Alleged Chinese hacker tied to Silk Typhoon arrested for cyberespionage

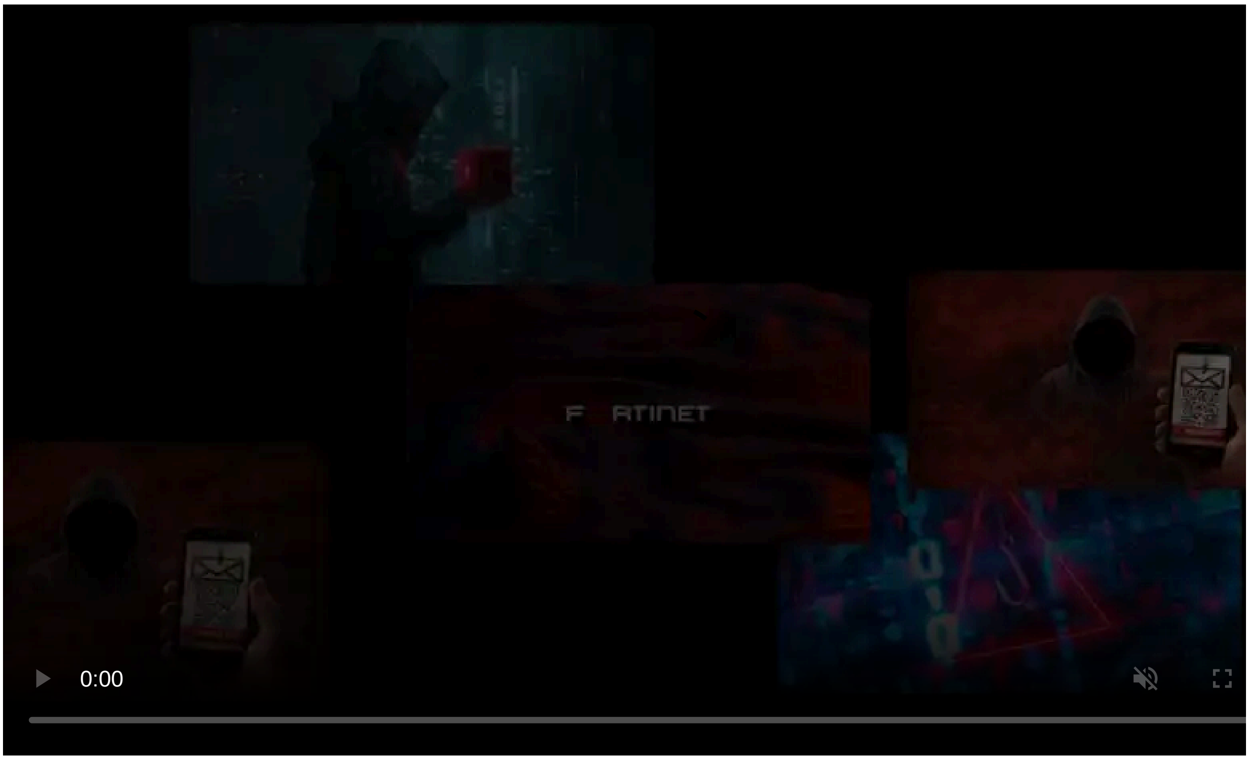
By Lawrence Abrams

Published: 2025-07-08 · Archived: 2026-04-05 21:23:31 UTC

A Chinese national was arrested in Milan, Italy, last week for allegedly being linked to the state-sponsored Silk Typhoon hacking group, which responsible for cyberattacks against American organizations and government agencies.

According to Italian media ANSA, the 33-year-old man, Xu Zewei, was arrested at Milan's Malpensa Airport on July 3rd after arriving on a flight from China. Italian police arrested the suspect on an international warrant from the U.S. government.

ANSA reports that Xu is accused of being linked to the Chinese state-sponsored Silk Typhoon hacking group, aka Hafnium, which has been responsible for a wide range of cyberespionage attacks against the U.S. and other countries.


0:00

In particular, Italian media reports that Xu is linked to the 2020 Silk Typhoon cyberattacks on infectious disease researchers and healthcare organizations, which aimed to steal data on anti-COVID vaccines.

"These actors have been observed attempting to identify and illicitly obtain valuable intellectual property (IP) and public health data related to vaccines, treatments, and testing from networks and personnel affiliated with COVID-19-related research," read the joint advisory.

The hacking group has also been linked to more recent cyberespionage campaigns, including those on the U.S. Treasury's Office of Foreign Assets Control (OFAC) and the Committee on Foreign Investment.

In March, Microsoft reported that Silk Typhoon had begun targeting remote management tools and cloud services in supply chain attacks to gain access to downstream customers' networks.

Xu is currently being held in Busto Arsizio prison with the U.S. seeking extradition to face trial in the States.
