



## FAQ: Conficker (aka Downadup) worm

### What is the Conficker worm?

The Conficker worm (aka Downadup) and its variants made headlines at the beginning of 2009 when more than nine million PCs were infected worldwide. The worm was first discovered in November 2008. The worm exploits the [MS08-067](#) vulnerability in the Windows Server Service and propagates itself quickly over a network. Although a patch from Microsoft has existed for this vulnerability since October, delays in applying the patch allowed for such widespread infection. However, even companies that rely on patches alone to protect their networks are finding that, in the case of this worm, their patching process may fail to prevent large-scale infection of network machines.

### What systems are infected?

The following systems are infected: Windows 2000, Windows 95, Windows 98, Windows Me, Windows NT, Windows Server 2003, Windows Vista and Windows XP.

### How does it enter a system?

The worm uses several methods to spread apart from exploiting the vulnerability in Windows Server Service. It also attempts to propagate throughout a network by guessing passwords using brute force as well infecting USB devices, such as memory sticks.

After gaining access to a computer or system the worm installs itself by adding randomly-named dynamic link libraries (.dll) into the system directory, including a system service to be able to execute itself. Registry settings are also created to hide the creation of the service.

### What happens then?

The virus then starts finding ways to spread through local networks using brute-force techniques on usernames and passwords. The worm thus attempts to exploit any weak passwords on the network. Furthermore, the worm will try and copy itself to any external devices that are attached to the network. These include external hard drives, flash memories and memory cards etc. The worm creates a special autorun file to trick users into browsing the contents of the external device.

### What will happen to my system?

Although the worm does not cause specific damage to your system it does disable a number of services that make it hard to remove. For example, account lockout policies are tripped while automatic updates, Background Intelligent Transfer Service (BITS), Windows Defender and Error reporting services are disabled. The worm also causes domain controllers (DC) to respond slowly to client requests and congestion can be seen on the network. Finally, a number of security-related Websites cannot be accessed.

### Can something happen in future?

Some security experts believe that the Conficker worm may only be dormant and it has the capacity to cause damage if it is triggered to release a malicious payload. A computer that has been infected with the worm begins to generate hundreds of web domains and attempts to connect to them daily to download an executable. The risk is that hackers or spammers may use these addresses to insert a malicious executable with any payload they wish. Damage could include the execution of code on a vulnerable system, Denial of Service (DoS) attacks and vulnerable machines being used in a huge botnet.

### How can I protect my systems from being infected?

First of all make sure that your systems have been updated with the latest patches from Microsoft, especially the critical patch released by the company in October 2008 to address the vulnerability. Also ensure that your anti-virus is up-to-date and that you have a firewall installed (inbound and outbound traffic).



## FAQ: Conficker (aka Downadup) worm

Patching alone is not enough to eliminate the risk. Since the worm infects external devices and network shares using the autorun file, administrators need to disable the autorun feature. This is easily achieved by editing group policy:

Go to Start and select Run. Type the command: gpedit.msc. This will open the Group Policy window. Select Computer Configuration – Administrative Templates – System. Under System, double-click the Turn Off AutoPlay in the right hand pan. Then select Enable and choose All Drives from the menu. This will prevent the worm from executing itself when an infected USB is connected to the network.

Since the worm also attempts to propagate itself by using brute-force techniques on usernames and passwords, administrators should instruct all employees to change their password and ensure that these passwords meet the minimum requirements, i.e. alpha-numeric passwords with at least eight (8) characters. Weak passwords have aided the distribution of the worm in companies.

### Do GFI's products provide protection against the worm?

GFI products can help SMBs to protect their networks from the Conficker worm and myriad threats that exist.

This infection has highlighted the importance of fully patched systems and that administrators taking too long to install patches are only increasing the risk of infection or worse. GFI's answer is to install a vulnerability management product like **GFI LANguard** which allows administrators to scan, identify and assess vulnerabilities in servers or workstations and then take the required action by, for example, downloading missing security updates or critical patches from Microsoft. The software's network auditing function will also identify weak passwords. A company running GFI LANguard would have drastically reduced the risk of infection from the Conficker worm.

Portable and external devices such as USB sticks are an administrator's nightmare unless these are properly controlled. Using **GFI EndPointSecurity**, for example, an administrator can restrict the use of portable devices, restrict read/write privileges as well as specify which brand / make of device is allowed to be connected to the network.

Hackers and virus writers always seek the path of least resistance and nothing is simpler to crack than a password that is weak – a fact that the Conficker worm has been designed to exploit. Apart from enforcing strict password policies, you can install **GFI EventsManager** to monitor security event logs and alert you to any unusual log on activity and multiple attempts to log on to numerous accounts.

The worm is constantly trying to download modified versions of itself from a list of randomly generated websites. As there are hundreds of different domain names that could be used, it is impossible to locate and block them all in time. With **GFI WebMonitor**, all downloads are checked for viruses and malware. If a download or website is found to contain malicious payloads, GFI WebMonitor will block that file or script.

The creation of this massive botnet serves no other purpose but to generate a massive spam and malware distribution network. An indirect impact of the worm this may be but still of concern due to the volume of spam/malware that could flood email servers. Installing **GFI MailEssentials** and **GFI MailSecurity** on email servers will block over 99% of spam and with five anti-virus engines running, the risk of malware infection is greatly reduced.