Singapore considers steps to combat phishing, cryptojacking amid steep rise in cyber attacks

Published 22-Sep-2020 by
Yixiang Zeng, Regulatory Intelligence

The number of cyber attacks reported in Singapore has risen sharply, and many financial institutions are concerned that a dearth of funds to invest in digitisation may hamper their ability to recognise and detect malicious wrongdoing, a cyber-security firm has said.

"Almost half — 41% — of businesses continue to [say] that the high costs of investment [together with] a lack of financing and funding are major barriers holding them back from digitalisation," Stephan Neumeier, managing director, Asia-Pacific at Kaspersky, said during an online press briefing.

"The implications of this statistic are significant, as it means cyber security may not be a key priority for businesses during this period of cost-cutting."

Phishing attacks increased by 61% to 89,351 incidents in Singapore during the first six months of the year, from the same period last year, amid the COVID-19 pandemic.

Malicious mining, also known as cryptojacking, is emerging as a major cyber-security threat for small- and medium-sized companies in Singapore, according to Kaspersky. The cyber-security firm said it had prevented 14,141 mining incidents against business devices in the city-state during the first half-year, a 90% rise on the same period in 2019.

Neumeier encouraged the sector to be more vigilant about tackling malicious conduct, although he recognised that the pandemic might put a strain on companies' detection capacities.

Singapore v Southeast Asia

Cyber attacks in Vietnam increased by 70% to 464,316 in the first six months of the year, from the same period last year, while Indonesia experienced the lowest percentage increase year-on-year — attacks were up by 18.2% to 406,229.

"Although Singapore [89,351] continues to fare better than ... Indonesia [406,229], Malaysia [269,533], the Philippines [125,473], Thailand [247,621] and Vietnam [464,316] [and has] witnessed the lowest volume of phishing attacks in Southeast Asia, the 61% increase suggests that more can be done by Singapore's small- and medium-sized companies to improve their cyber security," Neumeier said in the press briefing.

Emerging IT industries present "ideal target"

Information technology industries in Southeast Asian countries such as Vietnam have grown dramatically in size and sophistication in recent years, according to Kyung Kim, head of cyber security, Asia-Pacific at FTI Consulting.

"However, their cyber-security [protection] has not matured at a comparable pace to their wider IT environments," Kim told Thomson Reuters Regulatory Intelligence via e-mail.

"For a cyber criminal looking to cryptojack, [for example], this creates an ideal target. They can access the computing power they require to mine cryptocurrency without the end-user being aware, allowing them to successfully conduct malicious attacks against untrained users."

Combatting cyber attacks

Against such a backdrop, Neumeier said companies should implement measures to fight against cyber attacks, including phishing and cryptojacking.

"[Companies should] enforce the use of legitimate software, downloaded from official sources," he said. "[They should] configure wi-fi encryption. It is imperative to configure your network connection correctly and set your router's log-in and password regularly."

Keeping track of server load and monitoring web traffic would also help firms to recognise and detect any malicious mining, as illegal miners' activities can cause increases in web traffic and high server loads, or even surges in electricity, he said.

Cultural and regulatory implications

Despite the introduction of sophisticated IT systems and processes to help companies develop their cyber-security procedures and build resilience, company staff can often be the weakest link in the equation, Kim said.

"Cyber security is everyone's responsibility and you should ensure that a culture is promoted throughout your business where employees are effectively trained to identify anomalies, such as suspicious emails, and have a robust escalation process in place to flag potential incidents as they arise. Also, now more than ever in this current remote-working environment, it is important to maintain a patching regime to ensure your systems remain secure and up-to-date," he said.

Kim pointed out that cyber criminals are not bound by geography or physical location. "They can initiate sustained cyber attacks from the other side of the world, so it can be challenging to track them down and take action," he said.

"As global cyber threats continue to evolve and grow ever-more complex, it is going to be important for both public and private sector institutions to work together. Sharing knowledge and learning from previous incidents will allow organisations and nation states to take the right steps to mitigate future cyber risk and work to improve global resilience."

Complaints Procedure

Produced by Thomson Reuters Accelus Regulatory Intelligence 22-Sep-2020