Integrating Fraud Detection Solutions into Security and Fraud Operations

When reviewing fraud detection and solutions to reduce possible losses suffered due to fraud, an organization should ensure they can easily **integrate solutions** into their operations. Oftentimes, this is not the case given the level of scrutiny that solutions deserve. Questions an organization should consider while doing research: Is the solution easy to deploy? What is the ease of consuming the solution? Is the solution easy to operate? Resources are easily stretched when implementing new protocols. Organizations should know what resources are required for implementation of solutions, as well as how the integration of their daily workflow will be impacted.

Mamba Ransomware

The United States Federal Bureau of Investigations (FBI) and Department of Homeland Security (DHS) have **issued a warning** about the Mamba Ransomware. This ransomware utilizes a legitimate, open-source encryption software, DiskCryptor **to lock victims out of their systems**. The alert was issued after a spike in the Mamba ransomware attacks noticed by federal authorities. The Bureau states this ransomware warrants a high-level warning because it is difficult to detect and is widely used. The alert does not provide much detail on the number of Mamba-related attacks, but it notes that attackers are using the ransomware to target a wide variety of targets, including local governments, transportation agencies, legal services, and technology firms as well as industrial, commercial, manufacturing and construction businesses.

The attack begins when access is gained on a victim's system by using unsecured methods of remote access. The next step is to setup an encryption key and password, then the ransomware extracts a set of files and installs DiskCryptor. The encryption process then runs for the next two hours, at which point the system reboots. Once the encryption process is completed, the system displays the ransom note, including the attacker's email address, the ransomware filename, and a place to enter the decryption key. Instructions are given to the victim to contact the attacker to pay the ransom in exchange for the decryption key. The alert does not mention the amount of the ransom. The FBI alert offers defensive measures to take and other risk mitigation tips - such as implementing network segmentation, disabling remote access/RDP ports and using a VPN.

Mobile Malware Attacks Experienced in Over 90% of Organizations

According to a report by **Check Point**, who surveyed 1,800 customers, nearly all of the global organizations in the survey suffered at least one mobile malware attack in 2020. Nearly 93% of the attacks revealed were in a device network with the following breakdown: 52% were phishing attempts, 25% were C&C communication with malware previously within the device and 23% involved infected websites/URL. One warning that came from Check Point was mobile device management (MDM) could be a possible major new target for attackers. The report reiterated claims that roughly 40% of the world's mobile devices are more susceptible to attacks.

US Department of Labor Announces Cybersecurity Guidance for Retirement Market

On 14 April 2021, the United States Department of Labor announced new **guidance for plan** sponsors, plan fiduciaries, record keepers and plan participants on best practices for maintaining cybersecurity, including tips on how to protect the retirement benefits of America's workers. The department's Employee Benefits Security Administration (ESBA) has issued **cybersecurity guidance**. This guidance is directed at plan sponsors and fiduciaries regulated by the Employee Retirement Income Security Act, and plan participants and beneficiaries. The guidance comes in three forms, they are:

1. Tips for Hiring a Service Provider
2. Cybersecurity Program Best Practices
3. Online Security Tips

The guidance announced today complements EBSA's regulations on electronic records and disclosures to plan participants and beneficiaries.

FS-ISAC 2021 Virtual Europe Summit

The intersection of financial services and cybersecurity took on a new depth in 2020, with the rapid digitization of products and services and the wholesale shift to remote working caused by the pandemic. We now know many of these changes are here to stay, and cybersecurity is increasingly central to being competitive in a digital marketplace. New cyber challenges and risks call for increased sharing across borders and the only way to stay ahead of sophisticated threat actors is to collaborate. **Join our two-day virtual summit** to stay at the forefront of these new technology trends and emerging paradigms. A mix of live and on-demand sessions covering relevant topics around:

- Technology, Cloud, Application, and Data Security
- Governance, Risk Management, Compliance, and Resilience
- Payments and Currency
- Cross-Border Intelligence

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.