Checking Microsoft Windows® Systems for Signs of Compromise

Version: 1.3.4
28/10/05

Licence: http://creativecommons.org/licenses/by-nc-sa/1.0/p

Please Note this Document is updated frequently.
The latest version may be downloaded from

http://www.ucl.ac.uk/cert/win_intrusion.pdf
http://users.ox.ac.uk/~patrick/files/win_intrusion.pdf
http://www.ict.ox.ac.uk/oxford/compsecurity/win_intrusion.pdf

Simon Baker, UCL Computer Security Team
Patrick Green, OXCERT
Thomas Meyer
Garaidh Cochrane

Aims

One of the main aims of this document is to address the lack of documentation concerning concrete actions to be taken when dealing with a compromised Microsoft system.

A secondary goal is an explanation of methods of examining this information via tools. Utilizing these tools we can then :

- investigate the system
- find the points of entry and type of compromise
- identify areas for further investigation and issues for attention.

Introduction

This guide does not cover the administrative aspects of a compromise, rather it is intended to outline useful tips in finding malware, links to tools for examining the system and define the reasons for undergoing this work.

This document will deal with basic levels of intrusion analysis, aimed mainly at intrusions on desktop systems, or initial examination of servers. It is not an in depth technical discussion of recovery of mission critical servers. It should also be noted that a number of these tools will change the file system - this will more than likely make the drive inadmissible as evidence. If you think you might want to involve law enforcement, this isn't the guide to read!

A compromise can occur in a number of ways, possibly a machine was unpatched against a certain vulnerability, or the user is using weak passwords (particularly on Windows shares) or the user 'clicked on the wrong thing'. However the machine has been compromised, it is important to analyze the system to work out how the intruders got in, as this will give you the means for preventing entry in the future - it is useless to reformat and reinstall a box, only to leave the same way in wide open. Understanding the mode of entry can also help determine if other machines on your site have been compromised, i.e. was entry gained through a service unique to this machine, or common to the whole site or department ?

However entry was gained, one of the most important things you can do is run `Windows Update', but you should also be aware that Windows update is only used to update Windows, it doesn't update things like Office, MSDE or SQL (although it will update IE). Simply going to `Windows Update' will not actually fix the problem, though it may prevent further compromises from other attackers.

A second important aid to examining intrusions is logging, but be aware that Windows systems are notorious for having little logging in force on a default install. As such, trying to track down intrusions and the actions an intruder has taken is extremely difficult. However it is possible for a large amount of auditing information to be logged, providing the appropriate settings and changes are made, and this should of course be done. Another problem however is that it is common for intruders to wipe log files when they gain entry to a system so, if possible, for mission critical machines, you may want to consider central storage for log files.

It is worth pointing out that while certain anti-virus products can and indeed do detect certain backdoors, this is not their primary function. An anti-virus scanner is precisely that, it will not detect how an intruder gained access in the first instance, nor will it alert you to what actions or other backdoors they may have placed on the system. Indeed, many attackers will use tools and backdoors which are specifically designed to evade anti-virus scanners.

If a rootkit is installed on your system, it will be extremely hard to detect. At present, there are only two tools that we aware of that can aid the discovery of a rootkit, and the associated procedures are extremely difficult to follow. It is for precisely this reason we would recommend simply reinstalling the operating system ; it will take far less effort and time. Indeed, it could be argued that these procedures should only be used for either academic curiosity and forensics of an attack, or if the system is of extreme importance. Regardless of your findings, it is still highly likely that a compromised machine will always remain compromised, and thus cannot be trusted.

In nearly all cases, the easiest way to recover from a compromise is a fresh re-install of the machine, with any appropriate data being restored from known, **good and trusted backups**, again at this point it helps if you know when the machine was first compromised. In certain cases it can be argued

that a re-install is not feasible, due to political or operational reasons. In cases like this, it is worth considering the fact that if you do not re-secure the machine effectively, the miscreants may damage the machine's operating system and programs beyond repair, and also steal files or information such as usernames and passwords for websites, credit card details, etc. We are also seeing a rise in keyloggers and sniffers being used to access this information also, and usually it is automatically emailed or uploaded to other sites as it is captured.

First Steps

Before you begin, let us give you one piece of advice. DON'T PANIC!

You are not the first person this has happened to, and you **certainly** won't be the last!

The first step in recovering any system from a compromise is to **physically** remove any network cables. The reason for this is that if a system is under external control, an attacker could be monitoring what is happening on a machine and if they are aware of your actions could take drastic action to conceal their actions, such as formatting a drive.

However, it should be noted, that if the network cable is unplugged you may lose information about the attacker, you will not see active network connections. This of course is important if you wish to trace the miscreants, however your site security contacts may have policies forcing a disconnection after a break-in, and if your local CERT requests you remove the machine from the network you should of course fully comply with their requests. Your local CERT team may also require you to report any system break-in to them, for compliance purposes as well. Your local security policies should contain information about any actions you need to take.

Next, you should take a notebook (a paper one, not electronic) as this will be used to take notes in. Write down any important details about the system, starting with the time and date, the IP address and name of the machine, the timezone that the machine's clock is set to, whether the clock was accurate, patches that were installed on it, user accounts, how the problem was found, etc. If anything during the course of your investigation seems pertinent, jot it down.

It will be a handy reference for the future.

It may be difficult to regain control of a seriously compromised Windows system which has so many resource consuming programs running at start-up but simply restarting up in safe-mode will stop a large number of Run key based malware loading at boot up, giving some control back to the user for clean-up tasks.

One final point, your local security contact or CERT team will almost certainly be interested in your findings. Very often an attacker will automate an attack, and will almost certainly be targeting other machines in your network. Providing details to your security contacts will enable them to disseminate your findings to other people who may be in a similar situation. And of course your findings may turn up in here!

File System

There are well known tricks for hiding malware on Windows systems, these include manipulation of the file system.

So, be prepared to find files in %systemroot%\recycled (or any drive\recycled). The recycled folder is system hidden, so will not show up by default, and isn't searched through by default.
%systemroot%\recycler also exists on many systems (containing the individual SID-identified recycle bins) and should also be checked.

Which leads us onto system and hidden folders - these are attributes that can be very easily set by intruders, so you should turn off the 'hide system folders' and turn on 'show hidden files' as a matter of course. These options can be found in the 'Tools' 'Folder Options' 'View' menu from the file explorer, explorer.exe.

Running `cmd.exe' can often be the most powerful way of looking at a windows filesystem. For instance, changing directory to the c:\winnt\systems32 directory and running "dir /o:d" one can quickly see when the majority of the OS was installed, then the various service packs/patches, and sub-dirs that update themselves frequently like catroot2 and drivers. The most recently dated items are often the ones you should concentrate on looking in.

The other useful tool, which comes with Windows, is the search function. This can be used if you have an idea of the date and time the intrusion took place. Use the advanced option to search for hidden folders and system files. This of course assumes that this feature has not been tampered with, via a rootkit or trojan.

Intruders have a high propensity to call files and folders by legitimate looking names. Do not be surprised to see nvsvc32.exe or serv1ces.exe in the system32 folder. The aim is obfuscation, and goes hand in hand with hiding their automatic startup services.

Other places to look for things starting up is the registry, specifically any of the keys under:

HKEY_LOCAL_MACHINE, HKEY_CURRENT_USER or HKEY_USERS\.DEFAULT

\Software\Microsoft\Windows\CurrentVersion\Run
\Software\Microsoft\Windows\CurrentVersion\RunOnce
\Software\Microsoft\Windows\CurrentVersion\RunOnceEx
\Software\Microsoft\Windows\CurrentVersion\RunServices
\Software\Microsoft\Windows\CurrentVersion\RunServicesOnce
\Software\Microsoft\WindowsNT\CurrentVersion\Winlogon

Another problem is viruses and trojans that put themselves in HKEY_CLASSES_ROOT*, attaching themselves to all file extensions.

It is not unusual to obfuscate malware by using alternate data streams. This is the hiding of one file in the data stream of another. The method can be used to hide very large files, and any user can manipulate the system in this way. For example:

rundll32 c:\winnt\system32:malware.dll

This indicates that the the system will start rundll32 (an exe will execute a .dll file as a executable) called malware.dll. The use of the second colon indicates that the file is actually stored in an

alternate data stream. The tool, lads (http://www.heysoft.de) will list alternate data streams to help find the files involved.

Do not rely on the extensions that a file is given, for example, a .dll file may in fact just be a plain text .ini file, with a different extension. For the same reason, it is important not to double click on a file to open it, it may be called .txt, but is actually a .exe. Instead, the best way to look at the file would be by using a HEX editor or failing that 'right click' on the file, and choose 'open with' and select 'notepad' on a windows system.

Another problem is a legitimate sounding process running out of an unusual directory, such as :

C:\winnt\microsoftdrivers\etc\lsass.exe

This process above is actually a known backdoor, irc.ratsou.b
http://securityresponse.symantec.com/avcenter/venc/data/backdoor.irc.ratsou.b.html

A useful guide to editing the registry is available at:
http://msdn.microsoft.com/library/en-us/dnexnt01/html/ewn0201.as

This article explains in a sensible, clear way what the registry is and how it works. Even if you believe you understand the registry, it's a good idea to read this article anyway.

The other place that you should look for unauthorized programs is in the `services' control panel. This can be found by going to the control panel, selecting 'Administrative Tools', 'Services'. A useful list of known services for XP and 2000 is available at:

http://www.blackviper.com/WIN2K/servicecfg.htm
http://www.blackviper.com/WinXP/servicecfg.htm

Please be aware however that common anti-virus programs, video drivers, and other programs actually make legitimate use of running as a service, so don't be alarmed if you see more services running than you expect, though of course each of these should be investigated thoroughly. A good resource is to `google' for the process, more often than not someone else has found this service and explained exactly what it is.

Do not rely on anti-virus products alone to detect malware, for a number of reasons. Firstly, malware continually evolves and you may have something on the machine which has yet to be included in your anti-virus products database. Secondly, a number of infections have ways of turning off virus protection, so the scanner may not show up anything. Finally, a number of the programs used in a compromise are legitimate but used in an illegitimate way. For example, an ftp server is a normal application, or it can be installed by intruders to serve out 'warez', neither use will be flagged by the virus checker, as it looks at the application, not how it is being used.

Following on from that, Google (www.google.com) is an excellent resource for tracking rogue programs. If you find any programs that look suspicious, simple search for that programs name, and you will very probably turn up some very useful information.

Finding the malware directory is the first task, this will (hopefully) give you a number of .ini files which show you what is running, where, and also have lots of other software which they run. Use the tools from your cd to try to find the directory - if there is a something listening on a port tcpview should show you the full path to the directory, although this can be confused by reserved names.

Reserved name directories are such as 'com1' 'lpt1' and 'con2' and are hidden from Windows and MS-

DOS. Quite often the intruder will include a large number of spaces after the directory name e.g.

'lpt1 '

will display the same as lpt1, but is in fact a different directory all together. These can be difficult to navigate to and harder to remove.

There is an excellent Microsoft article on removing files with reserved names available here
http://support.microsoft.com/?kbid=320081

Infections from viruses or spyware may also hijack the hosts file on a windows machine. When a windows machine resolves a hostname into an IP address, it first looks at the hosts file located in,

%windir%\system32\drivers\etc\hosts

If there is no entry for the host there, it forwards the request onto the DNS. However, for example, if the infection modifies the hosts file to read,

www.google.co.uk 127.0.0.1

It would render the machine unable to connect to www.google.co.uk. This has significant impact if a false entry for windowsupdate is added. Cleaning up this sort of problem is very easy - just remove the errant entries in the host file, but be aware that it is is a symptom of some other infection, rather than the infection itself.

If the infected host still exhibits resolve problems, it would be worth checking that the machine has the correct DNS entries, both in networking properties and in the registry, if the virus writers controls a DNS outside of your network, they can rewrite the DNS entries on the local machine and have it resolve all hostnames through their own DNS, at which point they can map any hostname to IP address they choose.

Batch Files (Files ending in .bat)

The current trend for compromises is very rarely against single boxes, the are more often against dozens of machine (within your campus) and hundreds / thousands across the Internet. For this reason the act of compromising a machine is as automated as possible. Sometimes during an investigation, you can get lucky and find the batch file they used to install all their software.

These batch files can be called anything - all they need to do is to run it. Examples we have seen are 'licenses.bat', 'secure.bat' and 'securing.bat'. The `bat' files can be very simple - from adding registry entries to quite complex scripts which affect the very set up of windows, and its security.

If you have the date and time of the compromise, you can search for .bat files created within that timescale. Below, we have given an example as to what sort of things you may find in one of these batch files (lets called it 'hacked.bat'). The information is based on a real compromise, but the filenames have been changed (as these are generic, you don't want to get caught up in searching for specific names - remember they can call their files whatever they want).

So, hacked.bat starts with,

```
cd "%windir%\system32"
```

Whatever else happens in this file, it will be relative to that directory - possibly a good place to look for malware. It is a legitimate directory, so be careful what files you delete! (Its always a good idea to save the files off to another directory, for checking).

The next few lines read,

```
dtreg -AddKey \HKLM\SYSTEM\RAdmin
dtreg -AddKey \HKLM\SYSTEM\RAdmin\v2.0
dtreg -AddKey \HKLM\SYSTEM\RAdmin\v2.0\Server
dtreg -AddKey \HKLM\SYSTEM\RAdmin\v2.0\Server\Parameters
```

This is a manipulation of the registry - they are adding keys for the radmin program, so that when they actually install it there are no problems with registry errors. If you don't use radmin, you may want to delete these keys. The next lines populate the keys,

```
dtreg -Set REG_BINARY \HKLM\SYSTEM\RAdmin\v2.0\Server\Parameters\DisableTrayIcon=01000000
dtreg -Set REG_BINARY \HKLM\SYSTEM\RAdmin\v2.0\Server\Parameters\Port=e5080000
```

These set the port and make sure that that the tray icon has been disabled - that would be too easy to spot! If you can decode the port, you can match it up to the tcpview settings and confirm that you have the right target. Being able to get traffic data for that port wold be really useful in finding other machines compromised in the same way.

```
dtreg-Set REG_EXPAND_SZ "\HKLM\SYSTEM\CurrentControlSet\Services\pnpext\ImagePath=%windir%\system32\mybackdoor.exe /service"
```

This line is the big one. It sets a registry entry, as a service which starts the file 'mybackdoor.exe' out of the system32 directory. The following line defines the 'pnpext' service,

```
serv.exe INSTALL pnpext /n:"Universal Serial Bus Control Protocol" /b:%windir%\system32\mybackdoor.exe /u:LocalSystem /s:AUTO
```

serv.exe is a way to install a service onto the machine, the '/n' switch gives the name of the service (once you see this, go check the services control panel) '/b' lists the full directory and full name for the service, '/u' outlines the privilege the service is to run at and '/s' tells windows when to start the service - in this case automatically whenever windows starts up.

Final lines of the file will start the services, and any other applications they want to run.

As we said before, the batch file might be more complex than this, or be split into separate files. So you may find a securing batch file which has entries such as,

```
net share /delete C$ /y >>del.log
net share /delete D$ /y >>del.log
```

Which deletes the hidden windows shares (and pipes the results to 'del.log'). Once in the machine, they don't want anyone else breaking in and taking it away from them!

Finding these batch files can be a real benefit, as the list exactly what you need to clean the backdoor from the machine. Unfortunately, they are often deleted.

Using Built-in Tools

Many of the built-in tools on windows machines are also quite useful. For instance running a command prompt (Start -> Run -> cmd.exe) on XP and running the command netstat -ano shows pids (Process Identifiers) which can then be used to map ports to process names.

One of the best places to look for help on the utilities available and their usage is at the Microsoft site, in the Knowledge Base: http://support.microsoft.com/default.aspx

Checking System Files

One excellent way of checking MS Windows files on newer versions of Windows(Windows XP and Windows 2000) is to run `sigverif'.

To run this, Click Start, click Run, type sigverif, and then click OK. Click the advanced option, select "Look for other files that are not digitally signed", and then select c:\Windows or c:\winnt depending on the version of Windows..

This tool checks the digital signatures on all the system files, and will alert you of any that aren't correct, or not signed. Be aware however that this program can produce a very verbose output, as it will of course inform you that a log file is not signed for example.

Tools

The following tools are considered essential by the authors for tracking down system activity anomalies. Remember, the existing utilities on the victim machine may well have been trojaned.

It is advised that a cd is created with these tools on - this cd can then be taken to a machine and used locally. You are well advised to check the files' md5sums (or similar) and that they run on the version of Windows you are aiming to investigate.

Many of these utilities will need Administrative access to run, and most will provide more information if run as an administrator.

SQL Critical Update Kit

(http://www.microsoft.com/SQL/downloads/securitytools.asp)

If you receive a report that you are scanning for port 1434, and that you should check your system for signs of compromise it is extremely likely that you have been infected with the SQL Slammer worm (also called Sapphire). This tool will identify vulnerable systems and also patch them as needed. Once fixed, you *must* reboot to clear the problem.

TCPView

(http://www.sysinternals.com/ntw2k/source/tcpview.shtml)

TCPView is a Windows program that will show you detailed listings of all TCP and UDP endpoints on your system, including the local and remote addresses and state of TCP connections.

On Windows NT, 2000 and XP TCPView also reports the name of the process that owns the endpoint. TCPView provides a more informative and conveniently presented subset of the Netstat program that

ships with Windows. Please note there is one small issue with this program, when it is run from a floppy it does not display process names.

TDIMon
(http://www.sysinternals.com/ntw2k/freeware/tdimon.shtml)

TDIMon is an application that lets you monitor TCP and UDP activity on your local system. It is the most powerful tool available for tracking down network-related configuration problems and analyzing application network usage.

Filemon
(http://www.sysinternals.com/ntw2k/source/filemon.shtml)

FileMon monitors and displays file system activity on a system in real-time.

Its advanced capabilities make it a powerful tool for exploring the way Windows works, seeing how applications use the files and DLLs, or tracking down problems in system or application file configurations. Filemon's timestamping feature will show you precisely when every open, read, write or delete happens, and its status column tells you the outcome.

Deleted File Analysis Utility
(http://www.execsoft.com/freeware/undelete/download.asp)

This freeware can directly view your hard drive partition and list all deleted files that have not yet been completely overwritten. Runs on Windows NT, Windows 2000 and Windows XP.

DumpSec
(http://www.systemtools.com/somarsoft/)

SomarSoft's DumpSec is a security auditing program for NT/2000. It dumps the permissions (DACLs) and audit settings (SACLs) for the file system, registry, printers and shares in a concise, readable format, so that holes in system security are readily apparent. DumpSec also dumps user, group and replication information.

DumpReg
(http://www.systemtools.com/somarsoft/)

DumpReg is a program for Windows NT and Windows 95 that dumps the registry, making it easy to find keys and values containing a string. For Windows NT, the registry entries can be sorted by reverse order of last modified time, making it easy to see changes made by recently installed software, for example.

Fport
(http://www.foundstone.com/knowledge/proddesc/fport.html)

Fport reports all open TCP/IP and UDP ports and maps them to the owning application. This is the same information you would see using the 'netstat -an' command, but it also maps those ports to running processes with the PID, process name and path. Fport can be used to quickly identify unknown open ports and their associated applications.

MBSA
(http://www.microsoft.com/)

MBSA scans for common security misconfigurations in Windows, Internet Information Services (IIS), SQL Server, Internet Explorer, and Microsoft Office. MBSA also scans for missing security updates in Windows, IIS, SQL Server, Internet Explorer, Windows Media Player, Exchange Server, Microsoft Data Access Components (MDAC), Microsoft XML (MSXML), Microsoft virtual machine (VM), Content Management Server, Commerce Server, BizTalk Server, Host Integration Server, and Office (local scans only). A graphical user interface (GUI) and command-line interface are available in version 1.2.

MBSA version 1.1 replaced the stand-alone HFNetChk tool and fully exposes all HFNetChk switches in the MBSA command-line interface (Mbsacli.exe).

Spybot Search & Destroy
(http://www.safer-networking.org/)

Spybot - Search & Destroy can detect and remove spyware of different kinds from your computer. Spyware is a relatively new kind of threat that common anti-virus applications do not yet cover. If you see new toolbars in your Internet Explorer that you didn't intentionally install, if your browser crashes, or if you browser start page has changed without your knowing, you most probably have spyware. But even if you don't see anything, you may be infected, because more and more spyware is emerging that is silently tracking your surfing behavior to create a marketing profile of you that will be sold to advertisement companies.

Autoruns
(http://www.sysinternals.com/ntw2k/freeware/autoruns.shtml)

This applet shows you what programs are configured to run during system bootup or login. These programs include ones in your startup folder, Run, RunOnce, and other Registry keys. You'll probably be surprised at how many executables are launched automatically. Autoruns works on Windows 9x and Windows NT/2K/XP. It provides a safer way to look at the myriad run keys and startup folders without directing users to use Regedit.

Ad-aware
(http://www.lavasoftusa.com/software/adaware/)
One of the first applications built to find and remove adware and spyware, Ad-aware's good reputation is well justified. Ad-aware does an excellent job of finding and removing most adware and spyware components, although you will have to restart and rescan for a seriously infected machine.

Investigating Kernel Rootkits

The use of Kernel level rootkits is becoming far more widespread. Once on a machine, the hacker will try everything they can to stay there. This document has already looked at obfuscation techniques, and batch files that secure the machine, the next step is to make the system lie to you. This is currently the most successful way to hide a compromise - the intruder will break into the machine, secure the machine, install the rootkit and then install the services they require. The rootkit will then protect those services, making sure you don't find them and remove them.

A remote administration application such as "VNC" or "radmin" is exactly that, an application. A rootkit, on the other hand, patches the already existing paths within the target operating system.

One of the most popular rootkits for Windows systems is the "Hacker Defender" toolkit. This installs itself as a service, and thus is quite straightforward to identify if you follow the correct procedures. One of the easiest ways to detect if a rootkit backdoor is installed on a system is to use tools such as tcpview or netstat on the suspect machine, and then to correlate these results with a network scan of the system from another clean machine, using a utility such as the excellent nmap (www.insecure.org/nmap/). If the clean machine reports an extra open port, it is almost certain that the suspect machine has a rootkit installed.

There are currently only a small number of applications which can help discover the presence of rootkits. This document outlines some of them, but will not give a preference - these tools will likely mature faster than this document will be updated. Along with the other tools on detailed in this document, keeping a selection of rootkit detectors on a c.d. would be good practice.

RKDetect

(http://www.security.nnov.ru/files/rkdetect.zip)

RKdetect runs remotely, enumerating services through WMI (user level) and Services Control Manager (kernel level). The tool then compares results and displays any differences. This method allows you to find the hidden services that start the rootkit. Process Explorer and TCP/IP View (both from SysInternals) should also be used in conjunction with RKDetect. It is recommended that you use the sc.exe in the windows resource kit rather than the one supplied by the Rkdetect authors. The Windows resource kits can be downloaded from one of the following locations:

http://www.microsoft.com/windows2000/techinfo/reskit/tools/default.asp
http://go.microsoft.com/fwlink/?LinkId=4544
http://www.microsoft.com/ntworkstation/downloads/Recommended/Featured/NTKit.asp

To actually run the script:

```
cscript rkdetect.vbs <machine_name/ip>
```

Example:

```
C:\detector>cscript rkdetect.vbs 192.168.0.100
Microsoft (R) Windows Script Host Version 5.6
Copyright (C) Microsoft Corporation 1996-2001.
All rights reserved.
Query services by WMI...
Detected 79 services
Query services by SC...
Detected 80 services
Finding hidden services...
Possible rootkit found: HXD Service 100
```

```
Done
C:\detector>
```

RKDetector

(http://bagpuss.swan.ac.uk/comms/RKDetectorv0[1].62.zip)

Runs on the local machine and attempts to provides information about hidden processes and services Once it identifies the hidden processes, RKDetector will try to kill those hidden tasks and then scan the service database in order to detect hidden services and hidden regkeys (Run, Runonce). RKDetector also contains a MD5 database of common rootkits, which it can compare output from against which it will compare output. To actually run the tool,

```
c:\rkdetector.exe
. .. ...: Rootkit Detector Professional 2004 v0.62 :... .. .
Rootkit Detector Professional 2004
Programmed by Andres Tarasco Acuna
Copyright (c) 2004 - 3wdesign Security
Url: http://www.3wdesign.es
-Gathering Service list Information... ( Found: 271 services )
-Gathering process List Information... ( Found: 30 process )
-Searching for Hidden process Handles. ( Found: 0 Hidden Process )
-Checking Visible Process.....
-Searching again for Hidden Services..
-Gathering Service list Information... ( Found: 0 Hidden Services)
-Searching for wrong Service Paths.... ( Found: 1 wrong Services )
```

Blacklight, Fsecure

(http://www.f-secure.com/blacklight/)

The rootkit detector, Blacklight, from Fsecure is currently in beta form, so is likely to change at anytime. It also doubles up as an eliminator - so if it finds a rootkit, it may be able to remove it from the system. It is currently a free download, which requires administrator privileges to run. Once passed the licensing agreement, the window will ask to perform a scan of the machine - you also have an option to show all running processes. Once the scan is complete, a summary will be presented - showing if it has found anything, and the software will allow you to move onto the cleaning process.

Rootkitrevealer, Sysinternals

(http://www.sysinternals.com)

Rootkitrevealer is produced by sysinternals, whose tools feature often in this document. Again it is a free download, requiring administrator privileges to run (strictly speaking, the help file identifies the permissions it requires, and administrator gets these permissions by default). Once again it works from within windows, and presents a small window which displays options and scan results. Rootkitrevealer will not clean the machine, it does, however, scan the hard drive and the registry for possibly problematic files / entries. These are then highlighted for the user to take action, if required. This has its own benefits and problems. Using Psexec, rootkitrevealer can also be run against a remote system.

Unhackme

(http://www.greatis.com/unhackme/)

Unhackme can be downloaded for free, but has an evaluation version - the paid-for version comes with free support and updates. Unlike other rootkit detectors, unhackme requires installation on the machine - which in turn requires administrator privileges. It does come with a 'monitor' which will

check your machine every minute (default setting). Once in the application, it has a very simple interface which will allow you to scan the system, get help etc. The software will also act as a rootkit cleaner.

As it requires installation, this may be of more use to people wanting to keep their system secure, rather than those responding to incidents.

RegdatXP
(http://people.freenet.de/h.ulbrich/)

This isn't strictly a rootkit detector - it is actually a raw registry editor. This means it can be used to load up the existing registries on a machine (files like ntuser.dat and usrClass.dat). It has good searching tools, so admins can look for autoruns, suspicious registry keys etc. This has benefits over signature based detection, although it requires a greater degree of time and effort. It bypasses the problems when a rootkit prevents the inbuilt RegEdit from working correctly. The software is shareware.

Removing a Rootkit

It should be noted that both these tools suffer from false negatives, so further testing and examination of the machine should be undertaken. Once you have a better idea of the rootkit involved you may want to try and disable it - boot windows into Rescue mode:

- Insert the Windows OS Installation CD into the Drive.
- Boot from the CD
- Choose 'R' to enter the Rescue Console
- Choose the Windows installation you want to Clean from the list presented to you.
- Enter the Administrator Password.

Once in the recovery console, you have a few commands for this, including:

listsvc - lists services that can be enabled or disabled

enable <servicename> <start-type> - enables a service, with a service type,

- SERVICE_DISABLED
- SERVICE_BOOT_START
- SERVICE_SYSTEM_START
- SERVICE_AUTO_START
- SERVICE_DEMAND

disable <servicename> - disables a service, but prints out the previous start-type, which should be recorded in case you need to re-enable the service.

More info on the XP Recovery Console can be found here
http://support.microsoft.com/default.aspx?scid=kb;EN-US;314058

Use listsvc to find any undesirable services, make a note of them, HackerDefender is usually called something along the lines of HackerDefender if the attacker is careless, however it could also be renamed to be something that sounds like an "official" service.

Once these have been disabled you can reboot safely into full Windows without HackerDefender starting up.

After the reboot search the registry for the name of the service that you disabled in the previous section, this should lead you to the executable for HackerDefender and more importantly its .ini file (not necessarily a .ini file, but may have a different extension).

Open/Edit the .ini file and in there you should find a number of files, ports and services that HackerDefender is defending. Systematically find each of these services in the registry and delete them (they will probably appear more than once), likewise find all of the referenced files and delete them also.

The .ini file can be obfuscated in a variety of ways, these 2 examples contain the same lines, but with different levels of obfuscation

1.
```
[H<<<idden T>>a/"ble]
raddrv.dll
```

2.
"/:<|>:\"["/:<|>:\"H"/:<|>:\"i"/:<|>:\"d"/:<|>:\"d"/:<|>:\"e"/:<|>:\"n"/:<|>:\" "/:<|>:\"T"/:<|>:\"a"/:<|>:\"b"/:<|>:
\"l"/:<|>:\"e"/:<|>:\"]"/:<|>:\"
"/:<|>:\"r"/:<|>:\"a"/:<|>:\"d"/:<|>:\"d"/:<|>:\"r"/:<|>:\"v"/:<|>:\"."/:<|>:\"d"/:<|>:\"l"/:<|>:\"l"/:<|>:\"

Final point - these tools cannot be used to determine that there is no rootkit on the machine, they are limited in what they can find.

One of the biggest problems with these tools that can occur is if some piece of malware that runs as a service has been detected and removed by a virus scanner (which won't fix the registry entries), it will alert the user that this is a component of a rootkit.

F-Secure (and to a lesser degree Sophos) seems quite good at identifying most of the malware executables once you have killed the service that is the problem but they leave the registry a bit of a mess with regard to service entries.

These 'bad' service entries can also occur for older legitimate software that doesn't uninstall/reinstall itself properly. The problem isn't so much with the utilities as with the older software not conforming to the Microsoft rules about how software should be installed or upgraded.

Conclusion

We hope that this guide has made things a little clearer about how to track down malware and other leftovers from an intrusion. We've tried to make this as easy to use as possible, but if you feel we are missing something, or something is not clear then please email one of the authors:

Simon Baker, UCL Computer Security Team, ccaasib@ucl.ac.uk
Patrick Green, OXCERT, patrick.green@oucs.ox.ac.uk
Tom Meyer, TomMeyer@venda.com
Garaidh Cochrane

Other Contributors

Martin Connell (Liverpool John Moores University), Stephen Gardner(Imperial College London), Paul X. Christopher (University College London), Andrew R. King (University College London).

References

http://www.phrack.org/phrack/55/P55-05

http://www.microsoft.com/technet/community/columns/secmgmt/sm0504.mspx

http://members.chello.nl/s.pechler/Backdoor_stealth_proxy_server.htm