ZEROFOX INTELLIGENCE

Flash

FBI Seizes Dark Web Forum RAMP

F-2026-01-29a

Classification: TLP:CLEAR

Criticality: LOW

Intelligence Requirements: Dark Web, Threat Actor

January 29, 2026

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 7:00 AM (EST) on January 29, 2026; per cyber hygiene best practices, caution is advised when clicking on any third-party links.

| Flash | FBI Seizes Dark Web Forum RAMP

| Key Findings

- On January 28, 2026, the Federal Bureau of Investigation (FBI) seized the dark web forum RAMP in a coordinated action with the U.S. Attorney's Office for the Southern District of Florida and the Computer Crime and Intellectual Property Section of the U.S. Department of Justice (DoJ).
- The RAMP forum's primary purpose was to advertise ransomware-as-a-service (RaaS) activities, and it was the only known dark web forum where such activity was explicitly permitted.
- Following news of the seizure, screenshots from a suspected leaked RAMP database appeared in a Telegram channel—including an email address allegedly used by well-known RaaS operator "LockBit" to register on RAMP.
- The seizure of RAMP is likely to have a significant impact on the cybercriminal community in the short term. As RAMP was the only known dark web forum to explicitly allow RaaS operations on its platform, it is an environment that will not be easy to replace quickly. It is also highly likely that arrests derived from the seizure of the RAMP forum will be made within the next six months.

Detail

On January 28, 2026, the 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 DoJ.

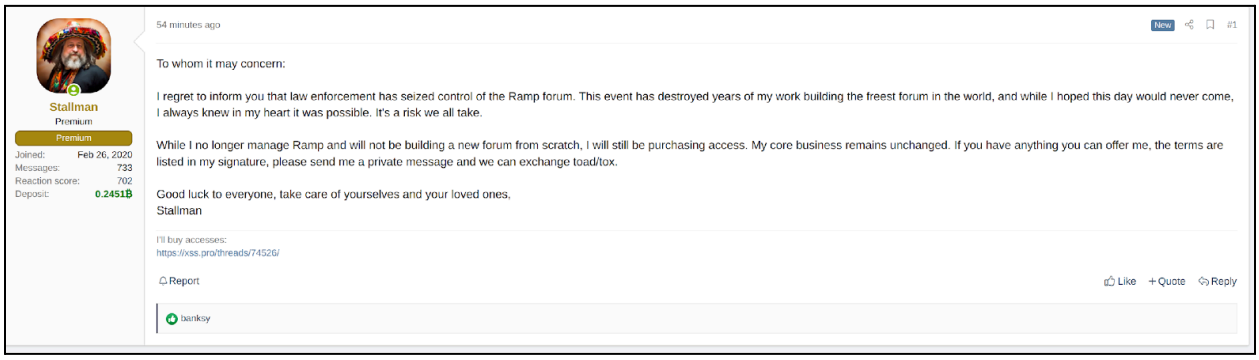
- RAMP had been active since 2021, and numerous ransomware groups (including Qilin, LockBit, DragonForce, RansomHub, and ALPHV/BlackCat) promoted their RaaS operations there, making it one of the most popular forums among RaaS collectives.
- The RAMP forum was the only known dark web forum where RaaS 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.

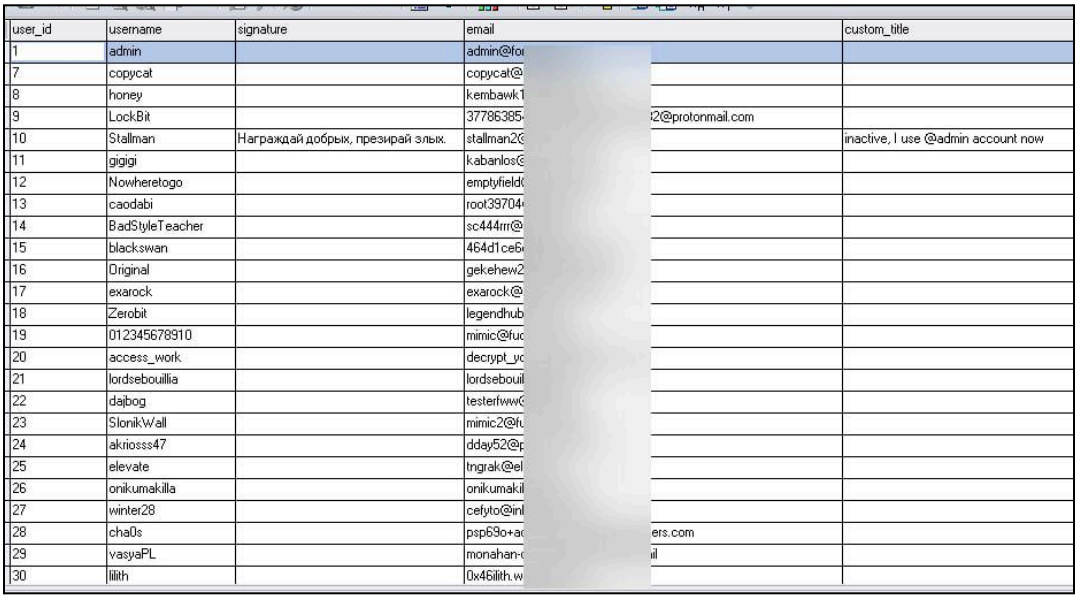


Stallman's XSS post

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 would likely 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		0x46ilith.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.

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%