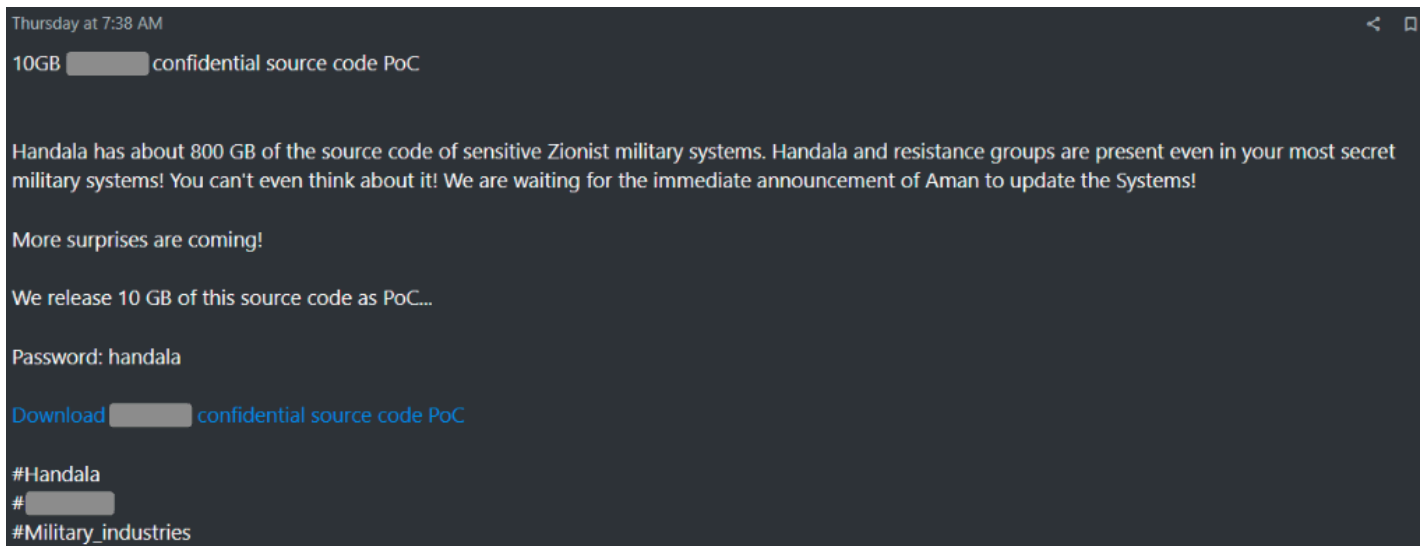
Source: ZeroFox Intelligence

| Israeli Defense Organization Targeted in New Data Breach

On August 22, 2024, the hacktivist collective “Handala” posted in deep and dark web (DDW) forums RAMP and BreachForums announcing a data breach targeting an Israel-based organization that specializes in the design and development of embedded electronic systems for industrial and military customers. According to the announcement, Handala successfully exfiltrated approximately 800 gigabytes of source code correlating to “sensitive military systems.”

A download link and password was included, with Handala claiming that 10 gigabytes of information has been made available for download to serve as a proof of concept (PoC). It is unclear how the remainder of the information can be obtained, but it is likely for sale.

- Historically, Handala has primarily conducted transactions via its Telegram channels. However, these have been disrupted on multiple occasions—most recently on August 25, 2024, three days after the announcement of this data breach. There is a roughly even chance that this disrupted or delayed any sale of the stolen information.



BreachForums post advertising Handala data breach, with victim obfuscated by ZeroFox

Source: ZeroFox Intelligence

On August 25, 2024, Handala posted a subsequent thread revealing a number of allegedly top-secret design schematics related to electronic equipment used by the “Zionist Air Force” (almost certainly a reference to the Israel Air Force branch of the Israeli Defense Force). This post also included links to Telegram channels and a password.

- This post was very likely intended to serve as a further PoC for the data breach, as well as provide examples of the types of information available. It is very likely that information such as this is treated as proprietary or classified in accordance with government security standards by both governmental defense agencies and their contracted partners and suppliers.



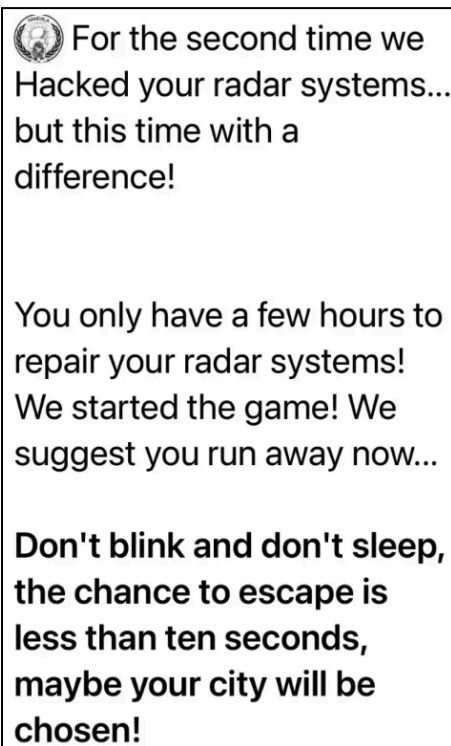
Handala emblem

Source: ZeroFox Intelligence

Handala was first observed in approximately December 2023, two months after the escalation in hostilities between Hamas and Israel. At that time, the hacktivist group began conducting cyberattacks against high-profile targets based in Israel and other allied nations. Below are some of the most prominent alleged incidents:

- Beginning in December 2023, Handala’s attacks targeted unspecified Israel-based users of F5 networking products with a strain of wiper malware. The campaign leveraged sophisticated social engineering techniques to target users of Microsoft Windows and Linux operating systems.

- In April 2024, Handala claimed to have breached networks associated with Israeli military radar systems and the Iron Dome national missile defense system. Though alleged screenshots were posted to demonstrate the network access, it is not clear if any operational disruption was caused as a result or if any sensitive information was stolen. Subsequently, thousands of SMS messages were sent to Israeli citizens, warning that only “a few hours” remained to “repair your radar systems.”

**Handala SMS message sent to Israeli citizens**

Source: [https://thecyberexpress\[.\]com/handala-hacker-group-warns-israel/](https://thecyberexpress[.]com/handala-hacker-group-warns-israel/)

- In June 2024, Handala posted in BreachForums claiming to have successfully breached the network of a cloud security organization, deleting and exfiltrating 51 terabytes of data—including intellectual property and customer information. Handala also posted several screenshots of the victims’ network dashboards to serve as a PoC.

- In July 2024, Handala posted in BreachForums claiming to have successfully stolen five terabytes of information from networks belonging to one of Israel's largest hospitals. The data is alleged to include staff and patient details, financial records, and medical research documentation. Fifty gigabytes was published to serve as a PoC.

Handala is almost certainly primarily politically and ideologically motivated, as exemplified by its name, emblem, statements appearing to mock Israeli security capabilities, and consistent attacks against Israeli organizations and those in countries perceived as sympathetic to Israeli strategic objectives. However, unlike other hacktivist groups that have been observed conducting attacks against Israeli entities in response to Israel-Hamas hostilities (such as "SiegedSec" and "Anonymous Sudan"), Handala has also demonstrated an intent to monetize its attacks where possible, either by the sale of stolen information or digital extortion methods.

If the stolen information is as described, it is very likely to attract interest from an array of threat actors that range from politically impartial cybercriminals seeking to enhance their social engineering campaigns to state-aligned or state-associated actors able to exploit data relating to military hardware and pursue a strategic advantage. Given the notably positive reception its posts have received and the permissible nature of DDW forums, Handala is very likely to continue targeting Israeli organizations with the intent of stealing sensitive information or causing operational disruption.

| Alleged Stealer Logs from Various Government Announced for Sale

On August 17, 2024, threat actor "dk0m" posted in the deep web hacking forum BreachForums, announcing the sale of stealer logs allegedly acquired from the government systems of multiple countries. Dk0m, who has a positive reputation on the forum, claimed that some of the advertised logs contain credentials correlated to specific ministries of the source country. Each country-specific collection is priced at USD 30, though the advertisement specifies that this may vary depending on the size of the log.

Contact me on [Telegram](https://t.me/r0z3na): <https://t.me/r0z3na>

Name	Date modified	Type	Size
 Afghanistan [af]	8/8/2024 1:28 PM	File folder	
 Albania [al]	8/8/2024 1:33 PM	File folder	
 Algeria [dz]	8/8/2024 1:30 PM	File folder	
 Angola [ao]	8/8/2024 1:28 PM	File folder	
 Argentina [ar]	8/8/2024 1:27 PM	File folder	
 Armenia [am]	8/8/2024 1:28 PM	File folder	
 Australia [au]	8/8/2024 1:34 PM	File folder	
 Azerbaijan [az]	8/8/2024 1:28 PM	File folder	
 Bahamas [bs]	8/8/2024 1:31 PM	File folder	
 Bahrain [bh]	8/8/2024 1:27 PM	File folder	
 Bangladesh [bd]	8/8/2024 1:27 PM	File folder	
 Barbados [bb]	8/8/2024 1:28 PM	File folder	

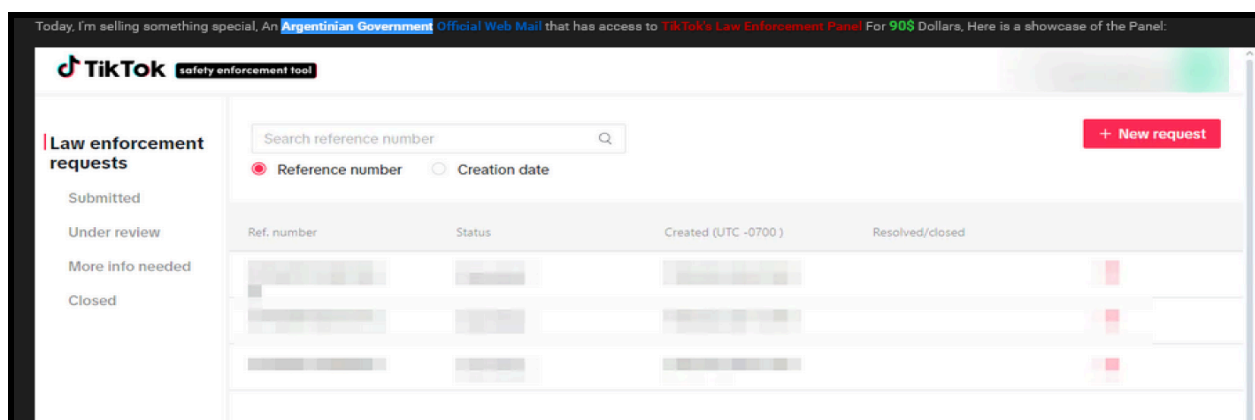
BreachForums post advertising stealer logs

Source: ZeroFox Intelligence

- Stealer logs are compilations of various types of information that have been stolen from devices and networks infected with a strain of malware known as an “infostealer.”
- Typically, stealer logs are composed of information such as URL login and password combinations, personally identifiable information (PII), personal financial information (PFI), network and system information, and web browser data such as cookies and session tokens.

Dk0m likely specializes in the curation and selling of government-related data. The actor has previously been observed selling data allegedly relating to various government entities, including judiciary, law enforcement, and other departments.

- On August 11, 2024, dk0m claimed to be selling credentials associated with the government websites of the United States, Argentina, Ukraine, Brazil, Serbia, Malaysia, and Egypt.
- On August 3, 2024, dk0m claimed to be selling access to an official Argentinian government email service via which potential buyers could allegedly make KODEX (law enforcement) accounts and submit Emergency Data Requests (EDRs) against domains and IP addresses. Such fraudulent requests can likely enable threat actors to illicitly access sensitive data, leading to malicious activity such as enhanced social engineering attacks, impersonation, and fraud.



dk0m advertising access to TikTok's law enforcement (EDR) panel

Source: ZeroFox Intelligence

Dk0m's activities reveal a market demand for government data derived via infostealer logs. This likely indicates governmental data is being included with traditional infostealer-based offerings of gaming, crypto, and social media information. If as advertised, stealer logs such as these can enable threat actors to illicitly obtain personal details and network information, leading to potential further network compromise, digital extortion, or exfiltration of sensitive data.

Sensitive government data obtained from infostealer malware is likely to be of significant interest to a variety of threat actors with motives both ideological and financial.

Adversarial nation-state-backed actors could use such data to deduce confidential and strategic inferences, including military and security intelligence. Actors seeking to conduct election-related cyber operations are likely to use such stolen data to fine-tune their mis-, dis-, and mal-information campaigns. Considering dk0m's past record, the actor is likely to continue advertising government-related data packages for sale. Such activities are very likely to inspire other actors to collect and offer for sale similar data, especially if such advertisements garner significant interest and traction in underground forums.

| High-Profile Seller Receives Praise for Sale of Ransomware Tool

On August 14, 2024, well-regarded actor “Nikazon” announced in the dark web forum RAMP that they are selling the source code of a “locker” for a price of USD 320,000. The thread gained notable traction and very positive feedback from actors such as “Bratislava”, “brothers”, and “Pipe”, all of whom are well-regarded members of the ransomware community and very likely have experience working with either the locker or Nikazon.

- A “locker” very likely refers to a type of malicious software that is primarily intended to block legitimate users from accessing the target system, thereby preventing access to organizational information and disrupting business output. Lockers are less common than other types of ransomware, with many digital extortion outfits instead opting to either encrypt or exfiltrate the victim’s data.

Aug 14, 2024

New < □ #1

Selling the source code of the locker with permanent support in one hand. The software is written in Rust, supports both Windows and Esxi.

Own configuration format with Twofish encryption and serialization. XChaCha12 encryption algorithm with parallelism is used, the key is encrypted each time with ECIES protection (an encryption scheme on elliptic curves). Protection against theft of the key stream is implemented using our own one-time number generator based on the file.

The software is very fast and reliable, has three encryption modes - headeronly mode, smart mode (own algorithm based on hashing the metadata value), full mode.

The software handles errors and memory safety to ensure stability at each startup.

Windows build has the following functionality: encryption of disks and shares, automatic search for shares, asynchronous indexing of files, escalation of access rights to processes to terminate processes and stop services, SMB distribution over the network.

Esxi build - each binary metamorphoses and re-encrypts itself at each launch, deletes snapshots and disables VM, deletes shell history, optional safe self-removal after launch, ignoring most signals that can interrupt the software.

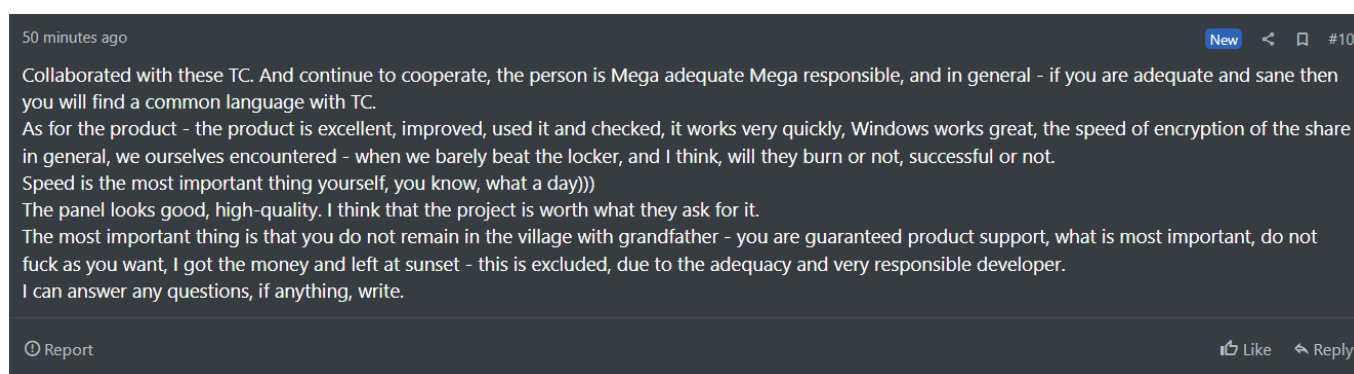
Price: 320k with constant support and any modification/improvement of the software. The price includes the software itself, builder, chat, panel, blog. + also the source code of the locker with chat and panel for toxic access types as a bonus.

Write to Tox: 2D9023EF39515C46F51C06DBDDE38CA080BA9DB0BD2D07CC241BE5A4E7220166959E08E9D48B

RAMP post advertising locker ransomware

Source: ZeroFox Intelligence

Dark web offerings that include ransomware source code are rare. The last notable example ZeroFox observed was in June 2024, when an unspecified ransomware tool that appeared to lack impressive features was advertised in the same forum and sold for USD 50,000. Nikazon's locker, however, allegedly possesses relatively advanced features, such as three encryption modes, encryption of connected storage assets, and privilege escalation to terminate obstructive processes and services. The tool is allegedly written in the Rust language and is designed to attack Windows operating systems, as well as ESXi—a virtual machine software.



RAMP post showcasing positive feedback for Nikazon

Source: ZeroFox Intelligence

The locker will very likely appeal to threat actors involved in digital extortion activities, such as the numerous new ransomware and digital extortion collectives observed quickly gaining traction in 2024. Given that the tool comes complete with permanent support, a payload builder, an admin panel, and a blog—and is bolstered by the positive feedback rarely seen in DDW forums—it is likely that ransomware-as-a-service (RaaS) collectives will consider purchasing the tool to scale their operations. It is very likely that a sale will take place for the approximate price specified.

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 DDW forums.
- Leverage cyber threat intelligence to inform the detection of relevant cyber threats and associated tactics, techniques, and procedures (TTPs).

| 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%