ZEROFOX INTELLIGENCE

Brief

The Underground Economist: Volume 6, Issue 16

B-2026-07-30b

Classification: TLP:CLEAR

Criticality: LOW

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

July 30, 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 July 30, 2026; per cyber hygiene best practices, caution is advised when clicking on any third-party links.

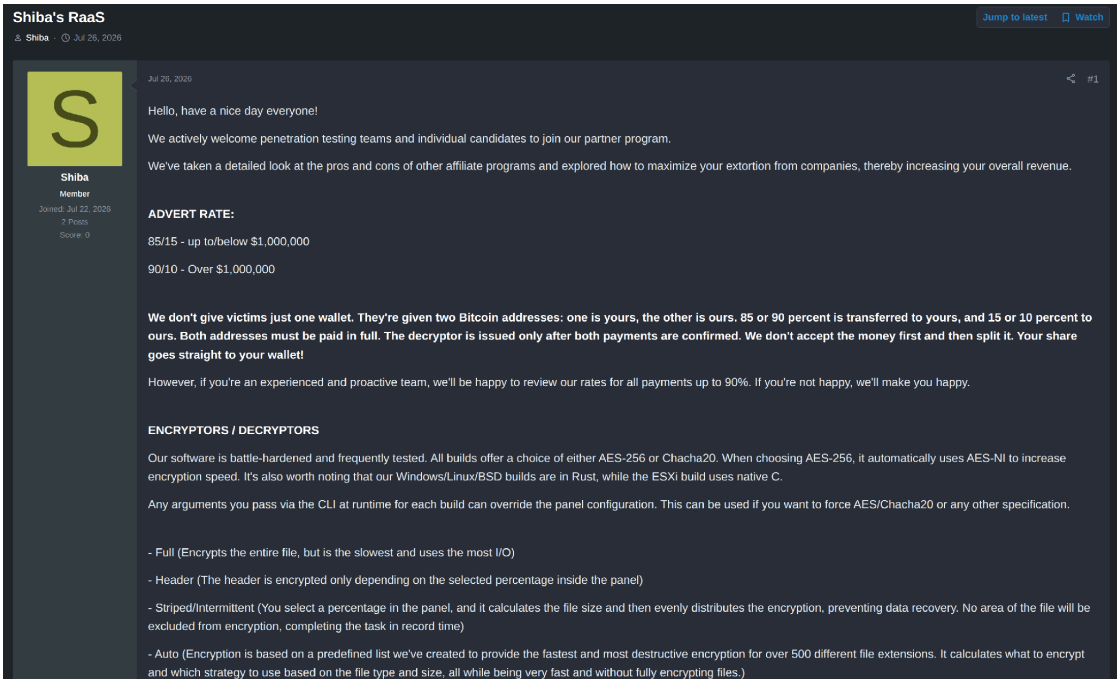
| Brief | The Underground Economist: Volume 6, Issue 16

| New Ransomware Affiliate Program

On July 26, 2026, untested threat actor "Shiba" announced the launch of a new ransomware-as-a-service (RaaS) affiliate program on the private-access dark web forum T1erOne. The actor is actively recruiting experienced penetration testing teams, initial access brokers (IABs), and intrusion operators to participate in the operation.

The advertisement promotes a business model offering 85–90 percent of ransom proceeds to affiliates through direct cryptocurrency wallet splitting—a mechanism likely intended to reduce reliance on operator trust. According to Shiba, the ransomware framework includes cross-platform encryptors supporting Windows, Linux, and VMware, among other environments. The RaaS platform also allegedly includes:

- Multiple encryption modes
- Configurable payload generation
- Automated test decryption
- Comprehensive victim management features
- An integrated data leak site with searchable indexing designed to increase extortion pressure



Shiba's post on TierOne
Source: ZeroFox Intelligence

The program prohibits attacks against organizations located in Commonwealth of Independent States (CIS) countries, suggesting the threat actor is very likely a Russian speaker residing in a CIS nation. The actor explicitly stated that attacks against sectors such as healthcare, education, and local government are permitted and encouraged affiliates to demand ransoms of no less than USD 50,000.

This announcement almost certainly marks the emergence of another ransomware operation seeking to rapidly establish an affiliate network by combining a competitive revenue-sharing model with mature tooling and broad targeting flexibility. If Shiba successfully recruits experienced affiliates, the operation will likely increase the volume and sophistication of ransomware attacks affecting organizations across multiple sectors.

ZeroFox assesses that the group's willingness to target hospitals, schools, and public sector entities very likely suggests a comparatively aggressive operating model with limited self-imposed restrictions.

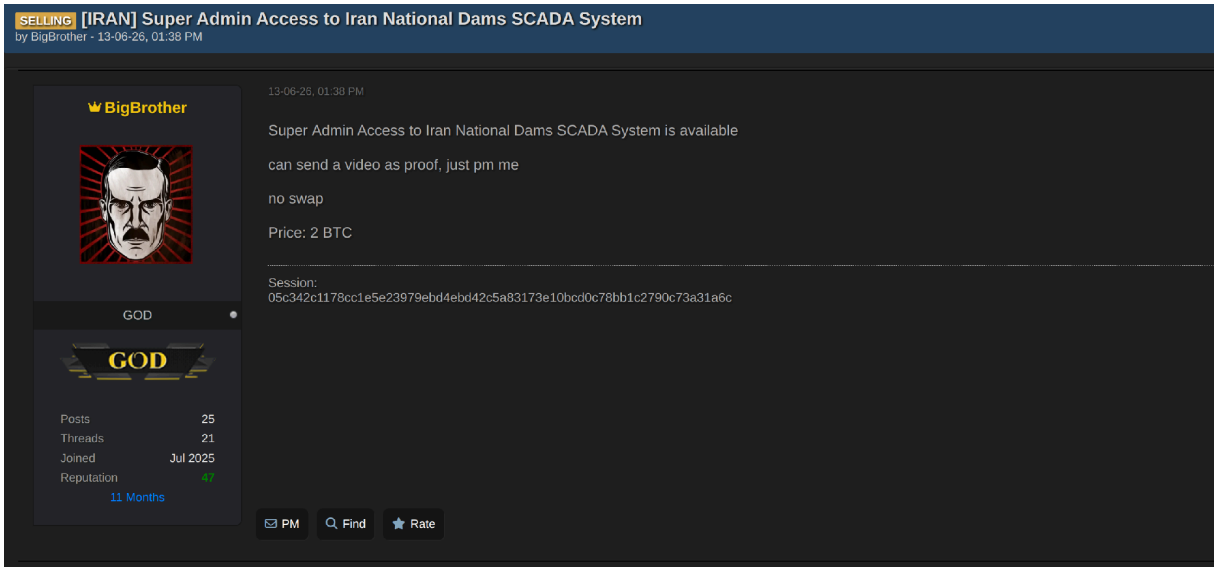
Privileged Access to Iranian National Dams' SCADA System Remains Available on DarkForums

On July 20, 2026, well-regarded threat actor "BigBrother" confirmed on the dark web forum DarkForums that their alleged super administrator access to Iran's National Dams' Supervisory Control and Data Acquisition (SCADA) system remained available for purchase. The actor originally advertised the access on June 13, 2026, signifying over a month on the forum without a buyer.

- BigBrother priced the access at 2 BTC (approximately USD 120,000, as of writing) and offered to provide a video demonstrating the claimed access as proof to prospective buyers.
- ZeroFox assesses that the actor's asking price is unusually high, given the uncertainty surrounding the longevity and validity of privileged access to operational technology (OT) environments.

BigBrother has been a member of DarkForums since at least July 2025; they have made 25 posts within the last year and garnered an overall positive reputation score. As of writing, ZeroFox is unable to confirm the credibility of the actor's claims; however, other forum users likely find this offer to be less credible or desirable, considering it remains unsold and the post lacks public screenshots showing proof of access.

If the actor's claims are genuine, privileged access to the National Dams' SCADA system is likely to enable malicious actors to manipulate or disrupt critical water infrastructure, likely resulting in significant operational, economic, environmental, or public safety consequences. Given the heightened geopolitical tensions involving Iran, Israel, and the United States, such access is very likely to increase the risk of cyber-enabled sabotage or false-flag operations, with the possibility of malicious activity against Iranian critical infrastructure being misattributed and contributing to further regional escalation.



BigBrother's post on DarkForums
Source: ZeroFox Intelligence

Dossiers of U.S. Political Figures Published

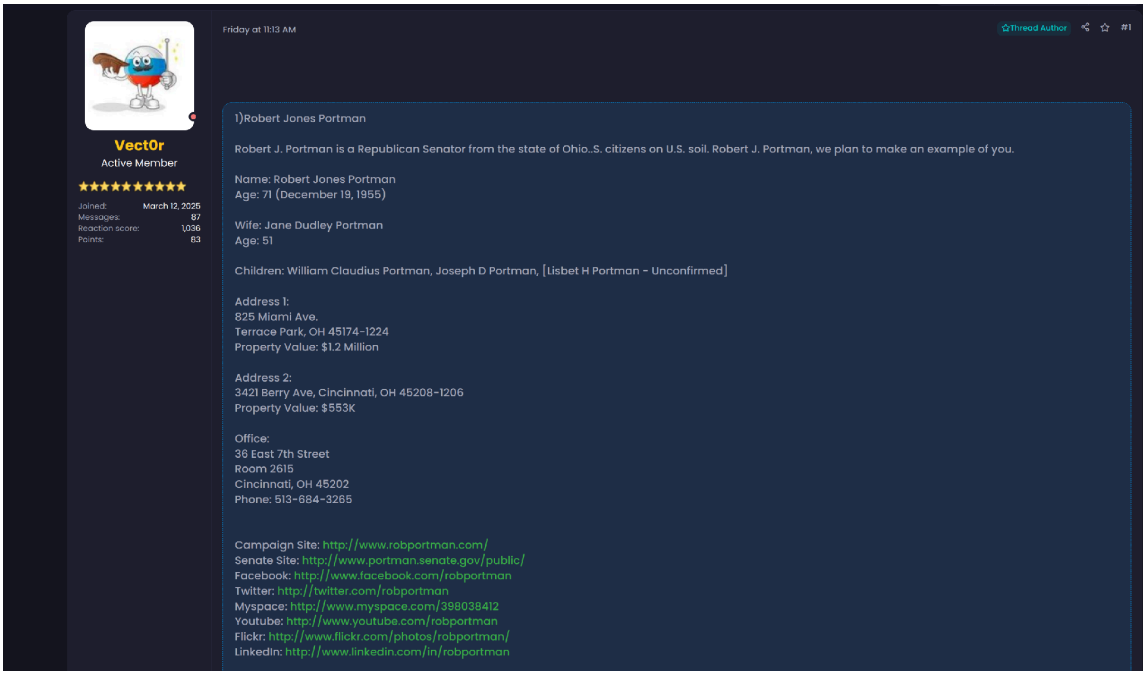
On July 17, 2026, well-regarded threat actor "Vect0r" published a free collection of dossiers containing personal information related to numerous current and former U.S. political figures on the dark web forum DarkNetArmy. The dossiers pertain to senators, congressional representatives, governors, committee leaders, chiefs of staff, and other governmental personnel; the actor also claimed to possess information related to certain family members of the listed individuals.

- The published dossiers contain varying levels of personal information, including dates of birth, social media profiles, personal telephone numbers, email addresses, residential addresses, educational background, investment-related information, and details concerning family members.
- The actor notably did not claim that the disclosed information resulted from a compromise of U.S. government systems or disclose any motivation for releasing the information.

ZeroFox assesses that a substantial portion of the disclosed information very likely originates from publicly available sources and open-source intelligence (OSINT) rather than a recent data breach or unauthorized compromise. Consequently, the publication

does not currently indicate a significant exposure of non-public government information; however, the aggregation of personal data into readily accessible dossiers likely lowers the barrier for malicious actors seeking to conduct targeted social engineering, spear phishing, harassment, impersonation, doxxing, or other influence operations against the affected individuals.

- The post demonstrates continued interest within underground communities in collecting and disseminating detailed information pertaining to high-profile public officials.



Vect0r's post on DarkNetArmy
Source: ZeroFox Intelligence

Threat Actor Advertises eSIM-Generating Capability on Exploit

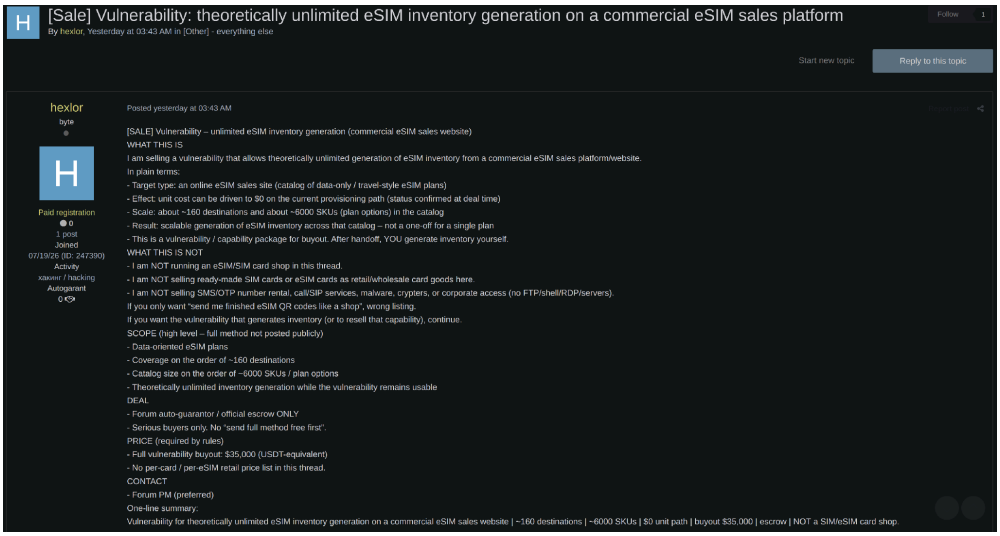
On July 15, 2026, untested threat actor "Hexlor" advertised on the dark web forum Exploit a vulnerability that "allows theoretically unlimited" generation of eSIM inventory from a commercial eSIM sales platform, spanning approximately 160 destinations and 6,000

stock keeping units (SKUs). The actor has priced the vulnerability at USD 35,000, with transactions restricted to forum escrow/guarantor services.

- Hexlor joined the Exploit forum on July 19, 2026.
- As of writing, the post has not garnered any public replies from other forum members.

Notably, eSIM provisioning platforms manage the digital issuance of mobile connectivity plans at scale, very likely making a flaw in their inventory or provisioning workflow a high-value target for fraud operators and those seeking anonymous communications infrastructure.

- As of writing, no eSIM providers or news organizations have publicly confirmed the existence of such a vulnerability.



Hexlor's advertisement on Exploit

Source: ZeroFox Intelligence

In the advertisement, Hexlor described the offering as a one-time "vulnerability/capability package" transfer rather than a retail eSIM service, claiming buyers would receive the method needed to generate inventory themselves after handoff rather than obtaining pre-made eSIMs or access to an ongoing service relationship. The seller stated that the capability targets online data-only/ travel eSIM catalogs.

ZeroFox assesses that prospective buyers likely view the advertisement as less credible due to the lack of concrete details about the platform and the alleged vulnerability, as well as the relatively high asking price of USD 35,000. Hexlor is likely attempting to market the offering as a high-value exclusive capability, but the claims remain unverified and likely include promotional or exaggerated elements intended to attract interest.

- ZeroFox is unable to confirm the credibility of Hexlor's claims, as the actor has not provided any samples or a demo to prove the functioning of this tool.
- Hexlor has not provided any additional details about the platform or the geographical limits of this alleged eSIM inventory-generating vulnerability.

Hexlor claims they are not selling ready-made eSIMs, SIM cards, SMS services, malware, or stolen company access, likely suggesting this is not a stolen or otherwise compromised account or product. Instead, the claim is that a flaw in the eSIM provider's online ordering or activation system could let a buyer generate many travel data eSIMs themselves without normal payment or inventory checks.

If genuine, ZeroFox assesses that the claimed capability is likely to have meaningful operational implications and risk of fraud for the affected eSIM provider and downstream mobile network operators.

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%

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.