Doctor Web doesn't register significant decrease in BackDoor.Flashback.39 bot number

Published: 2012-04-20 · Archived: 2026-04-10 03:05:41 UTC

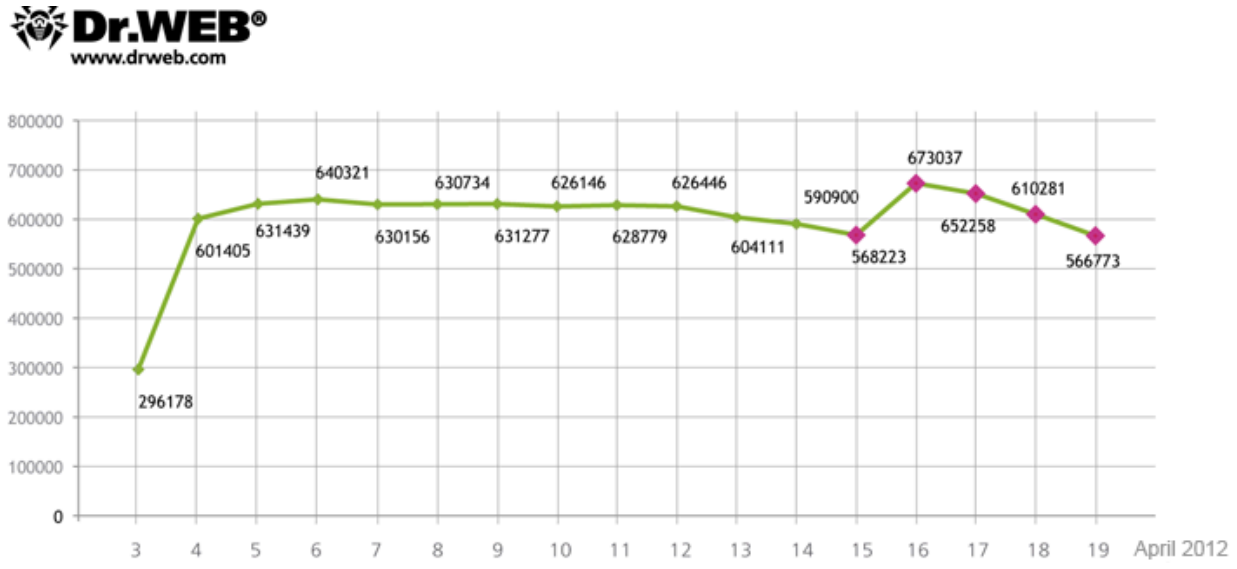
20.04.2012

Hot news | All the news | Virus alerts

April 20, 2012

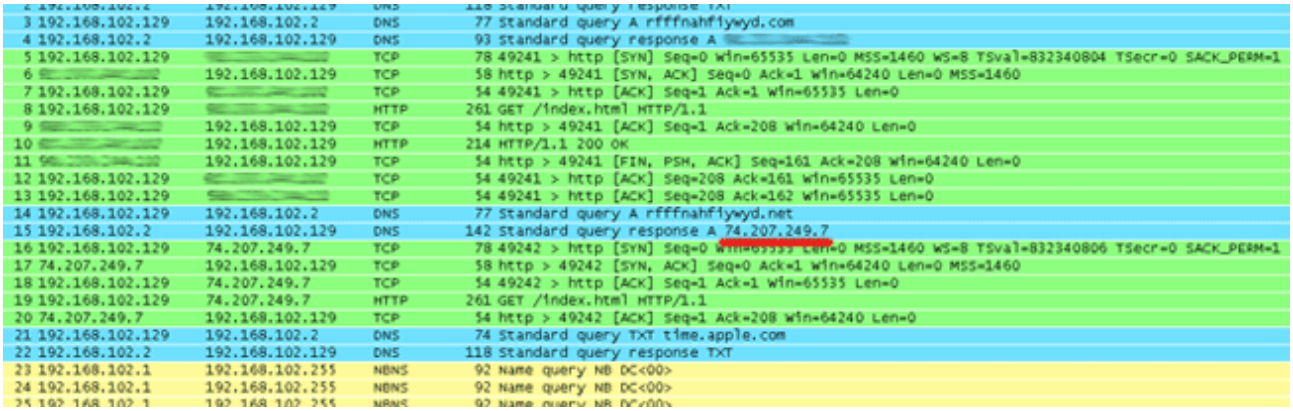
Doctor Web's virus analysts continue to monitor the largest to date Mac botnet discovered by Doctor Web on April 4, 2012. The botnet statistics acquired by Doctor Web contradicts recently published reports indicating a decrease in the number of Macs infected by BackDoor.Flashback.39 The number is still around 650,000.

According to Doctor Web, 817 879 bots connected to the **BackDoor.Flashback.39** botnet at one time or another and average 550 000 infected machines interact with a control server on a 24 hour basis. On April 16, 717004 unique IP-addresses and 595816 Mac UUIDs were registered on the **BackDoor.Flashback.39** botnet while on April 17 the figures were 714 483 unique IPs and 582405 UUIDs. At the same time infected computers, that have not been registered on the **BackDoor.Flashback.39** network before, join the botnet every day. The chart below shows how the number of bots on the **BackDoor.Flashback.39** botnet has been changing from April 3 to April 19, 2012.



However recent publications found in open access report a reduction in the number of **BackDoor.Flashback.39** bots. Typically, these materials are based on analysis of statistics acquired from hijacked botnet control servers. Doctor Web's analysts conducted a research to determine the reasons for this discrepancy.

BackDoor.Flashback.39 uses a sophisticated routine to generate control server names: a larger part of the domain names is generated using parameters embedded in the malware resources, others are created using the current date. The Trojan sends consecutive queries to servers according to its pre-defined priorities. The main domains for **BackDoor.Flashback.39** command servers were registered by Doctor Web at the beginning of April, and bots first send requests to corresponding servers. On April 16th additional domains whose names are generated using the current date were registered. Since these domain names are used by all **BackDoor.Flashback.39** variants, registration of additional control server names has allowed to more accurately calculate the number of bots on the malicious network, which is indicated on the graph. However, after communicating with servers controlled by Doctor Web, Trojans send requests to the server at 74.207.249.7, controlled by an unidentified third party. This server communicates with bots but doesn't close a TCP connection. As the result, bots switch to the standby mode and wait for the server's reply and no longer respond to further commands. As a consequence, they do not communicate with other command centers, many of which have been registered by information security specialists. This is the cause of controversial statistics — on one hand, Symantec and Kaspersky Lab reported a significant decline in the number of **BackDoor.Flashback.39** bots, on the other hand, Doctor Web repeatedly indicated a far greater number of bots which didn’t tend to decline considerably. The image below shows how a TCP-connection to the command center makes a **BackDoor.Flashback.39** bot freeze.



Doctor Web once gain warns Mac OS X users of the **BackDoor.Flashback.39** threat and strongly recommends you to install Java updates and scan the system to determine whether it has been infected. For more information about BackDoor.Flashback detection and neutralization visit https://www.drweb.com/flashback/. To remove the Trojan, you can use Dr.Web for Mac OS X Light available free of charge.

2386 en 5

0

Doctor Web’s Q1 2026 review of virus activity on mobile devices

01.04.2026

Virus reviews

Read

Doctor Web’s Q1 2026 virus activity review

01.04.2026

Virus reviews

Read

Dr.Web for personal computers receives SKD AWARDS product excellence distinction

24.03.2026

Corporate news | Dr.Web products

Read
