FINANCIAL SERVICES | Information Sharing and Analysis Center

FS-ISAC Securities Industry Risk Group Global Cybersecurity Brief **March 2017**

Finalized Cyber Regulations

The NY Department of Financial Services (**NYDFS**) unveiled final cybersecurity regulations that will be phased in starting on March 1, which require banks, insurance companies, and other financial services institutions regulated by NYDFS to adhere to minimum standards to prevent and avoid cyber breaches, including:

- Controls relating to the governance framework for a robust cybersecurity program, including adequate staffing, funding and oversight; mandatory chief information security officer; cybersecurity training for employees, and oversight of third-party service providers

- Risk-based minimum standards for technology systems including access controls, data protection including encryption, and penetration testing

- Cyber incident response plans, preservation of data to respond to such breaches, and notice to NYDFS of material events and identification and documentation of material deficiencies, remediation plans and annual certifications of regulatory compliance to NYDFS

The proposed rules were first released in September 2016 and the FS-ISAC and FSSCC submitted comment letters in conjunction with other associations. The comment letters urged DFS to adopt a risk-based approach in harmony with existing federal regulatory requirements.

Attention to cyber regulation world-wide is increasing with developments in the US in addition to China's new cybersecurity law and the European Union's General Data Protection Regulation (GDPR). Bank Info Security news highlighted 11 take-aways from the recent RSA Conference (**LINK**) and, among the list, included increased interest in policy and regulation. Please share your insights with us (**FS-ISAC SIRG Team**).

Watering Hole Attacks on European Regulator

In early February, an investigation of a watering hole attack against a Polish regulator uncovered a larger campaign to compromise financial sites in Europe and Latin America (**Symantec**). At least four sites in four different countries redirected users to sites hosting

exploits. Although investigations are ongoing, initial reports on successful infections suggest data was stolen, but due to encryption, it is unknown what type of data was exfiltrated. Malware analysis suggests links to the SWIFT- related heists in Bangladesh and Vietnam, attributed by some to North Korean actors. The FS-ISAC assesses with high confidence that a cross-regional, coordinated campaign has been targeting the financial services sector since at least October 2016. However, attribution of who is responsible cannot currently be made.

'Invisible' Attacks Recently Discovered

Researchers at Kaspersky lab have discovered that 140 organizations such as banks, telecommunications and government organizations in over 40 countries have been victim to new attacks (**Kaspersky Labs**). These 'invisible' attacks use available tools, including administration software as well as the PowerShell, to hide the malware in computer memory rather than the common practice of saving the malware files onto the victim's hard drive.

This form of an attack leaves little to no evidence that the attack took place. Any indication of an incident is removed when the system is rebooted (**TechRepublic**). The discovery came when researchers where contacted by banks that noticed Meterpeter software, along with PowerShell Scripts running in the memory of a server that is should note be running.

Researchers do not know who initiated these attacks, and with the use of the utilities, open source code and unknow domains make it difficult to identify those responsible. Researches mention that the cybercriminal groups such as the Carbanak gang and the GCMAN group have used similar approaches (**ZDNET**).

Firms should ensure all software running on all servers and PCs are update with the latest fixes and patches, and monitor what programs are running in memory.

New CryptoMix Ransomware Variant Discovered

Researchers have discovered a new variant of the CryptoMix ransomware that is being distributed via the RIG exploit kit (**SecurityWeek**). CryptoMix (also known as CryptFile2) has been delivered through the RIG-E and Rig-V exploit kit and targets users of the Chrome Browser on Windows computers. Once installed on a compromised computer, the malware generates a unique ID and begins to scan the computers for over 400 different types of files and encrypts them using AES-256 encryption. All encrypted files are then renamed using the '.CRYPTOSHIELD' extension to the file name.

The malware also creates ransom notes in each of the folders where encrypted files are located. The notes refer to the ransomware as 'CryptoShield 1.0' and provide victims with three email addresses they can contact to begin the ransom payments. These notes are basically the same from prior versions of the ransomware expect for the email addresses used to collect the ransom. Firms are urged to ensure that the latest software and security patches are installed on their systems and networks, and that they give their end user proper notification to their end users

---

Update from the FS-ISAC Analysis Team

Oracle Critical Patch Update - January 2017

As part of its quarterly Critical Patch Update (CPU), Oracle patched 270 vulnerabilities in January 2017 across 45 different products. This included E-Business Suite and MySQL database. Around 40 percent of the issues fixed were remotely exploitable without authentication. In 2015, the average number of vulnerabilities Oracle patched was 153 per quarterly patch. Last year that figure shot up to 227. Oracle strongly recommends that customers remain on actively-supported versions and apply Critical Patch Update fixes without delay.

Zeus Sphinx Trojan infection campaign leveraging Sundown EK

With the disappearance of the Angler and Nuclear exploit kits, a gap was left in the market that has been quickly filled by more prominent kits such as RIG EK and its variants. Smaller players like Sundown, however, have also stepped up to claim their place in the market.

According to Trend Micro, the newly updated Sundown EK was used by multiple malvertising campaigns to distribute malware. The most affected countries were Japan, Canada, and France, with Japanese users accounting for more than 30% of the total targets. IBM Trustee reported on new Zeus Sphinx Trojan infection campaigns, with configurations targeting banks in Canada. In other previous campaigns, Sphinx variants targeted UK banks in 2015, or Brazilian banks just last summer coinciding with the summer Olympics. In this case, Sphinx's operators focused the target list on Australian banks and Canadian credit unions (likely seeing them as the lower hanging fruit in Canada's financial sector). These operators have been using two distribution methods in their recent campaigns, including malvertising that leads to the Sundown exploit kit.

The ISAC Analysis Team will continue monitoring Zeus Sphinx Trojan infection campaigns and Sundown EK updates for any activity that may affect financial institutions.

Registration Now Open for the APAC and Annual Summits

Registration is now open for both the Asian Pacific **APAC Summit**(3-4 April, 2017 in Singapore) and **Annual Summit** (30 April-3 May, 2017 in Lake Buena Vista, FL)! Don't miss your chance to attend!

FS-ISAC Summits are focused around peer-to-peer networking and building relationships or circles of trust with financial services organizations. We invite you to attend and see what new sessions and exciting innovations are developing around information sharing amongst financial institutions and threat intelligence practices.
Register for the APAC Summit | **Register for the Annual Summit**

About the FS-ISAC

The Financial Services Information Sharing and Analysis Center (FS-ISAC) helps assure the resilience and continuity of the global financial services infrastructure through sharing threat and vulnerability information, conducting coordinated contingency planning exercises, managing rapid response communications, conducting education and training programs, and fostering collaborations with and among other key sectors and government agencies.

This newsletter is not intended to replace the benefits of joining FS-ISAC's member-based organization.

Thank you,

Peter Falco and Richard Livesley
pfalco@fsisac.com rlivesley@fsisac.com

If you have any questions about this report, please contact the **FS-ISAC**.

Financial Services Information Sharing Analysis Center **www.fsisac.com**