CryptoLocker ransomware

The most dangerous malware

Tamás Ludman

tamas@ludman.hu

12th of May 2014

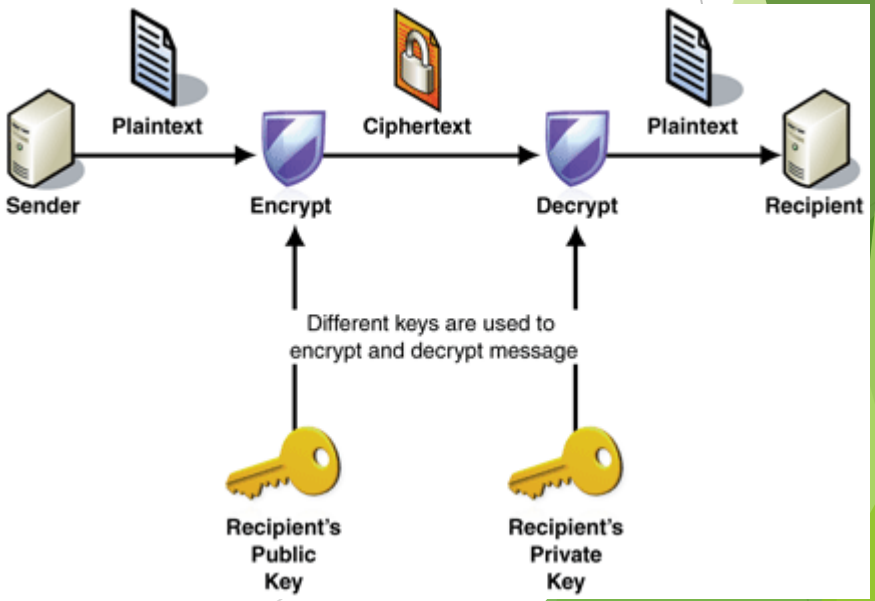
About CryptoLocker

- One of the ransomwares, CL was detected in September 2013 first time.
- It encrypts all important files with RSA cryptography on attached storage devices
- It demands money (ransome) for file restore
- Nobody will be able to restore the encrypted files without unique private key

Sources of the infection:

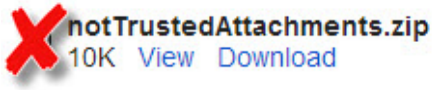
- First version of CL has been spreading by spam (with zip file attachment) mainly, or it is able to infect by visiting malicious websites.

- The newer versions of CL is able to infect through the mobile storage devices,
eg. memory cards, pen drives, etc.

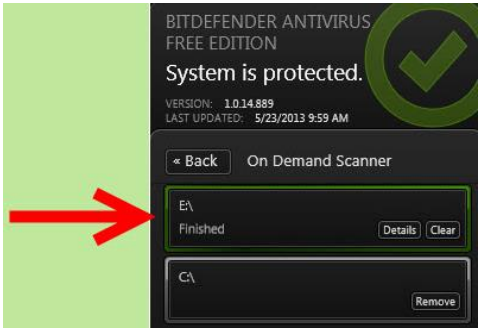


Prevention

- Effective AV security software (i.e. Webroot with rollback function)
- Windows operating sytem should be updated
- All of applications should be up-to-date
- Should not open any zip-attachment from unknown e-mail senders



- Shouldn’t connect any portable storage devices to PC without virus scanning

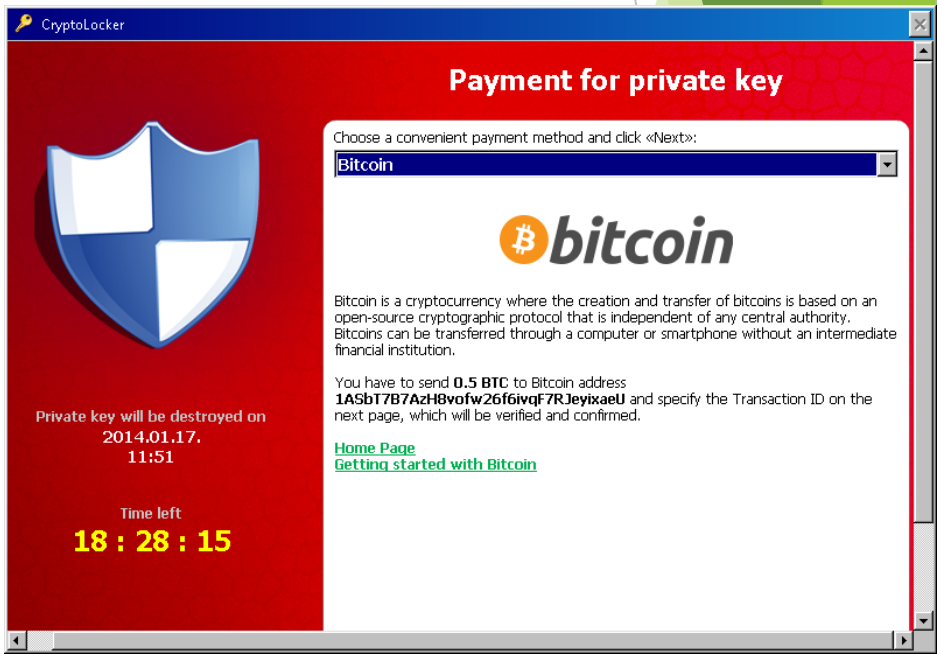


- Should not visit warez and other suspicious webpages

Problem solving (after infection)

I. If you don’t have any up-to-date backup:
   - Have to pay the ransom for the unique private key ASAP.

II. If an up-to-date backup of the files exist:
   a) Remove CryptoLocker with an effective antivirus software, or reinstall the operating system.
   b) Restore all data from the backup.



Helpful hints

Do's

+ Install effective antivirus software and update virus definition daily.
+ Turn on „Install updates automatically"
+ Make backup copy about important files orderly.
+ Scan portable devices by AV before copy/open any files from it.
+ Detach all redundant drives from PC.
+ Visit only secure webpages and use webfilter.
+ Use content filter for email software.
+ Be distrustful user against suspicious, unusual things. (Healthy paranoia is required. ☺)

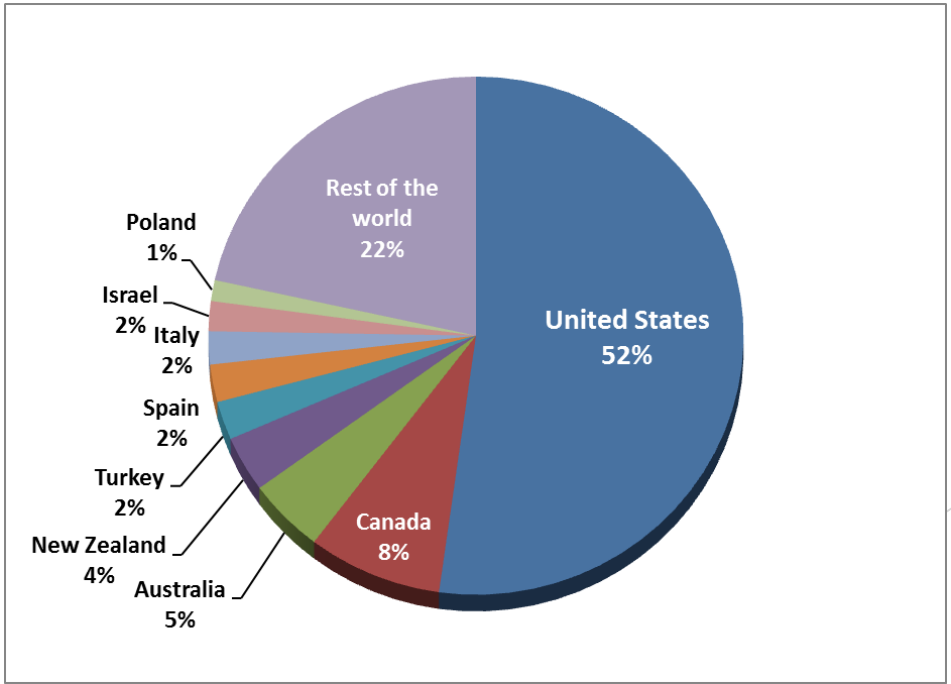
Don'ts

- Don't use any computer without AV software.
- Don't visit any unreliable webpages.
- Take care when a website asks you to install a „plug-in".
- Shouldn't use a PC without important Windows updates (Security patches).
- Shouldn't use a PC without backup copy about valuable files.
- Needn't be attach portable data storages always.
- Don't open e-mail attachment unless you are sure it is safe (warning: unknown senders)
- Mustn't give out personal data to just anyone!

Experiences

- Without unique private key the file-restore is impossible
- Most virus scanning softwares can’t restore the encrypted files
- Usually the users don’t have an up-to-date backup from their important data
- The data recovery companies didn’t have any solution for data restore
- The infections are spreading all over the World

As shown by the ESET LiveGrid® detection statistics below, the country most affected by this ransomware is the United States.



Thank you for watching.

Any question?

Sources:

en.wikipedia.org/wiki/CryptoLocker

www.hwsw.hu/hirek/51349/cryptolocker-virus-ransomware-malware-symantec.html

www.theguardian.com/money/2014/feb/27/pc-users-beware-cryptolocker-malware-royal-mail

blog.malwarebytes.org/intelligence/2013/10/cryptolocker-ransomware-what-you-need-to-know/

www.welivesecurity.com/2013/12/19/cryptolocker-2-0-new-version-or-copycat/

support.microsoft.com/kb/129972/en-US

www.google.hu/?q=cryptolocker#q=cryptolocker

My colleagues at the Semmelweis University.

IT Conferences: GDATA and IDC, etc…