



# Conficker Yourself Informed!

*By: Steve Norbury, VMS Hardware Manager*

Yep, that's a caricature of me at the top and yep, I don't deny it's a good likeness, accurately portraying me as the once hard lined RAF policeman of 15 years and now as the bastion of the VMS Hardware Support department of some 10 years. Irritating I often am. Rude, never intentionally. stubborn and argumentative, maybe sometimes. I speak my mind but with the interests of my/VMS clients being at the forefront of my work ethics, you'll never get anything more than "the truth, the whole truth and nothing but the truth" and 100% effort to meet your expectations. Right that's you informed and my introduction out of the way but have I got your attention? This is important!

For those of you who don't know, there is a virus/worm out there. Named "Conficker" (also referred to as "DownAdUp"), it's unwelcome presence is currently being felt on an estimated 15 million PC's worldwide and the number of reported infections is growing at a speed hitherto unseen on a daily basis. More than 3,000 British organisations – including hospitals, the Ministry of Defence, councils, and what are described as "well-known firms" – have been hit. They and the hundreds of thousands of other victim organisations in countries such as the US, Russia, China and India are now bracing themselves for the virus to be triggered and do whatever malicious work it has been designed to do. Yes, you read right, at the time of writing, the worm has no payload. In other words whilst it infects systems it currently causes no more harm than that of being a nuisance causing any one or more of the following symptoms;

- Account lockout policies are being tripped resulting in users being unable to logon to the network/domain.
- Automatic Updates, Background Intelligent Transfer Service (BITS), Windows Defender, and Error Reporting Services being disabled.
- Domain controllers responding slowly to client requests.
- The network/Internet traffic being slow and congested.
- Various security-related Web sites cannot be accessed.
- Up to date AntiVirus clients constantly reporting the infection regardless of whether the end user elected to delete the infected file during a previous notification.

There remains the possibility that Conficker has no function other than to demonstrate its originator's skill, but many security experts think it unlikely a worm so sophisticated has no ulterior purpose. Many believe this could be to capture confidential information, such as online account details and passwords, but it is more likely to be a "rootkit", which gives the virus designer administrative access – effectively, control over the computer and then, perhaps, its network. However, such is the sophistication of the worms code and the way in which it reports it's presence to other Internet hosts, it is possible that the worm authors or others could re-engineer it's code and employ "Internet bots" armed with any malicious instruction and inflict untold widespread damage to network infrastructures.

## **Now have I got your attention?**

Within the last month I have had the unpleasant fortune to witness the worm first hand (the unpleasantness bears no reflection of the worms hosts (thanks Steve and Mark for your hospitality during the four days spent on site eradicating the varmint from the network). During those four days the sophistication of the worm became very apparent such that once infected, re-infection was all too easy with the methods of re-infection being numerous such as via USB memory sticks and other external media including attaching infected mobile phones/memory cards (the worm creates an infected Autorun.inf file and then exploits the Operating Systems' inherent abeyance of the Autorun facility), through to open file and printer shares, hidden tasks schedules and general access to the internet. Without careful planning and a methodical approach, re-infection can take micro seconds and can undo hours/days of work. This is one virus/worm where a "One Click and it's gone" solution is not possible.

So how did infections on this scale start?

The worm, which does not affect Apple Macs, exploits a vulnerability in Windows, for which Microsoft provided a security patch as long ago as October 2008. Many companies and organisations did not install it because they were worried about disrupting their existing setup. A version of Conficker (W32/conficker.A) began circulating at the same time as Microsoft released its patch, but had little effect. However, the lack of updating left a huge security hole which hackers abruptly exploited in mid-January when a new version of a "worm" (w32/Conficker.b) that exploited the weakness appeared, apparently written by the same team that wrote the original. Amongst other routines/methods, the new worm attempts to crack the passwords of machines on a network using the computing power of the infected machine to apply a "brute force" approach – so that passwords such as "admin", "password" or "123456" (and numerous other common/easy passwords) on potential target machines will quickly be broken.

Once it has infected a machine, the software also tries to connect to up to 250 different domains with random names every day. Researchers believe that one of them will be the intended "control" domain, and that when the computers connect to it they will download a fresh program that will take over the infected computer.

The Conficker worm is now in its third incarnation (W32/Conficker.b++ although some antivirus organisations are identifying it as W32/Conficker.c) with increased infection and re-infection capabilities but still no destructive payload.

So here comes the important bit and the main purpose of this "From The Techies" article. To safeguard from infections of this and future malicious programs, it is important that all servers and PC's employed within your organisation are updated with the latest Microsoft Windows updates and security patches released by Microsoft on a regular basis. Internet Explorer can be configured to check and download Windows updates automatically with the options to have the updates installed immediately (which may invoke an automatic reboot) or updated at next shutdown or when instructed manually. Where updating windows on such a scale is not possible then at the very least the following two Windows updates should be downloaded and installed;

Microsoft Security Bulletin MS08-067 at <http://www.microsoft.com/technet/security/bulletin/MS08-067.msp>

How to correct "disable Autorun registry key" enforcement in Windows at <http://support.microsoft.com/kb/967715>

Unfortunately, whilst Windows Updates installs a patch to allow for the disabling of the autorun facility of attached devices such as USB and flash based memory cards (in mobile phones etc), the technote above should be followed manually to disable the functionality either from the server using Group Policies or an individual PC basis.

In addition to Windows Updates, Antivirus solutions should be scheduled to check and download definition files on a regular basis. Antivirus solutions in their own right cannot rid or prevent the infection they predominantly deal with the infection that they can see or have been instructed to seek out. It is important therefore to periodically verify that such updates are taking place (we have seen above, one of the traits of this virus is to block access to Antivirus websites to prevent updates of this nature taking place).

Finally one more tip, consider employing the use of strong passwords on the network. Further information about strong passwords can be found at;

<http://www.microsoft.com/uk/athome/security/privacy/password.msp>

Other informative and technical details about the Conficker virus/worm can be found at;

<http://www.microsoft.com/protect/computer/viruses/worms/conficker.msp>