Security Tip (ST19-001)

Protecting Against Ransomware

Original release date: April 11, 2019

What is ransomware?

Ransomware is a type of malware threat actors use to infect computers and encrypt computer files until a ransom is paid. (See Protecting Against Malicious Code for more information on malware.) After the initial infection, ransomware will attempt to spread to connected systems, including shared storage drives and other accessible computers.

If the threat actor's ransom demands are not met (i.e., if the victim does not pay the ransom), the files or encrypted data will usually remain encrypted and unavailable to the victim. Even after a ransom has been paid to unlock encrypted files, threat actors will sometimes demand additional payments, delete a victim's data, refuse to decrypt the data, or decline to provide a working decryption key to restore the victim's access. The Federal Government does not support paying ransomware demands. (See the FBI's ransomware article.)

How does ransomware work?

Ransomware identifies the drives on an infected system and begins to encrypt the files within each drive. Ransomware generally adds an extension to the encrypted files, such as .aaa, .micro, .encrypted, .ttt, .xyz, .zzz, .locky, .crypt, .cryptolocker, .vault, or .petya, to show that the files have been encrypted—the file extension used is unique to the ransomware type.

Once the ransomware has completed file encryption, it creates and displays a file or files containing instructions on how the victim can pay the ransom. If the victim pays the ransom, the threat actor may provide a cryptographic key that the victim can use to unlock the files, making them accessible.

How is ransomware delivered?

Ransomware is commonly delivered through phishing emails or via "drive-by downloads." Phishing emails often appear as though they have been sent from a legitimate organization or someone known to the victim and entice the user to click on a malicious link or open a malicious attachment. A "drive-by download" is a program that is automatically downloaded from the internet without the user's consent or often without their knowledge. It is possible the malicious code may run after download, without user interaction. After the malicious code has been run, the computer becomes infected with ransomware.

What can I do to protect my data and networks?

- **Back up your computer.** Perform frequent backups of your system and other important files, and verify your backups regularly. If your computer becomes infected with ransomware, you can restore your system to its previous state using your backups.
- **Store your backups separately.** Best practice is to store your backups on a separate device that cannot be accessed from a network, such as on an external hard drive. Once the backup is completed, make sure to disconnect the external hard drive, or separate device from the network or computer. (See the Software Engineering Institute's page on Ransomware).
- **Train your organization.** Organizations should ensure that they provide cybersecurity awareness training to their personnel. Ideally, organizations will have regular, mandatory cybersecurity awareness training sessions to ensure their personnel are informed about current cybersecurity threats and threat actor techniques. To improve workforce awareness, organizations can test their personnel with phishing assessments that simulate real-world phishing emails.

What can I do to prevent ransomware infections?

- **Update and patch your computer.** Ensure your applications and operating systems (OSs) have been updated with the latest patches. Vulnerable applications and OSs are the target of most ransomware attacks. (See Understanding Patches and Software Updates.)
- **Use caution with links and when entering website addresses.** Be careful when clicking directly on links in emails, even if the sender appears to be someone you know. Attempt to independently verify website addresses (e.g., contact your organization's helpdesk, search the internet for the sender organization's website or the topic mentioned in the email). Pay attention to the website addresses you click on, as well as those you enter yourself. Malicious website addresses often appear almost identical to legitimate sites, often using a slight variation in spelling or a different domain (e.g., .com instead of .net). (See Using Caution with Email Attachments.)
- **Open email attachments with caution.** Be wary of opening email attachments, even from senders you think you know, particularly when attachments are compressed files or ZIP files.
- **Keep your personal information safe.** Check a website's security to ensure the information you submit is encrypted before you provide it. (See Protecting Your Privacy.)
- **Verify email senders.** If you are unsure whether or not an email is legitimate, try to verify the email's legitimacy by contacting the sender directly. Do not click on any links in the email. If possible, use a previous (legitimate) email to ensure the contact information you have for the sender is authentic before you contact them.
- **Inform yourself.** Keep yourself informed about recent cybersecurity threats and up to date on ransomware techniques. You can find information about known phishing attacks on the Anti-Phishing Working Group website. You may also want to sign up for CISA product notifications, which will alert you when a new Alert, Analysis Report, Bulletin, Current Activity, or Tip has been published.
- **Use and maintain preventative software programs.** Install antivirus software, firewalls, and email filters—and keep them updated—to reduce malicious network traffic. (See Understanding Firewalls for Home and Small Office Use.)

How do I respond to a ransomware infection?

- **Isolate the infected system.** Remove the infected system from all networks, and disable the computer's wireless, Bluetooth, and any other potential networking capabilities. Ensure all shared and networked drives are disconnected whether wired or wireless.
- **Turn off other computers and devices.** Power-off and segregate (i.e., remove from the network) the infected computer(s). Power-off and segregate any other computers or devices that shared a network with the infected computer(s) that have not been fully encrypted by ransomware. If possible, collect and secure all infected and potentially infected computers and devices in a central location, making sure to clearly label any computers that have been encrypted. Powering-off and segregating infected computers and computers that have not been fully encrypted may allow for the recovery of partially encrypted files by specialists. (See Before You Connect a New Computer to the Internet for tips on how to make a computer more secure before you reconnect it to a network.)
- **Secure your backups.** Ensure that your backup data is offline and secure. If possible, scan your backup data with an antivirus program to check that it is free of malware.

What do I do if my computer is infected with ransomware?

- **Home users:** immediately contact your local FBI office or local U.S. Secret Service office to request assistance.
- **Organizations:** immediately report ransomware incidents to your IT helpdesk or security office.
- **All users:** change all system passwords once the ransomware has been removed. You can submit ransomware files to CISA for analysis via https://www.malware.us-cert.gov/MalwareSubmission/pages/submission.jsf. (See Choosing and Protecting and Passwords and Supplementing Passwords.)

References

- CISA Ransomware page
- CISA Malware Analysis Submission page
- CISA Mailing Lists and Feeds page
- Protecting Against Malicious Code
- Protecting Your Privacy
- Understanding Firewalls for Home and Small Office Use
- Understanding Patches and Software Updates
- Using Caution with Email Attachments
- Handling Destructive Malware
- Choosing and Protecting Passwords
- Supplementing Passwords
- Anti-Phishing Working Group's website
- Carnegie Mellon Software Engineering Institute blog post: Ransomware: Best Practices for Prevention and Response

- FBI article: Incidents of Ransomware on the Rise
- FBI Tech Tuesday: Building a Digital Defense Against Ransomware at Home

Author
CISA