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).

Experts: Iran could use cyberattacks to retaliate against sanctions. President Donald Trump this week reimposed economic sanctions on Iran. While no specific threats have been made, the move may lead Iran to retaliate through cyberattacks, security experts say. (PBS)

Survey: CMOs worry most about data breaches. Twenty-nine percent of global marketing chiefs say a potential data breach is their biggest strategic risk concern, per Dentsu Aegis Network. Data is like the currency of marketing, so "the CMO must guard it with his or her life or career," says Zenna Consulting’s Warren Zenna. (eMarketer)

BankBot Anubis still a threat, gets upgrade. Mobile devices (particularly Android) have become the most common means of browsing the web. Over the past few years mobile banking trojans have been a persistent threat. Using plain text for command and control (C2) URLs makes it easy for security researchers to identify and report malicious URLs. What’s significant about BankBot Anubis malware is that it is still being actively developed and enhanced. These latest developments make it significantly harder for the security community to disrupt Anubis’ infrastructure. (Phislabs)

Security conferences to shed light on hacking trends. Were you interested in attending this year’s Defcon conference to learn about evolving threats and couldn’t attend? Right now, there are three big trends to watch:

- **Mobile threats.** Mobile devices take on more responsibility and control in a user’s life (financial, retail, multi-factor, biometrics, etc.), they also become more important for the hacker. In order to continue their illicit operations, hackers now increasingly have to gain access to these devices. Hackers must gain access to this platform in order to remain relevant.

- **Internet of Things.** For hackers, the growth of IoT devices in the home and office is a wonderful revenue opportunity for certain types of malware.

- **Audio hacking.** Voice biometrics are currently used by many financial institutions to verify customers. Additionally, voice-based authentication and control are used by an increasing number of devices and services from mobile phones to IoT products making it an enticing target of opportunity.

   Just as technology is constantly evolving, so too are the tactics used by hackers. These will be harder to defend against, so it is important for businesses and consumers to be aware of the risks they are facing. (Yahoo Finance)
Summary:

FS-ISAC members have reported a ransom-based distributed denial of service (RDoS) attack purporting to come from the hacktivist group, Apophis Squad, which demands 2.01 BTC in payment in exchange for not launching a RDoS attack.

Apophis was the ancient Egyptian deity who embodied chaos and was the opponent of light and Ma’at (order/truth); it also is the adopted name of the suspected Russian Hacker group Apophis Squad.

Apophis Squad’s Twitter account boasts numerous campaigns some of which include Defcon, ProtonMail, VanityMC as well as financial institutions. They also claimed the responsibility for making bomb hoax attacks against UK schools. The group also warns others in the internet community not to take them on lest they be attacked. Table 1 reveals they also enjoy taunting US federal agencies and the NCA.

What is RDoS?

RDoS is a potent combination of a ransomware attack (seizing a computer after malware on it is activated) and a DDoS attack. Prior to launching such an attack, the malicious actor demands a ransom be paid, typically with a letter or even a Twitter post threatening to launch an attack at a certain day and time unless a ransom is paid. The attacker may choose to validate the threat, by launching a sample attack on the victim's network. If unpaid, the DDoS attack is executed.

A prior example

In March 2018, Cybereason's security team discovered that the memcached servers used in the largest DDoS attack to date included a ransom note in the payload. The analysis report stated the attacker “dedicated a gigabyte of data to the ransom note, which instructs victims to pay 50 XMR (XMR is the ticker symbol for the Monero cryptocurrency), is included in a line of Python code and repeats many times. As of this writing, 50 XMR equals approximately $15,000. Like all currencies, the Monero exchange rate fluctuates so the amount of money victims has to pay can change.”

While there is no evidence that the victim of the attack had paid any ransom, in June 2017, Radware reported the South Korean hosting service Navanna reportedly paid $1M after being held for ransom.

Risks to Organizations:

- Financial institutions face a variety of risks from cyber-attacks involving extortion, including liquidity, capital, operational, compliance and reputation risks, resulting from fraud, data loss, and disruption of customer service.

Remediation:

- The FFI EC joint statement on Cyber-attacks Involving Extortion states, Financial institutions should ensure that their risk management processes and business continuity planning address the risks from these types of cyber-attacks, consistent with the risk management practices identified in previous FFIEC joint statements and the FFIEC Information Technology Examination Handbook. Consistent with FFIEC and member guidance, financial institutions should consider taking the following steps:
  - Conduct ongoing information security risk assessments;
  - Securely configure systems and services;
  - Protect against unauthorized access;
  - Perform security monitoring, prevention, and risk mitigation;
  - Update information security awareness and training programs, as necessary, to include cyber-attacks involving extortion;
  - Implement and regularly test controls around critical systems;
  - Review, update, and test incident response and business continuity plans periodically; and
  - Participate in industry information-sharing forum.
Do You Smell a RAT at Your Institution?
Remote Access Trojans gnaw away your institutions security

Summary:

Have you ever gotten the feeling that there’s someone else on your computer? Things just don’t seem the same. Let’s face it, you smell a RAT.

We are not talking about the little four-legged rodent you hear in your walls, but a RAT or Remote Access Trojan. A RAT gives a malicious hacker access to your desktop and they are easily attainable on the dark web.

“But wait,” you say, “what is the difference between a Remote Access Trojan and a Remote Administration Tool?” However, as one blog states, the real problems start when the most important division line dissolves - the one between intentionally malicious programs and the legitimate clean programs.

How a RAT Works

These remote access trojans are programs that run behind the scene and provide unauthorized access to your machine or system. Regardless of the malicious actor’s goal or use, these applications can perform specific tasks once you have accidentally installed the RAT on your system.

A Remote Access Trojan* (RAT) is a malware program that includes a back door for administrative control over the target computer. RATs are usually downloaded invisibly with a user-requested program such as a game or sent as an email attachment. Once the host system is compromised, the Intruder may use it to distribute RATs to other vulnerable computers and establish a botnet.

A Remote Administration Tool# is remote control software that when installed on a computer it allows a remote computer to take control of it. A Remote Administration Trojan (RAT) allows an attacker to remotely control a computing system and typically consists of a server invisibly running and listening to specific TCP/UDP ports on a victim machine as well as a client acting as the interface between the server and the attacker.

Misdiagnosing an innocent data packet containing malware might have severe implications for your network, resulting in a wide range of damage including financial, legal, regulatory or reputational impact. Your institution will most certainly create operational issues with which to contend.

Training Employees and Customers:

- Do not click on suspicious links.
- Do not open attachments of emails sent by unknown senders.
- Use common sense while using social media.
- Update your operating system and security software regularly.
- Report suspicious activity to your IT department or CI.

Remediation Options for RDoS and DDoS attacks:

- Obtain more bandwidth to handle increased activity. Block unused or notoriously used ports and protocols on firewalls and border routers.
- Configure your network hardware against attacks. Refrain from providing web content in .pdf format on websites to discourage multiple request RDoS/DDoS.
- Build in redundancy into your infrastructure. Deploy a RDoS/DDoS protection appliance. Include DDoS protection in your contract with your ISP.
- Protect your DNS servers. Partner with a DDoS mitigation service provider before an attack occurs.

*Remote Access Trojan; #Remote administration tool

Delivering Threat Intel Content and Experts to You. The FS-ISAC Threat Intel Roadshow is delivering an interactive and engaging forum focused on the threats that member companies stare down daily. The highly curated sessions feature intel trend experts, executive leaders, front line analysts that know this business of stopping bad actors. Topics include insourcing versus outsourcing threat intel; how to use threat intel findings; nation-state capabilities and destructive attacks; threat intell management and operations; and emerging trends and TTPs. Join your local FS-ISAC members in Atlanta, Boston, Dallas and Phoenix in September for a day of closed-door, collaborative deep-dives into the threats keeping you awake at night. Learn more and register today.

© 2018 FS-ISAC, Inc. | All Rights Reserved.
Tip of the Week: Reducing FS-ISAC Information

Learning how to balance information sharing

Summary:

Members often ask: How can I control the amount of information that my institution receives from FS-ISAC? Solely selecting the FS-ISAC Intelligence Report within the Collective Intelligence Reports menu in the FS-ISAC portal will reduce SOC Alerts to one per day. It provides a daily snapshot of information that can be further investigated. Each institution should decide what is right for them. Please review the “FS-ISAC Alerts by Job Title” document in the Member Resources folder (Library Tab) for information regarding which alerts go with which role or job title.

**Step One:** How many regular fulltime employees are dedicated to disaster recovery, loss prevention, information and physical security, information technology, etc. Can I delegate information alerts to other employees?

**Step Two:** What is the risk appetite for your institution?

**Step Three:** Selecting what you want to receive and determining if it is sufficient for your institution.

1. Log into FS-ISAC Portal (https://portal.fsisac.com), and
2. Enter the USER ID, PASSWORD and TOKEN NUMBER
3. In the upper MENU bar, SELECT: MY PROFILE
4. Select members individual EMAIL ADDRESS. The Point-of-Contact can sign other employees to receive alerts by selecting 🎯. ADD the email address then SELECT SAVE. Please note that only authorized users (have an assigned token) can log into the portal.
5. CLICK on the SELECT CISCP REPORTS drop down menu to see the list of available reports. CHECK (SELECT ALL) to receive all reports or select/deselect reports of interest
6. CLICK on the COLLECTIVE INTELLIGENCE REPORT drop down menu
7. SELECT FS-ISAC INTELLIGENCE REPORT ONLY DESELECT the remaining REPORT TYPES if desired
8. REVIEW the list of remaining reports where you would only have one report per day
9. EMAIL MEMBER SERVICES to be added or removed from mail lists you are subscribed to

Tip of the Week:

Reducing FS-ISAC Information Learning how to balance information sharing

October 9-10 or 16-17 - CAPS Exercise. North America (NA) Sessions. Register. Information and locations. Read more.