Anatomy of a Crypto-Ransomware Attack

Crypto-Ransomware is used by cybercriminals to scramble an organisation's data with a 'key' so it is no longer readable. This type of ransomware affects servers, mobile devices and any additional storage device that is attached to the infected machine - such as USB sticks, SD cards and external hard drives.

5 Stages of Crypto-Ransomware

Installation

After a victim's computer is infected, the crypto-ransomware installs itself, and sets itself to start automatically every time your computer boots up.

Contacting Headquarters

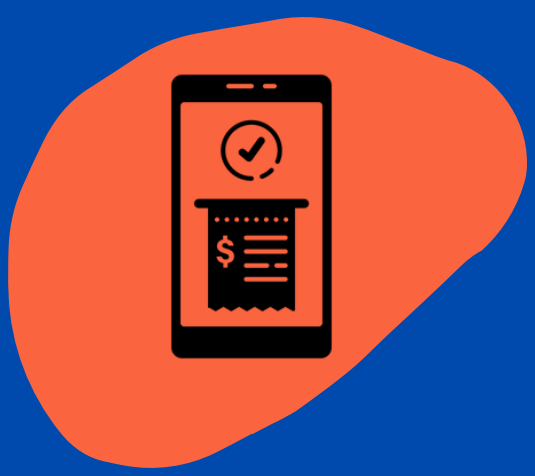
Before crypto-ransomware can attack you, it contacts a server operated by the criminal gang that owns it.

Handshake & Keys

The ransomware client and server identify each other through a carefully arranged "handshake," and the server generates two cryptographic keys. One key is kept on your computer, the second key is stored securely on the criminals' server.

Encryption

With the cryptographic keys established, the ransomware on your computer starts encrypting every file it finds with any of dozens of common file extensions, from Microsoft Office documents to .JPG images and more.



Extortion

The ransomware displays a screen giving you a time limit to pay up before the criminals destroy the key to decrypt your files. They will usually ask for payment in Bitcoin or other electronic payments.

Staying Safe

RESTRICT WRITE PERMISSIONS
On servers as much as possible

USE ADVANCED ENDPOINT PROTECTION that can identify new malware variants and detect malicious traffic

USE WEB AND EMAIL PROTECTION to block access to malicious websites and scan all downloads

EDUCATE USERS to contact IT if they encounter suspicious pop-ups

SET UP REGULAR OFFSITE BACKUPS and test backups to ensure they can be restored from reliably

DISCONNECT FROM NETWORKS IMMEDIATELY if you suspect infection

Learn more at www.eastmidlandscybersecure.co.uk

EAST MIDLANDS CYBER SECURE