

OpenOffice worm attacks the operating system

Security firm Symantec warned a malicious code to attack OpenOffice.org could infect many different operating systems and be hacked to the Internet.

Security firm Symantec warned a malicious code to attack OpenOffice.org could infect many different operating systems and be hacked to the Internet.

Information from Symantec Security Response indicates that the aforementioned malicious code is a computer worm attached to malicious OpenOffice files spread by email. This worm is capable of infecting Windows, Linux and Mac OS X operating systems.

This computer worm was discovered late last month. But at the time, security experts said they were not spread widely on the Internet.



If the user opens the worm file OpenOffice **badbunny.odg** will immediately be started with a macro that defines the operating system that the user is using.

If it is a Windows operating system, the worm will implant a file called ' **drop.bad** ' into the system. The main function of this file is to move the system file the system.ini into the mIRC folder. It also implements a **badbunny.js** JavaScript that replicates other files in the directory it exists.

On Mac OS X, the worm implements two Ruby Script viruses called ' **badbunny.rb** ' and ' **badbunnya.rb** '. The

Linux system is infected with two XChat Script ' **badbunny.py** ' and Perl Script ' **badbunny.pl** ' viruses .

Symantec rated the new OpenOffice worm as a medium risk. Security companies recommend that users should not open OpenOffice files sent from an unknown source.

Hoang Dung

You finished reading the article "**OpenOffice worm attacks the operating system**" edited by the [TipsMake](#) team. We hope this article has provided you with many useful tech tips and tricks. You can search for similar articles on tips and guides. Thank you for reading and for following us regularly.