ZEROFOX INTELLIGENCE

Flash

Major Cybercrime Forum Disrupted by Law Enforcement

F-2025-07-24b

Classification: TLP:CLEAR

Criticality: LOW

Intelligence Requirements: Dark Web, Threat Actor, Ransomware

July 24, 2025

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 (EDT) on July 24, 2025; per cyber hygiene best practices, caution is advised when clicking on any third-party links.

| Flash | Major Cybercrime Forum Disrupted by Law Enforcement

| Key Findings

- On July 23, 2025, prominent deep web forum XSS went offline; its associated web domain, xss[.]is, is currently displaying an announcement about the forum's seizure by multiple law enforcement (LE) entities.
- The forum outage follows an announcement by the same LE bodies about the arrest of an individual suspected of fulfilling an administrative role within XSS. Reporting suggests that the arrest, which took place in Ukraine, is part of an LE operation that commenced in 2021.
- While the arrest of the alleged deep web forum moderator does not itself allude to long-term disruption of the xss[.]is forum, there is a likely chance that subsequently obtained information will lead to the identification of additional individuals involved in operating the XSS forum, as well as the acquisition of critical digital infrastructure by LE.

Details

On July 23, 2025, the prominent deep web forum XSS went offline, with the associated domain xss[.]is displaying an announcement about the forum's seizure by multiple LE entities—including La Brigade de Lutte contre la Cybercriminalité, the Security Service of Ukraine (SBU), and Europol. The outage follows an announcement by the same LE bodies of the arrest of an individual suspected of fulfilling an administrative role within XSS. Reporting suggests that the arrest, which took place in Ukraine, is part of an LE operation that commenced in 2021.[1][2]

- The dark web version of the forum, which is accessible via an [.]onion URL, is also unavailable as of the writing of this report. Users are seemingly being required to re-register; however, ZeroFox's attempt to do so was unsuccessful.
- This activity is the latest in a series of LE operations that have occurred this year, including the April 2025 outage of the popular deep web hacking forum BreachForums; the alleged June 2025 arrests of prominent threat actors IntelBroker and ShinyHunters; and, more recently, the July 2025 arrest of individuals thought to be associated with a string of digital extortion attacks targeting UK-based retail organizations.

Law enforcement message displayed at xss[.]is

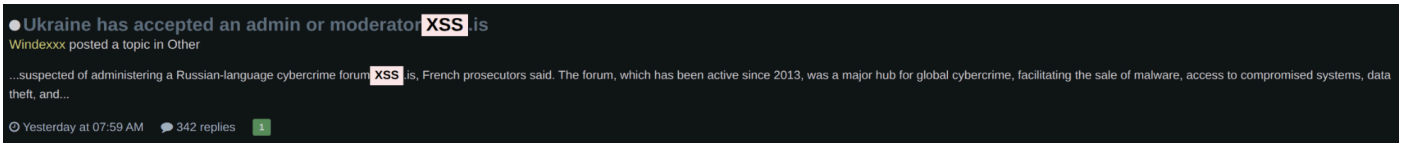
Source: ZeroFox Intelligence

[1] hXXps://x[.]com/parquetdeparis

[2] hXXps://www.europol.europa[.]eu/media-press/newsroom/news/key-figure-behind-major-russian-speaking-cybercrime-forum-targeted-in-ukraine

XSS is a closed Russian-language forum that was founded as DaMaGeLaB in 2004, making it one of the oldest dark web forums. The site was rebranded in 2018 to XSS, a name very likely associated with cross-site scripting (a web security vulnerability); today the forum maintains over 46,000 members. XSS is generally perceived as one of the most "professionalized" forums within the deep and dark web (DDW), largely due to the rules and norms that govern the behavior of frequenting actors, as well as the nature of transactions that take place within it.

- XSS was once a premier DDW forum for ransomware-as-a-service (RaaS) collectives to operate and hosted prominent outfits such as REvil, LockBit, and ALPHV. However, the forum banned RaaS-associated activities in 2021, a prohibition that remains in place as of the writing of this report. This was very likely intended to reduce the risk of any LE scrutiny that could follow ransomware and digital extortion (R&DE) collectives—particularly those targeting sensitive targets, such as critical national infrastructure (CNI).



DarkForums thread containing discussion surrounding XSS outage
Source: ZeroFox Intelligence

ZeroFox observed discussion surrounding these events taking place in the popular hacking forum Exploit, with one thread having over 350 replies as of this writing. While no general sentiment is clear among forum members, many pose different theories as to the fate of both XSS and the apprehended individual. Further threads created by alleged moderators within other DDW forums alluded to a replacement XSS domain and warned users against visiting the original xss[.]onion domain, though no further details were observed.

The extent to which LE entities have acquired access to digital infrastructure associated with XSS is currently unclear, as is the likely scope and duration of any further forthcoming disruption. In the coming weeks, threat actors relying on DDW forums to acquire or sell malicious services are very likely to seek membership within similar

forums, such as Exploit or RAMP—the latter of which upholds notably stringent joining procedures. While the arrest of a DDW forum moderator does not itself allude to long-term disruption of the domain, there is a likely chance that subsequently obtained information will lead to the identification of additional individuals involved in operating the XSS forum, as well as the acquisition of critical digital infrastructure by LE.

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%