Financial consortium steps up efforts to fight COVID-19 themed cyber threats in Asia

Published 13-May-2020 by
Yixiang Zeng, Regulatory Intelligence

Financial institutions across South-East Asia, especially smaller ones, are at a greater risk of falling victim to organised cyber crime amid the COVID-19 pandemic, said Brian Hansen, executive director at the Financial Services Information Sharing and Analysis Centre (FS-ISAC). FS-ISAC, which aims to help financial institutions reduce cyber risks within the international financial system, has monitored and investigated a list of more than 92,000 high-risk website domains that have a COVID-19 theme.

The findings showed fraudsters and cyber criminals have been using these domains to take advantage of the crisis to commit financial fraud, scams and potentially malicious activity, Hansen said. As of early April, 1,500 domains had been identified as high-risk, containing both a COVID-19 and a financial theme, data in an FS-ISAC report showed.

"According to domain name keyword analysis, the biggest category by far is loans, with 44% of domain names containing keywords such as loan, financing, credit. This is likely malicious actors and scammers attempting to lure people in financial need caused or worsened by the COVID-19 crisis," the report said. Some 14% of the domains identified included insurance as a keyword and 3% included bailout, tax relief or stimulus.

Cyber crime: phishing attack

In the first quarter of 2020, the number of FS-ISAC member submissions reporting phishing attacks to the organisation's intelligence-sharing portal increased by 33%, Hansen said during a media briefing.

"This indicates a broader trend visible across the threat landscape, as cyber criminals look to leverage the uncertainty and panic around COVID-19 to their advantage in phishing campaigns and other tactics."

In one case, cyber criminals sent out COVID-19-themed phishing e-mails with malicious Microsoft documents attached. Such e-mails are intended to lure targeted victims to fake websites which aim to collect their credentials, according to a recent KPMG report on COVID-19-themed cyber threats.

Raising awareness

Against the backdrop of the novel coronavirus pandemic, raising awareness and information sharing are essential if organisations are to mitigate cyber threats and risks, Hansen said.

"The biggest trend is the [need for] awareness, as some of the countries or markets potentially have less experience when it comes to cyber-security tools," he said. FS-ISAC wanted to help organisations gain a better understanding of such tools to help them overcome cyber threats amid the pandemic, he said.

Had COVID-19 not happened, institutions might well have encountered other black swan events, such as natural disasters, and that hackers might well employ similar malicious strategies to target financial institutions to commit financial crimes, Hansen said.

As a result, the best way to keep on top of cyber crime was to raise awareness among team members and keep people aware of the heightened risk of organised cyber crimes such as phishing attacks.

Intelligence sharing

Information or intelligence sharing is another good way to offset cyber threats amid the crisis, FS-ISAC said.

The organisation shares a weekly watch report with the banking community in the APAC region in a bid to keep it informed about the latest trends in cyber threats and financial crime.

FS-ISAC's investigation of high-risk website domains showed that cyber criminals adopt fast-switching strategies to entice targeted victims. Information and intelligence sharing among firms has therefore become more important than ever, the consortium's report said.

Sharing advice on how to avoid cyber attacks and stay safe, as well as the provision of regular updates within an organisation, also will also help to tackle cyber crime-related issues amid the COVID-19 pandemic.

FS-ISAC is headquartered in the United States, with branch offices located in Singapore and the UK.

THOMSON REUTERS™