EUROPEAN CYBERCRIME CENTRE

EC3 EUROPOL

The Hague, September 2016

Intelligence Notification No. 23/2016

CYBER BITS
Series: Trend

Fantom Ransomware

What happened?

A new ransomware called 'Fantom' has recently been discovered. It works by displaying a fake Windows Update screen that creates the impression that a new critical update is being installed. In the background, all the user's files are being encrypted. The screen shows a percentage counter to appear legitimate but also to account for the increased activity on the user's hard drive. This window can be closed by the user, but the encryption still continues in the background. Once complete, a ransom note is displayed that shows the victim's ID key and provides instructions to get the files decrypted. The victim is told to email the cybercriminals using one of two supplied email addresses in order to do this. This is different to other previously-seen ransomware variants, which have required the user to pay by accessing a site on Tor; this may be to target less technically-able victims.

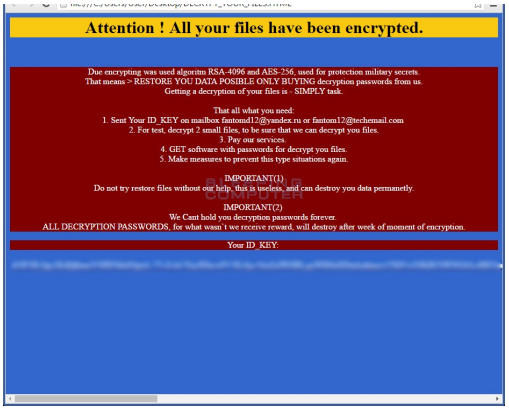

Image downloaded from: http://www.bleepingcomputer.com/news/security/fantom-ransomware-encrypts-your-files-while-pretending-to-be-windows-update/

Currently, there is no known way to decrypt the files and it is unclear where the criminals originate from, given that the email addresses provided to the victim are attributable to Russian and Californian service providers. In addition, the English used in the ransom note is of a very poor standard, suggesting that the culprits are not native English speakers and raises questions regarding how easily victims are able to communicate with the extortionists via email.

How does it work?

Once the ransomware has been downloaded onto the victim's machine, the computer executes a file called WindowsUpdate.exe (which appears harmless). The file properties of the ransomware state that it is a critical update from Microsoft, so making it appear legitimate. When displayed, the fake Windows Update screen does not allow the user to switch to any other open applications.

It has been found that the ransomware itself is similar to others in the sense that it is based on EDA2 code and encrypts files with AES-128 encryption. When a file has been encrypted, '.fantom' is appended to the end of the extension of the file and the ransom note DECRYPT_YOUR_FILES.HTML is created in each directory where a file has been encrypted. When the encryption is finished, two batch files are created and executed which delete the shadow volume copies and the fake Windows update executable.

For more information, see:

- http://www.bleepingcomputer.com/news/security/fantom-ransomware-encrypts-your-files-while-pretending-to-be-windows-update/
- http://www.digitaltrends.com/computing/fantom-ransomware-windows-update/
- https://www.webroot.com/blog/2016/08/29/fantom-ransomware-windows-update/

Why do you need to know?

- This is a new threat and currently, it would appear that there are still gaps in knowledge regarding who is responsible and how prevalent it is;
- Computer users are reminded of the importance of backing up files regularly to avoid the loss of valuable data, particularly as there is currently no known way of decrypting files.

EC3 would welcome feedback on this note. Please mail to O311@europol.europa.eu.
(note that "O" is *a letter not a number)*