Talhah Khalifa

Mr. Wong

Help Desk

March 14, 2022

Cybersecurity: China Breaches Six U.S State Agencies

A few days ago, it was reported that China has hacked at least six different state governments in the United States in the past year. It is believed that this was the work of a hacking group which is supported by the Chinese government, known as the APT 41, advanced persistent threats. Other cybersecurity firms have identified what people believe is probably the same group with names as "Barium," and "Wicked Panda." Although the Chinese government has denied their relations with this specific hacking group, evidence suggesting otherwise have resurfaced. Prosecutors have mentioned that at one point one of the hackers had actually boasted about his affiliation with the Chinese Ministry of State Security. Back in 2020, the Justice Department had cited five members of the group for hacking into more than 100 U.S companies such as "computer software and hardware firms, telecom providers, video game companies, universities and think tanks."[1] Back in December the CISA, Cybersecurity and Infrastructure Security Agency, had publicly warned many that Log4J which was a software that was used by big tech firms, had a flaw that could be exploited easily in order to gain access to computer systems. The hackers used this software flaw in order to break into networks and target a wide range of state agencies which included "health, transportation, labor (including unemployment benefit systems), higher education, agriculture, and court networks

[1] Marks, Joseph. "Chinese hackers breached six state governments, researchers say." Washington Post, March 8, 2022. https://www.washingtonpost.com/politics/2022/03/08/chinese-hackers-breached-six-state-governments-researchers-say/. March 10, 2022

and systems."[2] Although they are not fully aware of the reasons or goal behind these hackings, information obtained from these state agencies could provide a lot of useful information to foreign spies, whether it is data related to elections or the government. It was reported that for one state, the hackers had accessed "personal data on some Americans, including names, email addresses and mobile phone numbers."[3] This just goes to show that vulnerabilities in softwares can be easily exploited in order to get information into the wrong hands. I believe these tech firms should have at least listened to the warnings the CISA was giving as they are a group of professionals trained to detect any flaws in these government networks.

[2] Lyngass, Sean. "Cybersecurity firm says Chinese hackers breached six US state agencies." CNN, March 8, 2022. https://www.cnn.com/2022/03/08/politics/china-hacking-state-governments-mandiant/index.html. March 9, 2022.

[3] "Cybersecurity firm says Chinese hackers breached six US state agencies." KSL TV, March 8, 2022. https://ksltv.com/486251/cybersecurity-firm-says-chinese-hackers-breached-six-us-state-agencies/#:~:text=No%20Use%20France.&text=(CNN)%20%E2%80%94%20A%20Chinese%20government,cybersecurity%20form%20 Mandiant%20said%20Tuesday. March 10, 2022.