FS-ISAC

Executive Brief

March 2023

2023 FS-ISAC Board Election Process

The 2023 FS-ISAC Board of Directors (Board) election nomination period begins 13 March. There are five seats up for election, which means five FS-ISAC members have the opportunity to be voted in as an FS-ISAC Board member to have a stronger voice in the industry, build their professional network, and help form the strategic direction of FS-ISAC and its community. From 13 – 31 March, any member can nominate themselves or another member to be potentially considered for election. Individuals employed by any Tier level (1-8) member can be nominated. Only organizations at the Tier 1 through 4 levels can vote, with one vote per organization entered by the primary point-of-contact (POC). The Nominating and Governance Committee will pick a final slate for the ballot. FS-ISAC urges all members to carefully study the ballot when the formal election period starts, and to communicate the organization's choices to their primary POC for voting. Learn more information including criteria, requirements, additional considerations, and the full process timeline by logging into the *Intelligence Exchange* and selecting the *2023 Board Election* app.

New Malware Delivery Method Using Microsoft OneNote File Attachments

FS-ISAC members have reported a marked increase in a new malware delivery method with Microsoft OneNote file attachments. Malware files can be embedded in OneNote files which allows them to bypass the Mark-of-the-Web (MOTW) controls used by Microsoft to identify and restrict the actions of files from untrusted sources. Following Microsoft's announcement that macros (series of commands used to automate a repeated task in an Office 365 app) from untrusted sources would be blocked by default, threat actors who previously used malicious macros in Office 365 files began experimenting with other methods of delivery. FS-ISAC members have proactively shared YARA rules to aid in the detection of these malicious OneNote files, these submissions can be found in *Share*.

Cyber Insurers Unlikely to Significantly Increase Coverage Limits in Near Future

On 14 February, *The Wall Street Journal (WSJ)* reported that cyber insurers, "don't expect the amount they are willing to cover through cyber policies to expand dramatically in the near future, despite signs of a recovery from shock losses in recent years." Most major cyber insurers write single insurance policies for their largest customers up to roughly $15 million, according to *WSJ*. There doesn't appear to be a comfort level from many firms to issue policies in the range of $20-$50 million. Some large companies sometimes need that level of coverage and must do it by piecing together coverage from any multiple insurers. The threat landscape evolving rapidly over the last several years has dramatically impacted the cyber insurance industry. Starting in 2019, a rapid growth in ransomware claims led to direct loss ratios for insurance providers rising from an average of 47% in 2019 to 72% in 2020. Cyber insurers responded broadly in 2021 by raising premiums, implementing stricter underwriting standards, and tightening amounts of coverage limits. This decreased direct loss ratios to an average of 65% in 2021. The *WSJ* article claims that "some insurers maintain that strict underwriting, rather than making policies more widely available, is central to keeping the cyber insurance industry healthy." Another factor in providers not extending coverage limits is insufficient data on the extent to which longer-term events like class-action data breach lawsuits can impact insurance claims.

Singapore's Scam and Cybercrime Cases Increased by 25% in 2022

On 8 February, *ZDNet* reported that Singapore saw a 25% increase in reported scam and cybercrime cases in 2022 (33,669 total), up from 26,886 total reported cases in 2021, according to a report from the Singapore Police Force (SPF). The actual money lost from these cases only saw a 4.5% increase from 2021 (SG$632 million) to 2022 (SG$660 million). Phishing, e-commerce, and investment scams were in the top five most common tactics used, with phishing cases topping the list as there was a 41% increase from 2021. The most common victims by age group were 20-29 representing 26.7% of all victims and 30-39 representing 26.8% of all victims. According to the SPF report, "scammers typically turned to social media, messaging, and online shopping platforms as modes of contact, where the majority of victims in these age groups falling prey to job and phishing scams." Singapore has enacted several initiatives and tools to better combat the trend, including most recently tagging business SMS senders as 'likely scam' if they are not registered with the Singapore SMS Sender ID Registry.

Threat Intelligence Update

The *LockBit* gang are currently one of the most prolific ransomware gangs in circulation, running a Ransomware-as-a-Service (RaaS) operation that provides tools to third-parties that may not have the ability to conduct their own ransomware attacks. On 31 January, the ION Group – a prominent supplier of software and SaaS to the financial sector – was attacked by *LockBit*. While the initial attack vector has still yet to be officially confirmed, the attackers were able to encrypt ION's VMware environment. The attack impacted ION's cleared derivatives markets SaaS services, resulting in delays and disruption to trading, processing, and clearing, with some customers having to process trades manually. ION has now largely restored its services via data backups and new servers to enable reconnection for its clients after a certification process from the incident response team. While the US Treasury declared the incident as not presenting a systemic risk to the market, the cyber attack's disruption of a key processor to the derivative market demonstrates a potential for more serious incidents in the future. FS-ISAC was able to support members with daily updates via an incident-specific *Connect* channel for ION customers.

This monthly brief is for CEOs and other senior leaders. This brief is deemed Traffic Light Protocol (TLP) Green - information may be shared with employees and trusted partners but may not be shared in public forums. Please contact the FS-ISAC communications team at communications@fsisac.com with comments or questions.