Kaspersky Lab offers 'Kaspersky Flashfake Removal Tool'

MOSCOW, RUSSIA: As recently published, Kaspersky Lab's experts analysed the Flashfake botnet and found a total of 670 000 infected computers worldwide, with more than 98% of the computers most likely running Mac OS X.

It is anticipated that the other 2% of machines running the Flashfake bot are very likely to be Macs as well. This is the largest Mac-based infection to date, with the largest number of victims targeting developed countries.

Users can check if they're infected with Flashfake by visiting Kaspersky's safe verification site, and can remove it using the Kaspersky Flashfake Removal Tool. By connecting to Flashfake, Kaspersky Lab's experts are able to continuously monitor the botnets communication with active bots and have published their findings.

Bots on the back foot

Kaspersky Lab experts have seen a decline in the number of active bots: on 6 April the total number was 650 748. At the conclusion of 8 April, the number of active bots was 237 103; however, the decrease in infected bots does not mean the botnet is rapidly shrinking. The statistics represent the number of active bots connected to Flashfake during the past few days - it is not the equivalent of the exact number of infected machines. Infected computers that were inactive during this time would not be communicating with Flashfake, thus making them not appear as an infected bot.

Since connecting to the botnet for analysis, Kaspersky Lab's sinkhole server has registered all the data sent by bots from the infected computers and recorded their UUIDs in a dedicated database. Based on this information, Kaspersky Lab's experts have created an online resource where all users of Mac OS X can check if their computer has been infected by Flashback / Flashfake.

How to determine if your computer is infected:

- Visit Kaspersky Lab's site at www.flashbackcheck.com to determine if you're infected.
- This dedicated site is safe for users to visit and enter their UUID, which will be checked in Kaspersky Lab's Flashfake

database of infected computers. Instructions for entering user UUIDs are included as well.

How to disinfect your computer:
If your UUID is found in our database, you need to disinfect your Mac. Here are three recommendations to do this:
1. Use a free special utility, the Kaspersky Flashfake Removal Tool (http://support.kaspersky.com/viruses/utility). It will automatically scan your system and remove Flashback if it is detected. This is a free-to-download and free-to-use program.
2. Download a trial version of Kaspersky Anti-Virus 2011 for Mac. This program offers comprehensive protection against all known malicious programs for Mac OS X, including Flashback.

For more information on the Flashfake botnet and the Flashfake Trojan, go to the FAQ sheet - http://flashbackcheck.com/whatis.html.

To learn about the latest research results by Kaspersky Lab's experts, go to Securelist.