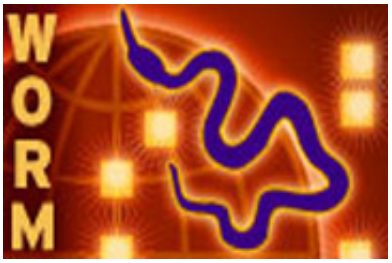
Conficker Worm Prepares For A New Release On April 1

March 27 2009, by John Messina



(PhysOrg.com) -- The conficker worm created havoc last year when it infected over 10 million computers on a global scale. The unique design of the conficker worm allowed for this large scale attack to over 8 million business computers and scores of individual computers in 2008.

The conficker worm is periodically evolving by downloading updates that creates thousands of false domains daily to throw off security investigators. On the day it chooses to update, it selects 500 correct domains out of the 50,000 candidates to download malware and updates from.

• **On the first release** it tried to download and execute a file called loadav.exe. It turned out that the file was never uploaded and the next generation did away with this. This led investigators to believe it was a malware program trying to promote itself as fake antivirus software.

• **The second release**, the worm used Windows Services, on unpatched machines, to spread. This new release also had the power to spread over network shares by trying to log in autonomously into network machines with weak passwords. It developed the ability to infect USB sticks connected to infected machines, giving it another means of transmission.

• **On the final and third release**, which became know as the Downadup virus, peer-to-peer communication between infected systems was added to it's arsenal of weapons. The virus also added new domain-generation algorithms to help it disguise where it was receiving its updates from.

Microsoft is offering a bounty for the worm's writers and security experts are no closer to having any clue as to the individual or individuals who are writing the Conficker code.

As Conficker continues to spread and get smarter, there is little doubt it's creating an army of infected machines, one that can cause serious damage. On April 1 we will see the attacks be taken to the next level. One can only guess what this next release has in store for the Global Internet Community.