

RANSOMWARE 101

WHAT, HOW, & WHY



WHAT IS IT?

Ransomware is a serious security threat that has **data-kidnapping** capabilities. It limits access to files or system functions, or even render systems totally useless. Then it forces victims to **pay ransom** to regain access to their files/systems.

HOW DO YOU GET INFECTED?

You can be infected when you unknowingly download ransomware from



Compromised websites

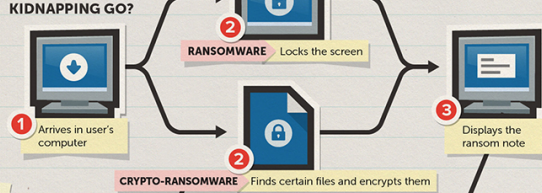


Spammed emails



Other malware

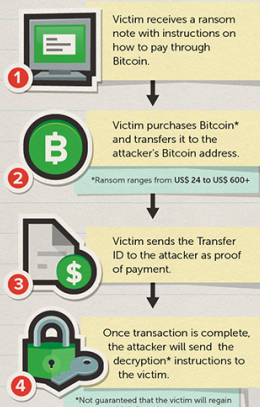
HOW DOES DATA KIDNAPPING GO?



HOW DOES THE FILE ENCRYPTION WORK?



HOW IS THE RANSOM PAID?



*Not guaranteed that the victim will regain access to his infected system.

WHY IS IT A SECURITY THREAT?

Ransomware is no longer just a scareware. From when it was first sighted, it has gone a long way from just issuing empty threats. It is now known for its sophisticated **file-encrypting ability**.



2006
A ransomware variant seen in Russia that **zipped files** and left password-protected zip files in the victim's system.



2011
An SMS ransomware threat emerged, asking victims to pay up by dialing a **premium SMS number**.



2012
A slew of ransomware spread across Europe, U.S., and Canada that **impersonated victims' local police agency** instead of leaving a typical ransom note.



2013
CryptoLocker, a new type of ransomware, surfaced. It has the ability to encrypt files aside from locking systems.



2014
15,000 of the **48,000** ransomware detections were flagged as **crypto-ransomware**, a 27% increase since it was discovered.

HOW CAN YOU PROTECT YOURSELF?

An antidote to a ransomware infection has yet to be discovered. However, one can certainly avoid falling victim to it with the following practices:



BACK UP REGULARLY

Practice the **3-2-1 rule**: Three backup copies of your data on two different media, and one of those copies in a secured separate location.



BOOKMARK WEBSITES

Bookmarking frequently visited and trusted websites will prevent you from typing in the wrong address.



VERIFY EMAIL SOURCES

Check the sender's email address against your contacts before opening any link or downloading anything from your email.



UPDATE YOUR SECURITY SOFTWARE

An up-to-date security software adds an extra layer of protection. Update it regularly so it can protect you against the latest ransomware variants.