COMMUNITY INSTITUTION & ASSOCIATIONS RISK SUMMARY REPORT

Week of November 12

FINANCIAL SERVICES ISAC

● TLP: Green ● ACTL: Guarded ● PTL: Guarded ● Terrorism TL: Elevated Follow Us in + ✉

In This Issue

STOP | THINK | CONNECT

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 (CIs).

NEWS

US, Russia and China decline to join Macron's cyberpact. The Paris Call for Trust and Security in Cyberspace (PCTSC) from French President Emmanuel Macron was signed by 51 countries, more than 200 businesses and 92 nonprofits and advocacy groups. The PCTSC was launched by French President Emmanuel Macron on Monday and represents an attempt to set clear rules for the use of cyber-weapons. The pledge is a mostly symbolic gesture to work toward preventing cyberthreats. The US, China and Russia, however, are among a list of countries that have not signed the pact. (*Telegraph*)

RISKS

Emotet campaign ramps up with mass email harvesting module. *Threat Post* states that a large-scale spam campaign has launched, spreading the Emotet banking trojan. The offensive has launched about a week after a fresh module for mass email-harvesting was detected for the malware. Recently, Emotet added a new module to up the ante on its ability to harvest victim email account credentials and contact lists: It can now exfiltrate entire email contents stretching back 180 days. The emails are currently targeting English and German-speaking users in this latest Emotet campaign and appears to be most active in the Americas, the UK, Turkey and South Africa. Researchers at ESET state the spam is well-crafted and contains malicious links or Microsoft Word and PDF attachments disguised as invoices, bank account alerts or payroll reports. In terms of protection, since the Word documents distributed in this campaign require users to enable macros, admins should adjust Office settings to restrict or disable that option altogether.

Unpatched Android OS flaw allows adversaries to track user location. A flaw in the Android mobile operating system could allow an attacker with physical proximity to a WiFi router to track the location of users within the router's range. The issue (CVE-2018-9581) allows information leakage stemming from inter-process communication. While applications on Android are usually segregated by the OS from each other and from the OS itself, there are still mechanisms for sharing information between them when needed. One of those mechanisms is the use of what Android calls "intents." The implication for traveling leadership or political dignitaries could result in hostage, ransom, physical intrusion and terrorism scenarios. (*Threat Post*)

Attackers exploit GDPR compliance plug-in for WordPress. A WordPress plug-in that's supposed to help with General Data Protection Regulation (GDPR) compliance contains a dangerous privilege escalation vulnerability that attackers have been actively exploiting to compromise websites. Known as the WP GDPR Compliance plug-in, the software module helps ensure compliance with the regulation by providing tools through which site visitors can permit use of their personal data or request data stored by the website's database. Wordfence reports that malicious actors have been leveraging this ability to change values in order to add new admin accounts onto affected sites. Gaining admin privileges then allows these attackers to seize control of websites in order to potentially redirect users or potentially install malware. (*SC Magazine*)

This Week's Top Risks

- **Threats, Malware and Cybercampaigns**
  - Emotet
  - Cryptomining
  - Maldoc
  - MalSpam Bitcoin Miner
  - Spytector keylogger
- **Physical Security Threats**
  - California wild fires in Paradise and Malibu, CA
- **System Vulnerabilities (multiple)**
  - Adobe, Alien Vault, Apache Struts, Brocade Fabric OS, Cisco, Google Chrome, HP, IBM, Intel, McAfee, Microsoft, PostgreSQL,RSA, Red Hat, SUSE, VMware and WordPress.
- **Themed Phishing Campaigns**
  - Bank-themed (multiple)
  - New Voice Mail
  - Payment Remittance

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.

Threat of the Week: System Vulnerabilities

Significant vulnerabilities highlight the need for patching

Summary:

This week has seen a significant number of system vulnerabilities harkening the need again for patch management programs that mitigate gaps in your various software including operating systems, information disclosure, client denial of service bypass, content collector for email Apache Struts and the list continues.

Patch Management Best Practices

Know What You Have	• Identify devices and software • Create and maintain an inventory
Identify Prioritize	• List absolute updates to resolve a major vulnerability • Minimize the amount of patching without compromising the security
Create Program & Maintain it	• Establish and enforce policies; ensure everyone is in sync; avoid untested patches • Lock down systems to avoid tampering
Cover Everything and Test	• Servers, PCs, mobile devices, embedded and legacy systems • Make testing an absolute a priority to minimize any negative impact
Formalize Your Program	• Formalize your process, be consistent and regularly apply patches • Check regularly for vulnerabilities and apply tested patches

Physical Security Checklist

Is your institution investing the same resources on physical security as cybersecurity?

Summary:

The focus on cybersecurity continues to be a key focus for many institutions and regulators. Institutions spend thousands of dollars each year assessing and testing their cyber perimeter for vulnerabilities; employee awareness surrounding phishing and ransomware; and the list goes on. It’s important for institutions to remember their physical offices hold a tremendous amount of paper containing sensitive corporate information (merger/acquisition), personally identifiable information. Continued on page 3.

UPCOMING EVENTS

FREE WEBINARS:

Financial Services - Is Your Organization Prepared for a Phishing Attack?

Thu, Dec 7, 2018 10:00 a.m. EST

Register

EXPERT WEBINAR SERIES:

Overcoming the Top Ten Challenges to Omnichannel Fraud Management

Tue, Nov 27, 2018 10:00 a.m. EST

Register

Using the Power of Threat Intelligence to Disable Banking Trojans

Tue, Dec 11, 2018 10:00 a.m. EST

Register

CYBER-RANGE RANSOMWARE EXERCISES:

Federal Reserve Bank of Boston

Wed, Jan 30, 2019

Federal Reserve Bank of Atlanta

Tue, Mar 19, 2019

Federal Reserve Bank of Chicago

Thu, Jul 25, 2019

Federal Reserve Bank of St. Louis, MO

Thu, Aug 22, 2019

In addition, branches contain large amounts of cash in their vaults, daily cash limits for teller cash drawers, loan centers where hard copy loan documents are stored, and data centers containing servers.

Physical access and damage or destruction to physical components can impair the confidentiality, integrity, and availability of information. Financial institutions should implement appropriate preventive, detective, and corrective controls for mitigating the risks inherent to those physical security zones.

Access should be restricted to the following equipment or areas:

- Operations centers (e.g., data center operations, security operations center, and network operations center) or server rooms; uninterruptible power supplies and backup generators.
- Funds transfer and automated clearinghouse routers.
- Telecommunications equipment.
- Media libraries.
- Equipment removed from the network and awaiting disposal.
- Spare or backup devices.

FFIEC Physical Security Guidelines

Detection devices, when applicable, should be used to prevent theft and safeguard the equipment. The devices should provide continuous coverage. Detection devices have two purposes-to send alarms when responses are necessary and to support subsequent forensics. Alarms are useful only when response will occur.

Using a Checklist

BankInfoSecurity posted a sample checklist institutions may find useful in the event you do not yet possess one currently. The below list is a useful start; however, each institution must assess the risks to their individual organization.

1. Are physical controls documented?
2. Are secure areas controlled?
3. Are review and maintenance of access controls taking place?
4. Are there non-standard entry points to secure areas?
5. Are these non-standard entry points secured and/or monitored?
6. Are visitors required to have supervision at the institution?
7. Are visitors allowed within secure areas?
8. If your organization shares access to your facility, does it have proper controls to segregate access?
9. Is sharing physical access to the institution by other organizations documented?
10. Are there contracts or agreements with the organization regarding this physical access?
11. Has a physical penetration test been performed?
12. Are magnetic media stored in accordance with regulatory requirements and manufacturers' suggested standards?
13. Do guards at entrances and exits randomly check briefcases, boxes or portable PCs to prevent unauthorized items from coming in or leaving?
14. Do guards allow visitors to bring laptop computers into the institution without proper signoff or authorization?
15. Are fire detectors and an automatic extinguishing system installed on the ceiling, below the raised flooring and above dropped ceilings in computer rooms and tape/disk libraries?
16. Are documents containing sensitive information not discarded in whole, readable form? Are they shredded, burned or otherwise mutilated?
17. Are DVD and CDs containing sensitive information not discarded in whole, readable form? Are they "shredded" or mutilated with no restoration possible? (This also should be asked of hard drives and other data storage technology prior to disposal).
18. Are data center and server center activity monitored and recorded on closed-circuit TV and displayed on a bank of real-time monitors?
19. Does access to a controlled area prevent "Tail-gating" by unauthorized people who attempt to follow authorized personnel into the area?

2019 Annual Summit Call for Presentations is OPEN!

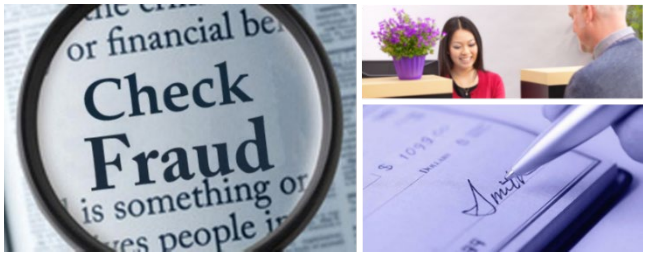
Submit your proposal by December 5 to share your ideas and expertise with your peers and attend for free!

Tis' The Season

The holiday season marks the beginning of increased fraud activity, follow our series on preventing financial loss

With the large number of on-line financial transactions that are expected to be conducted during the holidays, financial institutions are reminded to be on the look-out for cyber-criminals hoping to take advantage of poor cyber-hygiene, unpatched operating systems and security software. In addition, fraud attempts against your payment systems, online and mobile banking could place your customers in the cross-hairs of bad actors.

This week we begin our annual series of the common fraud scams to help institutions avoid monetary loss and cyber incidents, particularly during the holiday season.



Week One: Check Fraud

Check fraud is still a major vector used by malicious actors to commit financial crimes.

There are several basic forms of check fraud used by grifters and they all contain "Red Flags" that will enable you to quickly and accurately identify them. Fraudulent checks have similar characteristics.

Red Flags

1. The account is opened with minimal cash funds
2. The account has been opened for less than one year
3. The deposit amount is out of normal for this customer
4. The CI does not have "recourse" meaning there are insufficient funds in the account to make the CI whole
5. The check is in payment for Internet Auction, Lottery or Online Work at Home job
6. The customer depositing the item into their account for family or friend

About the Item

1. Identify the Red Flags association with various forms of check fraud
2. Take advantage of security features found on checks, cashier's cheques, and Traveler's cheques
3. Use fraud detection tools
4. Determine if your institution has "recourse?"
5. Ensure the item is within your check cashing guidelines
6. Take the item to your supervisor if you suspect something wrong with the item
7. For commercial customers, use Positive Pay

Next week's article will discuss card fraud.

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

FS-ISAC Analysis Team:
IAT@fsisac.com
Toll-Free: 877-612-2622 – prompt 2

For more TLP White about FS-ISAC information, follow us on Twitter @FSISAC and join the discussion on LinkedIn.