FS-ISAC

The Rise and Rise of **Ransomware**

The Rise and Rise of Ransomware

An Irresistible Business Model

Once thought to be on the decline, successful ransomware attacks against all types of companies and organisations have dotted the headlines in the last two years. In 2019, the FBI's Internet Crime Complaint Center (IC3) received more than 2000 ransomware complaints, accounting for US$8.9 million in losses. We expect these numbers to grow, as the attack strategy now has multiple revenue streams.

Criminals used to simply hold systems or data for ransom; if you paid the money, access would be granted. However, multiple threat actors are now using a new extortion tactic: publicly naming victims and publishing their data online, which can impact firms in terms of both reputation and compliance. A third monetization strategy is auctioning compromised data off to the highest bidder on the dark web.

While the financial sector has proven resilient to these types of attacks – thanks to our strong cybersecurity culture and habits – we are not immune to this rapidly evolving threat.

In the last four months, ransomware operators have publicly claimed successful attacks against eight financial institutions, including three banks, around the world (not all have been confirmed with the firms). Large institutions with robust cybersecurity programs may be able to prevent ransomware attacks on their own networks, but they can still be impacted by third party suppliers. The Sodinokibi attack against foreign currency firm Travelex on New Year's Eve knocked online travel money services at several banks offline. A fintech company which services some of the world's biggest banks was hit in March by Ryuk, causing the company to pull infected servers offline. While these examples display an impact to business continuity, the supply chain vector also is a significant concern to financial institutions' security teams. Attacks delivered via third parties have proven to be highly effective in circumventing cybersecurity defenses.

Smaller institutions with less sophisticated defenses are even more vulnerable to direct attacks; not just from highly sophisticated criminal groups but also from novice criminals who buy ready-made attack products or kits from the more technical actors using a ransomware-as-a-service (RaaS) model.

Know Who You're Dealing With and What To Do

As cyber criminals are adept at adjusting to our prevention and mitigation strategies, further successful ransomware attacks against financial institutions and third parties are inevitable.

Threat intelligence can prove invaluable to a ransomware victim. Knowing the type of ransomware used in the attack can assist in determining the possible extent of the damages (as not all ransomware performs equally), the attacker's motivations and associated attack patterns, and whether the attacker is known to offer a decryption tool after payment. This type of information can help firms determine next actions, such as contacting law enforcement or obtaining decryption tools (see no more ransom), etc. It can also raise red flags on suspicious activity and help you build pre-emptive defenses to protect against specific ransomware tactics.

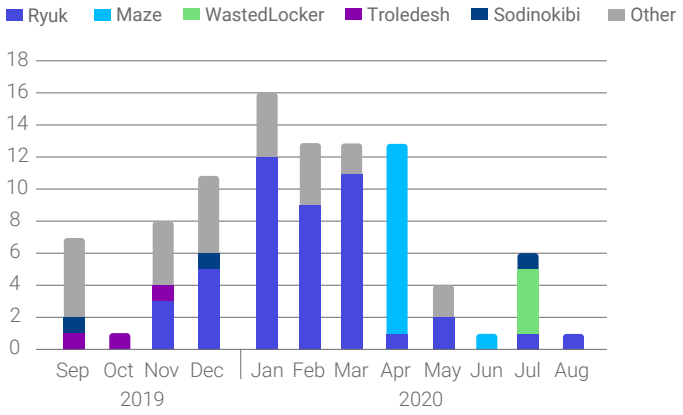
While individual institutions obtain threat intelligence from a variety of sources, no one institution can anticipate all threats all the time. FS-ISAC is the industry's trusted hub for cyber threat intelligence sharing, allowing members to both report and access threat intelligence on the latest ransomware actors (as well as the whole range of cyber threats facing the sector). Through FS-ISAC, institutions who do not have large threat intelligence functions in-house benefit from those who do, which helps better protect their firms and the industry as a whole.

Top 5 Threat Actors

While ransomware types can be delivered through many means, phishing is a common mechanism.

FS-ISAC members regularly report on phishing campaigns sent to staff, including those which lead to ransomware. Ryuk largely dominated the first quarter's notifications to FS-ISAC with 9 to 12 campaigns noted per month; however, Maze started in earnest in the second quarter with 12 campaigns observed in April.

Ransomware Incidents Reported
by members in last 12 months



Should You Pay the Ransom?

Thus far, several high-profile companies have opted to negotiate their ransoms in exchange for decryptors. Although there is appeal in paying the ransom, such as possible coverage from cyber-insurance and avoiding the cost of a network rebuild or legal fees, there also may be substantial costs.

In a recent example, Garmin, a GPS technology provider operating in various industries, fell victim to WastedLocker ransomware. The threat actors—attributed to Evil Corp—demanded $10 million in bitcoin to decrypt the Garmin network. Garmin began negotiations with its ransomware attackers, who are sanctioned by the US Department of Treasury for their part in Dridex campaigns. By paying a ransom to Evil Corp, organizations might be in non-compliance with sanctions that prohibit US individuals or organizations from engaging in transactions with Evil Corp or any of its individual members. These sanctions would likely also apply to organizations operating, but not headquartered in the US.

Symantec detailed how prolific these threat actors are, identifying at least 31 organizations—including financial firms—targeted with WastedLocker this year. According to Symantec, the attackers behind this threat appear to be skilled and experienced, capable of penetrating some of the most well-protected corporations, stealing credentials, and moving with ease across their networks. Those who become victim to WastedLocker may have to grapple with difficult choices about how to restore their systems and remain in compliance with sanctions.

FS-ISAC Tools

- Access to the new FS-ISAC Intelligence Exchange including Share, our re-designed threat intelligence sharing application.
- Recommendations and best practices related to prevention, mitigation and recovery around threats, bad actors and attacks including ransomware.
- Active peer-to-peer information sharing and discussions on FS-ISAC Connect channels and email lists.
- Engagement of a global intelligence network of more than 70 jurisdictions.
- Exercises on ransomware around the world.
- Coordination with other ISACs and agencies.

#DareToShare

With its attractive business model and multiple revenue streams, ransomware is a growing threat to financial services. Large institutions with robust security functions still must contend with potential impact of attacks on third parties, and small institutions face threats not only from sophisticated threat actors or nation-states but novice criminals who buy ransomware kits on the dark web. As ransomware perpetrators vary widely, threat intelligence is a critical tool in understanding how to respond to a ransomware attack.

FS-ISAC is the financial industry's trusted peer-to-peer intelligence sharing network, which offers not only standardized ways of both sharing and accessing threat intelligence from across the entire sector, but also tools and resources to help build strong cyber defenses and improve resiliency in the face of evolving threats - like ransomware.

Strengthen Your Defenses

Prevention is easier and more cost-efficient than dealing with a ransomware attack and restoring operations. Consider these best practices to help prevent ransomware attacks.

People

- Regularly educate and train employees to maintain situational awareness and report any potential issues immediately. Provide real-world examples and repercussions of successful ransomware exploits.
- Perform regular phishing tests to assess your employees' knowledge and ability to prevent ransomware attacks.
- Train cyber teams to coordinate a response with other parts of the organization including finance, communications and the executive team to respond when ransomware hits.

Process

- Ensure your incident response and business continuity plan includes ransomware response protocols (see below for details).
- Perform exercises to test playbooks and responses periodically, evaluate the lessons learned and modify your plan as required.
- Participate in cybersecurity information sharing organizations.
- 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 pay ransoms.

Business Continuity and Incident Response Plans Should Include:

- Details for employees about who to call if a ransomware ploy is successful.
- Ability to isolate the infected system from the network.
- Steps to isolate or power-off affected devices that have not yet been completely corrupted.
- Way to immediately secure backup data or systems by taking them offline and ensuring backups are free of malware.
- Tools to change all online account passwords and network passwords after removing the system from the network.
- How to work with law enforcement as appropriate.

Technology

Backups

- Back up critical data files regularly and frequently; keep them secured; test your processes and have files available to reload when needed.
- Test backup systems to ensure full recovery operations can be completed rapidly and seamlessly in case data recovery is required.

Access

- Assess the configuration of your network, software and where your data is securely stored regularly.
- Configure access controls such as file, directory and network share permissions with the least privilege in mind.
- Use firewalls to block access from known malicious IP addresses.

Email

- Set antivirus and anti-spam solutions to scan all incoming and outgoing emails for threats and filter out executable files. Automatically conduct regular scans.
- Enable strong spam filters to prevent phishing emails from reaching end users.
- Authenticate inbound email using technologies like Sender Policy Framework (SPF), Domain Message Authentication Reporting and Conformance (DMARC) and DomainKeys Identified Mail (DKIM) to prevent email spoofing.

Vulnerability Management

- Patch operating systems, software and firmware on devices. Consider using a centralized patch management system.
- Disable macro scripts from office files transmitted via email and autorun capabilities. Consider using a viewer software to open files via email instead of full office suite applications.
- Implement software restriction policies (SRP) or other controls to prevent programs from executing using common ransomware locations, such as temporary folders or compression/decompression programs, including the AppData/LocalAppData folder.
- Conduct an annual penetration test and vulnerability assessment.
- Consider disabling the remote desktop protocol (RDP) if it is not being used.

Resources

Global
NoMoreRansom.org

US
Federal Bureau of Investigation (FBI) Cyber Task Force
United States Secret Service (USSS) Economic Crime Task Force
Internet Crime Complaint Center (IC3)
DHS Computer Emergency Readiness Team (US-CERT)
NIST Cybersecurity Framework
NSA/IAD Top 10 Information Assurance Mitigations Strategies

UK
NCSC UK Guidance on Ransomware
National Crime Agency: Cyber Threats to UK Business
UK Action Fraud (run by the City of London Police)

Europe
Interpol Cybercrime Threat Response
Dutch National Cybersecurity Centre

APAC
Australian Cybersecurity Centre