BEST PRACTICES FOR BANKS

Reducing the Risk of Ransomware

(Developed by the Bankers Electronic Crimes Task Force)

INTRODUCTION

Ransomware is a form of extortion that uses malicious software to encrypt a device and/or data. Once encrypted, the owner is denied access, and the data is held "hostage" until the victim pays a ransom. Often, payment is demanded in an electronic form, such as Bitcoin. Another tactic cyber criminals use to extort payments from victims is to threaten the launch of a denial-of-service (DOS) attack if payment is not made. That form of extortion is covered in the DDoS Best Practices developed by the Bankers Electronic Crimes Task Force.

BACKGROUND ON RANSOMWARE

If a financial institution holds and uses customers' sensitive information, the financial institution should be concerned about the threat of ransomware. It can impose serious economic costs; because, it can disrupt operations or even shut down a business entirely.

The FBI reported that it received more than 2,400 complaints regarding ransomware in 2015, with reported losses of more than $24 million. Losses reported to the FBI in only the first 3 months of 2016 were up to a staggering $209 million. There is no indication that ransomware is declining, since it is incredibly profitable to criminals.

HOW IS RANSOMWARE DELIVERED?

Ransomware typically requires a user to take some kind of action such as clicking on a link or downloading a malicious attachment such as a Microsoft word document. However, ransomware can be applied without any user intervention, such as with the global ransomware attack in May 2017. Other campaigns simply require a user to visit a malicious or compromised website, which can cause the ransomware to download automatically onto the user's computer.

Other delivery methods are more sophisticated because they can occur even on trusted websites through third-party ad networks that redirect the user to an infected server. More recently, attackers have exploited specific weaknesses to deliver ransomware by searching for networks that failed to patch known vulnerabilities.

SUMMARY

BEST PRACTICES FOR BANKS

Reducing the Risk of Ransomware

(Developed by the Bankers Electronic Crimes Task Force)

Ransomware is devastating malicious software. But, there are a number of measures banks can take to reduce the risk of being a victim to ransomware, some of which are provided below. Resources for lowering your risk are abundant, and you are encouraged to be proactive in developing a defense.

BEST PRACTICES FOR BANKS

Reducing the Risk of Ransomware

(Developed by the Bankers Electronic Crimes Task Force)

IDENTIFY

1) *What are you trying to protect (business network, critical applications, data, policies and procedures, etc.)?*

2) *What are the primary forms of ransomware that are currently a threat (update this each time you review your practices)?*

I1 Identify the financial institution's systems, and ensure ransomware is included as a potential threat.

- Review existing risk assessments, which should include ransomware.
- Gain situational awareness by identifying what is needed to maintain critical business functions:
  - Identify critical data, it's location, and it's source.
  - Identify backup processes used and discuss how they are protected from being corrupted to enable timely recovery.
  - Identify what device, system change, and software are needed to maintain or recover operations (e.g routing tables, firewall configuration files, etc.).
  - Identify the source of critical data, processes, and systems.

I2 Identify the current variations of ransomware to gain a better understanding of what the different attacks are targeting. This identification and understanding of what the attacks are targeting will help drive development of appropriate practices.

I3 Identify all potential attack vectors for ransomware, so appropriate practices can be developed. There are currently three primary attack vectors for ransomware:

- Phishing emails containing malicious attachments and/or containing links to compromised websites.
- Frequently visited websites that have been compromised (also known as watering holes), which infect users that visit the website if they have outdated browsers or browser plugins, and/or other unpatched software.
- Self-propagating worms that crawl through your network looking for open or unpatched systems.

Attack vectors also include malicious ads and malicious third-party apps (available in mobile app stores). Attack vectors are likely to change over time, so it is important to review attack vectors periodically.

To stay current with ransomware threats, participate in industry information sharing forums, such as FS-ISAC and/or support forums of the antivirus software that you use.

I4 Identify potential weaknesses in your environment. Consider the gap between threats and protective controls.

- The risk assessment should consider ransomware.
- Ensure your security awareness training program adequately covers ransomware.
- The incident response program should adequately cover ransomware.
- Are backups secure?
- Ensure that patching practices are adequate to cover all software on all devices and in a timely manner. Unless there is a business reason not to, consider having patches automatically installed that the vendor identifies as critical.

PROTECT

Protect network, critical applications, data, policies and procedures against the ransomware threats identified earlier.

P1 Implement mitigating controls to protect the financial institution's network, critical applications, data, policies and procedures.

Controls will vary depending on the available budget, resources, and personnel. Every financial institution is unique, but the following are best practices every institution should consider.

- **Policies and Procedures** – Policies and procedures should address ransomware risk. Policies should be reviewed, updated, and approved at least annually.
- **Employee Training** – Since email phishing is the most common attack method, financial institutions should focus on employee training as a key line of defense. All employees should be trained at least annually on the dangers and risks associated with ransomware, as well as the most common infection techniques. Training should include indicators that their work station may be compromised and the importance of immediately notifying the IT department to reduce the risk of ransomware spreading.
- **Patching** – All endpoints (servers, desktops, laptops, mobile devices, virtual hosts, etc.) should be patched as soon as practical after patches against vulnerabilities are released. Consider automatic patching if practical in your environment.
- **Bank Websites** – Bank websites should inform retail and business customers about ransomware risks, threats, controls, and response procedures.
- **Enable Strong Spam Filters** – Since email phishing is the most common attack method, a key defense is preventing those emails from getting through. Evaluate authenticating emails with technologies such as DMARC (Domain Message Authentication Reporting and Conformance) and DKIM (DomainKeys Identified Mail).
- **Monitoring** – System access logs and reports, change management reports, and failed log in attempts should be part of every institution's routine monitoring. Software that will automate the monitoring process with trend analytics combined with some manual monitoring is ideal.
- **Disable Macro Scripts** –Ensure that Microsoft macros scripts are disabled, as this is a common infection method. Instead of using the full office suite, consider using Office Viewer software to view MS Office files transmitted by email.
- **Redundancy** – Every financial institution should have redundant capabilities on systems, assets, and critical data. This may include backups, server snapshots, secondary hardware, secure cloud storage, etc. Consider deploying data vaulting solutions in addition to deploying offline backups. While redundancy is not immune from ransomware, it can assist in the recovery process.

- **Backups** – Every financial institution has backups of critical data and files. Backups are required to be securely kept off site. To mitigate risk of ransomware, backups should be disconnected from the network. Keeping an off-line full image backup of crucial systems can significantly reduce the impact of a compromised system.
- **Limited Access** – Limit access to all systems, assets, data and capabilities based on job requirements. This will assist in accidental exposure to ransomware.
    - Employees, vendors, consultants and customers should only have the access credentials needed to perform their tasks or banking activities.
    - Restrict the use of administrative credentials.
    - Administrators should use separate credentials for normal and administrative access.
- **Multi-Factor Authentication (MFA)** – If multi-factor authentication (MFA) is available, it should be used as another control layer.
- **Restrict File Sharing** - To reduce the risk of ransomware spreading from machine to machine, evaluate options for restricting filing sharing. This might include restricting with access control lists, or user permissions granted via domain assignment or group memberships, or as an extreme measure, disabling file sharing.
- **Security Monitoring** – Some type of security monitoring software (firewall, network, endpoint, DNS blacklisting) and/or reliance on third-party service providers can help stop ransomware. While this is an additional expense, it can greatly enhance security and ransomware prevention. Many vendors have services tailored to an institution's budget.
- **Network Segmentation** – Network segmentation can help control the spread of malware should an infection occur.
- **Maintain a Continuous State of Alertness** – Maintain a continuous state of alertness to be poised to take prompt actions. Have a thorough knowledge of the components, training, vectors, detection technology, ongoing risk assessments, monitoring, information sharing and incident response.

P2 Establish the priority of planned enhancements to security and mitigation practices, if all potential weaknesses cannot be remediated in the near term.

P3 Implement the "Foundational Cyber Hygiene" controls of the Center for Internet Security (CIS). CIS provides a list of 20 top critical security controls (CSC) that if implemented will significantly reduce cyber risks. The first five CSCs (listed below) are referred to as "Foundational Cyber Hygiene" and can reduce cyber risk by 85%. Each of the five controls requires implementation of several underlying measures. All institutions should implement these industries recognized essential controls. Refer to the Center for Internet Security for more information.

- CSC 1: Inventory of Authorized and Unauthorized Devices
- CSC 2: Inventory of Authorized and Unauthorized Software
- CSC 3: Secure Configurations for Hardware and Software on Mobile

Devices, Laptops, Workstations, and Servers

- CSC 4: Continuous Vulnerability Assessment and Remediation
- CSC 5: Controlled Use of Administrative Privileges

Cyber defense must be driven by prioritization. You will have to determine what you should do first to get the most value and protection.

P4 Regularly test mitigating controls and training programs to ensure they are functioning.

- **Social Engineering Tests** – Phishing emails remain the number one method to initiate ransomware. Test phishing emails should be sent to employees at least quarterly, after employees have been taught how to recognize a phishing email. Outsourced phishing email testing is offer by several vendors at a very low cost.
- **Ransomware Testing** – Ransomware testing should be one of the testing scenarios contained in your Incident Response Plan.
- **Strengthen and Retest** – Strengthen and retest controls if weak or if ineffective controls are discovered.

P5 Follow proper Change Management Processes to reduce the risk of introducing vulnerabilities that Ransomware exploits.

- Take into account if the changes made to systems, assets, or data expose the institution to ransomware risk.

P6 Incorporate ransomware protection into communications plans.

- The communication plan should address the possibility of a ransomware attack.
- Prioritize who will be called and when.
- Maintain printed and/or off-line versions of critical items like the communications plan to ensure plans are accessible in the event of a ransomware attack.
- A public relations communication script should be prepared in advance.

DETECT

Develop and implement the appropriate activities to detect a ransomware attack.

D1 Monitor server, network, endpoint and backup systems.

- While using monitoring tools can add to budget costs and staff resources, monitoring tools can detect unusual file access activities, abnormal network traffic, and abnormal CPU activity to potentially block ransomware.

D2 Monitor known good file extensions.

- This is an effective method for detecting suspicious activity. Create a baseline standard of good file extensions, and incorporate into a third party tool to detect abnormal behavior.

D3 Monitor for the renaming of files.

- Renaming files is not a common action on network file shares. Ransomware often results in a large amount of file renaming. Third party tools should be configured to alert institutions of this type of activity.

D4 Use client based anti-ransomware agents.

- Anti-ransomware agents are designed to run in the background and block attempts by ransomware to encrypt data. Client based anti-ransomware agents can be used to monitor the Windows registry for text strings known to be associated with ransomware. Multiple third party vendors provide anti-ransomware software that will meet specific financial institution needs.

RESPOND

Develop and implement activities to restore systems, assets, data and capabilities.

Rd1 Prevent or isolate ransomware from spreading to other systems

- The first priority upon detection is to isolate other devices from the network to prevent the spread of the ransomware.
    - Prioritize devices that contain critical data such as servers.
    - Determine in advance how to shut down routers, switches, wireless access points, and all other related communication equipment in a manner that minimizes disruption.
- Machines identified with ransomware should not be powered down rather removed from the network for further investigation.

Rd2 Determine the scope of the infection.

- Perform forensic analysis of infected systems as well as other network devices (routers, firewalls).
- Search for malware artifacts, such as file names, registry entries, and installed programs.
- Update and re-run security scanning tools frequently as detection of zero-day exploits can be updated by tool providers quite often.

Rd3 Initiate Incident Response Plan

Activate the plan to respond to the specific ransomware incident. The Incident Response Plan should cover the following areas:

- To contact law enforcement, as they periodically obtain decryption keys for some variants of ransomware through their investigation activities
- Steps for containing the problem
- Assessment factors for evaluating the scope of the incident / infection
- How to restore systems / data (if needed)
- Notification process (incident response contacts)
- Consider pre-arranged service contracts with security response providers so that legal and contract issues do not delay response. These contracts can often be arranged with no up-front cost.
- Consider whether law enforcement and regulatory activities should be handled by legal counsel to protect client-attorney privilege
- Consider several factors when evaluating if you will pay the ransom if compromised.
    - In 15% of cases when the ransom is paid – files are still not recovered.
    - Paying ransom is discouraged as doing so encourages more ransomware, sometimes results in a demand for a higher ransom, often funds illegal activity, and can result in victims being targeted again.
    - Learn in advance how Bitcoins are obtained, if this is part of your strategy.

- Incident Response Contacts – include updated contact information for:
  - Incident Response Team,
  - Executive Management,
  - Third Party Security Response Team,
  - Law Enforcement,
  - Legal Counsel,
  - Board of Directors,
  - Regulatory Agencies,
  - Marketing / Investor Relations (Customer / Public Notifications),
  - Third Party Vendors, and
  - Insurance.

RECOVER

Develop and implement the appropriate activities to restore systems, assets, data and capabilities. A good backup strategy is the best defense against data loss.

Rr1 Remediate malware

Where effective, use software tools to remove the malware from systems. Often ransomware only encrypts data and leaves the operating system intact, but still infected. A complete operating system restore may be required.

Rr2 Restoration from last known good backup

If systems / data must be restored, it is important to ensure systems/data are restored using a last known good backup unaffected by the ransomware incident.

- Document how you will determine which backup is unaffected.

Rr3 Confirm and communicate successful restoration of systems

After systems have been restored, systems should be tested by appropriate departments to ensure the successful restoration of data.

- Document the process for departments to test the restored data, and
- Document the process to communicate that their data has been successfully restored.

Rr4 Document lessons learned

Review processes, procedures, and technology to strengthen identified weaknesses to prevent potential future ransomware incidents.

ADDITIONAL RESOURCES

US Secret Service
https://www.secretservice.gov/forms/Cybersecurity_Joint_USSS_ECTF_HSI_Ransomware_Advisory.pdf

US-CERT
https://www.us-cert.gov/security-publications/Ransomware

FBI
https://www.fbi.gov/file-repository/ransomware-prevention-and-response-for-cisos.pdf

FTC
https://www.ftc.gov/news-events/blogs/business-blog/2016/11/ransomware-closer-look

FS-ISAC 2017 Incident Response Playbook
Contact your local financial trade association(s) to obtain the Incident Response Playbook that was developed with FS-ISAC for your state

The following information is from For-Profit Corporations. However, the reports include non-product specific information that can be helpful to non-customers. No endorsement is implied.

Symantec Special Report: Ransomware and Businesses 2016
http://www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/ISTR2016_Ransomware_and_Businesses.pdf

McAfee Labs Threat Report
https://www.mcafee.com/us/resources/reports/rp-quarterly-threat-q1-2015.pdf