

United States, Australia, and United Kingdom Sanction Russian Cybercrime Infrastructure Supporting Ransomware

Today, the Department of the Treasury's Office of Foreign Assets Control (OFAC), Australia's Department of Foreign Affairs and Trade, and the United Kingdom's Foreign Commonwealth and Development Office are announcing coordinated sanctions targeting **Media Land**, a Russia-based bulletproof hosting (BPH) service provider, for its role in supporting ransomware operations and other forms of cybercrime. OFAC is also designating three members of Media Land's leadership team and three of its sister companies in coordination with the Federal Bureau of Investigation.

BPH service providers sell access to specialized servers and other computer infrastructure specifically designed to evade detection and defy law enforcement efforts to disrupt malicious cyber activities.

In addition, OFAC and the United Kingdom are designating **Hypercore Ltd.**, a front company of Aeza Group LLC (Aeza Group), a BPH service provider designated by OFAC earlier this year. OFAC, in coordination with its UK partners, is also designating two additional individuals and two entities that have led, materially supported, or acted for Aeza Group.

"These so-called bulletproof hosting service providers like Media Land provide cybercriminals essential services to aid them in attacking businesses in the United States and in allied countries," said **Under Secretary of the Treasury for Terrorism and Financial Intelligence John K. Hurley**. "Today's trilateral action with Australia and the United Kingdom, in coordination with law enforcement partners, demonstrates our collective commitment to combatting cybercrime and protecting our citizens."

MEDIA LAND: A KEY LAUNCHING PAD FOR RANSOMWARE

Media Land LLC (Media Land), headquartered in St. Petersburg, Russia, has provided BPH services to criminal marketplaces and ransomware actors, including prolific ransomware actors such as Lockbit, BlackSuit, and Play. Media Land infrastructure was also utilized in multiple distributed denial-of-service (DDOS) attacks against U.S. victim companies and critical infrastructure.

ML Cloud is a Media Land sister company whose technical infrastructure is often used in conjunction with Media Land, including in ransomware and DDOS attacks.

Aleksandr Volosovik (Volosovik) is the general director of Media Land and has frequently advertised the Media Land business on cybercriminal forums under the alias "Yalishanda." He has provided servers and conducted troubleshooting for ransomware and DDOS actors.

Kirill Zatolokin (Zatolokin) is a Media Land employee who is responsible for collecting payment from customers and coordinating with other cyber actors. He also works closely with Volosovik on Media Land's overall operations.

Yulia Pankova (Pankova) is aware of Volosovik's illicit activity, has assisted Volosovik with legal issues, and has handled his finances.

Media Land Technology (MLT) and **Data Center Kirishi (DC Kirishi)** are 100 percent-owned subsidiaries of Media Land.

MAINTAINING PRESSURE ON AEZA GROUP

After OFAC's designations of Aeza Group (Aeza) and its leadership on July 1, 2025, Aeza leadership initiated a rebranding strategy focusing on removing any connections between Aeza and their new technical infrastructure. OFAC's designations today serve as a reminder that OFAC will take all possible steps to counter sanctions evasion activity by malicious cyber actors and their enablers.

Hypercore Ltd. (Hypercore) is a UK company registered and utilized by Aeza Group after its designation to move its IP infrastructure and evade sanctions. OFAC is designating Hypercore pursuant to E.O. 13694, as further amended, for being owned or controlled by, or having acted or purported to act for or on behalf of, directly or indirectly, Aeza.

Maksim Vladimirovich Makarov (Makarov) is the new director of Aeza. He has made key

Ilya Vladislavovich Zakirov (Zakirov) helped establish new companies and payment methods to obfuscate Aeza's continuing activity.

Smart Digital Ideas DOO (Smart Digital) and **Datavice MCHJ** (Datavice) and are Serbian and Uzbek companies utilized by Aeza to evade sanctions and set up technical infrastructure that is not publicly associated with the Aeza brand.

As a result of today's action, all property and interests in property of the designated or blocked persons described above that are in the United States or in the possession or control of U.S. persons are blocked and must be reported to OFAC. In addition, any entities that are owned, directly or indirectly, individually or in the aggregate, 50 percent or more by one or more blocked persons are also blocked.

Dated 19 November, 2025

