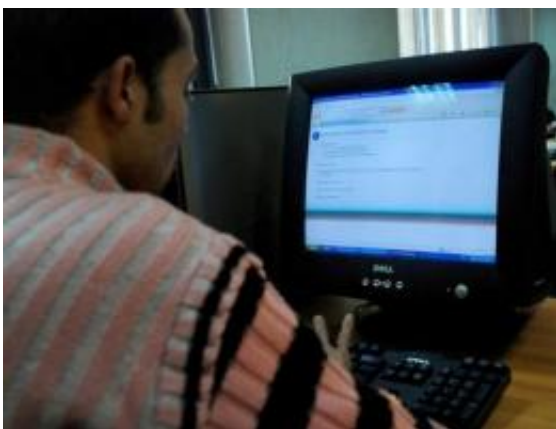# New homeland security tool to detect Conficker worm

March 30 2009

The US Department of Homeland Security released a tool to detect whether a computer is infected by the Conficker worm

The US Department of Homeland Security released a tool on Monday to detect whether a computer is infected by the Conficker worm.

The department, in a statement, said the detection tool for the Conficker worm, also known as DownAdUP, had been developed by the US Computer Emergency Readiness Team (US-CERT).

"While tools have existed for individual users, this is the only free tool -- and the most comprehensive one -- available for enterprises like federal and state government and private sector networks to determine the extent to which their systems are infected by this worm," said US-CERT

director Mischel Kwon.

"Our experts at US-CERT are working around the clock to increase our capabilities to address the cyber risk to our nation's critical networks and systems, both from this threat and all others," he added.

The worm is suspected to have infected million of computers running the [Windows operating system](#) and Windows maker Microsoft has offered a 250,000 dollar bounty for those responsible for the worm.

US-CERT recommended that Windows users apply Microsoft security patch MS08-067 to help provide protection against the worm.

The patch is designed to prevent an attacker from remotely taking control of an infected computer system and installing additional [malicious software](#).

Malware could be triggered to steal data, generate spam attacks or turn control of infected computers over to hackers amassing "zombie" machines into "botnet" armies.

The worm is programmed to modify itself on Wednesday, April Fool's Day, according to [computer security](#) specialists.

Conficker had been programmed to reach out to 250 websites daily to download commands from its masters, they said, but on Wednesday it will begin connecting with 50,000 websites daily for instructions.

The hackers behind the worm have yet to give it any specific orders.

"That's the interesting thing. The only thing the worm is being asked to do is to ask for further instructions," Steve Trilling, vice president of security firm Symantec, told the CBS program "60 Minutes" in a story

aired on Sunday.

More information:

-- US-CERT recommends that Windows Operating Systems users apply Microsoft security patch MS08-067 ([www.microsoft.com/technet/secu … lletin/MS08-067.mspx](www.microsoft.com/technet/secu)) as quickly as possible to help protect themselves from the worm.

-- Instructions, support and more information on how to manually remove a Conficker/Downadup infection from a system have been published by major security vendors. Each of these vendors offers free tools that can verify the presence of a Conficker/Downadup infection and remove the worm:

Symantec:
[www.symantec.com/business/secu … =2009-011316-0247-99](www.symantec.com/business/secu)
Microsoft:
support.microsoft.com/kb/962007
[www.microsoft.com/protect/comp … worms/conficker.mspx](www.microsoft.com/protect/comp)

(c) 2009 AFP