Publication: The New Paper, p 6
Date: 9 November 2013
Headline: Curious? Clicked? Your PC may be infected

PMO, Istana sites 'compromised'

Curious? Clicked? Your PC may be infected

Reports by RONALD LOH
rloh@sph.com.sg

Were you one of those who were curious about the images which appeared on subsites of the Prime Minister's Office and the Istana?

Did you click on the URL posted on some forums?

Well, your computer may now be infected with malware or viruses, said the Infocomm Development Authority (IDA) yesterday.

Between 11pm on Thursday and 12.20am on Friday, hackers created an alpha-numeric code which, when pasted on a search engine of the two sites, led to pictures posted by the hackers. (See other report.)

But IDA said the two subpages were removed within 15 minutes and that they are taking measures to strengthen all government websites.

This comes after an alleged call by the hacker collective Anonymous to mark Nov 5 with a protest.

On that day, a spike in hacking activity showed up on IDA's radar.

Despite unusually high traffic to many government websites on Nov 5, IDA said there were no successful cyber intrusions or denial-of-service attempts on both transactional and non-transactional government sites.

But even a hacking attempt is illegal and could be punishable under the Computer Misuse and Cybersecurity Act, said criminal lawyer Rajan Supramaniam.

"Once you make an attempt, there is an intention to hack. If you're traced and caught, you have to be prepared to face the consequences," he said.

Last week, Anonymous allegedly threatened to bring down Singapore's infrastructure in a show of protest against the Internet licensing framework.

On Wednesday, Prime Minister Lee Hsien Loong said the Singapore Government "will spare no effort to track down" anyone who attempts to bring down the Republic's cyber infrastructure.

Cyber security experts told The New Paper on Thursday that a lot of resources are needed to track down these hackers.

But experience shows it can be done despite sophisticated tactics employed by hackers to cover their tracks.

'Compromise' explained

A subpage of the Istana and Prime Minister's Office (PMO) websites each were compromised on Thursday night and yesterday morning, said the Infocomm Development Authority (IDA).

In a statement released yesterday, IDA said authorities detected a "compromise" in a subpage of the PMO website at about 11.15pm on Thursday. A similar "compromise" was detected in the Istana's page just after midnight yesterday.

The affected subpages were taken down within 15 minutes, said IDA. It said that both main websites remained functional.

"There was a vulnerability in the search engine function of both websites," said Mr James Kang, IDA's assistant CEO, government chief information office.

First, the hacker created images of the PMO and Istana's websites using components of both pages and his own images, said IDA.

He then exploited the vulnerability in the websites' search engine to direct people to the image, which IDA said does not belong to the main website.

It is believed screenshots of the two images were also shared on forums.

The matter is under investigation by IDA and the police.

Meanwhile, IDA said it is strengthening all government websites.

This includes checking of vulnerabilities and software patching.

IDA also said it received an unusually high number of denial-of-service attempts on Tuesday but said there were no successful cyber intrusions.

Mr Alex Nian, manager of IT firm SecureIT-NET, said hackers usually gather networks of infected computers – known as botnets – by hacking into PCs and installing malware in them.

They then use botnets to carry out hacking activities, such as denial-of-service – making a network/service unavailable to users by diverting a high amount of traffic to the website – or remotely controlling the botnets to hack into government servers.

VIRAL VIDEO

They could have even used an infected computer to upload the video, which went viral last week.

These infected PCs could be all over the world, and locating them will be difficult, said Mr Nian.

"Our Government would have to seek permission from the country's Internet Service Providers to get the IP address of these overseas computers. Their requests could take a while to be processed.

"The request could even be rejected due to privacy laws," he said.

There would also be no guarantee the original computer can be traced, he said.

Is it worth the effort to track them down?

Yes, said political analyst Eugene Tan, a Singapore Management University law professor.

"It would send a strong signal that our Government has the resolve and also to deter future perpetrators," he said.

Given that cyber attacks have now become a transnational crime, there is a greater need for countries to work together, said cyber security expert Eric Chan, Fortinet's regional technical director for South-east Asia and Hong Kong.

An example would be Singapore's initiative to set up a cybercrime working group at the 9th Association of South East Asian Nations (Asean) Ministerial Meeting on Transnational Crime in September.

Regional law enforcement agencies will then have a special platform to discuss strategies to fight cybercrime.

Said Mr Chan: "The Internet is without borders and cyber criminals often reside outside the country where the attacks take place.

"Cooperation among international authorities is extremely important in bringing cyber criminals to justice, and that's where organisations like Interpol and Asean can play a part."

"The PMO's website incident was a result of a typical cross-site scripting where the cyber criminal exploited the 'search' function on the website, and injected content from external sources. In this particular instance, the cyber criminal had redirected the URL to the criminal's intended image.
— Software security firm Trend Micro spokesman saying it's not a hack