

# Conficker virus begins to attack PCs:

Mon Apr 27, 2009 9:02am EDT

By [Jim Finkle](#)

BOSTON (Reuters) - A malicious software program known as Conficker that many feared would wreak havoc on April 1 is slowly being activated, weeks after being dismissed as a false alarm, security experts said.

Conficker, also known as Downadup or Kido, is quietly turning thousands of personal computers into servers of e-mail spam and installing spyware, they said.

The worm started spreading late last year, infecting millions of computers and turning them into "slaves" that respond to commands sent from a remote server that effectively controls an army of computers known as a botnet.

Its unidentified creators started using those machines for criminal purposes in recent weeks by loading more malicious software onto a small percentage of computers under their control, said Vincent Weafer, a vice president with Symantec Security Response, the research arm of the world's largest security software maker, Symantec Corp.

"Expect this to be long-term, slowly changing," he said of the worm. "It's not going to be fast, aggressive."

Conficker installs a second virus, known as Waledac, that sends out e-mail spam without knowledge of the PC's owner, along with a fake anti-spyware program, Weafer said.

The Waledac virus recruits the PCs into a second botnet that has existed for several years and specializes in distributing e-mail spam.

"This is probably one of the most sophisticated botnets on the planet. The guys behind this are very professional. They absolutely know what they are doing," said Paul Ferguson, a senior researcher with Trend Micro Inc, the world's third-largest security software maker.

He said Conficker's authors likely installed a spam engine and another malicious software program on tens of thousands of computers since April 7.

He said the worm will stop distributing the software on infected PCs on May 3 but more attacks will likely follow.

"We expect to see a different component or a whole new twist to the way this botnet does business," said Ferguson, a member of The Conficker Working Group, an international alliance of companies fighting the worm.

Researchers had feared the network controlled by the Conficker worm might be deployed on April 1 since the worm surfaced last year because it was programed to increase communication attempts from that date.

The security industry formed the task force to fight the worm, bringing widespread attention that experts said probably scared off the criminals who command the slave computers.

The task force initially thwarted the worm using the Internet's traffic control system to block access to servers that control the slave computers.

Viruses that turn PCs into slaves exploit weaknesses in Microsoft's Windows operating system. The Conficker worm is especially tricky because it can evade corporate firewalls by passing from an infected machine onto a USB memory stick, then onto another PC.

The Conficker botnet is one of many such networks controlled by syndicates that authorities believe are based in eastern Europe, Southeast Asia, China and Latin America.

(Editing by Jason Szep and Philip Barbara)

© Thomson Reuters 2009. All rights reserved. Users may download and print extracts of content from this website for their own personal and non-commercial use only. Republication or redistribution of Thomson Reuters content, including by framing or similar means, is expressly prohibited without the prior written consent of Thomson Reuters. Thomson Reuters and its logo are registered trademarks or trademarks of the Thomson Reuters group of companies around the world.