United States, Australia, and the United Kingdom Jointly Sanction Key Infrastructure that Enables Ransomware Attacks

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 jointly designating Zservers, a Russia- based bulletproof hosting (BPH) services provider, for its role in supporting LockBit ransomware attacks. LockBit, a Russia-based ransomware group best known for its ransomware variant of the same name, is one of the most deployed ransomware variants and was responsible for the November 2023 attack against the Industrial Commercial Bank of China U.S. broker- dealer. BPH service providers sell access to specialized servers and other computer infrastructure designed to evade detection and defy law enforcement attempts to disrupt these malicious activities. OFAC is also designating two Russian nationals who are key administrators of Zservers and have enabled ransomware attacks and other criminal activity.

"Ransomware actors and other cybercriminals rely on third-party network service providers like Zservers to enable their attacks on U.S. and international critical infrastructure," said Acting Under Secretary of the Treasury for Terrorism and Financial Intelligence Bradley T. Smith. "Today's trilateral action with Australia and the United Kingdom underscores our collective resolve to disrupt all aspects of this criminal ecosystem, wherever located, to protect our national security."

This action builds on last year's trilateral cyber sanctions with Australia and the United Kingdom against Russian ransomware actor Alexander Ermakov and members of the Evil Corp ransomware group. It also reflects a shared commitment to combatting cybercrime and degrading the support networks that enable bad actors to target victims in the United States and in allied countries. This action was developed with the support of the Department of Justice and the Federal Bureau of Investigation.

ZSERVERS: A RUSSIAN BULLETPROOF HOSTING SERVICES PROVIDER SUPPORTING RANSOMWARE AND CYBERCRIME

Zservers, headquartered in Barnaul, Russia, has advertised BPH services on known cybercriminal forums to evade law enforcement investigations and takedowns, as well as scrutiny from cybersecurity firms. Zservers has provided BPH services, including leasing numerous IP addresses, to LockBit affiliates, who have used the hosting services to coordinate and launch ransomware attacks. During a 2022 search of a known LockBit affiliate, Canadian law enforcement uncovered a laptop operating a virtual machine that was connected to a Zservers' subleased IP address and running a programming interface used to operate LockBit malware. In 2022, a Russian cybercriminal purchased IP addresses from Zservers, almost certainly for use as Lockbit chat servers to discuss ransomware operations. In 2023, Zservers leased infrastructure, including a Russian IP address, to a Lockbit affiliate.

OFAC is designating Zservers pursuant to Executive Order (E.O.) 13694, as further amended by E.O. 14144, for having materially assisted, sponsored, or provided financial, material, or technological support for, or goods or services to or in support of, LockBit ransomware, a cyber- enabled activity originating from, or directed by persons located, in whole or substantial part, outside the United States that is reasonably likely to result in, or has materially contributed to, a threat to the national security, foreign policy, or economic health or financial stability of the United States and that has the purpose of or involves causing a misappropriation of funds or

economic resources, intellectual property, proprietary or business confidential information, personal identifiers, or financial information for commercial or competitive advantage or private financial gain.

KEY ZSERVERS PERSONNEL

Alexander Igorevich Mishin (Mishin) is a Russian national and administrator of Zservers. Mishin has marketed Zservers' BPH services to cybercriminals, including LockBit affiliates and other ransomware groups, with the understanding that they would use those services in their cybercriminal activities. He has also directed virtual currency transactions to be made in support of those activities.

Aleksandr Sergeyevich Bolshakov (Bolshakov) is a Russian national and administrator of Zservers. In 2023, Bolshakov and Mishin shut down an IP address in response to a complaint from a Lebanese company alleging that a Zservers-associated IP address had implemented Lockbit in a ransomware attack. Zservers likely enabled ransomware attacks to continue by assigning a new IP address to the malicious Lockbit user. Mishin instructed Bolshakov to change the IP address of the malicious user and then told the Lebanese company that the original IP address was cut off.

SANCTIONS IMPLICATIONS

As a result of today's action, all property and interests in property of the 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. Unless authorized by a general or specific license issued by OFAC, or exempt, OFAC's regulations generally prohibit all transactions by U.S. persons or within (or transiting) the United States that involve any property or interests in property of designated or otherwise blocked persons.

Dated 11th February, 2025