

## The Hindu Business Line\_ Computer worm Conficker spreading fast\_April 10'09

<http://www.thehindubusinessline.com/2009/04/11/stories/2009041150910300.htm>

### Computer worm Conficker spreading fast

The worm exploits vulnerability in the Windows Server Service used by Windows 2000, XP, Vista, Server 2003, 2008 and Windows 7 Beta.  
R. Savitha

Pune, April 10 April 1 was a terrifying day for many Windows customers as the updated variant of Conficker, also known as Downup, hit the screens.

The worm exploits vulnerability in the Windows Server Service used by Windows 2000, XP, Vista, Server 2003, 2008 and Windows 7 Beta.

Mr Govind Rammurthy, Managing Director and Chief Executive Officer, MicroWorld, told Business Line: "Conficker is spreading fast and it auto updates itself via downloads from random domains, making it almost impossible to stop as whatever countermeasures come out it can just download itself the latest version and bypass them. Close to 30,000 domains have been identified and blocked."

He said that Conficker limits itself to 50,000 possible domain names to find its rendezvous point to get updates. Until those domain names are registered, they are up for grabs. On a daily basis, Conficker will randomly generate 500 domain names from among its pool of 50,000 possible names. It will try to connect to all of those 500. If it fails, it will try again tomorrow. If it connects, it will download update files to run and get its new orders from the author of the worm.

He noted that it also has multiple infection vectors, including travelling via USB drives. Conficker has slithered on to as many as 12 million Windows computers by February 2009.

The highest number of affected computers are in China (2,62,082), followed by the Russia (1,91,052), Brazil (1,76,901) and India (1,22,338). The least affected is Bulgaria with 10,134 infections. Infections were also reported from Japan (11,050), Turkey (11,369), the US (30,369) and Taiwan (38,656). Conficker has struck in 28 countries. Mr Rammurthy said that India stood fourth in the number of infections worldwide as on January 29.

Mr Govind said that infections of a worm that spread through low-security networks, memory sticks and PCs without the latest security updates was "skyrocketing".  
Infection rate

The malicious program – known as Conficker, Downadup, or Kido – was first discovered in October 2008. It has a high infection rate – in October 2008 the infection was 9 million and it reached 12 million in January 2009, a rate of one million infections a month. He noted that the updated variant had expanded to generate 50,000 domains from which 500 are queried on a less frequent basis. "On top of attempting to kill security processes, it also blocks Web traffic to certain domains, including Fortinet. Additionally, it will block security updates such as Windows updater – killing a good portion of patch management practices," he said.

He said that eScan, the security software from MicroWorld, had been successful in preventing the damage since Conficker was detected.

eScan 10 provides comprehensive protection against viruses, worms, trojans, spyware and other security threats. It also provides protection from threats infecting via email, downloads and chatting, among others, by its faster and heuristic scanning ability. The inbuilt advanced firewall also prevents systems from network-based attacks. MicroWorld is the only Indian AV company to provide solutions in India and its worldwide customer base for Conficker.

According to a Symantec note given to Business Line, a mitigation option was now available to effectively bypass the Conficker domain blocking feature that prevents a user on an infected machine from accessing a security site to get a fix tool. The user can go to DOS prompt and type "net stop dnscache", which disables the DNS cache. The user will get a message that the DNS client service is stopped and can proceed to access the security Web site or download the fix tool.