Treasury Sanctions Company Associated with Salt Typhoon and Hacker Associated with Treasury Compromise

Published: 2026-02-13 · Archived: 2026-04-05 19:24:26 UTC

WASHINGTON — Today, the Department of the Treasury's Office of Foreign Assets Control (OFAC) is sanctioning **Yin Kecheng**, a Shanghai-based cyber actor who was involved with the recent Department of the Treasury network compromise. Additionally, OFAC is sanctioning **Sichuan Juxinhe Network Technology Co., LTD.**, a Sichuan-based cybersecurity company with direct involvement in the Salt Typhoon cyber group, which recently compromised the network infrastructure of multiple major U.S. telecommunication and internet service provider companies. People's Republic of China-linked (PRC) malicious cyber actors continue to target U.S. government systems, including the recent targeting of Treasury's information technology (IT) systems, as well as sensitive U.S. critical infrastructure. As highlighted in the most recent Office of the Director of National Intelligence Annual Threat Assessment, Chinese state-backed cyber actors continue to present some of the greatest and most persistent threats to U.S. national security.

"The Treasury Department will continue to use its authorities to hold accountable malicious cyber actors who target the American people, our companies, and the United States government, including those who have targeted the Treasury Department specifically," said Deputy Secretary of the Treasury Adewale O. Adeyemo.

This designation follows a series of recent Treasury sanctions actions aimed at combatting increasingly reckless cyber activity by the PRC and PRC-based actors, including the January 3, 2025 designation of Integrity Technology Group, Inc. for its role in Flax Typhoon malicious cyber activity, the December 10, 2024 designation of Sichuan Silence Information Technology Company, Ltd. and one of its employees for dangerous firewall compromises, and the March 25, 2024 designation of Wuhan Xiaoruizhi Science and Technology Company, Ltd. and two of its employees as Advanced Persistent Threat (APT) 31 malicious cyber actors. These all represent dangerous cyber activities directed at the United States, its partners, and allies.

The U.S. Department of State's Rewards for Justice program is offering a reward of up to $10 million for information leading to the identification or location of any person who, while acting at the direction or under the control of a foreign government, engages in certain malicious cyber activities against U.S. critical infrastructure in violation of the Computer Fraud and Abuse Act. More information about this reward offer is located on the Rewards for Justice website.

Chinese malicious cyber actor yin kecheng

Yin Kecheng has been a cyber actor for over a decade and is affiliated with the People's Republic of China Ministry of State Security (MSS). Yin Kecheng was associated with the recent compromise of the Department of the Treasury's Departmental Offices network.

OFAC is designating Yin Kecheng pursuant to Executive Order (E.O.) 13694, as further amended by the new E.O. on Strengthening and Promoting Innovation in the Nation's Cybersecurity, 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 United States person, the United States, a United States 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.

Chinese malicious cyber group SALT typhoon

Salt Typhoon has been active since at least 2019 and has been responsible for numerous compromises of U.S. companies in the communication sector. Recently, Salt Typhoon compromised the network infrastructure of multiple major U.S. telecommunication and internet service provider companies, marking a dramatic escalation in the Chinese cyber operations against U.S. critical infrastructure targets. The Salt Typhoon intrusions are one example of an increasing number of PRC state-backed malicious cyber activities, which necessitate costly remediation efforts.

Sichuan Juxinhe Network Technology Co., LTD. (Sichuan Juxinhe) had direct involvement in the exploitation of these U.S. telecommunication and internet service provider companies. The MSS has maintained strong ties with multiple computer network exploitation companies, including Sichuan Juxinhe.

OFAC is designating Sichuan Juxinhe pursuant to E.O. 13694, as further amended by the new E.O. on Strengthening and Promoting Innovation in the Nation's Cybersecurity, 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 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 harming, or otherwise compromising the provision of services by, a computer or network of computers that support one or more entities in a critical infrastructure sector.

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 Specially Designated Nationals and Blocked Persons (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. For detailed information on the process to submit a request for removal from an OFAC sanctions list, please click here.

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

###
