Overview

Ransomware is a type of malware that infects a user’s computer then encrypts certain files on that machine. Once the files are encrypted the user is prompted to pay to have them unencrypted. In many cases the user is accused of conducting illegal activities and the ransomware claims to be an entity of the law. When ransomware behaves this way, it may be referred to as scareware.

Variations

Lock Screen Ransomware – Ransomware that runs a program on the infected system which displays a full screen image or webpage and does not allow the user to access anything else on the computer until a fee has been paid. This type of ransomware will often claim to be an authoritative agency such as FBI, police departments, or copy right agencies.

Encrypting Ransomware – Ransomware which encrypts only certain files. The infected user only notices the issue when attempting to open those files. This type of ransomware will often claim to have placed child pornography or other illegal content within the encrypted files and threaten to alert the authorities if the ransom is not paid.

Non-Encrypting Ransomware - Ransomware which displays various pop-ups (often pornographic) and additional pop-ups would occur prompting the infected user to pay a fine to stop the pop-ups from occurring.

Removal

Scan for and Delete the Ransomware. The user should start by removing any mobile media from his/her computer (CD’s, USB drives, and external hard drives). To locate ransomware, the user should boot his/her computer into Safe Mode with Networking by restarting their computer and pressing the key for boot options at the startup (usually F12) then selecting “Boot to Safe Mode with Networking” (Some ransomware will use rootkits to edit the registry and disable the Safe Boot feature). The user must then scan his/her computer with an anti-malware program.
System Restore

If scanning and deleting the ransomware does not work the user should do a system restore to reload the system to a recent backup. He/she may do this by using the Windows System Restore Tool by booting into Safe Mode and typing `rstui.exe` (Microsoft’s System Restore program) into the command prompt, or by using a backup on an external hard drive. (It is highly recommended to maintain an up to date backup of all systems at all times on an external storage device.)

If all else fails, the user can reinstall their Operating System by inserting the Operating installation disk and running it. However, this method is last resort and should not be done unless it is absolutely necessary. A backup of only the files you need to keep should be made (pictures, music, videos, etc.) DO NOT backup system files as these are likely corrupted.