

Charges Against Alleged Chinese Military Hacker Unsealed

 ntd.com/charges-against-alleged-chinese-military-hacker-unsealed_1017715.html

September 17, 2024



By Catherine Yang

September 17, 2024 US News





The Department of Justice (DOJ) in Washington on July 29, 2024. (Madalina Vasiliu/The Epoch Times)

Charges against Chinese national Jia Wei were unsealed on Sept. 17, alleging unlawful access to U.S. communications company networks to steal proprietary information on behalf of Chinese entities.

Wei, a member of the Chinese Communist Party's (CCP) People's Liberation Army (PLA), was assigned to Unit 61786, which is tasked with obtaining communications and information via hacking, according to the Department of Justice.

In March 2017, Wei and co-conspirators allegedly hacked an American company's network about two days after the company sued a China-based competitor for theft of trade secrets.

According to the indictment, the hackers obtained documents related to the company's "civilian and military communication devices," as well as "product development information, testing plans, and internal evaluations." They also copied documents that discussed the China-based competitor.

In April 2017, the hackers allegedly tried to install malicious software on the company's network.

The hackers continued to unlawfully access the network through May 2017, according to the indictment.

A special grand jury convened in May 2021 returned a six-count indictment in March 2022, charging Wei with wire fraud, conspiracy to commit computer intrusions, computer intrusions, and aggravated identity theft for using an employee's account to access the company network.

Wei, also known as "chansonJW," "JWT," "JWT487," "asmikace," "asmikace3d," "askikace3d," and "haber william," has not yet been arrested.

If convicted, he would face a maximum of 20 years in prison for wire fraud charges, five years in prison for conspiracy and computer intrusion charges, and two years for aggravated identity theft.

The United States has recognized CCP-backed cyber attacks as a top threat to national security. PLA hackers and other hacking rings tied to the CCP have been identified as responsible for several large-scale data breaches, such as the 2017 Equifax hack that compromised personal information, including social security numbers for 145 million Americans, 2021 Microsoft Exchange cyberattack that compromised some 10,000 networks, 2023 breach of government emails, and the ongoing "Volt Typhoon" campaign where hackers have infiltrated critical American infrastructure and are biding their time, according to FBI Director Christopher Wray.

The DOJ announced the unsealing of the indictment the same day it issued a major update of criminal charges in five separate cases resulting from the multiagency Disruptive Technology Strike Force.

The defendants include a Russian national who tried to illegally export drones to Russia and an employee of a Chinese regime-run aerospace conglomerate who allegedly tried to obtain software and source code from NASA, U.S. military branches, and the Federal Aviation Administration from 2017 to 2021.

Song Wu, a Chinese national, was indicted for running a large phishing campaign wherein he impersonated U.S.-based researchers and engineers to obtain aerospace engineering trade secrets. According to the DOJ, the technologies have industrial and military applications and could be used in the development of missiles and weapons.

Song was charged with 14 counts of wire fraud, which carries a maximum of 20 years in prison for each count, and 14 counts of aggravated identity theft, which carries a mandatory consecutive two-year term penalty.

From The Epoch Times