Kaspersky Lab confirms Flashfake/Flashback botnet infection impact

MOSCOW, RUSSIA / JOHANNESBURG, SA: Kaspersky Lab's experts recently analysed Flashfake, a massive botnet that infected more than 600 000 computers worldwide, and concluded that more than 98% of the infected computers were most likely running a version of Mac OS X.

To infect victims' computers, the cyber criminals behind the Flashfake botnet were installing a Flashfake Trojan that gained entry into users' computers without their knowledge by exploiting vulnerabilities in Java. To analyse the botnet, Kaspersky Lab's experts reverse-engineered the Flashfake malware and registered several domain names which could be used by criminals as a C&C server for managing the botnet. This method enabled them to intercept and analyse the communications between infected computers and the other C&Cs.

The analysis showed that there were more than 600 000 infected machines, with the largest regions being the United States (300 917 infected computers), followed by Canada (94 625), the United Kingdom (47 109) and Australia (41 600). Using a heuristic "OS fingerprinting" method, Kaspersky Lab's researchers were able to gauge which operating systems the infected computers were running, and found that 98% were 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.

Cyber criminals use social engineering techniques

Flashfake is a family of OS X malware that first appeared in September 2011. Previous variants of the malware relied on cyber criminals using social engineering techniques to trick users into downloading the malicious program and installing it in their systems. However, this latest version of Flashfake does not require any user-interaction and is installed via a "drive-by download," which occurs when victims unwittingly visit infected websites, allowing the Trojan to be downloaded directly onto their computers through the Java vulnerabilities. After infection the Trojan uploads additional payload which hijacks victims' search results inside their web browsers to conduct a "click-fraud" scam.

Although no other malicious activities have currently been detected by the Trojan, the risk is still significant as the malware functions as a downloader on users' computers, which means the cyber criminals behind Flashfake can easily issue new, updated malware - capable of stealing confidential information such as passwords or credit card details - and install it onto infected machines.

Update now to avoid infection

Although Oracle issued a patch for this vulnerability three months ago, Apple delayed in sending a security update to its customer base until 2 April. Users who have not updated their systems with the latest security should install and update immediately to avoid infection.

"The three-month delay in sending a security update was a bad decision on Apple's part," said Kaspersky Lab's chief security expert, Alexander Gostev. "There are a few reasons for this. First, Apple doesn't allow Oracle to patch Java for Mac. They do it themselves, usually several months later. This means the window of exposure for Mac users is much longer than PC users. This is especially bad news since Apple's standard AV update is a rudimentary affair which only adds new signatures when a threat is deemed large enough. Apple knew about this Java vulnerability for three months, and yet neglected to push through an update in all that time! The problem is exacerbated because - up to now - Apple has enjoyed a mythical reputation for being 'malware free'. Too many users are unaware that their computers have been infected, or that there is a real threat to Mac security."

Mac OS X users are advised to install the latest security updates from Apple.

To learn more about the Flashfake botnet, please visit Securelist to read the latest analysis, written by Kaspersky Lab expert Igor Soumenkov.