Treasury Sanctions China-Linked Hackers for Targeting U.S. Critical Infrastructure

March 25, 2024

The U.S. and UK take action against actors affiliated with the Chinese state-sponsored APT 31 hacking group.

WASHINGTON — Today, the Department of the Treasury's Office of Foreign Assets Control (OFAC) sanctioned **Wuhan Xiaoruizhi Science and Technology Company, Limited** (**Wuhan XRZ**), a Wuhan, China-based Ministry of State Security (MSS) front company that has served as cover for multiple malicious cyber operations. OFAC is also designating **Zhao Guangzong** and **Ni Gaobin**, two Chinese nationals affiliated with Wuhan XRZ,for their roles in malicious cyber operations targeting U.S. entities that operate within U.S. critical infrastructure sectors, directly endangering U.S. national security. This action is part of a collaborative effort with the U.S. Department of Justice, Federal Bureau of Investigation (FBI), Department of State, and the United Kingdom Foreign, Commonwealth & Development Office (FCDO).

People's Republic of China (PRC) state-sponsored malicious cyber actors continue to be one of the greatest and most persistent threats to U.S. national security, as highlighted in the most recent Office of the Director of National Intelligence Annual Threat Assessment.

"The United States is focused on both disrupting the dangerous and irresponsible actions of malicious cyber actors, as well as protecting our citizens and our critical infrastructure," said Under Secretary of the Treasury for Terrorism and Financial Intelligence Brian E. Nelson. "Through our whole-of-government

approach and in close coordination with our British partners, Treasury will continue to leverage our tools to expose these networks and protect against these threats."

Today, the Department of Justice unsealed indictments of Zhao Guangzong, Ni Gaobin, and five other defendants; and the U.S. Department of State announced a Rewards for Justice offer for information on these individuals, their organization, or any associated individuals or entities; and the UK Foreign, Commonwealth & Development Office implemented matching sanctions.

APT 31: A CHINESE MALICIOUS CYBER GROUP

An Advanced Persistent Threat (APT) is a sophisticated cyber actor or group with the capability to conduct advanced and sustained malicious cyber activity, often with the goal of maintaining ongoing access to a victim's network. Information security researchers will categorize and name certain APTs based on observed patterns such as the location of the perpetrators, the types of victims targeted, and the techniques used in the malicious cyber activity. APT 31 is a collection of Chinese state-sponsored intelligence officers, contract hackers, and support staff that conduct malicious cyber operations on behalf of the Hubei State Security Department (HSSD). APT 31 has targeted a wide range of high-ranking U.S. government officials and their advisors integral to U.S. national security including staff at the White House; the Departments of Justice, Commerce, the Treasury, and State; members of Congress, including both Democrat and Republican Senators; the United States Naval Academy; and the United States Naval War College's China Maritime Studies Institute.

APT 31 has targeted victims in some of America's most vital critical infrastructure sectors, including the Defense Industrial Base, information technology, and energy sectors. APT 31 actors have gained unauthorized access to multiple Defense Industrial Base victims, including a defense contractor that manufactured flight simulators for the U.S. military, a Tennessee-based aerospace and defense contractor, and an Alabama-based aerospace and defense research corporation. Additionally, APT 31 actors gained unauthorized access to a Texas-based energy company, as well as a California-based managed service provider.

In 2010, the HSSD established Wuhan XRZ as a front company to carry out cyber operations. This malicious cyber activity resulted in the surveillance of U.S. and foreign politicians, foreign policy experts, academics, journalists, and pro-democracy activists, as well as persons and companies operating in areas of national importance. In 2018, employees of Wuhan XRZ conducted an APT 31 malicious cyber operation on a Texas-based energy company, gaining unauthorized access.

OFAC is designating Wuhan XRZ pursuant to Executive Order (E.O.) 13694, as amended by E.O. 13757 (E.O. 13694, as amended), 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 has 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 harming, or otherwise significantly compromising the provision of services by, a computer or network of computers that support one or more entities in a critical infrastructure sector.

Zhao Guangzong is a Chinese national who has conducted numerous malicious cyber operations against U.S. victims as a contractor for Wuhan XRZ. Zhao Guangzong was behind the 2020 APT 31 spear

phishing operation against the United States Naval Academy and the United States Naval War College's China Maritime Studies Institute. Additionally, Zhao Guangzong has conducted numerous spear phishing operations against Hong Kong legislators and democracy advocates.

OFAC is designating Zhao Guangzong pursuant to E.O. 13694, as amended, for being owned or controlled by, or having acted or purported to act for or on behalf of, directly or indirectly, Wuhan XRZ, an entity whose property or interest in property are blocked pursuant to E.O. 13694, as amended.

Ni Gaobin is a Chinese national who has conducted numerous malicious cyber operations against U.S. victims. Ni Gaobin assisted Zhao Guangzong in many of his most high profile malicious cyber activities while Zhao Guangzong was a contractor at Wuhan XRZ, including the 2020 spear phishing operation against the United States Naval Academy and United States Naval War College's China Maritime Studies Institute.

OFAC is designating Ni Gaobin pursuant to E.O. 13694, as amended, for being owned or controlled by, or having acted or purported to act for or on behalf of, directly or indirectly, Wuhan XRZ, an entity whose property or interest in property are blocked pursuant to E.O. 13694, as amended.

SANCTIONS IMPLICATIONS

As a result of today's action, all property and interests in property of the designated persons and entity 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.

In addition, financial institutions and other persons that engage in certain transactions or activities with the sanctioned entities and individuals may expose themselves to sanctions or be subject to an enforcement action. The prohibitions include the making of any contribution or provision of funds, goods, or services by, to, or for the benefit of any designated person, or the receipt of any contribution or provision of funds, goods, or services from any such person.

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. 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.