Veteran Worm re-invents itself

Submitted by: MJO Associates
Thursday, 15 January 2009

Win32.Worm.Downadup uses new tricks to spread itself without being easily detected

BUCHAREST, Romania – January 15, 2009 – Win32.Worm.Downadup, a worm which spreads by exploiting a vulnerability in the Windows RPC Server Service, has been detected by BitDefender®. The Downloadup worm (also called Conficker or Kido) made its first appearance late November 2008, exploiting the MS08-067 vulnerability to spread unhindered in local area networks. Its purpose was to install rogue security software on infected computers.

In late December, BitDefender Labs uncovered a new version of the worm called Win32.Worm.Downadup.B. The malware features some enhancements to its characteristics, as well as the distribution routine.

The worm uses USB sticks to infect other computers. It operates by copying itself in a random folder created inside the RECYCLER directory. This is used by the Recycle Bin to store deleted files, and creat an autorun.inf file in the root folder. The worm executes automatically if the Autorun feature is enabled.

Certain TCP functions are also patched to block access to security-related websites by filtering every address that contains certain strings. This makes it harder to remove since information about it is virtually impossible to gather from an infected computer. Additionally, it removes all access rights of the user, except execute and directory usage, to protect its files.

Antivirus detection is avoided by working with rarely used APIs (application programming interface) in order to circumvent virtualization technologies. The worm disables Windows updates and certain network traffic, optimizing Vista features to ease distribution.

The Win32.Worm.Downadup.B malware comes with a domain name generation algorithm similar to the one found in botnets like Rustock. It composes 250 domains every day and checks some of them for updates or other files to download and install.

Commenting on this new outbreak, head of BitDefender Anti-Malware Labs, Viorel Canja said: “This malware exploits the fact that many people do not patch their systems. With its updated configuration and good protection scheme, this worm could become a rival to already established botnets like Storm or Srizbi.”

For more technical details please visit the Malwarecity Blog at: http://www.malwarecity.com/blog.html and the BitDefender description: http://www.bitdefender.com/VIRUS-1000462-en--Win32.Worm.Downadup.Gen.html

About BitDefender®
BitDefender is the creator of one of the industry's fastest and most effective lines of internationally certified security software . Since its inception in 2001, BitDefender has continued to raise the bar and set new standards in proactive threat prevention. Every day, BitDefender protects tens of millions of

home and corporate users across the globe — giving them the peace of mind of knowing that their digital experiences will be secure. BitDefender solutions are distributed by a global network of value-added distribution and reseller partners in more than 100 countries worldwide. More information about BitDefender and its products are available at the company's security solutions press room. Additionally, BitDefender's www.malwarecity.com provides background and the latest updates on security threats helping users stay informed in the everyday battle against malware.
# # #

Contact details:

Mike Ottewell
MJO Associates for BitDefender UK
Tel: 01538 361217
E-mail: mottewell@bitdefender.co.uk

Nick Billington
BitDefender Country Manager
(UK and Ireland)
Tel:08451305096
E-mail:nbillington@bitdefender.co.uk
Fax:- 0845 130 5069