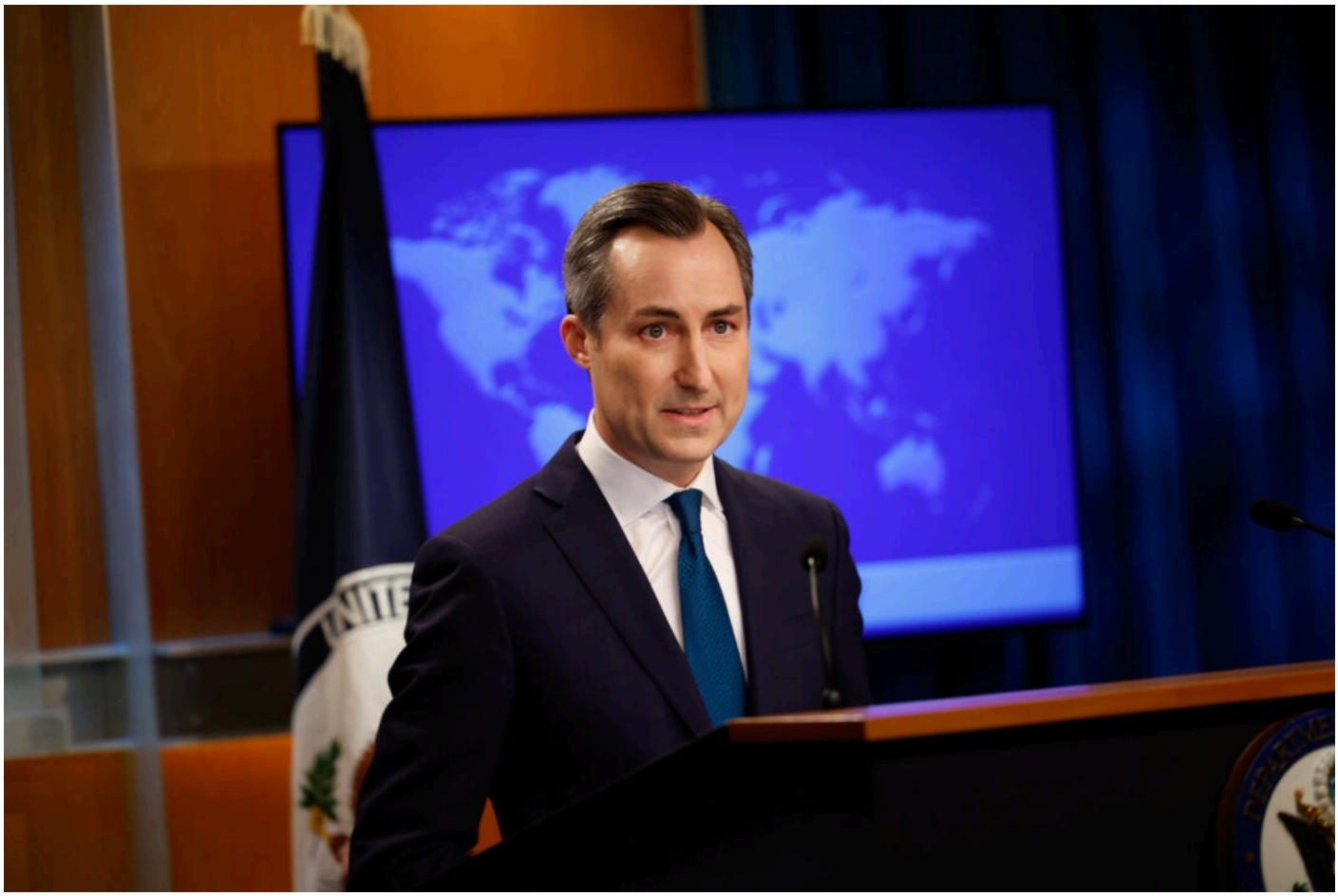
US > NATIONAL SECURITY

US Sanctions Chinese Company Over Flax Typhoon Hacking

Flax Typhoon, which had a botnet of 200,000 devices worldwide, was operating from Integrity Technology's infrastructure, the U.S. Treasury said.



State Department spokesperson Matthew Miller speaks at the State Department in Washington on Oct. 01, 2024.
Kevin Dietsch/Getty Images

By Lily Zhou
1/3/2025 Updated: 1/3/2025

The United States sanctioned a Chinese cybersecurity company on Friday over its role in the hacking of U.S. computer systems by China-backed cyber espionage group Flax Typhoon.

The company, Beijing-based Integrity Technology Group, Incorporated, is a state contractor linked to the Chinese regime's Ministry of State Security, according to a statement by U.S. State Department spokesperson Matthew Miller.

The Treasury said that Flax Typhoon actors used infrastructure tied to Integrity Tech during the group's hacking campaign between the summer of 2022 and the fall of 2023, routinely sending and receiving information from the infrastructure.

It also said Flax Typhoon "has been active since at least 2021, often targeting organizations within U.S. critical infrastructure sectors," and that Chinese cyber actors continue to target U.S. government systems, including the Treasury's infrastructure.

According to a letter sent to lawmakers on Dec. 31 by Assistant Treasury Secretary Aditi Hardikar, Chinese hackers compromised a third-party software service provider on Dec. 8 and stole unclassified documents from its workstations.

Friday's sanctions mean all Integrity Technology's property and interests in property in the United States will be blocked and must be reported to the Treasury's Office of Foreign Assets Control (OFAC), the office said.

U.S. persons are banned from having transactions that involve any such property or interests in property. Financial institutions and others in violation of the sanctions could get sanctioned themselves.

“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.”

Multi-agency actions against Flax Typhoon “reflect our whole-of-government approach to protecting and defending against PRC cyber threats to Americans, our critical systems, and those of our allies and partners,” said Miller, using the official acronym of the Chinese regime under the Chinese Communist Party, the People’s Republic of China.

“The United States will continue to use all the tools at its disposal to safeguard U.S. critical infrastructure and the American people from irresponsible and reckless cyber actors.”

The cyber-espionage group was dubbed Flax Typhoon by Microsoft, which said in August 2023 that the Chinese state-backed group had been active since 2021 and had spied on organizations “across a broad range of industries” in Taiwan “for as long as possible.”

In September 2024, the U.S. Department of Justice (DOJ) said a court-authorized law enforcement operation had disrupted Flax Typhoon’s botnet which consisted of 200,000 infected devices in the United States and worldwide.

According to the department, Flax Typhoon actors used malware to infect cameras, digital video recorders, routers, and many other consumer devices.

An investigation by the FBI found that the group had managed to compromise “corporations, universities, government agencies, telecommunications providers, and media organizations” in the United States and elsewhere, the DOJ said.

The DOJ said the court-authorized operation was able to destroy the botnet despite the hackers’ attempt to prevent the FBI’s actions.

In recent months, the United States has identified another Chinese hacking group, dubbed by Microsoft as Salt Typhoon, which the White House said has compromised nine U.S. telecom networks and targeted high-profile government officials and politicians.

On Dec. 10, the FBI said malware from Salt Typhoon, Flax Typhoon, and a third Beijing-backed group Volt Typhoon, were still embedded in some U.S. systems.

On Dec. 29, AT&T and Verizon confirmed that they were among the telecommunications companies targeted by Salt Typhoon, with a small number of high-profile customers being the focus of the target. The two companies said they believe their networks have since been secured.

Emel Akan contributed to this report.

Lily Zhou
Author

Lily Zhou is an Ireland-based reporter covering China news for The Epoch Times.

Author's Selected Articles

India Raises Concerns With China Over Mega Dam Project in Tibet
Jan 03, 2025

China Adds 28 US Companies to Export Control List, Including Defense Contractors
Jan 02, 2025

Taiwanese President Warns Citizens Against Chinese ID Cards

Jan 02, 2025

Jimmy Carter: The President Who Changed US–China Relations

Jan 01, 2025