INTELLIGENT TECHNICAL SOLUTIONS

Everything You Need to Know About Ransomware: Before, During and After an Attack

TABLE OF CONTENTS

Introduction

Ransomware is a booming cybercriminal attack method. It's a very lucrative endeavor for hackers and cybercriminals. How lucrative, you ask? In 2024, ransomware gangs have set new records. One notable case involved a staggering $75 million payment to the Dark Angels group, the largest ransomware payout ever recorded.

Did that get your attention? Some of you might be thinking these cybercriminals are only after these massive payouts. Unfortunately, they frequently target small to midsize businesses (SMBs), too. The truth is that every company is at risk; it's just that large enterprises get the headlines. But that doesn't mean a ransomware attack wouldn't have the same potential to cripple a small company. No matter your size or industry, you should be concerned about ransomware. Thankfully, you're reading this eBook because we'll discuss everything you need to know about it.

As a managed security service provider (MSSP), Intelligent Technical Solutions (ITS) is always keeping an eye out for ransomware trends to improve our security offerings for clients. We've also helped businesses prevent and respond to attacks over the years. In this eBook, you'll get a comprehensive guide to things you must do before, during, and after an attack. After reading, you'll have a better grasp of how to prevent, respond, and recover from ransomware incidents.

Chapter 1: Understanding Ransomware

What is Ransomware?

Ransomware is one of the biggest and most dangerous cybercrimes that organizations face today. It takes the form of malicious software (malware) that encrypts your files and data. In this context, encryption means turning your data into code that you can't read without a special key.

Ransomware footholds are commonly delivered via phishing emails with an infected attachment or malicious webpage. Once the attachment is clicked, it will install the malware on your device or spread throughout your network.

After the malware encrypts your data, you are left with a few choices: pay the ransom to get access back (hopefully), try to restore data from your backups, or lose your data forever and start over from scratch.

6 Most Common Types of Ransomware

One of the biggest problems when dealing with ransomware is that there are different types. So, there's no single solution to address it. Let's go over some of the most common ones that your business needs to watch out for:

1. Encrypting Ransomware

Encrypting ransomware is a type of attack where the malware encrypts your files, preventing you from accessing them unless you have the decryption key, a piece of code that reverses the encryption. In theory, hackers will provide you with the key after the ransom is paid. However, in the wild, there have been cases where the victim paid the ransom and was still given the wrong decryption key.

2. Locker Ransomware

Locker ransomware operates differently from encrypting ransomware as it kicks you out completely from your device rather than just encrypting your files. In this type of attack, cybercriminals typically disable all computer functions except for the mouse and keyboard. They leave those functions alone so you can still use them to pay the ransom.

3. Scareware

Scareware refers to a method of malware delivery. It uses scare tactics to trick you into downloading a product or service, unwittingly installing the malware on your device. Try to picture this: you're browsing the internet when suddenly a window pops up, stating a virus was detected on your computer. Clicking on that pop-up's buttons will install malware that gives hackers access to your device.

4. Doxware

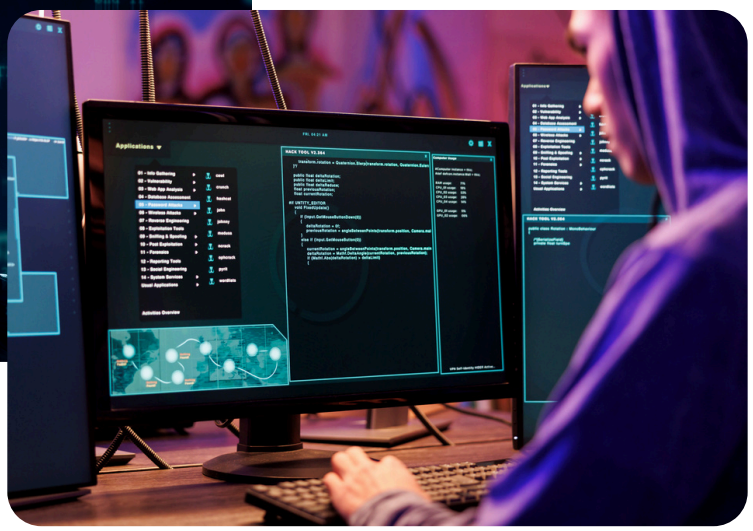
Doxware is one of the more dangerous types of ransomware. It doesn't just encrypt your files or lock you out of your device. Cybercriminals often use doxware to steal personal identifying information (PII) like birth dates, passport information, social security numbers, etc. They will then use that stolen data to threaten you by saying your information will be released publicly if their demands aren't met. The scary part is that leaking your PII opens you up to identity theft and, in some cases, physical harm.

5. Extortionware

Extortionware refers to the type of ransomware where a cybercriminal not only encrypts your data but threatens to leak it, too. They will look for private information, including company secrets and proprietary data, and use it to extort you for a ransom payout.

6. Wiper Malware

Unlike other forms of ransomware, wiper malware can inflict the greatest amount of damage because it destroys any file it infects. That type of attack can stop your operations in its tracks. In most cases, cybercriminals use a time-based trigger that will destroy your files once time runs out. They do that to give you a chance to pay the ransom before your data gets wiped. However, there have also been examples where the perpetrators don't even ask for a ransom. That's because not all ransomware attacks are financially motivated.



Main Motivations for Ransomware Attacks

Ransomware attacks are primarily motivated by financial gain. But there are other motives aside from it. Here are the main motivations for ransomware attacks:

1 . Financial Gain

Financial gain is the most common motivation behind ransomware attacks. Cybercriminals seek to extort money from individuals, businesses, or organizations by encrypting their data and demanding a ransom payment in exchange for decryption keys. The ransom amount can vary widely, depending on the perceived value of the data and the financial resources of the victim.

2. Political or Ideological Motives

Ransomware attacks may also be carried out for political or ideological reasons. Hacktivist groups or state-sponsored actors may use ransomware as a means of protest, retaliation, or espionage against governments, corporations, or individuals they perceive as adversaries.

3. Disruption and Destruction

In some cases, ransomware attacks may be motivated by a desire to cause disruption or destruction rather than financial gain. Cybercriminals may target critical infrastructure, such as healthcare facilities or government agencies, to disrupt operations, sow chaos, or even cause physical harm.

Chapter 2: What to Do Before a Ransomware Attack

In any crisis, preparation is the key to survival. It's crucial to do the following to give yourself the best chance of surviving a ransomware attack before it even occurs:

1. Risk Assessment and Mitigation Strategies

- ### Risk Assessment

  Conduct a thorough risk assessment to identify potential vulnerabilities in your systems and processes. Assess the likelihood and potential impact of a ransomware attack on your business. After that, you should be able to create essential strategies to defend yourself against them.

- ### Employee Training and Awareness

  Your team is your first line of defense against ransomware. That's why it's crucial to get them involved and train them to identify suspicious emails and other common attack vectors. Also, try to foster a culture of cybersecurity awareness and accountability within your organization. You can do that by encouraging employees to report suspicious activity promptly and reward good cybersecurity practices.

- ### Data Backup and Recovery

  Implement a robust backup and disaster recovery plan to ensure that critical data can be restored in the event of a ransomware attack. To do that, you need to regularly back up your data to secure offsite locations or cloud storage. You also need to test your backup systems regularly to verify their integrity and effectiveness.

- ### Legal and Regulatory Compliance

  Ensure your organization complies with relevant legal and regulatory data protection and cybersecurity requirements. That will mitigate further losses brought on by penalties and legal action in case of an attack. In addition, you need to understand your obligations in the event of a ransomware attack. That's why it's vital to have processes in place to notify regulators, law enforcement, and affected individuals as required.

- ### Cyber Insurance

  Consider purchasing cyber insurance to help mitigate the financial impact of a ransomware attack. Review your insurance policies carefully to understand what is covered and any limitations or exclusions that may apply, and work with your insurer to tailor coverage to your organization's specific needs.

2. Robust Cybersecurity Measures

- ## Email Security

  Implement email security solutions to detect and block phishing emails and malicious attachments. Use spam filters, email authentication protocols (such as SPF, DKIM, and DMARC), and email encryption to reduce the risk of email-based ransomware attacks.

- ## Endpoint Protection

  Deploy endpoint security solutions, such as antivirus software, antimalware programs, and endpoint detection and response (EDR) tools, to detect and block ransomware threats on endpoints (such as desktops, laptops, and mobile devices). Ensure that endpoint security software is regularly updated and configured to scan for threats in real time.

- ## Update/Patch Management

  Keep your operating systems, software applications, and firmware up to date with the latest security patches and updates. Regularly apply patches and security updates to address known vulnerabilities that could be exploited by ransomware attackers.

- ## Managed Detection and Response (MDR)

  MDR is an advanced cybersecurity service that provides continuous monitoring and response to threats, quickly identifying and stopping ransomware. Delegating detection and response to a professional security team is a more effective way to manage risks before they severely affect your organization's network.

- ## Application Whitelisting

  Application whitelisting ensures that only pre-approved programs can be executed on your system. This effectively keeps unwanted and potentially hazardous software, such as ransomware, from running on your network.

- ## Access Control and Least Privilege

  Limit access to sensitive data and systems to only those employees who need it to perform their duties. Enforce the principle of least privilege; it's a security concept that limits users' access rights to only what is strictly required to do their tasks. Doing that will minimize the impact of a ransomware attack and prevent lateral movement by attackers.

3. Incident Response Plan (IRP)

During a crisis like a ransomware attack, time is invaluable. You need to be able to respond to the incident swiftly and effectively if you want to mitigate the possible impact. To do that, you must develop a comprehensive IRP to guide your organization's response to a ransomware attack.

- ## Build Your Incident Response (IR) Team

  The first and most crucial step in creating an incident response plan is building the team to craft and carry out the plan. They are the ones who get the call when disaster strikes.

  This team should include everyone who will need to be contacted or take action in the event of a cybersecurity incident like a ransomware attack. The team doesn't just involve people from the IT department. It should include everyone in your organization who must be involved, including the legal and communications teams.

  To compile your team, you'll need to determine who in your organization is qualified to fulfill the following functions and roles:

  1. Leadership
  Coordinating the overall direction and strategy of each incident response ensures that everyone working on it is focused on minimizing damage, recovering quickly, and operating efficiently.

  2. Investigation
  Getting to the bottom of the incident as quickly as possible is paramount. That information enables teams to close security gaps, mitigate the damage, limit downtime, and begin recovery. Knowing how an incident started is also critical for learning to prevent the same thing from happening again.

  3. Communications
  Making sure that relevant internal and external communications are reaching the right people is essential. Facilitating communications may be required across an organization's teams and departments or with external stakeholders. This keeps everyone on the same page.

  4. Documentation
  Everyone must be cognizant of the need to create and preserve accurate records of every facet of an incident response. This serves two purposes: making sure that you can analyze the response effort and find areas of improvement and acting as a reference for similar future incidents.

5. Legal Representation

An incident always carries legal repercussions. It is important to ensure that incident response actions are being done in accordance with applicable laws and regulations to protect the organization. In some industries, regulators or authorities will need to be notified and kept apprised of the situation, or other actions may be needed to ensure legal compliance.

Follow the 4-Step NIST Incident Response Cycle

This 4-step Incident Response Cycle was developed by the National Institute of Standards and Technology (NIST). It provides a systematic framework for effectively managing cybersecurity incidents. Using this structured approach will allow your organization to minimize the impact of incidents, reduce downtime, and improve your overall resilience to cyber threats.

Step 1: Preparation

- Identify and prioritize critical assets and data that are most at risk of ransomware attacks.
- Develop policies and procedures for preventing, detecting, and responding to ransomware incidents.
- Establish roles and responsibilities for key personnel involved in incident response, including the incident response team, IT staff, legal counsel, and senior management.
- Implement technical controls, such as endpoint security solutions, network segmentation, and data backup and recovery systems, to mitigate the risk of ransomware attacks.
- Conduct regular training and awareness programs to educate employees about ransomware threats, phishing awareness, and best practices for cybersecurity hygiene.

Step 2: Detection and Analysis

- Implement monitoring solutions to detect indicators of ransomware activity, such as unusual file modifications, network traffic patterns, and unauthorized access attempts.
- Develop procedures for quickly triaging and analyzing potential ransomware incidents to determine their scope, impact, and severity.
- Establish communication channels and reporting mechanisms for employees to report suspicious activity and potential ransomware incidents promptly.
- Document and preserve evidence related to ransomware incidents for forensic analysis and legal purposes.

Step 3: Containment, Eradication, and Recovery

- Develop response procedures for containing the spread of ransomware within the network, including isolating affected systems and disconnecting them from the network.
- Implement technical controls, such as endpoint isolation, network segmentation, and firewall rules, to prevent ransomware from spreading to other systems and encrypting additional data.
- Develop recovery procedures for restoring encrypted data from backups, ensuring that backups are regularly tested and securely stored offsite.
- Coordinate with law enforcement, legal counsel, and incident response partners to investigate the ransomware incident and explore options for recovering encrypted data and identifying the perpetrators.
- Communicate with stakeholders, including employees, customers, partners, and regulatory authorities, about the ransomware incident and the steps being taken to mitigate its impact and recover from it.

Step 4: Post-Incident Activity

- Conduct a post-incident review to assess the effectiveness of the response to the ransomware incident, identify lessons learned, and implement improvements to the IRP and cybersecurity controls.
- Update policies, procedures, and technical controls based on the findings of the post-incident review to enhance preparedness for future ransomware incidents.
- Share information and best practices with industry peers and partners to help improve collective resilience against ransomware threats.
- Conduct regular exercises and simulations to test the effectiveness of the IRP and ensure that key personnel are familiar with their roles and responsibilities during a ransomware incident.

Chapter 3: What to Do During a Ransomware Attack

Ransomware attacks can be chaotic and stressful situations. Having a structured plan in place can help ensure that you take the appropriate actions promptly and effectively. This section can help guide you through a ransomware incident:

Am I Under Attack? 10 Tell-Tale Signs of a Ransomware Attack

Recognizing the signs of a ransomware attack early on can help you take swift action to minimize the damage. Here are ten tell-tale signs that you may be experiencing a ransomware attack:

1. Unusual Pop-up Messages

If you start seeing unexpected pop-up messages on your computer or device claiming that your files have been encrypted and demanding payment in exchange for decryption keys, it's a strong indication of a ransomware attack.

2. Files Suddenly Inaccessible or Renamed

Ransomware typically encrypts your files, making them inaccessible or renaming them with unusual file extensions. If you notice that your files have become unreadable or have been renamed in a strange manner, it could be a sign of ransomware.

3. Ransom Notes

Ransomware often leaves ransom notes behind, either as text files or as desktop backgrounds, providing instructions on how to pay the ransom and regain access to your files. If you find such notes on your system, it's a clear indicator of a ransomware attack.

4. Unexpected Encryption Processes

Monitor your system's processes and task manager for any unexpected or suspicious encryption processes running in the background. Ransomware typically employs encryption algorithms to lock your files, so unusual encryption processes may indicate an attack.

5. Sudden Network Activity

Ransomware may communicate with command-and-control servers or download additional malicious payloads from the internet. Monitor your network traffic for sudden spikes in activity or unusual connections to suspicious IP addresses or domains. You should also check for activities during off hours, like holidays, weekends, or closing hours.

6. Sluggish Performance

Ransomware can consume significant system resources, leading to sluggish performance or slower-than-usual operation of your computer or network. If you notice a sudden decline in performance without any obvious cause, it's worth investigating further.

7. Disabled Security Software

Some ransomware strains may attempt to disable antivirus or security software to avoid detection and removal. If you find that your security software has been turned off or is unable to update, it could be a sign of ransomware.

8. Phishing Emails or Suspicious Links

Ransomware often enters systems through phishing emails or malicious links. If you or your employees receive unexpected emails with attachments or links from unknown senders, exercise caution and avoid opening them.

9. Unexplained File Modifications

Keep an eye out for unexplained modifications to your files, such as changes in file sizes, timestamps, or permissions. These alterations may indicate that ransomware has tampered with your data.

10. Error Messages During Boot-Up

Some ransomware variants may modify the Master Boot Record (MBR) or boot sector of your computer, resulting in error messages or an inability to boot into the operating system.

Immediate Actions to Take: Ransomware Response Checklist

- ☐ Notify your IRP Team
- ☐ Determine which systems were impacted and isolate them immediately.
- ☐ Disconnect devices from the network or power them down to avoid further spread of infection.
- ☐ Figure out the scope of the attack. Triage impacted systems for restoration and recovery while prioritizing critical systems.
- ☐ Gather your team to document and develop an understanding of the incident.
- ☐ Implement your incident response plan.
- ☐ Gather and preserve evidence for forensic investigation.
- ☐ Identify the systems and accounts involved in the initial breach.
- ☐ When necessary, contact federal law enforcement and relevant regulatory agencies.

What Should I Do with Ransom Demands?

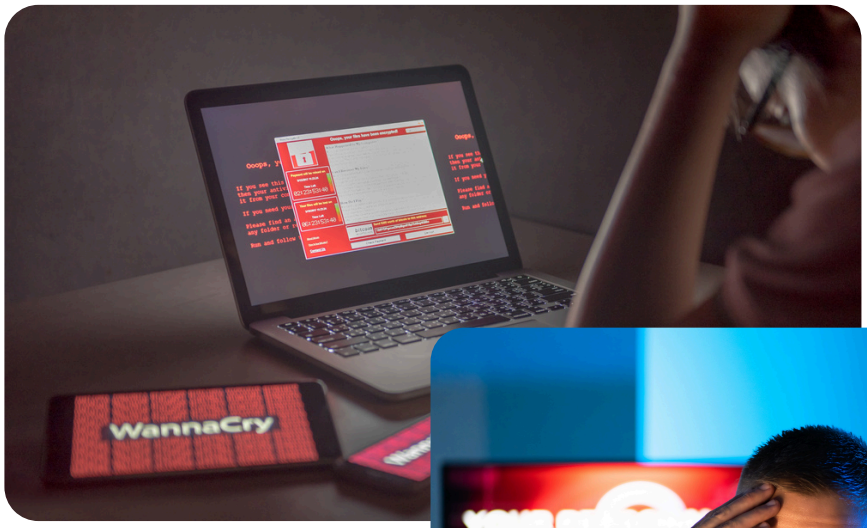
Handling ransomware demands requires careful consideration and should be approached with caution. Here are some general rules of thumb when faced with ransomware demands:

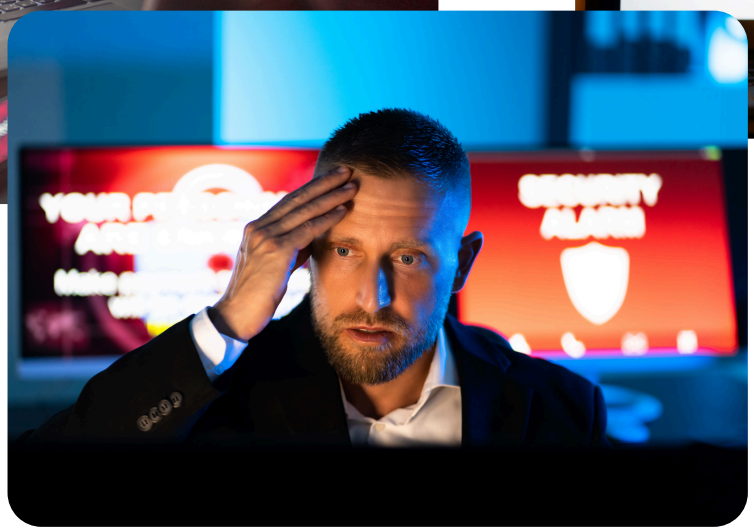
Do Not Pay the Ransom: The general recommendation from cybersecurity experts and law enforcement agencies is not to pay the ransom. Paying does not guarantee that you will regain access to your files, and it can fund further criminal activities. Additionally, paying the ransom only encourages cybercriminals to continue their malicious activities, potentially targeting others in the future.

Assess the Situation: Before making any decision, assess the ransomware attack's severity and its impact on your systems and data. Determine which systems and files have been affected and whether you have backups available for recovery.

Consult with Experts: Seek guidance from cybersecurity professionals, law enforcement agencies, or legal counsel experienced in dealing with ransomware incidents. They can provide valuable advice and assistance in handling the situation and may be able to offer alternative solutions for data recovery.

Consider Legal Implications: Paying the ransom may have legal implications, depending on your jurisdiction and organizational policies. Consult with legal counsel to understand the legal ramifications of paying the ransom and to ensure compliance with relevant laws and regulations.





Chapter 4: What to Do After a Ransomware Attack

The aftermath of a ransomware attack can be brutal. You can mitigate the impact of an attack as much as you can, but there will be damage either to your data or your reputation, or both. The only way to avoid any damage from ransomware is to prevent it from happening at all. That's why taking proactive steps is essential to ensure it doesn't happen again. In this section, we'll dive into all the steps you need to take during the aftermath of a ransomware attack:

Step 1: Gather Relevant Information

Collect all available information related to the ransomware incident, including incident reports, logs, communications with stakeholders, and documentation of response efforts.

Step 2: Assemble a Review Team

Form a multidisciplinary team comprising representatives from IT, cybersecurity, legal, compliance, and relevant business units. Ensure that the team includes individuals with knowledge of the incident and expertise in incident response and cybersecurity.

Step 3: Define Objectives

Clarify the objectives of the post-incident review, such as identifying root causes, evaluating response effectiveness, and recommending improvements to prevent similar incidents in the future.

Step 4: Prepare Your Data

Assess the quality and availability of your data. If necessary, clean and preprocess data to ensure it is suitable for training and testing AI models.

Step 5: Choose the Right AI Technologies

Select the right AI technologies based on your business objectives and data. It's important to determine which AI tools will deliver the biggest impact in helping you achieve your goals.

Step 6: Assess Response Effectiveness

Evaluate the effectiveness of the response efforts in containing the ransomware incident, minimizing impact, and restoring operations. Identify strengths and weaknesses in the response process and areas for improvement.

Step 7: Review Policies and Procedures

Evaluate the organization's incident response policies, procedures, and protocols. Determine whether they were followed effectively during the ransomware incident and identify any gaps or deficiencies that need to be addressed.

Step 8: Evaluate Communication and Coordination

Assess the communication and coordination among internal stakeholders, external partners, and relevant authorities during the ransomware incident. Identify areas where communication breakdowns occurred and recommend improvements.

Step 9: Document Lessons Learned

Document lessons learned from the ransomware incident, including insights gained, challenges encountered, and best practices identified. Capture recommendations for enhancing cybersecurity posture and incident response capabilities.

Step 10: Develop Action Plan

Based on the findings of the post-incident review, develop a comprehensive action plan with specific recommendations for improving security controls, updating policies and procedures, enhancing employee training, and implementing technical safeguards.

Step 11: Implement Recommendations

Prioritize and implement the recommendations identified during the post-incident review. Assign responsibilities, establish timelines, and track progress toward implementation to ensure accountability and effectiveness.

Step 12: Monitor and Iterate

Continuously monitor the effectiveness of the actions taken to address the findings of the post-incident review. Iterate on the action plan as needed based on evolving threats, organizational changes, or lessons learned from subsequent incidents.

Ready to Take Proactive Steps Against Ransomware?

Ransomware is one of the biggest threats to your business today. It doesn't matter the size or industry of your organization; you could fall victim unless you take action right now. It's important to stay ahead if you're going to defend against the threat of ransomware. Thankfully, this eBook covered all the essential strategies and best practices your organization should take to prepare, respond, and recover from an attack.

ITS has helped countless businesses take proactive steps against ransomware. If you need help setting up your defenses, schedule a free consultation with our cybersecurity experts. They can provide IT security assessments and guide you through your journey toward cyber resilience.

Intelligent Technical Solutions (ITS)
(885) 204-8823
www.itsasap.com