Securities Industry Risk Group (SIRG)

Global Cybersecurity Brief – April 2021

Navigating Cyber 2021 – The Case for a Global FinCyber Utility

FS-ISAC report finds cybercriminals and nation-state actors are converging, increasing cross-border and supply chain attacks. "Trying to outpace evolving cyber threats diverts resources from a financial firm's core business," said **Steve Silberstein, FS-ISAC CEO**. "As the global fincyber utility, FS-ISAC enables industry-wide cross-border sharing to pool resources, expertise, and capabilities to manage cyber risks and incident response." The report outlines the today's top threats:

- Convergence of nation-states and cybercriminals: Nation-state actors are leveraging the skills and tools of cyber criminals, either knowingly or not, to enhance their own capabilities.
- Third-party risk on an upward trend: Suppliers to financial firms will continue to be lucrative targets for threat actors, as shown by three highly visible incidents in the last two quarters.
- Cross-border attacks will increase: Cyber criminals test their attack in one country before hitting multiple continents and sub-verticals, as shown by a DDoS extortion campaign targeting roughly 100 financial institutions in months.

The Navigating Cyber 2021 report is derived from FS-ISAC's rigorous threat intelligence monitoring maintained by its intelligence operations team. The intelligence is sourced from FS-ISAC's thousands of member financial firms in more than 70 countries and further augmented by analysis by the Global Intelligence Office. Multiple streams of intelligence were leveraged for the curation of the round-up, which examined data across a one-year period from January 2020 to January 2021.

Guidance on Adoption of Zero Trust Security Policy Published by NSA

The US National Security Agency (NSA) recently published **guidance** on how organizations can integrate a Zero Trust policy withing their organization. The **document** highlights the challenges on how to execute the policy, while also detailing recommendations to implement the model within existing networks. The NSA does not recommend moving to a Zero Trust model all at once. Organizations should focus on securing critical data and access paths by eliminating trust as much as possible.

Fear and Uncertainty are the Real Friends of Threat Actors

In a year that provided so many changes to our daily work and personal lives, 2020 was also a year that provided a perfect storm for **threat actors**: the workforce was predominantly working remotely, a hyped-up political environment and surging cryptocurrency prices. Technology is trying to keep up with the ever-increasing threat landscape where threats that were originally thought to be a few years away are now happening in real time. A few of the major findings from 2020 are: Ransomware reaches new heights, more 'never-before-seen' malware variants were identified and intrusion attempts are up as attack patterns change.

Office 365 Phishing Campaign Targets Executives

While organizations strive to educate their employees on the importance of strong passwords, **data shows** that roughly 76 percent of employees at the world's largest organizations are still reusing passwords across personal and professional accounts A sophisticated and highly targeted Microsoft Office 365 phishing campaign is **aimed at company executives, executive assistants, and financial departments**. In a few instances of this attack, the attackers targeted newly selected CEOs before their appointments were made public. The campaign began in early December 2020, and according to researchers is still on-going. The threat actors are leveraging phishing kits and other sophisticated methods. The phishing emails are made to look like messages from the company, carrying fake alerts with subjects about either 'Important Service Changes' or 'Important Security Policy Update', and include a malicious attachment which leads the target to a spoofed Microsoft-themed notice, then takes the recipient to a fake Office 365 login page.

Office 365 Phishing Campaign Targets Executives

Microsoft has **released updates** to address four previously unknown or 'zero-day' vulnerabilities in Exchange Server that were being used in limited targeted attacks, according to Microsoft. Microsoft is urging customers to apply the updates as soon as possible due to the critical rating of the flaws. The flaws affected Exchange Server 2013, Exchange Server 2016, and Exchange Server 2019. Exchange Online is not affected. The FS-ISAC has two alerts are already out on SHARE about Microsoft Exchange Server 0-Days **Vulnerabilities** and **Member Reports**. Cybersecurity and Infrastructure Security (CISA) partners have observed active exploitation of vulnerabilities and issued an alert (**Alert AA21-062A**).

This monthly update is brought to you by the Financial Services Information Sharing and Analysis Center (FS-ISAC) in coordination with the Investment Industry Association of Canada (IIAC), the International Council of Securities Associations (ICSA), the Financial Services Institute (FSI), the Insured Retirement Institute (IRI), the Securities Industry and Financial Markets Association (SIFMA) and the SPARK Institute.

The information provided in this monthly newsletter highlights cybersecurity topics and emerging threats to the securities industry globally. It is intended to increase the cybersecurity awareness of an organization's end-users and to help them interact in a more secure manner. This newsletter is not intended to replace the benefits of joining FS-ISAC. Learn more at fsisac.com.