THE STRAITS TIMES

Cyber attacks on NUS, NTU: Singapore latest target of ever-growing cyber threat

The attacks by hackers on NUS and NTU, discovered last month, were aimed at stealing government and research data. PHOTO: BLOOMBERG

PUBLISHED MAY 13, 2017, 5:00 AM SGT

Hackers using advanced persistent threats require much sophistication and resources

Irene Tham Senior Tech Correspondent (mailto:itham@sph.com.sg)

Cyber attacks on governments and institutions have become a weapon of choice - and Singapore has not been spared the threat, said the Cyber Security Agency (CSA) of Singapore.

"Attackers are not just targeting government systems; they are (also) looking for any network that is remotely related to the Government," said Mr David Koh, chief executive of CSA. "Attackers are... always looking for the weakest link to exploit."

The attacks by hackers on National University of Singapore (NUS) and Nanyang Technological University (NTU), discovered last month, were aimed at stealing government and research data, CSA revealed yesterday.

The breaches were said to be advanced persistent threats (APTs) in which hackers gain unauthorised access to and lurk within computer networks undetected for a long period of time.

ST Explainer: What is APT?

Advanced persistent threats (APTs) are stealthy and continuous computer hacking processes to gain intelligence or steal information from another party.

The hackers gain unauthorised access into and lurk within computer networks. They exploit vulnerabilities in systems with sophisticated techniques using malware.

Once the malware is planted in the network, it gives hackers a back door to remotely monitor and extract data from the target network or system.

In 2010, the Stuxnet worm, designed by the United States and Israel, made its way into Iran's Natanz facility and infected specific industrial control systems through an infected USB drive.

The malware quickly propagated and temporarily crippled Iran's nuclear programme, though computer screens showed nothing amiss.

Irene Tham

State-sponsored APTs have plagued the French presidential election, which concluded last week, and last year's US presidential election, said security software firm Trend Micro.

Newly elected French President Emmanuel Macron's campaign team was repeatedly hit by phishing e-mails to trick his staff into parting with their passwords. Confirming the attacks, Mr Macron had said no campaign data was compromised. The same hacking group, dubbed Pawn Storm, was also believed to be behind the attacks last year on the e-mail accounts of the US Democratic National Committee to undermine Mrs Hillary Clinton's presidential bid.

Trend Micro said that one in five US organisations has suffered a cyber espionage-related attack in the past year.

Related Story

NUS, NTU systems hacked: What is 'advanced persistent threat'

Related Story

Cyber attacks on NUS, NTU in bid to steal sensitive data

Mr Nick Savvides, a security advocate for Asia-Pacific and Japan at cyber security software firm Symantec, said cyber attacks are either financially or politically driven.

"State-sponsored attacks are highly sophisticated and capable of obfuscating their source," he said.

Money could also be a motive.

Mr Aloysius Cheang, executive vice-president of global computing security association Cloud Security Alliance, said: "There is definitely valuable research data of commercial value."

In the case of NUS and NTU, hackers may have also assumed that the universities' systems had links to government systems, Mr Cheang added.

Mr Bill Taylor-Mountford, American security intelligence firm Log- Rhythm's vice-president in Asia-Pacific and Japan, said: "Any entities using APT need to have considerable resources."

Such threats demand a lot of sophistication, he added.

In a Facebook post yesterday, Communications and Information Minister Yaacob Ibrahim urged everyone to do their part to defend important data. For instance, individuals can practise good cyber hygiene.