

The new worm 'digs' a Windows vulnerability

A new worm with the name Win32 / Conficker.A is spreading quite strongly in the network of computers that install Windows operating systems

A new worm, called Win32 / Conficker.A, is spreading quite aggressively in the network of Windows-based computers, drilling into a security hole that Microsoft has patched in the October Security Bulletin.

According to the announcement from the software giant, the number of attacks has increased rapidly within the past few days.

All aimed at an extremely serious (critical) vulnerability that was originally handled in **MS08-067** .

The Conficker.A worm mostly spreads inside corporate networks, but it also attacked hundreds of home computers, Microsoft said on the Malware Prevention Center Blog.

This worm opens any port of any number from 1024 to 10000 and operates as a Web server.

It randomly spreads to computers in the network by exploiting the MS08-067 vulnerability.

Once the computer has been punctured, it will automatically download a deep copy of the HTTP route, based on the previously opened random port.

Mechanism



Source: **Security Labs** Conficker.A often uses a file with a .JPG extension when cloned, then it saves to the "Local system" folder under the name of the dll.

" One thing to keep in mind is that Conficker.A will fix the API vulnerability inside the memory, making the computer more secure.

It's not that hackers are "interested" in your computer, but he just wants to be assured that no other malware will take over the computer, "added Microsoft.

Most infected computers are located in the United States. But Microsoft has also received reports from Germany, Spain, France, Italy, Taiwan, Japan, Brazil, Turkey, China, Mexico, Canada, Argentina and Chile.

But for some reason, the Conficker.A worm has always avoided spreading inside Ukrainian computers, Microsoft said.

In addition to Conficker.A, the vulnerability is also being attacked by another malware called Backdoor: Win32 / IRCbot.BH.

The malware will release a backdoor trojan into the computer, allowing the trojan to connect to the remote IRC server and receive commands from hackers.

You finished reading the article "**The new worm 'digs' a Windows vulnerability**" 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.