FEATURE

RESCUE ME 2: DISINFECTION WITH BOOTABLE RESCUE MEDIA

Andreas Marx
AV-Test.org, Germany

These days, it is not an uncommon occurrence for a PC to become infected by a virus or worm, or for a backdoor to be installed on one's PC – at the time of writing, for example, *Trend Micro*'s free online virus scanner has found more than 1.6 million PCs infected with W32/Mydoom.A.

There is, and there always will be a time delay between the initial detection of a worm and the release of anti-virus definition updates (see *VB*, February 2004, p.4). Heuristics and the generic proactive malware detection techniques used by anti-virus products do not always work – for example, no AV scanner was able to detect W32/Sober.C or W32/Mydoom.A without updated signatures.

There may be an even longer delay between an anti-virus signature update being made available and the end user applying the update to his software. This is compounded by the problem that a lot of retail AV products for home users, such as *Norton AntiVirus 2004* and *McAfee VirusScan*, cannot be updated with non-administrator rights on *Windows XP*-based systems.

Malware infections can be rather complex. These days, it is not simply a case of removing a 'worm.exe' file (along with a registry key in the 'Run' section or an entry in the win.ini file – things a lot of anti-virus programs still omit to do). A lot of current malware threats, for example W32/Sober (see *VB*, December 2003, p.7), try to hide themselves from other applications or have self-protection mechanisms that prevent removal tools from working properly.

A number of current threats (for example, W32/Oror.C) attempt to deactivate or even delete any anti-virus software that is running on the infected machine – this is very easy considering that few anti-virus programs have any form of self-protection.

Some worms, like W32/Mydoom.B, change the *Windows* 'hosts' file so that certain websites cannot be reached. To my knowledge, no anti-virus program is able to check for (or remove) suspicious entries in the 'hosts' file. This means that the anti-virus product cannot easily be updated, and therefore is less likely to be able to detect the threat that has infected the PC.

It is essential, therefore, to have a good rescue (and/or backup/restore) solution that does not rely on the infected *Windows* system. This article – which is an update to the 'Rescue me' article in the May 2002 issue of *VB* (see *VB*, May 2002, p.10) – focuses on end-user products.

Some recovery solutions can be started from the installation CD, while others need to be created manually. This may call for up to nine disks in the case of *Norton AntiVirus* or a single CD-R/RW in the case of *G Data AntiVirusKit (AVK)*. Here, the CD image with up-to-date signatures is created using Mkisofs and burned using Cdrecord, both of which are available as free software for *Windows* (see http://www.fokus.gmd.de/research/cc/glone/employees/joerg.schilling/private/cdrecord.html). Maybe we will see rescue USB sticks in the not too distant future.

Today's rescue solutions can be classified into three main categories: DOS, *Linux* and *Windows* (*PE*)-based. In most cases, NTFS is supported only in read-only mode.

DOS-BASED SOLUTIONS

Most rescue media, like those from *Grisoft AVG*, *Command AntiVirus*, *Computer Associates eTrust*, *McAfee VirusScan* and *Norton AntiVirus*, are still based on DOS. This is useful if one wants to disinfect a boot virus, which is not possible when *Windows NT*-based systems are running because they deny access to this critical boot area. However, DOS incarnations support only FAT16 or FAT32 drives (e.g. FreeDOS, http://www.freedos.org/, or MS-DOS).

Some tools, such as *Norton AntiVirus*, claim that they have scanned all hard drives and found no infected files, despite the fact that the system only has NTFS drives which the product cannot scan at all.

Another problem is that most DOS-based rescue systems are extremely outdated. For example, the installation CD of *Norton AntiVirus 2004* from September 2003 is bootable, but contains signature files dating from mid-2001. The rescue disk that a user can create in *McAfee VirusScan* boots 'Dr Solomon's Magic Bullet' (the doctor has not left town, he is still alive!) with signatures from March 2000.

There are NTFS add-on drivers available, such as Winternals (NTFSDOS/NTFSDOS Professional, http://www.winternals.com/) or Active Data Recovery Software (NTFS Reader for DOS, http://www.ntfs.com/), but in the freeware editions they are only able to provide read-only support, and the products with both read and write support usually cost more per licence than the anti-virus product itself. In most cases, only file access is allowed, but the *Windows* registry cannot easily be modified.

Furthermore, memory limitations mean that it is almost impossible to get network drivers and a TCP/IP stack (for product updates) as well as the NTFS drivers, plus the AV program running at the same time. Therefore, DOS is no longer a good solution for scanning or cleaning if one is dealing with more than a boot sector or master boot record.

LINUX-BASED SOLUTIONS

The number of *Linux*-based rescue solutions has increased considerably over the last couple of months. *Central Command Vexira Antivirus* (available free of charge as an ISO image at: ftp://ftp.centralcommand.com/antivirus/rescue_disk/), *G Data AVK*, *BitDefender*, *H+BEDV AntiVir Professional*, *Kaspersky Anti-Virus*, *Norman Virus Control* and *Panda AntiVirus* are all based on *Linux*.

The good news is that *Linux* has no problems with read and write access to FAT16 or FAT32 drives. Read-only access to NTFS drives works too, however there are a couple of problems with write access to NTFS drives.

AVK is still based on *Linux* kernel 2.2.14 and it uses a 1998 beta version of *Kaspersky*'s *AVP* for *Linux* to scan a system. Unfortunately this old kernel cannot handle *Windows 2000* and *XP* NTFS5 very well, and will crash on the first EFS-encrypted file. This old kernel also has problems with Serial ATA (SATA) drives: it simply will not see them.

Kaspersky Anti-Virus and *Panda AntiVirus* are based on 2.4.x kernels with a minimal *Linux* system that fits on one floppy disk. *AntiVir* and *Vexira* are only slightly different: these products use a CD-R instead of a floppy disk.

BitDefender and *Norman Virus Control* are based on *Knoppix-Linux* (http://www.knopper.net/), a *Linux* distribution that can be started completely from the bootable installation CD. *Knoppix* attempts to detect all attached devices automatically and load the correct drivers. It works with both the 'older' 2.4.x and the more up-to-date 2.6.x *Linux* kernels. While the original *Knoppix* distribution includes several additional applications such as *OpenOffice*, the *BitDefender* version includes only the graphical user interface KDE (Kommon Desktop Environment, http://www.kde.org/) and the scanner itself. *Norman* has reduced the *Knoppix* installation even further, with its system based on a text console only.

However, even if NTFS drives can be read and scanned for malware, there is still the problem that infections cannot be removed. The NTFS drivers in the latest *Linux* kernel 2.6.x (http://linux-ntfs.sourceforge.net/) are good enough to replace files with other files safely if both files have the same name and length. Therefore, it's possible to remove 'malware.exe' and replace it with a helper file that completely repairs the system when *Windows* starts. This way, registry keys can easily be repaired as well.

Most of today's malware files are big enough to accommodate being replaced with well-working cleaner utilities. In order to make sure the replacement file has the same size as the malware being replaced, the rescue AV tool can simply add a few 0x00 or random bytes at the end. Another option would be to replace the 'malware.exe' file with a special file that triggers the detection of the *Windows* part of the AV program and the files can be successfully cleaned as well.

An alternative method that would avoid all these problems would be the use of *Captive* (http://www.jankratochvil.net/project/captive/), a free, fully-read/write NTFS driver for *Linux*. It uses the *Linux* kernel NTFS drivers to read the ntfs.sys and a few other *Windows* system files and finally it loads the native *Microsoft* NTFS driver. A more detailed description of the process can be found at http://www.amunra.co.uk/archives/000028.php.

Use of the native *Microsoft* drivers is a good way to avoid all the compatibility problems with the undocumented features of NTFS, but one should keep in mind that it's not a trivial task to load *Windows* drivers on *Linux*. For example, the *BitDefender* rescue media uses *Captive* to gain read and write access to NTFS partitions, but the beta version we used for testing was not yet able to remove a malware file from NTFS drives – probably due to a bug in the 'disinfect' or 'delete' program options.

If one uses *Linux*, the rescue media can be updated very easily: with all of the built-in drivers, it is easy to get a network card running in order to download updates from http or ftp sites, from SMB shares of other computers or even to grab the definition files which are stored on the HDD already.

WINDOWS (PE)-BASED SOLUTIONS

All of the aforementioned rescue tools share the problem that they are based mainly on reverse engineering of the file systems, regardless of whether they are FAT or NTFS, or that a lot of work-arounds and tricks need to be employed in order to get them working.

Microsoft has its own *Windows*-based solution, *Windows PE*, which can be started from a read-only medium, such as a CD-Rom. A lot of backup and rescue tools such as *Winternals Administrator's Pak* (http://www.winternals.com/products/repairandrecovery/) or *Symantec*'s *Powerquest V2i Protector* (http://www.powerquest.com/v2i/protector/sbe/) use *Windows PE* already.

Alwil Software has created the BART CD (Bootable Anti-Virus and Recovery Tools – see http://www.asw.cz/), which is also based on *Windows PE*. This not only includes a virus scanner which is able to read and write NTFS partitions without any problem, but it contains a disk checker, a registry editor, a file manager, plus a text editor.

All of these tools share one problem however: while they are easy to develop, because they are based on *Windows* and support most parts of the *Windows* API, they are also

expensive, because *Windows PE* licences are neither cheap nor easy to obtain.

It is possible that Bart Lagerweij thought of this when he developed *PE-Builder* (http://www.nu2.nu/pebuilder/), which is similar to *Windows PE*, but is free. Lagerweij used a number of components of the original *Windows PE* system in the first version of *PE-Builder* but, at *Microsoft*'s request, removed this version from his website. According to the author, today's versions are fully legal – as long as the user creates his own, personal CD from his own computer's *Windows XP* (SP1) or *Windows Server 2003* system. Lagerweij has developed his own additions and tools in cooperation with other developers worldwide and, in some areas, *PE-Builder* provides much more functionality than *Microsoft*'s own *Windows PE* (see http://www.www.nu2.nu/pebuilder/#plugins for details).

However, not all programs will run on *Windows PE* – in particular the more complex tools have problems. *SureBoot* (available for a 'rather small' licensing fee, see http://www.sureboot.com) could solve this problem. *SureBoot* can automatically create a backup copy of a user's specific *Windows 2000*/*XP* environment (including all drivers, specific user profiles, and AV/backup software), which boots and runs *Windows* from a hidden hard disk directory and can be burned onto a CD/DVD. Complex applications such as *Word*, *Excel*, *Outlook* and *IE* work as well.

After an infection, the virus definitions can be updated using standard *Windows* Internet connection services. The infected, non-running, but accessible *Windows* system can then be repaired directly from *SureBoot* with full NTFS and registry read and write capabilities, based on *Microsoft*'s own drivers. Most applications will run without problems and they won't see any differences, regardless of whether they are working on a real *Windows* system or a *SureBoot*-created rescue CD/DVD. Unfortunately, this solution is likely to be 'too big' for AV-only rescue media – but, combined with other rescue and administration tools, it could be very useful.

CONCLUSION

Recently malware has increased in complexity. The cleaning of an infected PC is becoming a harder task, especially if the malware 'kills' the AV product or prevents it from updating itself. We need better rescue solutions urgently. Today's DOS-based disks won't work any more, due to the lack of NTFS support. There are still lots of *Windows 9x*/*Me* systems in use that can be disinfected successfully. However, the number of *Windows 2000* and *XP* installations is growing fast and with it, the use of NTFS as the standard file system. I hope that we will see more really innovative products like *Alwil*'s BART CD in the near future.