The Raging Windows Worm has attacked over 8.9 Million Computers

January 19 2009, by John Messina

(PhysOrg.com) -- Last week the global internet community was hit by the Downadup worm also know as Conficker, or Kido. This worm is now using multiple ways of infecting computers, including USB sticks. If someone were to take a USB memory stick from one infected computer and plug it into another, it would infect that computer and the network as well. Once a USB memory stick is infected, there is no Microsoft patch to remove the worm.

This attack has been more widespread on corporate networks because companies did not have the patch installed in time. This could have been caused by any number of reasons. For instance an IT Department may have been short handed or have workload related issues preventing the patch from being installed in a timely manner. Microsoft did a good job in having home computers updated with the patch but corporate networks are still being infected.

This worm is very sophisticated because it exploits multiple secure flaws in Microsoft's Windows OS's. The worm starts by injecting itself into one of Microsoft's common system process, services.exe. From there it creates a new random five letter DLL file in the Windows system folder. The Windows registry is then edited to make reference to the DLL file and runs when the computer is restarted.

Once the worm is in the computer system, it creates an HTTP server and proceeds to download malware from the hacker's websites. System restore has been wiped clean and reset on the computer making it impossible to restore your system prior to the infection.

Each day there are hundreds of dummy domain names being generated by an algorithm coded in the worm but only one site is the actual malware site. With this trickery employed, it makes it very difficult to find what is being installed each day.

This worm spreads mainly through corporate networks. An infected computer will scan the network for other computers and gain access through the Windows secure flaw. Even though a password is needed to gain access to other computers, it will guess short passwords by brute force method thereby gaining access to those computers.

The only way to stop this worm is by applying Microsoft's patch MS08-067 before computer networks get infected.