

Safe as houses

Malware programs are finding new ways to sneak round firewalls, virus scanners and system tools to cause havoc on your PC. Jörg Geiger explains how this is done and provides some effective counter-measures so you can ensure your system is watertight

In theory Windows computers should be as secure as the Bank of England. Firewalls have never been as effective, virus scanners have never been so capable and spyware scanners have never been as widespread as they are today. The major proviso is that your security software has to be properly configured. Microsoft's Service Pack 2 for Windows XP introduced the Security Center, which reassured users that it was looking after their data and computers with automatic virus scanning and Updates. Unfortunately, this is misleading: in practice, Windows is like a crumbling building with cracks appearing all the time.

Malware finds new entry points

Research by the Computing Technology Industry Association (www.comptia.org) has shown that new threats adjust themselves according to the security measures in use. They simply look for new loopholes and weak points in the system. For example, targeted browser attacks increased by nearly 60 per cent in 2004 and 'phishing' attacks by about a quarter. Malware doesn't try to crudely break through firewalls any more, but uses more refined methods of attacking

At your own risk!

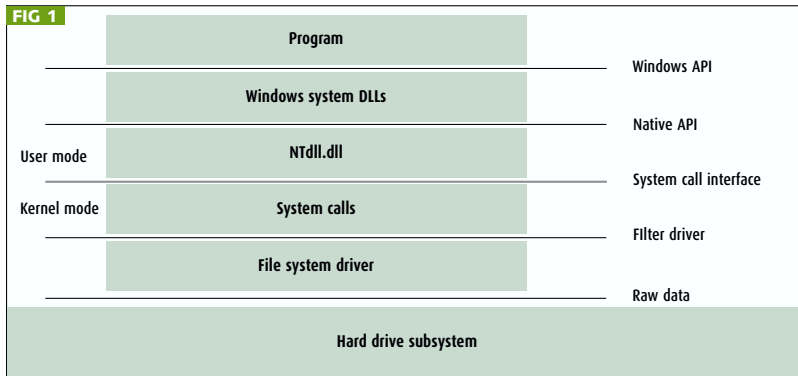
In this feature, we'll point out some of the back doors in Windows XP. However, you should be aware that experimenting with rootkits and the debugging tools can lead to stability problems. If you are going to experiment, it's best to use either a virtual machine (using Microsoft's Virtual PC trial version, for example) or a computer on which no important data is stored. You have been warned.



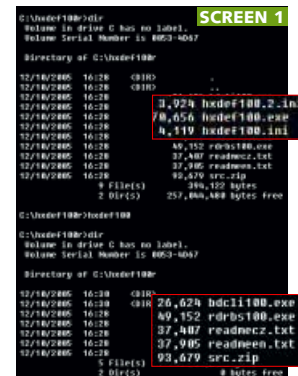
your PC. These include 'rootkits' that malware uses to sniff out loopholes. These rootkits are smuggled in through cracks in Windows or by unmonitored downloads. Mikko Hyppönen, chief research officer at Finnish company F-Secure, thinks powerful Windows rootkits could develop into a real problem. 'Rootkit programs gain access to all the data on a system and could cause chaos unnoticed,' he said. We'll explain later how these attackers behave and how you can protect yourself.

It's almost unbelievable that Microsoft's preferred file system, NTFS, allows files of

any size to be hidden using a little-known compatibility feature, Alternate Data Streams (ADSs), without leaving any traces. These data streams are also used in Vista, Microsoft's forthcoming operating system, which is based on NTFS. With a few exceptions, virus and spyware scanners will also ignore these hidden files. Later in this feature, there's information on tools you need to track down these files and step-by-step instructions on how to use them.



The Windows API is made up of layers – a fact that is often exploited by rootkits – and different search tools are needed for each hiding place



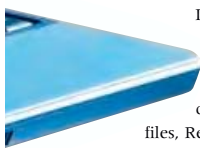
Hacker Defender hides all files with the character sequence hxd in their names

Cracks in Windows uncovered

Windows XP has more surprises: hidden user accounts, invisible file shares, readable password databases and hidden Registry keys are just the tip of the iceberg. For some hints on how you can plug those Windows security holes see page 115.

DANGEROUS ROOTKITS

Just when you think you've secured your PC using a virus scanner and a firewall, a new threat emerges. Using sophisticated techniques, rootkits burrow themselves into Windows and hide various malware programs. They not only deceive system tools, but also trick virus scanners and anti-spyware programs: they're parasites that are almost invisible to Windows.



In themselves, rootkits are not forbidden or particularly harmful. They simply allow processes, services, directories, TCP/IP ports, files, Registry entries or drivers to be hidden within the operating system. The catch is that malware can use this method too. There are already some viruses, such as Maslan or Padodor, which use rootkits to hide themselves. Since they camouflage themselves so well, this sort of threat is often referred to as a stealth virus.

Until now, the amount of malware using rootkits for disguise has been kept down to a reasonable level, although the source code for creating them is freely available. Some kits, for example, are available at www.rootkit.com including Hacker Defender and NT Rootkit. Information about the capabilities of programs like these can make a real difference to limiting the growing threat malware poses to a wider public.

Misdirected communication

The first rootkits for Unix were quite primitive in construction (see box below, 'The invisible threat') and no longer pose a challenge for up-to-date virus scanners. However, the new rootkits, which clearly have Windows in their sights, can hide malware in the system with alarming efficiency. They do this by applying leverage to the Windows APIs (application programming interfaces) which supply applications with information. The rootkits then, unnoticed, manipulate the communication between the system components, hide themselves and camouflage malware.

In order to do this, intelligent rootkits embed themselves at various places in the system. Windows can be divided, roughly speaking, into a user mode and a kernel mode (see figure 1). Applications such as your web browser or office suite run in user mode, whereas things that are internal to the system, such as the file system filter drivers, use kernel mode. Windows uses a layered model. The top layer is made up of

application programs and below that lies the Windows API, which is in turn supported by the system libraries (Dynamic Link Libraries, DLLs). Windows inserts a couple of intermediate layers before access to the raw data on the hard disk is possible. Communication within the system works best from one layer to the layer immediately above or below it in the hierarchy.

In a similar way to Windows modes, rootkits can also be divided into user mode and kernel mode varieties. Both types manipulate the system components' communications; kernel mode rootkits are more dangerous because they are more difficult to uncover. Kernel mode rootkits only work if you are logged in as an administrator, which is unfortunately the default case for most Windows XP users.

The greatest challenge when finding and uncovering rootkits is that the required tools must be able to access various layers within Windows. If a rootkit's manipulating a layer, then any scanner which relies on that layer or one above it becomes useless.

The invisible threat

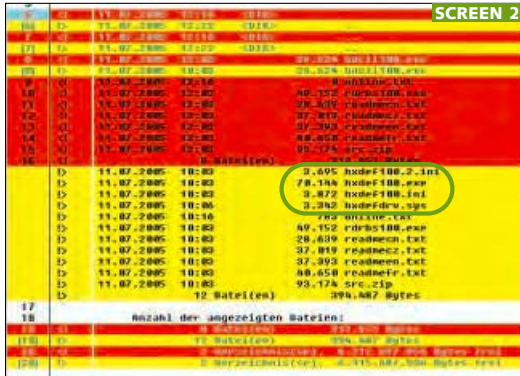
Rootkits are not a new discovery. The first rootkits for Unix systems emerged at the start of the 1990s, when shell commands were replaced with manipulated versions such as the frequently used command `ps`, with which all active processes can be listed. As tools altered like this were discovered by Unix root-level administrators they became known as rootkits.

If a Unix administrator typed the command `ps` into the shell, the rootkit only showed some of the active processes – the

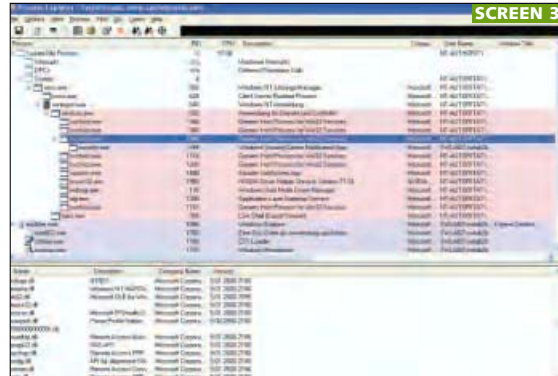
malware processes were hidden. The rootkit used the same method to falsify the directory listing produced with the `ls` command. As a result, the `ls` command, comparable with `dir` under Windows, no longer displayed all files. The rootkit filtered the operating system's view and hid malware files.

Rootkits first caused a furore in the world of Windows in the late 1990s when the Code Red worm buried itself successfully in Microsoft's Internet Information Server. Experts think that rootkits are a time bomb.

WINDOWS HACKING



Windiff compares two directory scans – the four files circled in green are hidden by a rootkit



The free Process Explorer utility shows more information than the Windows Task Manager and is not as easy to trick

Hide and seek under Windows

A favourite way for rootkits to hide a process is called a 'man-in-the-middle-attack'. The rootkit buries itself between the Task Manager and the Windows API. The Task Manager calls a Windows API in order to get a list of currently active processes. However, the rootkit intercepts the Task Manager's request to the API before passing it on. The rootkit also intercepts the API's reply and removes itself from the list of active processes (API filtering) before relaying the answer to the Task Manager. So the Task Manager doesn't show the rootkit process, although it is running. If the rootkit's being used to hide an attacker, not only are all references to the rootkit removed from the list, but all pointers to the running malware components are removed too.

This deceptive manoeuvre works with all programs that make their requests using the Windows API. The most obvious example is Windows Explorer. You can easily demonstrate how quickly files can be hidden before they're shown in Explorer, by using Hacker Defender, one of the User mode rootkits. It consists of an exe file and an ini file which acts as a configuration file. The exe file can be easily started with a double-click; it then processes the contents of the ini file.

Using its default settings, Hacker Defender hides all files with the character string 'hxdef' in their names (see screen 1). This will trick Explorer or the command-line 'dir' command – Hacker Defender hides itself. If you want to disguise other programs using Hacker Defender, then all you have to do is alter the relevant settings in the ini file.

Finding Hacker Defender

Files can be easily hidden using Hacker Defender. However, as they are not really invisible and it's easy to uncover them again. The trick is not to call the Windows API but to make use of a layer that lies deeper in the operating system. This means that by using

some system tools and free extra software it only takes a few steps to find out which files are really lurking on your system. The idea is that, while operating normally, you make an inventory list of all files on the system and save it as an online snapshot. You then boot from an external medium using a bootable live Windows CD such as Bart PE (www.nu2.nu/pebuilder) and create another inventory list (an offline snapshot). You then use the Windows command-line command windiff to compare the online and offline snapshots. Any differences reveal that files are being hidden by a rootkit (see screen 2). If you want to perform a comparison, follow the three steps below.

STEP 1 Choose Start/Run and enter the command cmd to get a Windows command prompt. Change either to the directory where you suspect a rootkit to be, or change to drive C:\. Enter dir/s/a > c:\online.txt to save an online snapshot to the file online.txt.

STEP 2 Choose an external boot medium. We recommend Bart PE, because it works best with NTFS drives. Start your computer using the Bart PE CD and once again open a command prompt. Use the command dir/s/a > c:\offline.txt to make an offline snapshot.

STEP 3 Compare the two lists by using the windiff command. Run the command 'windiff

c:\online.txt c:\off-line.txt' and the utility will present you with an overview of the differences between the two files. Two files hidden by Hacker Defender – hxddef100.exe and hxddef100.ini – stand out. Windiff is a component of the Windows Support Tools (<http://tinyurl.com/2zr2z>) which can also be found on the Service Pack 2 CD. If you only want windiff then you can download it separately from www.grigsoft.com/download-windiff.htm.

Finding hidden processes

The online-offline method described only works for hidden objects which are accessible in both modes. Although files can be found, hidden processes remain hidden as they don't run if you boot the computer from an external 'clean' live Windows CD. Help comes in the form of the free tool Process Explorer (www.sysinternals.com) which is so useful that it ought to be added to every XP PC (see screen 3). It bypasses the Windows API and can't be fooled by Hacker Defender. The utility displays in detail which programs have loaded which DLLs and Handles (pointers to data objects). However, Process Explorer does have its limits, and more and more rootkits are making attempts to fool the program. Hacker Defender, for example, is only found if you do an explicit search for handles.

Microsoft and rootkits

It must be serious – even Microsoft is developing a rootkit finder. At <http://research.microsoft.com/rootkit> there is already some information about Strider Ghostbuster, Microsoft's rootkit detection utility. When and how (perhaps as a part of Antispyware) Microsoft plans to release the program is not yet known. At present, the web pages referred to just contain downloadable information on rootkits and API filtering.



The rootkit finder Strider Ghostbuster is still some way off

Finding kernel mode rootkits

Kernel mode rootkits, the group to which things such as NT Rootkit belong, work in a similar way to their user mode counterparts. The system calls are redirected using modified pointers to the rootkit – and, in the same way, the rootkit intercepts the replies from lower-lying operating system layers. To ensure the rootkit's survival in user mode, it's disguised as a device driver. Kernel mode rootkits can, however, not only manipulate system calls but also modify kernel modules directly. For example, the rootkit known as FU can delete processes from the kernel's active process list. FU can't be found using Process Explorer.

Rootkit with virus scanner methods

NT Rootkit hides itself in a very refined manner. The program installs itself as a filter driver between the API and the file system and therefore knows about all file operations. It doesn't matter whether a system call is made via the API or bypassing it: the filter driver can influence the communication. Curiously, filter drivers are also used by virus scanners to search out pests.

Intelligent rootkits such as NT Rootkit can only be tracked down with heavy-duty developer tools such as Microsoft's Windows

'The problem with rootkits is you can never be sure you have found them all'

Kernel Debugger. You can download separate versions for x86 and x64 systems for free from www.microsoft.com/whdc/ddk/debugging. Rootkits that don't manipulate the kernel directly can be found by using the Debugger, but it's not recommended for novices.

The problem with the struggle against rootkits is you can never be sure whether you have found them all and that your scanner tool's output has not been tampered with. As a result, you need to supplement your virus and spyware scanners with as many analysis tools as possible.

Specialist anti-rootkit tools

The market is reacting to the new threat, so there are already tools available that specialise in sniffing out rootkits. F-Secure's Blacklight, for example, is still in beta but the company plans to integrate it with the F-Secure virus scanner.

Another search tool is Rootkit Revealer (www.sysinternals.com/utilities/rootkit

[revealer.html](#)) from Sysinternals. It recognises rootkits that use API filtering and can therefore be used as a replacement for the online-offline method described above. It's easy to use: a single scan checks the whole system for rootkits, although it's important to note that Rootkit Revealer doesn't remove any rootkits it discovers (see screen 4). If you are certain you have detected one or more rootkits, you will have to remove the corresponding files and Registry keys manually.

Little protection from rootkits

Rootkits present a completely new danger, but the situation isn't hopeless. Each of the rootkit types described here has its weaknesses and can be detected using the right tools. The bad news is that if you do find a rootkit on your system, you'll probably need to reformat the hard disk and reinstall Windows as there's no guarantee that all the hidden nasties have been found. The best strategy is not to let your computer get infected in the first place. You need to take several steps to accomplish this:

- Install a firewall between your computer or network and the Internet. If you are on a budget, a DSL router with an integrated packet filter will do. Computers on an

BECAUSE MAYBE WORDS DO SOMETIMES SPEAK LOUDER THAN ACTIONS INTRODUCING NEW FineReader 8.0

Thought your camera was just for random snapshots? ABBY's FineReader 8.0 is so intelligent it reads text from digital camera images as well as those from scanners. New technologies help compensate for poor lighting, out of focus text and image distortions, making it possible for FineReader to transform documents that may be difficult to scan. Thick books or documents found while out of the office are no problem. As always, FineReader's reputed accuracy ensures documents are replicated with superior precision and formatting intact. Export documents to MS Word, MS Excel, HTML, MS Word XML, searchable PDF formats, and many more. Added new features include an Automation Manager, and a free Screenshot Reader application for registered customers. So why are you spending hours retyping your texts? Download and test a free trial version today at: www.misco.co.uk/go/abby



ABBYY FineReader - THE DEFINITION OF OCR



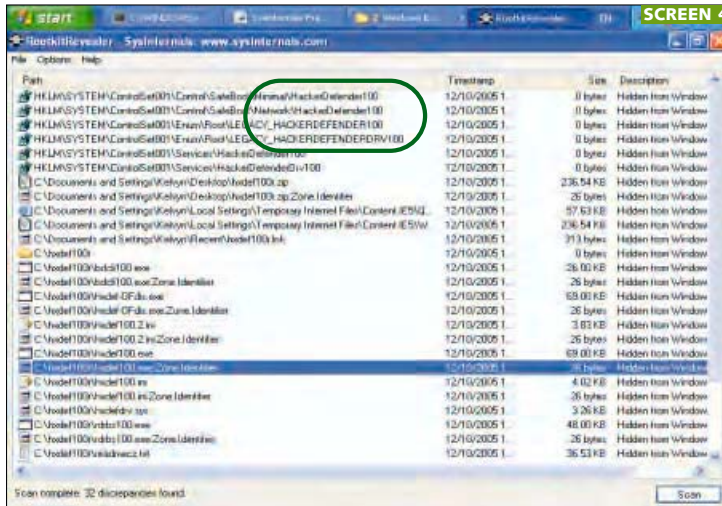
MISCO

salesdesk@misco.co.uk
Tel: 0800 038 8883, Fax: 0870 720 8686

www.ABBYY.com



WINDOWS HACKING



Specialist utilities such as Rootkit Revealer test for the presence of rootkits that try to manipulate the API

Intranet should also be protected by desktop firewalls.

- Configure your browser and email client securely. For example, turn off Internet Explorer's Active Scripting and turn off Javascript on Firefox.
- Only log in as an administrator to perform system maintenance and use a limited/restricted account for other tasks.
- Enable Windows automatic updates in order to keep your operating system and applications up to date.
- Customise the service configuration; set up Windows services to match what the computer is being used for.
- Install, use and update a virus scanner.
- Install, use and update a spyware scanner.
- Make backups of your important data at regular intervals.
- Make use of the utilities discussed here to keep an eye on your Windows XP system.

Further information

Controversial website on the subject www.rootkit.com
Rootkit detection from Microsoft <http://research.microsoft.com/rootkit>

TRACK HIDDEN OBJECTS

Since the beginning of the 1990s it has been possible to hide files in Windows operating systems in such a way that it's almost impossible to find them. These hidden files are not displayed by Explorer and they can't be found or removed by other Windows or command-line tools. It gets worse: even some security utilities miss or ignore these hidden files. Programs to verify the checksums are easily fooled and some virus scanners neglect the hidden code,

'Huge files that fill up the hard disk can be hidden in the ADS'

ADS to generate a Zone ID. If you open a file that is tagged like this after downloading, you will see a reminder that it's a file from the Internet – Windows has evaluated the ADS (see screen 5).

A big advantage of ADS is that it can keep details of access rights separate from the content. However, there are also two drawbacks. On the one hand, all types of data can be stored in ADS including executable files. Second, Windows doesn't provide a tool to find ADS. A further complication is that the size of the data and the files in the ADS need not bear any relationship to one another. A 10byte file might have a 4GB ADS, and Windows will still show a file size of 10bytes. This makes an ADS the ideal place to hide things.

To create an ADS, you do not need administrator privileges, just write permission for a file. ADS only works on NTFS – if you copy a file or directory with an associated ADS to a Fat32 partition, the ADSs will be lost (see screen 6).

DIY ADS

An ADS can be created very easily, for example using the Windows editor Notepad. Choose Start/Run and enter the command 'notepad test.txt'. This creates a new text file named test.txt. Enter some text, save the file and close Notepad. Start Explorer and select test.txt and have a Look at the file size via the context menu – just 17bytes under Windows XP. Next, open a command window and change to the

which can also be damaging. As we said earlier, the odd thing is that Microsoft built the ADS into NTFS.

Deceptive NTFS functions

Under NTFS a file consists of multiple data streams. The main data stream contains the usable data, that is the actual content of the file. In a Word document, it's the text; in an exe file, it's the executable program code. ADS information stores supplementary details about the file, such as its security settings, a preview in the case of pictures or pointers to other files. In theory, there's no limit on the number of data streams per file.

To give a practical example: when downloading a file, Internet Explorer uses

Are checksums the answer?

If you often download programs from the Internet you'll be aware of the value of checksums. The program authors use them to sign their work with a sort of digital fingerprint. By comparing the original checksum to the downloaded one, it's easy for a user to check whether or not they've downloaded the original file. The checksum also acts as a protection against running a file which has been illicitly modified.

We used md5sum and cksum (<http://unxutils.sourceforge.net>), to test whether or not checksum calculators could recognise ADSs.

Without ADSs we got the following checksums:

```
md5sum test.txt
dc15d819d604ceb6f8211f3ab35b2f85
cksum test.txt: 36716247 45
```

We then added the Windows calculator to an ADS using the following command:

```
type c:\windows\system32\calc.exe > test.txt:calc.exe
We then re-ran the checksum tests with the following result:
md5sum test.txt dc15d819d604ceb6f8211f3ab35b2f85
cksum test.txt: 36716247 45
```

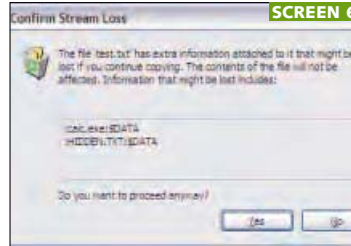
This shows that the checksums only take the main data stream into consideration and that ADS remain unrecognised, so they're of little use against clever malware.



Windows saves the warning about running exe files from the Internet in an ADS

directory where test.txt is located and enter the command dir test.txt which will confirm the 17byte file size that Explorer also reported. Next, choose Start/Run and enter the command notepad test.txt:hidden.txt and enter some text, for example 'This is a test with hidden content' and save the file. You must save this new file in the same directory where you saved the original test.txt. Now close Notepad.

The second file you created with Notepad is an ADS containing the new text. Check the test.txt file using both Explorer and the dir command. As before, both show a size of 17bytes. If you open



When copying NTFS files to Fat32 partition using ADS the alternative streams go missing

test.txt using Windows Explorer you will only see the original text displayed. There is no sign of the ADS – Windows search will not expose it either. However, if you use the command prompt and enter notepad test.txt:hidden.txt the content of the ADS is displayed. This proves that Explorer and dir only display the contents of the main data stream.

As shown in the example, you can use Notepad to display and change the ADS associated with a file, but this only works if you know the stream's name. Turning it round, this means if you do not know the ADS' name, you have no chance of finding it with Windows' own tools.

Attacking Windows using ADS

An ADS can hold data in any form. This means that a descriptive text, a secret message, a picture or an executable file can be hidden there. It's dangerous if the ADS contains an executable file which can be started automatically by a Registry entry. In our tests, we used the command type to hide an exe file in test.txt's ADS.

The exact command is type filename.exe > test.txt:filename.exe. The executable file can be run from the ADS using the command 'start .\test.txt:filename.exe'. For testing you could use one of the accessory files that comes with Windows, such as Notepad or the Calculator to embed in the ADS using a text file and run with the Start command. Executable stream contents can be started by a Registry entry or by a VB Script as well as manually as just described.

Starting hidden DoS attacks


Denial of Service (DoS) attacks usually hit servers from the Internet. In such an attack a vast number of client requests hit a server, which becomes overloaded and collapses. Another type of DoS attack can be carried out using ADSs. Huge files that fill up the hard disk can be hidden in the ADS. As a result, the computer becomes unstable

NETWORK OFFER • NETWORK OFFER

A complete 5 user network with E-mail/Internet from each PC, fully installed and cabled for less than £34 per week

Package includes

- Compaq P4 Windows 2003 server
- Router with Firewall for Internet and E-mail to desk
- Cat5 cabling for 12 points + 16 port switch
- 5 workstations with Windows XP
- Automated backup system
- 2 days on-site installation and configuration

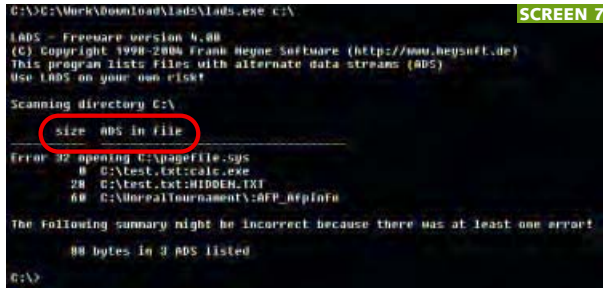


Call us now on
01279 718693
more offers on our website
www.hardsoft.co.uk

HARD SOFT

Hatfield Grange Farm, Hatfield Broad Oak
Bishop's Stortford, Herts. CM22 7JZ

WINDOWS HACKING



SCREEN 7

The freeware tool Lads finds invisible data

entry TrapHiddenDataStream to 1. But it only found one of the four contaminated streams. Norton, Bit Defender and Panda ignored ADS completely. In their favour, at least they sprang into action when the malware file was started from a script.

because it has run out of hard disk space, and the user is unaware why as Windows can't see the ADS.

The main problem with ADSs is that Windows and its built-in tools can't see them. If you know the name of the hidden file, you can view it using Notepad. To find out how virus scanners react to ADSs, we prepared five files with ADSs and hid them on a Windows system. One stream contained a harmless piece of text and the other four had viruses in attachments. Two were attached as zip files, one was disguised as a text file and another nasty had a .com ending.

We used six leading virus scanners to search for the ADSs. The tests checked the scanners' on-demand functions after both

'Out of six virus scanners, only two detected and got rid of viruses in the ADS'

standard and custom installs. To exclude the possibility of errors, we also copied the viruses on the hard disk as normal files. In a best-case scenario the scanners ought to find eight viruses on the system: four on the normal system and four hidden in ADSs.

The results were disappointing: out of the six virus scanners tested, only McAfee and Kaspersky detected and got rid of all the viruses hidden in the ADSs. PC-Cillin also scanned the ADSs, by changing the Registry

Spyware scanners can't cope either

ADSs are also ideal as hiding places for spyware. We tested three freeware spyware detectors: Ad-aware (www.lavasoft.com), Spybot Search & Destroy (http://security.kolla.de) and Microsoft Antispyware Beta 1 (www.microsoft.com/athome/security/spyware/software/default.msp). We placed copies of the well-known spyware program Cydoor on the hard disk and then hidden in a text file's ADS. Microsoft's offering ignored the ADS as did Spybot. Ad-aware found nothing in standard mode but we could turn on an ADS scan and discover the hidden menace (see table 'ADS awareness of virus and adware scanners').

Freeware ADS detection tools

You can find out whether there are ADSs on your system with some freeware tools. List Alternate Data Streams 4 (Lads) (www.heysoft.de/Frames/f_sw_la_en.htm) lists ADSs together with their names and

400

NEW

UK/PCW

400 Series Smart Label Printers

Smart Tools for Smart People

- 3 year warranty
- For Mac & PC

The fast, easy way to print labels one at a time

The user friendly Smart Label Printer makes it easy to mix and match fonts, graphics and bar codes all on the same label. Easily prepare customised formats with your own company logo without the hassle of using standard printers. The only cost is the labels. Direct thermal printing technology eliminates messy inks and pricey ribbons and toner.

from £64 ex VAT

www.siibusinessproducts.com

01276 505776

SII

Seiko Instruments Inc

www.insight.com/uk

0800 333333

www.jigsaw24.com

08707 306868

www.misco.co.uk

08000 388883

www.pcwb.co.uk

08701 652202

sizes (see screen 7). Lads is a command-line tool. To use it, open a command prompt by choosing Start/Run and entering cmd. Change to the directory where you unpacked LadsG. The full syntax for the command is: lads [Directory] [/S]/[D]/[A]/[Xname]. All parameters in square brackets are optional. If you don't specify a directory, then Lads scans the current folder. The /S switch scans subdirectories, /D is for Lads debugging and /A outputs a calculation of the space used by ADSs. You can use /Xname to exclude known ADSs of your choice from the scan.

An innovative new feature is that it's possible to pass complex instructions or queries to Lads in a text file. This is done using the /P switch. For example, lads /Pfile.txt runs the program using the parameters stored in file.txt. Lads reliably displays all ADSs. Freeware alternatives include Streams (www.sysinternals.com) and Crucial ADS (www.crucialsecurity.com), the only tool to use a graphical interface.

CLOSING BACK DOORS

Even years of experience with Windows is no guarantee that you won't find some nasty surprise in Microsoft's operating system. In this section we'll outline the most important back doors and explain how you can close them securely.

Hidden Admin shares

Shared drives for exchanging data over a network are a fact of life. However, you ought always to know which data you are allowing external access to. Shared folders under Windows can be displayed easily by entering net view at the command prompt. The catch is that this doesn't necessarily show all shares.

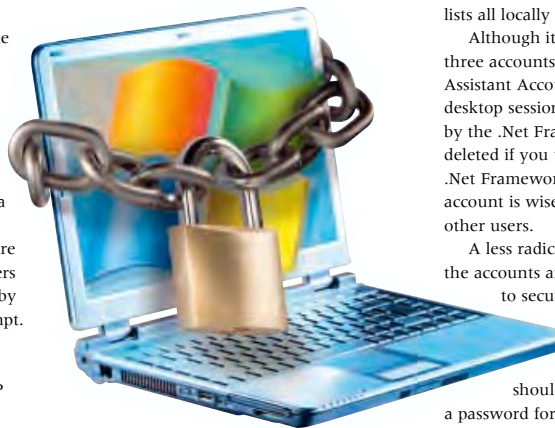
Windows XP Professional – unlike XP Home – recognises hidden shares. For example the system folder (%Systemroot%) is shared under the name ADMIN\$. All hidden shares end with a dollar symbol, which can be used to hide normal shares. You can also see hidden shares via the Control Panel (Administrative Tools/Computer Management/Shared Folders/Shares). You can view this information from the command prompt, too, by using the command 'net share'.

Administrator shares are easy to turn off. A simple 'net share [sharename]/DELETE' command gets rid of them. If you don't like using the command line, you can delete the share using the Computer Management section of the Control Panel's Administrative Tools. However, this will only work if simple file sharing is turned off. To do this, in Windows Explorer choose Tools/Folder options/View/Use simple folder sharing.

You can use Syskey to further secure the Windows XP password database

But take care: the next time the computer is restarted, the shares will be there again, or rather all the default administrative shares created by Windows – those you added yourself will be gone for good. We recommend you turn off all shares except IPC\$, which is also used for local process communication. If IPC\$ is no longer present, installed programs may produce unexpected errors. And obviously, if you want to share folders over your local network, shares shouldn't be turned off.

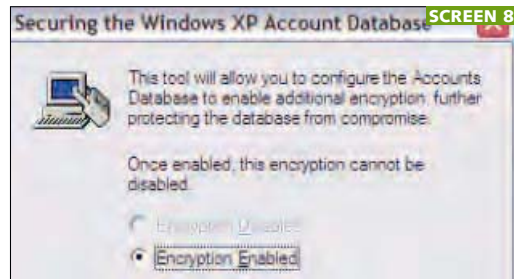
Admin shares can be turned off permanently. To do this use regedit and add a new DWORD entry called AutoShareWks with a value of 0 to the Registry's HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\



LanmanServer\Parameters branch. This removes all the administrative shares as far as IPC\$. To restore the shares delete the entry and restart the computer. If you do not need any file or printer shares than just turn off the Server service completely in the Services console (Start/Run/services/msc) – but again, don't do this if you want to share data over your network. The advantage is that the shares don't then reappear as if by magic when the computer is restarted.

Hidden user accounts

Security-conscious users should use a restricted user account, rather than an administrator account for their day-to-day work on the computer. As well as the user accounts you set up yourself, XP sneaks its own accounts into the system. These hidden accounts aren't obvious and can be



a potential security risk if you don't secure them properly.

You won't be much wiser if you look at the Control Panel's User Accounts section. At least you will see that, as well as your accounts created during installation, there is also an Administrator account and a Guest account. The System/Local Users and Groups option from the Control Panel's Computer Management section will normally list at least three further users: ASPNet, HelpAssistant and Support. The command-line command 'net user' also lists all locally stored user accounts.

Although it's possible to delete these three accounts, you will need the Help Assistant Account to run a remote desktop session, and ASPNet is installed by the .Net Framework and must not be deleted if you use programs based on the .Net Framework. Maintaining a Guest account is wise if your PC is accessed by other users.

A less radical solution is to right-click on the accounts and deactivate any you want to secure temporarily, by choosing Properties and selecting the 'Account is disabled' checkbox. Home users should also remember to set a password for the preconfigured Administrator account if this wasn't done during initial Windows installation.

Secure your passwords

During local login to an XP computer, a protected subsystem manages the user name and password. The Security Accounts Manager (Sam) stores the login information

ADS awareness of virus and adware scanners

| PRODUCT | ADS AWARE? |
|-------------------------|------------|
| Panda Antivirus | ✗ |
| McAfee Virusscan | ✓ |
| Softwin Bitdefender | ✗ |
| Trend Micro PC Cillin | Partial |
| Kaspersky Antivirus | ✓ |
| Norton Antivirus | ✗ |
| Ad-aware | ✓ |
| Spybot Search & Destroy | ✗ |
| Microsoft Antispyware | ✗ |

as encoded values in a database. Anyone with direct access to a computer – which includes malware installed on an infected PC – can attempt to use a password cracker to render the secret passwords into plain text. This could take several days for each password if a brute-force attack is employed. The Sam database is already encrypted but it can be further secured using Windows' Syskey tool (see screen 8).

Open a command prompt window and enter the command syskey. You must be logged in as an Administrator to use this tool. After entering the command a window appears in which you should ensure that the Encryption Enabled option is selected. Clicking on Update saves the Sam database key locally on the system and offers two further options: you can either set up an additional system password – which you will have to type in every time the system is started – or copy the key to a disk which then has to be inserted every time the system is started. The second method is more secure – but it requires a floppy disk and will not work with USB sticks.

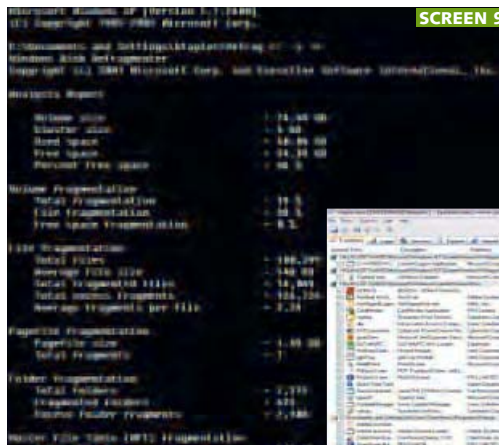
Repairing NTFS damage

Microsoft has chosen NTFS as the file system for the immediate future. Early experiments with the Windows Vista beta show that the new operating system can only be installed under this system. NTFS is more robust than Fat, can manage more memory and storage and offers granular access rights and refined extras such as encryption. Only a few users realise that all file changes can be logged. This means that the file system can be rebuilt quickly after a crash.

However, it can be dangerous if malware has got onto the system and tries to manipulate the log file. NTFS sets up a special area on the hard disk for file-related information, known as the Master File Table (MFT). This is a relational database

A watertight Registry

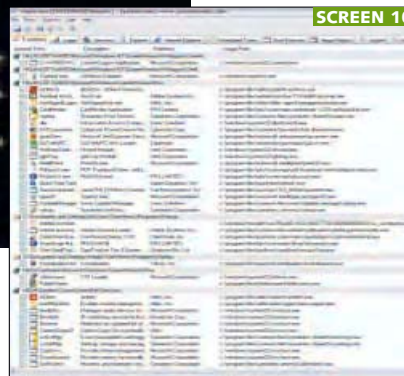
The registration database, also known as the Registry, is a total mystery to many users. Application setup routines usually make, or change, dozens of entries in the Registry. Spyware and rootkits often use disguised Registry entries to bury and anchor damaging functions deep in the system. If you use Windows' own tool, regedit, you'll find that it doesn't offer much help in searching for Registry entries. The freeware Regmon utility from www.sysinternals.com/Utilities/Regmon.html, on the other hand, shows you which programs are accessing which Registry key in real time.



SCREEN 9

Left: The command defrag c: -a -v gives detailed information about the NTFS Master File Table

Below: Autoruns gives you a list of programs that start when Windows loads



SCREEN 10

which, by default, reserves 12.5 per cent of the space on an NTFS partition for itself. The command 'defrag c: -a -v' shows information on the size, fragmentation and number of entries in the MFT (see screen 9).

Usually the space in the MFT is off limits for normal files; only if a hard disk looks full will Windows free up space in the reserved area. The catch is that the MFT becomes a target for malware because if the MFT area is damaged, file operations won't work and XP grinds to a halt. The same goes for damage to the MFT itself. The easiest way out of this is to restore a backup image. If you do not have a backup, you can start a repair process using the command 'chkdsk /f' which will attempt to fix disk errors – but success is never guaranteed.

Hidden autostarts

The startup process of an XP computer is very complicated, leading many users to get annoyed that the computer takes so long to boot. Only a few consider what is happening behind the boot screen. If you are trying to identify programs that start automatically when Windows loads, you'll usually look in the Startup folder first.

Often you'll be surprised at what's there: even if you've not added anything yourself there will probably be the Office quickstart and a few other tools. A tip for power users is to make use of the msconfig system tool, which you can start via Start/Run. On its Systemstart tab it lists the objects that start up automatically with Windows.

However, this tool only shows a small portion of what's really going on in the background. A better utility is Autoruns (see screen 10) which you can find at www.sysinternals.com/Utilities/Autoruns.html. This will give you a full overview of what really happens when XP starts and let you remove unwanted services or programs.

Are your files really deleted?

Under Windows, files and folders can't be fully deleted from the hard disk. The entries are just de-referenced so they no longer show up in Explorer or at the command prompt. This means data you had thought was deleted is in fact still on the hard disk; valuable data often remains on discarded hard disks. Windows marks the space as being available, so sooner or later other data will overwrite the remaining fragments of information. Nonetheless, it's still possible to make the file fragments visible.

Using Windows' built-in tools you can't remove the files completely. Add-ons to do the job can be found for free, for example Eraser (www.heidi.ie/eraser) or as paid-for products such as Safe Erase (www.oo-software.com/de/products/ooasafeerase). Programs such as the freeware PC Inspector File Recovery (www.pcinspector.de), can show you which files can be salvaged from the digital dustbin. We'll be looking at the tools available for such data recovery in a future issue of PCW.

Peace of mind

It's easy to get paranoid about computer security, but one of the keys to remaining sane is to understand the problem. We've highlighted here some of the new methods hackers can use to compromise your system, which is the first step to being able to defeat them at their own game. It's a sad reflection on the state of personal computing that so much effort these days is consumed just securing your system, but in the long run it's worth it for the peace of mind it brings. PCW