UC SANTA BARBARA

UCSB Information Technology
Information Security
4101 SAASB
Santa Barbara, CA 93106-3020
security.ucsb.edu

Ransomware Attack Response Checklist

Step 1:

Disconnect everything

- ❑ Unplug the computer from the network via the Ethernet cable
- ❑ Turn off any wireless functionality: Wi-Fi, Bluetooth, NFC
- ❑ Disconnect all external storage: memory sticks, attached phones/cameras, external hard drives, USB drives
- ❑ Do not turn the computer off. The message on the screen may be required to determine the ransomware type
- ❑ If you have not already done so, report the incident to the IT Services Desk at (805) 893-5000

Step 2:

Determine the scope of the infection and check the following for Signs of Encryption from a known good, uninfected computer

- ❑ Mapped or shared drives
- ❑ Mapped or shared folders from other computers
- ❑ Network storage devices of any kind
- ❑ External Hard Drives
- ❑ USB storage devices of any kind (USB sticks, memory sticks, attached phones/cameras)
- ❑ Cloud-based storage: DropBox, Google Drive, OneDrive etc.

Step 3:

Remove user's access to data

- ❑ Remove permissions to folders/files of the user that initiated the infection until the source is identified. It should be decided if permissions to all folders/files are removed

or just the location where the infection took place. This is to prevent reinfection of the same location or multiple locations.

Step 4:

Determine the ransomware strain

- ❏ What strain or type of ransomware? E.g., CryptoWall, Teslacrypt, etc.
  - ❏ Bit Defender Ransomware Recognition Tool
  - ❏ ID Ransomware Malware Hunter Team
- ❏ Look for available decryptors
  - ❏ Bit Defender Ransomware Recognition Tool
  - ❏ No More Ransom Decryption Tools

Step 5:

Determine response

Now that you know the scope of your encrypted files and the ransomware strain you're dealing with, you can make a more informed decision about next steps.

Response 1: Restore Your Files From Backup

- It is very important to determine the last known good backup in which files/folders are not infected and apply that backup to restore.

- Make sure as in Step 3, the user that initiated the infection has not logged back into the network from any computer after the ransomware event. It would be prudent to disable the user's account until data is restored and an infection source has been identified. Permissions to the data for that user will be returned after the restore completes.

- After the restore, initiate an immediate backup of the files/folders(or complete file system.

- ❏ Locate your backups
  - ❏ Ensure all the files you need are there
  - ❏ Verify backups' integrity (e.g., media not reading or corrupted files)
  - ❏ Check for Shadow Copies if possible (may not be an option on new ransomware)
  - ❏ Check for any previous versions of files that may be stored in the cloud (e.g., Box, DropBox, Google Drive, OneDrive)

- ❏ A good practice: Back up the encrypted files in case a decryptor becomes available
- ❏ Rebuild the system from known good sources. Do not trust antivirus programs to completely remove all malware from a system. Install all patches to avoid reinfection from network-transmitted malware
- ❏ Restore your files from backups
- ❏ All credentials stored anywhere on the local network (including those saved inside Web browsers and password managers) could be compromised and need to be changed
- ❏ Many ransomware cases are the result of phishing. Look for phishing messages and corrupt downloads and permanently delete to avoid reinfection

Response 2: Try to Decrypt

- ❏ If you determined the ransomware's strain and version, see if there is a decryptor available
- ❏ A good practice: back up the encrypted files in case the decryptor doesn't work
- ❏ Attach any storage media that contains encrypted files (hard drives, USB sticks, etc.)
- ❏ Decrypt files
- ❏ Back up the newly decrypted files for reloading
- ❏ Rebuild the system from known good sources. Do not trust antivirus programs to completely remove all malware from a system. Install all patches to avoid reinfection from network-transmitted malware
- ❏ Restore your files from backups
- ❏ All credentials stored anywhere on the local network (including those saved inside Web browsers and password managers) could be compromised and need to be changed
- ❏ Many ransomware cases are the result of phishing. Look for phishing messages and corrupt downloads and permanently delete to avoid reinfection

Response 3: Do Nothing and Lose Files

- ❏ Back up the encrypted files in case a decryptor becomes available
- ❏ Rebuild the system from known good sources. Do not trust antivirus programs to completely remove all malware from a system. Install all patches to avoid reinfection from network-transmitted malware
- ❏ Restore your files from backups
- ❏ All credentials stored anywhere on the local network (including those saved inside Web browsers and password managers) could be compromised and need to be changed

- ❏ Many ransomware cases are the result of phishing. Look for phishing messages and corrupt downloads and permanently delete to avoid reinfection

Response 4: Negotiate and/or Pay the Ransom

- This is *not recommended*. If you consider this option, it is imperative to consult with the UCSB Chief Information Security Officer (CISO) for proper guidance. After consultation, if you choose to proceed, follow these steps:
  - ❏ Back up the encrypted files in case the decryptor provided by the criminals doesn't work
  - ❏ Decrypt files as instructed
  - ❏ Back up all the files
  - ❏ Rebuild the system from known good sources. Do not trust antivirus programs to completely remove all malware from a system. Install all patches to avoid reinfection from network-transmitted malware
  - ❏ Restore your files from backups
  - ❏ All credentials stored anywhere on the local network (including those saved inside Web browsers and password managers) could be compromised and need to be changed
  - ❏ Many ransomware cases are the result of phishing. Look for phishing messages and corrupt downloads and permanently delete to avoid reinfection

Step 6:

Report the incident

- ❏ Resolve the previously reported ransomware incident by completing the Security Mediation Survey at the IT Services Catalog