Details Released on FIN7's Hacking Group's Malware

Researchers have published details about the malware variant from the FIN7 hacking group called **JSSLoader**. While the malware is believed to be used during **several campaigns**, details about the malware have been hard to come by. The hacking group is financially motivated and is believed to target victims through spear-phishing campaigns and operates within Eastern Europe. The United States Department of Justice (**US DOJ**) had reported in 2018 that three members of the group were charged for allegedly stealing more than 15 million customer payment card records from over 6,000 point-of-sale terminals at over 3,000 business locations.

Researchers analyzed a recent failed attack and reported that the attack started with a phishing email that downloads a VBScript. A second script is downloaded, which then attempts to download and install the main JSSLoader. The JSSLoader then functions as a remote access tool (RAT) which seeks to collect network and system information about the device, such as active directory information, patches and desktop files. All information collected is then encrypted before it is sent back to the group. The JSSLoader is also designed to carry out commands, such as executing PowerShell scripts.

Fileless Malware – Unseen and Hard to Detect

Fileless Malware, where the malware actions reside solely in memory, has recently become more of a go-to method for attackers. Fileless Malware techniques never touch the victim's storage, which increases the difficulty of identifying and blocking the initial moments of an attack. An unintended result of this Malware is triggering false positives and preventing the same tools from carrying out legitimate activities. One point worth noting, files that are monitored only by endpoint defenses would have missed the attack outright. Strong passwords and multi factor authentication are still an organization's best defense in curtailing attacks.

70% of UK's Finance Industry Attacked in 2020

A report published by the Ponemon Institute shows that **70% of UK financial firms** fell victim to a cyberattack in 2020. A majority of these attacks were derived from exploiting the mass shift of employees working away from the office due to COVID-19. This opportunity gave attackers access to company information while employees were in remote environments. The report shows that the increased use of personal devices by employees without sufficient guidance or security controls resulted in sensitive corporate information being accessed using platforms unprotected by enterprise security infrastructure. The report states that the use of personal devices has left much of the finance industry in the UK vulnerable, with 70% claiming that their use has hindered business security.

CISA:- Don't Blame "Employing Reporting" of Suspicious Cyber Activities

The Cybersecurity & Infrastructure Security Agency (CISA) has raised **concerns** regarding cloud services that organizations rely on. Attackers are targeting employees working remotely and organizations with weak cyber hygiene practices. While CISA is aware of several recent cyberattacks that were successful, their report is not related to any one threat actor or incident. The latest phishing attempts targeted high profile executives who had access to sensitive financial information, more specifically email forwarding rules focusing on users sending business emails to personal email accounts. Employees should feel safe in reporting any suspicious activity, whether they fell victim to an attack or not.

Monetary Authority of Singapore Revises Guidelines to Combat Heightened Cyber Risks

On 18 January, the Monetary Authority of Singapore (MAS) **published** revised Technology Risk Management Guidelines to address emerging technologies and shifts in the cyber threat landscape for financial institutions (FIs). The revised guidelines focus on the cyber risks associated with the growing use of cloud technologies, application programming interfaces (APIs), and rapid software development. The MAS set out two enhanced risk management strategies for FIs: to establish a robust process for the timely analysis and sharing of cyber threat intelligence within the financial ecosystem, and to conduct or participate in cyber exercises to stress test defenses by simulating cyber-attacks. Additionally, there is guidance on the roles and responsibilities of the board of directors and senior management. According to the MAS, "the board and senior management should ensure that a chief information and a chief information security officer, with the requisite experience and expertise, are appointed and accountable for managing technology and cyber risks."

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.