ZEROFOX INTELLIGENCE

Brief

The Underground Economist: Volume 6, Issue 3

B-2026-01-29b

Classification: TLP:CLEAR

Criticality: LOW

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

January 29, 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 (EST) on January 29, 2026; per cyber hygiene best practices, caution is advised when clicking on any third-party links.

| Brief | The Underground Economist: Volume 6, Issue 3

| FBI Seizes Dark Web Forum RAMP

On January 28, 2026, the Federal Bureau of Investigation (FBI) seized dark web forum RAMP in a coordinated action with the U.S. Attorney's Office for the Southern District of Florida and the Department of Justice.

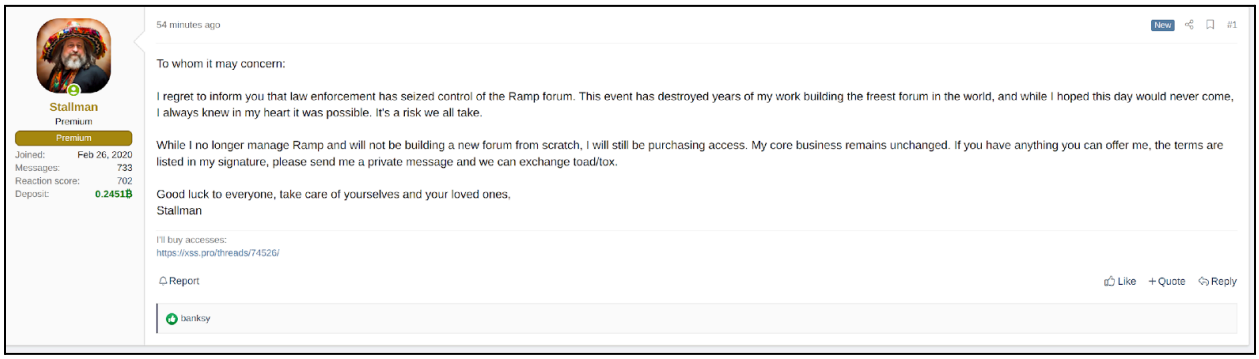
- RAMP had been active since 2021, and numerous ransomware groups (including Qilin, LockBit, DragonForce, RansomHub, and ALPHV/BlackCat) promoted their Ransomware-as-a-Service (RaaS) operations there, making it one of the most popular forums among RaaS collectives.
- The RAMP forum was the only known dark web forum where RaaS activities were explicitly permitted.
- While there has been no confirmation from U.S. law enforcement, RAMP's domain name servers have been changed to those typically used by the FBI when seizing domains.[1] The FBI likely has access to personal details associated with RAMP users—including RaaS operators that failed to practice strong operational security measures.

[1] hXXps://www.bleepingcomputer[.]com/news/security/fbi-seizes-ramp-cybercrime-forum-used-by-ransomware-gangs/

Seizure banner on RAMP

Source: ZeroFox Intelligence

The seizure was subsequently confirmed by RAMP's administrator, "Stallman", who posted about it on the dark web forum XSS and stated that he would not create a successor forum. However, Stallman indicated that he would continue purchasing initial network access to large organizations for ransomware and other illicit activities.

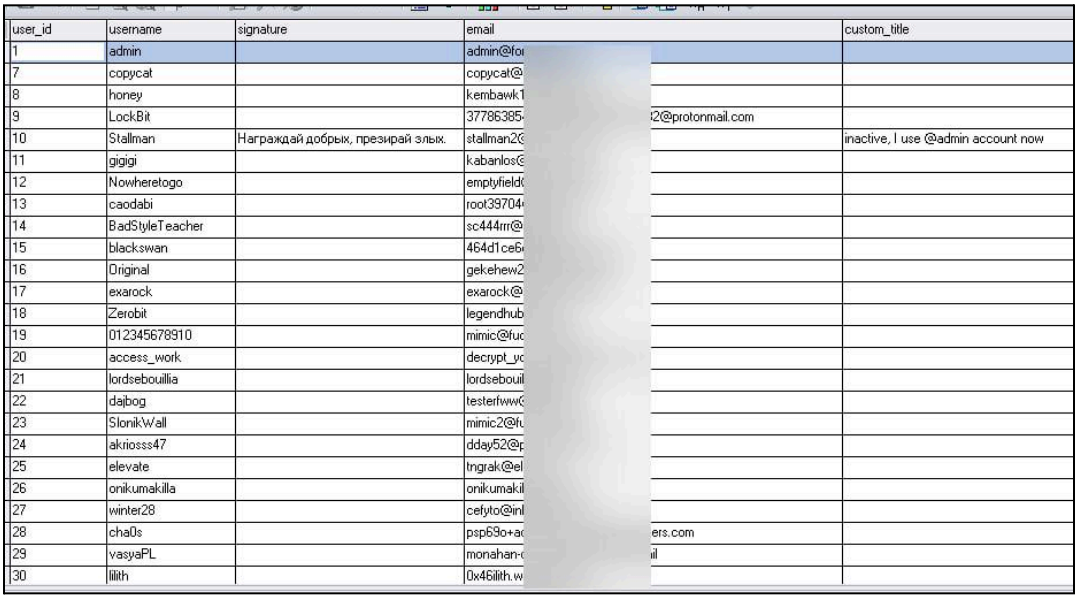


Stallman's XSS post

Source: ZeroFox Intelligence

Shortly after news of the seizure broke, screenshots from a suspected leaked RAMP database appeared in a Telegram channel. The screenshots show partially blurred user email addresses, including an email address allegedly used during forum registration by well-known RaaS operator LockBit. The screenshots also contain private messages exchanged between forum users.

- The source of the Telegram leak remains unconfirmed; however, if the leaked information is verified, it is likely to lead to further deanonymization of multiple threat actor groups. That being said, it is highly likely that law enforcement already has control over the forum's database and infrastructure.



user_id	username	signature	email	custom_title
1	admin		admin@fo	
7	copycat		copycat@	
8	honey		kembawk1	
9	LockBit		37786385	2@protonmail.com
10	Stallman	Награждай добрых, презирай злых.	stallman2	inactive, I use @admin account now
11	gigigi		kabanlos@	
12	Nowheretogo		emptyfield	
13	caodabi		root39704	
14	BadStyleTeacher		sc444rrr@	
15	blackswan		464d1ce6	
16	Original		gekehew2	
17	exarock		exarock@	
18	Zerobit		legendhub	
19	012345678910		mimic@fuc	
20	access_work		decrypt_yc	
21	lordsebouillia		lordsebouil	
22	dajbog		testerfww	
23	SlonikWall		mimic2@fu	
24	akriosss47		dday52@p	
25	elevate		tngrak@el	
26	onikumakilla		onikumakil	
27	winter28		cefyto@inl	
28	cha0s		psp69o+ac	ers.com
29	vasyaPL		monahan-	il
30	lilith		0x46lilith.w	

Telegram screenshot of RAMP database

Source: ZeroFox Intelligence

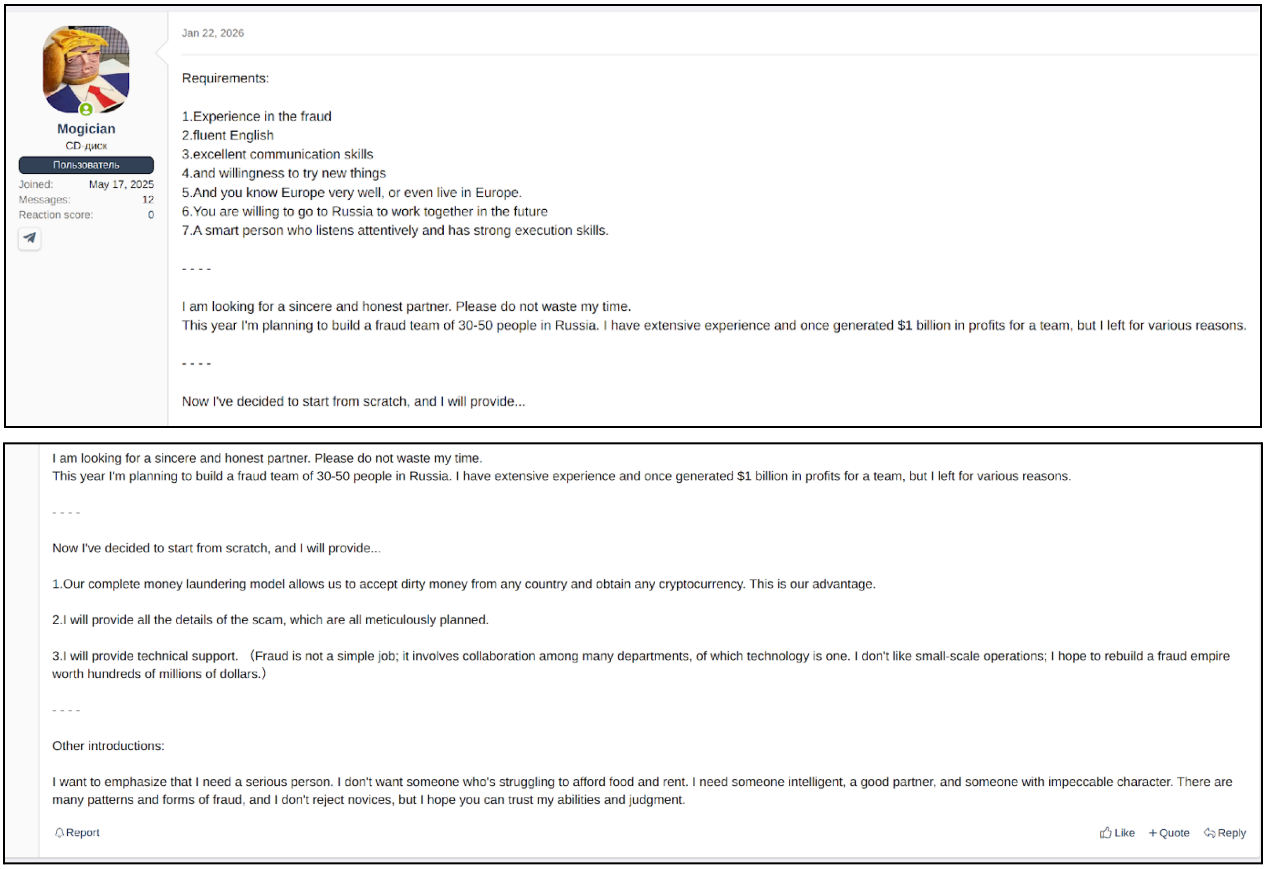
The seizure of RAMP is likely to have a significant impact on the cybercriminal landscape. Before the takedown, RAMP was the only known dark web forum to allow RaaS operations on the platform; this is an environment that will not be easy to replace quickly. While other Russian-language forums will almost certainly see more traffic, until a new dark web forum that explicitly allows RaaS comes online, a slight downturn in ransomware attacks in the short term is expected.

The FBI and other Western law enforcement agencies will almost certainly develop new leads from the data seized from RAMP and will likely exploit identities, IP addresses, and other information gathered to conduct investigations and make arrests of RAMP operators located in the West. It is highly likely that arrests derived from the seizure of the RAMP forum will be made within the next six months.

Fraud Ring Recruitment Announcement on XSS

On January 22, 2026, an untested English-language actor known as "Mogician" posted an inquiry on the dark web forum XSS, seeking interested actors to partner in the development of a fraud ring in Europe. Mogician claimed to have extensive fraud experience that allegedly includes having generated USD 1 billion in profits for an unspecified team; this has seemingly influenced the actor's plans to build a fraud team of 30–50 people in Russia. The actor's requirements for all potential team participants include:

- Experience in fraud
- Fluent in English
- Strong knowledge of Europe or residence in Europe
- Willingness to travel to Russia
- Excellent communication skills, a willingness to try new things, the ability to listen, and strong execution skills



Mogician's original post on XSS
Source: ZeroFox Intelligence

Mogician stated that all details of the scam campaign would be provided as well as technical support, noting that they are seeking sincere and honest partners and that this campaign has been meticulously planned with the goal of building a fraud empire worth hundreds of millions of U.S. dollars. In addition, Mogician claimed to offer a complete money-laundering model that would allow participants to accept illicit funds from any country and convert them into any cryptocurrency, which they deemed a "significant advantage."

This alleged operation is very likely a fraud campaign not related to ransomware; instead, it likely involves a sophisticated network of financial mules in Europe, as well as on-the-ground operatives managing financial scams such as phishing, botnet log abuse, account takeovers, and call-center fraud. Due to the apparently large scale of the

proposed campaign, multiple members of the XSS forum are likely to apply for this opportunity.

Posts such as the one made by Mogician are considered rare, as they are very likely to attract the attention of security researchers and law enforcement; actors who develop legitimate criminal syndicates are unlikely to make public announcements recruiting participants. However, ZeroFox cannot rule out that Mogician is affiliated with, or acting on behalf of, intelligence agencies in order to collect information on criminal activities.

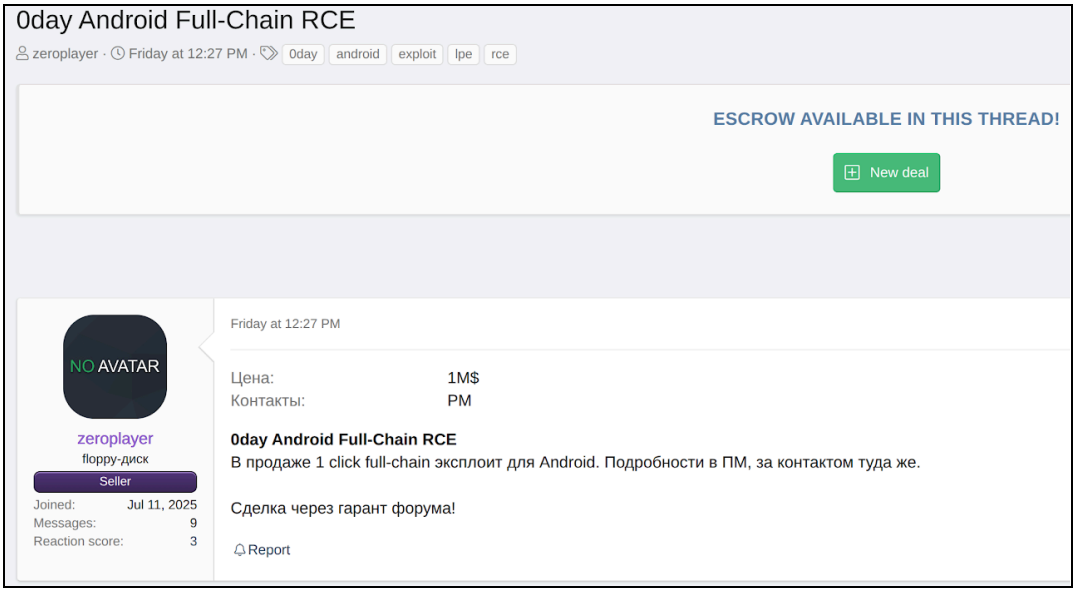
Zero-Day RCE for Android for Sale on Dark Web

On January 16, 2026, an actor known as "zeroplayer" announced the sale of a full-chain, zero-day remote code execution (RCE) affecting the Android operating system. The listing was posted on the dark web forum XSS, and the actor did not share any technical details other than the price, which is set at USD 1 million.

- A zero-day exploit refers to a vulnerability not yet identified by the network administrator. It is a term used to indicate that the system administrator has had "zero days" to fix the vulnerability.

A one-click, full-chain RCE is an attack in which the victim only needs to perform a single, simple action, such as opening a link or file. The attacker exploits a complete sequence of vulnerabilities that work together, from the initial entry point to the final impact. An attack of this type can be executed remotely using arbitrary code to gain access to a target system.

Zero-day vulnerabilities are almost impossible to identify unless the individual that discovered it is willing to disclose the exploit code and attack path. In this case, the sale of a zero-day almost certainly means zeroplayer is unwilling to help mitigate the vulnerability.



Zeroplayer's original post on XSS
Source: ZeroFox Intelligence

The seller is considered a relatively reputable member of the XSS community. However, because zeroplayer did not share technical details or any proof of the exploit, ZeroFox cannot determine the legitimacy of this post; further, this offering is likely among the most expensive zero-day exploits advertised on the deep and dark web (DDW) in recent months.

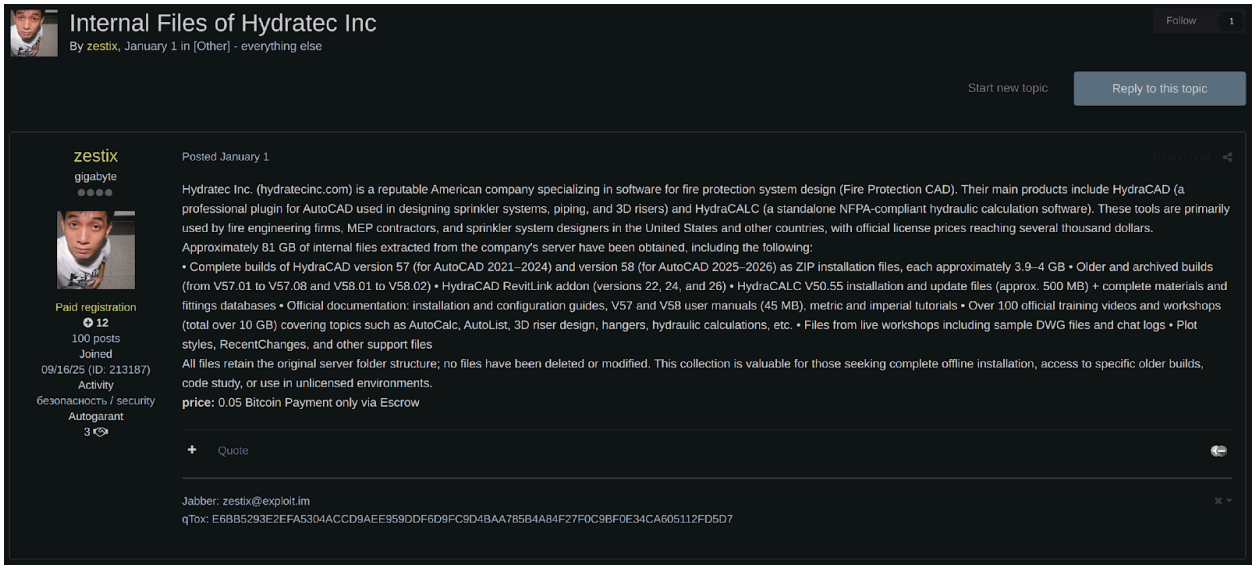
If legitimate, this exploit would very likely impact millions of Android users—at least temporarily. Android regularly issues updates to patch known vulnerabilities; however, until they are made aware of the specifics in this case, it is unlikely Android will patch it in time to mitigate the risk to its users.

Zestix Advertises 81 GB Data from Fire Protection Software Firm Hydratec

On January 1, 2026, threat actor "Zestix" advertised 81 GB of data allegedly exfiltrated from Hydratec, a U.S.-based fire protection software company, on the Russian language dark web forum Exploit.

- The database is priced at BTC 0.05 (equivalent to approximately USD 420), which is likely a low price for such a large dataset.
- Zestix has not publicly shared any data samples, but their positive reputation suggests that the data is likely legitimate.
- ZeroFox assesses that Zestix is a trusted seller on Exploit, having accumulated 12 positive reactions and completed three successful escrow-backed transactions since September 16, 2025. (Escrow is a practice used on dark web forums to ensure payment and reduce risks of fraud.)

On January 7, 2026, Zestix claimed to have access to corporate file-sharing environments belonging to approximately 50 global organizations, including Hydratec.[2] ZeroFox assesses there is a roughly even chance that the data was obtained using employee credentials harvested by infostealer malware.



Zestix advertises Hydratec database on Exploit
Source: ZeroFox Intelligence

2 hXXps://www.bleepingcomputer[.]com/news/security/cloud-file-sharing-sites-targeted-for-corporate-data-theft-attacks/

The alleged leaked data—which contains complete builds, documentation, and training materials—is likely to be used for software piracy, grey-market redistribution, or sold as corporate intelligence.

- Threat actors are also likely to repackage the installers for grey-market redistribution with malware, turning trusted engineering software used by construction and infrastructure firms into a delivery vector for backdoors or infostealers.

Hydratec personnel are advised to prioritize establishing multi-factor authentication (MFA) to strengthen accounts against infostealers siphoning sensitive information. Moreover, clients are advised to be wary of unvetted vendors advertising heavily discounted, cracked, or free "trial" versions of Hydratec software.

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%