Securities Industry Risk Group (SIRG)

Global Cybersecurity Brief – December 2020

New Phishing Campaign Tied to Old Botnet

Researchers have **uncovered a phishing campaign** where the recipient receives a message stating that they have been fired from their job and the message attempts to install two types malware, Bazar and Buer using the Trickbot botnet. The Bazar malware helps the attacker maintain a persistent presence and the Buer malware delivers the ransomware to the victims' system and networks.

These **phishing emails**, which first appeared in October, contain a link that opens either a Google doc or Constant Contact file that is supposed to contain a list of employees who have been terminated. When opened, these documents display another link that tells the victims "If download does not start, click here." This second link will then download either Bazar or the Buer or both and will attempt to decrypt another payload which turns out to be Trickbot. The report states that once the backdoor is download and successfully installed, the attacker can remotely execute commands, exfiltrate sensitive data and deploy other payloads.

SEC Chairman Reminds Corporate America to Stay Vigilant

Securities and Exchange Commission (SEC) Chairman Jay Clayton is reminding corporate America to remain extra vigilant regarding their cybersecurity practices. While the pandemic and elections continue to dominate the news, threat actors remain active in looking for opportunities to infiltrate organizations. The SEC has issued warnings on **Ransomware and credential compromises**. Organizations need to ensure their employees are utilizing multi-level authentication as well as strong passwords.

FS-ISAC Insights - Laser-focused on the intersection of financial services and cybersecurity

The financial services industry is going through a rapid evolution. Customers now expect more speed and convenience, frictionless and borderless transactions, digitization of all types of services, and much more. This brings exciting new opportunities to the market. It also means that the attack surface continues to grow and evolve in novel ways. Amid all the clutter and the noise, FS-ISAC Insights is your go-to destination for clarity and perspective on the future of finance, data, and cybersecurity as seen by C-level executives around the world. When you **subscribe to FS-ISAC** Insights and you'll get a quarterly email with new insights from top names in the industry.

Living in a Zero Trust World

Zero Trust is enabling organizations and their employees to work safely and securely, regardless of their location. **Zero Trust** has laid the groundwork for future security measures during a time when they are needed now. With the majority of the workforce still accessing their organization's date remotely, Zero Trust has the capability to leverage tools, multi-factor authentication and active session-based risk detection, to fulfill higher levels of security.

COVID-19 Concerns Put Branch Exams on Hold

The Financial Industry Regulatory Authority (FINRA) has a proposal pending that would allow broker-dealers the ability to **conduct on-site branch exams remotely** until the end of 2021, this proposal comes as many broker-dealers have not conducted branch exams amid Covid-19 concerns. FINRA requires BDs to inspect branches that do not supervise other locations at least once every three years. Offices of supervisory jurisdiction and branches that supervise other locations must be examined annually.

Broker-Dealers could face challenges while conducting remote inspections such as malfeasance by an individual or outside business activities could be especially hard to spot from a remote inspection. With remote exams it would be harder to thoroughly inspect an office or look through files. Because of the three-year exam cycle, some branches may end up with as much as a six-year gap between on-site inspections. Broker-Dealers will now need to carefully evaluate how they are handling ongoing supervisory responsibilities in this remote environment.

Know Your Enemy

With its attractive business model and multiple revenue streams, ransomware is a growing threat to financial services and their third-party suppliers.

There are many steps you can take to prevent attacks, but threat actors are evolving their tactics all the time. If attacked, will you pay the ransom? Industry-specific threat intelligence is a critical tool in helping you decide.

With ransomware attacks growing globally, for Cyber Security Awareness Month we've released a **ransomware report** to help your financial institution prepare and combat ransomware.

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.