ZEROFOX INTELLIGENCE

Brief

The Underground Economist: Volume 6, Issue 1

B-2026-01-02b

Classification: TLP:CLEAR

Criticality: LOW

Intelligence Requirements: Deep and Dark Web, Threat Actor, Data Breach

January 2, 2026

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 10:30 AM (EST) on January 2, 2026; per cyber hygiene best practices, caution is advised when clicking on any third-party links.

Brief The Underground Economist: Volume 6, Issue 1

One Million Lines of U.S. Bank Logs Advertised on XSS

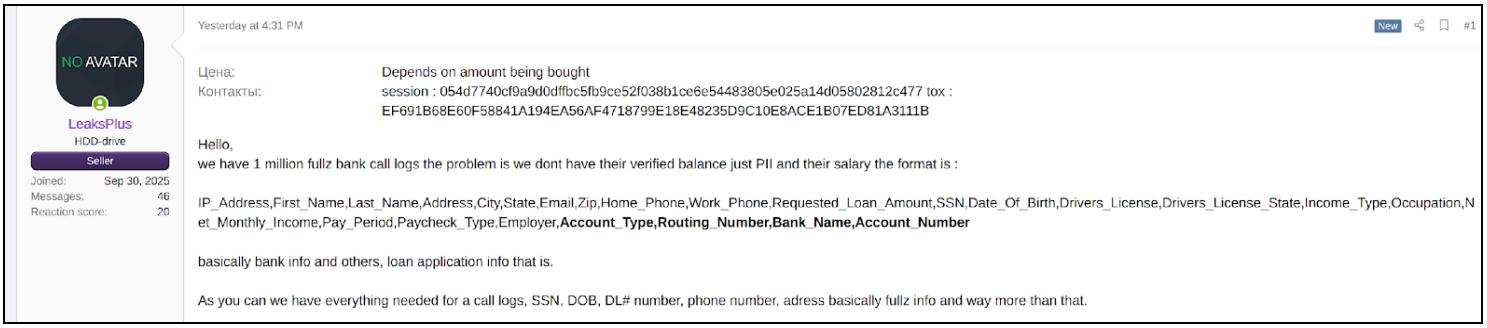
On December 30, 2025, newly registered and positively trending threat actor "LeaksPlus" advertised one million U.S. bank call logs on the primarily Russian-language dark web forum XSS. In the post, the actor specified that the logs contain only personally identifiable information (PII) and that verified account balances are not available.

- The logs allegedly display PII in the following format: IP address, first name, last name, address, city, state, email, ZIP code, home phone number, work phone number, requested loan amount, Social Security number (SSN), date of birth (DOB), driver's license number and state, income type, occupation, net monthly income, pay period, paycheck type, employer, account type, routing number, bank name, and account number.

The actor did not provide a set price for the logs, stating instead that they will determine the price based on how many lines of the data is purchased by the buyer. While LeaksPlus did not disclose the source of this leaked data, the actor included sample data, likely to provide credibility to their claims.

- LeaksPlus joined XSS on September 30, 2025, and has garnered a reaction score of 20. There is a roughly even chance that LeaksPlus's advertisement is legitimate, considering the large quantity of highly sensitive PII.

If the advertisement is legitimate, the information allegedly contained within the logs is rich and highly sensitive; other actors would very likely use this type of information in spear phishing campaigns, loan fraud, spamming, and other malicious activities.

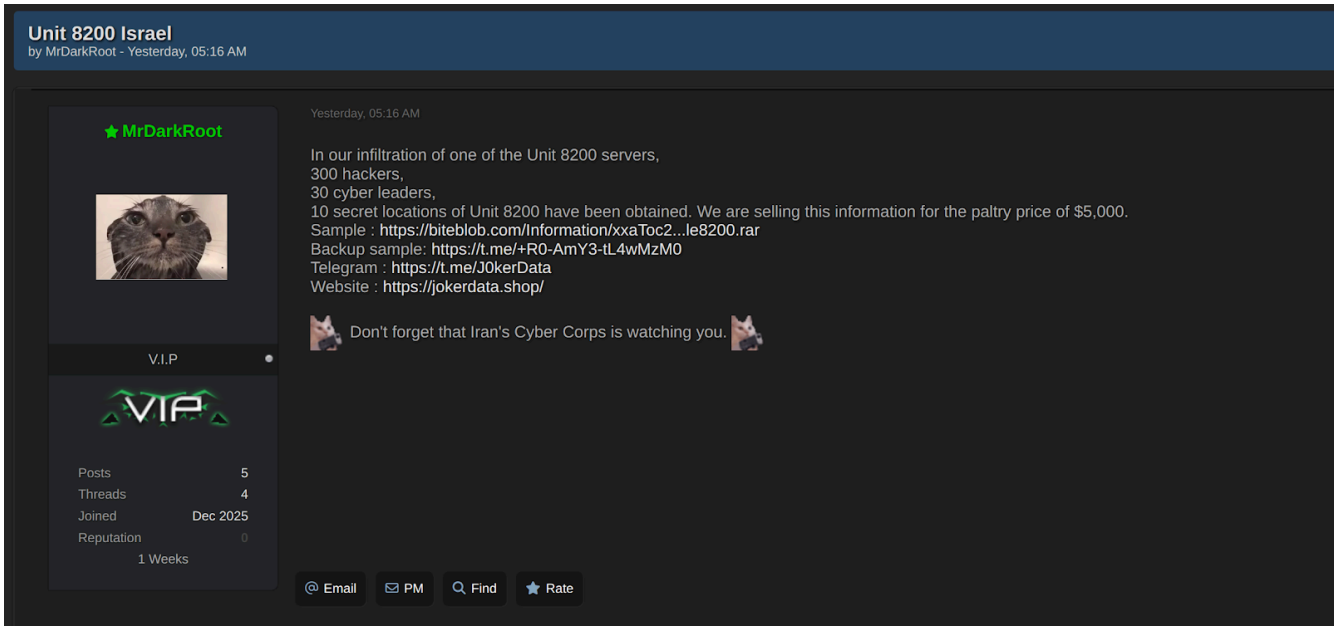


Original post on XSS by LeaksPlus
Source: ZeroFox Intelligence

Israel Defense Forces Intelligence Server Allegedly Compromised

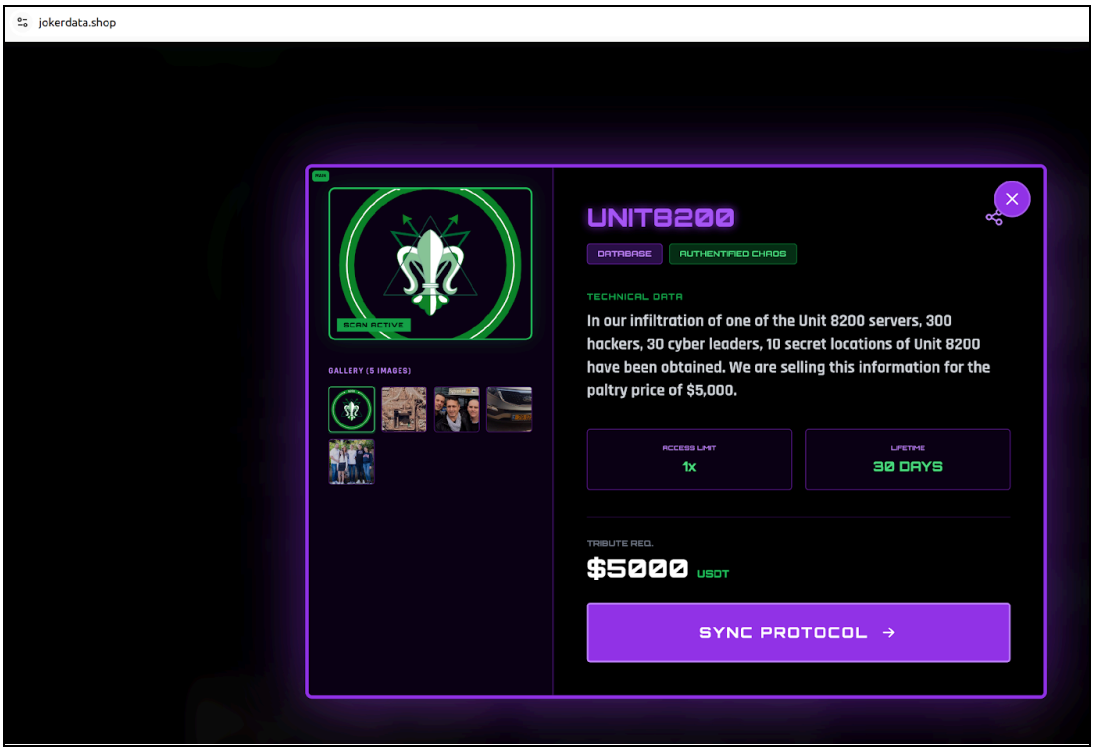
On December 30, 2025, newly registered and unvetted threat actor "MrDarkRoot" advertised access to an Israeli Intelligence Corps unit server of the Israel Defense Forces (IDF) on the deep web forum DarkForums. In the post, the actor claimed to have infiltrated and obtained access to a server belonging to "Unit 8200", with information allegedly pertaining to 300 hackers, 30 cyber leaders, and 10 secret Unit 8200 locations.

- MrDarkRoot provided samples of the allegedly exfiltrated data in their post, which included images of individuals allegedly associated with Unit 8200 and photographs from alleged military base locations.
- The actor advertised the data for USD 5,000 and provided links to their Telegram channel and data store website (jokerdata[.]shop/).



MrDarkRoot's post on DarkForums
Source: ZeroFox Intelligence

MrDarkRoot was first observed on DarkForums in December 2025. As of writing, the actor has at least five posts and zero reputation, and their claims are unlikely to be considered credible by other forum users. Additionally, based on the sample data shared by the actor, the information available does not appear to be highly sensitive. However, the Israeli Intelligence Corps is known to use honeypots to collect information on potential attackers. As of writing, ZeroFox is unable to determine the origin or authenticity of the alleged compromised server.



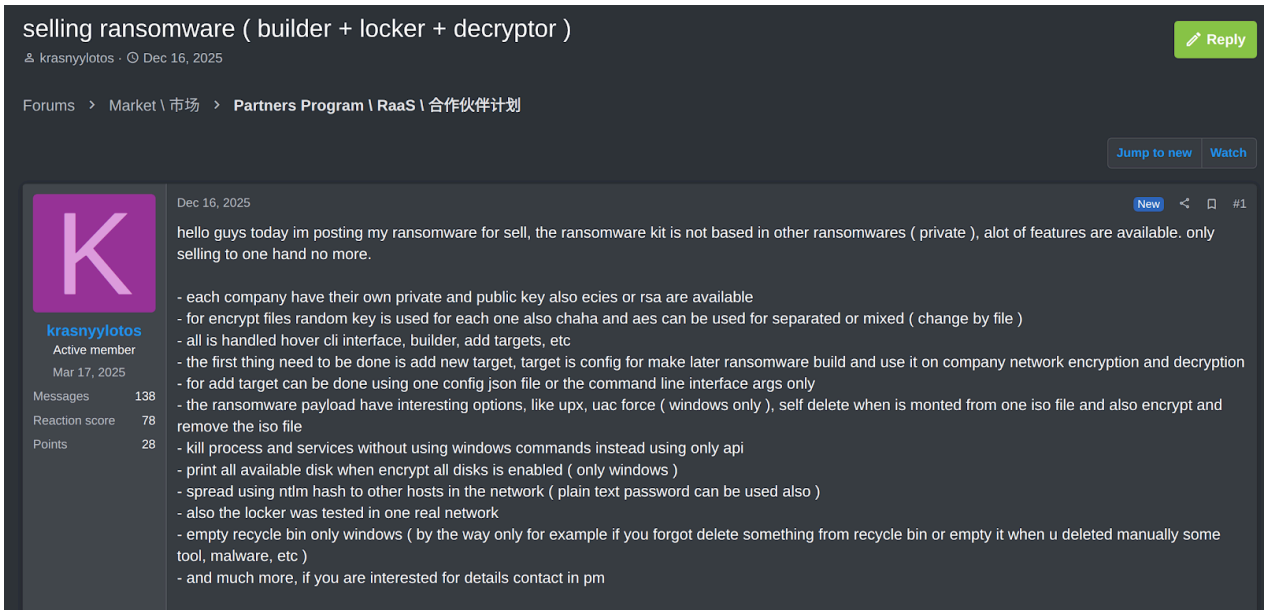
Official advertisement on jokerdata[.]shop
Source: ZeroFox Intelligence

Private and Original Ransomware Project Advertised on Dark Web Forum

On December 16, 2025, well-established actor "krasnyylotos" advertised their private and original ransomware project called HellLotus for USD 2,500–3,000 on the dark web forum Russian Anonymous Marketplace (RAMP). According to the actor, a data leak site (DLS) and an administrative panel are not currently available, and all operations are performed through a command-line interface (CLI).

- Compared to established full ecosystem ransomware operations, this project is likely less competitive due to the lack of a DLS and its CLI-only limitations.
- These limitations require threat actors to be more highly skilled and put in more effort. Additionally, as there is no administrative panel, there is poor potential for scalability, limiting profitability.

- However, the actor claims their ransomware is completely private and original, which likely would contribute to lower initial detection.



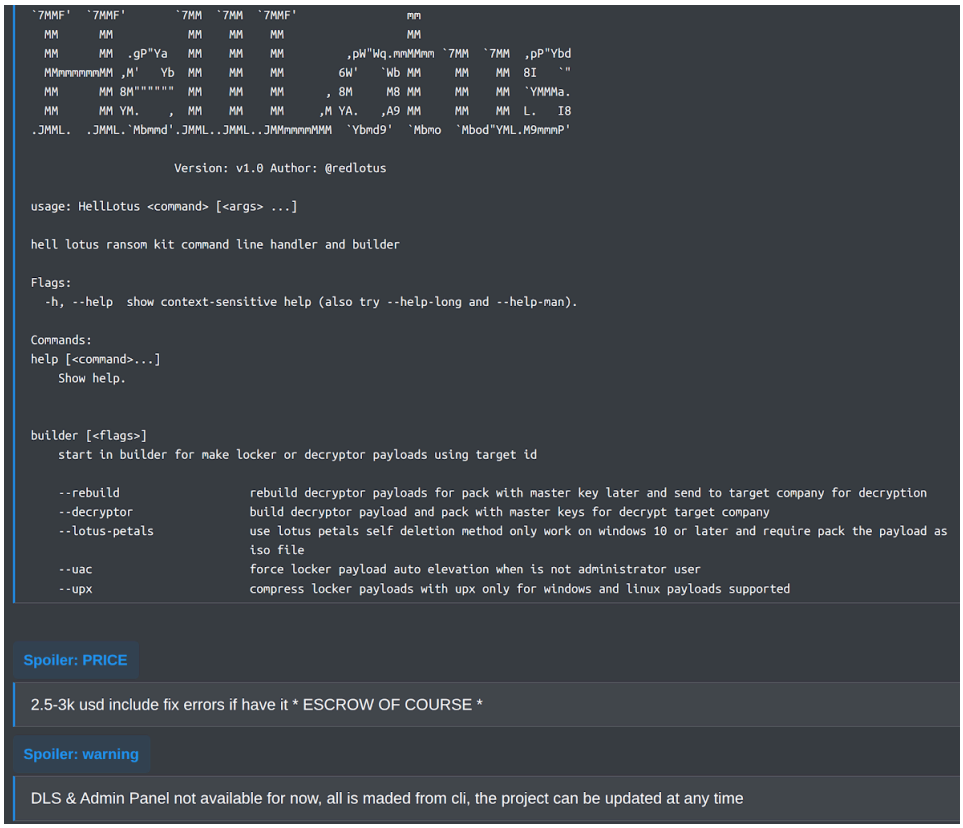
Original post on RAMP by krasnyylotos

Source: ZeroFox Intelligence

The actor provided a list of features allegedly available on HellLotus, which is as follows:

- **Per-organization cryptographic keys:** Each targeted organization is assigned unique public or private key pairs supporting Elliptic Curve Integrated Encryption Scheme (ECIES) or Rivest-Shamir-Adleman (RSA), enabling isolated encryption domains per victim.
- **Per-file symmetric encryption:** Individual files are encrypted using randomly generated keys, with support for ChaCha, Advanced Encryption Standard (AES), or combined usage, allowing flexible cryptographic configurations.
- **CLI-based management architecture:** All functionality—including payload building and target configuration—is handled through a CLI, with no graphical management panel.
- **Target-based deployment model:** Operations are organized around "targets," which define configuration parameters used to generate ransomware builds and control encryption or decryption behavior within a specific network.

- **Flexible target configuration input:** Targets can be defined either through structured JSON configuration files or directly via command-line arguments.
- **Payload customization options:** The ransomware supports optional features such as executable packing, privilege escalation bypass on Windows, self-deletion when executed from ISO media, and encryption or removal of ISO files.
- **System control and disk handling (Windows):** Processes and services are terminated via direct Application Programming Interface (API) calls, full disk encryption can enumerate all available drives, and the recycle bin can be emptied to limit recovery options.
- **Lateral movement capability:** The ransomware supports network propagation using NT LAN Manager (NTLM) hashes or plaintext credentials to access additional hosts.
- **Operational maturity claim:** The seller claims the locker has been tested in a real network environment, indicating basic functional validation.



```
`7MMF'  `7MMF'       `7MM  `7MM  `7MMF'              mm
  MM      MM           MM    MM    MM                MM
  MM      MM  ,gP"Ya   MM    MM    MM         ,pW"Wq.mmMMmm `7MM  `7MM  ,pP"Ybd
  MMmmmmmMM ,M'   Yb  MM    MM    MM        6W'   `Wb MM     MM    MM  8I   `"
  MM      MM 8M""""""  MM    MM    MM      , 8M     M8 MM     MM    MM  `YMMMa.
  MM      MM YM.    ,  MM    MM    MM     ,M YA.   ,A9 MM     MM    MM  L.   I8
.JMML.  .JMML.`Mbmmd'.JMML..JMML..JMMmmmmMMM  `Ybmd9'  `Mbmo  `Mbod"YML.M9mmmP'

                    Version: v1.0 Author: @redlotus

usage: HellLotus <command> [<args> ...]

hell lotus ransom kit command line handler and builder

Flags:
  -h, --help  show context-sensitive help (also try --help-long and --help-man).

Commands:
help [<command>...]
    Show help.


builder [<flags>]
    start in builder for make locker or decryptor payloads using target id

    --rebuild                 rebuild decryptor payloads for pack with master key later and send to target company for decryption
    --decryptor               build decryptor payload and pack with master keys for decrypt target company
    --lotus-petals            use lotus petals self deletion method only work on windows 10 or later and require pack the payload as
                              iso file
    --uac                     force locker payload auto elevation when is not administrator user
    --upx                     compress locker payloads with upx only for windows and linux payloads supported
```

Spoiler: PRICE

2.5-3k usd include fix errors if have it * ESCROW OF COURSE *

Spoiler: warning

DLS & Admin Panel not available for now, all is maded from cli, the project can be updated at any time

Original post on RAMP by krasnyylotos (Part 2)

Source: ZeroFox Intelligence

Overall, the ransomware does not significantly differentiate itself from other ransomware projects. However, it includes some specific functionalities related to payload, such as automatically deleting itself when mounted from an ISO file, as well as encrypting and removing the ISO. The asking price for the services allegedly offered is likely considered reasonable, especially considering krasnyylotos's established credibility on RAMP. As of writing, the ransomware project has not yet been sold.

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 multi-factor authentication (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 (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%