COMMUNITY INSTITUTION & ASSOCIATIONS RISK SUMMARY REPORT

Week of May 7

FINANCIAL SERVICES ISAC

TLP: Green | ACTL: Guarded | PTL: Guarded | Terrorism TL: Elevated | Follow Us

STOP | THINK | CONNECT™

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

CIO 100 Award Winners: FS-ISAC and Sheltered Harbor. We are proud to announce that both FS-ISAC and Sheltered Harbor have been recognized by IDG'S CIO as individual recipients of the 2018 CIO 100 Awards! The 31st annual award program recognizes organizations around the world that exemplify the highest level of operational and strategic excellence in information technology.

Twitter to All Users: Change Your Password Now! In a blog post, Twitter's Chief Technology Officer Parag Agrawal wrote, "When you set a password for your Twitter account, we use technology that masks it so no one at the company can see it. We recently identified a bug that stored passwords unmasked in an internal log. We have fixed the bug, and our investigation shows no indication of breach or misuse by anyone." For extra caution, though, they asked all 330 million users to reset their passwords as soon as possible at Twitter.com.

Additional recommendations in the blog post include changing your password on any other website where the same password was used; setting a strong Twitter password that isn't used on other websites; using a password manager to enable using a very strong password; and, most importantly, enabling login verification, also known as two-factor authentication. This is the single best action you can take to increase your account security.

RISKS

Hurry Up Patching Those Oracle Bugs: Attackers Aren't Waiting. The time from patches being released and attackers reverse-engineering the code to find and exploit the vulnerabilities is getting ever shorter; SANS Institute has determined it's now about three hours, which means that system admins and security teams need to come up with a better solution to patch bugs *quick*.

However, system admins who installed the patch for the CVE-2018-2628 remote code execution flaw are warned that the patch can be bypassed. Admins are recommended to restrict access to TCP/7001 web port (the default WebLogic Server Administration listen port) as much as possible. Port 7001 can be changed to anything from 7001-9000, so admins may consider researching and changing the port as well.

Cryptojacking Malware Exploits Drupal Flaws. Recently patched Drupal bugs are being exploited to install the Coinhive cryptojacking malware on websites and infect visitors. So far, over 400 sites were found hosting Coinhive, courtesy of the "Drupalgeddon" exploit.

Are New 'Spectre-Class' Flaws in CPUs About to be Exposed? A German website is reporting that eight new Spectre-like computer processor vulnerabilities are soon to be revealed. Dubbed "Spectre Next Generation" or "Spectre-NG", the flaws affect Intel and ARM processors; ongoing research will determine AMD's chip susceptibility. Four of the flaws are classified as high severity and four as medium severity; they all have CVE identifiers assigned. Patches and updates are being prepared for release.

This Week's Top Risks

- **Malware, Ransomware and Trojans**
  - » GandCrab ransomware
  - » SynAck ransomware
  - » SamSam ransomware
  - » Remcos RAT
  - » JBifrost RAT
  - » Ursnif
  - » Coinhive cryptominer
- **Physical Security Threats**
  - » Hawaii: Earthquakes, volcanic lava flow and poisonous gas leaks
- **System Vulnerabilities (multiple)**
  - » Adobe, Oracle, Cisco, Microsoft, Oracle, Red Hat, Linux
- **Themed Phishing Campaigns**
  - » Bank-themed (multiple)
  - » Dropbox
  - » Order-themed, MS Equation Editor
  - » "Purchase Order" or "PO##"
  - » Venmo
  - » SWIFT-themed

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.

Save the Date

May 15: *Expert Webinar Series: Perspectives on Achieving Cloud Security for Financial Institutions.* Presenters from *iBoss* and *Prevalent* will talk about how, as cloud solutions proliferate, organizations are reviewing their risk strategy and approach. In this webinar we navigate the complexity of adding cloud solutions to business operations, how cloud solutions intersect with data protection requirements and what cloud functions or features reduce risk. Best practices are discussed to highlight security solutions outside of the traditional and known firewall protections.

May 20-24: *FS-ISAC Annual Summit.* Members who will be in Boca Raton, FL later this month are invited to attend two special sessions created just for our CIAC members:

- May 21: 7:00–8:00 a.m. – Community Institution Welcome Breakfast, Grand Ballroom B
- May 22: 8:00–9:00 a.m. - Community Institution Council Roundtable Discussion, Veranda III

We will offer insight on how to get the most benefit from your time at the Summit, go over CI-recommended sessions and have time to discuss the issues you're facing and/or solutions you've found in your institution.

May 21: *FS-ISAC Fall Summit Call For Presentations Opens*! It's never too early to start brainstorming what you have to offer in a Summit presentation. The Fall Summit will be held in Chicago on November 11-14. To begin your thought process, consider an issue that you tackled in a savvy, smart or MacGyver-like way and then encourage yourself to share it with others.

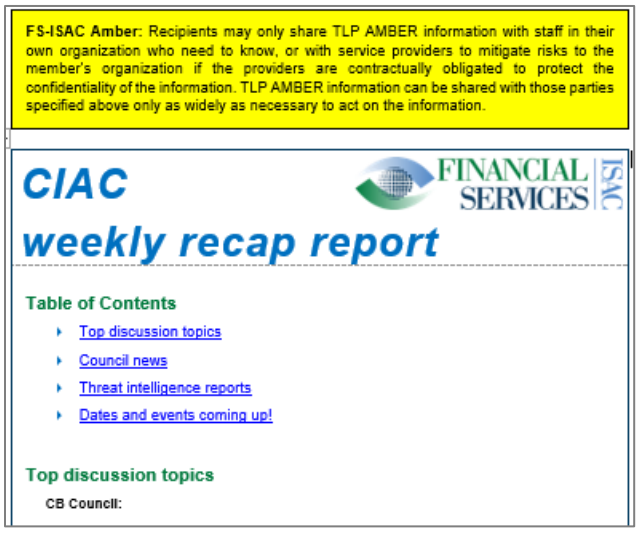
June 18: *Next CIAC Meeting.* Due to the Annual Summit occurring on the same date as our regularly scheduled meeting, there will be no May meeting. Our next CIAC meeting will be held on June 18, 2018 at 3:30 p.m. EDT.

New Weekly Recap Report

A new CIAC Friday report will summarize the bright points of the past week's activity

Summary:

For an information sharing community like FS-ISAC, it is a sign of success that we receive so much valuable threat intelligence information from our members and partners. It indicates that we have efficient information intake procedures and that we have built valuable *circles of trust* with our constituents.


FS-ISAC Amber: Recipients may only share TLP AMBER information with staff in their own organization who need to know, or with service providers to mitigate risks to the member's organization if the providers are contractually obligated to protect the confidentiality of the information. TLP AMBER information can be shared with those parties specified above only as widely as necessary to act on the information.

CIAC FINANCIAL SERVICES ISAC

weekly recap report

Table of Contents

- Top discussion topics
- Council news
- Threat intelligence reports
- Dates and events coming up!

Top discussion topics

CB Council:

However, this sign of success can also be a growing pain, especially for newer or smaller members who are just joining the mailing lists and are only now getting exposed to this threat intelligence. To keep members well-informed without sending individual emails, the Community Institution and Association Council (CIAC) has created a weekly recap report.

The curated TLP Amber content within this weekly recap pulls data from the CIAC mailing lists, cyber-intelligence list and other working groups in a concise format. The report will include a list of the most active discussion topics from the CBC, CUC and CIC; significant CIAC news; threat intelligence reports that members may have missed; and upcoming dates and events. Members can use this information to perform additional research on topics of interest.

Right Sizing Email

Members are reminded they can significantly reduce the number of emails they receive by logging into the FS-ISAC Portal and adjusting their alerts profile selection. By deselecting all alerts except for the COI: "FS-ISAC Intelligence" Report and Announcements members can reduce their alert volume to an average of two emails per day.

For additional instructions on how to make these changes, please review the following Risk Summary Report issues:

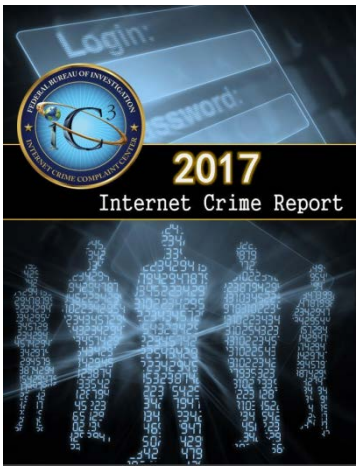
- 04-30-2018 Risk Summary Report – Managing FS-ISAC Alerts
- 02-15-2018 Risk Summary Report – Tip of the Week: Right Sizing FS-ISAC Emails

Remember: If you require assistance, please contact Jeffrey Korte, Heather McCalman or Member Services.

Threat of the Week: Fraud Losses Down, Complaints Up

The FBI releases the IC3's 2017 Internet Crime Report this week; here's what's inside

Summary



The Federal Bureau of Investigation (FBI) mission is "to protect the American people and uphold the Constitution of the United States." Included within "protect the American people" is the direction to investigate and prosecute crimes waged against US citizens.

As the trend for fraud to occur electronically and over the Internet increased, the FBI launched the Internet Crime Complaint Center (IC3) in 2000 to "provide the public with a reliable and convenient reporting mechanism to submit information to the FBI concerning suspected Internet-facilitated criminal activity, and to develop alliances with industry partners." When a citizen contacts law enforcement to file a complaint of electronic fraud, officers direct the citizen to make their complaints known via online submissions to the IC3. From these submissions, the FBI analyzes and aggregates the data, and provides that information to local FBI offices for intelligence and investigative purposes.

The IC3 2017 Internet Crime Report includes several success stories, where complaints filed by US victims of online fraud were used to correlate and investigate larger fraud schemes in Houston TX, Los Angeles CA and Knoxville TN. The result of the investigations were the apprehension and prosecution of the criminals defrauding and stealing the monies of innocent citizens.

Fraud Losses Down, Complaints Up

The following image shows the year-to-year statistics for fraud complaints versus fraud losses. Comparing 2016 to 2017, while fraud dollar losses dropped $32M, the number of complaints rose by 2,852 cases.

What may be most telling, though, is that in the past five years, there have been well over one million total complaints, which is an average of 284,000 complaints per year. Those 1.421 million complaints netted ***$5.52 billion*** in losses for the fraudsters. These figures show that fraud is still a very lucrative business.

Using the Report for Fraud Prevention

One of the important ways a community institution can use the IC3 annual report for is to understand fraud trends, who is getting duped and victimized, and what types of fraud methods are being used the most. CIs can use this information to put fraud analytics in place and more heavily monitor for signs of abuse and schemes with their customers and members.

For instance, last week's *Risk Summary Report* included an article on the financial abuse of vulnerable adults, primarily elders. The 2017 IC3 report shows that victims over age 60 suffered the greatest losses, both in the total count of fraud complaints (49,523) and in the total monetary loss (over $342M). To compare, the second-highest total monetary loss was $275M, showing that seniors who should be enjoying the fruits of their labor are prime targets and, therefore, should receive special attention as potential victims by institutions.

As a result of this increasing threat, on Feb. 22, 2018, the Department of Justice launched the Elder Justice Initiative.

(Story continued on page 4)

2017 Internet Crime Report Hot Topics

In addition to a focus on elder financial abuse and fraud, the other hot topics from the report include "Business Email Compromise" (BEC), "Ransomware", "Tech Support Fraud" and "Extortion". BEC and its variation, Email Account Compromise (EAC), accounted for the greatest fraud losses, as shown in the table below.

By Victim Loss			
Crime Type	**Loss**	**Crime Type**	**Loss**
BEC/EAC	$676,151,185	Misrepresentation	$14,580,907
Confidence Fraud/Romance	$211,382,989	Harassment/Threats of Violence	$12,569,185
Non-Payment/Non-Delivery	$141,110,441	Government Impersonation	$12,467,380
Investment	$96,844,144	Civil Matter	$5,766,550
Personal Data Breach	$77,134,865	IPR/Copyright and Counterfeit	$5,536,912
Identity Theft	$66,815,298	Malware/Scareware/ Virus	$5,003,434
Corporate Data Breach	$60,942,306	Ransomware	$2,344,365
Advanced Fee	$57,861,324	Denial of Service/TDoS	$1,466,195
Credit Card Fraud	$57,207,248	Charity	$1,405,460
Real Estate/Rental	$56,231,333	Health Care Related	$925,849
Overpayment	$53,450,830	Re-Shipping	$809,746
Employment	$38,883,616	Gambling	$598,853
Phishing/Vishing/Smishing/ Pharming	$29,703,421	Crimes Against Children	$46,411
Other	$23,853,704	Hacktivist	$20,147
Lottery/Sweepstakes	$16,835,001	Terrorism	$18,926
Extortion	$15,302,792	No Lead Value	$0
Tech Support	$14,810,080		

2017 Crime Types "By Victim Loss" table from IC3 Report, pg.21

Diving Deeper Into the BEC/EAC Topic

BEC/EAC, for the IC3, includes scams that target businesses or individuals performing wire transfer payments. Most of these victims report the use of wire transfers to send funds, while some reported using checks. Per the report, "Both scams typically involve one or more fraudsters, who compromise legitimate business email accounts through social engineering or computer intrusion techniques to conduct unauthorized transfers of funds."

These schemes have evolved over the years from targeting executives and finance staff to perform illicit wire transfers, to criminals impersonating lawyers or law firms and instructing secret or time sensitive wire transfers, to targeting Human Resources departments to steal employees' W2 information. In 2017, the real estate sector moved into the crosshairs with most victims reporting losses during real estate transactions.

BEC/EAC scams are heavily linked to other forms of fraud as well, including but not limited to: romance, lottery, employment and rental scams and may include the victimization of money mules to enable the illegal transfer of funds to others. Community institutions should consider increasing their authorization and performance of wire transfers over an increased threshold or for real estate transactions where the receiver's information is changed at the last minute.

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.