Tips to Defend Against Ransomware

FS-ISAC Shared Information, Tools With Members During May 2017 WannaCry Ransomware Attacks

Ransomware, a type of malware that encrypts a computer or system and demands a ransom payment, is a growing threat to many organizations. In May of 2017, a massive ransomware attack, labeled WannaCry, hit thousands of organizations in many sectors around the globe. The financial services sector was in a strong position to defend against these attacks and there was relatively minor impact across the sector. The Financial Services Information Sharing and Analysis Center (FS-ISAC) and its membership continuously evaluated the impact as the attacks unfolded and the sector was prepared to prevent and respond to the attacks. The majority of attacks appeared to target and impact non-financial sector entities around the world and FS-ISAC believes the first salvo of these attacks utilized known vulnerabilities for which there are available software patches but required firms and service providers to implement them.

The financial sector was prepared due in a great part to the industry's proactive approach in cyberhygiene and information sharing practices. The 7,000 members of FS-ISAC actively share threat intelligence in real time utilizing proper sharing protocols. This is like a "virtual neighborhood watch" of sorts.

FS-ISAC Provided Members With Real-Time Information and Tools

FS-ISAC provided information, tools and best practices to its members to improve sector readiness, resilience and response, if it had been needed. FS-ISAC recognizes that financial institutions participating in information sharing with properly patched systems and better cyberhygiene are positioned to stay ahead of cybercrime. FS-ISAC, its analysts and members vigilantly monitored the situation

Examples of actions taken include:

- Monitored active information sharing of members on numerous FS-ISAC email distro lists.
- Provided mitigation recommendations including best practices around handling ransomware attacks.
- Proposed countermeasures like fine-tuned network-blocking controls.
- Provided remediation strategies in case software infections were found.
- Coordinated with other ISACs and government agencies.
- Communicated to the Financial Services Sector Coordinating Council (FSSCC).
- Prepared and distributed a TLP Amber member advisory.
- Monitored news media and engaged the FS-ISAC's Media Response Team on Friday and thru the weekend. Distributed news articles.
- Co-sponsored 16 Ransomware 101 Roadshows during 2016 and in collaboration with the National Healthcare Information Sharing and Analysis Center (NH-ISAC) Multi-State Information Services and Sharing Center (MS- ISAC) and US law enforcement agencies. More than 3200 attended the series. The sponsors published a two- page summary including tips last December and is accessible directly to FS-ISAC members. A summary of recommendations and best practices from that show are below.
- Additional best practices, mitigation strategies and threat intelligence related to ransomware, Wannacry and other risks and threats are directly available to FS-ISAC members worldwide.

Ransomware 101 Roadshow Overview and Tips

Ransomware is a type of malware that encrypts files essentially blocking access to the file(s). The only way to access the encrypted contents is via the decryption key and/or through data back-ups. Ransomware can be delivered via many forms, such as, exploit kits, spear phishing emails, malicious links, drive-by downloads. Sometimes this is combined with social engineering, for example an infected email attachment that appears to come from someone's boss asking them to take action and open the file. The actor, or perpetrator, then demands a ransom payment and gives the targets a way to regain their data. The ransom amount is generally not large, averaging less than $1000, but the number of incidents has risen sharply in 2016, posting record growth in Q1 and Q2.

How Do You Mitigate Attacks?

Being prepared is essential to reduce the effects of a ransomware attack. Here are tips on how to address ransomware post-attack:

- Isolate the infected system from your network.
- Restore files by using files from regularly maintained backup.
- If available, utilize legitimate encryption keys to decrypt systems and clean or restore them.
- Work with law enforcement as appropriate (see below).

FS-ISAC

Tips to Defend Against Ransomware

How Do You Stay Prepared?

It is easier to prevent an infection or an attack than it is to clean one up. Best practice is to focus on defense, and utilize several layers of security:

- Employee education. Let employees know what to do during an incident.
- Security operations staff should rehearse ransomware scenarios during training exercises.
- Operating systems and antivirus software should be kept up to date.
- Files should be backed up and available to reload if necessary.
- Manage the use of privileged accounts – administrator level access should be minimized.
- Backups should be tested in a real-world environment to confirm ability to restore in a rapid fashion. High value backups should be tested more regularly.

Recommendations

Be aware of how your network is configured and what software you use on a regular basis. By knowing what your system looks like and how it works, you will be able to identify problems when they occur.

- Patch systems regularly and use automated patching when possible.
- Perform regular backups of all systems. Validate backups, especially for high value data.
- Test backup systems to ensure full recover operations can be completely rapidly and seamlessly in case data recovery is required.
- Know what is connected to and running on your network.
- Use antivirus and anti-spam solutions.
- Disable macros scripts in Office.
- Restrict Internet access.
- Train cyber teams to coordinate response with other parts of the organization including finance, communications and the executive teams to respond when ransomware hits.
- Educate and train employees to maintain situational awareness and report any potential issues immediately.
- Participate in cybersecurity information sharing organizations.
- Create a solid business continuity plan.
- Perform exercises to test playbooks and responses periodically.
- Understand that law enforcement agencies often work with the private sector to develop decryption tools quickly after ransomware attacks occur. These tools can be used to decrypt infected machines. Law enforcement can also help properly gather evidence when incidents occur.
- While not recommended by authorities, some experts recommend stockpiling cryptocurrency like Bitcoin and have an established process on when and how to utilize this option if needed.

Should You Pay the Ransom?

Law enforcement, including the US FBI recommend not paying the ransom. There are cases where the ransom has been paid and the attackers do not provide the decryption keys. Some organizations take an "opportunity cost" approach and believe that value of lost data that outweighs the relatively minimal cost of the ransom. Organizations that do believe in payment the ransom typically stockpile cryptocurrencies and have processes in place to activate a response when required. There is no guarantee, however, that these organizations will receive the decryption keys after payment.

How Do You Work with Law Enforcement?

When ransomware is reported within 72 hours, law enforcement agencies have a better chance of helping respond and gather evidence. Government agencies often quickly develop decryption keys and may be able to provide these keys as required. Also,

- Report the infection to the Federal Bureau of Investigation (FBI) www.fbi.gov/contact-us/field.
- Report home infections to the Internet Crime Complaint Center (IC3). www.ic3.gov.

Tips to Defend Against Ransomware

Contacts and Information

Who	Contacts and Helpful Info
FS-ISAC Security Operations Center (SOC)	iat@fsisac.com soc@FSISAC.COM
US FBI	Major Case Contact Center 1-800-CALL-FBI (225-5324). https://www.fbi.gov/contact-us
US Secret Service	http://www.secretservice.gov/ectf.shtml USSS Ransomware advisory (external link to pdf)
US Internet Crime Complaint Center (iC3)	https://www.ic3.gov/faq/default.aspx#item4 iC3 Ransomware brief (external link to pdf)