Flashback (Trojan)

OSX.FlashBack,[1] also known as the **Flashback** Trojan, **Fakeflash**, or **Trojan BackDoor.Flashback**, is a Trojan horse affecting personal computer systems running Mac OS X.[2][3] The first variant of Flashback was discovered by antivirus company Intego in September 2011.[4]

Infection

According to the Russian antivirus company Dr. Web, a modified version of the "BackDoor.Flashback.39" variant of the Flashback Trojan had infected over 600,000 Mac computers, forming a botnet that included 274 bots located in Cupertino, California.[5][6] The findings were confirmed one day later by another computer security firm, Kaspersky Lab.[7] This variant of the malware was first detected in April 2012[8] by Finland-based computer security firm F-Secure.[9][10] Dr. Web estimated that in early April 2012, 56.6% of infected computers were located within the United States, 19.8% in Canada, 12.8% in the United Kingdom and 6.1% in Australia.[6]

Details

The original variant used a fake installer of Adobe Flash Player to install the malware, hence the name "Flashback".[4]

A later variant targeted a Java vulnerability on Mac OS X. The system was infected after the user was redirected to a compromised bogus site, where JavaScript code caused an applet containing an exploit to load. An executable file was saved on the local machine, which was used to download and run malicious code from a remote location. The malware also switched between various servers for optimized load balancing. Each bot was given a unique ID that was sent to the control server.[6] The trojan, however, would only infect the user visiting the infected web page, meaning other users on the computer were not infected unless their user accounts had been infected separately.[11]

Resolution

Oracle, the company that develops Java, fixed the vulnerability exploited to install Flashback on February 14, 2012.[8] However, at the time of Flashback's release, Apple maintained the Mac OS X version of Java and did not release an update containing the fix until April 3, 2012,[12] after the flaw had already been exploited to install Flashback on 600,000 Macs.[13] On April 12, 2015, the company issued a further update to remove the most common Flashback variants.[14] The updated Java release was only made available for Mac OS X Lion and Mac

OS X Snow Leopard; the removal utility was released for Intel versions of Mac OS X Leopard in addition to the two newer operating systems. Users of older operating systems were advised to disable Java.[12] There are also some third party programs to detect and remove the Flashback trojan.[13] Apple worked on a new process that would eventually lead to a release of a Java Runtime Environment (JRE) for Mac OS X at the same time it would be available for Windows, Linux, and Solaris users.[15] As of January 9, 2014, about 22,000 Macs were still infected with the Flashback trojan.[16]

See also

References

1. **^** This is the name used in Apple's built-in anti-malware software XProtect. Other antivirus software vendors may use different names.
2. **^** 5 April 2012, Flashback Trojan botnet infects 600,000 Macs, Siliconrepublic
3. **^** 5 April 2012, 600,000 infected Macs are found in a botnet, The Inquirer
4. ^ ***a*** ***b*** September 26, 2011, Mac Flashback Trojan Horse Masquerades as Flash Player Installer Package, Intego Security
5. **^** Jacqui Cheng, 4 April 2012, Flashback Trojan reportedly controls half a million Macs and counting, Ars Technica
6. ^ ***a*** ***b*** ***c*** 4 April 2012, Doctor Web exposes 550 000 strong Mac botnet Dr. Web
7. **^** Chloe Albanesius, 6 April 2012, Kaspersky Confirms Widespread Mac Infections Via Flashback Trojan, PCMag
8. ^ ***a*** ***b*** *"Half a million Mac computers 'infected with malware'". BBC. April 5, 2012. Retrieved April 5, 2012.*
9. **^** April 2, 2012, Mac Flashback Exploiting Unpatched Java Vulnerability F-Secure's News from the Lab
10. **^** 11 April 2012, Apple crafting weapon to vanquish Flashback virus, Sydney Morning Herald
11. **^** *Kessler, Topher. "How to remove the Flashback malware from OS X". CNET.*
12. ^ ***a*** ***b*** *"About Flashback malware". Apple. April 10, 2012. Retrieved April 12, 2012.*
13. ^ ***a*** ***b*** *"flashbackcheck.com". Kaspersky. April 9, 2012. Retrieved April 12, 2012.*
14. **^** *"About Java for OS X Lion 2012-003". Apple. April 12, 2012. Retrieved April 12, 2012.*
15. **^** *"Mac Security: A Myth?". eSecurity Planet. April 13, 2012. Retrieved April 16, 2012.*
16. **^** *"It's alive! Once-prolific Flashback trojan still infecting 22,000 Macs". January 9, 2014. Retrieved January 9, 2014.*

External links

Apple Delays, Hackers Play April 12, 2012