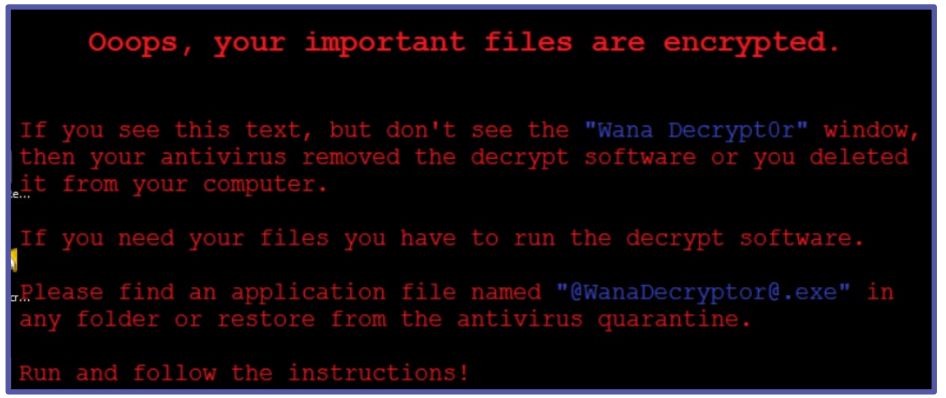
Cybersecurity

2.4.2 - Ransomware

CYBER.ORG
THE ACADEMIC INITIATIVE OF THE CYBER INNOVATION CENTER

Ransomware

- Malware that encrypts, or locks, a victim's access to files and/or the system and demands a ransom to regain access
- Often, the demand is met with an ultimatum of the ransom increasing and/or the data being deleted after a certain period.
- Attackers use ransomware to target data that is valuable
  - Personal data such as finances, photos, and documents
  - Corporate data such as company financials, proprietary or trade secrets, customer data



Types of Ransomware

- Cryptomalware encrypts files, folders, or hard drives but the operating system itself may still be available.
  - Cryptomalware can also mean ransomware that asks for cryptocurrency for payment.
- Lockers or locker-ransomware can lock a user out of their device completely, preventing them from accessing anything on the device.
- Scareware alerts a user of an issue and demands payment to fix it. This threat is often accompanied by pop-ups and other issues on the device
- Doxware, exortionware, or leakware threatens to release the stolen data if the ransom is not paid.
  - Often used against public officials and celebrities with threats to release private or sensitive information

To Pay or Not to Pay?

- Ransomware is profitable for malicious actors simply because so many people pay the ransom to recover their files, which may or may not be returned in either case.
- Preventing an attack from occurring or eliminating the need to pay for the return of the data is the best defense.
- This can be done with:
  - Training on potential threats
  - Backing up data, preferably offsite or cloud-based
  - Keeping systems and backups updated so there is little to no loss between the attack and recovery