NATURE | NEWS

'Ransomware' cyberattack highlights vulnerability of universities

Staff at Canadian university given little guidance on how to mitigate future problems.

Brian Owens

17 June 2016

Matej Moderc/Getty

These kinds of attacks — holding data hostage — are becoming increasingly common.

The first Patrick Feng knew about a cyberattack on his university was when one of his colleagues told him that her computer had been infected by hackers and rendered unusable.

Feng, who studies technology and sustainability policy at the University of Calgary in Canada, immediately checked the Dropbox folder that he was sharing with that colleague — and found that it, too, had been compromised.

“The hackers had created encrypted copies of all my Dropbox files and deleted the originals,” he says. “And there was a ransom note demanding bitcoin to unlock them.” Bitcoin is an online, anonymous currency, making it an attractive option for cybercriminals.

The attack, which started on 28 May, left many researchers locked out of their data and university e-mail. Most staff and faculty regained access to the school's networks by 30 May, and e-mail was back up by 6 June.

Feng’s Dropbox folder contained data and draft manuscripts for a research paper that he is writing on innovative ways of teaching research methods to undergraduates, but he wasn't too concerned. His personal laptop was unaffected, and he asked Dropbox to restore his folder to the last saved version before the attack, which the company was able to do in a couple of days.

Locked out

Others were not so fortunate. Two of Feng's colleagues, including the one who had informed him about the hack, had to have the hard drives of their university-issued computers wiped and restored.

A few of the most badly affected faculty and staff have yet to regain full access to their data. But, there is no indication that any personal or school data were released to the public, according to the university. “Research data that was stored on our systems was backed up prior to the attack and remains intact,” says Marina Geronazzo, a university spokesperson.

The university is confident that it will be able to restore all data from those back-ups, she says. But the school did pay a ransom of

Can$20,000 (US$15,500) for the decryption keys as a precaution. They say it will be used only as a last resort.

This kind of "ransomware" attack is becoming increasingly common, says James Scott, a cybersecurity specialist at the Institute for Critical Infrastructure Technology, a think-tank in Washington DC — and universities are hardly immune. In the United States, the education sector is the third most common target for hackers, after healthcare and retail, he says.

In many cases, the ransom money that hackers can extract from their victims is a secondary goal. "Ransomware is the new DDoS," Scott says, referring to a Distributed Denial of Service attack, in which a network of infected computers overwhelms a target with more connection requests than it can handle. Hackers use these attacks as a distraction while they steal data, he explains.

Multiple vulnerabilities

City of Calgary police are still searching for the perpetrator. Past incidents, Scott says, make him suspect that Chinese sources may have been involved. The country has allegedly targeted Canadian researchers before. In 2014, the Canadian government accused "Chinese state-sponsored actors" of hacking the National Research Council, a federal research agency headquartered in Ottawa.

It's a matter of Chinese policy to use espionage to bring their country up to speed, technologically, with the West, says Scott, who is not a part of the investigation. "Universities are a huge target for China because of their advanced research."

Scott says that universities are particularly vulnerable to cyberattacks because they often have multiple overlapping public and private networks, and staff, faculty members or students with infected devices might connect with any number of them. Many labs also have devices "frankensteined" into their networks that were never intended to be there, which opens up new avenues of attack.

Feng says that aside from requiring everyone to change their passwords, the university has provided little guidance on how researchers can better protect themselves against such attacks in the future. He says that it is up to researchers to be aware of the risks, and to take the proper precautions by automatically backing up their data on external hard drives, or to the cloud. "Even though I teach technology policy, and am aware of these kinds of issues, I still thought it was never going to happen to me," he says.

Nature | doi:10.1038/nature.2016.20111