Mysterious virus quiet, but attack may be in works

Malicious software that has infected millions of computers across the globe failed to wreak havoc on Wednesday as some feared, but researchers warned the powerful Conficker worm could still strike.

Also known as Downadup or Kido, Conficker turns infected PCs into slaves that respond to commands sent from a remote server that effectively controls an army of computers.

The fears of an attack, however, may have been a windfall for anti-virus software makers, who warned consumers about the worm, industry analysts say.

Symantec Corp, McAfee Inc and Trend Micro Inc spend millions of dollars a year on promotional campaigns that warn about threats to personal computers.

"A scare like this could make consumers think twice before deciding to let their subscriptions lapse," said FBR Capital Markets analyst Daniel Ives.

The industry had been under pressure because the recession caused some customers to hold off buying new software and others to delay renewing subscriptions.

Researchers feared the network created by Conficker might be deployed on Wednesday for the first time since the worm surfaced last year because it was programed to increase communication attempts with its master server from April 1.

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

That group thwarted the worm partially by using the Internet's traffic control system to block access to servers that control the slave computers. But in cases where the slaves did connect, they did not receive new marching orders.

Researchers warned the botnet's commanders are probably waiting until they are under less scrutiny before they mobilize the network of infected computers.

"I never thought it would happen April 1," said Roger Thompson, chief research officer at AVG, an anti-virus firm. "It might be tomorrow. It might be next week. It might be next month."

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.

While the Conficker botnet is still inactive, analysts say millions of machines in other networks are regularly ordered to perform tasks for their masters.

The botnet's owners often sell the slaves or rent them out, offering services such as credit-card and banking information theft. They can be customized to perform other tasks, such as knocking down websites and bringing down corporate networks.

"The worst thing is that no one really knows what these things can do. These things can be programed to do anything," said Mel Morris, CEO of anti-virus company Prevx.

Analysts say Conficker garnered unprecedented attention in recent days because it is unusually large -- most have no more than a few million slaves -- and because it was coded to mutate on April Fool's Day.

While estimates vary greatly, researchers say tens of millions of machines are compromised without the knowledge of their owners.

Alfred Hunger, a senior researcher with Symantec, thinks Conficker has the stamina to survive several years. He believes the motives of the army's commanders are the same as those of the other botnets in cyberspace.

"I think it will be a fairly vanilla botnet," he added.

New York Times, New York, 1 abr. 2009, Technology, online. Disponível em <www.nytimes.com>. Acesso em: 2 abr. 2009.