Be Proactive! Block CryptoLocker Before it Installs

CryptoLocker, a particularly malevolent virus, continues to claim victims, both consumers and businesses alike. The devastating Trojan is a form of ransomware that spreads mainly through fake emails, mimicking the look of legitimate businesses. Other users report being tricked into installing the ransomware via phony FedEx and UPS tracking notices.

How does CryptoLocker work?

Once the user opens the malicious message, CryptoLocker installs itself and scans the hard drive to sniff out files within the network. If one computer on a network becomes infected with CryptoLocker, mapped network drives could also become infected. Then, the ransomware encrypts selected files and renders them inaccessible to the user until he or she pays a ransom to receive a decryption key!

Defend your system against CryptoLocker

The best defense against CryptoLocker is to never let it enter your system in the first place. The great news is that SMBs and enterprises using **Comodo Endpoint Security Manager** are fully protected. ESM and its Comodo Endpoint Security (CES) software has been proven to proactively stop threats including the CryptoLocker ransomware by automatically isolating all unknown applications (malicious or not).

How does Comodo Endpoint Security work?

Comodo Endpoint Security focuses on prevention, not purely detection. Comodo's patent-pending Auto Sandboxing technology creates a real time, isolated environment that identifies safe, unsafe, and questionable files and executables and **automatically** isolates both unsafe and unknown files, allowing only known, trusted files to penetrate your system.

If a threat is known to be malicious, Comodo's Antivirus (AV) will detect its signature and prevent any damage from occurring, i.e. the encryption of your files. If the threat is unknown, the HIPS and Auto-Sandbox will intercept the malware, stopping it in its tracks, as the virus is never actually installed on your system. Comodo AV labs detect blacklist signatures for malicious files such as CryptoLocker, so the ransomware would go straight into the Quarantine Manager where the admin could delete it.

CESM 3 packages unsurpassed protective power within our next-generation remote administrative console. This enables the administrator to receive real-time alerts through a panoramic view of all endpoints and

system management capabilities, a feature generally found only in dedicated RMM systems. So, when the user opens the malicious message containing CryptoLocker, CES will detect the malicious (or unknown) file, automatically sandbox it, and alert the administrator. If the admin gets to the alert before Comodo labs, the administrator is able to remotely remove the ransomware from the end user's computer, regardless of the end user's location.

Four clicks to security:

1. Administrator views the list of files within the sandbox.
2. Administrator selects the malicious executable(s) to be removed.
3. Administrator remotely accesses the end user's computer to select the malicious file running on the sandbox.
4. Administrator deletes the file location to rid the user's system of the malicious application.

Four clicks to security. It's really that simple! But don't just take our word for it. Comodo Endpoint Security (CES) is powered by the same patent-pending prevention-based technology that our consumer product, Comodo Internet Security (CIS), uses to protect consumers against CryptoLocker. CIS was recently awarded the top position in the Proactive Security Challenge 64 by matousec.com, a project run by a respected group of independent security experts dedicated to improving end user security. Following the challenge, matousec.com named CIS the ***"Ultimate Protection Machine"***.

In addition to its ability to protect enterprises from malware like CryptoLocker, ESM has many other great capabilities. For instance, the latest upgrade to ESM added several capabilities such as centralized monitoring of sandboxed (unknown) and malicious files, endpoint auto-synchronization via Active Directory, encrypted VNC sessions to local and remote endpoints, and support for Windows 7 Embedded Standard.

Be proactive and protect your endpoints from CryptoLocker and other malware with ESM today!

Download a **60-Day, 60 user free trial** now.