FS-ISAC

Ransomware Essentials

A Guide for Financial Services Firms Around the World

Overview

Targeted ransomware is a top threat to private companies and governments alike, and is used as a tool for political and financial gain by both nation-state actors and cyber criminals. Ransomware threat actors are becoming increasingly audacious with a rising number of reports of attacks affecting the financial sector either directly or indirectly via the supply chain.

This document focuses on ransomware best practices, awareness, and recommendations to reduce the risk of ransomware among both members and non-members, with information and resources for organizations and individuals to use, and is based on operational insight from FS-ISAC and its members. The audience for this guide includes information technology (IT) professionals as well as others involved in developing cyber incident response policies and procedures, or coordinating cyber incident response.

What is Ransomware?

Ransomware is a type of malicious software, or malware, designed to infect computers and encrypt files until a sum of money or other form of ransom is paid. After the initial infection, ransomware will attempt to spread to connected systems, including shared storage drives and other accessible devices. Such malware can potentially be highly destructive, rendering systems inoperable.

To gain initial access, threat actors make use of any available attack vector, such as spearphishing, the use of valid (compromised) accounts, USB drives and network shares, remote access services, and exploitation of public facing applications. While some ransomware is spread via untargeted attacks, through phishing emails or "drive-by downloads," ransomware is often deployed as a secondary payload once a device has been compromised by other malware. Attacks delivered via supply chains have also proven to be highly effective.

The top ransomware threats are human-operated attacks, whereby following the network intrusion, threat actors will move laterally, taking steps to disable security tools and backup systems. Such attackers can exhibit extensive knowledge of systems administration and common network security misconfigurations, perform thorough reconnaissance, and adapt to what they discover in a compromised network.

Ransomware incidents can severely impact business processes and leave organizations without the data they need to operate and deliver mission-critical services. Many ransomare operators now also exfiltrate sensitive data from compromised networks, threatening to disclose the data - publicly naming and shaming the victim - as further incentive to pay the ransom. The monetary value of ransom demands has also increased, with demands on high profile victims often reaching USD $50 million / EUR €42 million. Some reports indicate the average payment demand for ransomware is now USD $850,000 / EUR €730,000.

USD $50 million
Ransoms demanded of high-profile victims

USD $850,000
Average ransomware payment demand

Ransomware incidents have also become more destructive and impactful in nature and scope. Once malicious actors have gained access to a victim's network, they will propagate ransomware across entire networks, deleting system backups to make restoration and recovery more difficult or even infeasible for impacted organizations. The economic and reputational impacts of ransomware incidents, throughout the initial disruption and, at times, extended recovery, have also proven challenging for organizations both large and small.

Best Practices and Healthy Cyber Habits

FS-ISAC emphasizes 10 key measures that promote smart cyber behaviors or actions that individuals and organizations should implement to help prevent and mitigate ransomware attacks.

01

Be prepared and practice your plan

Create, maintain, and exercise a basic cyber incident response plan and associated emergency communications plan that includes response and notification procedures for a ransomware incident. Use initiatives and tools such as the Cybersecurity and Infrastructure Security Agency's (CISA's) free Cyber Security Evaluation Tool (CSET) which helps organizations assess their posture against ransomware attacks.

02

Preventative patching

Patching is essential. Keeping hardware and software up to date with regular patching is an effective way to prevent threat actors exploiting known vulnerabilities to compromise your devices and networks.

03

Train staff to counter social engineering

While technical solutions can filter or block some malicious email traffic, it is important to ensure staff are trained to recognize suspected phishing emails, that they have a clear process for reporting them, and that an organization-wide, positive culture exists around reporting incidents.

04

Use multiple authentication factors

Implement multifactor authentication (MFA) to prevent data breaches and cyber attacks. This includes a strong password and at least one other method of authentication. The use of MFA for any remote access service or method is particularly prudent.

05

Use offline and remote backups

It is critical to create offline, encrypted backups of data and to regularly test those backups. Keep your backup media in a safe and physically remote environment - these backups must be resilient to the possibility of a malicious actor with the highest administrative privileges on your network. Identify critical systems and evaluate the need for having backups on hand to quickly restore service.

06

Employ best practices for Remote Desktop Protocol (RDP) Services

Threat actors often gain initial access to a network through exposed and poorly secured remote services. Therefore:

- **Use strong passwords**
- **Use multifactor authentication**
- **Update your software**
- **Restrict access using firewalls**
- **Enable network-level authentication**
- **Limit users who can log in using RDP**
- **Set an account lockout policy**

07

Implement internal and external threat hunting processes

An active search for threats inside and outside the network, including periodic penetration testing and vulnerability scanning, will increase defensive capabilities against threats, detecting exposed infrastructure or other information that could be exploited to carry out an attack. In addition, searching for malicious patterns will enrich/improve the generation of relevant alerts or events from internal controls.

08

Keep your asset inventory updated

You cannot defend what you cannot see. Make sure you have identified all network segments where your organization's assets exist. Maintaining an updated and complete inventory – everything from servers to CCTV cameras - is important for internal defensive management. Everything connected to the internet is a potential entry point for an attacker.

09

Implement whitelisting and Zero Trust Network Access

Deploy software restriction policies to allow only the execution of approved software. Anything inside or outside its perimeters should automatically not be trusted. Verify anything and everything trying to connect before granting access. Secure/disable your Server Message Block (SMB) to prevent lateral movement through connected systems. Maintain strict hardening policies for connected equipment, and implement asset discovery processes on the network.

10

Keep your cybersecurity alert notification and escalation matrix updated

Good management of alerts, use-cases, and escalations is key to responding in a timely manner to a possible cybersecurity incident. Include in your matrix response service-level agreements (SLAs), contact numbers and emails for key people, which alerts are manual, and which are automated.

>>>

Response Checklist

In case of a ransomware attack, institutions should do the following:

01

Isolate the infected computer immediately

Infected systems should be removed from the network as soon as possible to prevent ransomware from attacking network or shared drives.

02

Isolate or power off affected devices that have not yet been completely corrupted

This may afford more time to clean and recover data, contain damage, and prevent worsening conditions.

03

Secure backup data

Immediately secure backup data or systems by taking them offline. Ensure backups are free of malware.

04

Contact your local authority

Know who your local authority on ransomware is ahead of time so you can contact them immediately upon discovery to report an incident and request assistance.

05

Collect information

Collect and secure partial portions of the ransomed data that might exist.

06

Change passwords

If possible, change all online account and network passwords after removing systems suspected of being compromised from the network. Furthermore, change all system passwords once the malware is removed.

07

Check registry values

Delete any registry values that may be related to ransomware to stop the malware from loading.

08

Use response tools and initiatives

Make use of international initiatives such as NoMoreRansom, or free tools aimed at recovering from ransomware attacks.

09

Rebuild and recover

Identify the systems and accounts involved in the initial data breach and conduct an examination of existing detection or prevention systems. Once the environment is fully cleaned and rebuilt, issue password resets for all affected systems, and address any associated vulnerabilities and gaps in security or visibility.

Risks of Paying the Ransom

FS-ISAC does not encourage paying a ransom to criminal actors. However, after systems have been compromised, whether to pay a ransom is a serious, individual business decision, requiring the evaluation of all options to protect shareholders, employees, and customers. Ransomware victims may consider the following factors:

Paying does not guarantee a solution

Paying does not guarantee an organization will regain access to their data; in fact, some individuals or organizations were never provided with decryption keys after paying a ransom.

You are not protected from future attacks

Some victims who paid the demand were targeted again after paying the ransom.

Subsequent demands

After paying the originally demanded ransom, some victims were asked to pay more to get the promised decryption key.

Encouraging criminal activities

Paying the ransom simply funds further criminal activity and perpetuates the ransomware business model.

Sanctions

The US Department of the Treasury's Office of Foreign Assets Control (OFAC) has imposed sanctions on a number of cyber criminal threat actors and groups. By paying a ransom you may be violating those sanctions.

References and Further Reading

- **Cybersecurity and Infrastructure Security Agency (CISA): "Reduce the Risk of Ransomware" Awareness Campaign**
- **Cybersecurity and Infrastructure Security Agency (CISA): Ransomware Guide**
- **Cybersecurity and Infrastructure Security Agency (CISA): Stop Ransomware Webinars**
- **Cybersecurity and Infrastructure Security Agency (CISA): Stop Ransomware Fact Sheet**
- **Cybersecurity and Infrastructure Security Agency (CISA): Protect your Center from Ransomware**
- **Federal Bureau of Investigation (FBI): Common Scams and Crimes – Ransomware**
- **Federal Bureau of Investigation (FBI): Ransomware Prevention and Response for CISOs**
- **Europol: “NoMoreRansom” International Initiative**
- **National Cyber Security Centre (NL): Ransomware**
- **National Cyber Security Centre (UK): Phishing Attacks: Defending your Organisation**
- **National Cyber Security Centre (UK): Ransomware: What Board Members Should Know About Ransomware**
- **National Cyber Security Centre (UK): Mitigating Malware and Ransomware Attacks**

Thank you to our
contributing members:

Banco Falabella

Netherlands

MassMutual

Santander

WINTON

FS-ISAC Ransomware Working Group

FS-ISAC is leading a ransomware working group to create and share joint products related to ransomware, of which this is the first. If your institution is an FS-ISAC member and interested in joining this group to propose or contribute to such papers, please contact **intelligence@fsisac.com** to request an invitation to the group on Connect. If your institution is not yet an FS-ISAC member, **join** today.