FINANCIAL SERVICES | Information Sharing and Analysis Center

FS-ISAC Monthly Newsletter | January 2018 TLP WHITE

Newsletter Contents

Upcoming Events and Webinars

*** FS-ISAC members-only**

FS-ISAC Expert Webinar Series: Combatting BEC with Active Defense – Turning the Tables on Cybercriminals* | 23 January

Splunk Webinar: Improve Your Cybersecurity Posture with NIST Standards-Based Solutions | 23 January

Cymmetria Webinar: Cyber Deception and Responder | 25 January

EclecticIQ Webinar: How to Overcome the Threat Intelligence Cycle Paralysis? | Download until 13 February

Attivo Networks Webinar: Helping Financial Institutions Change the Game on Modern-Day Attackers | 15 February

Mumbai Member Meeting* | 23 February

London Member Meeting* | 1 March

Zurich Member Meeting* | 7 March

2018 FS-ISAC Annual Summit
20-23 May | Boca Raton, FL

London Member Meeting* | 14 June

2018 FS-ISAC AP Summit
18-19 July | Singapore

2018 FS-ISAC EMEA Summit
1-3 October | Amsterdam

2018 FS-ISAC Fall Summit
11-14 November | Chicago

FS-ISAC Responds to Spectre and Meltdown

While vulnerability management is a core part of most financial institutions cybersecurity practices, FS-ISAC and our members continue to assess the actual risk and seek additional information about the vulnerabilities and their potential impact. The FI community takes all vulnerabilities seriously and takes proactive measures to ensure proper risk mitigation.

In addition to the security considerations raised by this design flaw, performance degradation is expected which could require more processing power for affected systems to compensate and maintain current baseline performance. Additional costs may also be a factor to maintain current system and application performance.

Even outside of the known performance hit, fixing kernel level vulnerabilities typically requires more testing than browser, office productivity applications and other patches due to the underlying direct link to the operating system. There will need to be consideration and balance between fixing the potential security threat vs the performance and other possible impact to systems. The current general thought is that the security risk will be lower on dedicated servers and end points (due to the expected exploit requirement to run code on an individual system) and higher on shared computers such as hosting and cloud services which use the same physical hardware (and processor) to share different (user) virtual machines.

FS-ISAC held a special members-only call on Tuesday 9 January and the ISAC Analysis Team provided that “Speculative Execution” is a CPU feature designed to accelerate program execution and ensure efficient CPU utilization. This allows a

continued page 2

Leadership Changes at Sheltered Harbor – Trey Maust Appointed CEO

Sheltered Harbor, an initiative designed to ensure consumers have access to critical account assets in the event of a major incident, announced the appointment of Trey Maust to be its new chief executive officer and Carlos Recalde to be its president and chief operating officer. Maust replaces former CEO Steven Silberstein, who successfully led the organization during his two-year term. Sheltered Harbor is an FS-ISAC subsidiary. More information at www.shelteredharbor.org

Reminder: Deadline Approaching for EU General Data Protection Regulation

The GDPR, which goes into effect on 25 May 2018, aims to strengthen and harmonize data protection requirements for individuals that reside in European Union (EU) countries. The GDPR impacts financial institutions that do business in the EU. To prepare FS-ISAC members for the new regulation, FS-ISAC’s

continued page 2

ISAC Analysis Team Update

Death Threat Used in Cyber-Related Extortion

Death threat extortion emails have been documented for some time going back to at least 2006. Through open source research the IAT identified a campaign reported by NBC happening in Radnor, PA consisting of a death threat along with a demand for bitcoin payment in mid-December 2017. Preventative measures for such messages are email filtering and domain name protection in case someone hacks your organizations email server and sends similar type messages. In addition, US law enforcement suggest if you receive a similar email don't reply and report it to the FBI, if a computer network is involved, it almost certainly becomes a federal crime. Outside the US recipients of these emails should report this type of threat to their local law enforcement who should have a process to respond to this type of threat.

Hidden Cobra

DHS and the FBI released two joint Technical Alerts (Tracking IDs 935365 and 935348) on 14 November 2017 that described the malware FallChill and Volgmer reportedly used by the North Korean government in cyber-activities against various sectors including the financial, media and aerospace sectors. The US Government refers to malicious cyber-activity by the North Korean government as HIDDEN COBRA. Both FallChill and Volgmer are Remote Access Trojans (RAT) with various capabilities including remote command execution, system information collection and file transfer. In addition, FallChill can obfuscate network traffic between victims and threat actors via multiple proxies and using what appears to be Transport Layer Security (TLS) encryption but is RC4 encryption. Volgmer has reportedly been in existence since 2013 while FallChill since 2016. So far, IAT has not received any information about specific vulnerabilities that could be exploited resulting in the installation of either malware. DHS and the FBI provided threat detection and risk mitigation strategies for both malware. Members are encouraged to review and consider implementing them.

Building Cybersecurity Diversity (BCD) Scholarship – Sponsorship Opportunities

The women's scholarship program is going global. FS-ISAC is now offering scholarships to women in Singapore, Australia, the United Kingdom and the United States but we need your support. If you are interested in sponsoring a scholarship or sharing your contacts at educational institutions to provide an outstanding opportunity to female students in cybersecurity please visit us online or email us today.

Deadline to commit for 2018

- AP Scholarship Program: 15 January 2018
- US Scholarship Program: 1 February 2018
- EMEA Scholarship Program: 31 March 2018

Products and Services Discounts

Did you know that as a member of FS-ISAC you can take advantage of special offers and discounts on product and services from our Affiliates and Strategic Partners? **Visit the member discount page** to see current offers. Make sure to bookmark and check back often as offers are updated and added frequently!

Spectre/Meltdown, continued

processor to execute code in advance even before it is certain it needs to be done, so the results are ready as quickly as possible if needed and simply ignored if not. However, security researchers have demonstrated that this feature could be taken advantage of by malicious actors to read system memory that should be inaccessible. In Intel's x86-64 hardware it appears that programs may be able to speculatively execute code that would not have permission to run under normal circumstances, allowing carefully-constructed, malicious code to essentially read the kernel memory space without the proper permission. The potential impact of such an attack is unauthorized access to sensitive information including passwords or login files.

- CVE-2017-5753: bounds check bypass - Intel, AMD and ARM are reported to be affected.
- CVE-2017-5715: branch target injection - Intel, AMD and ARM are reported to be affected.
- CVE-2017-5754: rogue data cache load - Intel and ARM are reported to be affected. This is also known as KPTI (formerly KAISER)

Proof of Concepts (POC)

- POC for Meltdown
- Another security researcher has reportedly already mentioned via Twitter that a working POC has been validated.
- Please note there is a POC for Spectre.

Mozilla has released statements that claim "*it is possible to use similar techniques from Web content to read private information between different origins.*"

EU GDPR, continued

European Legal and Regulatory Working Group issued a paper in 2016 on how to create a more consistent and streamlined incident/fraud reporting framework in the EU. The paper can be viewed on the FS-ISAC Member Portal. On 8 May FS-ISAC hosted a members-only Expert Webinar Series on the impact of the European Union's General Data Protection Regulation (GDPR) on how financial firms must handle personal data, and its influence on how financial institutions may share intelligence with other institutions. View the on-demand webinar.