COMMUNITY INSTITUTION & ASSOCIATIONS RISK SUMMARY REPORT

Week of July 23

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

STOP | THINK CONNECT™

In This Issue

Threat of the Week: Cyber-Insurance Policy Riders

Six Things to Learn from Previous Attacks

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

FS-ISAC CEO Bill Nelson addresses attendees of World Credit Union Conference. The 2018 World Credit Union Conference (WCUC), an annual conference of the World Council of Credit Unions, was held in Singapore earlier this month. FS-ISAC's CEO Bill Nelson spoke to 200 attendees on the topic "Current and Future Cyber Threats to Credits Unions." After, attendees from Kenya, Ghana, Australia and other countries stopped to speak with him and expressed interest in joining FS-ISAC. Later, he was interviewed by Mike Lawson in the *CU Broadcast* studio at the conference.

Chrome's HTTP warning seeks to cut web surveillance, tampering. On July 24, Google released Chrome v.68, which is the de facto deadline set for websites to use encrypted formats. In other words, when viewed in Google Chrome, any site still using the HTTP:// technology, instead of the HTTPS:// encryption, will have the words "Not Secure" pre-pended to the URL in the address bar. Hypertext Transfer Protocol (HTTP) is the code that allows a browser to show a webpage with easy-to-read images and text; however, it is notoriously unsecure when it comes to sensitive communications. The new security warning is one more way browser makers are pushing site developers to protect consumer information.

RISKS

Bluetooth implementations may not sufficiently validate elliptic curve parameters during Diffie-Hellman key exchange. The *Carnegie Mellon Computer Emergency Readiness Team* (CERT) issued an alert regarding additional risks associated with the use of nearly all Bluetooth devices. In addition to the previously reported "Invalid Curve Attack," CERT is reporting a new vulnerability that may allow a remote attacker within wireless range to "inject an invalid public key to determine the session key with high probability." This would allow the attacker to passively intercept and decrypt all messages and/or forge and inject malicious messages. CIs using Bluetooth-enabled devices should do so with caution and apply updates as soon as they are released.

"MoneyTaker" hackers stole $1 million from Russian bank. *SecurityWeek* highlighted a report by cybercrime research firm Group-IB on the cybertheft of $1 million by threat actors on July 3. The cybercriminal group MoneyTaker stole the funds from PIR Bank (Russia) via the Russian Central Bank's Automated Workstation Client, an interbank funds transfer system. The hackers transferred the funds to 17 other Russian banks and then cashed out the monies. A compromised router at a regional branch was used as the entry point.

This Week's Top Risks

- **Cybercampaigns**
  - Fraudulent web account registration attempts
- **Malware, Ransomware and Trojans**
  - Emotet
  - TrickBot
  - Hancitor
  - Gozi
  - Pony
  - Nanocore RAT
- **Physical Security Threats**
  - Destructive Wildfires Raging in US West
- **System Vulnerabilities (multiple)**
  - Bluetooth, FoxIT Reader, Apache, Microsoft, Cisco, Oracle, Google
- **Themed Phishing Campaigns**
  - Bank-themed (multiple)
  - DDOS Extortion Email from "Anonymous"
  - "DHL Shipment Notification"
  - "Outstanding Payment Invoice"

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.

NCCIC Webinar Series on Russian Government Cyber Activity. The National Cybersecurity & Communications Integration Center (NCCIC) will conduct a series of webinars on Russian government cyber-activity against critical infrastructure. The same webinar will be held from 1-2:30 p.m. ET on:

- Monday, July 30
- Wednesday, August 1

NCCIC encourages users and administrators to attend one of the webinar sessions by visiting https://share.dhs.gov/nccicbriefings or dialing 1-888-221-6227. Attendees may access the webinar as a guest on the day of each event; a registered account is not required for attendees.

Threat of the Week: Cyber-Insurance Policy Riders

Not understanding a cyberpolicy coverage can add insult to injury

Summary:

Because no organization can mitigate 100% of the risk 100% of the time, the response strategy of "transferring risk" was developed. While a supplier or third-party vendor may be the first choice for a transfer of risk, cyber-insurance policies are an increasingly sought after and utilized option for "transferring risk."

Essentially, transferring risk to a cyber-insurance policy basically says that the insurance company will cover damages, response efforts and loss of funds when all other risk mitigation strategies fail, and an unavoidable compromise occurs. This new source of risk mitigation has been so popular that many Community Institution and Association Council email list conversations have focused on the nuances of cyberpolicies and at least one FS-ISAC survey has been conducted to gauge members' use.

The Wild, Wild West of Cyber-Insurance

However, like most everything in cybersecurity these days, cyber-insurance is not a panacea that will save an organization from loss of funds, or even make them whole after the loss. More so, a lack of thorough awareness by the cyber-insurance policyholder can end up being a boomerang that comes back to strike the covered party.

The stories of cyber-insurance providers refusing to meet claims from financial institutions are increasing. Many of the claim denials have resulted in lawsuits; indeed, this area of the cybersecurity landscape is uncharted territory. It involves court staff rectifying cybersecurity attack methods in the realm of historical insurance verbiage and stipulations.

As quoted in an article about the latest publicized lawsuit, Charisse Castagnoli, an adjunct professor with The John Marshall Law School, said "While it is fairly easy to write a policy around data breach liability, when it comes to actual intrusions and managing intrusions, it's a wild, wild west. The policies and definitions they use are not consistent across carriers."

The Latest Lawsuit

This week, *Krebs On Security* reported about a recently filed lawsuit between a Virginia community bank and its cyber-insurance provider. The bank suffered two intrusions in eight months that resulted in a total loss of $2.4 million. Both thefts began with phishing attacks and the compromise of computers that managed credit and debit card limits. After the first intrusion, the bank hired a forensics firm to determine what happened and resolve the compromise; as well, they implemented security practices recommended by their payments processor. However, the efforts were unable to prevent the second attack.

After recovering from the attacks, the bank filed cyber-insurance claims with their provider using the "computer and electronic crime rider" (C&E) and "debit card rider." The provider denied the C&E claim saying that the funds were withdrawn using the bank's card network, so only the debit card rider applies. However, the bank is now suing the insurance provider, citing that use of the card network wasn't possible without the C&E compromise.

Risks to Organizations:

- Community institutions should consider and heavily weigh the options of securing cyber-insurance policies; if the amount used to purchase policies is higher than a denied claim, it may be more worthwhile to forgo a policy and purchase a service-level agreement with a well-known forensics firm.

Remediation:

- CIs should review and scrutinize all riders and exceptions in cyber-insurance policies; as well, share policies with legal counsel for their review.
- CIs may also consider involving their cyber-insurance provider in incident response scenarios.

Six Things to Learn from Previous Attacks

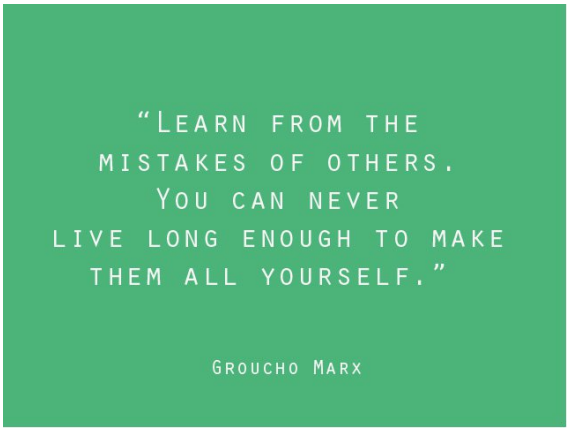
Enterprises can learn "what went wrong" from the DNC hacking attack of 2016

Summary:

The *Risk Summary Report* authors are huge fans of learning from others, especially when it comes to cyber-attacks and organizations that have been hacked. We always want to know "what went wrong?", "what went right?" and the other "who, when, where and how" questions. ("Why" is a short list: money, information, revenge or intellectual property.)

So, we're going to set aside all political ideas and opinions to go over the six things that community institutions can learn from the 2016 Democratic National Committee (DNC) hacks. Partisanship doesn't matter much when it comes to cybersecurity, as all organizations are susceptible depending on the threat actor and their specific motive.

McAfee obtained a copy of the United States Department of Justice unsealed judicial indictment against individuals involved in the DNC hacking in 2016. Below are the things to learn from the attack, with RSR author recommendations for community institutions.



1. **Nation-State Activity is Real.** While government agencies, manufacturing facilities and utilities have their own attraction for nation-state attacks, financial institutions have an attraction as well. It is for the very reason that bank robbers rob banks: Because that's where the money is.

   While cyber-criminals and gangs may target CIs for theft of funds to further their illicit and terrorist activities, nation states tend to target CIs because of global sanctions or a poor economy. While attribution is difficult to determine in many attacks, a fair number of the massive, million-dollar thefts in recent years have been attributed to nation states that are unable to trade on a global scale.

   For these bad actors, their victims' national currency of the monies stolen matters less than the insecurity of the institutions victimized.

2. **Geo-Location is Practically Irrelevant.** It once was standard to block all access from a known-rogue nation state or allow only access from countries or locations where business interests were clear. This mindset is no longer feasible, considering the global economy and the capabilities of The Onion Router (TOR) browser to obfuscate where connections are originating from.

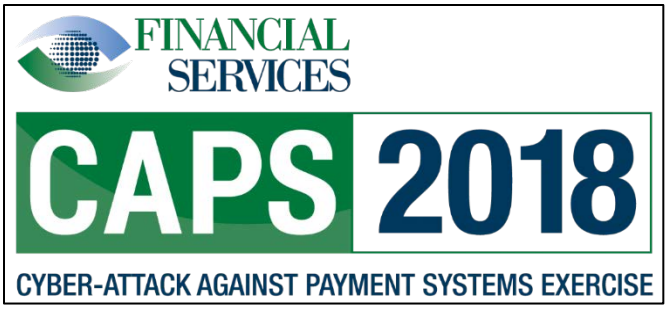
   Instead, institutions should begin analyzing the behaviors of users and systems, alike, and the access to resources. Demographic identifiers can no longer be trusted to authenticate or verify the identity or veracity of a connection. Complex two-factor authentication should be applied wherever available.

3. **URL Shorteners can be a Risk Indicator.** Oh, who doesn't love a good Bit.ly link to a video? A community institution can shorten a link, so it can be tweeted and retweeted by all their members or customers!

   For the uninitiated in the world of social media lingo, a URL shortener will reduce the character size of a very long URL so it can be posted, used in blogs or shared via other social media channels. For example, using the Bitly service, the URL for the upcoming FS-ISAC Threat Intelligence Roadshows (https://fs22.formsite.com/FS-ISAC/form228/index.html) was shortened to https://bit.ly/2v1UfYj. (If you don't trust the links in this report, please feel free to go to https://bitly.com/ and use the tool to shorten a URL yourself. Anyone, even cybercriminals can use it and it's free!)

   When paired with spear phishing campaigns, though, these innocuous looking links can become the downfall of an institution. Do your staff know what a shortened URL looks like and why they shouldn't trust them? Do they know how to determine the legitimacy of a shortened URL? These are just some questions to consider.

4. **Vulnerability Management is a Key Risk Indication.** This quote from the McAfee author is so true: "I've never known a security professional who skips into the office with their coffee and announces, *I love patching servers.* Never." In fact, Microsoft's Patch Tuesday used to come with its own special groans from the IT department of one credit union.



October 9-10 or 16-17 - CAPS Exercise. North America (NA) Sessions. Register.

(cont'd from page 3)

Patching is hard. Patches break systems. Patches break users' abilities to work efficiently. Rolling patches back isn't easy either. And, at some point, the patch needs to be applied, because, as evidenced by the Oracle WebLogic vulnerability highlighted this week, once patches are released, criminals start exploiting the vulnerabilities.

However, despite all the headaches that patches cause, the vulnerabilities they address are notoriously the path of least resistance used by cybercriminals to compromise systems and networks. In addition to vulnerabilities of public-facing systems, the DNC hacking event involved cyber-recon activities like finding public IP ownership, DNS information, routing advertisements, job listings and a host of other usable information.

Vulnerability management, in all its forms, is hard and very necessary.

5. **Response Threat Hunting is Hard – Trust Nothing.** When an organization becomes aware of the presence of a malicious actor on the network, the immediate desire is to remove the actor. However, this is not as easy as it may sound. First, cybercriminals who have successfully managed to compromise a system or a network have a very strong desire to remain hidden and to remain on the system, despite the actions taken by organizations or third-party forensics experts.

   Usually, they will either create or maintain multiple backdoors and/or points of compromise. Today's threat actor is very skilled and sophisticated; they have means and motive to "remain engaged" on a network, when their presence has been discovered. As quoted in the article, "Threat hunting in an incident is a time for humble approaches that recognize the adversaries are at or above our own skill level (and hope that is not the case)."

   The core fundamentals of "trust nothing" come in handy during an incident response and for a time afterwards. Zero trust computing and requiring validation of all activity is a must, especially since business practices, serving customers and members, is usually required while incident response is ongoing.

   If the pre-work for this type of skeptical business operation are built into the incident response plan, the implementation during an incident should be moderately time-consuming.

6. **Your organizational data is in the cloud. Your Incident Response needs to be, too.** Essentially, incident response (IR) plans should incorporate and involve cloud computing partners. While the IR plan may address compromises on the local or wide area networks, it should also address the forensic verification and recovery actions for data and services hosted with cloud providers.

   Lacking this crucial element may allow an attacker to either maintain a backdoor connection to the network or, as worse, to gain access to sensitive consumer or institution information.

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.