Conficker's victim has reached 7 million

Security experts estimate that there are about 7 million computers infected with Conficker worldwide.

***Network* security experts estimate that there are about 7 million computers infected with Conficker worldwide.**

Yesterday, researchers at the Shadowserver Foundation tested a series of computers from more than 7 million different IP addresses, all of which were infected with user-known variants of Conficker.

Researchers can track the spread of Conficker by deciphering the algorithm used by the worm to search for instructions on the Internet and to include them in isolated servers on the Internet domains that are made Process to invade. Conficker receives instructions in many different ways, so they can still take control of the computer, but based on isolated servers, researchers can statistically count the number of infected computers.

Andre Deminno, co-founder of Shadowserver Foundation, commented that Conficker might be a well-known computer worm, but many computers continue to be infected. He said *'The number of computers infected with Conficker is increasing and this number has reached 7 million.'*

Conficker caught the attention of security experts for the first time in November last year, and in early 2009 many media also paid attention to this dangerous computer worm. Conficker has demonstrated a special ability to restore itself and is very skilled in making the system infected even though it has been destroyed.

This computer worm is very popular, especially in China and Brazil. Members of the Conficker Working Group,

an affiliate group formed last year to deal with the worm, suspect that many infected computers are illegally using copies of Microsoft's Windows operating system, therefore, it will not be possible to download the Microsoft Malicious Software Removal Tool patches or tools that can eradicate this worm.

Although the influence is quite large, Conficker is rarely used by hackers to control it. Researchers cannot explain this reason. Some members of the Conficker Working Group speculated that Conficker's author might want to draw attention only by spreading it.

Eric Sites, chief technology officer of Sunbelt Software and a member of the Working Group, said: *'I think the one who created Conficker is' cowardly'. Many companies and computer users have to spend a lot of money and energy to deal with this worm, and if they find out who has caused it, they will have a sad consequence. '*

IT staff often detect a Conficker infection when the user suddenly cannot log on to the computer. That's because infected computers will try to connect to other computers on the network and constantly guess passwords on these computers, repeated times will cause those computers to be locked out of the network. .

However, Conficker can do much more if it is used in distributed denial of service (DDoS) attacks.

DeMinno said *'This is a botnet that can be armed. When there is this amount of botnet, you will be able to do a lot of things. '*