

Anatomy of a Crypto-Ransomware Attack

New variants of ransomware known as CryptoLocker, CryptoDefense and CryptoWall are spreading via spam emails, drive-by downloads, or by malware already on your computer. Once you're infected, crypto-ransomware hijacks all your files, locks them up with unbreakable encryption, and demands a ransom of \$300-\$500 in bitcoins to unscramble them.

5 STAGES OF CRYPTO-RANSOMWARE

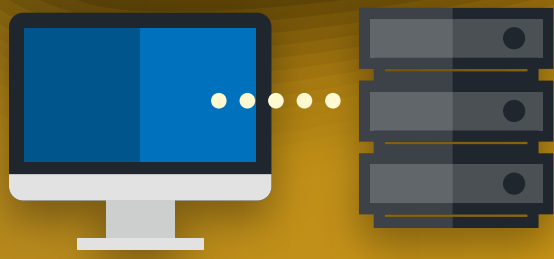
1 INSTALLATION

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



CONTACTING HEADQUARTERS 2

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



3 HANDSHAKE AND 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 4

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.



5 EXTORTION

The ransomware displays a screen giving you a time limit to pay up before the criminals destroy the key to decrypt your files. The typical price, \$300 to \$500, must be paid in untraceable bitcoins or other electronic payments.



STAYING SAFE



RESTRICT WRITE PERMISSIONS on file 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



MAKE TIME FOR REGULAR OFFLINE BACKUPS; test backups to ensure they can be restored from reliably



DISCONNECT FROM NETWORKS IMMEDIATELY if you suspect infection

NEXT-GENERATION ENDUSER PROTECTION

Sophos Next-Generation Enduser Protection detects and blocks malicious files and web traffic used by crypto-ransomware.