National Computer Board

Computer Emergency Response Team of Mauritius

(CERT-MU)

Spyware Alert

Spyware Targeting Facebook Users

Detected on: August 19, 2014

Severity Rating: High

Malicious messages are circulating on Facebook whereby users are being prompted to follow a link leading to supposedly their own video. The aim of this message is to have a **Spyware** installed in the victims' machine to gather login credentials of the user.

PS: A Spyware is a software that collects information about a person or organization without their knowledge and may send such information to another entity, or that asserts control over a computer without the user's knowledge.

Attack Methodology

1. Facebook users are receiving messages such as ***"This video belong to you? That's funny.. Click to watch video".***

   An example of the message is shown below:

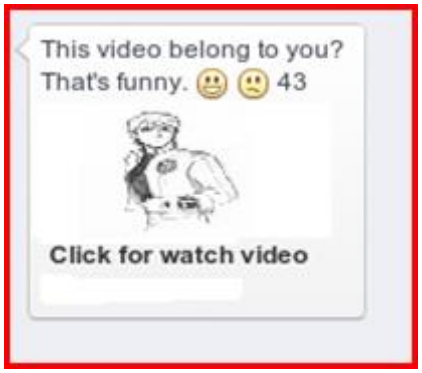

Image 1

It is to be noted that the profile picture of the Facebook user is also embedded in the above message to convince the user to view the video by clicking on the links : ***fun-metin2.com*** or ***fun-mastic2.com***

2. Upon clicking on the link, Facebook users are redirected to the following page: **www.amk-mt2.com** .

   This website has been classified as RISKY by many intrusion detection softwares, as shown below:

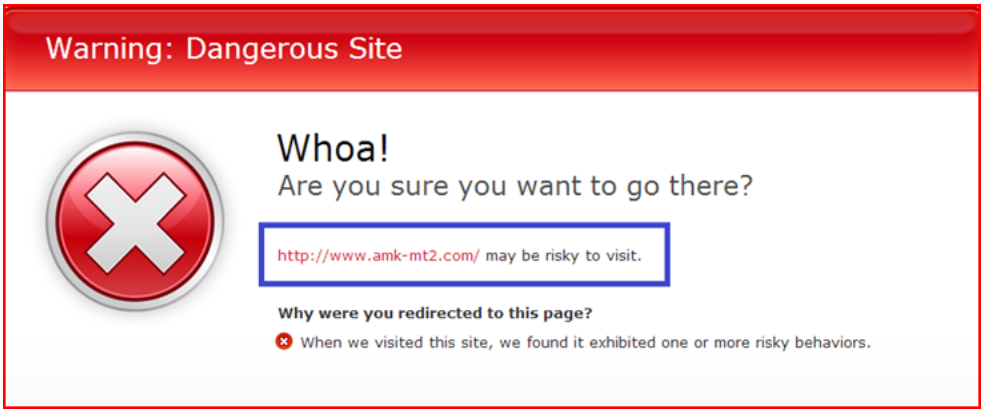

Image 2

An extract of the website **www.amk-mt2.com** is copied below for your reference:

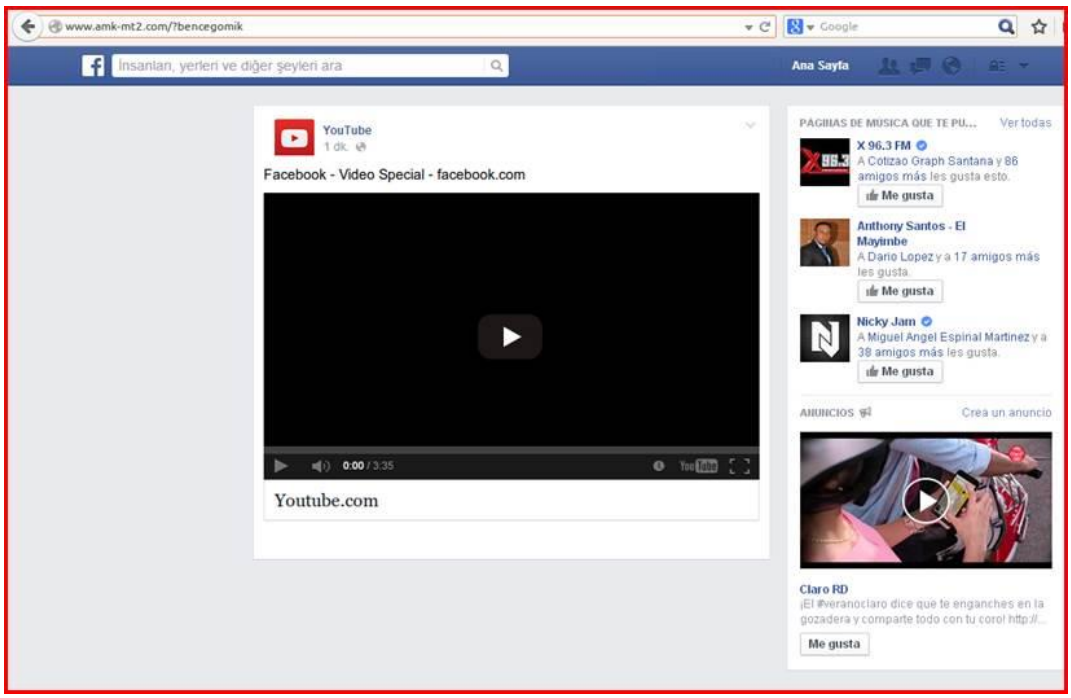

Image 3

3. When users click on the PLAY button to view the video, a pop up appears which prompts the user to install a Plugin (Facebook Video Plugin). It is to be noted that only users browsing through Google Chrome will be asked to install the plugin from Chrome Web Store.

Image 4

The installation of the plugin will allow gathering user activity data.

If the user is not using Google Chrome browser or deny the installation of the Plugin, the following window appears:

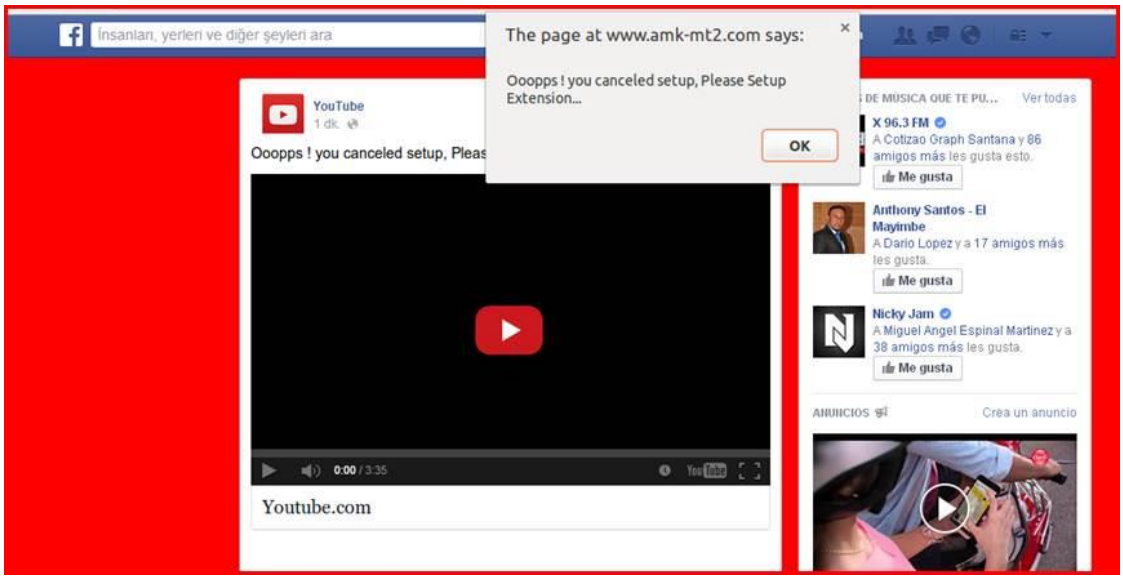

Image 5

CERT-MU wishes to inform you that the **Facebook Video Plugin** has already been removed from Chrome Web Store. However, it is recommended to **NOT TO CLICK** any links when receiving such messages.

Contact Information

To report any incident, you can contact CERT-MU on the following:

Hotline No: (+230) 800 2378

Fax No: (+230) 208 0119

Incident: incident@cert-mu.gov.mu

Website: http://www.cert-mu.org.mu