

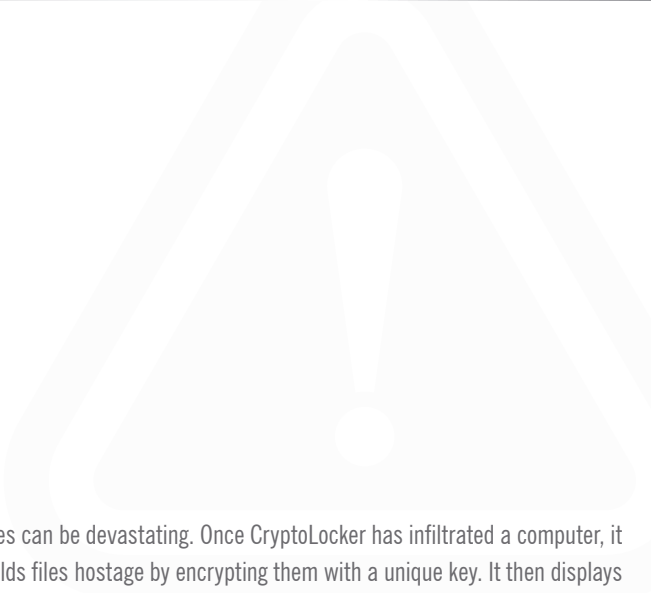
# CryptoLocker

## *Your Money or Your Life*

### BACKGROUND

As of September 2013, a new and vicious form of malware has been wreaking havoc. CryptoLocker belongs to a family of malware called “ransomware”, which is designed to extort money from victims by denying them access to their personal files. It targets all Windows Operating Systems, from Windows XP to Windows 8, and typically remains unnoticed by victims until it’s too late and the damage to their files is irreparable.

These days, many people store everything on their computers, from important documents to music and family photos. Malware that affects



files can be devastating. Once CryptoLocker has infiltrated a computer, it holds files hostage by encrypting them with a unique key. It then displays a pop-up ransom note with instructions to pay approximately US\$300 within 72 hours or the encryption key will be destroyed and the files will become unrecoverable.

For further details on CryptoLocker, visit the following website:

[www.bleepingcomputer.com/virus-removal/cryptolocker-ransomware-information](http://www.bleepingcomputer.com/virus-removal/cryptolocker-ransomware-information)

### THE CHALLENGE

Because of the complex encryption strategy it utilizes, malware of this type is nearly impossible to remediate once it has infected a computer. Antivirus software alone cannot break the encryption, and, due to the time limit for the ransom, a live technician would also be ineffective.

The only way to unlock the files is by using the unique decryption key, so there is no way to retrieve the private decryption key without paying the ransom. The best protection against such infections requires a preventive approach.

### THE SOLUTION

New viruses, and updated versions of existing viruses, are released daily, even hourly. Because of this, signature-based threat detection cannot be effective. Instead, Internet security solutions that use behavioral detection are necessary.

Webroot SecureAnywhere solutions use cloud-predictive behavioral intelligence to discover malware as soon as it attempts to infect a user, and then protect all other users against such attacks without the hassle of time-consuming signature updates. Using Webroot® Intelligence Network™ cloud security services, Webroot solutions deliver comprehensive real-time protection. Endpoints all over the world collect

over 200 gigabytes of behavioral execution data each day. Unique URL and IP data feeds from strategic partners further enrich Webroot malware intelligence. As a result, Webroot SecureAnywhere security solutions become more powerful every minute, and more effective each time an endpoint is added anywhere in the world.

When a SecureAnywhere solution is installed on a machine, a CryptoLocker infection variant should be detected automatically before it can infect and make changes to the computer. Even if a new variant of the infection infiltrates a given system, SecureAnywhere technology includes automatic journaling to undo changes to a computer’s files.

It is important to note that the journaling, roll-back and file recovery that a locally installed Webroot SecureAnywhere solution performs will only account for the changes made on the computer's local hard drives. Changes made to network shares would not be journaled, so those files

cannot be restored. This vulnerability can be addressed by ensuring that computers and servers on a given network are protected with Webroot SecureAnywhere, and that any network shares are set to a read-only mode wherever practical.

## SUMMARY

True security against ransomware infections requires a proactive, preventive protection method. By leveraging global threat data delivered from the cloud, Webroot Internet security solutions stay ahead of malware and safeguard your important data.

Keep in mind, however, that remaining protected from malware does not depend solely on adequate preventive security measures, but also depends on responsible usage practices. In addition to Internet security software, avoiding suspicious emails, attachments or links; making sure the OS and applications are up to date; and backing up data regularly will ensure that your system or network are protected from online threats like CryptoLocker.

### About Webroot

Webroot is bringing the power of cloud-based software-as-a-service (SaaS) to Internet security with its suite of Webroot SecureAnywhere® solutions for consumers and businesses. Founded in 1997 and headquartered in Colorado, Webroot is the largest privately held Internet security organization based in the United States – operating globally across North America, Europe and the Asia Pacific region. For more information on our products, services and security visit [www.webroot.com](http://www.webroot.com).

### World Headquarters

385 Interlocken Crescent  
Suite 800  
Broomfield, Colorado 80021 USA  
800 772 9383

### Webroot EMEA

6th floor, Block A,  
1 George's Quay Plaza  
George's Quay, Dublin 2, Ireland  
+44 (0)870 1417 070

### Webroot APAC

Suite 1402, Level 14, Tower A  
821 Pacific Highway  
Chatswood, NSW 2067, Australia  
+61 (0) 2 8071 1900