https://www.wsj.com/articles/chinese-hackers-target-universities-in-pursuit-of-maritime-military-secrets-11551781800

POLITICS | NATIONAL SECURITY

Chinese Hackers Target Universities in Pursuit of Maritime Military Secrets

University of Hawaii, University of Washington and MIT are among schools hit by cyberattacks

Woods Hole is the largest independent oceanographic research institution in the U.S. Here, a mechanical engineer at Woods Hole looks on as a crane lifts a specially designed system of sonars and cameras. PHOTO: DAVID L. RYAN/THE BOSTON GLOBE/GETTY IMAGES

By Dustin Volz

Updated March 5, 2019 5:47 p.m. ET

Chinese hackers have targeted more than two dozen universities in the U.S. and around the globe as part of an elaborate scheme to steal research about maritime technology being developed for military use, cybersecurity experts and current and former U.S. officials said.

The University of Hawaii, the University of Washington and Massachusetts Institute of Technology are among at least 27 universities in the U.S., Canada and Southeast Asia that Beijing has targeted, according to iDefense, a cybersecurity intelligence unit of Accenture Security.

The research, to be published this week, is the latest indication that Chinese cyberattacks to steal U.S. military and economic secrets are on the rise. The findings, reviewed by The Wall Street Journal, name a substantial list of university targets for the first time, reflecting the breadth and nature of the cyber campaign iDefense said dates to at least April 2017.

Chinese officials didn't immediately respond to a request for comment, but have denied they engage in cyberattacks.

iDefense said it identified targeted universities by observing that their networks were pinging servers located in China and controlled by a Chinese hacking group known to researchers interchangeably as Temp.Periscope, Leviathan or Mudcarp. Researchers at the U.S. cyber firm FireEye , who have studied the same group, said the iDefense findings were generally consistent with their own intelligence.

The majority of the universities targeted either house research hubs focused on undersea technology or have faculty on staff with extensive experience in a relevant field, and nearly all have links to a Massachusetts oceanographic institute that also was likely compromised in the cyber campaign, iDefense said.

Some have been awarded contracts by the Navy. Others, including Sahmyook University in South Korea, appeared to be targeted because of their proximity to China, and relevance to the South China Sea, the analysts said.

Several affected schools aren't named in the report because of investigative efforts related to the cyber campaign, iDefense said. Other people familiar with the hacking activity said the applied research laboratory at Penn State, among the top earners of Defense Department research dollars, was among the targets. Duke University was another, these people said.

The Chinese hacking group, which multiple security firms and officials have linked to Beijing, is the same one that has been linked to breaches of Navy contractors and subcontractors that have resulted in the theft of sensitive military information, such as submarine missile plans and ship-maintenance data.

Most universities named in the report didn't respond to requests for comment, declined to answer questions about the potential breaches, or said they deployed robust cybersecurity measures to protect their networks. Many said they were unaware of any recent theft of sensitive information from their networks.

The Navy said it recognizes the seriousness of cyber threats and is working to bolster defenses, but didn't comment on the hacking at universities.

Previous cybersecurity research has identified American universities as a favored target for Temp.Periscope because they often possess valuable military research and are viewed as having weaker defenses than the U.S. armed services or defense contractors.

The cyberattacks appeared to leverage trust between academics at different research institutions to craft spear phishing emails that looked like legitimate messages from one university but instead came loaded with malicious software, according to iDefense, former U.S. officials and other security researchers.

"Universities are pretty willing to share information in pursuit of academic information," said Howard Marshall, who leads iDefense threat intelligence operations. "But as a lot of our adversaries have discovered, that is a sweet spot for them to operate."

Brandon Catalan, an intelligence analyst at iDefense, said many of the targeted universities may have fallen victim to the cyberattacks but that researchers couldn't determine which ones had been breached. But iDefense found that nonpublic files belonging to the University of Hawaii's Applied Research Laboratory were laced with malware and sent to other targets, suggesting a successful intrusion at Hawaii. People familiar with the matter said one of those targets was Penn State.

The University of Hawaii declined to comment. A Penn State spokeswoman said the school immediately notifies the government and relevant partners whenever a breach is encountered. She declined to say whether the university had been compromised.

FireEye researchers corroborated some of iDefense's general findings, though it didn't name specific universities that were targeted. They have observed the group attempt to steal maritime research since 2013, and said it had been the most active of any Chinese hacking group it tracked over the past year. Among other tactics, the hackers have at times posed as journalists or the Navy itself when sending malicious emails to

TARGETED TECHNOLOGIES

A U.S. Navy attack submarine. **PHOTO:** ABIGAYLE LUTZ/ZUMA PRESS

Some of the maritime technologies in which a Chinese hacking group has shown interest, according to cybersecurity firms:

- Submarine technologies associated with a Defense Department program code-named Sea Dragon, which iDefense researchers believe could allow U.S. submarines to fire antiship missiles while submerged.
- Deployment of unmanned aerial vehicles from a submerged submarine, possibly through a boat's external trash disposal unit or cruise missile tubes.
- The controlled ascents of objects submerged underwater, possibly related to tests conducted in the Arctic Sea, including changing buoyancy to move vertically in order to avoid collision with obstacles.
- Systems related to undersea acoustic communications, particularly underwater modems.
- Other information related to specific projects sponsored by the U.S. government, including ship-maintenance data, financial figures, plans and drawings and other raw data.

Sources: iDefense, FireEye, other people familiar with the cyber espionage campaign

academic targets, FireEye said.

"They are a full-fledged operation," said Ben Read, senior manager for cyber espionage analysis at FireEye. "And they are not going anywhere."

FireEye this week renamed Temp.Periscope, calling it Advanced Persistent Threat 40, or APT 40, a designation the firm reserves for hacking squads it has high confidence it has correctly identified.

Mr. Marshall of iDefense, formerly deputy assistant director of the Federal Bureau of Investigation's cyber division, said the Chinese want to steal research to match U.S. weapons capabilities and understand the Pentagon's future plans. "To have knowledge of where our military capabilities are going is of extreme importance to them," he said.

Nearly all of the universities shared a common link to Woods Hole Oceanographic Institution, a research and education nonprofit located in Woods Hole, Mass. iDefense said it had high confidence that Woods Hole's network likely had been breached by the Chinese hackers.

With specialization in marine science and engineering, Woods Hole is the largest independent oceanographic research institution in the U.S., boasting notable achievements that include locating the Titanic in 1985, more than 70 years after it sunk.

Some of the targeted schools, including MIT, Penn State and the University of Washington, are affiliated with a unit at Woods Hole known as the Acoustic

Communications Group, which works on undersea communications technology, according to the nonprofit's website.

That group also partners with the Navy's Naval Undersea Warfare Center in Newport, R.I. Reports last year said the Temp.Periscope team had hacked into an unidentified company under contract with the warfare center and stolen secret plans to build a supersonic antiship missile planned for use by American submarines.

The hackers also attacked universities that had sent students to a summer fellowship at Woods Hole between 2016 and 2018. iDefense said students may have brought university devices with them to Woods Hole that were compromised and then infected university computers once the students returned to campus.

Woods Hole announced in October 2015 that it had shut its computer network for several hours due to an aggressive cyberattack that FireEye at the time had determined was carried out by Chinese hackers who sought to obtain "intellectual property derived from research activity."

It is possible the 2015 intrusion was also carried out by Temp.Periscope and may be connected to the more recent activity, people familiar with the matter said.

Christopher Land, general counsel for Woods Hole, said the group believes those hackers were kicked off its network in 2015 and has no reason to suspect its systems have been compromised. Woods Hole had implemented added cybersecurity measures since the 2015 intrusion, but recognized it remained an appealing foreign espionage target due to the nature of its work, Mr. Land said.

Mr. Catalan, the iDefense researcher, said his team's analysis suggested Woods Hole was again compromised. "Just because they [hackers] were removed from a network doesn't mean that they give up," he said.

Write to Dustin Volz at dustin.volz@wsj.com