APT Gang Branches Out to Medical Espionage in Community Health Breach

By Michael Mimoso

Published: 2014-08-19 · Archived: 2026-04-06 00:36:09 UTC

The Community Health Systems data breach has been tied to a Chinese APT gang that has branched out to medical espionage, stealing patient data in an effort to target intelligence on medical device development.

At first blush, the Community Health Systems data breach by Chinese hackers seems to be an anomaly. State-sponsored attackers generally target intellectual property for the purposes of military or economic gain; stealing healthcare credentials and personal patient records seems incongruous.

But experts say the breach is a perfect storm of poorly secured health systems, desperately trying to catch up to the security standards imposed in other critical industries, and a bevy of exposed information that can be leveraged for China's gain.

"This is done for the purposes of both economic espionage—stealing valuable intellectual property from healthcare and pharmaceutical companies that is critical for enhancing healthcare services in China for their aging population—as well as national security," said CrowdStrike cofounder Dmitri Alperovitch. "Collecting intelligence on key persons of interest, such as government officials and individuals that may be targeted for human recruitment, so PII data and medical records could be of great use there."

The breach surfaced yesterday when Reuters reported that the attackers had made off with Social Security numbers and personal data of 4.5 million patients. Community Health Systems said in an 8-K filing with the Securities and Exchange Commission that its network was breached in and April and again in June. The filing pinned the hack on an APT group from China adept in using "highly sophisticated malware and technology" to target its network.

"The attacker was able to bypass the company's security measures and successfully copy and transfer certain data outside the company," the 8-K filing said.

Mandiant, hired by Community Health Systems to investigate the breach and remediate the damage, told Threatpost via email that the group responsible is known to them as APT 18.

"This group typically targets companies in the aerospace and defense, construction and engineering, technology, financial services, and healthcare industry verticals," said Charles Carmakal, managing director at Mandiant, which was acquired by FireEye earlier this year. "The attacker has been known to steal intellectual property related to medical technology and pharmaceutical manufacturing processes."

Carmakal refused to answer questions about how the attackers breached the victim's network, what type of malware was used, or how Community Health Systems learned of the attack, citing its and law enforcement's ongoing investigation.

CrowdStrike's Alperovitch confirmed the APT 18 connection, though CrowdStrike calls the gang Dynamite Panda.

Community Health Systems said the data lost in the breach included non-medical patient identification data related to its physician practice operations. The 4.5 million victims were patients who were referred to or received services from physicians tied to Community Health Systems, the company said in its SEC filing. No credit card, medical or clinical information was lost, the company said, adding that the data is considered protected under the Health Insurance Portability and Accountability Act (HIPAA). HIPAA requires breach victims to notify affected patients; it said it carries cyber and privacy liability insurance protecting it from losses.

While the loss of patient data is significant, experts speculate the hackers may have been after intellectual property tied to medical device development. Hospital networks have also been under intense scrutiny from the security research community. Hackers have demonstrated serious vulnerabilities in medical devices, and network security at health care facilities has been exploited in other high profile attacks.

"For cyber security professionals, healthcare environments are riddled with challenges and are perhaps one of the most difficult industries to protect," said Trey Ford, global security strategist at Rapid7. "For example, you have a great deal of personally identifiable information (PII) that achieves high values on the black market; healthcare practitioners often sharing workstations and passwords, coming and going on shifts or in emergencies; and medical devices and systems that are highly regulated and certified for set configurations, so they cannot easily be patched. For these reasons, standard industry practices like network segmentation and scanning are often prohibited."
