CANADIAN CENTRE FOR
CYBER SECURITY

UNCLASSIFIED

HOW TO PREVENT AND RECOVER FROM RANSOMWARE

SEPTEMBER 2021 | ITSAP.00.099

WHAT IS RANSOMWARE?

Ransomware is a type of malware that ultimately denies a user's access to files or systems until a sum of money is paid. Ransomware can use your network to spread to all connected devices. There are two prominent types of ransomware:

- **Crypto ransomware** removes access to your files by replacing them with encrypted data.
- **Locker ransomware** blocks the login access on your device.

Devices are often infected with ransomware by clicking on links or downloading attachments placed in 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 destroy your data permanently, or release your data publicly, if you do not pay the ransom in the time limit requested. Payment is often requested in the form of digital currency, like bitcoin, since the transfer would be difficult to trace. Prepaid credit cards or gift cards may also be requested.

HOW CAN I PREPARE MY ORGANIZATION?

There are several ways you can minimize your risk and prepare your organization if a ransomware attack occurs.

Plan ahead. Develop an incident response plan to address how your organization will monitor, detect and respond to an incident, such as a ransomware attack. Your plan should also include a backup, recovery, and communication plan. Your incident response plan should designate roles for your employees and provide them with detailed instructions in the event of an incident.

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.

Practice recovering. Test your incident response and recovery plan by conducting simulations or walk-through exercises. The scenario should test the effectiveness of your response and highlight areas requiring improvement.

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

HOW CAN I PROTECT MY ORGANIZATION?

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 occur 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 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.

Practice the principle of least privilege. Manage and monitor user accounts and access by applying the principle of least privilege, which advises on providing employees with access to only those functions and privileges necessary to complete their tasks. Restrict administrative privileges and require confirmation for any actions that need elevated access rights and permissions.

Update and patch systems. 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.

Disable macros. Ensure you disable macros as your default to reduce the risk of ransomware being spread through Microsoft Office attachments.

Segment Networks. Divide your network into several smaller components, which makes it more difficult for ransomware to spread across the entire network.

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.

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

Communications Security Establishment | Centre de la sécurité des télécommunications

Canada

Cat. No. D97-1/00-099-2021E-PDF ISBN 978-0-660-40187-4

HOW DO I RECOVER FROM AN 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. **Identify the type of ransomware**. Use the information in the ransom note (e.g. 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, proceed to Step 3.
3. **Remove the ransomware.** Use the online decryption tool to remove the ransomware from your devices, which should decrypt your files and make them accessible.
4. **Reset the device and wipe all the data**. If there is no decryption tool available online for your strain of ransomware, safely wipe your device and reinstall the operating system.
5. **Restore from your backup.** Analyze your backup files and ensure they are free of the ransomware or any other malware. Store your backups offline to mitigate the chance of the ransomware infecting your backup files. Once you are confident, restore your systems and devices from your secure backup.
6. **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 are up to date.
7. **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.
8. **Provide training**. Train users on cyber security to help reduce the risk of future attacks. Training should address 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.

SHOULD I REPORT IT?

Although it may not feel essential in the moment, reporting the ransomware incident to law enforcement, the Canadian Centre for Cyber Centre and the Canadian Anti-Fraud Centre is important. If you are the first to be targeted by this strain of ransomware, then law enforcement will be aware and can monitor for subsequent occurrences. These organizations can also help your mitigation and recovery efforts.

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:

- The ransom will not guarantee access to your files. 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. In this case, your files are not recoverable as the malware alters or permanently deletes them once the ransom is paid.
- Your data has likely been copied and can be leaked by the threat actor for profit. They may also continue to extort you with the copied data.
- Your payment may be used to support other ransomware attacks or terrorist organizations.

LEARN MORE

If you want to learn more about some of the key points identified, check out the following publications on our website (cyber.gc.ca).

- *Implementation Guidance: Email Domain Protection*
- *Cyber Security Considerations for Consumers of Managed Services (ITSM.50.030)*
- *Developing Your IT Recovery Plan (ITSAP.40.004)*
- *Have You Been Hacked? (ITSAP.00.015)*
- *Preventative Security Tools (ITSAP.00.058)*
- *Tips for Backing up Your Information (ITSAP.40.002)*
- *Offer Tailored Cyber Security Training to Your Employees (ITSAP.10.093)*
- *Spotting Malicious Email Messages (ITSAP.00.100)*