Securities Industry Risk Group (SIRG)

Global Cybersecurity Brief – June 2021

Three New Variants of Malware Found in Global Finance Phishing Campaign

On 4 May, the cybersecurity team at FireEye stated that **three malware strains** called Doubledrag, Doubledrop and Doubleback were detected in December 2020. The report states that the threat actors behind the malware are experienced and well-resourced and are targeting organizations in the US, EMEA region, Asia, and Australia and are labeled as UNC2529.

The report states that potential victims received phishing messages that had subject lines tailored to the targeted victims and would masquerade as an account executive touting services for different industries. Over fifty domains were used to manage the global phishing scheme. In one attack, UNC2529 successfully compromised a domain owned by a US heating and cooling services business and launched its phishing attacks against more than a dozen organizations. The fake emails contained links to URLs with malicious payloads and Java script file within a zip archive to trick the victim to launch the Java script file, which then launched the Doubledrag downloader.

Organizations are advised to inform their employees of these phishing tactics listed in the report and ensure systems are up to date with the latest antivirus and malware protection.

Credential Stuffing Attacks Hit Financial Services

According to a report published by Akami, there were 193 billion **credential stuffing attacks globally with financial services organizations** being hit with 3.4 billion, a 45% year-over-year increase. From the beginning of 2018 to year end 2020, DDoS attacks increased by 93% in the financial services sector, highlighting criminals' continued reliance on systemic disruption to get the most out of their efforts. According to Steve Ragan, Akami security researcher and author of the report, "the ongoing, significant growth in credential stuffing attacks has a direct relationship to the state of phishing in the financial services industry." Attackers are more in tune on utilizing various methods to enhance their credential collections, with phishing being one tool they focus on more often.

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.

Cybersecurity Viewed as a Business Mission by European Executives

A new report published by Trend Micro suggests that a **large number of European executives** consider cybersecurity part of their business mission more so than their American counterparts. The report claims that 73% of European business and IT leaders view cybersecurity as either partially or entirely a business area versus 58% of their counterparts in North America. The report also found that four out of five European organizations with multiple board members were knowledgeable about cybersecurity. European businesses are also more mature in areas such as GRC, or third-party risk management.

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.