Ransomware: How to prevent and recover

CANADIAN CENTRE FOR CYBER SECURITY

April 2024 | ITSAP.00.099

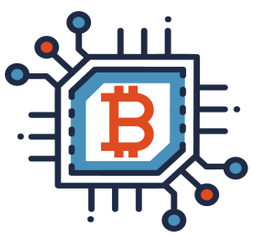
Ransomware is a type of malware that denies a user's access to files or systems until a sum of money is paid. Ransomware can infect your network and spread to all connected devices. Threat actors can deny your access to organizational files by encrypting your data, blocking your ability to log into organizational devices and using extortion methods to coerce you into paying the ransom to avoid your data being leaked.

Threat actors can purchase ransomware on the dark web. The malicious code needed for the attack is already written, eliminating the need for them to know how to write the code themselves. This is known as ransomware-as-a-service (RaaS). In addition, generative AI tools can help threat actors, with little or no coding experience, write functional ransomware. This publication provides tips to help your organization prepare for and recover from ransomware.

How ransomware infects devices

Ransomware can infect devices through malicious links or attachments found on unsecure websites, phishing emails and social media applications. Threat actors often scout your networks for information they can exfiltrate and monitor your communication methods prior to deploying the ransomware.

If your device is infected with ransomware, you will receive a ransom notice on your screen indicating your files have been encrypted and are inaccessible until the ransom is paid. Threat actors will often threaten to permanently destroy or leak your data publicly if you do not pay the ransom in the time limit requested. They'll often request payment in the form of digital currency, like bitcoin since the transfer would be difficult to trace. They may also request prepaid credit cards or gift cards.



Prepare your organization

Review the following steps to help prepare your organization to stay ahead of ransomware attacks.

Plan ahead

Develop an incident response plan to address how your organization will monitor, detect, and respond to an incident. Your plan should also include backup, recovery, and communications plans. Your incident response plan should designate roles for your employees and provide them with detailed instructions in the event of an incident. Your plan should be available offline, in the event your systems are unavailable.

- Developing your incident response plan (ITSAP.40.003)
- Tips for backing up your information (ITSAP.40.002)
- Developing your IT recovery plan (ITSAP.40.004)

Prepare for recovery

Your organization should have a recovery plan in place. In conjunction with your incident response plan, you should test your recovery plan by conducting simulations or walk-through exercises. The scenario should test the effectiveness of your response and highlight areas requiring improvement.

Provide security awareness training for employees

Provide employees with tailored cyber security and device management training to ensure they don't fall victim to malicious activities such as phishing emails and infected downloads.

- Offer tailored cyber security training to your employees (ITSAP.10.093)

Consider cyber insurance

Research cyber insurance providers and policy details to determine whether it would benefit your organization.

Communications Security Establishment Canada | Centre de la sécurité des télécommunications Canada

Canada

Cat. No. D97-1/00-099-2024E-PDF ISBN 978-0-660-70607-8

CANADIAN CENTRE FOR CYBER SECURITY

Protect your organization from ransomware attacks

Use the following guidance to protect your organization from ransomware attacks.

Enforce strong authentication methods

Activate phishing resistant multi-factor authentication as well as strong and unique passphrases or passwords on all devices and for every account. Consider using a password manager to create and store passphrases and passwords.

- Steps for effectively deploying multi-factor authentication (ITSAP.00.105)
- Best practices for passphrases and passwords (ITSAP.30.032)
- Password managers: Security tips (ITSAP.30.025)

Backup your data

Implement a backup plan for your organization. A backup is a copy of your data and systems that can be restored and provide you with access to your critical systems in the event of an incident. Backups should be done frequently to ensure your data is as close to real time as possible. Create many security barriers between your production systems and your backups and ensure your backups are encrypted and stored offline without connection to the Internet or local networks. Threat actors can infect your backups with ransomware if they are connected to your networks, which will hinder your efforts to recover. Testing your backup process is also crucial to a quick and effective recovery.

- Tips for backing up your information (ITSAP.40.002)
- Using encryption to keep your sensitive data secure (ITSAP.40.016)

Practice the principle of least privilege

Manage and monitor user accounts and access by applying the principle of least privilege. Provide employees with access to only the functions and privileges necessary to complete their tasks.

Implement a Zero Trust security model

Use a Zero Trust (ZT) security model to protect data and infrastructure from unauthorized access. ZT security models work on the principle of applying zero trust to all users, applications, and devices unless they have authentication and authorization. Authentication and authorization are re-assessed continuously and verified each time access is requested to a new resource.

- Zero Trust security model (ITSAP.10.008)

Restrict administrative privileges

Implement required confirmation for any actions that need elevated access rights and permissions and limit the number of users with administrative accounts and privileges. Ensure administrative functions are conducted from a dedicated administrative workstation. Consider implementing two-person integrity (TPI) or dual authentication to validate and verify sensitive administrative tasks.

- Managing and controlling administrative privileges (ITSAP.10.094)

Update and patch systems and devices

Check for updates and patches to repair known bugs and vulnerabilities in your software, firmware, and operating systems. Threat actors can exploit unpatched or unsupported systems and devices easily.

- How updates secure your device (ITSAP.10.096)

Deactivate macros

Ensure you deactivate macros as your default to reduce the risk of ransomware being spread through Microsoft Office attachments. Newer versions of Microsoft will deactivate macros from the Internet by default.

Segment Networks

Divide your network into several smaller components. This makes it more difficult for ransomware to spread across the entire network.

- Top 10 security actions: No.5 segment and separate information (ITSM.10.092)

Set up security tools

Install anti-malware and anti-virus software on your devices to detect malicious activity and secure your network with a firewall to protect connected devices. Consider installing Domain Name System (DNS) filtering on your mobile devices to block out malicious websites and filter harmful content. You can also implement Domain-based Message Authentication, Reporting and Conformance (DMARC), an email authentication and reporting system that helps to protect your organization's domains from spoofing, phishing, and other malicious activities. Ensure users access your network using your virtual private network (VPN).

- Protective Domain Name System (ITSAP.40.019)
- Implementation guidance: Email domain protection (ITSP.40.065 v1.1)
- Virtual private networks (ITSAP.80.101)

Seek professional cyber security assistance

Engaging with a cyber security professional early on may allow you to recover your systems and data more quickly than relying on your internal IT staff when facing a cyber incident.

Communications Security Establishment Canada | Centre de la sécurité des télécommunications Canada

Cat. No. D97-1/00-099-2024E-PDF ISBN 978-0-660-70607-8

Canada

CANADIAN CENTRE FOR CYBER SECURITY

How to recover from a ransomware attack

Consider the following steps to help remove and reduce the spread of ransomware.

1. **Isolate the device immediately**: Take your devices offline to stop the ransomware from spreading to other connected devices. Some strains of ransomware are designed to stay dormant on a device and quietly spread to other network-connected devices before encrypting the files. In these cases, you may not be able to stop the ransomware from spreading.
2. **Report the incident:** Report the ransomware attack to local law enforcement, the Canadian Anti-Fraud Centre and the Canadian Centre for Cyber Security. Communicate the incident to the employees who are listed in your incident response plan and give them clear direction as to their roles and responsibilities to help manage the incident.
3. **Change passwords**: Reset credentials including passwords on all systems, devices, and accounts. Threat actors often save this information for future attacks. Consider using passphrases on your devices as they are more secure and easier to remember.

4. **Identify the type of ransomware**: Use the information in the ransom note (such as listed URLs) and the new file extensions your encrypted files inherited, to research possible reoccurring attacks and identify the ransomware.
    - if you locate a decryption tool online, or law enforcement is able to provide you with one, proceed to the next step
    - if there is no decryption tool available online for your strain of ransomware, safely wipe your device and reinstall the operating system
5. **Remediate the point of entry:** Before connecting your systems and devices back toy our network or Internet, identify how the threat actor entered your network, systems or devices and apply security measures to prevent a repeat attack.

6. **Restore from your backup:** Analyze your backup files and ensure they are free of ransomware or any other malware. Store your backups offline to mitigate the chance of ransomware infecting your backup files. Once you are confident, restore your systems and devices from your secure backup.
7. **Update and patch:** Apply any available updates to your devices, hardware, and software. Patch your operating system and ensure all anti-virus, anti-malware, and firewall software is up to date.
8. **Review the incident and provide ongoing training**: Review the incident with your employees and provide ongoing training that addresses preventative actions against ransomware attacks, such as learning how to identify suspicious emails and attachments. Use common threat examples and past occurrences to keep up to date and prepared for the future.

Risks of paying the ransom

The decision to pay a cyber threat actor to release your files or devices is difficult and you may feel pressured to give in to the demands of the threat actor. Before you pay, contact your local police department and report the cybercrime. Paying the ransom is not usually advised, due to the following:

- it will not guarantee you access to your files.as threat actors may demand more money despite receiving the first ransom payment
- it encourages threat actors to continue infecting your devices or those of other organizations with ransomware as they assume you will continue to pay with each attack
- threat actors can use wiper malware that masquerades as ransomware to alter or permanently delete your files once the ransom is paid, making them unrecoverable
- your data has likely been copied and the threat actor can leak it for profit or use it to continue to extort you
- your payment may be used to support other ransomware attacks or terrorist organizations

Learn more

Consult the following guidance to learn more about the key points we have identified:

- Ransomware playbook (ITSM.00.099)
- Cyber Security Considerations for Consumers of Managed Services (ITSM.50.030)
- Have You Been Hacked? (ITSAP.00.015)
- Preventative Security Tools (ITSAP.00.058)
- Spotting Malicious Email Messages (ITSAP.00.100)

Communications Security Establishment Canada | Centre de la sécurité des télécommunications Canada

Canada

Cat. No. D97-1/00-099-2024E-PDF ISBN 978-0-660-70607-8