COMMUNITY INSTITUTION & ASSOCIATIONS RISK SUMMARY REPORT

TLP: Green | CTL: Elevated | PTL: Guarded | Terrorism TL: Elevated | Week of June 12

In This Issue

News and Risk Information

Summary:

Below are some of the top news and risks that the Financial Services Information Sharing Analysis Center (FS-ISAC) has observed this week for community institutions (CI).

NEWS

Regional Tabletop Exercise. On June 6, Greg Gist, Brian Tishuk and Susan Rogers in partnership with US Treasury, led a regional table-top exercise hosted by the Dallas Federal Reserve. The exercise simulated a cyber-attack against the administrative and core functions of local institutions examining escalation, notification and communications protocols. Institutions and associations participated in the exercise with US government agencies including US Treasury, federal regulators, DHS, FBI and the US Secret Service. The key action items from the exercise included how to better harmonize escalation and incident levels between institutions and governmental entities to ensure the proper assessment of a potential crisis. Action items will be monitored by the After-Action Subcommittee of the FS-ISAC & FSSCC's Exercise Committee.

OCC Releases FAQ on Bank Relationships with FinTech. As with the 2013 guidance, the OCC encourages banks to incorporate the FAQs into their third-party relationships and assessments. In addition, the OCC encourages third-party service providers to banks to anticipate questions from their bank customers based on the OCC's guidance and expectations. The OCC also encourages banks to engage with information sharing organizations to monitor and better understand cyber threats and vulnerabilities and specifically mentions the FS-ISAC, the US Computer Emergency Readiness Team (US-CERT), and InfraGard.

CAPS Deadline Registration Update. The deadline to register to participate in the Cyber-Attacks Against Payment Systems is September 6, 2017. Those wanting to participate can register at: FS-ISAC CAPS.

Community Institution and Association Council Meeting Reminder. A reminder that the CIAC will meet on June 19 at 3:30 PM EDT.

RISKS

Auto Loan Fraud Losses Accelerate at Credit Unions. *CUTimes* is reporting that CUs could experience accelerated fraud losses due to auto loans according to Frank McKenna, Chief Fraud Strategist for PointPredictive. McKenna's research, based on reviews of past auto loan applications, statistical modeling and other industry expertise, found that auto fraud losses are expected to hit in the estimated range of $4 to $6 billion USD in 2017, from the estimated $2 to $3 billion USD in auto loan losses in 2015. Although the cost of auto lending fraud erodes the bottom line for all lenders, it may not be categorized or recognized as a fraud loss. The schemes have become much more sophisticated, complex and elaborate, making it more challenging than ever for financial institutions to detect and prevent the fraud.

This Week's Top Risks

- **Malware, Ransomware and Trojans**
  - Jaff (phishing)
  - Multiple Malware Campaigns (see SOC reports)
  - TrickBot
  - Ursnif (aka Gozi aka Gozi ISFB) Malware
- **System Vulnerabilities**
  - Adobe (multiple), Android (Multiple), IBM (multiple)
- **Themed Phishing Campaigns**
  - Bank themed, Dropbox, Password Reset Notification

The Financial Services Information Sharing and Analysis Center (FS-ISAC) is a non-profit corporation that was established in 1999. FS-ISAC is a member-driven organization whose mission is to help assure the resilience and continuity of the global financial services infrastructure and individual firms against acts that could significantly impact the sector's ability to provide services critical to the orderly function of the global economy. FS-ISAC shares threat and vulnerability information, conducts coordinated contingency planning exercises, manages rapid response communications for both cyber and physical events, conducts education and training programs and fosters collaborations with and among other key sectors and government agencies.

Leaked Exploits Used in Ongoing Cyber-attacks

Summary:

When the anonymous hacking group Shadow Brokers released a set of previously unknown vulnerabilities in commonly used software, security practitioners feared the potential for incredible damage. Upon the release of the vulnerabilities, Microsoft stated almost immediately that the exploits had been patched in previous updates, or were not able to be replicated on supported platforms (operating systems that have not gone "end-of-life"). Two of the released exploits, EternalBlue and DoublePulsar, were used in the May 12 *WannaCry* ransomware/worm attacks infecting more than 200,000 computers globally in one day; however, because financial institutions are diligent in patching and running supported programs, they were protected against *WannaCry*. Yet, other vulnerabilities may impact financial institutions.

Before *WannaCry*, there was Adylkuzz

A cryptocurrency miner known as Adylkuzz was infecting machines using EternalBlue and DoublePulsar prior to *WannaCry's* outbreak. In fact, this malware may have kept more machines from being infected with *WannaCry*, as part of the Adylkuzz infection process blocked SMB communications. Because Adylkuzz is a cryptocurrency miner, it may seem less impactful to community institutions (CIs); however, systems infected with a cryptominer will run considerably slower than normal, which can cause a loss of productivity and frustration for end users and customers.

EternalRocks lacks direction

EternalRocks hasn't yet been weaponized to perform malicious actions other than spreading itself via worm capabilities; however, once established on a system, command and controls servers may send infected machines whatever instructions are needed at any time. EternalRocks uses six of the released exploits: EternalBlue, EternalChampion, EternalRomance and EternalSynergy for the compromise; SMBTouch and ArchiTouch for SMB reconnaissance; and DoublePulsar to spread to new machines and remain as a backdoor on infected machines. Just because this exploit lacks a definitive purpose today doesn't mean the malware currently on systems won't receive new instructions and launch new attacks tomorrow or next week.

An exploit by any other name is EternalRed

What happens when the EternalBlue exploit is repurposed to infect Samba deployments on systems running Linux and UNIX? It becomes EternalRed and the vulnerability and attack are dubbed *SambaCry*. Samba is used on *NIX systems for file and print services over the SMB protocol, for Windows network integration. SambaCry doesn't install ransomware, though; instead, like the Adylkuzz malware above, it installs a cryptominer that drains system resources. Considering the platform, it is designed to attack, EternalRed is likely to infect servers and, specifically, core servers running CI production databases.

Risk to Community Institutions:

Potential risks from the exploits include:

- Impact to productivity for systems that are conscripted into botnets mining cryptocurrencies, causing PCs and servers to run considerably slower than normal.
- Loss of productivity and data if systems are locked by ransomware, rendered unusable until a decryption key is obtained or the system is reformatted.
- Exploits sitting in stealth mode can quietly perform data analysis and determine the most sensitive data to harvest later.

Remediation:

- Patch systems in a regular and timely fashion or, for legacy systems, migrate to supported operating systems ASAP;
- Backup critical data regularly;
- Continuously monitor and log network traffic, segment internal networks based on criticality, and disable unnecessary protocols like SMB on servers and network devices;
- Employ endpoint protection for anti-virus, anti-malware purposes and set to alert on wholesale, simultaneous file format changes; and
- Provide continuous security awareness training for employees.

Supplemental Material:

- Indicators of compromise (IOCs) for each of the exploits can be reviewed at: Medium.com.

Is Your Institution Overestimating Cyberpreparedness?

Summary:

The Experian *2017 Data Breach Industry Forecast* documented a recent study of 307 risk managers, insurance brokers and legal experts by *Advisen* to understand which cyber-threats concerned them the most. According to a *CUTimes* article, topping the risk list for 2017: **ransomware** or holding the network hostage for extortion; **electronic funds transfer** to unauthorized recipient due to phishing or social engineering; and **breach** of personal or financial information due to phishing or social engineering.

While organizations and their support teams generally align on top security threats according to the report, they do not agree on businesses' ability to effectively avoid and respond to these threats.

Risk to Community Institutions:

The report mentions three overriding concerns:

1. Companies overestimate their cyber-preparedness. While more than 72% of risk managers rated their network protection as above average, most data brokers and legal experts rated their clients as average or below average (67% and 52%, respectively). Both legal experts and brokers (54% and 61%, respectively) stated their clients do not have the knowledge required to work with vendors and the government to navigate cyber-risks.
2. Cybersecurity remains a challenge for small businesses, many of which fall in the credit union wheelhouse. Seventy-five percent of brokers and legal experts noted that their small business clients are either "not prepared at all" or "not very well prepared" to respond to a cybersecurity incident.

Based on our experience, the top data breach trends of 2017 are anticipated to include the following:

- Aftershock password breaches will expedite the death of the password
- Nation-State cyber-attacks will move from espionage to war
- Healthcare organizations will be the most targeted sector with new, sophisticated attacks emerging
- Criminals will focus on payment-based attacks despite the EMV shift taking place over a year ago
- International data breaches will cause big headaches for multinational companies

2017 Fourth Annual Data Breach Industry Forecast. Courtesy of Experian

3. Employee negligence is a concern across the board. All three groups of respondents recognize the need to continue to educate employees, rating it as the top area of cyber-incident prevention that companies should prioritize (brokers 35.6%; legal 41.6%; risk managers 31.6%).

Remediation:

Do the above observations resonate within your institution? As anyone in a leadership role knows, finding the balance between products, service, maximizing protection against cyberthreats and remaining cost effective can be a challenge for smaller institutions.

To avoid solely becoming a cost center within your CI, *Ayehu* outlined a return-on-investment model that can help you to move your security departments forward and raise the effectiveness and confidence of your business unit.

- First identify and capture, as accurately as possible, the costs associated with a security incident. For instance, the following factors can and often do influence cost:
  - Percentage of incidents that lead to an actual breach
  - Percentage of threats that are major incidents
  - Average cost of a major incident
  - Percentage of threats that result in minor incidents
  - Average cost of a minor incident
  - Average annual growth of security threats and incidents
- Account for additional operation factors such as:
  - Average number of incidents per day
  - Number of incidents being addressed daily using current resources
  - Gap between addressed and unaddressed incidents
  - Number of incidents addressed daily using new incident management strategy
- If you are a one- or two-person shop with multiple responsibilities, developing such metrics can assist you in obtaining support from the top and pave the way towards security maturity.

Tip of the Week: Member Benefits – Live Info Sharing

There are many ways to participate in live information sharing. A full catalog of events and instructions on how to participate or request an event can be found on the website at: fsisac.com/events.

Bi-weekly Threat Calls

Bi-weekly threat calls are held for Standard, Premier, Gold, Platinum and MSP members. In the US, they are held two Thursdays a month at noon eastern time (ET), EMEA calls are held two Thursdays a month at 14:00 GMT/15:00 CET and our APAC calls are offered the last Wednesday of every month. The latest threats are discussed, a briefing is provided by a leading security vendor and the overall threat level for the entire financial services sector is set during these calls. No action is needed to receive an invitation to these calls; a Portal announcement is sent out prior to each meeting with call-in information.

Emergency Member Calls

FS-ISAC convenes emergency member calls if there is an imminent threat or if a significant incident has occurred. An example of this type of call is the series of calls held prior to, during and in the aftermath of Hurricane Sandy in the US; the calls around the Heartbleed and Shellshock vulnerabilities globally; the Charlie Hebdo attacks from 2015; and the Apache Struts or WannaCry. Notification of such calls will be sent out through a Portal announcement.

Member Summits

FS-ISAC holds four annual Summits: two are held in the US in the spring and fall; one in the EMEA region and one in the APAC region. The Fall Summit will be held at the **Baltimore Marriott Waterfront** on **October 1-4, 2017**. Information is available at: fsisac-summit.com/2017-Fall-Summit-Overview.

Information Sharing Workshops and Member Meetings

FS-ISAC provides a forum for members to attend in-person events in various regions of the world, bringing together members in the same locality to discuss current high-priority and relevant topics and trends. In Europe, there are workshops throughout the year and member meetings each quarter. In the APAC region, FS-ISAC hosts several workshops a year in countries with members (including Australia, Japan and Singapore). These meetings are open to any member organization with relevant staff in the region. Information on these opportunities can be found at: fsisac.com/events.

Webinars

Members and partners from the vendor community host ongoing webinars open to all members. Some webinars are recorded and can be accessed for those who register but are unable to attend. Members who want to view a webinar are highly recommended to register to ensure access to the recorded version. Webinars are posted to the Portal on a situational basis that is related to the vendor's willingness to make the recorded version available for future use. Not all webinars are recorded and it is recommended that you register for any webinars in which you are interested. A listing of upcoming webinars can be found at fsisac.com/events.

Training

The FS-ISAC hosts Cyber-Intelligence Tradecraft Trainings, which is conducted by Treadstone 71 and analytic trainings, developed in part with Globalytica. These trainings are open to FS-ISAC member organizations and subject to approval. The week-long Cyber-Intelligence Tradecraft Training is usually held at the FS-ISAC's headquarter offices in Virginia, but can also be held at other locations worldwide. Attendees are expected to have the technical ability to install software on laptops, have a knowledge of social media and a knowledge of web browsers and search engines. The analytic training program provides onsite and online options in a variety of topics including: fundamentals of intelligence analysis, critical thinking skills, effective writing and briefing, the use of structured analytic techniques and managing analysis. You can find more information on the training, including the course requirements, cost and registration on FS-ISAC's trainings page at: fsisac.com/trainings.

Questions:

If you have any questions about this week's report, please contact Community Institution & Associations. Content provided for internal use by FS-ISAC members. Copyright owners retain all copyrights to material referenced.

Member Services:
admin@fsisac.com
Toll-Free: 877-612-2622 – prompt 1 Outside US: 1 571-252-8517

Security Operations Center:
soc@fsisac.com
Toll-Free: 877-612-2622 – prompt 2