Saturday, June 27, 2020

THE BUSINESS TIMES

BT businesstimes.com.sg

Cyber threats against Singapore businesses surge in 2019: CSA

By Rachel Chia
rchia@sph.com.sg
@RachelChiaBT
Singapore

THE frequency and sophistication of various cyber threats such as website defacements, phishing incidents, and malware activities rose in Singapore last year, said a report published by the Cyber Security Agency (CSA) of Singapore on Friday.

The report, which outlined cyber threat trends for the year, also featured a special section on threats related to Covid-19, in which it noted that cyber-threat actors are exploiting the panic and fear caused by the pandemic to conduct malicious activities.

These actors range from cyber criminals seeking financial gain to groups attempting to gain access to classified information. Cybersecurity vendors observed that successful Covid-19-themed phishing attacks were on the rise through the first few months of 2020.

In its Singapore Cyber Landscape 2019 report, the CSA noted the rise in cyber threats targeted at various local industries, such as e-commerce, banking and finance. These cyber threats included common malicious activities such as website defacements, phishing incidents and malware infections.

Last year, 873 websites were defaced, up from 605 in 2018. The majority of these websites belonged to small and medium-sized enterprises (SMEs) from sectors such as education, finance, manufacturing and retail.

The report attributed the increase in cases in part to an Indonesia-based hacker group, and ongoing developments in the Middle East.

As for phishing activity, 47,500 Singapore-hosted phishing URLs were detected last year, a sharp increase from 16,100 in 2018.

Local firms that fell victim included technology firms, banking and financial organisations, and e-mail service providers.

The most commonly hit government organisations were the Immigration & Checkpoints Authority, Ministry of Manpower and Singapore Police Force.

CSA last year also detected about 530 unique "command-and-control" servers in Singapore, compared to 300 the year before. Such servers are computers controlled by cyber criminals to send commands to compromised systems infected with malware. Close to 370 malware variants were detected in Singapore last year.

Meanwhile, a daily average of about 2,300 botnet drones with Singapore Internet protocol addresses had been observed, the report said. Botnets are a network of compromised computers and smartphones infected with malware and controlled by a criminal to perform malicious tasks.

The CSA report attributed the rise in cases in part to an Indonesia-based hacker group, and ongoing developments in the Middle East. PHOTO: REUTERS

CSA received 35 reports of ransomware cases last year, up from 21 cases in 2018. The majority of organisations that fell victim to ransomware attacks were from the travel and tourism, manufacturing and logistics industries.

The report also noted a global rise in cyber threats capitalising on the Covid-19 pandemic to target frontline organisations, businesses and individuals.

"Such malicious cyber activities emerged globally in late December 2019 and may persist beyond 2020," it added.

CSA chief executive David Koh said the Covid-19 outbreak had provided threat actors with new opportunities and attack surfaces to capitalise on.

"As one of the most connected countries in the world, Singapore remains a target for cyber attacks and cyber crime," he said. "Threat actors have continued to evolve their tactics, resulting in an intensification of malicious cyber activities in 2019."

Cyber crime accounted for more than a quarter of all crimes in Singapore last year, with the total number of reported cases at 9,430 in 2019, up from 6,215 in 2018.

The report identified two trends that are expected to increase the cyber security "attack surface": the transition by organisations into cloud computing, and security risks associated with working from home in the post-pandemic "new normal".

Other trends expected to have an impact on cybersecurity include artificial intelligence (AI), 5G, the surge in Internet of Things devices, and quantum computing.