The first Trojan in history to steal Linux and Mac OS X passwords

news.drweb.com/show/

Doctor Web

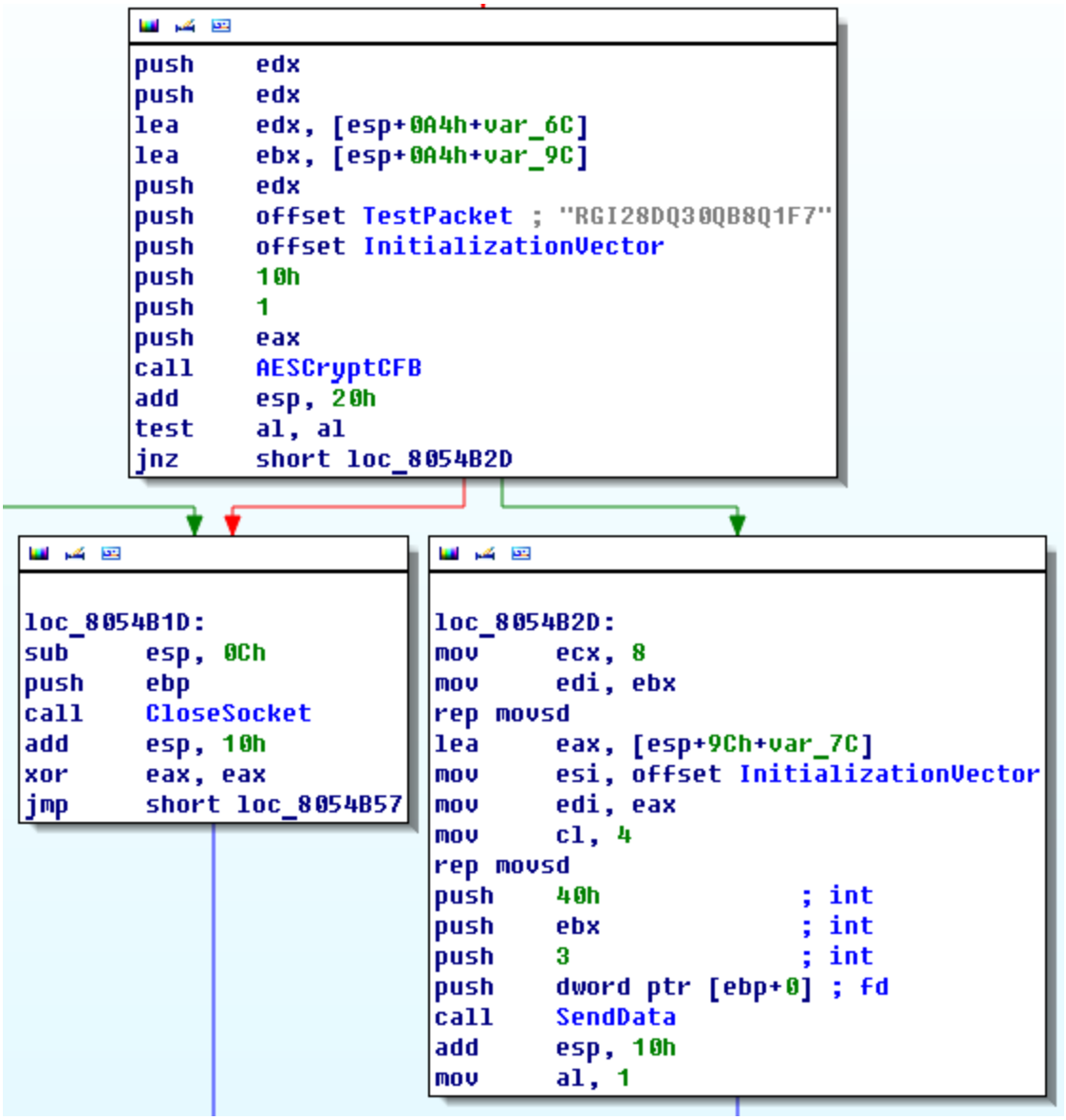
Back to news

August 22, 2012

Russian anti-virus company Doctor Web is reporting the emergence of the first cross-platform backdoor to run under Linux and Mac OS X. This malicious program is designed to steal passwords stored by a number of popular Internet applications. Mac.BackDoor.Wirenet.1 is the first such Trojan capable of running under any of these operating systems.

It's not clear yet how the Trojan, which was added to the Dr.Web virus database as **Mac.BackDoor.Wirenet.1**, spreads. This malicious program is a backdoor that can work under Linux as well as under Mac OS X.

When launched, it creates its copy in the user's home directory. The program uses the Advanced Encryption Standard (AES) to communicate with its control server whose address is 212.7.208.65.



Mac.BackDoor.Wirenet.1 also operates as a keylogger (it sends gathered keyboard input data to intruders); in addition, it steals passwords entered by the user in Opera, Firefox, Chrome, and Chromium, and passwords stored by such applications as Thunderbird, SeaMonkey, and Pidgin. Anti-virus software from Doctor Web successfully detects and removes the backdoor, so the threat does not pose a serious danger to systems protected by Dr.Web for Mac OS X and Dr.Web for Linux.

What is the benefit of having an account?

Tell us what you think

To ask Doctor Web's site administration about a news item, enter @admin at the beginning of your comment. If your question is for the author of one of the comments, put @ before their names.

Other comments