Ransomware Troubleshooting

Archived: 2026-04-06 15:29:12 UTC

Ransomware Directory

Ransomware encrypts your files and sends you a warning that your files will only be released if you pay a ransom. The ransom is usually a very hefty amount, and it increases if you don’t pay within a certain amount of time.

Ransomware: Holding Your Data Hostage for a Payment

Ransomware is a new form of malware that has a devastating effect on users who store important documents on their computer. This malware also looks for files that might not be business related, but they are still important to the user such as pictures. Ransomware encrypts your files and sends you a warning that your files will only be released if you pay a ransom. The ransom is usually a very hefty amount, and it doubles or triples if you don’t pay within a certain amount of time.

Ransomware Background

Ransomware is basically cyber extortion. This type of software hasn’t been around for very long, but it’s an extremely nasty form of malware. Some users never get their files back even after they pay the ransom. Files include anything from documents to images to AutoCAD drawings.

The most popular ransomware was distributed in 2013. Its name was CryptoLocker. CryptoLocker was spread through standard malware vectors such as email or packaged software masquerading as another application. It was

even cleverly disguised as a harmless attachment to email, which took advantage of Windows default behavior of showing an icon for the first extension in the file name without regarding the ending extension, which in this malware's case is EXE.

Once it runs on the computer, it searches for specific file types such as AutoCAD drawings, Microsoft Office documents, pictures, and OpenDocument documents. Once it found its target files, it encrypts the files using public key cryptography. A popup is then shown asking the user for a ransom, which was usually $400. If the user did not pay within a certain amount of hours, the ransom doubled.

Some users paid the ransom, and they were lucky enough to get their files back. Others reported that they were never given the key and were not able to recover files. ZDNet reported that the hackers were able to earn $27 million from CryptoLocker.

What Does Ransomware Do?

CryptoLocker is just one example of ransomware, although it's one of the most malicious. Ransomware can also limit access to the computer itself. When users boot their computers, they are presented with a window that tells them they must pay a ransom to access the machine. This is a step up from CryptoLocker, because users aren't able to access anything on their machines.

Users are again given a link to where they can pay for their files. While this doesn't seem as bad as encrypting files, users aren't able to access their machine at all, so they lose more in the end. Plus, they need to format their hard drive and recover their system using backups, provided those backups aren't infected as well.

If the ransomware isn't completely removed, the user has a chance of going through the same issue again.

A newer form of ransomware poses as police. For instance, the Reveton trojan was a form of ransomware. The malware identifies the geographic location of the user and uses this location to display a warning window on the user's desktop. For instance, if you are located in the US, the window displays a ransom note with the FBI logo. The ransom note tells users that they were caught doing something illegal on their machine, and they need to pay a ransom or go to jail.

Most ransomware uses a high level of encryption. It uses a two-way system where one key is used to encrypt the files, and a second key is used to decrypt the files. The first key is used by the malware, and users pay for the decryption key. The malware also uses AES and RSA encryption algorithms, which are virtually impossible to crack. For this reason, most users gave in and paid the ransom instead of waiting for a fix.

After CryptoLocker, another form of ransomware was released. It took advantage of an internal command line application called PowerShell. PowerShell is similar to the Windows command line, except it uses internal commands called cmdlets. It's mostly used by system administrators, but desktop operating systems such as Windows 8 and Windows 7 also have PowerShell installed by default. The malware's name is POSHCODER. Because PowerShell cmdlets are native to Windows, POSHCODER would use the application to infect and encrypt files. Windows wouldn't flag the application as malicious since most PowerShell cmdlets are native to the operating system and don't normally pose a threat. The result was that POSHCODER was able to avoid detection from most antivirus applications including the Windows antivirus installed with the operating system.

How to Avoid Ransomware

To avoid data loss, all users should back up files. If the computer gets infected with ransomware, it's sometimes easier to format the machine and restore the lost files. Ensure that you don't keep your backups on the same computer, or ransomware will encrypt or block you from the backups as well. Keep important files in backups located on a cloud server. Users can also use external media such as a hard drive or RW-DVDs.

Applying software patches to applications with known threats is also a big issue. Most users skip important security updates until it's too late. Always apply patches when they are released. This includes operating system patches such as Windows Updates.

Ensure that you don't keep your backups on the same computer, or ransomware will encrypt or block you from the backups as well.

Don't ever click on a link or download an application with a suspicious file attached. Some hackers gain access to other email addresses, and then send malicious software using the victim's contact list. The recipient is more inclined to open an attachment from someone they know, but the message is often suspicious. Don't open executable files without verifying with the sender first.

Keep antivirus software updated, and scan your system occasionally with a full-system scan at night.

Removing Ransomware

Most ransomware can't be manually removed. Users need a specific program that removes ransomware from the system. Some anti-malware creators offer ways to remove malware and get files back. While this isn't guaranteed, it is an option for people who are infected with the malware.

The best way to deal with ransomware is to always have an antivirus running that protects against them. McAfee, Trend Micro, and Symantec have specific ransomware removal tools and protection against further infection. Trend Micro even has a smartphone application that protects mobile device users.
