WASHINGTON — Today, the U.S. Department of the Treasury’s Office of Foreign Assets Control (OFAC) took action to designate Genesis Market, one of the world’s largest illicit marketplaces, for its part in the theft and sale of device credentials and related sensitive information. Genesis Market gains unauthorized access to victim devices and offers stolen data, including usernames and passwords, for sale. This action was coordinated with the U.S. Department of Justice (DOJ) and international partners from a dozen countries, who are taking law enforcement actions against Genesis Market users across multiple jurisdictions and seizing the website domains associated with Genesis Market.

“The United States, along with our international partners, will not allow illicit marketplaces to operate with impunity,” said Under Secretary of the Treasury for Terrorism and Financial Intelligence Brian E. Nelson. “Treasury will continue to work closely with our law enforcement colleagues to disrupt this activity and hold malign cyber actors accountable.”

Treasury has long recognized the illicit finance risks associated with darknet markets, and today’s sanctions designation builds upon previous actions against darknet marketplaces, such as the designation of Hydra Market, which OFAC designated on April 5, 2022. In addition, Treasury’s 2022 National Money Laundering Risk Assessment identified that darknet markets provide an opportunity for criminals to profit from unauthorized access to victim computers by selling stolen data to other criminals for further exploitation. Furthermore, FinCEN’s “Advisory on Illicit Activity Involving Convertible Virtual Currency” warns that darknet markets frequently include offers for the sale of illicit goods and services that use virtual currencies as a method of payment.

**GENESIS MARKET: A KEY RESOURCE FOR CYBERCRIMINALS**

Genesis Market operates a criminal marketplace and is believed to be located in Russia. It has both a clearnet (traditional internet) and a darknet presence and is one of the most prominent brokers of
stolen credentials and other sensitive information. Genesis Market identifies victim computer systems and gains unauthorized access to them, selling this access to cybercriminals for further exploitation. Its website compiles stolen victim data—including computer and mobile device identifiers, email addresses, usernames, passwords, and other credentials—from malware-infected systems around the globe and packages it for sale. As of February 1, 2023, there were approximately 460,000 packages listed for sale on Genesis Market, each of which represents a single, compromised victim computer or device. These packages contain stolen passwords and personal information for a variety of online accounts, including email, social media, and video streaming platforms, among others.

Genesis Market sells stolen credentials from leading U.S. and international companies and facilitates cybercrimes against them. In June 2021, a U.S. company was breached by hackers who stole sensitive data, including a software engine and source code. The hackers were able to access the U.S. company’s system because of a cookie purchased from Genesis Market.

Genesis Market has also been used by cybercriminals to target U.S. government organizations.

Genesis Market is being designated pursuant to Executive Order (E.O.) 13694, as amended by E.O. 13757, for being responsible for or complicit in, or having engaged in, directly or indirectly, cyber-enabled activities originating from, or directed by persons located, in whole or in substantial part, outside the United States that are reasonably likely to result in, or have materially contributed to, a significant threat to the national security, foreign policy, or economic health or financial stability of the United States and that have the purpose or effect of causing a significant misappropriation of funds or economic resources, trade secrets, personal identifiers, or financial information for commercial or competitive advantage or private financial gain.

**SANCTIONS IMPLICATIONS**

As a result of today’s action, all property and interests in property of the entity that are in the United States or in the possession or control of U.S. persons must be blocked and reported to OFAC. OFAC’s regulations generally prohibit all dealings by U.S. persons or within the United States (including transactions transiting the United States) that involve any property or interests in property of a blocked or designated entity.

In addition, persons that engage in certain transactions with the entity designated today may themselves be exposed to sanctions.

The power and integrity of sanctions derive not only from OFAC’s ability to designate and add persons to the Specially Designated Nationals and Blocked Persons (SDN) List but also from OFAC’s willingness to remove persons from the SDN List consistent with the law. The ultimate goal of
sanctions is not to punish but to bring about a positive change in behavior. For information concerning the process for seeking removal from an OFAC list, including the SDN List, please refer to OFAC’s Frequently Asked Question 897. For detailed information on the process to submit a request for removal from an OFAC sanctions list, please refer to OFAC’s website.

See OFAC’s Updated Advisory on Potential Sanctions Risk for Facilitating Ransomware Payments here for information about actions that OFAC would consider to be mitigating factors in any related enforcement action involving ransomware payments with a potential sanctions risk. For information on complying with sanctions applicable to virtual currency, see OFAC’s Sanctions Compliance Guidance for the Virtual Currency Industry here.

For more information on the entity designated today, click here.

###