Ransomware Playbook

CyberAlberta

February 13, 2024

Contact Information:
Cybersecurity Division
Technology and Innovation
5th floor, Terrace Building
9515 – 107 ST NW
Edmonton, AB T5K 2C1

Published by:
Technology and Innovation, Cybersecurity Division

Classification: Public
Disclaimer

Preface

This document is a generic playbook based on the Government of Alberta's ransomware standard operating procedure. You can use this document to construct your own organization's ransomware playbook or process. References to internal teams or policy instruments have been encapsulated in brackets ("< >"). These should be replaced with information specific to your organization. For more information, please contact the CyberAlberta general mailbox:

CyberAlberta Support
cyberalberta@gov.ab.ca

Ransomware attacks can be detected through various channels, including, but not limited to:

- automated antivirus (AV) alerts;
- detection from email filters;
- noticing unusual activity on end-point devices, servers, or phones; &
- reports from end users.

Anyone identifying a potential ransomware attack should report it immediately to <your help desk or IT service desk>, per the <your organization's Security Incident Response Process>, where the incident will be tracked and managed.

Note: This page can be excluded or re-written to be a preface tailored to your organization.

Effective Date

This publication takes effect on February 16, 2024.

Approved by: Martin Dinel	**Owner:** CyberAlberta (Martin Dinel, ADM)	
Approval date: 16-02-2024	**Reviewed date:** 16-02-2024	**Next review date:** 16-02-2025
Contact: Martin Dinel, ADM for the Cybersecurity Division Email: martin.dinel@gov.ab.ca	**Policy Instrument type:** Playbook	

Table of Contents

Overview

Ransomware is a type of malware that denies a user access to a system or data until a ransom is paid. It is a serious and evolving threat with a devastating impact for an individual or an organization. Vital data and devices can become inaccessible to organizations, leaving them unable to conduct their business or serve their clients. Recovering from a ransomware incident also consumes many resources time and significant budget, beyond the cost of the ransom in the event one is paid out.

Over the past year, threat actors have adjusted their tactics to compensate for victims having the ability to recover their data from backups to include coercing these victims to pay the ransom under the threat of publicly posting stolen and encrypted data to further embarrass the organization. Ransomware has become more sophisticated, targeted, and complex. It is increasingly difficult for organizations to prevent and to recover from these attacks, especially when an organization has limited cybersecurity resources or investment.

Threat actors are now operating more covertly. They silently gain access to an organization’s environment and proceed to identify critical systems, high-value data, personal information, and information that could cause reputational damage if leaked to the public. Threat actors then deploy the ransomware to identified datasets and systems, leaving the organization compromised. Threat actors also actively monitor the organization’s communication channels as well as activities around the discovery and resolution of the ransomware incident to undermine response efforts and further infiltrate networks and connected devices.

This document outlines the three phases and various steps to respond to a ransomware attack:

1. Assessment
2. Response
3. Post-Incident

If you have been the victim of ransomware and need advice or guidance to recover from it, skip to the Assessment Phase and report the ransomware incident to <your Help Desk or Service Desk> at <phone number or contact information>.

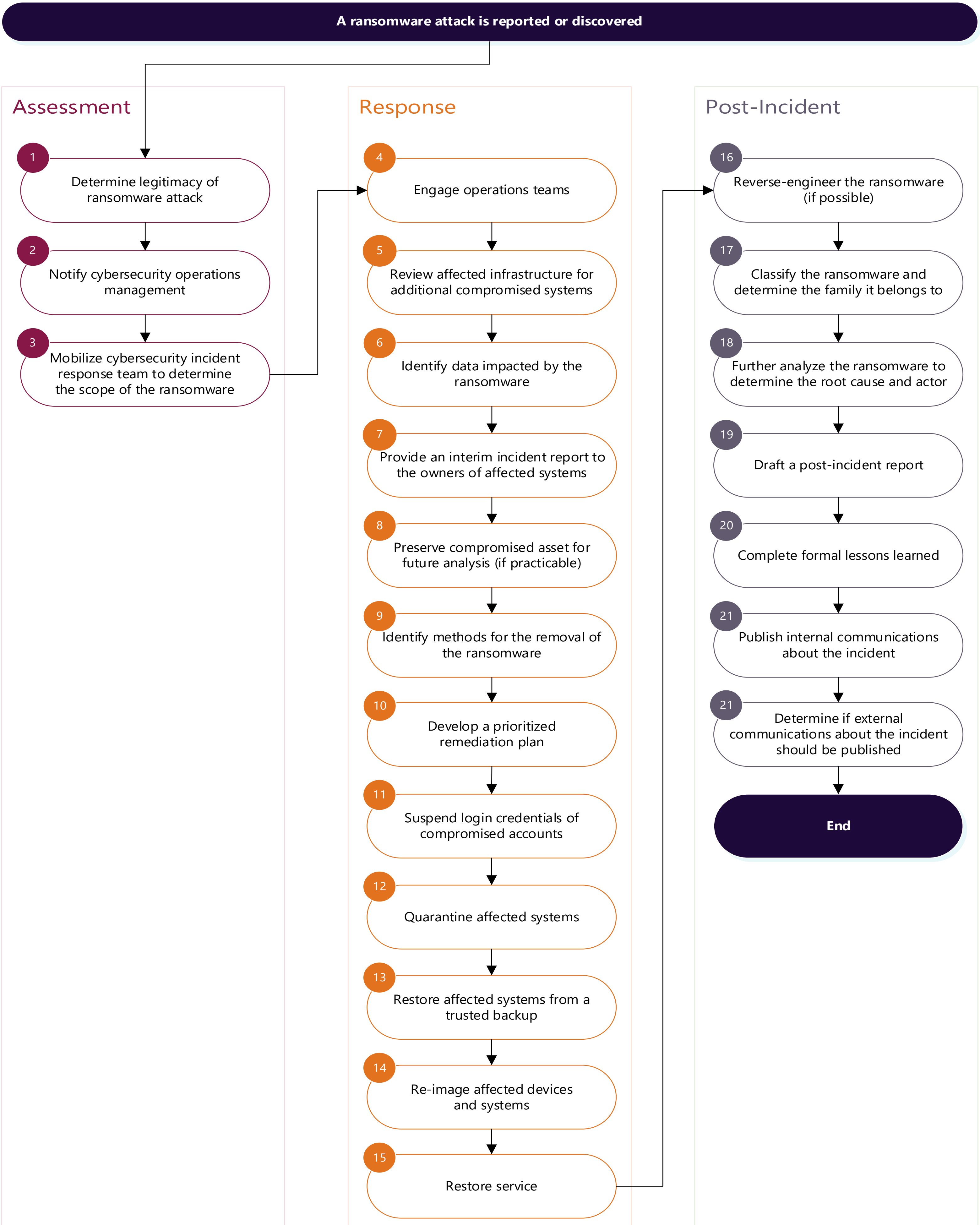
Once your recovery efforts are in place, please refer to the Protecting Against Ransomware appendix for advice on how to improve your cybersecurity environment.

We also advise not to comment whether your organization paid a ransom. Admitting to paying a ransom may direct attention to your organization from additional threat actors as they may assume that your organization has technical weaknesses and are opened to paying a ransom to get your data back. The admission also encourage more threat actors to leverage ransomware as a way to make money.

For more information on ransomware or other cybersecurity-related topics please email <your cybersecurity department mailbox>

Ransomware Flowchart Template

2024-01-26



A ransomware attack is reported or discovered

Assessment

1 Determine legitimacy of ransomware attack

2 Notify cybersecurity operations management

3 Mobilize cybersecurity incident response team to determine the scope of the ransomware

Response

4 Engage operations teams

5 Review affected infrastructure for additional compromised systems

6 Identify data impacted by the ransomware

7 Provide an interim incident report to the owners of affected systems

8 Preserve compromised asset for future analysis (if practicable)

9 Identify methods for the removal of the ransomware

10 Develop a prioritized remediation plan

11 Suspend login credentials of compromised accounts

12 Quarantine affected systems

13 Restore affected systems from a trusted backup

14 Re-image affected devices and systems

15 Restore service

Post-Incident

16 Reverse-engineer the ransomware (if possible)

17 Classify the ransomware and determine the family it belongs to

18 Further analyze the ransomware to determine the root cause and actor

19 Draft a post-incident report

20 Complete formal lessons learned

21 Publish internal communications about the incident

21 Determine if external communications about the incident should be published

End

Assessment

Once a ransomware incident has been reported, it enters the assessment phase. Key activities that occur during the assessment phase include, but are not limited, to the following:

Activity	Actions
1	□ Determining the legitimacy of the ransomware attack (e.g., is it genuine? Another type of malware masquerading as ransomware? Etc.)
2	□ Notifying your leadership and communications team within your organization accordingly. Leadership or communications can start drafting holding messages, start media/social scans, and other early response activities. This may help avoid embarrassing issues, like unknowingly releasing a planned social post about a service that is currently experiencing issues
3	□ Mobilizing cybersecurity incident response team to determine the scope of the ransomware. This initial investigation will include the following steps: o determining whether data loss or data breach has occurred; o determining the preliminary business impact; o determining how the cyber incident was reported; o determining where the ransom messages are appearing; o determining the initial number of affected assets across the organization and the extent of travel of the ransomware; o identifying the attack email or ingress point; o identifying indicators of compromise and determining if there is a risk of further ransomware propagation; o pinpointing the location of detection(s), both physical and logical; o determining if there are any infected network drives and, if so, which ones; o examining additional reporting relating to affected assets, including AV logs, system event logs, and network monitoring logs; o examining threat intelligence feeds to determine if the ransomware attack is bespoke and targeted at specific accounts, infrastructure, or systems; o researching threat Intelligence sources to gain further intelligence and support mitigation by others; & o noting any current action(s) being undertaken.

Essential communications during the assessment phase of a ransomware attack can include:

Timing	From	To	General Message
After initial investigation and confirmation of ransomware incident	Cybersecurity	Senior Management Corporate Communication Canadian Centre for Cybersecurity (CCCS) Local Law Enforcement CyberAlberta (Recommended)	Confirmation of incident and extent of incident, as well as high level plan to resolve the incident. It is important to also notify CCCS so that they are aware of the issue. They may provide assistance depending on the severity of the incident and will ensure that other Canadian organizations are alerted to potential related attacks. Ransomware is a crime and just as any other crimes, the information should also be reported to law enforcement. Consider identifying a contact for your Corporate Communications team who can facilitate reviews and approvals.

Timing	From	To	General Message
			CyberAlberta may be able to provide assistance, as well as reach out to COI members to warn of potential attacks.
If a privacy breach is suspected	Cybersecurity	Office of the Information Privacy Commissioner (OIPC)	Communicate incident details and evidences suggesting that this may result in a privacy incident. Provide details as to the records and individuals whose data might be compromised.
In response to multiple public concerns or media inquiries	Communications	Public	High-level messaging noting that service impacts are being investigated and thanking clients for their understanding. At this stage, public communications should remain reactive. Avoid sharing undetermined information, including details about the potential attack and restoration timelines. Messaging should be approved by appropriate members of cybersecurity and leadership. Responding to public comments can help control the narrative and reduce speculation.

Response

There are several key activities to the response phase when dealing with a ransomware incident, with the main goal being to recover from the incident in the least amount of time possible:

Activity	Actions
1	□ Engage the forensics team, if one exists, to preserve evidence, to be used for root cause analysis.
2	□ Engaging operations teams (e.g., server team, storage team) to aid in the implementation of the response plan.
3	□ Reviewing affected infrastructure for indicators of compromise derived from the malware analysis to identify any additional compromised systems and verifying all infected assets are in the process of being recalled and quarantined.
4	□ Identifying any data impacted by the ransomware attack, including data-in-transit. Data owners and the business should be engaged to understand the business impact of the compromised data.
5	□ Determining the likelihood that any identified data's confidentiality, integrity or availability was compromised.
6	□ Providing an interim incident report to the service owners of the affected system(s).
7	□ Preserving the compromised asset or a copy of it, if possible, for future analysis including forensic investigation.
8	□ Identifying methods for the removal of ransomware from the results of the malicious code analysis and trusted sources (e.g., AV providers, law enforcement, Canadian Centre for Cyber Security (CCCS), etc.).
9	□ Incorporating technical and business analysis in developing a prioritized remediation plan which includes a communication strategy.
10	□ Suspending the login credentials of confirmed and suspected compromised accounts.

Activity	Actions
11	□ Reduce any further malicious activity by quarantining affected systems (either using manual or automatic means) and removing them from the network, where possible, or applying access controls to isolate them from production networks. Business data owner(s) and stakeholders should be kept abreast of the progress of containment activities. □ The scope of containment can be defined by searching for the: ○ SHA-1 process name; ○ executable file name; & ○ URL or IP address of similar connections on the network. □ Protection measures derived from the results of malicious code analysis to protect infrastructure from the malicious code and other ransomware that may attempt to infect using the same mechanism should also be developed at this time.
12	□ Conducting a restoration of affected networked systems from a trusted and tested backup. The priority of recovery of these systems will be based on business impact analysis and business criticality.
13	□ The systems/ devices that have been affected should be re-imaged. This includes, at a minimum the following: ○ Re-installing any standalone systems from a clean Operating System (OS) backup before updating with trusted data back-ups. ○ Re-setting the credentials of all involved system(s) and users' account details. ○ Coordinating the implementation of any necessary patches or vulnerability remediation activities.
	□ Once the system(s)/ device(s) have been restored and re-imaged the restoration of service can begin. Activities involved in this step include, but are not limited to: ○ Completing ransomware scanning of all systems, across the environment. ○ Reintegrating previously compromised systems. ○ Restoring any corrupted or destroyed data. ○ Restoring any suspended services. ○ Continuing to monitor for signatures and other indicators of compromise to prevent the ransomware attack from re-emerging. □ Confirming policy compliance across the organization.

Essential internal and stakeholder communications during the response phase of a ransomware attack can include:

Timing	From	To	General Message
After initial assessment is completed and initial communication occurred	Cybersecurity	Forensics Team IT Support Teams Leadership	Notify Forensics team to preserve any evidence as required for root cause analysis. IT support teams (namely, server, storage and/or back-up teams) to resolve encrypted files. Leadership should be provided a high-level resolution plan.
Routinely according to the impact and urgency to restore the data	Cybersecurity	Leadership	Leadership should retrieve routine status updates.
After the initial impact has been assessed	Cybersecurity	Communications Team	If your organization has a communications team, they may be able to support stakeholder, internal, and public communications.

Timing	From	To	General Message
			Ensure communications is aware of high-level updates, as they may impact messaging. Public communications materials and approach should be approved by appropriate members of cybersecurity and leadership.
After privacy impacts have been discovered	Cybersecurity	Privacy Team	The Privacy team will need to be notified to initiate their own processes for response to privacy beaches.
After the initial impact has been assessed and there are any suspected acts, regulation, or policy violations	Cybersecurity	Legal Team	The legal team should be notified of the nature of the impact, including the type of data, and whom the stakeholders are for this data. They may need to look at the legal implications the breach could present.

Depending on the severity of the incident, essential public communications during the response phase of a ransomware attack can include:

Timing	From	Tactic	General Message
Upon notification	Communications	Communications plan Key messages	Outline the overall communications approach for stakeholders, staff, and the public. Develop key messages that share the most important pieces of information with the audience to help keep messaging consistent. Consider timing and messaging. Be transparent without sharing sensitive information. The plan and messaging should be approved by appropriate members of cybersecurity and leadership.
In response to public inquiries	Communications	Social media	Provide high-level updates to keep clients informed on the situation. Responding to public comments can help control the narrative and reduce speculation. Individuals will often go to social media when experiencing a technical issue. Avoid sharing sensitive or undetermined information, including restoration timelines. Depending on the level of public impact, consider whether a reactive or proactive approach is most appropriate. Reactive may be more suitable when public impacts are minimal, whereas proactive may be more suitable for larger incidents. Never report whether ransom was paid by the organization.
In response to media inquiries	Communications	Media statement or response	Provide information about the incident. Never report whether ransom was paid.

Timing	From	Tactic	General Message
		Web content Direct stakeholder communications	Consider creating library of media questions and responses to ensure consistent messaging is shared with all inquirers. If a breach results in significant public impacts, inform stakeholders of the incident and steps being taken to resolve the situation. Use existing channels and, if required, provide multiple updates. This will help reduce speculation and assure clients they are being considered during response. Be transparent without sharing sensitive information. Avoid undetermined information, including restoration timelines. It should be approved by appropriate members of cybersecurity and leadership.

Post Incident

If the organization does fall victim to ransomware, conducting lessons learned exercises post-recovery is an excellent method to implement further mitigation measures and corrective actions and strategies that did not go as planned. Revising the incident response plan based on these lessons learned will ensure that the organization has the most robust response and recovery plans possible. These lessons learned may also be shared through secure channels with other organizations, such as the CyberAlberta Community of Interest, as sharing these lessons can benefit other organizations and the cybersecurity community, ensuring greater all-around protection for Albertans.

Key activities of the post-incident phase include, but are not limited to:

Activity	Actions
1	□ Reverse-engineering the ransomware in a secure environment to understand its mechanisms and the functionality it implemented ○ The reverse-engineering may be helped by executing the ransomware in a secure environment or sandbox, segregated from the business network, to determine its behaviour on a test system, including created files, launched services, modified registry keys, and network communications
2	□ Classifying the ransomware by submitting it to AV vendors and determining the family it belongs to.
3	□ Completing further analysis of the ransomware, including a potential forensic investigation and a root cause analysis to identify and remediate underlying vulnerabilities.
4	□ Drafting a post-incident report that includes the following details as a minimum: ○ details of the cause, impact, and actions taken (successful or otherwise) to mitigate the cyber incident; ○ timings, type, and location of the incident; ○ any effects on users and/or clients caused by the attack or during the remediation; ○ activities undertaken by relevant operations groups, service providers, and business stakeholders that enabled normal business operations to resume; ○ recommendations of any aspects of people, processes, or technology that could be improved across the organization to help prevent a similar cyber incident from reoccurring; & ○ a review of staff welfare (e.g., working hours, overtime, time off in lieu and expenses).

Activity	Actions
5	□ Completing the formal lessons identified process to feedback into future preparation activities.
6	□ Publishing internal communications to inform and educate employees on ransomware attacks and security awareness.
7	□ Publishing external communications, if appropriate, inline with the communications strategy to provide advice to customers, engage with the market, and inform the press of the cyber incident. ○ These communications should provide key information about the cyber incident without leaving the organization vulnerable or inciting further ransomware attacks.

Essential communications during the post incident phase of a ransomware attack can include

Timing	From	To	General Message
After the incident has been resolved	Cybersecurity	Leadership	Post incident report, including: • Root cause analysis • High level information about what happened, when, how it was resolved, and any potential repercussions or related advice to stakeholders • Lessons Learned • Planned preventative measures
After post incident report has been communicated to leadership	cybersecurity and leadership or Communication team	Clients/ stakeholders/ or the public if it makes sense for the organization	High level information about what happened, when, how it was resolved, and any potential repercussions or related advice to stakeholders. Consider alignment with previously shared messaging. Never report whether ransom was paid.

Appendix

A.1 How does Ransomware Work?

When ransomware infects a device, it either locks the screen or encrypts the files, preventing access to the information and systems on your devices. Threat actors can also use compromised networks to spread the ransomware to other connected systems and devices.

- Networks and devices can be infected with ransomware in the following ways:
- Visiting unsafe, suspicious, or compromised websites (known as a drive-by download);
- Opening emails or files from familiar or unfamiliar sources (phishing);
- Clicking on links in emails, social media, and peer-to-peer networks;
- Inserting an infected peripheral device (e.g., USB flash drive) into a device; or,
- Exposing systems to the internet unnecessarily or without robust security and maintenance measures, such as patching vulnerabilities and multi-factor authentication (MFA) in place.

If your device is infected with ransomware, you will receive a notice on your screen indicating your files are encrypted and inaccessible until the ransom is paid. You may also receive a message on your lock screen indicating your device is locked and inaccessible until the ransom is paid. The message will instruct you to pay a ransom to unlock the device and retrieve the files. Payment is often requested in the form of digital currency, such as bitcoin, because the transfer would be more difficult to trace. Prepaid credit cards or gift cards may also be requested. You will be provided with a time limit to pay the ransom, after which threat actors may increase the ransom amount, destroy your files permanently, or leak your data. As an additional extortion method, a threat actor may threaten to release your data publicly if you do not pay the ransom.

Ransomware has become more sophisticated and often employs a combination of attack vectors, such as sending a phishing email to various personnel along with brute force attacks, where the threat actor uses extensive login attempts or password guessing to access systems and

Ransomware Vectors

Phishing is an attack that uses text, email, or social media to trick users into clicking a malicious link or attachment. Phishing attempts are often generic mass messages, but the message appears to be legitimate and from a trusted source (e.g. a bank). Malicious code will execute commands using your account privileges. Threat actors may also use this opportunity to install a backdoor to your devices.

Drive-by download occurs when a user unknowingly visits an infected website where malware is downloaded and installed without the user’s knowledge.

Malvertising injects malicious code into legitimate online advertisements. When a user clicks the ad, malware spreads to their device.

Exposed services, such as Remote Desktop Protocol (RDP) and content management systems, allow access to your devices. Threat actors can use a variety of tactics, such as exploiting common vulnerabilities and password spraying, to access your devices via these exposed systems and deploy ransomware.

Ransomware Aids

While the following items are not traditional vectors, they are available options for threat actors to use to initiate a ransomware attack.

Third parties and managed service providers (MSP) identities can be used by threat actors to spoof emails or conduct phishing attacks against your business.

Supply chain attacks allow threat actors to infiltrate a service supply organization and force an update to connected customers, infecting their systems and devices with ransomware.

Ransomware as a Service (RaaS) is a model in which threat actors, regardless of their skills, can purchase malware from developers on the dark web. The developers receive a portion of the ransom paid by the victim.

networks. Ransomware can also spread to the systems and networks of organizations connected via their supply chain. For example, an organization that provides services to its clients via inter-connected networks and client management systems could be targeted by ransomware.

A.2 Protecting Against Ransomware

Ransomware is one of the most common types of malware and can be one of the most damaging cyber-attacks for any organization. Single mitigation measures are not robust enough to combat the evolving threat of ransomware.

Key activities to prepare to respond to a ransomware attack include:

- Reviewing and rehearsing cyber incident response procedures including:
  - technical roles and responsibilities;
  - business roles and responsibilities; &
  - escalation to a major incident.
- Reviewing recent cyber incidents and outputs
- Reviewing threat intelligence for threats to organizations, brands, and the ministry, as well as common patterns and newly developing risks and vulnerabilities
  - This should include reviewing and defining threat and risk indicators and alerting patterns within the organization's security information and event management (SIEM) solution based on the research.
- Ensuring appropriate access to any necessary documentation and information, including out-of-hours access
- Setting up a retainer-based agreement to have the ability to quickly access the services of a third-party, should they be required"
- Conducting regular awareness campaigns to highlight information security risks faced by employees, including:
  - phishing attacks and malicious emails;
  - importance of system patches;
  - ransomware; &
  - reporting a suspected cyber incident.

  In addition to general awareness training, regular security training must be mandated for those employees managing personally identifiable information (PII) or protected or high-risk data and systems.

- Some general tips that can be taken to reduce the effects of ransomware on systems include, but are not limited to:
  - In the case of an email attack:
    - Block the sender and the message by marking it as spam; &
    - Block the IP address identified in the email header.
  - In the case of a website compromise:
    - Block the website at the network perimeter;
    - Sinkhole the domain on internal DNS servers;
    - Block the site IP address on the network firewall;
    - Ensure all web browsers have the latest patches; &
    - Encourage users to switch to newer browsers.
  - Blocking access to any identified Remote Access Tools to prevent communication with command and control servers, websites, and exploited applications.

A.3 Abbreviations

Abbreviation	Definition
AV	Antivirus
CCCS	Canadian Centre for Cyber Security
CISO	Chief Information Security Officer
MSP	Managed Service Providers
MFA	Multi-Factor Authentication
OS	Operating System
PII	Personally Identifiable Information
RaaS	Ransomware as a Service
SIEM	Security Information and Event Management

A.4 Glossary

Term	Definition
Defence-in-Depth	An IT security concept (also known as the Castle Approach) in which multiple layers of security are used to protect the integrity of information. These layers can include antivirus and antispyware software, firewalls, hierarchical passwords, intrusion detection, and biometric identification.
Malware	Malicious software designed to infiltrate or damage a computer system, without the owner's consent. Common forms of malware include computer viruses, worms, Trojans, spyware, and adware.
Malvertising	Injects malicious code into legitimate online advertisements. When a user clicks the ad, malware spreads to their device. A common method for delivering ransomware.
Multi-Factor Authentication	Authentication is validated by using a combination of two or more different factors including: something you know (e.g. a password), something you have (e.g. a physical token), or something you are (a biometric).
Phishing	An attempt by a third party to solicit confidential information from an individual, group, or organization by mimicking or spoofing, a specific, usually well-known brand, usually for financial gain. Phishers attempt to trick users into disclosing personal data, such as credit card numbers, online banking credentials, and other sensitive information, which they may then use to commit fraudulent acts.
Spoofing	A threat actor uses the Internet Protocol (IP) address of another computer to masquerade as a trusted source to gain access to an individual's or organization's computer, device, or network.
Ransomware	A type of malware that denies a user access to files or systems until a sum of money is paid. Ransomware incidents can devastate an organization by disrupting its business processes and critical functions reliant on network and system connectivity.