Forest Computers

359G Johnson Ave. West, Winnipeg, MB, Canada R2L 0J2
Phone: (204) 956-6590 Fax: (204) 956-6595
www.forestcomputers.com

Release Regarding the "Crypto Virus"

With kind contributions from Lucas Kandia of Seerx Technologies Inc., Winnipeg, MB

It appears that a very powerful and destructive virus is spreading across the Internet - the Crypto Virus. The way it works is best described here:

http://www.bleepingcomputer.com/virus-removal/cryptolocker-ransomware-information

It appears the infection comes through email. Most current antivirus programs and spam filters have not had much success in catching the infection. This virus is new and mutating from week to week. Double clicking on the attachment and installing the program starts a cascade of events to take place:

a) It runs from a local temporary file area in the user's own profile on their own machine.

b) It contacts a Command and Control Center up in the Internet.

c) It then creates a private key which is stored only at that Command and Control server, destined to be erased in 96 hours.

d) It uses that same private key to encrypt all the user created data files the infected computer had access to using a mixture of RSA and AES Encryption. INCLUDING NETWORK DRIVES.

e) It needs simultaneous Internet and drive letter access to do the encrypting. Taking the infected machine off the Internet breaks the encryption cycle.

f) It encrypts as many user created data files (like xls, pdf and doc to mention a few) as it can get its digital paws on and displays a ransom message (this is not a typo – ransom in every sense of the word). It documents which files it encrypted, and keeps that list stored in registry.

The ransom can be paid by either BitCoin or MoneyPak vouchers (instead of credit cards) – which protect the identity of the ultimate recipient of both forms of commerce (we can't easily find out who is behind this scam) as opposed to using a credit card.

BitCoin - http://bit.ly/b3mVDm

MoneyPak - http://bit.ly/1igukg6

By paying the ransom, you are promised to be given a code to have the virus unlock the encrypted files. This would potentially be a way out (you don't use a credit card in dealing with these people), if you don't have backups of your files.

If you don't do regular backups of your important data, now is a great time to start!

Forest Computers

359G Johnson Ave. West, Winnipeg, MB, Canada R2L 0J2
Phone: (204) 956-6590 Fax: (204) 956-6595
www.forestcomputers.com

Technical Information

We are highly recommending inoculating all computers that have access to email and the Internet.

Here is a great program that only allows certain programs to work on the network, essentially does a whitelisting of applications.

Lumension - http://bit.ly/1bj3QrQ

The inoculation steps are ¾ of the way down the "bleeping computer" page referenced above.

Make sure that you do 2 EXTRA things not mentioned in their blog.

1. Manually check the %AppData% folder that you have inoculated and LOOK for a random folder in there like XHGR34, etc. In that randomly named folder check for a randomly named executable. If you find such a folder delete it and any files inside.

2. Place a downloaded executable into the %AppData% area and try to run it AFTER inoculating the machine. If it runs, you either haven't put the file in the right place OR you didn't run the inoculation properly.

How do you find out where to put your "test" executable?

Open a command prompt

Type "set" and hit return

My %AppData% folder was:

APPDATA=C:\Users\lkandia\AppData\Roaming

DO NOT RUN THE INNOCULATION WITHOUT CHECKING FOR RANDOM FOLDERS IN %AppData%

Please note: Neither Forest Computers or Seerx Technologies accept any responsibility for the use or misuse of information contained in this document. If you are unsure of the status of your system, have it checked professionally.