FEATURE 1

THE SOBER EFFECT: DISINFECTION DISASTERS

Andreas Marx
AV-Test.org, University of Magdeburg, Germany

Despite going almost unnoticed by the rest of the world, Win32/Sober hit a lot of computers in Germany. The worm's trick was rather simple: social engineering using a German email subject and message body (instead of English text, which is more suspicious here) to entice the user into double-clicking on the attachment.

Once started, the worm displays the message, 'Error: File not complete!'. It collects all email addresses it can find on the PC and sends itself with a BAT, COM, EXE, PIF or SCR attachment to these addresses using a built-in SMTP engine. The file the worm sends out is not constant, but some random data will be appended every time it is sent out and the MIME structures of the mails are sometimes heavily corrupted and likely to fool (i.e. bypass) email scanners. However, Win32/Sober is not only an email worm; it also propagates via the *KaZaA* 'My Shared Folder' by overwriting existing files in this folder. The worm was written in a German version of Visual Basic and packed with a modified version of UPX (http://upx.sourceforge.net/) to complicate its analysis. These facts suggest it's likely that the virus author lives in a German-speaking country.

SELF-PROTECTION OF THE WORM

Win32/Sober uses a few interesting tricks to make its detection and disinfection quite difficult. On *Windows 9x*/*Me* and *NT*/*2000*/*XP* systems there are always two processes of the worm running and the worm checks the status of the other worm process every few milliseconds. If the user or another program terminates one process, the second process of the worm will restart the task. So Win32/Sober cannot easily be killed in memory by using the *Windows* task manager, for example.

On *Windows NT*-based systems the worm uses a stealth-like trick to hide itself from detection by anti-virus programs. The worm's EXE files are located in the Windows System (*Win9x*/*Me*) or System32 (*Win NT*/*2000*/*XP*) folder. The two tasks open the EXE files exclusively (non-shared). Like the *Windows* swap file, these cannot be opened by other programs for inspection – and, of course, this includes virus scanners. On an infected PC, most AV tools will silently skip the two worm files without any warning or will report something along the lines of: 'Cannot open file. Skipped.'

As a result of its protection mechanism, disinfection of the worm in memory is a little tricky. At first, the two worm tasks have to be suspended, so that they are no longer able to check each other. Only once this has been done can both tasks be killed. Any disinfection program that skips the suspend action will likely kill only one task, which is immediately restarted by the other and so on, so the memory disinfection will fail.

The virus adds a key in the usual 'Run' parts of the registry at HKEY_LOCAL_MACHINE and HKEY_CURRENT_USER so that it will be started on every reboot of the system. The worm tasks check the existence of this key every few milliseconds and restore the settings if the key has been deleted or changed.

Once the worm has successfully been killed in memory, of course, it is very easy to delete all worm files on the local disk and the added registry keys.

For an unknown reason the worm always creates a copy of itself in the System folder (when running on *Windows 9x*/*ME*) or System32 folder (when running on *Windows NT*/*2000*/*XP*) with the name 'similare.exe'. This copy is not protected and can easily be scanned and killed. However, at the next reboot the worm will create the file again, so it's just an indicator of an infection – and virus scanners can use this file to report an infected system and are able to disinfect it, too, even if they are not able to scan the memory. For this, they would only need to add a 'delete files' entry in the wininit.ini file of *Windows 9x*/*Me* systems to delete the two possible worm files (i.e. in the simplest case just using a list of the known names of the executables the virus uses) and restart the PC. After this, the cleaner can remove the registry keys of the now deleted worm files and can scan for other traces of the worm on the formerly infected PC (e.g. the file which actually caused the initial infection).

On *Windows NT*-based systems the disinfection steps to delete or rename the worm files during start-up are slightly different, but similar. However, this method always requires a reboot, so it would be easier and faster to disable the worm in memory at the start of the scan and to delete all worm files on the PC after this.

TESTING TIMES FOR WIN32/SOBER CLEANING

Due to the fact that most 'out-of-the-box' virus scanners are not able to detect or clean the Win32/Sober worm reliably, a number of special cleaner utilities were released by various anti-virus companies. Because of the tricky disinfection of this worm, combined with a high number of infection reports in Germany, we were interested in testing how well these clean-up tools performed.

We tested nine cleaner utilities on the German versions of *Windows 98 Second Edition* (with *Office XP* installed to get the worm working on this platform, because it requires a Visual Basic runtime DLL), and *Windows XP SP1*. Every product test was performed three times on both *Windows 98* and *XP* and the platforms were recreated to a known state using *Symantec Ghost Image* files. After a run of the tool (plus a reboot, if needed), we inspected the PC to see whether it was indeed worm-free and whether the registry keys created by the worm were removed, too.

AntiVir Sober Removal Tool

The special fix-up tool from *H+BEDV* in Germany runs only at the command-line: if one starts it with the help of *Windows Explorer*, it will open a DOS box which closes immediately. Only if one starts it with a parameter like 'C:\Windows' (location to scan) will it start working, detect the worm reliably in memory, disinfect it there, and start to scan the PC for the worm. However, in our tests the registry keys were not removed. On *Windows 98* the version of the tool we tested contained a bug which prevented it from working most of the time: if the user wanted to scan 'C:' or 'C:\' the tools wouldn't scan the whole hard disk, but would silently do nothing. *H+BEDV* has already released a new version of the tool in which all of the above problems have been fixed.

Avast! Virus Cleaner

This tool is not only designed to kill Sober, but it can be used against a couple of other worms, too. Neither on *Windows 98* nor on *Windows XP* did we encounter any problems: the tool worked as it should and detected and killed the worm in memory and later on the disk. The registry keys were removed, too. This is what we would expect from a proper disinfection tool.

BitDefender Sober Removal Tool

BitDefender's tool worked well only on *Windows 98*, even if the disinfection required a restart of the PC. But on *Windows XP* the cleaner was not able to detect the worm in memory and therefore it missed the two 'hidden' worm files and only found and deleted the unprotected similare.exe file. Even when the scanner reported that it had 'successfully cleaned' the PC, Sober was still active and running. According to the developers, this problem has been fixed in the latest version of the tool.

McAfee Stinger

Using *McAfee Stinger* one can rid the PC of various worms which are tricky to disinfect. The disinfection only worked on *Windows 98*. The tool did not scan memory reliably on *Windows XP* and it missed Sober in some cases. As with the *BitDefender* cleaning tool, the worm was not removed after an apparently 'successful' cleaning operation. *Network Associates* has now updated *Stinger* to work reliably on *Windows XP*.

NOD32 Sober Disinfection Tool

This tool is labelled as 'NOD32 disinfection tool', however it was not developed by *Eset*, but by their Italian distributor Paolo Monti. Like the *BitDefender* and *Stinger* tools, it worked reliably on *Windows 98*, and after a reboot the worm was gone. However, the registry keys were not removed. On *Windows XP* the worm was still active after a virus 'cure'. According to the developer an updated version is now available for download, in which the reported problems have been fixed.

Panda PQRemove

Like *McAfee Stinger*, *PQRemove* by *Panda Software* is able to disinfect a couple of common worms. But for this operation its 1.3 MB file size is much too large. The disinfection works properly on *Windows 98* and *XP*, but in some rare cases (likely caused by a bug in the worm) the tool will leave a null byte file created by the worm plus a registry key on the system. A new version of the tool which handles this situation well is already available.

Safetysoft Sober-Killer

It was a little surprising to discover that not all disinfection tools are free-of-charge and used to advertise their own scanner or security products. This one is sold for 6.50 Euros plus one Euro for shipping – by email(!). We expected something special here, but on *Windows 98* the tool did not work at all, leaving the PC infected and virtually unusable (the cursor only blinked heavily on such a 'disinfected' PC and the system had a high workload)! Multiple disinfection attempts, combined with reboots did not fix the problem. On *Windows XP* the tool worked. At the time of writing the developer is still investigating the problem.

Symantec W32.Sober@mm Removal Tool

The *Symantec* cleaning tool is as easy as it is useful: after a run of the tool the worm was disinfected successfully on *Windows 98* and *XP*. This is how a clean-up tool should perform.

Trend Micro Worm Cleaner

Like *McAfee Stinger*, the worm clean-up tool from *Trend Micro* is not only effective against Win32/Sober infections, but helps against various other worms, too. Like *PQRemove* it is quite large (1.3 MB). It runs only at the command-line, but a user needs only to double-click on the EXE file to start an automatic scan and clean process. Due to the lack of feedback (no information is displayed on screen about infections found or removed), it is most useful for companies as part of network log-in scripts, but it is not designed for home users. However, the worm was cleaned successfully in all cases and the registry keys created by the worm were removed.

CONCLUSION

I was really rather surprised to find that two thirds of the so-called cleaner tools we tested did not work at all. It seems as if they were released in a hurry without proper testing. Maybe some virus researchers saw only that the similare.exe had been found and deleted successfully and concluded that the worm disinfection worked. I hope that such a debacle won't happen again and that proper system disinfection abilities will be built into the standard anti-virus program versions in the near future. However, it was good to see that (with the exception of two companies) the tools available on the AV companies' web pages were already fixed at the time of writing.

Download addresses

AntiVir Sober Removal Tool
Size: 35 KB
Download address: http://www.antivir.de/vireninfo/sober.htm

Avast! Virus Cleaner
Size: 262 KB
Download address: http://www.avast.com/i_idt_171.html

BitDefender Sober Removal Tool
Size: 63 KB
Download address: http://www.bitdefender.com/bd/site/virusinfo.php?menu_id=1&v_id=163

McAfee Stinger
Size: 714 KB
Download address: http://vil.nai.com/vil/content/v_100778.htm

NOD32 Sober Disinfection Tool
Size: 297 KB
Download address: http://www.nod32.ch/download/tools.stm

Panda PQRemove
Size: 1334 KB
Download address: http://www.pandasoftware.com/virus_info/encyclopedia/overview.aspx?idvirus=41441

Safetysoft Sober-Killer
Size: 305 KB
Download address: http://www.schutzsoftware.info/

Symantec W32.Sober@mm Removal Tool
Size: 191 KB
Download address: http://www.symantec.com/avcenter/venc/data/w32.sober@mm.html

Trend Micro Worm Cleaner
Size: 1322 KB
Download address: http://www.trendmicro.com/vinfo/virusencyclo/default5.asp?VName=WORM_SOBER.A