

The Salt Lake Tribune

Worm infecting millions of Windows-based computers

Updated: 01/23/2009 04:22:39 PM MST

In the most severe outbreak in years, a computer worm continues to spread after infecting millions of personal corporate computers and servers.

The worm is called Downadup or Conficker, and takes advantage of a Microsoft Windows vulnerability. About 1.2 million networks were contaminated as of Thursday, said Mikko Hypponen, chief research officer at Helsinki-based Internet security software maker F-Secure Oyj.

The worm has been found in Utah computers, said Thomas Olsen, owner of CMIT Solutions of Sandy, which provides computer services to small- and medium-sized businesses.

"We saw it on one of our clients, one of their PCs," said Olsen,

The program is spread through devices like flash drives that pick it up from an infected computer and spread it to another, or by e-mails or from Web sites.

The worm can affect operations of infected computers but its aim may be to steal personal information. It can sit unnoticed on computers for some time before it is activated to try to obtain personal information.

"It'll pop up with a box that says your antivirus software is out of date. 'Please give me your credit card and we'll update it for you,'" Olsen said.

It also can infect cameras and other devices that are plugged into computers, he said.

Microsoft released a patch for the security flaw exploited by Downadup in October. Customers who think they have the worm can also download the free Malicious Software.

Removal Tool at <http://www.microsoft.com/security/malwareremove/default.aspx>, according to a Microsoft statement.

Olsen said antivirus programs like those from Symantec's or McAfee can remove the worm from personal computers. But they might not always be effective and the last resort is to reinstall the computer's operating system, he said.

tharvey@sltrib.com