Doctor Web discovers Linux Trojan written in Rust

news.drweb.com/show/

Doctor Web

Back to news

September 8, 2016

Doctor Web's specialists have discovered a new Linux Trojan written in the Rust programming language. The Trojan has been named Linux.BackDoor.Irc.16.

Linux.BackDoor.Irc.16 is a typical backdoor program that executes commands issued by cybercriminals via the IRC (Internet Relay Chat) protocol. The Trojan connects to the public chat channel specified in its configuration and awaits its instructions.

The Trojan can execute just four commands. It can connect to a specified chat channel; send cybercriminals information about an infected computer; send cybercriminals data about the applications running in a system; and delete itself from an infected machine.

Unlike the majority of its counterparts, **Linux.BackDoor.Irc.16** is written in Rust, a programming language whose creation was sponsored by Mozilla Research. Its first stable version was released in 2015. **Linux.BackDoor.Irc.16** was designed to be a cross-platform Trojan—to make a version for Windows, for example, cybercriminals can just recompile this malware program. Doctor Web's analysts believe that Linux.BackDoor.Irc.16 is, in fact, a prototype (Proof of Concept), because it cannot replicate itself, and the IRC channel used by the Trojan to receive commands from cybercriminals is not currently active.

The signature for **Linux.BackDoor.Irc.16** is already in the Dr.Web for Linux database, and it is successfully detected and removed by Doctor Web Anti-virus products.

More about this Trojan

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