ZEROFOX INTELLIGENCE

Brief

The Underground Economist: Volume 6, Issue 10

B-2026-05-07b

Classification: TLP:CLEAR

Criticality: LOW

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

May 7, 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 7:00 AM (EDT) on May 7, 2026; per cyber hygiene best practices, caution is advised when clicking on any third-party links.

| Brief | The Underground Economist: Volume 6, Issue 10

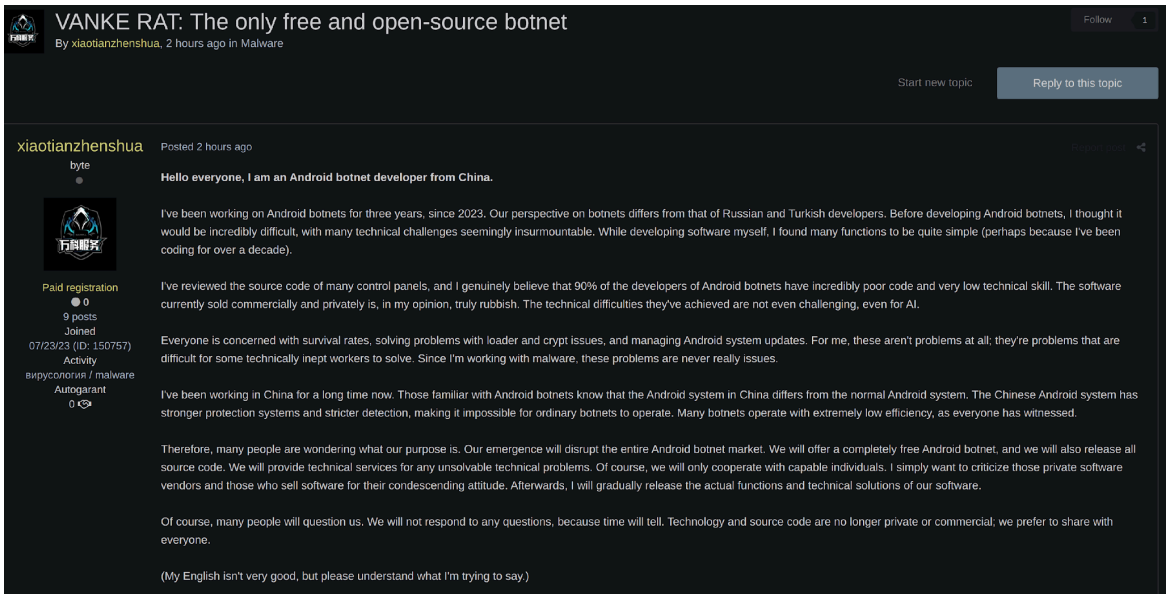
| Chinese Android Botnet VANKE RAT

On May 5, 2026, a moderately credible actor on the Exploit forum using the alias "xiaotianzhenshua" announced the development of an Android botnet named VANKE RAT, which the actor claims will be the first free and open-source Android bot. As justification for making the software freely available, the actor cited dissatisfaction with the practices and attitudes of other Android malware developers operating on deep and dark web (DDW) forums.

- Xiaotianzhenshua claims to have reviewed the source code of numerous botnet control panels and assesses that approximately 90 percent of Android botnet developers lack sufficient technical expertise, resulting in poorly written code.
- The actor emphasized that Chinese Android systems differ significantly from standard Android environments and feature stronger protections and stricter detection mechanisms, which allegedly prevent less advanced botnets from operating effectively.

The actor is reportedly sharing details regarding VANKE RAT, including the source code, via private communication channels. However, ZeroFox's analysis of the botnet dashboard indicates that configurations for targeting at least 12 major U.S. banking and payment apps—including Wells Fargo, Chase, Bank of America, Citi Mobile, U.S. Bank,

Truist, TD Bank, American Express, Citizens Bank, USAA, Capital One, and PNC—are already built-in.



xiaotianzhenshua's original post on Exploit

Source: ZeroFox Intelligence

Although the malware remains untested, xiaotianzhenshua's offering will very likely have a significant impact on the Android botnet ecosystem. There will almost certainly be an increase in attacks against Android users, particularly in the United States. VANKE RAT is very likely designed to steal credentials, hijack sessions, and intercept calls and SMS messages, enabling unauthorized access to victims' financial accounts; thus, a marked increase in such attacks on Android users is very likely.

ShinyHunters Offers Vercel Inc. Data for Sale

On April 25, 2026, the threat actor group ShinyHunters announced an alleged data breach of Vercel Inc. (Vercel) for sale on BreachForums for an initial asking price of USD 1 million. The group stated they contacted Vercel on April 19, 2026, and shared a sample of the allegedly breached data with the company.

- Vercel is an American cloud computing company that provides a platform for instant web application development, hosting, and deployment. The company is

widely known as the creator and maintainer of Next.js, one of the most popular web development frameworks.

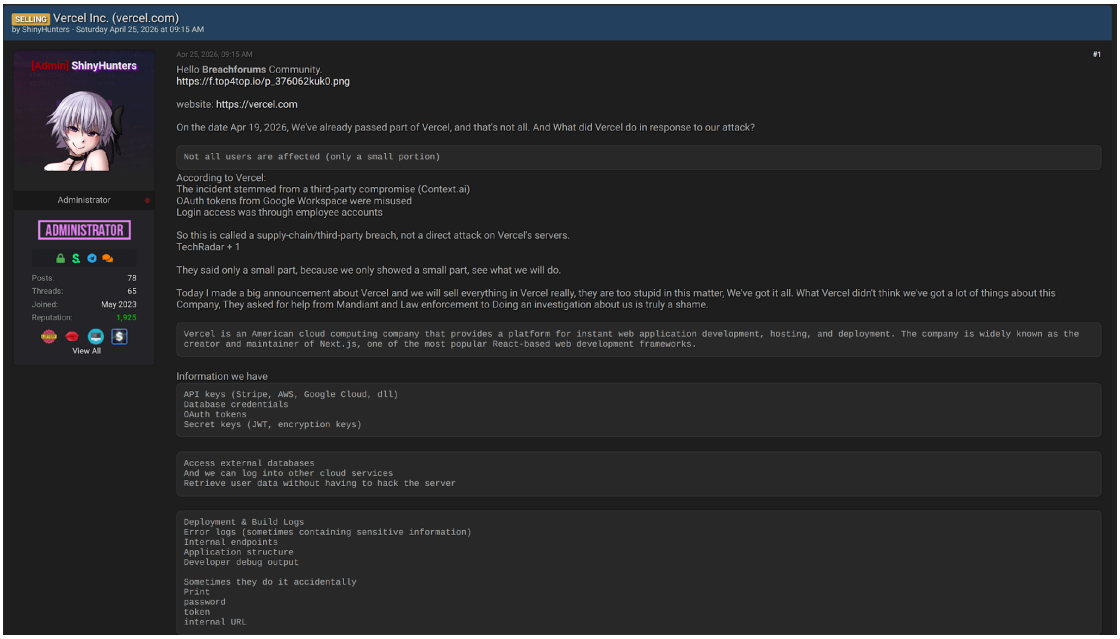
Vercel reportedly responded by claiming the breach affected only a small portion of its users. According to ShinyHunters, the breached data grants access to extensive internal assets, which the group likely believes justifies the high asking price.

ShinyHunters claims to have access to several key elements of Vercel's network infrastructure, including:

- API keys for access to Stripe, Amazon Web Services, and Google Cloud
- External databases (including a claim they are able to access Vercel's cloud services "without having to hack the server")
- Deployment and build logs (including error logs that may contain sensitive information, internal endpoints, and debug output)

Additionally, ShinyHunters allegedly has access to Vercel's internal project lists and associated data, which likely includes personally identifiable information (PII) for Vercel employees.

The sample data ShinyHunters provided is very likely legitimate and has not appeared in previous breaches. This is likely the largest data breach thus far in 2026; given the number of companies that rely on Vercel's cloud infrastructure and services, the impact of this breach will almost certainly be extensive. Additionally, the risk of follow-on attacks and breaches for Vercel end users is very likely to be elevated.

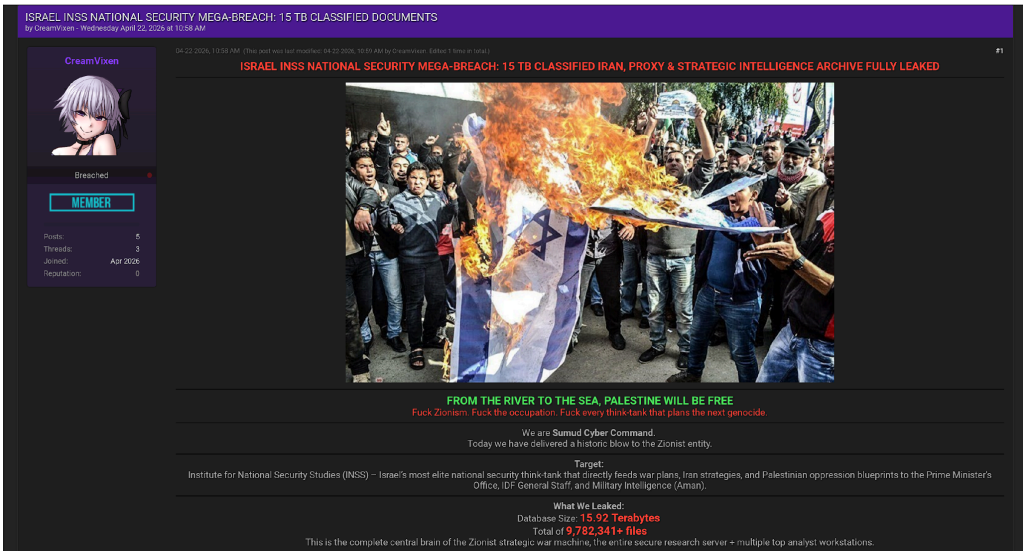


ShinyHunters' post on BreachForums

Source: ZeroFox Intelligence

CreamVixen Advertises Stolen Data from Israel's Institute for National Security Studies

On April 22, 2026, untested, pro-Palestinian threat actor "CreamVixen" advertised a 15.92 TB database of documents associated with Israel's Institute for National Security Studies (INSS) on the dark web forum PwnForums for USD 800. Several PwnForum users expressed interest in the post, but thus far there have been no indications a sale has occurred.

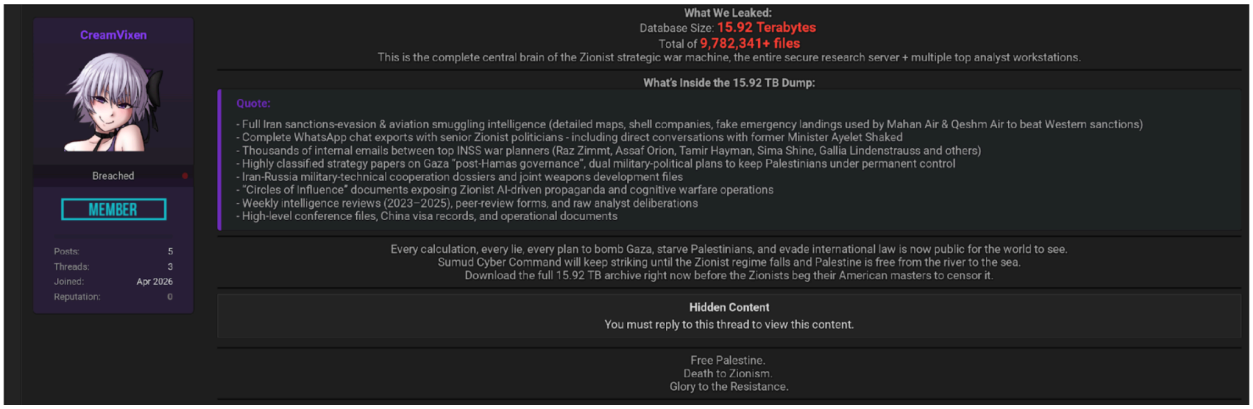


CreamVixen's post on PwnForums

Source: ZeroFox Intelligence

According to CreamVixen, the database was allegedly exfiltrated from a secure research server and includes data from multiple analyst workstations. The alleged dataset, which consists of over nine million files, reportedly contains a broad mix of intelligence, policy, and internal communications data, as well as:

- Sanctions-evasion and smuggling intelligence tied to Iranian aviation, private communications with officials, internal emails and analyses from think-tank and military-linked experts, and classified strategy papers on Gaza governance
- Internal emails between top INSS members (Raz Zimmt, Assaf Orion, Tamir Hayman, Sima Shine, Gallia Lindenstrauss, and others)
- Iran–Russia military cooperation files, "cognitive warfare", and propaganda-related documents



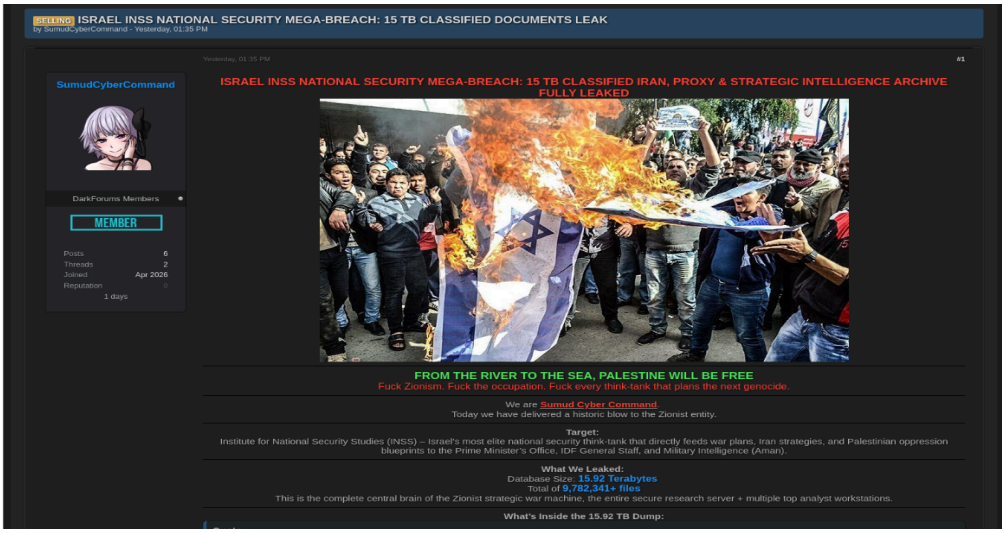
CreamVixen's claim about the contents of the database

Source: ZeroFox Intelligence

In recent months, ZeroFox has observed several other posts on DDW forums specifically targeting INSS. This is likely a result of the U.S./Israel war with Iran, which began on February 28, 2026.

- On April 20, 2026, untested actor "SumudCyberCommand" also advertised a 15.92 TB dataset allegedly stolen from INSS on DarkForums, offering it for USD 800.[1]
- On March 5, 2026, pro-Iran hacktivist group Handala Hack Team alleged on its leak site to have prolonged access to INSS' internal systems and to have monitored high-level discussions. The group claimed it had obtained classified documents, communications, and recordings.[2]

[1] https://cloud.zerofox.com/intelligence/advanced_dark_web/103295
[2] https://cloud.zerofox.com/intelligence/advanced_dark_web/101069



SumudCyberCommand's post on DarkForums

Source: ZeroFox Intelligence

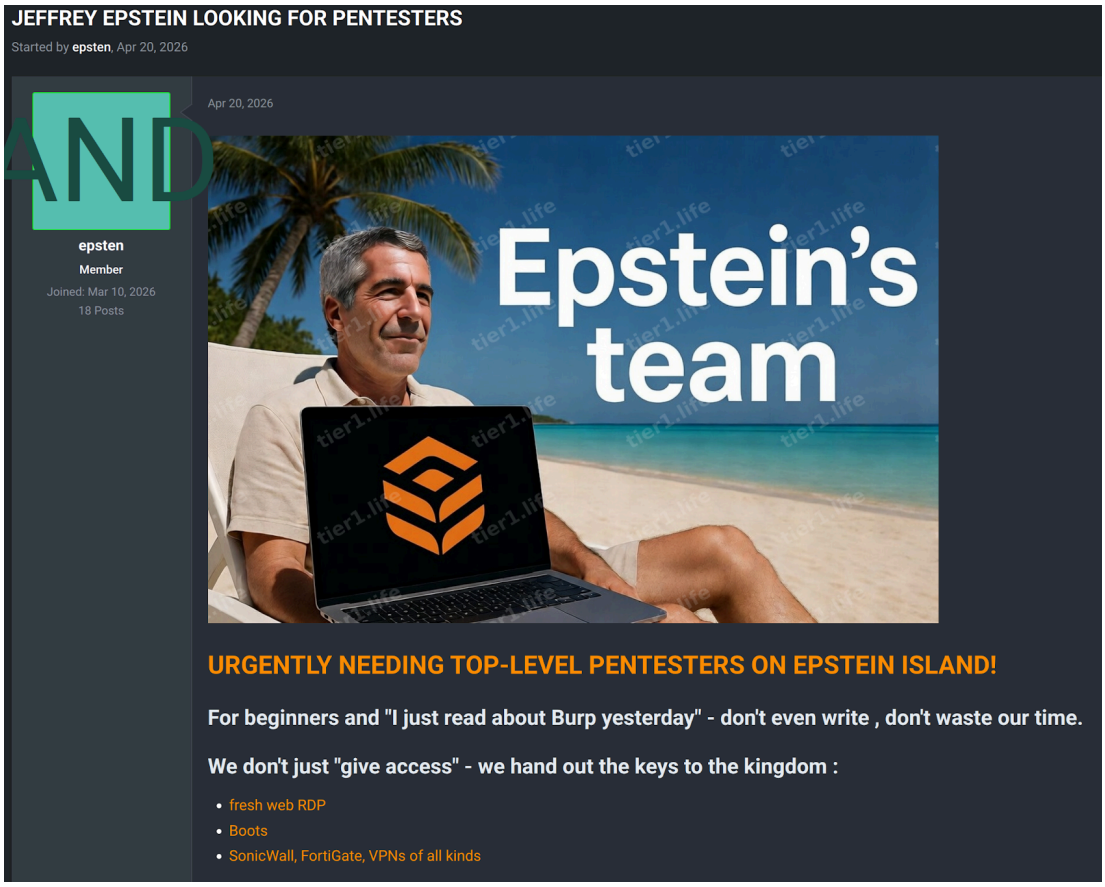
The body of CreamVixen's advertisement on PwnForums contains the statement, "We are SumudCyberCommand. Today we have delivered a historic blow to the Zionist entity," likely indicating the content has been copied or repurposed from SumudCyberCommand's original advertisement.

Moreover, the advertised price of USD 800 is notably low for a dataset of this claimed scale and sensitivity. If authentic, the combination of cross-posting by multiple actors and low pricing likely indicates an effort to increase uptake, amplify impact, and broaden the potential exploitation of the data.

Threat Collective Appeals for Pentesters

On April 20, 2026, a newly registered and untested threat actor using the alias "epsten" posted on the private-access dark web forum TierOne, seeking experienced pentesters. The actor claimed to be able to provide everything needed for skilled pentesters to achieve persistent access to multiple targets and provided a Tox ID for potential affiliates to get in contact.

- Epsten joined TierOne on March 10, 2026, and has contributed 18 posts on the forum as of the time of writing. Epsten frequently uses "we" in their posts, which is almost certainly indicative of a threat collective rather than a single threat actor.



epsten's original post on TierOne

Source: ZeroFox Intelligence

In the original post, epsten noted that they charge either a fixed rate for their services or a percentage of proceeds from what they refer to as the "full cycle", which the actor describes as revenue derived from data extortion, cyber espionage, or ransomware operations. The actor stated that they are interested in obtaining initial access to entities located in Germany, Switzerland, the United States, Austria, and Canada.

- Epsten highlighted a particular focus on U.S. healthcare organizations. While ransomware actors typically avoid targeting healthcare providers due to informal ethical norms within the cybercrime ecosystem, this group appears to be an exception to the rule.
- On April 22, 2026, epsten published a follow-up post providing additional details about their services, including the following pricing structures for different

accesses. Affiliates would allegedly receive up to 25 percent per user domain, up to 30 percent for local admin access, and up to 40 percent for admin domains based on the revenue derived from data extortion, cyber espionage, or ransomware operations.

Epsten alleges that they can supply fresh remote desktop protocol (RDP) access, bots, and SonicWall and FortiGate devices, as well as various types of VPN credentials. Epsten further claims to assist experienced attackers by sharing access, techniques, and private exploits. If the claims made by epsten are true, it would signify a relatively sophisticated and professional operation by this new threat collective.

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 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%

Appendix C: ZeroFox Intelligence Threat Actor Reputation Scale

Untested	Moderately Credible	Well-regarded	Prominent
Has garnered no reputation; credibility cannot be determined.	Has made up to 10 transactions; has been active on forum for at least three months.	Has at least 10 transactions; has been active on forum for three months to one year.	One of the most well-known and credible threat actors on the site; long-term, established presence on the forum of more than one year.