Treasury Sanctions a Cybercrime Network Associated with the 911 S5 Botnet

Published: 2026-02-13 · Archived: 2026-04-05 13:19:38 UTC

WASHINGTON — Today, the U.S. Department of the Treasury's Office of Foreign Assets Control (OFAC) designated three individuals, Yunhe Wang, Jingping Liu, and Yanni Zheng, for their activities associated with the malicious botnet tied to the residential proxy service known as 911 S5. OFAC also sanctioned three entities—Spicy Code Company Limited, Tulip Biz Pattaya Group Company Limited, and Lily Suites Company Limited—for being owned or controlled by Yunhe Wang.

""These individuals leveraged their malicious botnet technology to compromise personal devices, enabling cybercriminals to fraudulently secure economic assistance intended for those in need and to terrorize our citizens with bomb threats," said Under Secretary Brian E. Nelson. "Treasury, in close coordination with our law enforcement colleagues and international partners, will continue to take action to disrupt cybercriminals and other illicit actors who seek to steal from U.S. taxpayers."

The 911 S5 botnet was a malicious service that compromised victim computers and allowed cybercriminals to proxy their internet connections through these compromised computers. Once a cybercriminal had disguised their digital tracks through the 911 S5 botnet, their cybercrimes appeared to trace back to the victim's computer instead of their own. The 911 S5 botnet compromised approximately 19 million IP addresses and facilitated the submission of tens of thousands of fraudulent applications related to the Coronavirus Aid, Relief, and Economic Security Act programs by its users, resulting in the loss of billions of dollars to the U.S. government. The 911 S5 service enabled users to commit widespread cyber-enabled fraud using compromised victim computers that were associated to residential IP addresses. The IP addresses compromised by the 911 S5 service were also linked to a series of bomb threats made throughout the United States in July 2022.

Today's action was taken in partnership with the Federal Bureau of Investigation, Defense Criminal Investigative Service, U.S. Department of Commerce's Office of Export Enforcement, as well as partners in Singapore and Thailand.

911 S5: A Key RESOURCE FOR CYBERCRIMINALS

Cybercriminals covet stolen residential IP addresses to obfuscate malicious activity, particularly when carrying out credit card theft. 911 S5 is a residential proxy botnet that allows its paying users, often cybercriminals, to select the IP addresses through which they connect to the internet using intermediary, internet-connected computers that have been compromised without the computer owners' knowledge. 911 S5 essentially enables cybercriminals to conceal their originating location, effectively defeating fraud detection systems.

Yunhe Wang is the primary administrator of the 911 S5 service. A review of records from network infrastructure service providers known to be utilized by 911 S5 and two Virtual Private Networks (VPN) specific to the botnet

operation (MaskVPN and DewVPN) showed Yunhe Wang as the registered subscriber to those providers' services.

Jingping Liu was Yunhe Wang's co-conspirator in the laundering of criminally derived proceeds generated from 911 S5, mainly virtual currency. The virtual currency that 911 S5 users paid to Yunhe Wang were converted into U.S. dollars using over-the-counter vendors who wired and deposited funds into bank accounts held by Jingping Liu. Jingping Liu assisted Yunhe Wang by laundering criminally derived proceeds through bank accounts held in her name that were then utilized to purchase luxury real estate properties for Yunhe Wang.

OFAC is designating Yunhe Wang pursuant to section 1(a)(ii)(D) of 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, a cyber-enabled activity identified in section 1(a)(ii)(D) of E.O. 13694, as amended by E.O. 13757.

OFAC is designating Jingping Liu pursuant to E.O. 13694, as amended by E.O. 13757, for having materially assisted, sponsored, or provided financial, material, or technological support for, or goods or services to or in support of, Yunhe Wang, a person whose property and interests in property are blocked pursuant to E.O. 13694, as amended by E.O. 13757.

Yunhe Wang's luxury properties

Today's sanctions designations illustrate illicit finance and money-laundering risks associated with the real estate industry. The U.S. Department of the Treasury's 2024 National Money Laundering Risk Assessment warns that purchases of high-value assets such as real estate through shell companies – particularly when conducted with cash and no financing – can be an attractive avenue for criminals to launder illegal proceeds while masking their identities.

Yanni Zheng acted as the power of attorney for Yunhe Wang and his company, Spicy Code Company Limited. In addition, Yanni Zheng participated in numerous business transactions, made multiple payments, and purchased real estate property on behalf of Yunhe Wang, including a luxury beachfront condominium in Thailand. OFAC is designating Yanni Zheng for having acted or purported to act for or on behalf of, directly or indirectly, Yunhe Wang, a person whose property and interests in property are blocked pursuant to E.O. 13694, as amended by E.O. 13757.

Spicy Code Company Limited was utilized to purchase additional real estate properties by Yunhe Wang. Spicy Code Company Limited is being designated pursuant to E.O. 13694, as amended by E.O. 13757, for being owned or controlled by, or having acted or purported to act for or on behalf of, directly or indirectly, Yunhe Wang.

Tulip Biz Pattaya Group Company Limited and **Lily Suites Company Limited** were both purchased by Yunhe Wang. Tulip Biz Pattaya Group Company Limited and Lily Suites Company Limited are being designated pursuant to E.O. 13694, as amended by E.O. 13757, for being owned or controlled by, or having acted or purported to act for or on behalf of, directly or indirectly, Yunhe Wang.

The three individuals sanctioned today are Chinese nationals. All three entities sanctioned today are based in Thailand.

sANCTIONS IMPLICATIONS

As a result of today's action, all property and interests in property of the designated individuals and entities 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 designation.

The power and integrity of OFAC sanctions derive not only from OFAC's ability to designate and add persons to the SDN List, but also from its 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.

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 individuals and entities designated today, click here.

###
