Southeast Asian firms reporting surge in cryptojacking, warn security experts

Published 29-Jun-2020 by
Yixiang Zeng, Regulatory Intelligence

Financial services firms and cryptocurrency exchanges in Southeast Asia have been urged to increase their vigilance around cryptojacking and other forms of digital-currency-enable crimes. The warning comes as the number of illegal attempts to obtain cryptocurrency surged in the first quarter of 2020, sources have said.

Research carried out by cyber-security firm Kaspersky among small and medium-sized enterprises (SMEs) with 20-250 employees detected more than one million mining cases during the period — a 12% increase on the same period last year.

Cryptojacking is a type of malicious mining whereby cyber criminals install a malicious programme on a targeted computer or through fileless malware without the user's knowledge.

"This allows them to harness the victim's processing power for their own nefarious purposes," Siang Tiong Yeo, Kaspersky's general manager, Southeast Asia, told Thomson Reuters Regulatory Intelligence (TRRI) via e-mail. "[It can also] occur if a victim visits a site that has a mining script embedded in the browser," he said.

The proceeds are then typically laundered through cryptocurrency "tumblers" and digital currency exchanges, or moved into so-called privacy coins, to conceal the indelible digital trail left behind in cryptocurrency transactions.

The number of cryptojacking cases detected was also significantly higher than the number of phishing attempts — 834,993 — and the number of ransomware attacks — 269,204 — detected in the same group of companies during the period, according to Kaspersky.

Reasons behind the rise of cryptojacking

The increase has been fuelled by the COVID-19 pandemic, as home working has enabled cyber criminals to access personal laptops or desktops more easily, according to Andrew Mahony, head of cyber solutions and risk, Asia at professional services firm Aon.

"These devices do not typically have the same security controls and patching frequency that we would expect from corporate devices and are therefore susceptible to compromise," Mahony told TRRI via e-mail.

Internet users in other parts of the world are likely to be better educated about the prevalence of such scams than those in Southeast Asia, and are therefore better equipped to recognise malicious links and schemes, said Marcus Lim, chief executive officer and co-founder of the digital asset provider Zipmex.

Cryptojacking: Singapore v Indonesia

Statistics produced by Kaspersky set out the number of malicious mining attempts in each of the countries in Southeast Asia, and assign each country with a global ranking. A high ranking means that the country has experienced fewer malicious mining attempts, Yeo said.

Indonesia ranked third on the list,with 481,944 cases detected in the first three months of the year. This was largely attributable to its bigger population and to the relative youth of its internet users, Yeo said.

Signs and prevention of cryptojacking

Cyber-security experts said it is possible to alert victims if their devices have been taken over for illegal mining purposes.

"Users should also be on the lookout for signs of cryptojacking compromise, which may include a slowing down of systems, the overheating of components, or altered settings," Mahony said.

Other signs might include a substantial increase in electrical consumption and usage of central processing units, or batteries running down more quickly than usual.

Companies are encouraged to use secure virtual private networks, operate a strict access policy to restricted sites, ensure patching is up-to-date and train employees to identify cyber threats.

"Implementing the right cyber-security solution for every aspect of your business operations, both hardware and software-related, is essential," Yeo said. "Use a dedicated endpoint security solution equipped with web and application control [and] anomaly control and [employ] prevention components that monitor and block suspicious activity on the corporate network."

Regulatory implications

Some digital asset providers have called for harsher punishments for those found to have carried out malicious mining attacks.

"The regulators should make it illegal, together with harsher punishments for cyber crime as a first step to deter hackers from carrying out cryptojacking," Lim said. Regulators needed to work with digital asset exchange providers to educate the public, he said.

Tse Gan Thio, cyber risk leader at Deloitte Southeast Asia, said responsibility for combating cyber crime and cryptojacking should rest with users, cryptocurrency exchanges and custodians.

"Exchanges and custodians must continue to enhance their monitoring and surveillance capabilities in combating illicit and unknown transactions," he said. "Regulators could facilitate this by enhancing cyber-hygiene requirements of market participants and encouraging collaboration through market and cross-border information or intelligence sharing so that pre-emptive actions can be taken."

Complaints Procedure

Produced by Thomson Reuters Accelus Regulatory Intelligence 29-Jun-2020