Protect Your Computer From Downadad

A new sleeper virus that could allow hackers to steal financial and personal information has now spread to more than eight million computers in what industry analysts say is one of the most serious infections they have ever seen.
The Downadup or Conficker worm exploits a bug in Microsoft Windows to infect mainly corporate networks, where -- although it has yet to cause any harm -- it potentially exposes infected PCs to hijack. Mikko Hypponen, chief research officer at anti-virus firm F-Secure, says while the purpose of the worm is unclear, its unique "phone home" design, linking back to its point of origin, means it can receive further orders to wreak havoc. He said his company had reverse-engineered its program, which they suspected of originating in Ukraine, and is using the call-back mechanism to monitor an exponential infection rate, despite Microsoft's issuing of a patch to fix the bug. "On Tuesday there were 2.5 million, on Wednesday 3.5 million and today [Friday], eight million," he told CNN. "It's getting worse, not better."Hypponen explained to CNN the dangers that Downadup poses, who is most at risk and what can be done to stop its spread.How serious is it?It is the most serious large scale worm outbreak we have seen in recent years because of how widespread it is, but it is not very serious in terms of what it does. So far it doesn't try to steal personal information or credit card details.
affected?We have large infections in Europe, the United States and in Asia. It is a Windows worm and almost all the cases are corporate networks. There are very few reports of independent home computers affected.
is a complicated worm most likely engineered by a group of people who have spent time making it very complicated to analyze and remove. The real reason why they have created it is hard to say right now, but we do know how it replicates.
How does it spread?The worm does not spread over email or the Web. However if an infected laptop is connected to your corporate network, it will immediately scan the network looking for machines to infect. These will be machines that have not installed a patch from Microsoft known as MS08-067. The worm will also scan company networks trying to guess your password, trying hundreds and hundreds of common words. If it gets in, even if you are not at your machine, it will infect and begin spreading to other servers. A third method of spreading is via USB data sticks. How can I p
infecting my machine?The best way is to get the patch and install it company-wide. The second way is password security. Use long, difficult passwords -- particularly for administrators who cannot afford to be locked out of the machines they will have to fix. What can I do if it has already infected? Machines can be disinfected. The pro
companies with thousands of infected machines, which can become re-infected from just one computer even as they are being cleared. Source : CNN.