The Hague, October 2013

Intelligence Notification 011-2013

CYBER BITS

Encryption ransomware - CryptoLocker

What happened?

Ransomware is a well-known type of malware. It locks the victim's computer demanding a fee in order for the restriction to be removed. One of the most spread versions is *Police ransomware* where the victim is lead to believe that a police agency blocked his computer because illegal content was detected. With up to date anti-virus programmes and following simple instructions, this type of malware is not so difficult to remove.

Cybercriminals have therefore improved their malware. For over a year, there are ransomware versions at large which encrypt files on the victim's computer. The victim needs to pay around 300$ to receive the private key that decrypts the files.

CryptoLocker is such a type of malware, recently commented on by TrendMicro and Symantec.

How does it work?

After infecting the victim's computer, CryptoLocker generates a Unique ID and sends it to a server controlled by the attackers. The server then generates a public-private key pair (based on the received Unique ID) and sends the public key back to computer. The CryptoLocker malware, running on victim's computer uses this public key to encrypt different type of files (documents, spread sheets but also pictures as well as Internet Security Certificate files) found on the victim's machine. The virus will search for files to encrypt on all locations and drives it can access from the victim's computer, including network drives and resources on other computers or servers.

When finished, CryptoLocker pops up a page with instructions how to pay the ransom, giving the victim a limited time frame, normally 72 hours, to buy the private key which allows decrypting the personal files. Although the removal of the malware itself is not difficult, it is not possible to decrypt the encrypted files. If the victim doesn't pay, the files are lost.

This malware gets dropped on the victim's computer after the system has been exploited without user consent or knowledge due to security vulnerabilities in unpatched or out-dated software.

Why do you need to know?

- It represents an improved and more effective business model for cyber criminals which allow them to ask a higher "ransom" from the victim. Online payment methods, like Ukash or cashU) or 2 BTC (for Bitcoins) are proposed to increase the anonymity;
- In reaction to this threat, law enforcement and governments have to increase their efforts in improving cyber awareness amongst the public. This is a typical example of malware which can be prevented by basic security measures which should perhaps be communicated more regularly to the public:
  - Keep operating system and all installed programs up-to-date by ensuring automatic updates;
  - Install security tools like firewall and antivirus software and keep them updated;
  - Install latest versions of Internet browsers and update add-ons such as Java and Adobe Flash;
  - Avoid untrustworthy downloads from freeware or shareware sites;
  - Avoid surfing questionable sites, like online gambling, porn and illegal content sites;
  - Make regular backups: backup all sensitive data and personal files and store them somewhere safe (preferably offline, in a different media like an external hard drive);
  - Use Windows OS functionalities like Windows Backup and System Restore Points;
  - Avoid opening email and attachments from unknown persons/sources.

EC3 would welcome reactions on this note. Please mail to *O31@europol.europa.eu*.