What is Cryptolocker Ransomware? Are your Computer Files Safe?

John K Arnold November 04, 2013

Cyptolocker is a...

Cryptolocker is a very nasty virus that has infected millions of computers. If you use a computer, you need to know about this..

(Newswire.net -- November 4, 2013) Chicago, Illnois -- Cryptolocker is a very nasty computer virus. It is called ransomware because the virus hijacks your computer, encrypts your files and sends you a note to pay $300 within 72 hours or your files will be gone forever. By the time you realize it is there it is too late. Antivirus programs don't stop or protect from this.

Companies are not safe from attack and infection.

Hayden Hess: "One of my employees opened an email from "administrator@" with our domain name. The file contained what looked like a pdf file, but was in fact the Cryptolocker. It shut down all of the stuff on his desktop and started to encrypt his files. We did isolate his computer from the network, saved what we could, and then reformatted his computer.
Nasty, nasty program. Beware!"

This is not a joke or an idle threat.

If infected, your files will be there but you will not be able to read them. The encryption is very powerful. You either choose to pay the money of you lose your files. This means all your documents, pictures, videos and anything else you might have will be gone.

So far the virus only attacks Windows based computers.

It installs a program that uses a key that is needed to decrypt your files. It is estimated that it would takes thousands of years to break the key code.

Your antivirus program will not protect you.

With this malware by the time the virus is detected your computer is already infected. The virus can be removed but that does not decrypt your files. You may then a note that unless you reinstall the virus and pay the $300 your files are gone.

The main way of infection is by opening an email attachment.

The most common ways the virus enters is through email. Clicking on that unknown email could cost you all your files. Most are similar to phishing emails. These appear to be from well known businesses such as banks, UPS, Intuit, FedEx and others. The attachment is disguised as a PDF file but is really an executable program.

The attachment may have the Cryptolocker virus or it may have another program than will install the virus. The virus does not just stay on that computer but will spread through a network from hard drive to hard drive. If your backup drive is on the network then you will lose your backup as well.

Be very cautious about public networks.

If your computer is accessible on the network and someone else is infected you may be infected as well. You could then carry the virus with you and infect other hard drives in other networks. You may not even be aware as the virus is set to load when you start your computer.

Prevention is the best strategy. Do not do or do with great caution

- Open unknown or suspicious emails
- Click on a notice to upgrade a program you are not certain of as may be a botnet
- Connect into a public shared network

Do these things.

- Have a current backup that is not connected to your network
- Be sure windows and other security programs are current
- Pass the word on to others as the virus is contagious
- Check for updates

Be safe as the data you save may be your own, your families, your friends or people you don't know.. (Learn More)

John K Arnold is a Newswire featured author. He has over 35 years of business experience including doing online marketing and business since the 1990s.

You can view more Press Releases by the author and view his profile by clicking on author name at top.

For information on Press Releases for your business, event, cause or idea please contact by phone or email below.

JKA Marketing, Inc

910 W Van Buren # 340
Chicago, Illnois 60607
312-802-1208
john@jka-marketing.com
http://www.jka-marketing.com

Google+