COMMUNITY INSTITUTION & ASSOCIATIONS RISK SUMMARY REPORT

TLP: Green | CTL: Elevated | PTL: Guarded | Terrorism TL: Elevated | Week of September 25

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

66 Days Until Hurricane Season Ends. *The Weather Channel* is reporting that, due to weather patterns, the remainder of the 2017 hurricane season could continue to produce dangerous storms. We want to remind CIAC members that we've provided the *FS-ISAC Hurricane, Storm and Flood Checklist* on the public website here. As well, we encourage FS-ISAC members to sign up for Physical SOC Alerts via the Portal before a storm hits to receive up-to-date information and daily *Disaster Executive Briefs*.

NEWS

A Credit Freeze Won't Help with All Breach Threats. *Consumer Reports* published an article citing the other risks to information exposed in highly-publicized breaches. They mention at the beginning of the article the risks that freezing credit reports at the four credit bureaus will protect against; namely, opening new accounts in an ID theft victim's name, registering as an ID theft victim on the "My Social Security" site and attempting to steal a victim's Social Security benefits. However, where tax refund fraud, health insurance/ medical fraud and driver's license risks are concerned, placing a freeze on credit reports won't provide any protection. The article gives valuable, actionable steps that can be taken to help mitigate against these risks. Just as a layered defense is the best approach to security at an institution, so, too, it's the best approach for protection against ID theft and fraud.

Report: Deloitte Suffered Breach Last Year. The *Data Breach Today* website reports on the breach experienced last year at "big four" accounting firm Deloitte, based in New York. According to the ***Guardian***, information exposed includes five million internal emails as well as "usernames, passwords, IP addresses, architectural diagrams for businesses and health information." Deloitte has hired a consultancy to investigate the breach.

RISKS

Verizon Wireless Internal Credentials, Infrastructure Details Exposed in Amazon S3 Bucket. *Threatpost* reports that "organizations continue to leak data through publicly accessible Amazon S3 buckets". Verizon is the latest business having to recover from the public exposure of sensitive internal information, including usernames and passwords that could allow attackers to access internal networks. CI staff should use reports of these exposures as a reminder to check the security on cloud services employed by the institution.

Report Documents Vulnerabilities and Role of Patching. *The Register* provided the results of a study by NCC Group, that looked at the vulnerabilities found in the finance sector. Overall, the study found that vulnerabilities have increased by 418%; however, pen testers caution the increase may be the result of the growth of banking apps in recent years. Notably, updating and patching PHP, ASP.net and Apache Tomcat will provide the greatest risk mitigation.

This Week's Top Risks

- **Malware, Ransomware and Trojans**
  - » Kedi RAT
  - » Adwind
  - » Emotet
  - » Gozi v2
  - » Hanticor
  - » Trickbot IOCs
- **Physical Security**
  - » Puerto Rico without power or communications
- **System Vulnerabilities (multiple)**
  - » Apache Struts (Multiple), Google Chrome, Apple iOS, VMware
- **Themed Phishing Campaigns**
  - » DDoS Threats
  - » Bank-themed (multiple)
  - » ADP-themed
  - » Tech Support
  - » Insurance

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.

Targeted Supply Chain Attacks: Still, Update CCleaner Today

Summary:

Attackers and hackers seek the path of least resistance. Normally, this is in the form of spear phishing emails coming to institution staff or sweeping scans for vulnerabilities across public IP addresses to exploit what appears in the scan.

What is my "path of least resistance"? The people I trust.

There are many occasions, though, when the path of least resistance is a trusted third party, a vendor that provides updates and patches to systems running in the organization. In 2013, it was the "always-on" connection of the HVAC vendor that provided the initial point of compromise for Target and led to the theft of millions of payments cards in the middle of the holiday season.

Most merchant, restaurant and hotel breaches start with a point-of-sale (POS) platform vendor with a continuous connection to the payment network using default administrator passwords; with little to no effort, hackers gain access to the POS network and siphon off millions upon millions of credit and debit card numbers. And, more recently, in June 2017, an update from Ukrainian accounting software vendor M.E.doc unknowingly pushed out the Nyetya or NotPetya destructive ransomware variant.

Distributing malware along with an update

Taking a tip from the NotPetya campaign, unknown actors delivered malware to targeted tech firms *inside an update* to a very widely-used and highly trusted application known as CCleaner. Created by Piriform, CCleaner is used to optimize the performance of Windows systems by cleaning (deleting) temporary files and managing installed applications; it is a celebrated application found in the toolboxes of IT shops around the world and is used by millions of consumers.

Piriform was recently acquired by Avast. However, just before that acquisition went through in July, the Piriform servers were compromised and legitimate versions of CCleaner v5.33 and CCleaner Cloud v1.07 were replaced with modified copies that contained backdoor code. These modified versions were available for download between August 15 and September 12. The malicious versions were downloaded by over 2.27 million users.

A highly targeted attack

Not every user was the target of the attack, though. The malicious payload was designed to collect user information and send it to a command and control (C2) server; from the information collected, the attackers sent a heavily obfuscated Stage 2 payload that included a variety of hacking tools, including anti-debugging and anti-emulation capabilities, to only a select few organizations. Avast eventually confirmed that, while 700,000 machines reported back to the C2 server, 40 machines were infected with the Stage 2 payload.

According to the Cisco Talos team that investigated the attack, the organizations infected with the more sinister payload are in the technology and telecommunications sectors.

Cleaning CCleaner

As with most Windows applications, a variety of CCleaner versions were available for download; however, the compromised versions were limited to the 32-bit version of CCleaner v5.33 and CCleaner Cloud v1.07. Avast and Piriform immediately updated CCleaner Cloud with a newer, clean version. Businesses and consumers should immediately download CCleaner v5.34 from the Piriform website: www.piriform.com.

Risks to Organizations:

- Malware can allow malicious actors to gain a foothold into an organization's network and perform all sorts of bad actions. While it is thought that the CCleaner attack's end goal was intellectual property, it could easily have been theft of sensitive consumer information or to destroy systems and information.

Remediation:

- CCleaner users with v5.33 installed on any system should remove the malicious version immediately, reimage machines or restore from backup, change all privileged passwords to prevent the risk of compromised credentials and immediately update to CCleaner v.5.34.
- While there are elements of this attack that could not be avoided by users, CIs should still review patch management processes and utilize automatic updates where possible.
- Sign up for industry and manufacturer alerts where possible to know immediately when this type of situation occurs.
- Monitor authentication logs and activate incident response plans if unauthorized activity occurs.

Building a Risk Assessment Program for Small Institutions, pt. V

Assessing the Risk

There are several methods to assess risk once the assets and threats to the assets have been identified, and the risks have been treated. Risk assessments are usually either quantitative or qualitative.

With a quantitative risk assessment, the risk is factored as a figure or quantity. It could be in the dollar amount that would be lost if the threat was successful or the specific amount of time to recover from a threat. Quantitative risk analysis is very time consuming and may require specific tools to be determined. However, they will provide the Board with the specific nature of the risks present in the institution.

Qualitative risk assessments, on the other hand, use a pre-defined rating scale to measure the risk. The *value* of the information, or *impact,* and the *probability,* or *likelihood*, that a threat will be successful are each scored using the scale and then calculated to determine an "inherent likelihood" and "residual likelihood" of the risk.

The scales used in qualitative risk assessments may be from 0 to 1, from 1 to 5, or broader, with each extreme in the scale being given a pre-determined value; for example, on a scale of 1 to 5, "1" may represent the least probability that a threat will be successful and "5" may represent the greatest probability that a threat will be successful.

To go further, in the first case, the threat of person-to-person payments via a mobile app may be a "1" if the institution doesn't offer this feature; however, the threat of an insider stealing funds may be a "5" if there are no internal controls in place to prevent this threat.

An example of the qualitative risk measurement is shown here:

Impact (to the data) x Likelihood (of a successful threat with no controls in place) = Inherent Risk

Impact (to the data) x Likelihood (of a successful threat **with** controls in place) = Residual Risk

Testing the Controls

Once controls have been applied to the risk to reduce the likelihood that a threat will be successful to the information or system, it is very important to go back and verify the effectiveness of the controls. This is akin to locking your front door with a key or your car door with the fob and then turning right around to turn the knob or pull on the handle to check that the door is locked. Daily, we check the effectiveness of the controls we use personally.

The purpose of testing is to provide assurance to management and the Board that the controls are working, to indicate gaps where they exist and to show where additional controls may be needed. All testing that is used to verify the effectiveness of controls and the results of the testing should be documented, to prove to internal auditors and regulatory examiners that testing was performed. Every test performed should be able to be duplicated by another tester, auditor or examiner.

The testing plan that lists the controls to test is in the list of risk treatments as described in Part IV of this series (see the September 18 Risk Summary Report). Controls should be listed as "Administrative", "Physical", or "Technical", to provide a more detailed idea of the types of testing that will be performed. Testing may be performed either by internal staff or by external auditors under contract with the institution.

The type of testing and whether it's performed by internal staff or external testers depends on the control. Typically, administrative controls are tested by internal staff as they require a review of current network users, ensuring all users agree to use CI equipment appropriately or checking that all users have attended appropriate training. Physical controls may be tested by both internal and external testers through pulling on doors, verifying sign-in logs are accurate or checking cameras and DVRs for clear images. Finally, technical controls tests are usually performed by both internal and external testers and include verifying the latest patches are installed on systems, scanning for vulnerabilities on systems and performing full-scale penetration testing.

Gaps found in testing should be addressed depending on the criticality of the vulnerability found or control tested.

Reporting to Management and the Board

As it is the Board's responsibility to check-off on all risk incurred by the institution, the goal of the risk assessment is to provide the Board with the risk. The risk assessment should go to the Board for approval at least annually, and more often if there are drastic or severe changes to operations, products offered, or threats in the environment.

The report should include the inventory of assets, the list of threats, the controls applied to threats to mitigate the risk, the risk measurement and the results of testing. As well, recommendations for improvements may be included in the report.

It's Not Too Late!

Did you think your opportunity to attend was over?

That you'd missed this fabulous chance to attend valuable training, hear expert speakers and network with your peers? Great news! You can still attend the FS-ISAC Fall Summit in Baltimore this coming Sunday through Wednesday!

Here's what's happening:

- **Two Community Institution breakfast sessions** to network and mingle with your peers. Join Jeff and Heather both Monday and Tuesday mornings for coffee and Summit session planning.
- More than 90 content rich sessions.
- Keynote - John Brennan *The Cyberthreat: Security Solutions for a Rapidly Changing World*.
- Sessions are divided on the following tracks:
    - **Governance** (G): Topics include external regulatory organizations, public-private collaboration, compliance, internal risk management and human factors.
    - **Payments** (P): Payments-related topics include how payments work, how to prevent and mitigate against attacks on payment systems and review information gathered during the annual CAPS exercises.
    - **Resiliency** (R): Sessions will discuss industry exercises, Sheltered Harbor and FSARC, as well as incident response and crisis communication techniques.
    - **Technology and Operations** (TO): Sessions designed to address internal technology and operational functions, including identity management, insider threats and network tools like SIEMs and proxies.
    - **Testing and Security Assurance** (TS): Dedicated sessions on all things testing, from testing internal applications in accordance with SDLC and OWASP to penetration testing and cyber-ranges.
    - **Threat Intelligence** (TI): Topics cover current and emerging threats hitting the finance sector, as well as threat automation, threat analysis, and how financial organizations are mitigating against threats.
- Brochure with full sessions and agenda: fsisac-summit.com/2017fall-brochure.
- New in-depth trainings and initiatives:
    - **Two Exciting Initiatives:** *Innovation Challenge* and *Capture the Flag*.
    - **Three In-Depth Trainings:** *Oasis - Thinking in STIX*, *Treadstone 71 – Intelligence for the C-Suite and Stakeholders* and *NCSA - The NIST Cyber Security Framework - Small and Medium Business Cybersecurity Workshop*.

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