BIZCOMMUNITY

Kaspersky Lab uncovered unique 'fileless' bot attacks

MOSCOW, RUSSIA / JOHANNESBURG, SA: A simple teaser of Internet news headlines was the launch-pad for a unique malware attack, with cybercriminals creating malicious code which operated without creating files on the infected system.

Experts from Kaspersky Lab uncovered the hidden attack, which exploited a vulnerability in the teasers used by a number of popular Russian news sources - and warn that similar attacks could be used to target users outside of Russia.

The investigation by Kaspersky Lab shows that Russian media websites using the AdFox teaser system on their pages unwittingly infected visitors to their pages. While downloading the news teaser, the user's browser was secretly redirected to a malicious website containing a Java-exploit. However, unlike standard drive by-attacks, the malicious program was not loaded to the hard drive, but appeared only in the operating memory of the computer, making it much more complicated to track it down using anti-virus solutions.

Stealing confidential user information

Acting as a bot, the malware was sending requests and information about the user's browsing history to a control server. If that data included any sign of using e-banking services, the cybercriminals installed the banking Trojan Lurk to steal confidential user information required to access the online banking systems of a number of major Russian banks.

The investigation has shown, however, that the AdFox network itself was not the source of the infection. News banners were modified by adding links to the malicious website code via the hacked account of an AdFox client. Modifying the code in the teaser system allowed cybercriminals to attack not only visitors to a single news site but also to other resources using the same system. As a result, tens of thousands of potential victims may have been attacked.

'A unique attack'

"We are dealing with a unique attack. A teaser network used by cybercriminals is one of the most effective ways to install a malicious code, as many popular resources contain links to it," says Aleksander Gostev, Kaspersky Lab's chief security expert. "Moreover, for the first time in recent years, we faced a rare type of malware - the so-called 'bodiless' malware which does not exist as a file on the drive but appears in the operating memory of the infected machine, making its detection much more complicated. This incident was targeting Russian users. The same exploit and bodiless bot may well be used against users in other countries as they can be distributed via similar foreign banner and teaser networks. At the same time it's highly probable that not only Lurk Trojan, but also other malware, is used for these purposes."

Despite such programs being able to operate only until the operating system is restarted, it is quite likely that the user will return to the infected news site again. Kaspersky Lab's experts warn that the only reliable protection is the timely installation of updates. In this case, to remove the CVE-2011-3544 Java vulnerability, we recommend installing the Oracle patch - which can be downloaded here.

The detailed results of the investigation by Kaspersky Lab experts are available at www.securelist.com.