5 Essential Features Any Good Anti-Ransomware Solution Should Have

Dorothy Mitchell May 17, 2017

A ransomware will stop you from carrying out your daily business operations, as a result lead to loss of time and money.

Hackers use ransomware to lock you out of your computer resources; files, data and system and demand a ransom in return for access.

(Newswire.net -- May 16, 2017) -- Hackers use ransomware to lock you out of your computer resources; files, data and system and demand a ransom in return for access. It is created by scammers who are skilled and experienced in computer programming and if you don't have ransomware protection, they can enter your computer through email attachments, browsers (if you open an infected website) or through your network.

It is mainly carried out using a Trojan and can enter the system through downloaded files, or through a vulnerable network service. Once your computer is infected with ransomware, you will not be able to access your computer resources including applications and data files among other resources.

A ransomware will stop you from carrying out your daily business operations, as a result lead to loss of time and money. For this reason, there is a need of guarding computer systems against ransomware, or to recover your system in case of a ransom attack.

The most effective way of detecting, removing, and protecting your computer against a ransom is installation of a strong anti-ransomware tool. Apart from installing such a tool, you need also to ensure that your operating system and other software are clean.

Essential Features of a Good Anti-Ransomware Solution

Ransomware has evolved in a way that it distributes itself through the internet and grows into a bigger threat to your computer systems. With this evolution, anti-ransomware solutions have also advanced in the way they work and their effectiveness. Different anti-ransomware have different features and work in a different mechanism. However, there are some good features that a good and quality anti-ransomware software should have. It should have:

1. Real-time Protection – Real-time protection capabilities allows the anti-ransomware solution to react to a potential threat as it enters the computer system. The anti-ransomware should check all your files whenever you are using them. It should also be able to scan your computer for newly identified threats. It does so through file emulation, file analysis, and signature detection.

2. Automatic Full System Scan – The anti-ransomware software should be able to automatically scan your computer system for ransomware. It should have a scheduling feature, which allows the user to set the specific time of the day for scanning and the frequency at which the scan is conducted. Some anti-ransomware software detects when your computer is idle and performs an automatic full scan at the time.

3. Automatic Updates – Apart from addressing vulnerability, anti-ransomware software should be able to update automatically new ransom signatures discovered to ensure protection against latest threats.

4. Web/ Browser Protection – The internet browser opens up a gaping hole through which threats can enter your computer system. A good anti-ransom solution should have a browser protection feature. The software should have a particular browser plugin made by the same vendor or a developed spin of popular browser to ensure complete and

secure browsing experience. It should have an online account protection and URL checkers that can stop you from visiting known dangerous web pages.

5. Email Protection– A good anti-ransomware software should have email protection feature. The feature may work on certain email clients or as an add-on to popular web-based email clients.

Source: http://newswire.net/newsroom/blog-post/00096362-5-essential-features-any-good-anti-ransomware-solution-should-have.html