LAB NOTE

AVG Business

AVG MULTI-LAYERED RANSOMWARE PROTECTION

What is ransomware?

Ransomware is malicious software or malware - it goes by many names including Locky, CryptoLocker, TorrentLocker, or TeslaCrypt. When your computer is infected with ransomware, your files are, in effect, held hostage until you pay a ransom for their return. Ransomware can also prevent you from using your web browser, other applications, or entire operating system.

How does ransomware work?

Ransomware encrypts files so that you can no longer open them. A message pops up indicating that your files are now encrypted. It demands immediate payment of hundreds or thousands of dollars to unlock your files, usually in untraceable crypto-currencies like Bitcoin.

Why is ransomware so problematic?

Your company can permanently lose access to internal as well as customer information. It costs time and money to remove ransomware. It results in a loss of productivity, and may even harm your company reputation. And, even when the ransom is paid, there is no assurance that files will be restored. Ransomware is very profitable and there is a low risk of being caught.

Which files are affected?

Ransomware usually targets your highest-value files (documents, spreadsheets, presentations, drawings) – but can also lock down your photos, music, and system files. Ransomware can encrypt single files, whole directories of files, or complete drives. Furthermore, cloud and network storages are also at risk if they are connected during an infection.

How do ransomware infections occur?

Most commonly a ransomware infection is from an email link or attachment – sometimes it is concealed by changing the file extension and by compressing it into an archive. Ransomware can also be bundled into other applications – games, video players, any application from unknown publishers should be suspect.

How does AVG protect me from ransomware?

AVG's Business Editions utilize a multi-layered approach to detecting and eliminating ransomware. When a file passes successfully through one level of testing it is handed off to another layer for even more scrutiny.
See the process overview in the sidebar. . .

How effective is AVG's scanning engine?

AVG regularly submits its applications to independent test labs for testing and AVG Business Edition earned the highest rating for protection - 6 out of 6 in the latest round of testing by AV-Test.org

How do I restore access to my files if my machine has been infected?

It depends on your version of Windows and what features are enabled. Please see this article from Microsoft for more information. . .

Where can I learn more?

This article includes samples of the Ransomware messages and has additional tips on avoidance.

AVG Multi-Layered Ransomware Protection

Files pass through several layers of inspection and testing to identify malware. . .

1) Files are first compared to any known variants in a malware database – both the metadata and content of the files are analyzed

2) Then files are tested in an emulator (a virtual computer) where it can do no harm to your real computer

3) Now that the file is running, it's behavior is assessed using a variety of techniques, including Artificial Intelligence algorithms

Behavioral assessments occur in the AVG application and in the cloud, but they all work together behind the scenes and in real-time to determine whether a file is malicious

If the file is determined to be malware, it is quarantined, and AVG's Crowd Intelligence feature updates all AVG users software

www.avg.com