Downadup Worm Hits Over 3.5 Million Computers

January 16 2009, by John Messina

(PhysOrg.com) -- Security firm F-Secure has advised that the Downadup worm has spread to more than 3.5 million computers by exploiting a vulnerability Microsoft patched last October. This is achieved by trying to connect to various Web addresses. The worm then looks for an active Web server at one of these domains and downloads and runs a particular executable file. This allows the malware to do whatever it wants with all of the infected computers.

The Downadup uses a complicated algorithm which changes daily and is based on timestamps from public websites such as Google.com and Baidu.com. The worm then generates many possible domain names every day.

Names such as: qimkwaify .ws, mphtfrxs .net, gxjofpj .ws, imctaef .cc, and hcweu .org. It would be impossible to shut them all down because there's just too many and most of them aren't even registered. The bad guys running the show only need to register one domain for the day, register it, and set up a website. From there they can gain access to all of the infected machines.

In order for the F-Secure Response Team to determine just how many machines are infected, they will register some of the possible domains and connect to the infected machines.

Right now the Response Team is seeing hundreds of thousands of unique IP addresses connecting to the domains they have registered. A large portion of that traffic is coming from corporate networks, through firewalls, proxies, and NAT routers. This clearly shows that one unique IP address can be connected to thousands of corporate machines.

All this could have been avoided if more users had patched the vulnerability in how Windows processes remote procedure call (RPC) requests by the Windows Server service. Microsoft issued a critical out-of-band patch, bulletin MS08-067, to fix this problem.

Microsoft Security Bulletin MS08-067:
www.microsoft.com/technet/secu … lletin/MS08-067.mspx

© 2009 PhysOrg.com

Citation: Downadup Worm Hits Over 3.5 Million Computers (2009, January 16) retrieved 9 April 2024 from https://phys.org/news/2009-01-downadup-worm-million.html

This document is subject to copyright. Apart from any fair dealing for the purpose of private study or research, no part may be reproduced without the written permission. The content is provided for information purposes only.