COMMUNITY INSTITUTION & ASSOCIATIONS RISK SUMMARY REPORT

Week of January 01

FINANCIAL SERVICES ISAC

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

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).

ALERT

Researchers Discover Two Major Flaws in the World's Computers. A team of researchers from various universities and organizations has discovered major vulnerabilities with the computer CPUs that are powering almost all, if not all, of the PCs around the world. The flaws were dubbed Meltdown and Spectre and, according to *The New York Times*, they could allow attackers to access the memory contents of personal computers, mobile devices and servers, including those running cloud computing networks.

Meltdown may be remedied with a patch; manufacturers and cloud providers are addressing the issue as quickly as possible. Spectre, on the other hand, is more difficult to address and could require a redesign of computer processors. FS-ISAC members can access the Cyber Threat Alert about the flaws, Tracking ID 936983, via the Portal for more information.

NEWS

Financial Institutions Team Up on Data Security Push. The chairs of the House Committee on Energy and Commerce and the Subcommittee on Digital Commerce and Consumer Protection received a letter from seven trade associations representing banks and credit unions. The letter is a follow-up to the Data Security Act (DSA), unanimously supported by the financial industry in the 2016 Congress. The DSA outlined three goals to protect consumers' online data, including asking for stricter cybersecurity standards for all entities to protect sensitive personal and financial data.

According to a report in *American Banker* and as reported on *PYMNTS.com*, the letter was signed by the following associations and trade groups: American Bankers Association, Consumer Bankers Association, Credit Union National Association, Financial Services Roundtable, Independent Community Bankers of America, National Association of Federally Insured Credit Unions and The Clearing House. The signers hope that Congress will make consumers' data security a priority now that the tax reform bill has been signed.

Nissan Canada Finance Issues Data Breach Alert. The finance company that provides financing for Nissan buyers and leasers in Canada is warning 1.3 million current and former customers that their personal information may have been stolen. *Bank Info Security* reports that Nissan Canada Finance (NCF) issued a security alert that it is a victim of a breach. NCF is notifying customers by letter and email, where possible. Potentially exposed data includes customer name and address, vehicle make, model and identification number, credit score and loan and payment amounts.

On a good note, it only took NCF ten days to move from discovery of the breach to notification of its customers.

This Week's Top Risks

- **Malware, Ransomware, Trojans**
  - » QakBot
  - » Imminent Monitor RAT
  - » Gozi
  - » Pony
  - » TTP change in Cobalt Group emails
  - » Hidden Cobra
  - » TrickBot
  - » NanoCore RAT
  - » Adwind Trojan
  - » UDP flood (DoS/DDoS)
- **Physical Security**
  - » Severe winter weather across the US
  - » Iranian protests and counter-protests
  - » Increasing nuclear threat between US and North Korea
- **System Vulnerabilities**
  - » Apple (multiple), Linux (multiple), Mozilla Thunderbird, VMWare VNC
- **Themed Phishing Campaigns**
  - » Bank-themed (multiple)
  - » Account Verifications
  - » "Urgent Tax Settlement"
  - » Security alert-themed
  - » Payment Invoices & Purchase Orders
  - » Scanned documents

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.

New Portal Format Available

To make the FS-ISAC Portal more user-friendly and intuitive, changes have been made to the Portal menus. Now, when members login, they'll see a "Working Group/Committees" link replacing the previous "Documents" link.

Within the "Working Groups/Committees" link are three menu options:

- **Directory**. List of various Council/Working Groups, their mission and the FS-ISAC staff contact.
- **Documents**. Library of downloadable documents that are available for member use.
- **Library**. Consolidated resources that were previously located in various places within the Portal.

These changes are our first steps to making the Portal a more user-friendly experience. Please let us know what you think and how you like it. Feel free to drop us a note: **Jeffrey Korte** or **Heather McCalman**

Cybersecurity Trends for 2018

Summary

Predictions and prognostications can be tricky. Like weather forecasts that promise sunshine and warm weather when in real life it rains and grows chilly, most people only remember if the foretelling was wrong and caused problems or issues.

Sometimes, though, it's good to do a reality check and be honest about what the future holds. For information security and cybersecurity pros in all industries, but especially in community institutions, this is a crucial exercise; it is an exercise that, when done correctly, will allow CI staff and management to prepare adequately for what lies ahead.

The top ten list of cybersecurity trends outlined below comes from *Bank Info Security*. Here's what to expect in 2018:

1. **More Big, Bad Breaches.** Old breaches (breaches from previous years) will come to light and be exposed, while new breaches will continue to occur due to legacy systems that remain unpatched but in use.
2. **More Poor Security Practices.** In addition to organizations using outdated technology, the following bad practices will remain in use:
   - Poor passwords;
   - Lack of patching;
   - Out-of-date anti-virus software;
   - Lack of monitoring; and
   - Using vulnerable and old systems.
3. **More Endpoint Security Woes.** Patching, patching and more patching. Considering that 80 to 90 percent of ransomware uses common vulnerabilities, patching endpoints quickly should be a priority**,** but it remains a challenge for organizations.
4. **More Takedowns.** NOTE: Sharing information is required for takedowns to occur.
5. **More Bitcoin Heists.** While the surge in bitcoin is making it a valued commodity, it is also a growing target for threat actors. Cybercriminals and nation-states alike have shifted the focus of their attacks to bitcoin hacking.
6. **More Extortion Shakedowns.** As well, with the rise in the value of bitcoins, ransomware is more profitable. Pair these developments with Internet of Things vulnerabilities and every individual with a connected device becomes a potential victim.
7. **Online Proxy Wars.** Where nation-states battle, consumers' online lives may become more accidental casualties.
8. **Market Consolidation.** The result of mergers and acquisitions may be easier to manage technology offerings.

9. **More EU Breach Notifications.** Under the General Data Protection Regulation (GDPR), organizations must notify authorities within 72 hours of learning they may have been breached and they must stop using personal information upon request, unless there is a valid business reason to continue.

10. **GDPR Fines.** While fines of up to four percent of a company's global annual profits are possible, experts agree that the most severe fines for GDPR violations will be "reserved for organizations that not only failed to invest in proper information security practices but actively covered up breaches or engaged in other illegal behavior."

Here's to more takedowns, better security practices and to fewer breaches and GDPR fines for small organizations!

The Financial Sector's Best Cybersecurity Practices

CUES.org provides a list of processes and resources used by large institutions to protect against insider threats. Provided in the Tech Time section of the December 2017 magazine, insiders are cited as one of the leading causes of data breaches. Of course, insiders include any human risk posed by people with privileged access, including staff, vendors, strategic partners, administrators and managers. Insider threats may result from malicious intentions or through negligence. **Sector collaboration** is included with other best practices such as implementing the NIST Framework, understanding vendor permissions and planning and testing for incidents. FS-ISAC is named as the primary information sharing organization for the financial industry. "Credit unions should not only share cyberthreats but also resources to help prevent incidents before they occur."

Artificial Intelligence: The Solution to or the Source of Intrusion?

Summary

Cybersecurity pros who have been in the industry long enough know that there is no magic bullet or a one-size-fits-all solution to defend against threats and mitigate risks. Any security professional worth their salt will tell a novice or the as-yet uninitiated to layer defenses, train all employees according to their needs and prepare for the worst.

As well, security professionals who have survived the cycles of new and expanding technology know that any new advancements made in online or connected systems, even those used to defend against attackers, will one day be co-opted by attackers and used to wage attacks. The stories from 2017 of anti-virus software being used to retrieve confidential information or automatic software updates that delivered ransomware and malware are two recent examples. Open sourced and as-a-platform malicious code developments are other examples of tech advances that are now being used by threat actors.

Enter All Intelligence

Advances in computing power and concepts in artificial intelligence (AI) that are staged to be implemented in 2018 will allow for greater defenses against cyberthreats. While today's machines can't think outside the box like their human counterparts and provide all an organization's security, they are moving in that direction quickly.

Machine-learning algorithms and techniques stand ready to further aide or replace humans in detecting and thwarting attacks. With greater processing power and the ability to scan huge volumes of data, AI techniques are expanding to detect patterns of abnormal behavior that are imperceptible to humans.

But We're Not the Only Ones

Of course, any technological advancements made in the effort to defend against attacks will someday be weaponized and used to stage attacks. So, too, with AI. If they haven't already, the belief is that it's only a matter of time. Sixty-two percent of information security professionals surveyed by Cylance at Black Hat USA 2017 expect that hackers will begin using AI offensively in 2018.

In fact, at DEFCON in 2017, a data scientist showed how an automated tool learned to mask a malicious file from anti-virus engines, by changing just a few bytes of code in a way that maintains malicious capacity. Previously, phishers and hackers have manually modified code; this example showed how the process can be automated.

Add to this the increase in processing power (and the normal evolutionary ladder) and we can easily see an autonomous system that will adapt, learn new environments and identify flaws, and then morph itself to exploit those flaws.

Keeping up with the Cyber-Arms Race

To keep up with the changes, most experts indicate that, while AI is not a silver bullet that will solve all an organization's information security risks, it is important to use AI to defend against the expanding threats.

Start 2018 with Strong Firewall Security

Summary

With all the talk and articles about cryptocurrency, ransomware, AI and the latest and greatest in mobile payment systems, the importance of the basics of information security can sometimes be overlooked or undervalued. While the basics may not be as controversial or exciting as the newest Internet technology for the office refrigerator, the basics provide a foundation upon which all other layered defenses can be built.

Mind the A B Cs

One of the basic, yet essential, cybersecurity tools an organization can implement is a firewall. The firewall sits on the perimeter of the network and acts as a traffic cop for network activity. The firewall inspects traffic passing into or out of the network and, according to rules, determines if the traffic is approved to pass through.

For ingress (inbound) and egress (outbound) traffic the firewall can be configured to either allow or prevent activity from specific geographical areas, pre-set IP addresses or according to the type of traffic being communicated. Entire protocols may be allowed or restricted from being used; likewise, all traffic from a country with known malicious activity (like Russia or North Korea) may be blocked, while all traffic from the United States may be allowed.

Steps to Strong Firewall Security

There are a variety of different generations and types of firewalls and this article isn't going to attempt to explain them all. (For a basic rundown of the several types of firewalls and the level of security they provide, check Wikipedia.) However, there is a basic set of steps that can be used on all firewalls, from first generation to third or "next-generation", to ensure it will remain strong and secure:

- **Use safe password privileges and management.** Require that all employees with access to the firewall have complex passwords with additional length and strength requirements. As well, verify no employees with access to the firewall are sharing passwords to access the network or the protected device.
- **Use secure access methods.** Restrict access to the firewall to a subnetwork that only privileged users and/or machines may access. Consider providing additional layers of tunneling to access the firewall login to restrict unauthorized insiders or hackers from gaining access to the front end.
- **Use change management processes.** Since a modification to the firewall can result in carte blanche access to the wrong people outside the network, changes to the firewall, even seemingly minor changes, should be considered critical and require the highest levels of approval. At least, the Chief Technology Officer or Chief Information Security Officer should sign off on the change.
- **Verify rule efficiency.** Firewalls act on a set of rules. Some rules are pre-configured and out-of-the-box; other rules are added or edited for specificity to the organization. Invariably, rules will be implemented either by default or over a period of years but not necessarily needed long-term.

  Perform a review of the firewall rules once or twice a year to ensure only necessary and legitimate rules are in place. To make this task easier, perform an initial ruleset review and make this the baseline. Then, going forward, every six months copy the ruleset to a text editor and use a comparison software to check for changes. Compare the changes in the ruleset to the change management approvals.
- **Keep the firewall updated.** Good patch management can never be overemphasized.
- **Proactively monitor firewall security.** In addition to updates and reviews, monitor firewall events proactively.
- **Think like a cybercriminal.** It is always best for an organization's staff or a vendor with whom they have a contract to break the system, rather than wait for an attack. Once CI staff or a paid pen test vendor determines the vulnerabilities, patch them to ensure they cannot be used by a cybercriminal to access the network.

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:	Security Operations Center:
admin@fsisac.com	soc@fsisac.com
Toll-Free: 877-612-2622 – prompt 1 Outside US: 1 571-252-8517	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.