the Availability Digest

www.availabilitydigest.com
@availabilitydig

CryptoLocker – Destructive Ransomware

November 2013

Ransomware is a class of malware that locks up a computer and demands a ransom from the computer's owner to unlock it. Most ransomware only freezes a computer, and the computer can often be restored by an anti-virus service provider. PCs and Android phones have been common victims of ransomware.

CryptoLocker is a variant of ransomware and is much more dangerous. It does not simply freeze a computer. It encrypts all of the files on the computer. Though the computer still runs, it cannot do anything because all of the files to which it needs access are encrypted with a key that is not available to the user. No private or government agency has yet been able to break the encryption.

CryptoLocker will only release the files if a ransom of a few hundred dollars is paid within a specified time period.

How Does CryptoLocker Work?

CryptoLocker appeared in September, 2013, and has been slowly but dangerously infecting PCs and the networks to which they are attached. It attacks all versions of Windows, including Windows XP, Windows Vista, Windows 7, and Windows 8

It is spread through phishing. Phony emails designed to look like they are from legitimate businesses or that appear to be UPS or FedEx tracking notifications contain a malicious link or attachment that installs the malware. CryptoLocker installs itself in the Documents and Settings folder.

CryptoLocker uses an asymmetric encryption scheme that so far appears uncrackable. Asymmetric encryption uses a public key and a private key. The public key is known to all. However, decryption cannot be done without the private key.

For each victim, CryptoLocker connects to its command-and-control server to download a public key that is used to encrypt the data. For each new victim, a unique private key is created and only the CryptoLocker authors have access to these decryption keys. They are stored on their command-and-control server. The private key for each victim is different, so that an attacked user cannot simply use the private key that has been given to another victim who has paid the ransom.

All of the files accessible by the user are encrypted. This includes all files on the network to which the user has write access.

Once the encryption is complete, a pop-up window is displayed notifying the user that his files have been locked. It describes the amount of the ransom and how the ransom is to be paid. It also shows

a count-down clock showing how much time the user has to pay the ransom. The total time from encryption to ransom is typically three to four days.

The requested ransom is typically $100 or $300. Payment is requested in MoneyPak vouchers or bitcoins. Bitcoins are digital currency that is becoming quite popular for online payments. They are designed to be anonymous, just like cash.

If the ransom is paid before the deadline, CryptoLocker will decrypt the files. This process can take several hours. However, if the clock should run out with no ransom, the key is destroyed and the files are lost forever.

CryptoLocker can be detected and deleted by anti-virus utilities, but by the time this happens, it is too late. The files have been encrypted. Unfortunately, if the anti-virus malware deletes CryptoLocker before it has finished encrypting all of the files and displaying the pop-up window, there may be no way to pay the ransom and regain access to the encrypted files.

Prevention

The steps to take to prevent infection by CryptoLocker are those steps to prevent any malware infection;

- For emails from presumably known sources, check the sending email address to ensure that it is valid. Many spam filters show the actual email address of the sender. If the sender's address is

known to be billh@gmail.com, but the sender's address for the email is billh12@gmail.com, delete the email.

- Ignore email attachments from unknown senders.

- Don't open unexpected attachments from a known sender. Contact them first. .zip, .exe, .pdf, .doc, and .xls attachments can all contain viruses.

- Use caution with links in emails:
  - Banks and corporations can easily be spoofed.
  - Any email that contains only a link or a link and a distress message from someone you know is likely malware.
  - Before clicking any link, hover over it to see the true destination to which the link will take you. If the destination does not agree with the text in the link or is unknown, delete it.

- Do not accept any offers to install any anti-malware or other utilities.

- Think twice before visiting any unknown website.

- Conduct routine backups of important files. Use the services of a backup cloud such as Carbonite, or back up to disk and keep the backup disks offline.

- Maintain up-to-date antivirus software.

- Keep your operating system and software up-to-date with the latest patches.

- Follow safe practices when browsing the web.

- Do not grant write access to anyone for network files that they only need to read.

Mitigation

If you are attacked by CryptoLocker or any other kind of ransomware, immediately disconnect the infected system from the network to prevent the infection from spreading to other systems.

Consult with a reputable security expert to remove the malware from infected systems.

If you have backed up your files, delete the encrypted files and restore the files from the backup.

Change all passwords after the system has been removed from the network and after the malware has been deleted.

If all else fails, you may have to pay the ransom.

Further Information

A great deal of further information on CryptoLocker can found in a paper entitled CryptoLocker Ransomware Information Guide and FAQ.[1] It is a lengthy paper. Its Table of Contents follows:

[1] CryptoLocker Ransomware Information Guide and FAQ
http://www.bleepingcomputer.com/virus-removal/CryptoLocker-ransomware-information

Table of Contents:

Pay particular attention to the chapters on Software Restriction Polices (Chapters 17 and 18).

Summary

The good news, if there is any, is that the hackers have proven to be honest. Once paid the ransom, they have decrypted files and have not re-infected the computer. However, if the ransom is not paid, be prepared for further attacks. Security companies have yet to come up with any protection against CryptoLocker.

The FBI encourages victims to report infections to the FBI at the Internet Crime Complaint Center.

Acknowledgement

We would like to thank our subscriber, Locke Highleyman, for bringing CryptoLocker to our attention.

Material for this article was taken from the following resources:

CryptoLocker Ransomware Information Guide and FAQ, *Naked Security*; October 12, 2013.
CryptoLocker Ransomware – see how it works, learn about cleanup, protection and recovery; *Naked Security*; October 18, 2013.
CryptoLocker Virus: New Malware Holds Computers for Ransom, Demands $300 Within 100 Hours and Threatens to Encrypt Hard Drive, *IBI Times*; October 21, 2013.
CryptoLocker Wants Your Money, *Secure List*; October 25, 2013.
CryptoLocker Ransomware Infections, *US-CERT*; November 5, 2013.