Treasury Sanctions Technology Company for Support to Malicious Cyber Group

January 3, 2025

WASHINGTON – Today, the Department of the Treasury's Office of Foreign Assets Control (OFAC) sanctioned **Integrity Technology Group, Incorporated** (Integrity Tech), a Beijing-based cybersecurity company, for its role in multiple computer intrusion incidents against U.S. victims. These incidents have been publicly attributed to Flax Typhoon, a Chinese malicious state-sponsored cyber group that has been active since at least 2021, often targeting organizations within U.S. critical infrastructure sectors.

Chinese malicious cyber actors continue to be one of the most active 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. These actors continue to target U.S. government systems as part of their efforts, including the recent targeting of Treasury's own IT infrastructure.

"The Treasury Department will not hesitate to hold malicious cyber actors and their enablers accountable for their actions," said Acting Under Secretary of the Treasury for Terrorism and Financial Intelligence Bradley T. Smith. "The United States will use all available tools to disrupt these threats as we continue working collaboratively to harden public and private sector cyber defenses."

On September 18, 2024, the Federal Bureau of Investigation, in coordination with the Cyber National Mission Force, National Security Agency, and Five Eye partners, published a joint cybersecurity advisory, that highlights the tactics, techniques, and procedures of Flax Typhoon, as well as Integrity Tech's role in supporting its malicious cyber activities.

FLAX TYPHOON: A STATE-SPONSORED MALICIOUS CYBER GROUP

Flax Typhoon is a state-sponsored Chinese malicious cyber group that has been active since at least 2021, targeting organizations within U.S. critical infrastructure sectors. Flax Typhoon has compromised computer networks in North America, Europe, Africa, and across Asia, with a particular focus on Taiwan. Flax Typhoon exploits publicly known vulnerabilities to gain initial access to victims' computers and then leverages legitimate remote access software to maintain persistent control over their network. Flax Typhoon has targeted victims within a wide range of industries.

Between summer 2022 and fall 2023, Flax Typhoon actors accessed several hosts associated with U.S. and European entities. The actors maliciously used virtual private network software and remote desktop protocols to facilitate this access. In summer 2023, Flax Typhoon compromised multiple servers and workstations at a California-based entity.

INTEGRITY TECH SUPPORT TO FLAX TYPHOON

Between summer 2022 and fall 2023, Flax Typhoon actors used infrastructure tied to **Integrity Tech** during their computer network exploitation activities against multiple victims. During that time, Flax Typhoon routinely sent and received information from Integrity Techinfrastructure.

OFAC is designating Integrity Techpursuant 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 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.

SANCTIONS IMPLICATIONS

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