THE NATIONAL CYBERSECURITY SOCIETY

RANSOMWARE

Ransomware is a form of malicious software (or "malware") designed to prevent access to a system until a sum of money is paid, usually via virtual currency -- like Bitcoin.

There are two major types of ransomware: data kidnapping and lock-screen. In a **data kidnapping** attack, the ransomware encrypts its victim's files and/or data on systems and peripherals. The victim is notified that their files have been encrypted and a ransom is demanded to decrypt them. Recent variants (e.g., Locky, TeslaCrypt, Cerber) encrypt the victim's files, the content of those files, and the file names too – making the entire system unrecognizable. This type of heist can also take over a company's website.

In a **lock-screen** attack, the ransomware changes its victim's login credentials, effectively locking the user out of the system entirely. The ransomware displays a message stating the computer has been overtaken by law enforcement (or some other entity), often in relation to some sort of crime committed by the user. In many cases, the user's public IP address, Internet service provider, and geographic location are displayed, increasing the credibility of the attack. The message demands the victim pay a fine (ransom) or face criminal charges, additional fines, and/or imprisonment.

FACT 1: SYSTEM COMPROMISE

The most common sources of ransomware are 1) spam or phishing emails that contain malicious attachments, 2) website pop-up advertisements, and 3) infected systems in the network. When a victim manually clicks on a link in an email or on a pop-up ad, the victim is actually downloading software that infects their system. Some new ransomware versions are able to infect multiple systems on a network by spreading to other machines that are not kept up to date with the latest security patches.

Typical ransomware infection process:

1. User receives spammed message with attachment
2. Attachment is actually malware that connects to a website hosting the ransomware

DID YOU KNOW…

- ✓ The most common sources of ransomware are:
  - Spam or phishing emails with malicious attachments
  - Website pop-up ads
  - Infected systems
- ✓ If your system was compromised with ransomware, would you pay the bounty?
- ✓ Most ransom payments are through bitcoin
- ✓ Back up important data often to reduce overall vulnerability and mitigate potential impacts of a ransomware attack.
- ✓ Employee training is an essential prevention strategy to keep your systems safe

Still have questions, need help?
Contact us at our **"Ask-an-Expert"** service,
web@thencss.org or visit us at the link below.

© 2018 National Cybersecurity Society. All Rights Reserved.

JOIN THE NCSS

Become a member of **The National Cybersecurity Society** today and learn more about how to protect your business from a cyber attack.

RANSOMWARE continued….

3. Ransomware is downloaded onto the computer
4. Ransomware encrypts files on the affected computer
5. Ransom message is displayed with instructions
6. Victims must follow instructions and pay ransom with Bitcoins

FACT 2: WHEN YOU BECOME A VICTIM

If your system has been compromised, recovery options are dependent on a number of factors.

- Are there data backups available to restore the system?
- What is the criticality of the data that was compromised?
- What is the cost of the ransom compared to the cost of data recovery or data loss?
- Have you purchased cyber insurance and is coverage available?
- Has an interest group developed and published a fix to decrypt the files?

Unfortunately, once infected with ransomware, your system files are encrypted and inaccessible until either: (1) the ransom is paid and files are decrypted, (2) the system image and data are restored from a known backup, or (3) an interest group (such as law enforcement, security researchers, or a vendor) offers a fix that decrypts the files.

Depending on how well known or established the ransomware is that you're infected with, there may be a fix available. Try looking for information available on the Internet that references what your ransom is asking for and what the method of infection was (such as what the phishing email said) to determine if the version of ransomware is known in the market and if a fix exists. If there is no fix available, the remaining options are to pay the ransom or restore the system to a known backup (if available).

It is important to note that paying the ransom, while not ideal, may be the only option if backups are not available and a fix has not been identified in the market. It is also important to note that paying the ransom is no guarantee that data will be recovered. While it is in the best interest of criminals to ensure that data is recoverable, sometimes it is not. Ransomware does not come with a warranty or any kind of service-level agreement. Technical failures may occur that prevent successful recovery, and criminals will not provide a money-back guarantee if data decryption fails. Paying a ransom may make an organization the target of future attacks; therefore, paying a ransom should be considered only as a last resort and should be undertaken only after all other recovery options have been exhausted. Additionally, reasonable measures should be taken to ensure the organization does not immediately become subject to additional criminal activity subsequent to ransom payment.

Still have questions, need help?
Contact us at our "**Ask-an-Expert**" service,
web@thencss.org or visit us at the link below.

© 2018 National Cybersecurity Society. All Rights Reserved.

JOIN THE NCSS | Become a member of **The National Cybersecurity Society** today and learn more about how to protect your business from a cyber attack.

WWW.NATIONALCYBERSECURITYSOCIETY.ORG

RANSOMWARE continued….

FACT 3: PREVENTION MEASURES

1. Back up important data often to reduce overall vulnerability and mitigate potential impacts of a ransomware attack.

    - Use a backup provider to periodically backup your data either to tape, disk, or virtual environment (e.g. a cloud backup service)
    - If you handle your own backups, ensure that backup data is stored on a device that is not connected to the internet

2. Don't click suspicious looking links in email or web ads!

    - Don't open emails from senders you don't recognize
    - Be careful with emails from known senders that appear to be different from the emails you usually receive from that person
    - Avoid clicking on links from websites whenever possible
    - Use a pop-up blocker to reduce exposure to potentially malicious ads

3. Ensure that your employees are knowledgeable about the risks of ransomware

    - Provide training to your employees on the risks of ransomware and email/website scams in general
    - Test your employees resiliency by conducting simulated phishing emails – such as provided by https://cofense.com/free - a free tool

4. Control user and system access to critical business functions and data

    - Segregate data and access as much as possible - for example, sensitive data should only be accessible by employees who really need it for their job
    - Know where your most sensitive data resides on your systems and minimize the number of places that it is available
    - Establish a list of allowed applications (aka “whitelist”) that users can install, and require administrator privileges to install anything not on the whitelist
    - Make sure anti-virus software is installed on all machines and that it remains up-to-date. You can do this by enabling auto-update within your anti-virus software.

Still have questions, need help?
Contact us at our "**Ask-an-Expert**" service,
web@thencss.org or visit us at the link below.

© 2018 National Cybersecurity Society. All Rights Reserved.

JOIN THE NCSS | Become a member of **The National Cybersecurity Society** today and learn more about how to protect your business from a cyber attack.

WWW.NATIONALCYBERSECURITYSOCIETY.ORG