Treasury Sanctions China-based Hacker Involved in the Compromise of Sensitive U.S. Victim Networks

Published: 2026-02-13 · Archived: 2026-04-05 22:24:11 UTC

WASHINGTON — Today, the Department of the Treasury's Office of Foreign Assets Control (OFAC) is designating **Zhou Shuai**, a Shanghai-based malicious cyber actor and data broker, and his company, **Shanghai Heiying Information Technology Company, Limited** (Shanghai Heiying). In collaboration with another malicious cyber actor, U.S.-sanctioned Yin Kecheng, Zhou Shuai illegally acquired, brokered, and sold data from highly sensitive U.S. critical infrastructure networks. Malicious cyber actors, particularly those operating in China, continue to be one of the greatest and most persistent threats to U.S. national security, as highlighted in the Office of the Director of National Intelligence's most recent Annual Threat Assessment.

"Today's action underscores our resolve to hold accountable malicious cyber actors like Zhou who continue to target U.S. government systems, the data of U.S. companies, and our citizens," said Acting Under Secretary of the Treasury for Terrorism and Financial Intelligence Bradley T. Smith. "The United States is committed to disrupting all aspects of this criminal ecosystem leveraging all our available tools and authorities."

Today's designation follows a series of recent Treasury designations aimed at combatting increasingly dangerous cyber activity committed by cybercriminals in China. This includes the January 17, 2025 designation of Yin Kecheng and Sichuan Juxinhe Network Technology Company, Ltd. for their roles in the recent Department of the Treasury network compromise and the Salt Typhoon cyber group, respectively; the January 3, 2025 designation of Integrity Technology Group, Inc. for its role in the Flax Typhoon intrusion set; and the December 10, 2024 designation of Sichuan Silence Information Technology Company, Ltd. and one of its employees for their role in compromising firewalls.

Today, the Department of Justice is also unsealing indictments charging Yin Kecheng and Zhou Shuai based on their malicious cyber activity. Furthermore, the Department of State is announcing a Transnational Organized Crime Rewards Program offer of up to $2,000,000 for information leading to the arrest and/or conviction of Yin Kecheng or Zhou Shuai.

Zhou shuai: chinese Hacker and data broker

Since at least 2018, **Zhou Shuai** has acted as a data broker, selling illegally exfiltrated data and access to compromised computer networks. At least some of this data was acquired by known China-backed malicious cyber actor and former Shanghai Heiying employee Yin Kecheng. Yin Kecheng, who was sanctioned by OFAC on January 17, 2025, was involved in the 2024 compromise of the Department of the Treasury's network. Notable U.S. victims of Yin Kecheng and Zhou Shuai's partnership include technology companies, a defense industrial base contractor, a communications service provider, an academic health system affiliated with a university, and a government county municipality.

In 2020, Zhou Shuai appeared to be working from a set of intelligence requirements that included targets within the United States, Russia, and Western Europe. Data types of interest included telecommunications data, border crossing data, data on personnel in religious research, data on media industry personnel, and data on public servants. These requirements almost certainly originated from the CCP's intelligence services. In early 2021, Zhou Shuai brokered the sale of documents stolen from a U.S. cleared defense contractor.

OFAC is designating Zhou Shuai pursuant to Executive Order (E.O.) 13694, as further amended by E.O. 14144 ("E.O. 13694, as further amended"), for being responsible for or complicit in, or having engaged in, directly or indirectly, activities related to gaining or attempting to gain unauthorized access to a computer or network of computers of a U.S. person, the United States, a U.S. ally or partner or a citizen, national, or entity organized under the laws thereof, where such efforts originate from or are directed by persons located, in whole or substantial part, outside the United States and 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.

Shanghai heiying: a haven for hackers

Zhou Shuai established **Shanghai Heiying Information Technology Company, Limited** (Shanghai Heiying) in 2010 and is still its majority owner. Shanghai Heiying is a Shanghai-based cybersecurity company that has employed numerous known China-backed malicious cyber actors, including Yin Kecheng.

OFAC is designating Shanghai Heiying 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, Zhou Shuai, a person whose property and interests in property are blocked pursuant to E.O. 13694, as further amended.

Sanctions implications

As a result of today's action, all property and interests in property of the designated 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, U.S. sanctions 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.

Violations of U.S. sanctions may result in the imposition of civil or criminal penalties on U.S. and foreign persons. OFAC may impose civil penalties for sanctions violations on a strict liability basis. OFAC's Economic Sanctions Enforcement Guidelines provide more information regarding OFAC's enforcement of U.S. economic sanctions. In addition, financial institutions and other persons may risk exposure to sanctions for engaging in certain transactions or activities with designated or otherwise blocked persons.

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 here and to submit a request for removal, click here.

Click here for more information on the individuals and entities designated today.

###

Source: https://home.treasury.gov/news/press-releases/sb0042