KEEPING HACKERS AT BAY

Threat by hacktivist group Anonymous highlights vital need to secure nation's data, IT systems

IZWAN ISMAIL
KUALA LUMPUR
news@nst.com.my

THE recent alert from The National Cyber Security Agency (Nacsa) for government agencies to brace for a cyberattack from malicious players underscores the need to secure the nation's data, information technology infrastructure and systems.

The alert was issued after a social media user, called Anonymous Malaysia, published a video threatening to hack government websites.

ATTACK CONSEQUENCES

According to Trend Micro Malaysia and Nascent Countries' managing director Goh Chee Hoh, a potential attack on the systems that provide a gateway to sensitive and personally identifiable information, as well as the nation's infrastructure, will have far sweeping consequences, especially as the country is grappling with Covid-19.

Hacktivist groups, such as Anonymous Malaysia, are based on loose memberships, with members joining and leaving at any point in time and may also form alliances with other hacking groups for certain hacking campaigns.

"Therefore, it is crucial for government agencies to stay vigilant, secure all vulnerable endpoints, and keep systems and applications patched and up to date, especially as employees may be working remotely," said Goh.

Goh Chee Hoh

Hacktivists' attacks can cause many problems to the government, such as web defacements. This includes changing the contents of a website to show their message.

Besides that, they can also launch denial of service attacks to render a government agency website, for example, inaccessible to users.

Data leaks, as most websites contain databases, may also happen, as well as doxxing, which is the act of revealing personal information, such as addresses and phone numbers, mostly of notable public figures such as politicians or celebrities.

HOW HACKTIVISTS OPERATE

Trend Micro said hacktivists normally don't have a very high degree of technical proficiency, as compared with an experienced penetration tester.

However, this lack in technical proficiency is compensated by their use of various hacking tools, coordinated effort to scan for vulnerable websites and sharing of information between members.

"In the end, because of the volume of probing hacktivists carry out, they would likely be able to perform a successful attack.

"This is probably the biggest challenge for security professionals as it only takes a single successful hack for the attackers to claim victory," said Goh, adding that to minimise the impact of a hacktivist campaign, all relevant parties need to be alerted.

"In-house staff, as well as third-party service providers, should be included in briefings and be put on-call, ready to resolve any security incident.

"As it is almost impossible to determine what will be attacked and how, it is important to be ready to resolve the issue and make the successful hack as short-lived as possible."

THREAT SPIKE

Kaspersky general manager for Southeast Asia Yeo Siang Tiong said the current digital shift and the Covid-19-triggered disruptions have indeed created a spike on threats against individuals and public and private institutions in Malaysia and globally.

Yeo Siang Tiong

"The number of unique malware samples we have detected last year was at 360,000 daily, on average, which is a 5.2 per cent uptick compared with the year before," said Yeo.

"We have seen multiple, massive data breaches last year, not just in the country, but across the Southeast Asia region.

"As new malware and more sophisticated techniques are being employed by cybercriminal groups every day, you need to keep your systems intelligent and up to date by incorporating global threat feeds and threat intelligence reports, which provide in-depth visibility and detailed information about the most recent threats targeting organisations like yours."

Yeo applauds the efforts taken by the government to strengthen the security of both public and private networks in the country.

"Last October, the prime minister announced the Malaysia Cyber Security Strategy 2020-2024, which aims to step up the nation's cybersecurity preparedness and capabilities," he said.

"And just last week, he also spoke during the first Asean Digital Ministers' Meeting, where he emphasised the critical link between the region's digitalisation drive, during and after the pandemic era, and the need to beef up both regional and national security capacities through improved coordination across the Asean countries."

security policies. Continuous training and education go a long way towards enhancing skills and knowledge to build a proficient workforce for the digital age.