

Microsoft takes down major fake drug spam network

March 18 2011



Microsoft on Thursday announced the dismantling of a "notorious and complex" network of virus-infected computers used to send billions of email messages daily hawking fake drugs.

Microsoft on Thursday announced the dismantling of a "notorious and complex" network of virus-infected computers used to send billions of email messages daily hawking fake drugs.

The Rustock "[botnet](#)" consisted of about a million computers that were infected with [malicious code](#) to let hackers covertly control the machines from afar using "command and control" servers.

Owners of infected computers are typically not aware that hackers are using their machines.

"Bot-herders infect computers with [malware](#) in a number of ways, such as when a computer owner visits a website booby-trapped with malware and clicks on a malicious advertisement or opens an infected email attachment," said Microsoft Digital Crimes Unit senior attorney Richard Boscovich.

"Bot-herders do this so discretely that owners often never suspect their PC (personal computer) is living a double life."

Rustock was reported to be among the world's largest spam botnets and was capable of sending as many as 30 billion emails per day.

Much of the email sent by Rustock advertised counterfeit or unapproved knock-off versions of drugs like Viagra, while other spam tried to dupe people with bogus Microsoft lottery notices, according to Boscovich.

Microsoft worked with Viagra-maker Pfizer and network security firm FireEye during a months-long investigation that culminated with using US warrants to seize "command and control" servers in the western state of Washington.

Rustock was knocked offline on Wednesday when the connection was severed between infected computers and the machines used to give them orders, according to Boscovich.

Evidence seized was being analyzed for clues about the hackers and their operations. Microsoft was offering tools at support.microsoft.com/botnets to purge the malware from [infected computers](#).

(c) 2011 AFP

Citation: Microsoft takes down major fake drug spam network (2011, March 18) retrieved 23

April 2024 from <https://phys.org/news/2011-03-microsoft-major-fake-drug-spam.html>

This document is subject to copyright. Apart from any fair dealing for the purpose of private study or research, no part may be reproduced without the written permission. The content is provided for information purposes only.