Ransomware

The latest case from Spain demonstrates how the threat from 'ransomware' is still a 'clear and present danger' to average users of the Internet.

Even though the Spanish case was a very important blow to the criminals in this field, many other criminal networks are still committing this profitable crime and 'hi-jacking' innocent Internet users' computers to intimidate them into paying illegal fees.

Ransomware is a kind of malware that attempts to extort money from an innocent computer user by infecting and taking control of their machine. Normally, the malware will either 'lock' the computer to prevent use, or it will encrypt the documents and files on the computer to prevent access to the saved data.

The demand for ransom will then be displayed; usually either via a text file or as a webpage in the web browser, and users are encouraged to pay a ransom fee through, for example, Ukash or PaySafe.

Victims are normally embarrassed by the false 'accusation' included in the text – and some victims unfortunately pay the ransom fee to the criminal groups behind it, because they actually believe that the malware was launched by law enforcement. This is not the case. No EU law enforcement agency imposes fines in this way!

The development of the malware continues and EC^3 predicts that this crime will continue and expand in 2013.

It is very important that a victim of this crime does NOT pay the ransom fee. Instead you should shut down your machine and call an expert for help to remove the malware. But do not pay!

Please also consider visiting recognised security companies on the Internet and following their advice on how to remove malware if you are infected.

If you follow this link you can read in more detail about how this crime works, and how to act and react if infected.

Troels Oerting

Assistant Director

Head of European Cybercrime Centre (EC^3)