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).

Removal Attempt Turns Android Banking Trojan Into Ransomware. SecurityWeek reports that researchers at SfyLabs have detailed the capabilities of an Android banking Trojan named LokiBot that is designed to turn into a piece of ransomware when users attempt to remove it from their devices. Once it infects an Android device (running Android version 4.0 or later), the malware starts displaying overlay screens on top of banking and other popular apps to trick victims into handing over their information. The malware targets roughly 100 banking applications and popular apps such as WhatsApp, Skype and Outlook. The malware can also open the user’s web browser and navigate to a specified page, reply to SMS messages, and launch banking apps.

Study: 1.9B Records Exposed in First Six Months of Year. MediaPost reports that a total of 1.9 billion records were accessed through 918 data breaches through the first six months of 2017, a Gemalto study has found. Many of the records were compromised through the 22 largest breaches, the study found. This is a whopping 164% increase over the last six months of 2016.

AIG to Add Cybersecurity Coverage to Commercial Casualty Policies. Reuters reports that AIG has announced that it will be adding cybersecurity coverage to commercial casualty policies in the beginning of 2018. The company will also be assessing cyberrisk across its other products.

Most Consumers Satisfied with How FIs Handle Account Fraud. While 15% of US consumers spotted fraudulent activity on their accounts last year, 85% said they were satisfied with how their credit union or bank handled the incident, according to a new survey commissioned by the Ottawa, Canada-based March Networks.

The online survey of 1,000 credit union and bank consumers also found that 60% of consumers noticed a fraudulent transaction before their financial institution. This may open an opportunity for credit unions and banks to be more proactive when it comes to identifying and notifying their members and customers about potential fraud, according to March Networks, a provider of intelligent IP video solutions.

This Week’s Top Risks

- **Malware, Ransomware and Trojans**
  - Bad Rabbit
  - Emotet
  - Hantiver
  - Reaper
  - Trickbot
  - Ursnif (aka Gozi aka Gozi ISFB)

- **Physical Security**
  - ISIS New York City Attack
  - Northeast US Severe Storm

- **System Vulnerabilities (multiple)**
  - Apple, Avaya, F5, Fortinet FortiClient, IBM, Oracle, Red Hat

- **Themed Phishing Campaigns**
  - Bank-themed (multiple)
  - Account Verification Alert!
  - ACH Transaction
  - Customer Message
  - MailChimp-themed
  - “Scanned image from MX-2600N”
  - Secure Your Account Now
  - SMS Phishing
  - Whaling with MSWord

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.
Reaper Botnet Compromises Networks

Summary:
A botnet known as “Reaper” or “IOTroop” has infected systems at more than one million organizations. The malware spreads through at least nine vulnerabilities in Internet of Things (IoT) software and hardware. The discovered botnet is more sophisticated and potentially more damaging than the zombification tool Mirai. Reaper uses some of the code from the Mirai malware but uses a different method for compromising devices.

How it Reaps
Reaper uses a combination of nine attacks targeting known IoT vulnerabilities affecting routers from D-Link, Netgear and Linksys, as well as internet-connected surveillance cameras, including those sold by companies like Vacron, GoAhead and AVTech. These attacks affect many popular router brands as well as IP cameras, network attached storage devices and servers. Instead of merely guessing the passwords of the devices it infects, it uses known security flaws in the code of those insecure machines, hacking in with an array of compromise tools and then spreading itself further. Each time a device is infected, the device spreads the malware to other vulnerable devices - like a worm.

How is it Threatening?
To date, the Reaper botnet has not been used to launch a DDoS attack, as Mirai famously did last year. But Reaper is capable of more complex attacks.
It integrates a LUA (a lightweight programming language typically used for embedded systems) execution environment in the malware. This allows the operator to deliver code modules for tasks such as DDoS, traffic proxying or other attacks. The report notes that the botnet is not particularly aggressive, but it could quickly change and potentially cause damage on an even larger scale than Mirai.

IoT devices like IP cameras and routers are particularly susceptible to exploits. Users should check with their vendors to see if there are any available updates. They should also make it a point to regularly update all connected devices in their homes. Also, simply using a strong password will do a lot to secure IoT devices commonly targeted by hackers.

Risks to Organizations:
- The owners of IoT devices are racing with a botnet master to disinfect devices faster than the malware can spread, with serious potential consequences for vulnerable DDoS targets around the world. Given that Reaper has far more sophisticated tools than Mirai, the impending volley of attacks may turn out to be even more dire than the last one.

Remediation:
- **Minimize Non-Critical Network Exposure** – Establish policies that all unused features and services that the user does not use should be switched off. If the device is a non-critical one (important services do not depend on it) it can also be switched off when not in use. In the firewall setup, prevent administrator access from external networks can protect against brute force attacks. Devices that serve important functions can be segmented into another zone from the primary work or home network.
- **A Thorough Setup** – Enforce a strong password policy and measures that defend against brute force attacks by adding intrusion detection systems. Consider using secure protocols – VPN and SSH with a proper security configuration.
- **Security Updates** – Update systems as new patches and updates are available.
- **Implement Additional Security Measures** – If IoT devices are used in a corporate or production environment strengthen network security through monitoring active scanning, penetration testing, proactive network management and analysis.
Financial Services Industries Adopt Blockchain Technology

Originally used to secure and ensure the trust with bitcoin transactions, blockchain and other distributed ledger technologies are being adopted at an increasing rate by the financial services industry. A blockchain is a public distributed ledger, which is a digital record of ownership that does not include a central administrator or central location for stored data. Ideally, a distributed ledger will introduce trust and transparency to any online transaction.

CU Ledger, LLC

In January 2017, CreditUnionTimes reported that CUNA, Mountain West Credit Union Association (MWCUA), Best Innovation Group, credit union system partners and credit unions were partnering to form CU Ledger, LLC. The purpose of CU Ledger, LLC is to develop a proof-of-concept project to create a permissioned, distributed, shared ledger platform for credit unions. Unlike blockchain or standard distributed ledger platforms, CU Ledger, LLC’s platform is private and does not include a currency element at this time.

IBM, J.P. Morgan and Bank of Canada

Earlier this month, a DarkReading article explained how various financial institutions and vendors are looking to utilize blockchain technology to secure transactions. IBM is working with multiple technology partners and over a dozen institutions to roll out a banking product that will leverage its IBM Blockchain platform to clear and settle financial transactions worldwide in near-real-time.

J.P. Morgan partnered with financial institutions in Canada, Australia and New Zealand to launch the Interbank Information Network (IIN), a cross-border payment network built upon Quorum, J.P. Morgan’s internally developed blockchain technology. Immediately following the J.P. Morgan announcement, the Bank of Canada, Payments Canada and TMX Group Ltd, operator of the Toronto Stock Exchange, said they will partner to tech the use of blockchain for automating securities settlement.

NAFCU & Hyperledger

In a press release issued October 24, the National Association of Federally-Insured Credit Unions (NAFCU) is the first US financial trade association to join Hyperledger. The announcement was reported on CreditUnionTimes.

Hyperledger is an open-source blockchain collaboration started by the Linux Foundation in December 2015. As an open source distributed ledger framework, it helps credit unions and other financial institutions support streamlined settlement processes, improve liquidity, provide more transparency and create better product quality. Hyperledger currently has more than 160 members, representing a variety of sectors including finance, banking and information technology, supply chains and manufacturing.

Oracle has released patches for a security issue affecting the Oracle Identity Manager that has received a rare 10 out of 10 score on the CVSSv3 bug severity scale. Oracle describes the issue - tracked under the CVE-2017-10151 identifier - as a "default account" vulnerability, an umbrella term that's usually used to describe accounts with no password or hardcoded credentials (a.k.a. backdoor accounts). What's most concerning is that Oracle hasn’t released the exact vulnerability, due to the elevated risk of criminals creating exploits before Oracle and admins can get it patched.

htpRAT – An Addition to the Remote Access Trojan Family

Summary:

Remote Access Trojans (RATs) are malicious programs that provide the capability to gain unauthorized administrative access and control of a system through a backdoor. Due to the effectiveness of RAT programs, it has been adopted by a host of threat actors ranging from amateur to organized cybercriminal groups to nation states.

htpRAT is a dynamic RAT serving as a beachhead, while also capable of receiving several new builds and functionalities from a command and control server (C&C) to initiate a tailored action on the victim’s system. This gives the threat actors an agile and versatile way to further compromise a system.

Threat actors utilize phishing emails as a vector, containing a malicious file attachment with embedded malicious macros. Once the user clicks on ‘Enable Macros’, a number of commands are executed.
Risks to Organizations:

RATs can:

1. Delete and modify files, format hard disks, upload and download files; harass users and drop off other malware.

2. Capture every screen and keystroke, which means that intruders can gather users' passwords, directory paths, drive mappings, medical records, bank-account and credit card information and personal communications.

3. Give the threat actor's the ability to remotely control the host PC, a powerful tool when wielded in the wrong hands. Remote users not only can manipulate PC resources but can pose as the PC's legitimate user and send email on behalf of the user, mischievously modify documents and use the PC to attack other computers.

Remediation:

- As spear phishing is heavily used as an infection vector for this campaign, confirm that robust training and polices are in place regarding employees downloading and executing unknown applications on company assets in accordance with corporate policies.

- Encourage users to report suspicious emails and attachments, as these are often indicative of suspicious activity.

- Confirm antivirus is deployed and up to date definitions are being applied.

- Apply patches on regular basis.

- Verify that client implementations of Email Gateway security are updated with the latest patches; implement Domain-based Message Authentication, Reporting and Conformance (DMARC) or (Sender Policy Framework (SPF) and DomainKeys Identified Mail (DKM).

- Block or monitor non-standard ports that are open.

- Monitor SSL traffic through untrusted networks (IP address, domains hosted on free DNS platforms) having self-signed certificates.

- The use of Java should be streamlined for best practices.

PwC published key findings from the Global State of Information Security Survey 2018 (GSISS) in a report titled “Strengthening digital society against cyber shocks”. FS-ISAC CEO Bill Nelson provided commentary for the report about next steps global business leaders should take in response to cyber-attacks. Bill specifically mentions the importance of information sharing, the value of simulated cyber exercises, and the roles of the Financial Systemic Analysis & Resilience Center (FSARC) and Sheltered Harbor to enhance financial sector resilience. Bill also noted that Global Resilience Federation (GRF) can help other sectors and communities establish information sharing capabilities.

Tell Us What You Want: Complete the CIAC Survey

On Tuesday, October 24, an announcement went out about a survey being conducted only for Community Institution and Associations Council (CIAC) members. As we are a member-driven organization, your feedback and insight are incredibly important for us. We want to make sure we are providing the information you need to protect your institution and your customers and members.

Complete the survey. It will be available until the end of the day Friday, November 10.

You may contact Jeff Korte or Heather McCalman with any questions.