ZEROFOX INTELLIGENCE

Flash

UK Sanctions Prominent Bulletproof Hosting Provider

F-2025-11-26a

Classification: TLP:CLEAR

Criticality: LOW

Intelligence Requirements: Malware, Ransomware, Threat Actor

November 26, 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 8:00 AM (EST) on November 26, 2025; per cyber hygiene best practices, caution is advised when clicking on any third-party links.

| Flash | UK Sanctions Prominent Bulletproof Hosting Provider

| Key Findings

- On November 19, 2025, the United Kingdom's National Crime Agency (NCA), in coordination with partners in Australia, New Zealand, Canada, and the United States, announced sanctions against a Russian citizen for operating a bulletproof hosting (BPH) service.
- The BPH operates under the names "Media Land LLC" and "ML.Cloud LLC". Both of these companies are based in Russia and provide virtual and physical servers for cybercriminals to maintain digital privacy and evade law enforcement (LE) takedowns.
- BPH is a marketing term used by underground Internet Service Providers (ISPs) to promote services that aid cybercriminals in the conduct of their operations.
- The sanctioning will likely have a limited impact on cybercriminals' operational environment. Considering that this BPH is based in Russia, it is highly unlikely that any legal action to take down its operations will occur.

Details

On November 19, 2025, the United Kingdom's NCA, in coordination with partners in Australia, New Zealand, Canada, and the United States, announced sanctions against Russian citizen Alexander Volosovik for operating a BPH service. Volosovik, known online as "Yalishanda", "Downlow", and "Stas_vl", has been accused of providing infrastructure to several threat actors, including LockBit, Evil Corp, and Black Basta.

- BPH is a marketing term used by underground ISPs to promote services that aid cybercriminals in the conduct of their operations. BPHs provide physical and virtual infrastructure, including servers, proxy networks, command and control (C2) nodes, and back-end hosting.
- BPH services have very likely contributed to cyberattacks against organizations and their customers that have resulted in financial losses in the millions of dollars.

According to the NCA, Volosovik's infrastructure enables cybercriminals to launch cyberattacks targeting an array of organizations and government institutions—resulting in financial losses, operational disruptions, and reputational damage.[1]

- Volosovik's BPH operates under the company names Media Land LLC and ML.Cloud LLC. Both companies are based in Russia and provide virtual and physical servers for cybercriminals to maintain digital privacy and evade LE takedowns.

[1] hXXps://www.nationalcrimeagency[.]gov[.]uk/news/prolific-bulletproof-hosting-service-sanctioned-by-the-uk-and-allies

Alexander Volosovik

Source: hXXps://www.nationalcrimeagency[.]gov[.]uk/news/prolific-bulletproof-hosting-service-sanctioned-by-the-uk-and-allies

In addition to providing services to cybercriminal groups, Volosovik was reportedly responsible for restoring 8kun (formerly, 8chan), following the controversial forum's takedown by traditional ISPs.[2] While not illegal, Volosovik's involvement with 8kun is an illustration of the impact BPH providers can have. Without Volosovik, or BPH providers like him, it is likely that 8kun would have ceased operations, which would have limited the impact of the misinformation campaigns that originated on the site.

[2] hXXps://hackread[.]com/uk-bulletproof-hosting-operator-lockbit-evil-corp/

Example of BPH Advertisement

Source: hXXps://www.cyber[.]gov[.]au/about-us/view-all-content/publications/bulletproof-hosting-providers

Analyst Commentary

The sanctioning of Volosovik and his companies will likely have a limited impact on cybercriminals' operational environment. Considering that Volosovik is based in Russia, it is highly unlikely that any legal action to take down his operations will occur. However, the sanctions will make it illegal for any citizen of the countries that have sanctioned him to do business or exchange funds with him, which will likely impact his operations and make it more difficult for him to get paid or move money.

Enforcement against BPH providers remains extremely difficult, largely due to the physical location of their operations. It is likely that most BPH providers are based in countries such as Russia and China, which will not be responsive to sanctions or requests for LE takedowns from the West. This likely leaves Western regulators and LE agencies with limited options (such as sanctions) to disrupt these providers.

The sanctions are the latest indicator that Western nations are seeking to combat cybercrime in a holistic manner by targeting support structures and facilitators rather than solely focusing on threat actors. This comes on the heels of the Cyber Security and Resilience Bill put forward in the UK Parliament—a broad package that seeks to enhance the country's existing cybersecurity law and improve defenses against cyberattacks. It is almost certain that Western authorities will continue to seek new methods to bring down the cybercrime ecosystem as a whole and reduce the threat from cyberattacks.

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%