BloombergBusiness

Chinese Hackers Force Penn State to Unplug Engineering Computers

by Michael A Riley
12:00 PM EDT
May 15, 2015

The Old Main building on the campus of Penn State in State College, Pennsylvania.
Photographer: Mario Tama/Getty Images

Penn State University, which develops sensitive technology for the U.S. Navy, disclosed Friday that Chinese hackers have been sifting through the computers of its engineering school for more than two years.

One of the country's largest and most productive research universities, Penn State offers a potential treasure trove of technology that's already being developed with partners for commercial applications. The breach suggests that foreign spies could be using universities as a backdoor to U.S. commercial and defense secrets.

The hackers are so deeply embedded that the engineering college's computer network will be taken offline for several days while investigators work to eject the intruders.

“This was an advanced attack against our College of Engineering by very sophisticated threat actors,” said Penn State President Eric Barron in a letter to professors and students. “This is an incredibly serious situation, and we are devoting all necessary resources to help the college recover as quickly as possible.”

The Federal Bureau of Investigation notified the university of the breach in November 2014, spawning a months-long investigation that eventually found two separate groups of hackers stealing data.

State-Sponsored Hackers

The first group has been linked by investigators to the Chinese government, according to a person familiar with the probe. The second group has not been identified, the university says, but investigators believe it is the work of state-sponsored hackers.

The investigation and remediation efforts have already cost Penn State millions of dollars, said Nicholas Jones, the university provost.

U.S. engineering schools -- Massachusetts Institute of Technology, the California Institute of Technology, Berkeley, Carnegie Mellon, and Johns Hopkins University -- have been among the top targets of Chinese hacking and other intelligence operations for many years. These forays have been for both commercial and defense purposes, and universities have struggled to secure their computers against these advanced attacks.

Active Threat

U.S. officials said Chinese cyber and conventional espionage directed at American universities, companies and research laboratories has increased with the size and sophistication of Chinese computer spying.

One focus of the Chinese is the design and control of unmanned aerial, ground and undersea vehicles, along with the communications systems linking American reconnaissance and navigation satellites to ground stations, said three officials familiar with the issues who spoke on the condition of anonymity to discuss classified assessments and law enforcement matters.

In addition to online activities, the Chinese have sent legions of graduate students to U.S. schools and have tried to recruit students, faculty members and others at both universities and government research facilities, several recent law-enforcement investigations show.

“There is an active threat and it is against not just Penn State but against many different organizations across the world, including higher education institutions,” said Nick Bennett, a senior manager at Mandiant, a security division of FireEye Inc., which aided the university in the investigation.

Universities “need to start addressing these threats aggressively,” Bennett said in an interview.

Aerospace, Defense

Among Penn State's specialties is aerospace engineering, which has both commercial and defense applications important to China's government. The university is also home to Penn State's Applied Research Laboratory, one of 14 research centers around the country that work mainly for the military.

While the lab is not part of the College of Engineering, Jones said experts there have been alerted to the breach and are investigating whether the hackers could have moved there from those networks.

Bennett said the lab's computers are separated from the engineering college by "network-based controls," and its personnel use different passwords. The Applied Research Lab has been doing work for the Navy since 1945 and specializes in undersea propulsion and navigation.

That the hackers were in the network undetected for more than two years raises the possibility that they used connections between computers to move into more highly guarded networks, including defense contractors, government agencies or the Navy, according to the person familiar with the investigation.

Possible Risks

The university has already told 500 partners -- companies, government agencies, and other universities -- of the breach and possible risks. It has also notified 18,000 students and professors whose personal data, including social security numbers, were stored on one of the computers accessed by the hackers.

Jones said Penn State hopes to use its experience to help other universities that are also likely targets for advanced cyberspies and other intruders, providing information on the hack as well as advanced security measures the university is putting in place.

"We don't think we're alone," Jones said.

http://www.bloomberg.com/news/articles/2015-05-15/china-hackers-force-penn-state-to-unplug-engineering-computers