Ransomware criminals are targeting US universities

16 July 2020, by Nir Kshetri

As COVID-19 cases in the U.S. continue to climb, government and higher education leaders have been focused on doing what it takes to protect campus communities from the global pandemic.

But college and university leaders would be wise if they were just as vigilant about protecting their sensitive data from the cybercriminals who are becoming increasingly sophisticated about encrypting the colleges' data and making the colleges pay a ransom to get it back.

One of the latest examples is a ransomware attack that struck the University of California, San Francisco on June 1. In that case, cybercriminals used the NetWalker malware to encrypt data on the servers of the university's school of medicine. This malware targets corporate networks and encrypts the data it finds on the attacked devices. This means that the device owner cannot access data on the device until a ransom in cryptocurrency demanded by the criminal is paid. The criminal gang behind NetWalker has victimized dozens of organizations.

UCSF said that the attackers breached important data related to its medical school faculty's research . It says its COVID-19 research was not affected.

Such ransomware attacks on universities have become common. In 2019 alone, 89 U.S. universities, colleges and school districts became victims of such attacks, followed by at least 30 in the first five months of 2020.

Along with the financial services industry, the education sector is one of the two most common targets of these attacks.

Attempts to extort

I research cybercrime and cybersecurity. I've learned that obtaining ransom payments from their victims is the biggest challenge most cybercriminals face, and that universities perform poorly on cybersecurity. Their vulnerabilities are becoming easier to exploit thanks to cryptocurrencies, such as bitcoin, which make it easier for cybercriminals to extract payments from their victims.

In the case of UCSF, university officials transferred 116.4 bitcoins—the equivalent of US$1.14 million – to the cryptocurrency wallet of the NetWalker gang and received the key to decrypt its own files in return.

NetWalker is sophisticated malware. To distribute ransomware, NetWalker creators rely on phishing and spam as well as other large-scale network infiltration such as hacking unsecured wireless devices connected to Wi-Fi networks.

After penetrating a network, it can render antivirus software useless.

The criminal group behind NetWalker mainly pursues high-value targets, such as the Champaign-Urbana Public Health District in Illinois and Michigan State University.

The creators of NetWalker are believed to collaborate with about 10 to 15 affiliates to distribute the malware. The affiliates, who are often less skillful criminal hackers than the creators of NetWalker, infiltrate a victim's network and infect it with the ransomware. They later split any ransom money obtained with NetWalker's creators.

Why higher ed is a target

In my view, colleges and universities have become attractive targets for cybercriminals because of their weak cybersecurity measures. Research shows that the education sector is the least-prepared to fend off cyberattacks. In a vulnerability test of U.K. universities, hackers obtained sensitive and valuable data in all cases within two hours.

University networks contain highly sensitive information related to research, patents and other types of intellectual property data. These are targets cybercriminals desire.

Most students use the universities' wireless networks to access information. Email addresses and other information about faculty, staff and students are easily available. Cybercriminals can use such information to send phishing emails.

It doesn't help that some universities rely on outdated and insecure software. Or that departments and individual professors store some of the most sensitive data without help from cybersecurity specialists within their universities.

To pay or not to pay

Generally law enforcement agencies and cysersecurity professionals oppose paying ransom. The FBI has suggested that victims report to law enforcement, whether or not they are willing to make those payments.

Extortionists promise to provide the victims with encryption keys for unlocking encrypted data if ransom is paid. NetWalker and some other ransomware criminals threaten to publish victims' data on information leak websites otherwise.

Many victims distrust the extortionists and doubt their promises to unlock data after ransom payments. This fear is well-founded. In 2016, only a quarter of organizations that paid ransoms recovered their data.

Desperate victims may decide to pay, hoping that the criminals behind the attacks fulfill their promise to decrypt data. Cornell University reportedly bought bitcoins to pay to extortionists in case of a future ransomware attack. If companies rely on data, paying ransom could be less costly than the alternative.

Recently, ransomware criminals are becoming more selective, going after only victims for whom data is extremely important.

Some recent victims of NetWalker also reported that they successfully recovered most of their data after paying the ransom. In March, NetWalker had hijacked the computer networks of the Champaign-Urbana Public Health District in Illinois, which serves 210,000 people including the University of Illinois. After paying a $350,000 ransom, the Champaign-Urbana Public Health District retrieved 99% of its files.

A growing number of organizations now buy cyber insurance to protect against future losses from these attacks. An insurer, for example, paid all but $10,000 of the Champaign-Urbana Public Health District's ransom.

Tracking ransomware perpetrators

Most ransomware criminals, however, operate from jurisdictions that don't cooperate with the U.S. or European authorities fighting cybercrimes. For instance, the criminals behind NetWalker are believed to operate from Russia or other Commonwealth of Independent States.

To shore up their digital security, universities should mandate strong passwords and encourage all faculty, students and staff to report fake emails and other incidents. It would also help if they could constantly back up important data and purchase cyber insurance.

Provided by The Conversation

APA citation: Ransomware criminals are targeting US universities (2020, July 16) retrieved 6 December 2022 from https://techxplore.com/news/2020-07-ransomware-criminals-universities.html