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
- ❏ Report the ransomware incident by completing the Google Form at https://docs.google.com/forms/d/e/1FAIpQLSdz5Pvxh2acLR4_Zpq7OHeIa2WKFLsrNqjTefJMNxJbXAWVwA/viewform?usp=sf_link

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: Determine the ransomware strain

- ❏ What strain or type of ransomware? For example: CryptoWall, Teslacrypt, etc.
  - ❏ https://labs.bitdefender.com/2017/09/bitdefender-ransomware-recognition-tool/
  - ❏ https://id-ransomware.malwarehunterteam.com/
- ❏ Look for available decryptors
  - ❏ https://labs.bitdefender.com/2017/09/bitdefender-ransomware-recognition-tool/
  - ❏ https://www.nomoreransom.org/
    - ❏ https://www.nomoreransom.org/en/decryption-tools.html

.

STEP 4: Determine Response

Now that you know the scope of your encrypted files and the ransomware strain you are dealing with, you can make a more informed decision about what to do next.

Response 1: Restore Your Files From Backup

- ❑ Locate your backups
  - ❑ Ensure all the files you need are there
  - ❑ Verify integrity of backups (i.e., media not reading or corrupted files)
  - ❑ Check for Shadow Copies if possible (may not be an option on newer ransomware)
  - ❑ Check for any previous versions of files that may be stored on cloud storage, e.g., DropBox, Google Drive, OneDrive
- ❑ A good practice is to 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
- ❑ Report the ransomware incident by completing the Google Form at https://docs.google.com/forms/d/e/1FAIpQLSdz5Pvxh2acLR4_Zpq7OHeIa2WKFLsrNqjTefJMNxJbXAWVwA/viewform?usp=sf_link

Response 2: Try to Decrypt

- ❑ If you determined the strain and version of the ransomware, find out if there is a decryptor available
- ❑ A good practice is to back up the encrypted files in case the decryptor doesn't work

Continue steps...

- ❑ Attach any storage media that contains encrypted files (hard drives, USB sticks, etc.)
- ❑ Decrypt files

- ❏ Backup 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
- ❏ Many ransomware cases are the result of phishing. Look for phishing messages and corrupt downloads and permanently delete them to avoid reinfection
- ❏ 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
- ❏ Report the ransomware incident by completing the Google Form at https://docs.google.com/forms/d/e/1FAIpQLSdz5Pvxh2acLR4_Zpq7OHeIa2WKFLsrNqjTefJMNxJbXAWVwA/viewform?usp=sf_link

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
- ❏ Many ransomware cases are the result of phishing. Look for phishing messages and corrupt downloads and permanently delete them to avoid reinfection.
- ❏ 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.
- ❏ Report the ransomware incident by completing the Google Form at https://docs.google.com/forms/d/e/1FAIpQLSdz5Pvxh2acLR4_Zpq7OHeIa2WKFLsrNqjTefJMNxJbXAWVwA/viewform?usp=sf_link

Response 4: Negotiate and/or Pay the Ransom

- ❏ This is *not recommended* and if considering this option, **it is imperative to consult with the UCSB 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 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 your backup
❏ 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 them to avoid reinfection
❏ Report the ransomware incident by completing the Google Form at https://docs.google.com/forms/d/e/1FAIpQLSdz5Pvxh2acLR4_Zpq7OHeIa2WKFLsrNqjTefJMNxJbXAWVwA/viewform?usp=sf_link