Ransomware Survival Guide

Quick Survival Guide about Crypto-Ransomware

Quick Description

- A crypto-ransomware attack uses covertly installed malware to encrypt a victim's files and then demands a ransom payment in return for the decryption key required to recover the encrypted files.
- The first known ransomware was written in 1989. By 2013, the use of ransomware had become well established around the world.

Steps in the Attack

- The attacker generates a key pair and places the public key in a piece of malware.
- When the malware is released on a computer, it generates a random symmetric key and encrypts the victim's data with it. It uses the public key in the malware to encrypt the symmetric key.
- The malware displays a message to the victim with instructions about how to pay the ransom.
- When the victim sends the e-payment, the attacker deciphers the asymmetric ciphertext using the private key from the key pair, and sends the symmetric key to the victim, who uses it to decipher the encrypted files.

How to Spot a Ransomware Attack

- Monitor your file servers for the modification of massive numbers of files to unknown file extensions within a short period of time.
- Beware of system notifications asking you for money to decrypt your files. Some may be fake demands that have not encrypted any files. And be aware that even actual ransomware attacks do not encrypt all of your files.

How to Protect IT Infrastructure

- **Make regular backups of all your sensitive data and systems and store them offline.**
- Train your employees not to fall for phishing attacks, and don't give them admin rights on their workstations.
- Always keep your antivirus databases and software updated.
- Block known ransomware extensions via FSRM. If ransomware cannot create files with those extensions on your file server, it cannot encrypt your files.
- Make the most of Group Policy:
  - Set up Group Policy to show up hidden file extensions on all workstations so users can see the double file extensions (such as filename.doc.exe) that attackers use to disguise malware.
  - Configure the Application Control policy to blacklist everything and whitelist only needed software.
  - Configure the Software Restriction policy so that users can execute only authorized extensions.
  - Use Group Policy to disable AutoPlay and Autorun on all workstations.
- Either disable file execution in e-mail attachments, or quarantine all attachments using your spam filter.
- Configure your firewall to whitelist only the specific ports and hosts you need.
- Segregate your network into different zones with unique access to each.
- Minimize the risk of BYOD by creating a guest network for new or unknown equipment.
- Limit user access to shared drives by assigning NTFS permissions via security groups. Since ransomware can encrypt only the files the victim has access to, a strict least privilege model limits the damage it can do.
- Monitor your file servers for spikes in file modification activity.
- Maintain a complete and current inventory of all your equipment and its network addresses so you can quickly find the source of a ransomware attack and take it offline immediately.

Responding to a Ransomware Attack

- Since ransomware cannot encrypt all files within seconds, you may have time to trace its source. When you find the source workstation, take it offline immediately.
- Check the name of the ransomware. It may be old malware that has already been cracked by the IT community.
- Don't pay the attackers. Even if you get back your data, they will keep attacking you and forcing you to pay repeatedly.

Gain #completevisibility into effective permissions and anomalous user behavior with Netwrix Auditor for Windows File Servers: netwrix.com/go/trial-fs

Corporate Headquarters:
300 Center Drive, Suite 1100, Irvine, CA 92618

Phone: 1-949-407-5125
Toll-free: 888-638-9749

Int'l: 1-949-407-5125
EMEA: 44 (0) 203-318-0261

netwrix.com/social