

Ransomware. Game Over.

August 2, 2023

Ransomware is a type of malware attack (harmful software) that converts (encrypts) a victim's data to code and prevents access until a ransom payment is made. Ransomware attackers often use techniques, such as phishing, to gain access to a victim or company's files and data.

Rise of Ransomware Attacks

As technology evolves, ransomware attacks are growing among businesses and consumers. In 2022, the United States (U.S.) saw the highest number of ransomware attacks. The U.S. came in first with 217,486,516 attacks. In comparison, the United Kingdom was second with 71,350,221 attacks (2023 SonicWall Cyber Threat Report).

Over the last few years, colleges and universities are increasingly being targeted. These attacks take down key systems, close schools for days, and prevent faculty/staff from accessing lesson plans and student data.

As digital citizens (anyone who uses computers, the internet, and digital devices), it is important to be aware and vigilant about basic, best practices in an increasingly connected world.

Most Common Types of Attacks

Crypto Ransomware or Encryptors

Encryptors is the most well-known and damaging attack. Files and data are encrypted within a system, making the content inaccessible without a decryption key.

Lockers

Lockers completely lock you out of your system making files and applications inaccessible. A lock screen displays the ransom demand, possibly with a countdown clock, to increase urgency and drive victims to act.

Scareware

Scareware is fake software which claims to have detected a virus, or other issue, on your computer and directs you to pay to resolve the problem. Some types of scareware lock the computer, while others simply flood the screen with pop-up alerts, without actually damaging files.

Doxware or Leakware

Leakware threatens to distribute sensitive, personal, or company information online. Many victim's panic and pay the ransom to prevent private data from falling into the wrong hands or entering the public domain.

One form of attack is police-themed ransomware. The attacker claims to be law enforcement and warns illegal online activity has been detected. To avoid jail time, you may pay a fine.

Ransomware as a Service (Raas)

Raas refers to malware hosted anonymously by a "professional" hacker. They handle all aspects of the attack: distributing ransomware, collecting payments, and restoring access. In return, they receive a portion of the payment.

Major Keys to Ransomware Protection

Back-Up your Files

Ransomware will look for files to encrypt or delete. Ensure all files are backed up to a secondary location such as a secure, cloud storage service or another storage media. This protection can make files inaccessible to edits or deletion by cybercriminals.

Only Use Secure Networks

Cybercriminals look for individuals connected to unsecured Wi-Fi networks to track their internet usage. Using a verified and secure network will help add a layer of protection.

Keep Security Software Up-to-Date

Outdated security software is an easy target for cybercriminals trying to infiltrate systems. Software updates are recommended to protect against new cyber threats.

Never Pay Ransom!

Cybercriminals are always trying to deceive and take advantage of individuals. If you suspect you have fallen victim to a ransomware attack, make sure to disconnect any devices from your network and contact our IT team immediately.

Remember: Stop. Think. Connect.

Revision #1

Created 6 February 2025 21:50:25 by Laura J. Crapps

Updated 26 February 2025 03:35:37 by Laura J. Crapps