Securities Industry Risk Group (SIRG)

Global Cybersecurity Brief – August 2019

FS-ISAC on Cybersecurity Awareness

This monthly update is brought to you by the Financial Services Information Sharing and Analysis Center (FS-ISAC) in coordination with the Securities Industry and Financial Markets Association (SIFMA), the Investment Industry Association of Canada (IIAC), the International Council of Securities Associations (ICSA), the Financial Services Institute (FSI) and the Insured Retirement Institute (IRI).

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's member-based organization and readers from organizations who are not already members are encouraged to (join) FS-ISAC.

Threat Intelligence Update

Tensions between the US and Iran continue to escalate, prompting the global financial sector to increase vigilance regarding any related cyber-activity. Amid alleged military and cyber-activity and new sanctions by the US on Iran, the US Department of Homeland Security (DHS) issued a statement indicating a recent rise in malicious cyber-activity directed at US industries and government agencies by Iranian regime actors and proxies (DHS). DHS further noted that these actors are increasingly using destructive wiper attacks and other activities enabled by spear phishing, password spraying and credential stuffing. FS-ISAC is monitoring for suspicious activity against the financial sector. Financial institutions in the US, its allied countries or with operations in the Middle East and North Africa region are more likely to be targeted. As a historical target of Iranian cybercampaigns, FS-ISAC encourages financial institutions to implement strong cyberhygiene and review best practice guidance within FS-ISAC Threat Viewpoints on destructive malware and Distributed Denial of Service (DDoS) attacks.

Release of Actionable Guides to Cybersecurity for Smaller Financial Institutions

The Carnegie Endowment for International Peace released "Cyber Resilience and Financial Organizations: A Capacity-building Tool Box" (Tool Box) on July 16. The FS-ISAC along with the SWIFT Institute (which is the original sponsor), the International Monetary Fund (IMF), Standard Chartered, the Cyber Readiness Institute and the Global Cyber Alliance (GCA) contributed to the toolbox and are co-branding the documents and promoting their distribution and use.

The Tool Box contains: (1) Board-Level Guide: Cybersecurity Leadership; (2) CEO-Level Guide: Cybersecurity Leadership; (3) CISO-Level Guide: Protecting Your Organization; (4) CISO-Level Guide: Protecting Your Customers; (5) CISO-Level Guide: Protecting Connections to Third Parties; and (6) Incident Response Guide – each accompanied by a checklist and a supplementary report detailing the various standards and policies that informed the development of the tool box. The Tool Box is based on existing frameworks, policies, and standards from around the globe. The toolkit is the result of a year of work and engagement with experts in government and industry ranging from central banks to cybersecurity agencies and international bodies. These easy-to-use one-page guides and checklists provide senior management with actionable measures to improve their organization's cybersecurity.

The Tool Box is freely available from the Carnegie Endowment website in seven languages: Arabic, Dutch, English, French. Portuguese, Russian, and Spanish. **Learn more**.

Securities Industry Risk Group (SIRG)

Global Cybersecurity Brief – August 2018

Researchers Show the Dangers in BlueKeep Exploit

Firms who have not yet patched a severe vulnerability found two months ago for an exploit in Microsoft Windows are at risk. The CVE-2019-0708 vulnerability – known as BlueKeep – was first reported in May, and allows attackers to connected to Remote Desktop Protocol services (RDP) and issue commands which could steal or modify data, install malware and conduct other malicious activities (**CVE Details**). The software company considers this vulnerability dangerous enough that is has told customers repeatedly to apply the patches (**ZDNet**) and even the National Security Agency (NSA) had issued a warning to patch against BlueKeep (**NSA**). The vulnerability has a similar worm-like spreading functions which powered the WannaCry ransomware outbreak in 2017. This vulnerability affects computers running Windows XP, Windows 7, Windows Server 2003 and 2008. The risk is large enough that the software company has issued patches for Windows operating systems that are now considered unsupported.

There have been no reports of BlueKeep exploits in public, but researchers at Sophos have developed a proof-of-concept showing how an attacker could deploy an attack against RDP systems without any input from the victim required (**Sophos**). If an attacker is successful as described in the proof-of-concept, then they could use BlueKeep to issue destructive command on Windows systems. Firms are encouraged to apply the required patches provide by Microsoft.

FS-ISAC has published the *CISO Congress Security Viewpoint – Preventing RDP Attacks at the Perimeter.* This report provides considerations and guidance for FS-ISAC members to build resilience against wormable attacks. FS-ISAC and its CISO Congress in Europe, Middle East, Africa (EMEA) strongly recommends that all file sharing, database access and remote access protocol ports from external sources be blocked at the firewall. In general, this recommendation extends blocking to all inbound ports, with very few exceptions in special use cases. The recent disclosure by Microsoft of a new and serious vulnerability in its remote desktop services is a reminder that the best protection against exploitation is a properly configured firewall.

About FS-ISAC

The Financial Services Information Sharing and Analysis Center (FS-ISAC) is an industry consortium dedicated to reducing cyber-risk in the global financial system. Serving financial institutions and in turn their customers, the organization leverages its intelligence platform, resiliency resources, and a trusted peer-to -peer network of experts to anticipate, mitigate and respond to cyberthreats. FS-ISAC has nearly 7,000-member firms with users in more than 70 countries. Headquartered in USA, the organization has offices in the UK and Singapore. To learn more, visit www.fsisac.com. This newsletter is not intended to replace the benefits of joining FS-ISAC's member-based organization. Please consider joining if you're not already a member.

Thank you,

FS-ISAC SIRG Team

If you have any questions about this week's report, please contact the FS-ISAC SIRG.

Financial Services Information Sharing and Analysis Center

fsisac.com