



**FINANCIAL
SERVICES**

Information
Sharing and
Analysis Center

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

**September 2018
TLP: WHITE**

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) and the International Council of Securities Associations (ICSA).

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](#)).

GDPR and Privacy Concerns Increase Information Security Spending in 2019

Analysts at Gartner released results from a 2017 survey that shows spending on information security products will increase 12% from 2017 to 2018 to exceed \$144 billion in 2018 ([FORBES](#)). The survey showed several drivers for security spending: security risks, business needs, industry changes and General Data Protection Regulation (GDPR) privacy concerns. Looking forward, Gartner anticipates that in 2018-2019 at least 30% of organizations will spend more on GDPR-related consulting and implementation services.

In 2018, Gartner has identified key trends affecting information security spending in 2018-2019. Organizations are continuing to ensure they are compliant with GDPR, and it is expected to be the one focus of security service spending for EU-based organizations and for those customers who reside in Europe.

NIST Small Business Cybersecurity Act Signed into Law

After being introduced over a year ago, the NIST Small Business Cybersecurity Act ([GPO.GOV](#)) was passed and signed into law. The law requires the director of the National Institute of Standards

and Technology to issue guidance and a consistent set of resources to help small business identify, assess and reduce their cyber risks ([SC Magazine](#)). When developing these recommendations, they should be widely applicable, technology-neutral and include elements that promote awareness of simple, basic controls, a workplace cybersecurity culture, and third-party stakeholder relationships.

Fake Invoice Emails Deploy Ransomware

A new malspam campaign has begun in which emails sent to victims are presented as fake invoices for an outstanding payment. When victims click on these invoices, an information-stealing trojan named AZORult and the Hermes 2.1 Ransomware is installed on the recipient's computer ([Bleeping Computer](#)). The emails contain the subject 'Invoice Due' and pretend to show an outstanding balance in an attached Word document. The Word document is password protected, which makes it more difficult for antivirus vendors to detect the emails as malicious. The password is included in the email message, which is '1234'. Once the recipient enters the password, they will be greeted with the 'Enable Content' prompt which enables Macros or other embedded scripts to be executed from the Word document.

The Hermes 2.1 Ransomware is executed first and encrypts files on a computer but does not rename them. If a computer is infected, there will be a file named 'DECRYPT_INFORMATION.html' which contains ransom notes.

Firms should alert end-users of these malicious emails, including the text in the subject line, and to not open the attached Word document. They should ensure that their software, network devices and appliances are updated, and ensure they have mitigation plans in place in the event the malware attempts to install on their systems.

2018 FS-ISAC Fall and EMEA Summits

Fall Summit - Early Bird Registration Open – Register Today and Help FS-ISAC Support Veterans

The Fall Summit on November 11-14 in Chicago is shaping up to be a substantive event. The member-driven content committee has been hard at work this summer reviewing dozens of speaker proposals from members and expert speakers on a variety of tracks, including threat intelligence, security & technology operations, testing, cloud computing, compliance, and governance. In honor of Veteran's Day, FS-ISAC will donate \$10 USD to [Team Rubicon](#), a veterans' charity, for every person who [registers](#) before September 30. What are you waiting for? [Learn more](#), book your [hotel and travel](#) and [register now!](#)

FS-ISAC 2018 EMEA Summit Registration Open

Registration for the EMEA Summit is now open! This year's Summit will focus on trust and ensuring our members' security among increasingly volatile ransomware and phishing campaigns threatening our financial safety. With more than 30 sessions divided into six tracks, make sure you plan to join us in Amsterdam October 1-3, 2018. [Learn more](#), [view the agenda](#) and make sure you [register today](#).

FS-ISAC Cyber-Range Ransomware Exercises

Cyber-range exercises offer FS-ISAC members a more technical, hands-on keyboard experience that provides greater interaction and sharing between members in a way that helps raise capability maturity levels and resiliency across the sector. FS-ISAC has partnered with ManTech to build a network environment and facilitate the event. Learn more and register ([Register Here](#)) for one of these upcoming sessions:

- September 17 | Federal Reserve Bank of Chicago
- October 10 | Federal Reserve Bank of San Francisco
- October 24 | Federal Reserve Bank of Kansas City, MO

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. Please consider joining if you're not already a member.

Thank you,
[FS-ISAC SIRG Team](#)

If you have any questions about this report, please contact the [FS-ISAC](#).

This newsletter contains content developed by FS-ISAC as well as links to content developed by third parties. FS-ISAC makes no claims or warranties as to the accuracy of information provided by third parties. All copyrights remain with their respective owners.

Financial Services Information Sharing Analysis Center

www.fsisac.com

