# 501.5
# Malware

SANS

# Identifying and Removing Malware


Version A12_02

Identifying and Removing Malware

This page intentionally left blank.

# Course Outline (1)

**Our training will focus on two parts:**

Part I

- Using Microsoft Windows basic built-in CLI tools
- Using Microsoft Windows Advanced built-in CLI tools
- Using Microsoft Windows built-in GUI tools

Part II

- Using external tools to fight BHO
- Using Microsoft Windows external tools
- Fighting rootkits
- Using Network-based tools to identify malware traces
- Using online resources to get help

Identifying and Removing Malware

**Course Outline**

**Identifying and Removing Malware**

One of the biggest challenges facing an enterprise environment today is to make sure that all its lines of defense are actually effective against new threats. Sometimes, even with several lines of defense such as firewalls, Intrusion Detection Systems (IDS), Intrusion Prevention Systems (IPS), antivirus gateways, host-Based firewalls, and host-based antivirus programs, a new threat may be occurring in one or more machines in the networked environment.

**Using the Built-In Tools**

**Part I**

It is important that companies understand how to properly use certain tools that are already installed in your system by default, both command-line interface (CLI) and graphical user interface (GUI) tools.

There are three types of built-in tools:

- Basic
- Advanced
- GUI

Basic tools such as Dir, Netstat, tasklist, taskkill, and findstr are easily accessed because they are usually somewhere along the Windows path environment variable. Advanced CLI tools such as Windows Management Instrumentation Command Line, or simply WMIC, (an interface for the Windows Management Instrumentation) enables useful queries to be done on the system to assist in fighting malicious code. The basic GUI tools are utilities available in Microsoft Windows, which help to track down malware programs and remove them.

## Course Outline (2)

**Our training will focus on two parts:**

Part I

- Using Microsoft Windows basic built-in CLI tools
- Using Microsoft Windows Advanced built-in CLI tools
- Using Microsoft Windows built-in GUI tools

Part II

- Using external tools to fight BHO
- Using Microsoft Windows external tools
- Fighting rootkits
- Using Network-based tools to identify malware traces
- Using online resources to get help

Identifying and Removing Malware

Part II
Additional tools exist and can be included in our toolkit to identify and remove malware infections. These tools include

BHO Tools
Microsoft External Tools
Rootkit Detectors
APT Style RAT (Remote Administration Tool)
Network Based Tools
Online Resources

From "Browser Helper Objects" (BHOs) to rootkits, programs are available to help you determine the causes of unexpected activity on your network. A Browser Helper Object is a DLL that allows developers to customize and enhance Internet Explorer. When installed the BHO has access to all the events and properties of the browser session.

Rootkits are nasty pieces of software that become so tied into the operating system that sometimes it may be better to do a complete reinstall of the system.

Since 2010, we could see a lot of target attacks usually referred to as Advanced Persistent Threats (APT). Most of these attacks were performed with the help of the Remote administration tools, also known as RATs, such as Poison Ivy, BlackShades, Gh0st, and DarkCommet.

Some malware may generate network activity, such as downloading an external component, posting hijacked information, connecting to command and control servers, etc. Packet capture trace tools help to identify this type of traffic. Many additional resources exist on the Internet, providing tools and utilities that can help analyze malware and give you tips about where to look for it on your system.

## Tools for This Module

- Dir: Windows built-in tool
- Netstat: Windows built-in tool
- Findstr: Windows built-in tool
- Tasklist: Windows built-in tool
- Taskkill: Windows built-in tool

Identifying and Removing Malware

**Tools for This Module**

Windows built-In tools include:

- dir
- netstat
- findstr
- tasklist
- taskkill

Windows comes complete with some old tools as well as some new ones that have been added in Windows XP and 2003. Windows 7, which is the base operating system of our training, has all these tools. Using some new tricks with the good, old Dir command, recently updated options of Netstat, and understanding how it can be useful for us, and some not so common CLI tools such as Findstr, Tasklist and Taskkill may help us get to the bottom of a pesky malware problem. These tools are available at the command prompt, good old DOS. Each tool has a set of options available, which can be listed by using the */? switch*. Sometimes, this is all you have to help you identify and remove malware infections on a system.

All of these tools are now available on Windows 8, Windows 7, Windows XP, 2003, and Vista, and, some of them were added in resource kits for Windows NT and Windows 2000.

## Some Definitions and Terms

- **CLI**: Command-line interface
- **GUI**: Graphical user Interface
- **WMIC**: Windows Management Instrumentation Command Line
- **BHO**: Browser Helper Objects
- **Key**: Registry Key

Identifying and Removing Malware

**Some Definitions and Terms**

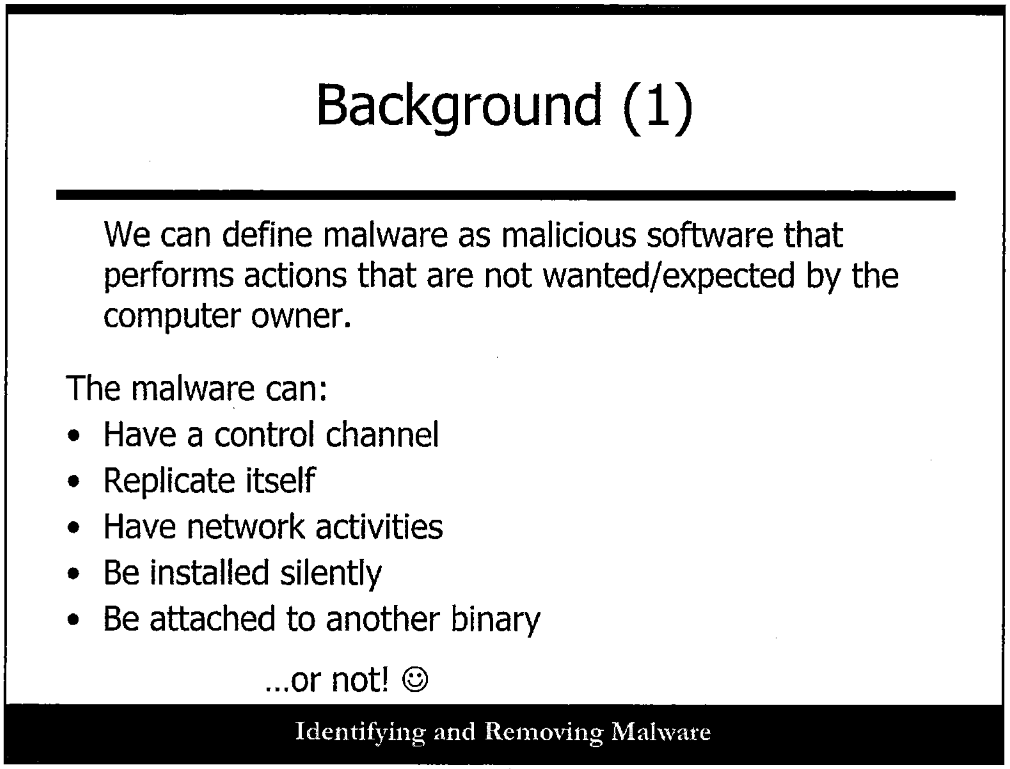
- CLI (Command Line Interface)
- GUI (Graphical User Interface)
- WMIC (Windows Management Instrumentation Command Line)
- BHO (Browser Helper Objects)
- Key (Windows Registry Keys)

If the terms on this page are not already part of your day-to-day vocabulary, they will be soon. They are critical tools and components of the Windows operating system and will be helpful as you begin to analyze and evaluate malware-infected machines.

- **CLI (Command Line Interface)**: These are tools that are built-in to Windows and that can easily be accessed from the DOS prompt (for example, dir, cd, del, and such).
- **GUI (Graphical User Interface)**: These are tools that are accessible through Windows and use graphical elements such as windows, icons, and buttons and allow the use of a mouse for point-and-click navigation (for example, Regedit, TaskManager, and Windows Explorer).
- **WMIC (Windows Management Instrumentation Command Line)**: A powerful extension of regular Windows CLI. Introduced on Windows XP and 2003, it offers a powerful range of tasks and has its own query language, called WQL.

- **BHO (Browser Helper Objects)**: Since Internet Explorer 4.x, developers got an opportunity to create special applications that can be loaded together with the browser and have almost complete control over Internet Explorer. These help monitor activities such as download attempts and calls to a downloader manager. But these are also used by malware to monitor browsing sessions, URLs, passwords, and so forth. Although the term BHO applies to Internet Explorer only, you can find the same type of objects in other browers such as Chrome or Firefox.

- **Key (Windows Registry keys)**: Stores operating system settings, options, and most software and hardware used by the operating system (OS). Malware programs often change some of these settings to hide themselves or to disable various operating system functionalities.




**Background (1)**

**Warm-Up**

Before starting with the tools, you need to understand some of the typical behavior of malware and the tricks used by some malware when installed on a computer, such as hiding itself or configuring the system to load the malware every time the system boots, and the usual places that malware hides. This understanding can help you to determine the type of malware you are dealing with.

A malware program can be described as malicious software that performs actions that are not wanted or expected by the computer owner. It can present different behaviors depending on its purpose. Today's malware falls into the following behavioral categories:

- **Control channel**: This is the typical behavior of Bot programs, robot programs that are controlled by a malicious third party. It connects to a remote server, usually an Internet Relay Chat (IRC) server, to receive instructions such as scanning for vulnerable machines on the network, searching for documents on the hard drive, and more. A lot of recent bots use HTTP as a command and control mechanism or even other Peer-to-Peer (P2P) protocols.
- **Install as add-on or plug-ins from shareware applications and display unwanted advertising:** A lot of "free" applications will install unwanted extensions and/or plug-ins for browsers.
- **Replicate**: Malware can copy itself to different folders/locations within the OS and hard disk. These folders can be, for example; P2P shared folders, folders with a random name, or may use names of popular things such as a rock star video.
- **Generate network activity:** It is typical behavior for a worm to infect a machine and then go looking for other machines to infect that have a similar vulnerability. The network traces for these worms can be similar to a Bot. The difference being a worm typically doesn't have a control channel whereas a Bot does.

- **Installed silently**: The binary may be installed silently, which means that when you try to run it, such as by double-clicking it, nothing visible happens. Or it may use a deceptive trick, like opening a file in notepad or displaying a picture to hide the real intent, which is to install the malware in the background.

- **Attached to another binary**: This is a typical parasitic behavior whereby the malware attaches itself to other legitimate programs on the computer. For example, it can attach itself to the Notepad application file, notepad.exe, and while the notepad program still works as wanted, it also performs other actions defined by the malware author.

## Background (2)

- Basic behavior of most malware:
  - Using the Windows environment and tools to hide itself:
    - Like using Attrib.exe
    - Adding itself to selected Registry keys so that it will reload on reboot
    - Copy itself to different directories to avoid "eye" detection!

Identifying and Removing Malware

**Background (2)**

Most malware attempts to keep running undetected on a system for as long as possible, sometimes using the own system environment and its tools to accomplish it. It uses various methods to avoid detection and makes removal extremely difficult.

One clear example of how effective some malware is at hiding is by looking at the world of botnets. On some communication channels that are used for command and control of the bot malware, it is possible to see the bots reporting their status as shown here:

[17:11] <[x]32705837> [MAIN]: Uptime: 2d 6h 49m.
**[17:11] <[x]62694986> [MAIN]: Uptime: 0d 7h 0m.**
**[17:11] <[x]77045269> [MAIN]: Uptime: 23d 8h 10m.**
[17:11] <[x]10568877> [MAIN]: Uptime: 0d 8h 8m.

The third entry shows that a bot malware has been running on a machine for more than 23 days, presumably without detection by the machine owner! To achieve this objective malware tends to use some basic techniques. One trick being utilized is scripting to mask the software after installed by changing the physical appearance of the file in the directory structure. A simple script may call the CLI tool attrib.exe to change the attributes of the malware, such as:

- **Attrib.exe +h *filename.exe***: To put the *filename.exe* in hidden mode and avoid it being shown when listing directories with the dir command.

- **Attrib.exe +r *filename.exe***: To put the *filename.exe* in Read-Only mode, avoiding deletion with the del command.
- **Attrib.exe +s *filename.exe***: To put the *filename.exe* in System file mode, preventing it from being shown when listing directories with dir and avoiding deletion with *del* command.

Also, most malware change some Registry keys to activate what may be termed the "I'll be back" mode. This means they have to make sure that when the user reboots the machine, the program will be loaded again.

And as a last common behavior, you can have multiple copies of it in different directories, always referenced in the Registry keys. But in almost 99% of cases, the most common directory used by malware is the windows\system32 folder, which is always in the path for the user.

In addition, they also try to use rootkits, which you learn more about later.

## Background (3)

### Most frequently used Registry keys:

- HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Run
- HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run
- HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\RunOnce
- HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\RunOnce

Identifying and Removing Malware

**Background (3)**

**Windows Registry Keys**
The Windows Registry stores operating system settings and options and settings for most software and hardware used by the OS. These options control the behavior of the computer hardware and software both at system startup and during system operation. Many programs that are started at boot time are configured using Registry keys. For example, you may have a Registry key with the name ITunesHelper, and the value of the key could be C:\Program Files\iTunes\iTunesHelper.exe. When malware infection takes place on a computer, entries or modifications may be made to those keys that allow the malicious program to take control of the computer. Using Regedit.exe, the Registry editing program that comes with Windows, you can quickly determine applications that are running at system startup by checking the entries in the locations described here.

For the newer version of Windows (XP, 2003, Vista, and 7)[1] the following four keys can perform this action:

- HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Run
- HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run
- HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\RunOnce
- HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\RunOnce

*On Windows 7, the standard user does not have permission to run from HKEY_LOCAL_MACHINE*

For older versions of Windows (95/98/ME/NT/2000)[2] Microsoft specifies seven Registry keys that make software run automatically when the system starts, ensuring the "I'll be back" mode.

- HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Run
- HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run
- HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\RunOnce
- HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\RunOnce
- HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\ RunServices
- HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\ RunServicesOnce
- HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\ RunOnce\Setup

[1] http://support.microsoft.com/kb/314866/EN-US/
[2] http://support.microsoft.com/kb/137367/EN-US/

# Background (4)

## Most frequently used directories:

- %windir% (\windows\)
- %systemroot%\system32 (\windows\system32\)
- \Documents and Settings\<username>\StartMenu \Programs\Startup
- \Users\<username>\AppData\Local\ (Windows 7)

Identifying and Removing Malware

**Background (4)**

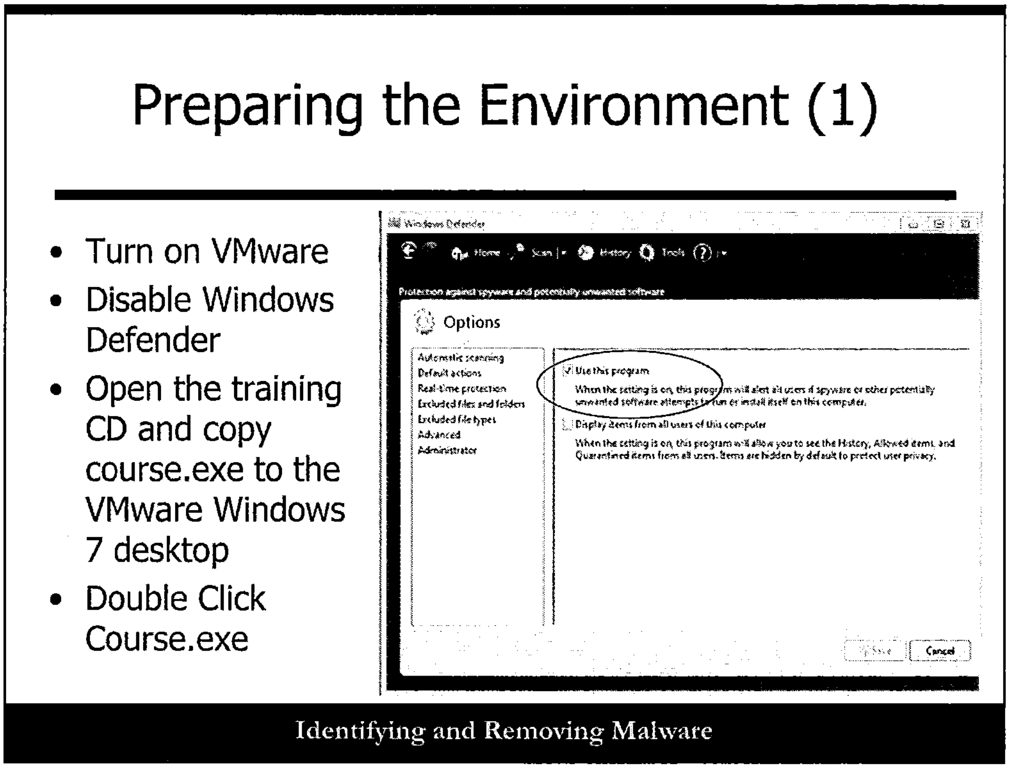
**Malware's Most Frequently Used Directories**

Most malware programs tend to copy themselves to the Windows and/or Windows\System32 directories. The main reason for this is that these directories are in the users PATH environment variable, and the programs can be started or run without having to be in the actual directory. This means that most of the time you can find the malware program by searching those directories for anomalies. This is not always the case, of course, and malware can reside in any folder and can be accessed either by adding the folder to the PATH environment variable or by referencing the malware application with a complete path such as c:\my malware folder\bad_app.exe

Another option that the malware author has is to use the computer startup folder to initiate and run the program each time Windows starts. All files or shortcuts that are in the startup folder will be executed each time Windows starts. The folder is usually at:

\Documents and Settings\<*username*>\StartMenu\Programs\Startup

One disadvantage to the malware author is that it is visible by looking in Start → Programs → StartUp. This is probably why this is the least preferred of the methods used. This folder has the same meaning as the "I'll be back" mode Registry keys because all programs in it will be loaded each time the user logs in to the system.




**Preparing the Environment (1)**

In this step, you prepare the training environment. There are just a couple of steps in this phase:

1. Turn on your Vmware.
2. Load the Windows Image that you pre-installed.
3. Disable Windows Defender:
   - Click the Start Button, type "Windows Defender," open it, click on Tools, and then click Options. Go to Administrator options and uncheck the box "Use this program."
   - This step is necessary to run some of the exercises that have real malware code.
4. Open the training CD that you received and copy course.exe to the VMware Windows 7 desktop.
5. Double-click course.exe file to complete the extraction of the files needed for the training.

## Preparing the Environment (2)

- Create a Snapshot of your clean Windows 7 install and call it Clean7
- Important: Run both tools and malware as Administrator
- Remember that the answers for all hands-on labs can be found in the end of the module.

Identifying and Removing Malware

**Preparing the Environment (2)**

6. Create a Snapshot of your clean Windows 7; install, and call it Clean7.
7. On the VMware menu, select VM, Snapshot, and then select the Take Snapshot option.

These steps prepare your system so you can follow the examples demonstrated in the course.

Important: When a malware gets installed on the system, it may be installed as Administrator. It depends on several aspects, such as the use of exploit, elevation of privilege, etc. For this reason, to mimic the worst scenario, you always run the malware as Administrator. The same rule applies for the tools you use to get most of them; you also run them as Administrator.

For the command-line tools, you open the CMD.exe as Administrator as well.

For CMD.exe, click Start -> Type CMD on the search box. Right-Click the CMD.exe and select Run as Administrator.

For Tools and Malware: Right-click and select Run as Administrator.

All answers for the Hands-On Labs can be found in the last section of today's module in the section "Hands-On Answers."

# Identifying and Removing

## Using Windows Basic Built-in CLI Tools to Identify and Remove Malware

Identifying and Removing Malware

**Using Windows Basic Built-In CLI Tools to Identify and Remove Malware**

Now that we have identified some of the behaviors and tricks used by most malware programs, we look at how to use the basic DOS tools to assist in identifying the malware and removing it. The basic CLI tools are already installed in your system. These tools Dir, netstat, tasklist, taskkill and findstr, can help us track down malware when it has damaged the Windows interface, and the only way to boot the computer is in Safe Mode – Command Prompt Only. In this mode, the GUI tools are unavailable so all that may be available is the Basic CLI tools.

# MS Windows CLI Tools: DIR (1)

- Introducing: Dir
  - Basic function: List files and directories
  - Old time tool!
  - Introduced on DOS 1.0 in 1981!
  - Still a valuable tool for looking for files!

Identifying and Removing Malware

**MS Windows CLI Tools: DIR (1)**

Remember dir? Yes, it is an old tool introduced with the first version of DOS, in 1981! The basic purpose of the dir command is to show the files and directories on a system. This command is still one of the most-often used CLI tools. Most people use it to show only the basic characteristics of the files in a specific directory—the date, time, file length, filename, and <DIR> if it is a directory. For example:

```
01/16/2012  04:16 PM    <DIR>        pedro
07/03/2011  11:25 AM    <DIR>        Public
           0 File(s)           0 bytes
           4 Dir(s)  206,438,273,024 bytes free
```

When you make use of the different options it offers, it can search for files flagged as *Hidden* or *System*. These attributes are often used by malware programs and may be indications of a malware program installed on the system. As you will see, there are some helpful options and switches that can be used with the dir command to provide some valuable information about the characteristics of the files listed.

# MS Windows CLI Tools: DIR (2)

- More options on DIR:
  - /a: show files with attributes –Useful and you can search the entire hard drive
  - /s: Scans the current directory and all subdirectories
  - /o: Sort the way the files display. I like the /O:d option, which sorts by date, so you can see the last files added!
  - /t: sort by timefield (Creation, Last Access, Last Written). It is also useful to use with scripts and finds recently accessed files!

Identifying and Removing Malware

**MS Windows CLI Tools: DIR (2)**

**More Options on dir**

In addition to the regular and common usage of the dir command, it also offers some more advanced and useful options that can make your life easier when looking for suspicious files.

There are many useful options:

- /a: With this option, used in combination with a colon ":" and the file attribute you are looking for, it also lists the files that have any attribute set such as hidden files (a:H", read-only files (a:R) and system files (a:S). Some malware can set the attribute of files as hidden, +h, to hide files from a normal dir listing. Using this option, you can list all files regardless if an attribute is set.

    Example: dir /a:R lists the files that are read-only

- /s: This option enables you to search for a file in a recursive way. This means that it searches for the requested filename in the current directory and all subdirectories. So, if you are on the root of C:\ it searches for the file in all the folders and subfolders of the C drive.

    Example: dir *.dll /s searches for all files in the target folder and all its subfolders and that have an extension of dll.

- /o: The sort option offers different ways to sort the way the files display. I prefer to sort by date. This allows me to see the last files added, which makes it easy to spot recently added files.

- /t: If you want to know when a file was last accessed, you definitely need this option. It can show when a file was last accessed or created, for example:

C:\dir /t:a putty.exe

*Results in the following being displayed:*

*Volume in drive C has no label.*
*Volume Serial Number is xxx-xxxx*

*Directory of C:*

*05/06/2007 20:01 421.888 putty.exe*
*1 file(s) 421.888 bytes*
*0 Dir(s) 9.680.445.440 bytes free*

C:\dir /t:c putty.exe

*Results in the following being displayed:*

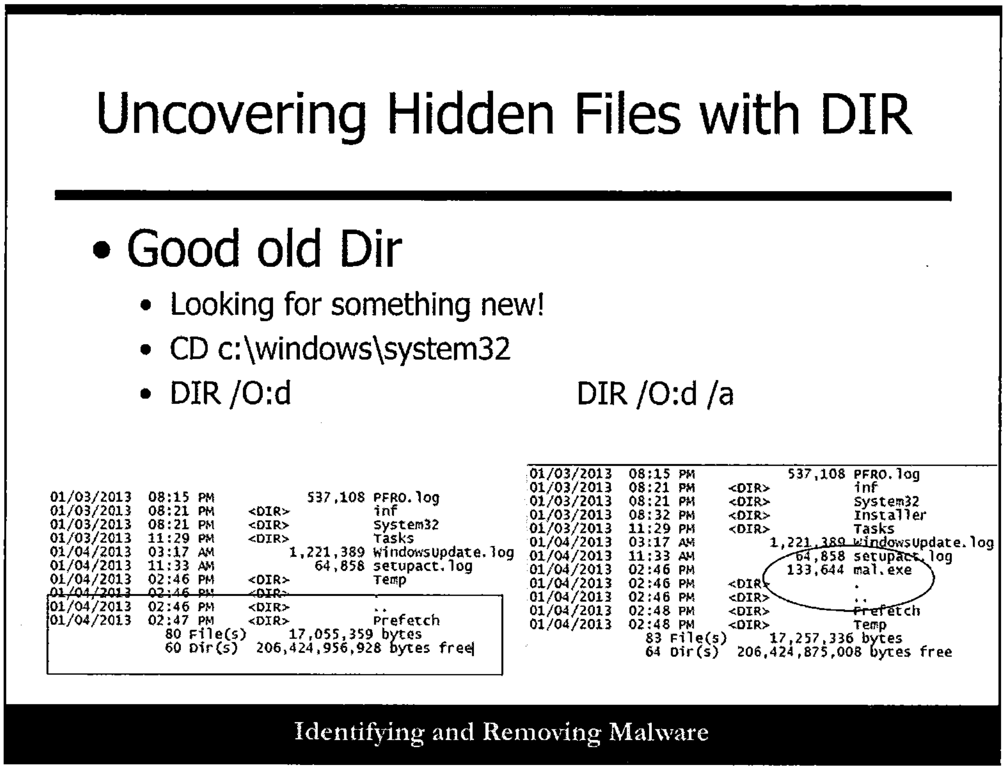
*Volume in drive C has no label.*
*Volume Serial Number is xxx-xxxx*

*Directory of C:*

*05/22/2006 21:13 421.888 putty.exe*
*1 file(s) 421.888 bytes*
*0 Dir(s) 9.680.445.440 bytes free*

To find out what other options are available with this helpful DOS command, you can get a complete list by using the /? switch.

C:\>dir /?




**Uncovering Hidden Files with DIR**

**Old and Good dir**

When a malware program is installed on the system, it can use some techniques to hide itself from detection such as using the attrib.exe tool. When using the dir command with the different switches, you can sort the directory view by date (dir /O:d), which shows the oldest first, making it easy to see the latest files added to that directory. You can combine sorting by date with other file attribute filtering such as:

dir /O:d /a:h (hidden)
dir /O:d /a:s (system file)
dir /O:d /a:r (Read-Only)

As shown in this example, using dir /O:d /a it is possible to see that the file mal.exe was recently added on the system and that it was not visible using the plain dir command on the left versus using the /a option in the second dir command (example on the right). That makes it suspicious!

## MS Windows CLI Tools: Tasklist (1)

- Introducing: Tasklist.exe
  - Basic function: List running processes on a local or remote system
  - Introduced in Windows XP
  - Useful to list applications when you have limited GUI access to the system, such as malware that blocks access to some GUI tools

Identifying and Removing Malware

**MS Windows CLI Tools: Tasklist (1)**

**Introducing tasklist.exe**

The program tasklist.exe is a great CLI tool added in Windows XP and is present in Windows 7 and 8. With this tool it is possible to list the standalone processes and services running on the computer directly from the DOS prompt, even remotely.

Remember that malware can be running on your computer as:

- A single process
- Multiple processes
- A service
- Injected into an existing, legitimate process or service

# MS Windows CLI Tools: Tasklist (2)

- More options of Tasklist:
  - /v: for verbose info. Useful because you can get extra information such as UserName and the Window Title of the process
  - /svc: Shows the services as well. A lot of times a malware can be executed as a service instead of a simple process!
  - /fi: Perhaps the most powerful option. It enables you to filter by any specified information shown with the /v option like Status,Imagename, PID, Session,SessionName, CPUTime, MemUsage, Username, Services, WindowTitle, and Modules. And can be used with operators such as eq, ne, gt, lt, ge and le
  - For example, to list any process in which the username is *not equal* to "NT Authority System" and the PID is greater than 2000, you could use:
    - TASKLIST /FI "USERNAME ne NT AUTHORITY\SYSTEM" /FI "PID gt 2000"

Identifying and Removing Malware

**MS Windows CLI Tools: Tasklist (2)**

**Using Options with tasklist.exe**

Tasklist is a powerful tool that enables you to combine different options to get the information that you need about the programs, processes, or services running on the system.

The tasklist.exe program has several built-in operators for filtering the information:

- **Eq**: equal
- **Ne**: not equal
- **Gt**: greater than
- **Lt**: less than
- **Ge**: greater than or equal
- **Le**: less than or equal

Some other options:

The filtering option: Enables you to filter the output based on username, that is:

- Tasklist /svc /fi "USERNAME eq pbueno"
  - This command lists all processes that are running with the username of pbueno

The format option allows you to get the output in the default 'table', csv, or list format:

The csv will show something like:

- "tasklist.exe","2280","N/A": respectively process, PID, Service

The list will show something like:

| | |
|---|---|
| Image Name: | tasklist.exe |
| PID: | 2280 |
| Services: | N/A |

To find out what other options are available with this helpful DOS command, you can use the /? switch to get a complete listing.

C:\>tasklist /?

## MS Windows CLI Tools: Tasklist (3)

- Introducing: tasklist.exe
  - On a previous slide we saw that a new file was found. Now, let's see if it is running on the system.
  - Basic raw usage gives you the Image Name, Process ID, Session Name, Session ID, and Memory usage:

| Image Name | PID | Session Name | Session# | Mem Usage |
|---|---|---|---|---|
| ============ | ====== | =============== | ======== | ======== |
| System Idle Process | 0 | Console | 0 | 28 K |
| <edited for better readbility> | | | | |
| mal.exe | 3332 | Console | 0 | 52 K |

Identifying and Removing Malware

**MS Windows CLI Tools: Tasklist (3)**

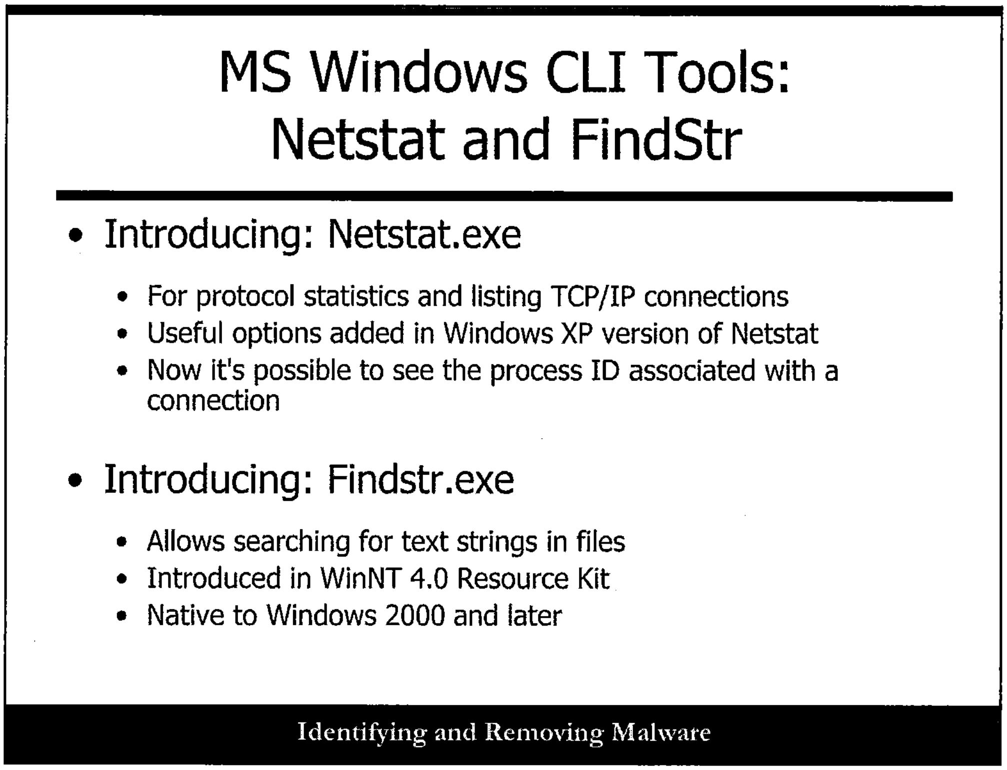
**Introducing Tasklist.exe**

Entering the basic command tasklist.exe with no options lists the Image Name (program), Process ID (PID), Session Name, Session#, and the amount of memory in use by the program (Mem Usage). The good thing is that you can see all running processes on the machine. The downside is that you can easily get lost with the large amount of information provided to you.

A better solution (if you already know the specific filename that you are looking for) would be:

```
tasklist /svc /fi "imagename eq mal.exe"
```

This would give information related to only the processes that are running as a result of the program specified. In this example, it shows the mal.exe file we found in the windows/system32 directory is running and has the process ID (PID) of 3332.




**MS Windows CLI Tools: Netstat and FindStr**

**Introducing netstat.exe and findstr.exe**

Two additional tools that may be of value in tracking down malware programs are Netstat and Findstr.

Netstat is a useful tool in the UNIX world, and over the past years in the Windows world as well. It helps you to identify the established network connections, as well as the ports and protocols your machine is serving to the outside world and locally.

Findstr is another interesting application that was added since Windows 2000. This application is equivalent to Grep in the UNIX world. It is useful when searching for specific strings inside of files, as well as for searching the output information generated by other applications.

## Useful Options of Netstat

- More options with Netstat:
  - -a: Shows you all running processes, which is what you want to see most of the time
  - -n: Does not try to resolve names. It is faster, and if you are in a hurry, is the option that you want to use
  - -o: Cool option added on recent versions of Windows XP, Vista, and 7. It also displays the Process ID (PID) associated with the connection. Useful to track any suspicious process

Identifying and Removing Malware

**Useful Options of Netstat**

**Using Netstat and Its Options**

When using netstat, two of the most used options are

- -a: The most common option shows you all the processes and enables you to see all the connections on your machine.
- -n: This option displays the addresses and port numbers in numerical format. It also displays the information faster because it doesn't have to resolve the IP to DNS names. If you are in a hurry, this is the option that you want to use.

So using these options you would have an output that looks something like:

| Proto | Local Address | Foreign Address | State |
|---|---|---|---|
| TCP | 0.0.0.0:80 | 0.0.0.0:0 | LISTENING |

This indicates that there is a process/application listening on port 80, but you don't know which one it is.

One missing option on Netstat prior to Windows XP that was present in the UNIX version was the ability to see the process ID associated with the connection. In the UNIX version the switch –p would show all associated processes. Starting with Windows XP, Microsoft decided to add this as a Netstat option as well. Now using the –o option, in Windows, allows you to see which process ID (PID) is associated with that connection. This option is still valid in Windows 7 and 8.

Another useful option is the –o option. This option according to the Netstat help:

- -o: Displays the owning process ID associated with each connection.

So the output of netstat –aon would result in something like:

| Proto | Local Address | Foreign Address | State | PID |
|---|---|---|---|---|
| TCP | 0.0.0.0:80 | 0.0.0.0:0 | LISTENING | 1832 |

Now you can do a specific query with task list, as discussed earlier, and identify this process!

To find out what other options are available with this helpful DOS command, you can get a more complete help file by using the /? switch.

C:\>netstat /?

# Using Findstr to Search the Output

## • More options with findstr:

- The simple usage of findstr is already useful, for example, to search for "URL" inside the mal-strings.txt you simply use:
  Findstr "URL" mal-strings.txt

- findstr can search for strings directly from the output of another application like this:
  Dir | findstr "mal": Shows you all files that have the string "mal" in the filename.
- -i option makes it case-insensitive:
  Dir | findstr –i "mal": Displays both MALware.exe and malware.exe

Identifying and Removing Malware

**Using Findstr to Search the Output**

**Using findstr.exe and Its Options**

If you have a large text file and want to know if there is a string "URLDOWNLOAD" inside this text file, you can simply do:

```
C:\ more textfile.txt | findstr "URLDOWNLOAD"
```

This command shows all instances of "URLDOWNLOAD" that appear in the file!

Maybe the best usage of findstr is the ability to use it to search the output of the information generated by another application, such as:

```
C:\dir /s | findstr "malware.exe"
```

In this example, the output from the dir /s command will be sent as the input to the findstr command, which then searches for filenames that have "malware.exe" in their name!

To make it case-insensitive just add the –i (or /i) and it is done!

To find out what other options are available, with the helpful little DOS command, you can get a more complete help file by using the /? switch:

```
C:\findstr.exe  /?
```

## Netstat and FindStr Together

- Introducing: netstat.exe and findstr.exe
- On previous slides, we noticed that a suspicious file was running on the system. Our next step is to identify if it has any kind of network traffic associated with it.
- Using netstat with options –ano and findstr, it is possible to query for our specific process ID (3332):
- C:\netstat -ano |findstr 3332

| Proto | Local Address | Foreign Address | State | PID |
|---|---|---|---|---|
| TCP | 192.168.0.12:1081 | xxx.34.124.34:6667 | ESTABLISHED | 3332 |

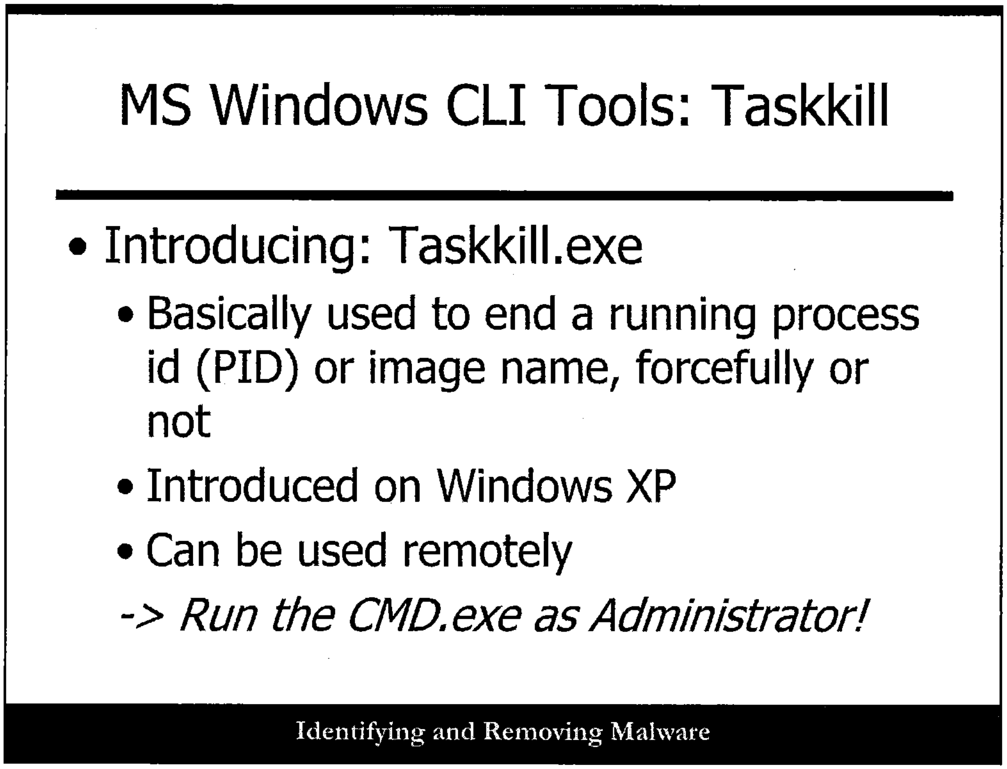
Identifying and Removing Malware

**Netstat and FindStr Together**

**Using Netstat.exe and Findstr.exe**

As we have discussed, you can use a combination of netstat and findstr to find the information you need to track down a process. You have already found the process ID (PID) of the running process, a netstat listing of the process IDs of all connections and a findstr to show only the process ID. That information is then quite useful to speed up the process of finding the malware!

In this case, you can see that the suspicious process had an established connection with a foreign address on remote port 6667! This makes this process even more suspicious because 6667 is the common port for the IRC service and is widely used by bots and botnets! This fact can lead to further investigation leaning in the direction of an IRC-related bot infection.




**MS Windows CLI Tools: Taskkill**

**Introducing Taskkill.exe**

Now you can query the system and get all the information regarding a malicious process such as the image name and/or process ID (PID); however you still lack a way to terminate it. In the UNIX world whenever you want to terminate a process, forcefully or not, you can use an application called kill.

Microsoft decided to create a similar useful tool and introduced Taskkill in Windows XP. This CLI tool makes it possible to kill standalone processes and/or services running on both the local computer and on a remote computer if you provide the proper domain username and password.

As with many of the commands executed in this course, it is recommended that you open the command prompt as Administrator. To do this on Windows 7, go to start, type cmd.exe on the search box, and wait for it to appear on the search results. Now, right-click and select Run as Administrator.

# Killing Processes and Services with Taskkill

- More options on taskkill:
- A "tasklist" to kill processes: Basically, same options as tasklist, but to kill a process
- Nice option to choose to kill by Process ID (PID) number or ImageName!
- Can also use operators:
    - eq, ne, gt, lt, ge, and le
    - And kill with a combination of Status,Imagename, PID, Session,SessionName, CPUTime, MemUsage, Username, Services, WindowTitle, and Modules
- Most common usage:
    - Kill by PID: taskkill /PID 2000
    - Kill by ImageName: taskkill /IM cmd.exe

Identifying and Removing Malware

**Killing Processes and Services with Taskkill**

**More Taskkill Options**

One of the basic features of this program is the ability to kill a process/application using either the Image Name (that you get from tasklist, for example) or by process ID (PID).

```
taskkill.exe /IM malware.exe
taskkill.exe /PID 1234
```

But it also allows you to combine different filtering options to kill the exact process using both operators like:

**Eq**: equal
**Ne**: not equal
**Gt**: greater than
**Lt**: less than
**Ge**: greater than or equal
**Le**: less than or equal

…and the regular filtering names such as Status, ImageName, PID, Session, CPUTime, MEMUsage, UserName, Modules, Services, and WindowTitle.

So you could get a command like:

TASKKILL /F /IM putty.exe — Force to kill the process with image name putty.exe

TASKKILL /F /FI "IMAGENAME eq putty.exe" — Force to kill all the process(es) that match the filtering criteria where imagename equals putty.exe

Two different ways to kill the same process using the ImageName!

To find out what other options are available with this helpful DOS command, you can get a more complete listing by using the /? switch.

C:\taskkill.exe /?

# Taking Action

- Taking action:
  - Recent file added on windows\system32 folder
  - The suspicious file is running on our computer
  - The suspicious process has an active connection to a foreign address on IRC port (port 6667)!

So, it is time to take an action!

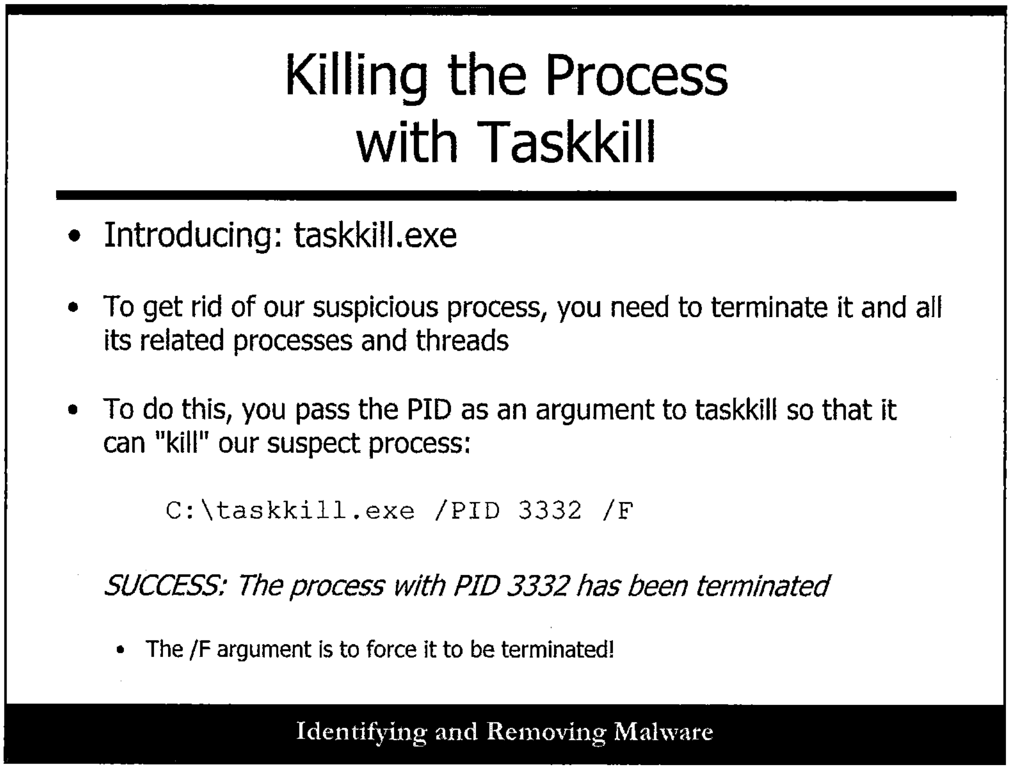
Identifying and Removing Malware

**Taking Action**

If you remember the steps followed so far, you can see that you have learned how to:

- Identify a recently added file on the system.
- See what is running on the system.
- See what has a network connection (on port 6667!).

Putting all these pieces together, it may be necessary to stop this running process so that you can actually remove it.




**Killing the Process with Taskkill**

**Using Taskkill.exe**

In the previous slides, we identified the running process and got the process ID, (PID 3332). We also learned that there is a tool in Windows XP that allows the termination of a process and/or service.

Using taskkill with the /PID switch, we can kill this process like this:

C:\taskkill.exe /PID 3332 /F

SUCCESS: The process with PID 3332 has been terminated

To be sure that you are successful in your attempt to stop the process, it is recommended that you use the /F switch to force it to be terminated. This allows the process to be terminated while the program is running, without getting a message that the process could not be terminated.

# Using Windows Basic Built-in CLI Tools to Identify and Remove Malware

# Hands-on – Lab 1

Identifying and Removing Malware

**Basic CLI Tools Hands-On**
In this module, you learn about some basic CLI tools provided on Windows 7. You can follow these examples on your VMware Windows 7.

To make it possible, open the Course.exe file on the desktop of your VMware Windows 7. Then, open the Part 1 folder, right-click the cli.zip file, and select the option Extract All to extract the contents.

Because it was compacted with a password, you will be prompted to enter this password. All files on the CD are protected with the password training, which you should enter without quotes. Now open the new folder created, called cli, and execute the cli.exe as administrator.

Go to the DOS command prompt and to the windows/system32 directory:

-> cd c:\windows\system32

**Questions**:

1. How many files were added to the Windows System32 directory? (Tools of interest: dir)
   2 Badfile1.exe ? Owned.log 1dir inetsrv contains smc.exe
2. Are any of them running? (Tools of interest: tasklist)
   smc.exe
3. Can you identify any network connections associated with those files? (Tools of Interest: netstat)
4. How can you kill that connection? (Tools of interest: tasklist, taskkill)

# Identifying and Removing Malware

## Using Windows Advanced Built-in CLI Tools to Identify and Remove Malware



This page intentionally left blank.

# Microsoft Windows WMIC

- Introduced in Win XP Pro and Win 2k3
- Interact with Microsoft WMI (Windows Management Instrumentation) framework
- No more complex scripts
- WMI gives direct access to configuration and settings

Identifying and Removing Malware

**Microsoft Windows WMIC**

**Introduction**

If you are one of those people frustrated with not having a more advanced way to perform tasks at the Windows command line, you will be happy to hear about Windows Management Instrumentation Command Line (WMIC), which was introduced in Windows XP Pro and Windows 2003. All the Windows advanced built-in CLI tools can be found in one utility: WMIC.

If you know the UNIX world, you know that you can have several scripting languages such as Python, TCL, and so on, so you can create scripts to perform various actions that you want. With WMI, you can also create scripts to access configurations and settings, but Microsoft creates an easier way to do it directly from the command line with WMIC.

## Microsoft Windows WMIC/WQL

- Introducing WQL: WMI query language!
- ANSI-like query language
- WMIC Console versus DOS prompt

Identifying and Removing Malware

**Microsoft Windows WMIC/WQL**

**Introducing WQL**

Now that you know there is a more advanced way to perform tasks from the command line, you learn how this can be accomplished. If you use the UNIX world example again, taking either Python or TCL, running the executable displays the version information.

Python example:

```
lab2:~# python
Python 2.3.5 (#2, Oct 16 2006, 19:19:48)
[GCC 3.3.5 (Debian 1:3.3.5-13)] on linux2
Type "help", "copyright", "credits", or "license" for more information.
>>>
```

TCL example:

```
lab2:~# tclsh
%
```

Those examples show the Python and TCL languages ways to access the console, and from the console execute the programs, which is pretty much what you will do with WMIC/WQL.

# Windows WMIC: Console

- Firing up WMIC console: `wmic`
- The WMI console prompt: `wmic:root\cli>`
- A simple /? switch gives you the help file
- Unfortunately, Microsoft documentation is not informative about WMIC!

Identifying and Removing Malware

**Windows WMIC: Console**

If you remember the previous slide, about the UNIX TCL and Python, you are familiar with the way to call the WMIC tool. Simply typing **WMIC** at the DOS prompt gives you the WMIC shell, so you can start to use it:

C:\Users\pedro>wmic
wmic:root\cli>

Or if you prefer you don't have to enter into WMIC console, just type on the Dos prompt: **wmic <command>** as you will see.

I prefer to use the console mode, but if you like to use redirectors, or pipe, you may want to use it directly from the Dos prompt.

To get complete help, you can just use:
C:\wmic /?

This command will generate a large output with a lot of helpful information for you.

Unfortunately, Microsoft doesn't provide adequate help information in either its Help file or online. As you can see at the Microsoft website, it provides only basic information about it (http://www.microsoft.com/resources/documentation/windows/xp/all/proddocs/en-us/wmic.mspx?mfr=true).

## Remembering SQL

- Query languages are usually intuitive
- Simple basic ANSI-SQL `select` query is powerful
- No need to understand advanced SQL queries

Identifying and Removing Malware

**Remembering SQL**

**SQL Queries**
For people that never played with databases, the SQL language may be a little difficult to use and understand. For this reason, you do not go into an advanced SQL example. Advanced SQL is not needed to accomplish our basic tasks with WMIC.

In the example, imagine a fictitious database called Corporate that can have multiple tables.

Our boss would like to know who inside the SANS organization has admin access to the system. A basic SQL query on the database can check the SANS table only and ask which users have the admin access field set. The resulting output would show the users that have Admin rights.

Our SANS table has the following fields:

| | |
|---|---|
| Username | – The username used on the system |
| City | – Location of the user |
| Date of Birth | – User's date of birth |
| E-mail | – User's e-mail |
| Admin | – If the user has Admin rights |

Our SANS table is populated with the following data:

| Username | City<br>e-mail | Date of Birth<br>Admin |
|---|---|---|
| Jbrain | Portland<br>john@55.sans.org | 03/04/73<br>no |
| Odeman | Boston<br>odeman@55.sans.org | 02/11/70<br>ok |
| Norain | Washington<br>norain@55.sans.org | 07/10/78<br>ok |

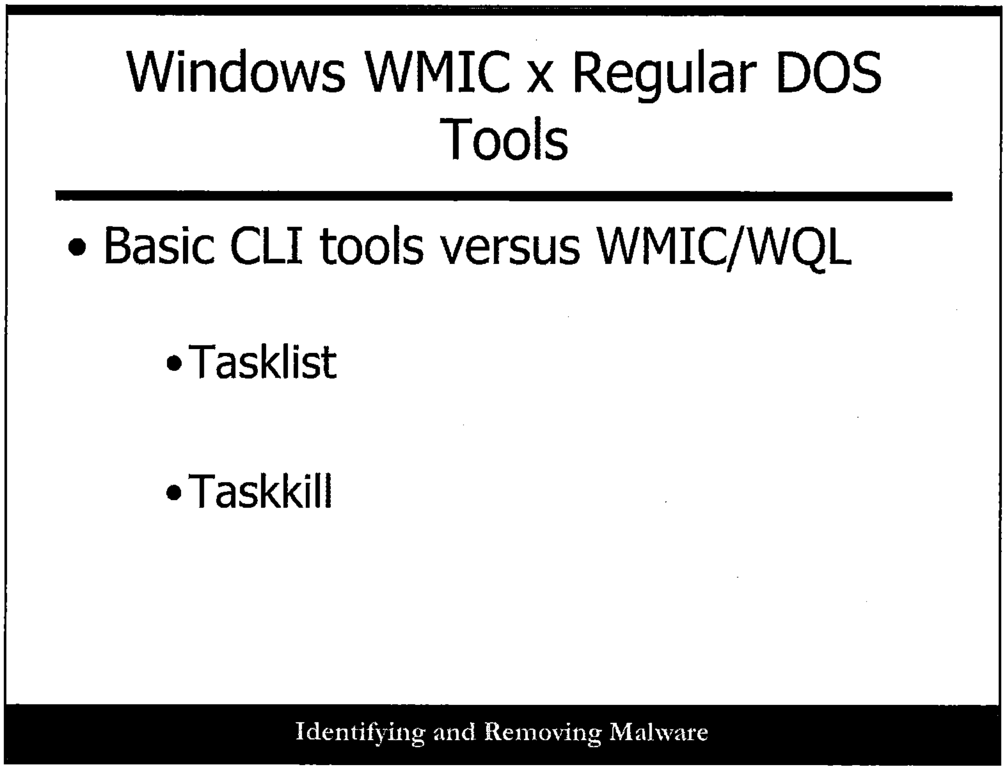
Then using the following, query on the preceding table:

>Select username from SANS where admin = 'ok'

would return the following information:

| | | | | |
|---|---|---|---|---|
| odeman | Boston | 02/11/70 | odeman@555.sans.org | ok |
| norain | Washington | 07/10/78 | norain@555.sans.org | ok |

This is a basic example of SQL language but helps us to understand how the WMIC and WQL applications work!




**Windows WMIC x Regular DOS Tools**

**Basic CLI tools Versus WMIC/WQL**
WMIC can provide a number of different actions to the user, such as the ones performed by some of the actions that you saw in the previous module: listing the processes with the tasklist.exe tool and terminating a process with the taskkill.exe tool.

To better understand how WMIC works, we start with a comparison between those standalone tools and WMIC/WQL.

# Windows WMIC: An Advanced Tasklist Command (1)

- The basic CLI tool tasklist shows the processes running on the machine
- Listing processes running with WMIC:
  - While in the WMIC console, simply ask it to list the process in a brief way:
  - wmic:root\cli>process list brief
  - This command shows the following fields: HandleCount, Name, Priority, ProcessId, ThreadCount, and WorkingSet

Identifying and Removing Malware

**Windows WMIC: An Advanced Taskkill Command (1)**

**WMIC Versus Tasklist**

One favorite use of WMIC is to list processes. It can give you different ways to see all the processes running on the machine. In our example, we use the output view called brief, which shows the most important fields in a malware analysis perspective, such as the name and PID.

| HandleCount | Name | Priority | ProcessId | ThreadCount | WorkingSetSize |
|---|---|---|---|---|---|
| 0 | System Idle Process | 0 | 0 | 1 | 28672 |
| 1936 | System | 8 | 4 | 78 | 253952 |
| 25 | smss.exe | 11 | 1412 | 3 | 372736 |
| 1061 | csrss.exe | 13 | 1508 | 13 | 5111808 |
| 533 | winlogon.exe | 13 | 1532 | 21 | 5795840 |

But there are other views of listing the process, such as:

- BRIEF
- FULL
- INSTANCE
- IO
- MEMORY
- STATISTICS
- STATUS
- SYSTEM

The syntax is the same, but instead of brief, you can choose among the preceding ones.

# Windows WMIC: An Advanced Tasklist Command (2)

- As with most of WMIC commands, the processes can also be seen with WQL
- To list all processes that have the name svchost.exe, you could use:

```
wmic:root\cli>process where
name='svchost.exe' list brief
```

Identifying and Removing Malware

**Windows WMIC: An Advanced Taskkill Command (2)**

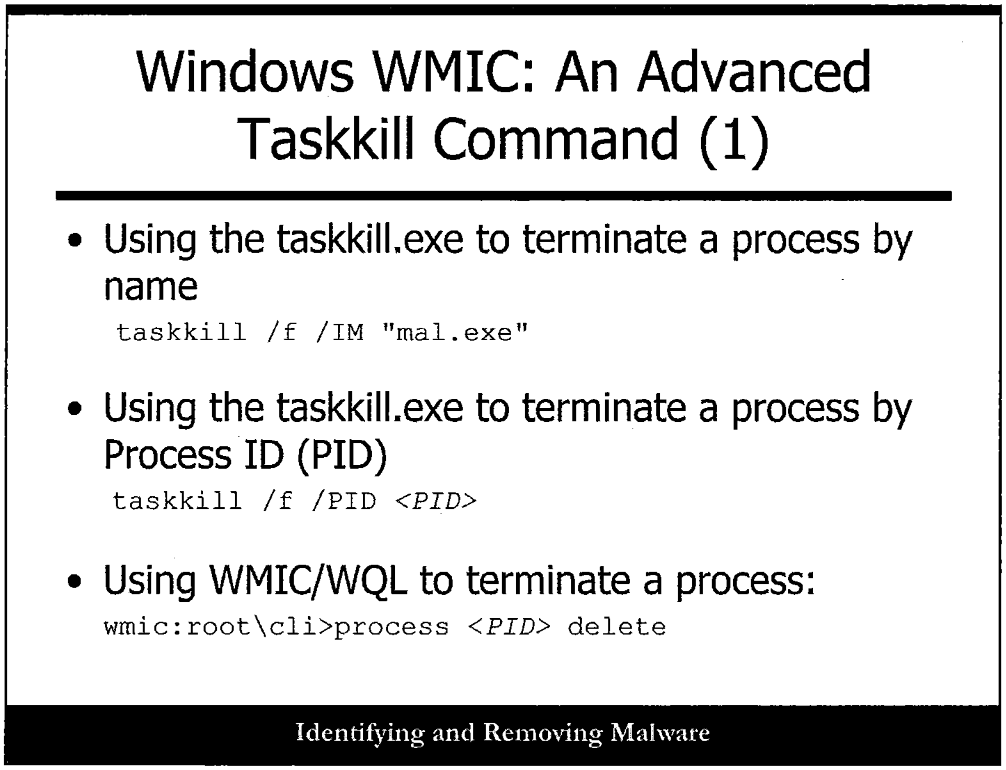
**WMIC Versus Tasklist**

In this slide, you see how to query the system to list all processes that have the name svchost.exe and list them in a brief way:

Remember that there are two ways to get the WMIC commands to be executed; one is entering the wmic console, by typing **wmic** ; the other is simply adding the **wmic** word before the command.

wmic:root\cli>process where name='svchost.exe' list brief

| HandleCount | Name | Priority | ProcessId | ThreadCount | WorkingSetSize |
|---|---|---|---|---|---|
| 259 | svchost.exe | 8 | 1752 | 19 | 4747264 |
| 540 | svchost.exe | 8 | 1844 | 10 | 4153344 |
| 1980 | svchost.exe | 8 | 440 | 81 | 27172864 |
| 134 | svchost.exe | 8 | 640 | 6 | 3387392 |
| 338 | svchost.exe | 8 | 1096 | 18 | 6955008 |
| 107 | svchost.exe | 8 | 1932 | 3 | 3182592 |
| 161 | svchost.exe | 8 | 812 | 5 | 3305472 |




**Windows WMIC: An Advanced Taskkill Command (1)**

**WMIC Versus Taskkill**

In this slide, you see how to terminate a process using the ImageName of "mal.exe." To do exactly the same thing with WMIC, ask it to delete a process with the specified PID:

wmic:root\cli> process 584 delete

Delete '\\pbueno\Root\CIMV2:Win32_Process.Handle="584"' (Y/N)? <- Here it asks for confirmation if you want to really terminate the process ID 584.

If you press Y you get the following message:

Deleting instance \\Pbueno\Root\CIMV2:Win32_Process.Handle="584"

Instance deletion successful.

That means that you successfully terminated the process mal.exe!

## Windows WMIC: An Advanced Taskkill Command (2)

- Use WQL to query for specific processes to terminate
- Similar to listing specific processes
- To kill all processes that have the name mal.exe, you would simply ask it
- Process where name='mal.exe' delete
  - Note: just name='mal' will not work, you need the exact process name!

Identifying and Removing Malware

**Windows WMIC: An Advanced Taskkill Command (2)**

**WMIC Versus Taskkill**

The advantage of WMIC with WQL is that it allows you to do the same and a lot more actions! With WMIC it is simple:

wmic:root\cli> process where name='mal.exe' delete

Delete '\\pbueno\Root\CIMV2:Win32_Process.Handle="584"' (Y/N)? <- Here it asks for confirmation if you want to really terminate the process ID 584.

If you press Y you get the following message:

Deleting instance \\Pbueno\Root\CIMV2:Win32_Process.Handle="584"
Instance deletion successful.

Delete '\\pbueno\Root\CIMV2:Win32_Process.Handle="3394"' (Y/N)?

If you press Y you get the following message:

Deleting instance \\Pbueno\Root\CIMV2:Win32_Process.Handle="3394"

That means that you successfully terminated all the processes mal.exe!

# Windows WMIC: Listing Auto-Loading Programs (1)

- Some programs modify Registry keys to allow a restart on reboot
- This mode, called "I'll be back," may be complicated to identify
- WMIC provides a way to query the system for all programs that will be loaded on each startup:

```
wmic:root\cli>startup list full
```

Identifying and Removing Malware

**Windows WMIC: Listing Autoloading Programs (1)**

**Listing Auto-Loading Modules**

In the previous module, you learned that some malware registers itself to ensure that the system runs it if the user decides to restart the machine. This is called "I'll be back" mode because even if the user decides to reboot, thinking about it as a cleaning mode, it will be executed again.

WMIC provides a way to query the system for which programs will be loaded at startup.

In the WMIC console, simply type:

wmic:root\cli>startup list full

This command generates a lot of output. For learning purposes, we use the Google Update example:

<snip>

Caption=Google Update

Command="C:\Users\pedro\AppData\Local\Google\Update\GoogleUpdate.exe" /c <- the command line to run this program

Description=Google Update

Location=HKU\S-1-5-21-33197649-3067814944-900194524-1001\SOFTWARE\Microsoft\Windows\CurrentVersion\Run <- <- The registry key!

SettingID=

User=pedro-laptop\pedro

## Windows WMIC: Listing Auto-Loading Programs (2)

- Using the `startup list full` you get a list of all startup programs in your system and even which Registry key it is associated with!
- The fields:

  Caption, Command, Description, Location, SettingID, and User

Identifying and Removing Malware

**Windows WMIC: Listing Autoloading Programs (2)**

**Listing auto-loading Modules**

The startup command is interesting because you can see all the programs that will be loaded on the system, and in this case, you may want to run it outside the WMIC console, so you can redirect the output to another file to examine it later!

```
C:\Users\pedro>wmic startup list full > startupfull.txt
```

## Windows WMIC: Listing Auto-Loading Programs (3)

- Text is good but what about a good html format?
- WMIC provides different kinds of formats to work with
- For example, to get an html formatted report, the command line will be

```
wmic startup list full
/format:hform
```

Identifying and Removing Malware

**Windows WMIC: Listing Autoloading Programs (3)**

**Listing Auto-Loading Modules in Other Formats**

When doing an analysis on a machine, you probably want to work with the data later, and sometimes text files can be quite hard to work with, especially if there is a lot of data.

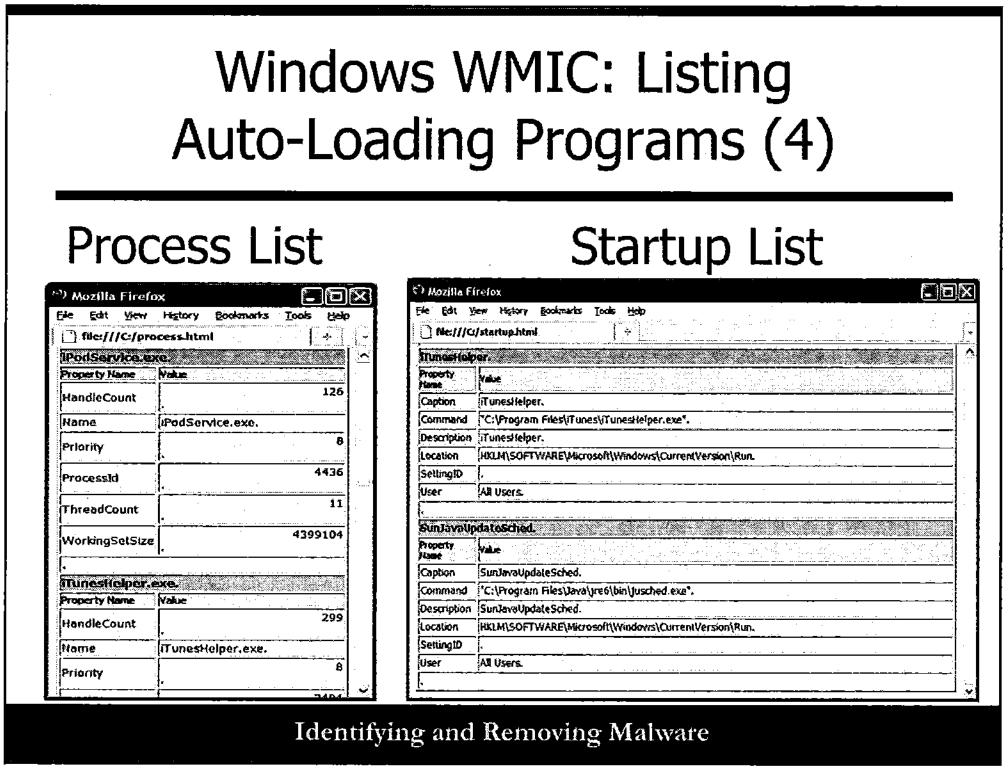
WMIC provides the following formats to work with:

- CSV
- HFORM
- HMOF
- HTABLE
- HXML
- LIST
- RAWXML

If you decide to get a plain CSV, you just have to specify it:

Wmic startup list full /format:csv

I prefer the Table format (/format:htable), but you have to choose one that works in your environment.




**Windows WMIC: Listing Autoloading Programs (4)**

**Listing Auto-Loading Modules in HTML**

These screen shots were generated in the Html format.

For the process list:

Wmic process list brief /format:hform > process.html

For the Startup list:

Wmic startup list full /format:hform : startup.html

# Windows WMIC
# Listing Shared Drives

- Sometimes, malware tries to spread through shared drives
- Identifying these shared drives is essential in determining possible infection vectors used by the malware
- Net share usually shows you this information but WMIC can provide even more information and in different formats:

```
wmic share list full /format:htable
```

Identifying and Removing Malware

**Windows WMIC Listing Shared Drivers**

Malware can behave in different ways, as you saw previously. One way is copying itself in all shares that it can find.

If you are trying to identify and track a malware, one useful way is to also identify which shares the computer has, so you can investigate further.

One commonly used command is net share, which shows you the shares in the following way:

```
Share name               Resource     Remark
----------------         --           -------------------------------------
ADMIN$                   C:\WINDOWS               Remote Admin
C$                       C:\                      Default Share
IPC$                                              Remote IPC
The command completed successfully.
```

Using WMIC, you can also use it and export the output using one of the several formats available.

You can choose between full or brief description. The brief description shows you the same information as net share, whereas full can give you plenty of details:

```
Wmic share list full /format:htable
```

# Windows WMIC:
# Listing Services (1)

- How to identify and list the services on the machine after a malware registers itself as a service
- Knowledge of computer's services is essential
- WMIC provides a comprehensive way to list those services:
  - `wmic service list full /format:htable`
  - Always suspect blank or weird service descriptions

Identifying and Removing Malware

**Windows WMIC: Listing Services (1)**

It is interesting to note that sometimes malware can register itself as a service on the system. There is actually no accredited reason for this, but it is known that a service is more difficult to terminate than a process, so this may be a reason.

Listing the services in a friendly way is also essential to quickly identify a possibly malicious one.

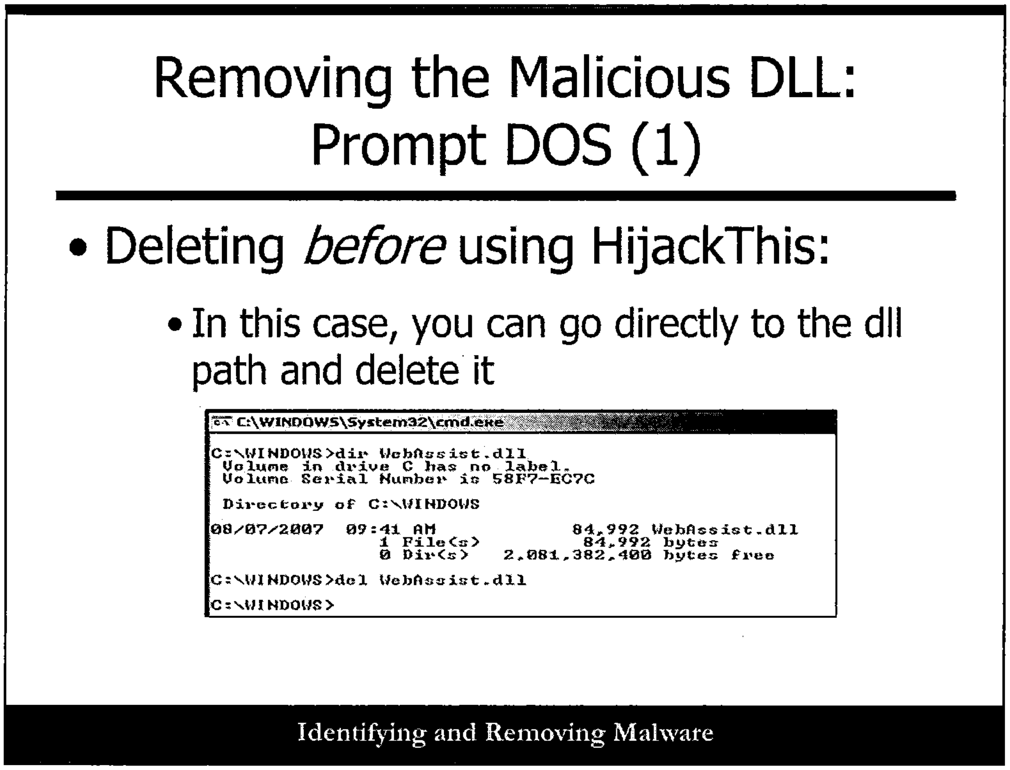
To list all services with full information in html format you can use

```
Wmic service list full /format:htable > services.html
```

Now you can open services.html in your browser and look for suspicious services.

# Windows WMIC:
# Listing Services (2)

- A friendly way to see the services




**Removing the Malicious DLL: Prompt DOS (1)**

If you decide to go directly to the path found by ListDLLs and delete the WebAssist.dll before running HijackThis, you can list it with DIR and delete it with the regular DEL command.

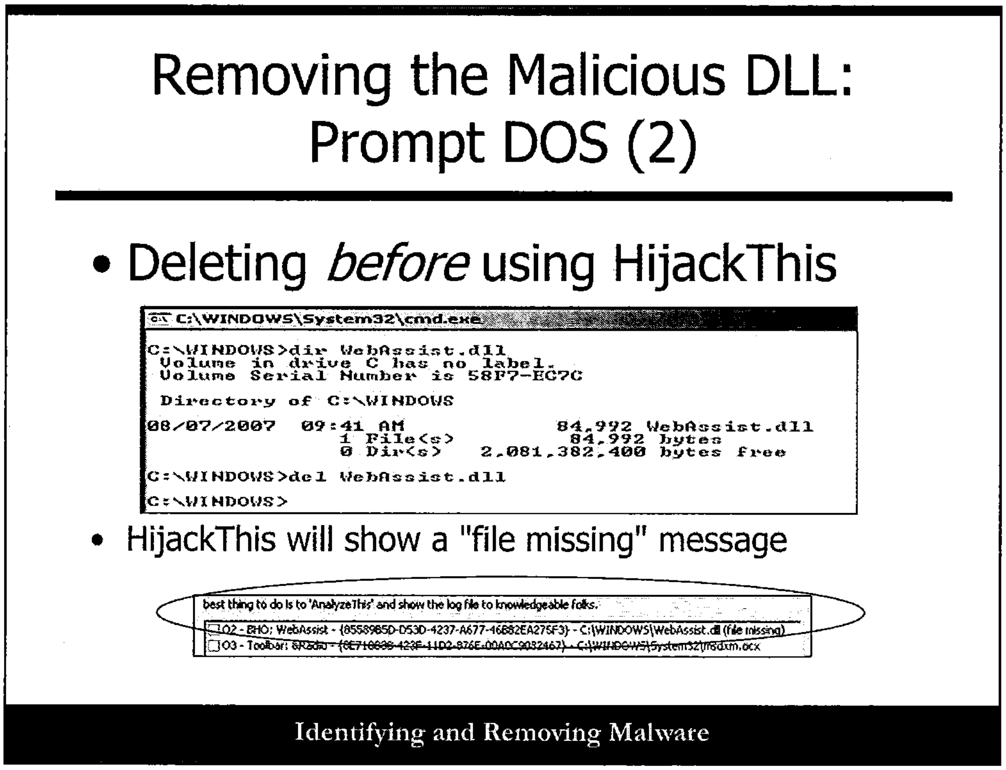
Basically:

C:\windows\dir webassist.dll

08/07/2007 09:41 AM 84,992 WebAssist.dll

And delete it:

C:\windows\del webassist.dll




**Removing the Malicious DLL: Prompt DOS (2)**

After a successful file deletion, you may want to run HijackThis to see if you did the job right. The System Scan from HijackThis still reports the presence of a BHO on the system. Because you manually removed the file, it reports that the BHO trace is there, but the DLL file associated with it is not:

O2 - BHO: WebAssist - {85589B5D-D53D-4237-A677-46B82EA275F3} - C:\WINDOWS\WebAssist.dll (file missing)

This means the BHO trace is there in IE, but the DLL file that makes the BHO work is not. The best thing to do in those cases is to check the BHO box and click the Fix Checked button so that HijackThis removes the BHO traces from the system.

Note, however, that because you manually removed the file, HijackThis cannot store it in the quarantine items folder and hence you cannot restore it from a backup later!

# Identifying and Removing Malware

## Fighting Alternate Data Streams (ADS)

Identifying and Removing Malware

This page intentionally left blank.

# Understanding ADS

Questions to be answered:

- What are ADSes?
- Are all ADSes malicious?
- Can Windows show ADSes on files?
- How can you identify ADSes on the system?
- How can you remove malicious ADSes from the system?

Identifying and Removing Malware

**Understanding ADS**

**Introduction**

In this module, you learn how to fight Alternate Data Streams.

First, we take a look at the different parts of files and attempt to determine whether they are malicious. Then, we identify Alternate Data Streams (ADS) on the system using Windows internal tools. We then take a look at some external tools. We also take a look at how to remove them.

# What Are ADS?

- What are ADSes?
  - Introduced on NTFS file system
  - Way to add an alternative stream of information/data onto an existing file
  - The size of the alternative stream doesn't matter

Identifying and Removing Malware

**What Are ADSes?**

Alternate Data Streams were added in the NTFS file system, which means that you won't have it on systems that use the FAT file system. It appears that Microsoft hasn't fully developed this feature due to the lack of Microsoft documentation on it.

Basically, it was created and introduced in NTFS on Windows NT to provide compatibility with Apple's Macintosh Hierarchical File System (HFS) and was completely ignored and forgotten.

Without getting into details about the file system, what you need to understand is that it allows every file in NTFS to create an ADS, which is a hidden file associated with the initial file. As a hidden file, it provides a nice way to hide malicious software, configuration files, illegal files, and any other content that you would like to keep hidden.

Another thing is that NTFS doesn't care about the size of the ADS. For example, you can have a large binary file as an ADS attached to a single small text file.

# ADS: Always Malicious?

- Are all ADSes malicious?
  - Simple answer: No
  - Extended answer: Maybe
  - Some AV vendors use it
    - Kaspersky AV is an example
  - Starting in XP SP2 Windows also uses it as file "zone identifier"
  - What about Backdoor PoisonIvy?

Identifying and Removing Malware

**ADS: Always Malicious?**

**Are All ADSes Malicious?**

I am tempted to answer yes, but the right answer is no.

Although most users, even Windows, ignore ADS. Some do use it, and even Microsoft started to use it with Internet Explorer on XP SP2. Kaspersky antivirus vendor also used the ADS feature, called iStreams by Kaspersky, which added an ADS to each scanned file to speed up subsequent scans. This feature was abandoned after Kaspersky released version 6 of its AV product and which also has an option to delete those streams left on the system.

For more information on this, visit http://www.kaspersky.com/faq?qid=156636746.

Windows also started to use streams as a "security" feature. Since Windows XP SP2 all files originating from the Internet got an ADS to identify the Zone (Trusted, Untrusted zones) it came from. This allows Windows to warn the user if they try to execute the file.

For example, a file received through Google Talk IM program will have an ADS like:

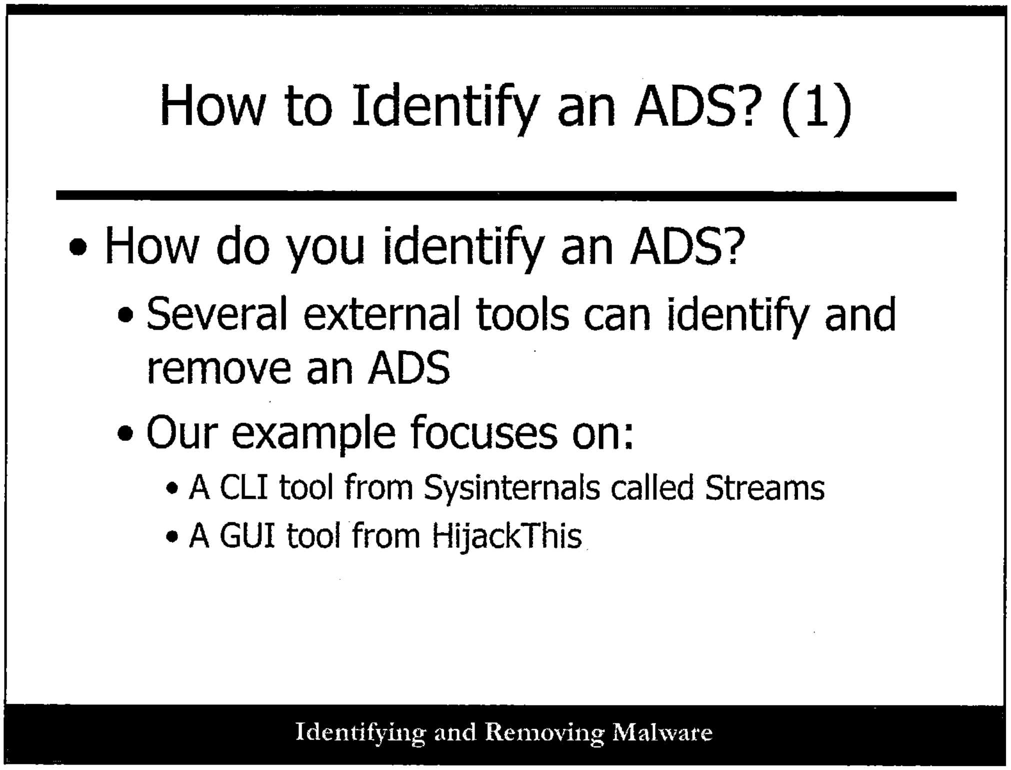
[ZoneTransfer]

ZoneId=3

In addition, if you right-click a file in Windows File Explorer, select properties, and add a summary, it will be safe in an ADS.

### What About Backdoor PoisonIvy?

This backdoor is created using a graphical utility. Although there have been no developments of this graphical utility since the end of 2007/2008, as of 2015, we have seen several backdoors created with this tool. This is because the SDK for it is also available. One of the options is to install it as an ADS on the infected machines, making it harder to be identified.



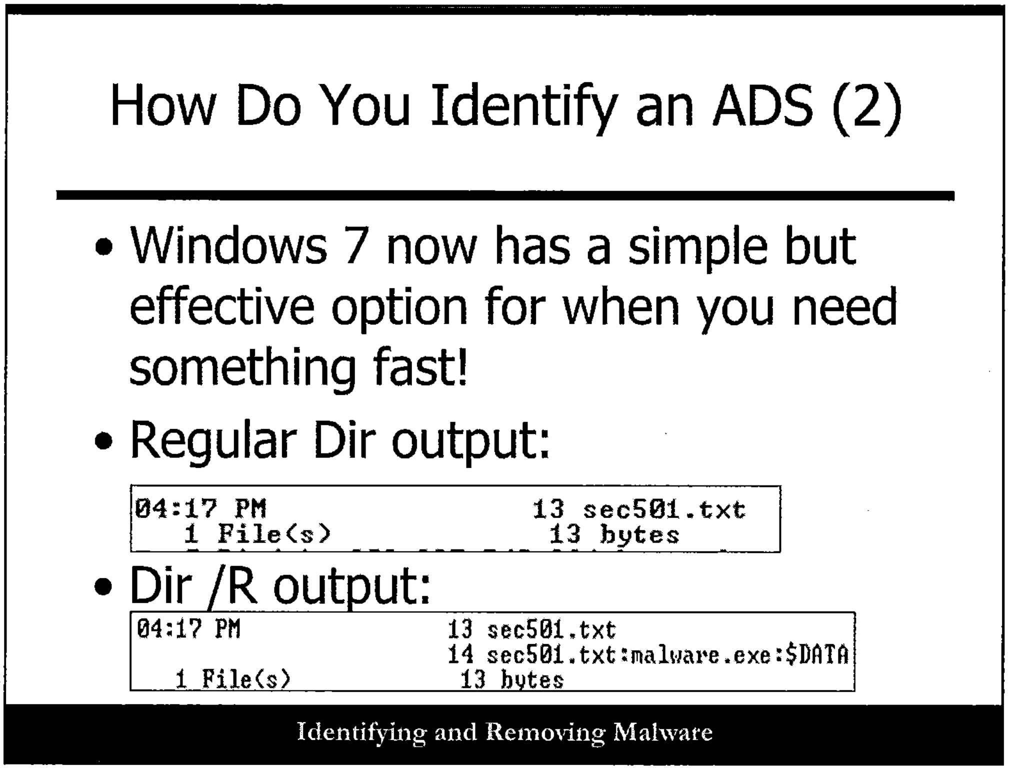

**How Do You Identify an ADS? (1)**

Various tools identify ADSes on a system, such as LADS from Heysoft, which you can find at http://www.heysoft.de/download/lads.zip (not Windows 7 compatible).

Today, most antivirus and antispyware products also detect ADS.

In this module, you learn how to deal with an ADS using two tools:

- A CLI tool called streams, from Microsoft SysInternals, which can be downloaded at http://technet.microsoft.com/en-us/sysinternals/bb897440.
- A GUI tool that was already used for other purposes, the HijackThis tool.




**How Do You Identify an ADS? (2)**

On Windows 7, Microsoft included an extra option that can be used in the already familiar dir.

When using the dir command with the option /R, it also shows files with the possible ADS present.

On the slide, you can clearly see this in the example used with the file sec501.txt. When you use a simple dir with no options, it shows just the regular file; but when you use the dir /R, it shows the regular file plus the file and the ADS attached to it.

MS Sysinternals Streams Tool (1)

- Introducing Sysinternals Streams
  - Scans the system, recursively if needed, and shows all the ADSes on the system with full path. Can also be used to delete an ADS

Identifying and Removing Malware

**MS Sysinternals Streams Tool (1)**

**Introducing Streams**

The Streams tool is another tool developed by Sysinternals.

This tool can be downloaded at http://technet.microsoft.com/en-us/sysinternals/bb897440.

Streams is a CLI tool that can scan a single file, a directory, or the hard drive searching for ADSes. It can also be used to delete those ADSes from the files and directories. If an ADS is found, the output will be the full path of the regular file plus the ADS "attached" to it using the colon ":" as a delimiter.

Example: C:\windows\clock.avi:testADS.txt

This means that the file clock.avi, which is in the c:\windows directory, has an ADS called testADS.txt.

# MS Sysinternals Streams Tool (2)

- Scanning the system with streams:
  - Using command-line interface:
    - *To scan a single directory*

      *Example:*

      *C:\streams.exe c:\windows\system32*
    - *To scan recursively all directories*

      *Example:*

      *C:\streams.exe –s c:*

  This command searches the entire hard drive c: for files with streams associated with them.

Identifying and Removing Malware

**MS Sysinternals Streams Tool (2)**

**Streams Basic Usage**
Streams lets you scan a single file, a single directory, or all files and directories on the hard drive by scanning all folders recursively.

The basic usage to scan a single file is
Streams.exe <filename>

To scan a directory with all subfolders:
Streams.exe –s <folder_name>

For example, scanning the Windows directory, including all subfolders:
C:\streams.exe -s c:\windows

Streams v1.56 - Enumerate alternate NTFS data streams
Copyright (C) 1999-2007 Mark Russinovich
Sysinternals - www.sysinternals.com

**c:\windows\clock.avi:**
    **:testADS.txt:$DATA 10**

This shows the ADS testADS.txt on the file clock.avi inside the folder c:\windows, and the file size of the ADS is 10 bytes.

## MS Sysinternals Streams

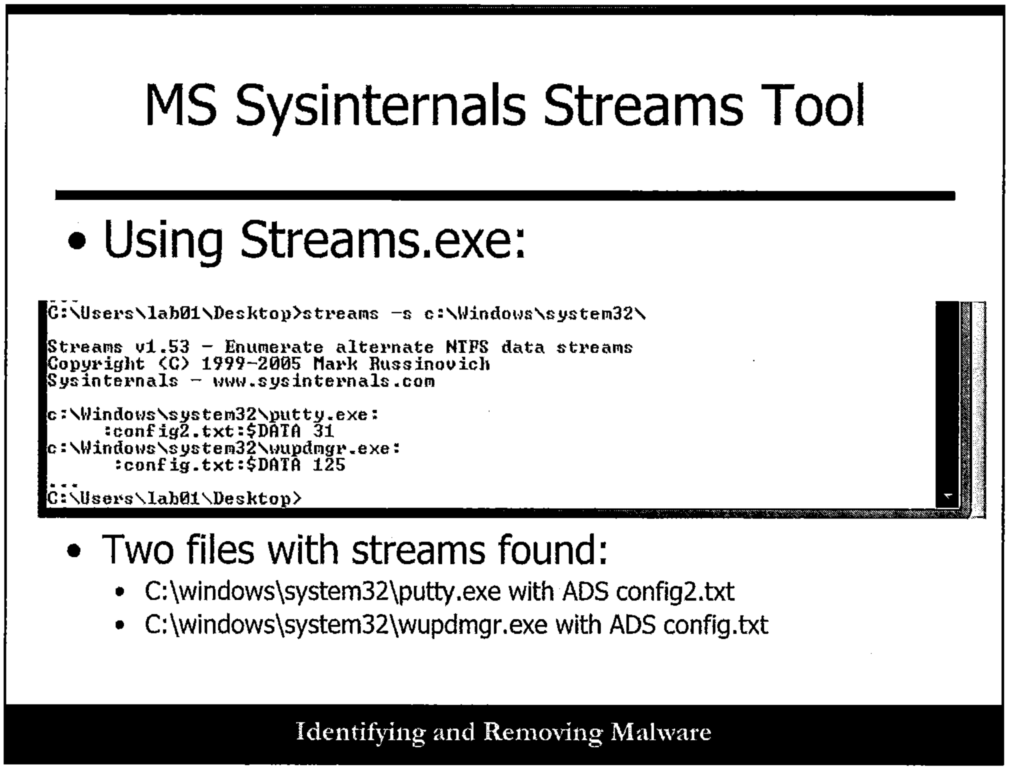
### Hands-on

Identifying and Removing Malware

On the MS Sysinternals Streams part, we start with the following steps:

1. Revert the VMware Windows 7 image to the Snapshot Clean7:
   VM -> Snapshot -> Select Clean7
2. Open the folder Course on the VMware Windows 7 Desktop.
3. Open the Part6 folder.
4. Right-click the badads.zip file, and then select Extract All. Enter the password **training**.
5. Double-click the new created folder; right-click the badads.exe file, and select Run as Administrator.
6. Run both tools and malware as Administrator!

Now, continue to follow the slides doing the same on the VMware Windows 7 image.




**MS Sysinternals Streams Tool**

**Our Learning Example**

In this module, you look at examples of two ADSes on the system, and you learn how to identify what they do and how to remove them if you decide that they are malicious.

Copy the streams.exe from the Part 6 folder to your desktop.
Start with streams doing a full scan on the System32 folder looking for all ADSes:

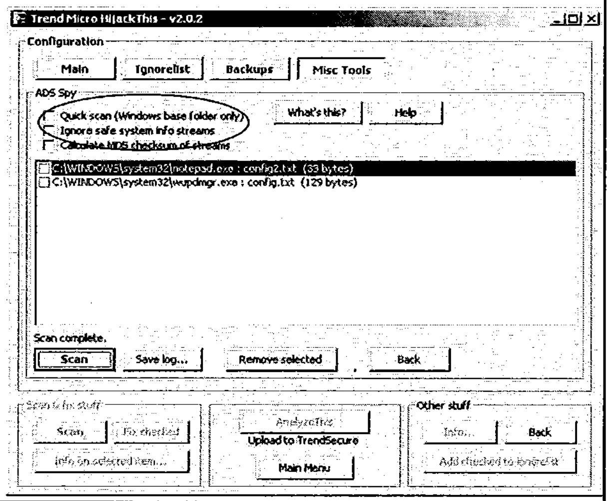
> C:\Users\<username>\Desktop\streams.exe -s c:\windows\system32\
>
> Streams v1.56 - Enumerate alternate NTFS data streams
> Copyright (C) 1999-2007 Mark Russinovich
> Sysinternals - www.sysinternals.com
>
> Error opening c:\pagefile.sys:
> The process cannot access the file because it is being used by another process.
>
> **c:\WINDOWS\system32\putty.exe:**
> **:config2.txt:$DATA 129**
> **c:\WINDOWS\system32\wupdmgr.exe:**
> **:config.txt:$DATA 33**

So, you find two ADSes attached to two legitimate files:

- putty.exe with the ADS config2.txt
- Wupdmgr.exe with the ADS config.txt

# HijackThis ADS Spy Tool (1)

- Another easy way to identify an ADS is with HijackThis
- The HijackThis misc. tool ADS Spy can search for an ADS on the system
- Be sure to uncheck:
  - Quick Scan
  - Ignore Safe ADS




Identifying and Removing Malware

**HijackThis ADS Spy Tool (1)**

**Our Learning Example**

The HijackThis tool also offers an easy way to identify and later remove an ADS from the system. On the Misc Tools section, it offers a tool called HijackThis ADS Spy. It also allows you to search all files and directories on the hard drive looking for ADS anywhere on the system.

By default, the tool scans only the Windows folder and ignores a list of ADSes that are known to be safe. So to get a complete view of the system, it is recommended to uncheck these check boxes:

- Quick Scan (Windows base folder only)
- Ignore safe systems info streams

And scanning the system, you find the same two streams that the Sysinternals tool found:

**C:\WINDOWS\system32\putty.exe : config2.txt (33 bytes)**
**C:\WINDOWS\system32\wupdmgr.exe : config.txt (129 bytes)**

# HijackThis ADS Spy Tool (2)

## Summary

- Two ADSes were found attached to legitimate files:
  - Putty.exe: Looks like the SSH Client
  - Wupdmgr.exe: Looks like part of Windows Update
- Are they malicious?
- Can you remove them?

Identifying and Removing Malware

**HijackThis ADS Spy Tool (2)**

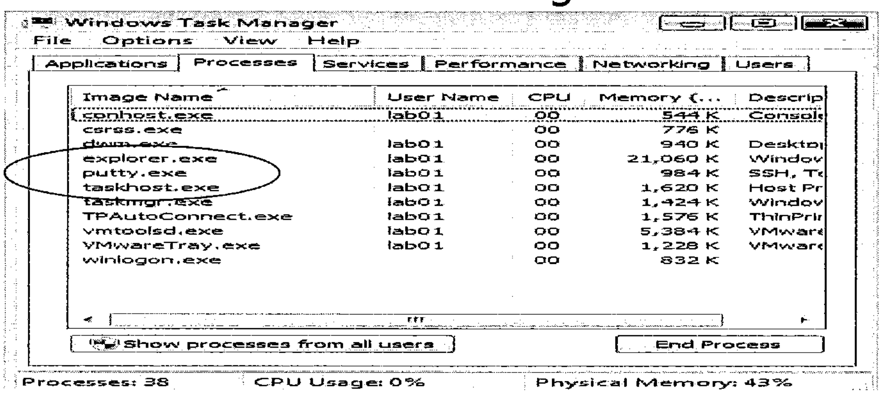
**Summary**
At this point in the example, you scanned the system and found two ADSes attached to files that normally would have no reason to have an ADS hidden in them:

- Putty.exe
- Wupdmgr.exe

Also, the ADS names config.txt and config2.txt make them at least somewhat suspect because they sound like configuration files. The next step is to identify whether they are malicious and, if they are determined to be malicious, determine how to remove them from the system.

## ADS and TaskManager

- Running putty.exe didn't show the ADS on Windows Task Manager



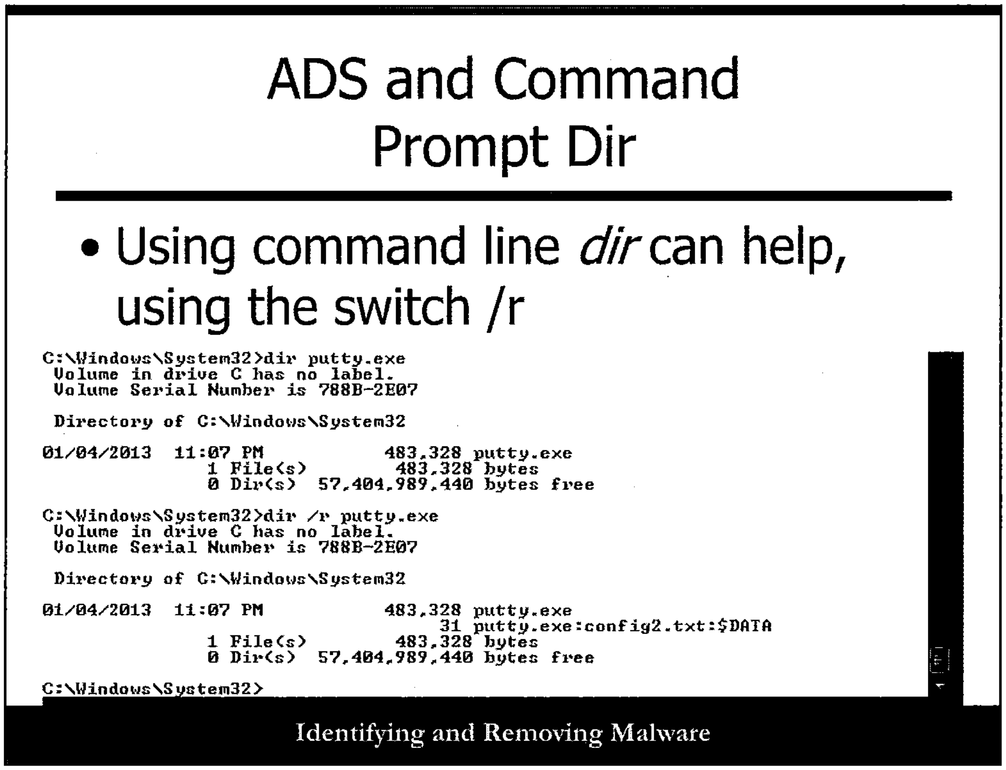

Identifying and Removing Malware

**ADS and TaskManager**

**How Does Windows See ADS?**

On this and the following slides, we show how Windows sees the ADS. On this slide, we opened the Putty.exe from the c:\windows\system32 folder, which has the ADS config2.txt. Then, we opened Windows Task Manager to check how it sees a file that has an ADS attached to it. With Task Manager opened (shortcut Ctrl+Shift+Esc), you can check both the Applications and Process tabs.

On the Application tab, you can see that a process called Putty running, which is normal because you just opened it. If you click the Process tab, you can also see putty.exe running. In neither case can you determine whether there is an ADS attached to it.




**ADS and Command Prompt Dir**

**How Does Windows See ADS?**

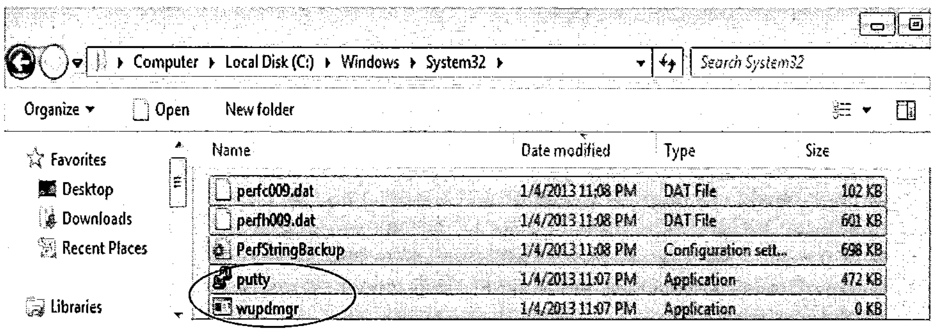
In an attempt to identify ADS with built-in Windows tools, you can see that Task Manager doesn't show anything. Now try to list the files to see whether you can determine the presence of an ADS. Using the *dir* command doesn't help. It shows only the regular files and filenames.

Fortunately, Microsoft improved the *dir* command with new features, and since Windows Vista, the *dir* command offers a switch that shows the ADS.

As you can see in the slide, using *dir* with the /r switch shows the ADS for us. But remember that if you are still on Windows XP, there is no such option.

# ADS and Windows Explorer

- Windows Explorer shows both files, but doesn't show the ADS!




Identifying and Removing Malware

**ADS and Windows Explorer**

**How Does Windows See ADS?**

Our tests with Windows TaskManager and *dir* didn't reveal any information on the ADS, so the next test is with Windows Explorer. Opening Windows Explorer on the folder c:\windows\system32 you can see both files but still no trace of the ADS.

## Working on the ADS Files

- The two files identified by the ADS tools look suspicious by:
  - Their location (windows\system32)
  - Where they are attached: putty.exe and wupdmgr.exe
  - The ADS names config.txt and config2.txt
- But before you remove them, you need to be sure they are malicious

Identifying and Removing Malware

**Working on the ADS Files**

**Identifying the ADS Content**

We already have a lot of information about the two ADSes:

- They are located in the windows\system32 directory.
- They are attached to two files on the Windows folder.
- They have suspicious names that look like configuration files.

Normally, this would be enough to warrant removing them from the system, but it would be better if we could be totally sure first. So now you have to find out what those ADSes are.

# Accessing the ADS Files

- Because you cannot see the ADS using Windows Explorer, you could try to access them directly from CLI:
- Using Type:
  C:\windows\system32\type putty.exe:config2.txt
- Using More
  C:\windows\system32\more putty.exe:config2.txt

Identifying and Removing Malware

**Accessing the ADS Files**

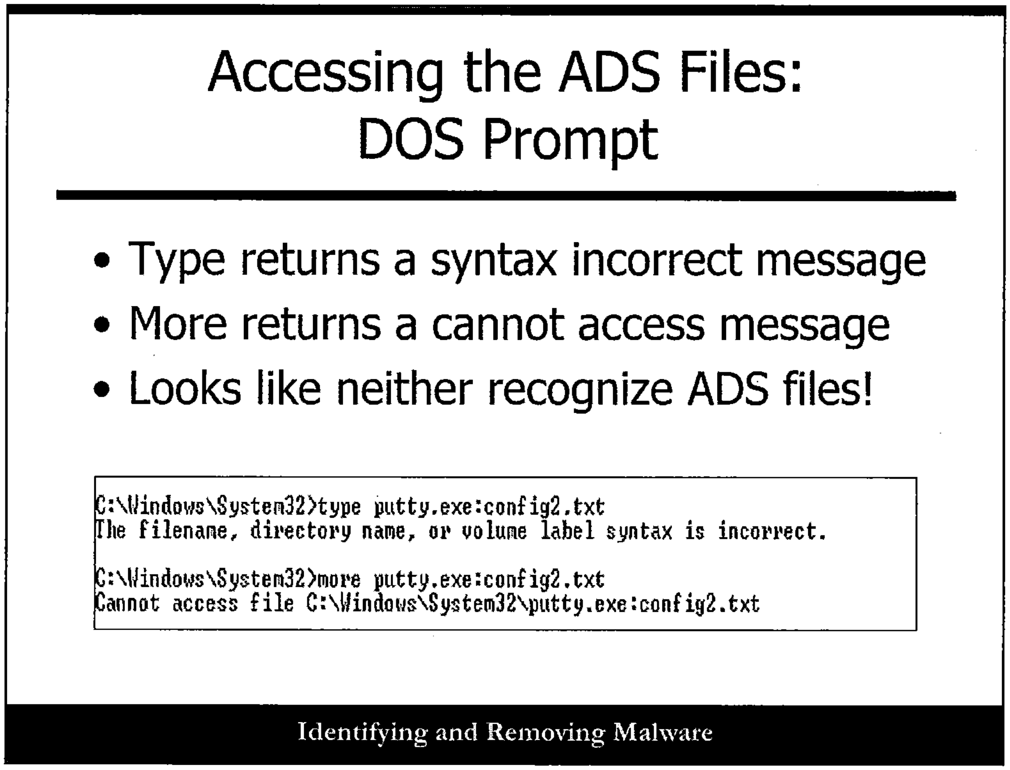
**Identifying the ADS Content**

You already know that you cannot see the ADS from Windows Explorer or from the *dir* command line. But you could try with a couple of other file utilities from Windows such as:

- more
- type

Usually to see a text file, you can use these two utilities to open them. The basic syntax for either of the commands is:

- type [filename]
- more [filename]




**Accessing the ADS Files: DOS Prompt**

**Identifying the ADS Content**
**Note that you may notice different behavior on Windows 7 32-bit and Windows 7 64-bit.**

Neither of the utilities produced a nice result. Type returned the following:

The filename, directory name, or volume label syntax is incorrect.

More returned the following:

Cannot access file C:\WINDOWS\system32\putty.exe:config2.txt

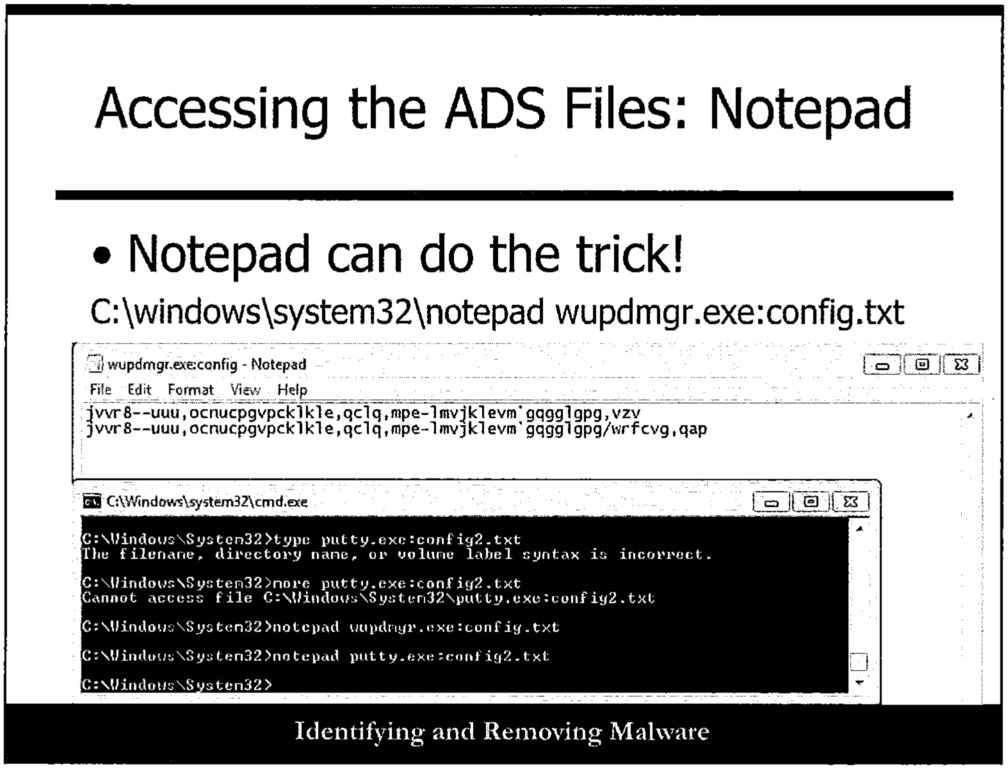
**But that's because we were using it in the wrong way!**

The more utility can be used to read ADS content! The right syntax would be:

**more < c:\windows\system32\putty.exe:config2.txt**
and
**more < c:\windows\system32\wupdmgr.exe:config.txt**

And if you want to send the content to another file, just add a redirection like:

more **< c:\windows\system32\putty.exe:config2.txt > resultADS.txt**




**Accessing the ADS Files: Notepad**

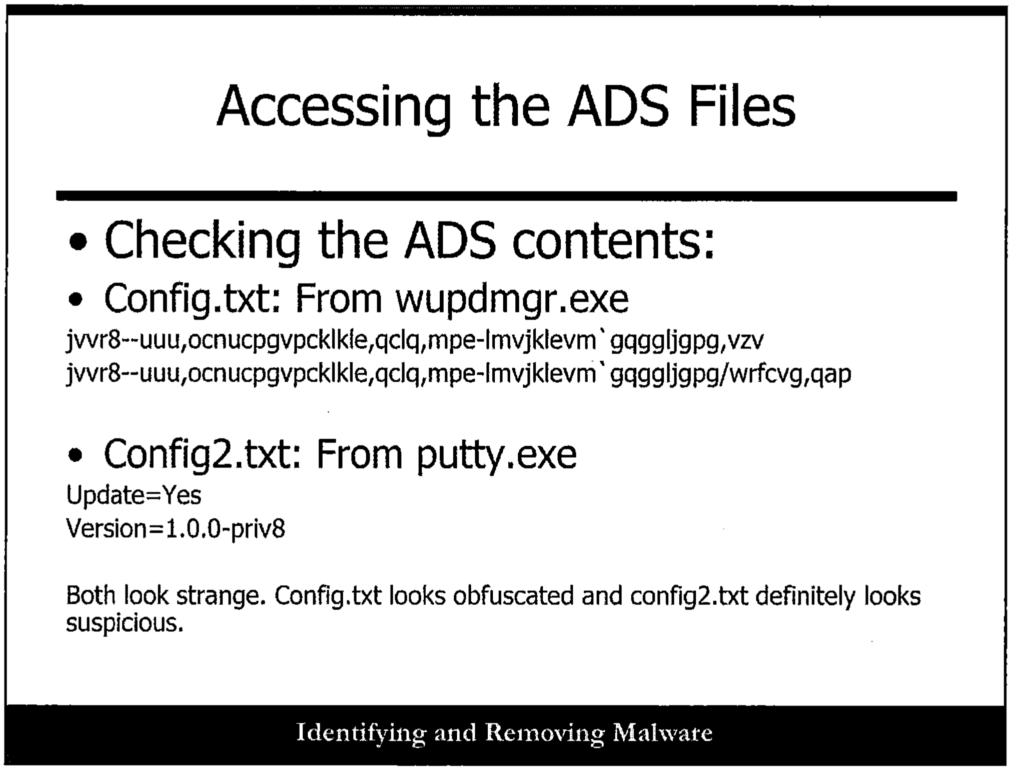
**Identifying the ADS Content**

Another nice way to see the contents of ADS is using the same Notepad. Notepad can understand the ADS and show you only the contents of the ADS. For example, from the DOS prompt, you can call Notepad to show us the content of both config.txt and config2.txt using the following:

**C:\Windows\System32\notepad c:\windows\system32\putty.exe:config2.txt**

and

**C:\Windows\System32\notepad c:\windows\system32\wupdmgr.exe:config.txt**




**Accessing the ADS Files**

**Identifying the ADS content**

Using both More and Notepad, you retrieve the content of both ADSes:

**Config.txt**

jvvr8--uuu,ocnucpgvpcklkle,qclq,mpe-lmvjklevm`gqggljgpg,vzv

jvvr8--uuu,ocnucpgvpcklkle,qclq,mpe-lmvjklevm`gqggljgpg/wrfcvg,qap

**Config2.txt**

Update=Yes

Version=1.0.0-priv8

Both ADSes look strange, but at least you can see something meaningful in Config2.txt. It looks like a configuration file for something. The file appears to have an update setting and the current version information. The version number is also suspicious due to the hacker style wording:

Priv8 = Private

The first file looks like it is protected by some kind of encoding to obfuscate the real content. You probably could try to work on this to find out the real content.

# Working on the Obfuscated ADS

- Working on the obfuscated ADS:

jvvr8--uuu,ocnucpgvpcklkle,qclq,mpe-lmvjklevm`gqggljgpg,vzv

- You can see the repetition of some letters, such as:
  - v ( jvvr )
  - u ( uuu )
- Maybe XOR encoding was used?

Identifying and Removing Malware

**Working on the Obfuscated ADS**

jvvr8--uuu,ocnucpgvpcklkle,qclq,mpe-lmvjklevm`gqggljgpg,vzv

You can clearly see some repetition of characters like:

v (on jvvr for example)
u (on uuu for example)

XOR encoding is generally used to encode text or binaries to flip the characters according to a given key. For example:

Given a key of 5 to XOR the word: "http" I would get "mqqu."

To explain this further, first you have to convert the ASCII to HEX. From the HEX, you get the binary representation. Then, you XOR it with the given key.

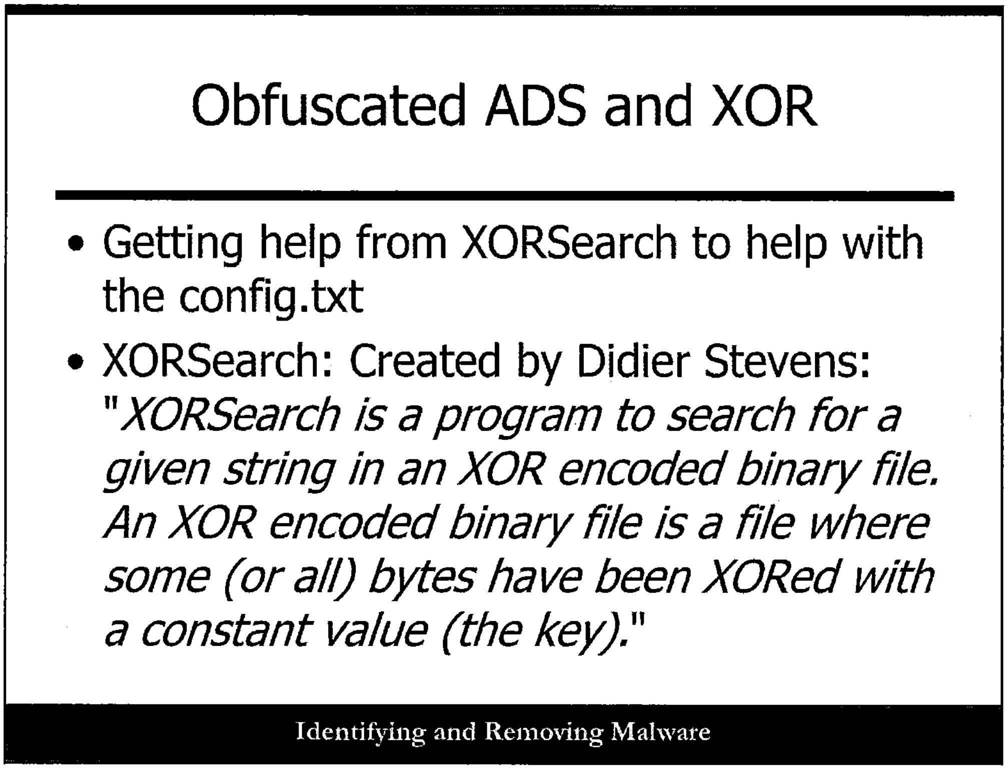
| h = Hex 68 | Key = Hex 5 | Result = Hex 6D = m |
|---|---|---|
| Binary | Binary | Binary |
| 1 | 0 | 1 |
| 1 | 0 | 1 |
| 0 | 0 | 0 |
| 1 | 0 | 1 |
| 0 | 1 | 1 |
| 0 | 0 | 0 |
| 0 | 1 | 1 |

Following the same math, you have:

t = Hex 74 + key 5 = Hex 71 = q
t = Hex 74 + key 5 = Hex 71 = q
p = Hex 70 + key 5 = Hex 75 = u

As a final result, you have:

| | |
|---|---|
| h | m |
| t | q |
| t | q |
| p | u |




**Obfuscated ADS and XOR**

**Working on the Obfuscated ADS**

The main problem is to get the right key to use with the XOR math. Fortunately, you have another option: Brute Force

Didier Stevens created a tool called XORSearch:

"XORSearch is a program to search for a given string in an XOR or ROL (Roll to the Left) encoded binary file. An XOR encoded binary file is a file where some (or all) bytes have been XORed with a constant value (the key). A ROL (or ROR – Rolled to the Right) encoded file has its bytes rotated by a certain number of bits (the key). XOR and ROL/ROR encoding is used by malware programmers to obfuscate strings like URLs. XORSearch will try all XOR keys (0 to 255) and ROL keys (1 to 7) when searching."

This tool can be downloaded at http://blog.didierstevens.com/programs/xorsearch/.

It is located in the same folder Part 6, created on your desktop, so you may need to copy your recovered ADS to this folder when running XORSearch.

## Obfuscated ADS and XORSearch (1)

- Because you don't know which strings to search for, you could try a single "'a" character and use a brute-force approach following these steps:
  1. Copy the contents of config.txt to another file, say ads.txt
  2. Run XORSearch on the ads.txt

     *xorsearch ads.txt a / more*

Identifying and Removing Malware

**Obfuscated ADS and XORSearch (1)**

**Working on the Obfuscated ADS**

The problem is that you don't know the key used and don't know which string to give to XORSearch to let it brute force to find the key and strings. We need to start some place, so first copy the contents of the config.txt ADS to another file for XORSearch to work with. This can be done with the more utility:

more < wupdmgr.exe:config.txt > ads.txt

Then, you can give it to XORSearch to try to brute force and find the most appropriate key:

xorsearch ads.txt a | more

This will make it brute force with string "a." The pipe (|) command will be useful because a lot of output should come up because it is a common string.

# Obfuscated ADS and XORSearch (2)

Output from xorseach looking for a encoded with XOR:

Found XOR 00 position 007D: ap
Found XOR 01 position 002D: afpffmkfqf-w{w..kwws9,,ttt-nbotbqfwqbjmjmd-pbmp-lq
Found XOR 01 position 006A: afpffmkfqf.vsgbwf-p`q
***Found XOR 02 position 000C: alwaretraining.sans.org/nothingtobeseenhere.txt..h***
***Found XOR 02 position 000F: aretraining.sans.org/nothingtobeseenhere.txt..http***
***Found XOR 02 position 0014: aining.sans.org/nothingtobeseenhere.txt..http://ww***
***Found XOR 02 position 0049: alwaretraining.sans.org/nothingtobeseenhere-update***
***Found XOR 02 position 004C: aretraining.sans.org/nothingtobeseenhere-update.sc***
***Found XOR 02 position 0051: aining.sans.org/nothingtobeseenhere-update.scr***
***Found XOR 02 position 0059: ans.org/nothingtobeseenhere-update.scr***
***Found XOR 02 position 0078: ate.scr***
Found XOR 04 position 0019: a(ughu(ita)hirnoharidcucchnctc(r~r..nrrv<))qqq(kgj
Found XOR 04 position 0022: a)hirnoharidcucchnctc(r~r..nrrv<))qqq(kgjqgtcrtgoh

XOR 02 got nice strings!!

Identifying and Removing Malware

**Obfuscated ADS and XORSearch (2)**

**Working on the Obfuscated ADS**
This output of XORSearch looking for string "a" is quite useful. There is some garbage when it is using key 00 and key 01:

Found XOR 00 position 007D: ap
Found XOR 01 position 002D: afpffmkfqf-w{w..kwws9,,ttt-nbotbqfwqbjmjmd-pbmp-lq
Found XOR 01 position 006A: afpffmkfqf.vsgbwf-p`q

But interesting strings when using key 02:

Found XOR 02 position 000C: **alwaretraining.sans.org/nothingtobeseenhere.txt..h**
Found XOR 02 position 000F: **aretraining.sans.org/nothingtobeseenhere.txt..http**
Found XOR 02 position 0014: **aining.sans.org/nothingtobeseenhere.txt..http://ww**
Found XOR 02 position 001C: **ans.org/nothingtobeseenhere.txt..http://www.malwar**
Found XOR 02 position 0049: **alwaretraining.sans.org/nothingtobeseenhere-update**
Found XOR 02 position 004C: **aretraining.sans.org/nothingtobeseenhere-update.sc**
Found XOR 02 position 0051: **aining.sans.org/nothingtobeseenhere-update.scr**
Found XOR 02 position 0059: **ans.org/nothingtobeseenhere-update.scr**
Found XOR 02 position 0078: **ate.scr**

Lots of meaningful strings!

# Obfuscated ADS and XORSearch (3)

- Because we got meaningful strings with XorSearch, let's use one of them and repeat the search:
  xorsearch ads.txt http | more

Found XOR 02 position 0000:
http://www.malwaretraining.sans.org/nothingtobeseenhere.txt..http://www.ma
lwaretraining.sans.org/not
Found XOR 02 position 003D:
http://www.malwaretraining.sans.org/nothingtobeseenhere-update.scr

- Two URLS!!

Identifying and Removing Malware

**Obfuscated ADS and XORSearch (3)**

**Working on the Obfuscated ADS**

Key 02 is the key and you get a lot of useful strings! Now, you can use XORSearch to brute force with some strings that are more meaningful, such as http.

To use xorsearch to search specifically for the http string, use the following command:

xorsearch ads.txt http –l 100

Found XOR 02 position 0000: http://www.malwaretraining.sans.org/nothingtobeseenh
ere.txt..http://www.malwaretraining.sans.org/not
Found XOR 02 position 003D: http://www.malwaretraining.sans.org/nothingtobeseenh
ere-update.scr

As the result of the execution, you can identify two URLs:

- http://www.malwaretraining.sans.org/nothingtobeseenhere.txt
- http://www.malwaretraining.sans.org/nothingtobeseenhere-update.scr

Maybe another configuration file and another updated version of a possible malware? It is possible, but we already know that they are highly suspicious.

## Removing the ADS

- Because you found out that both ADS files are suspicious, you can remove them from the system:
  - Using SysInternals Streams.exe
  - Using HijackThis ADS Spy

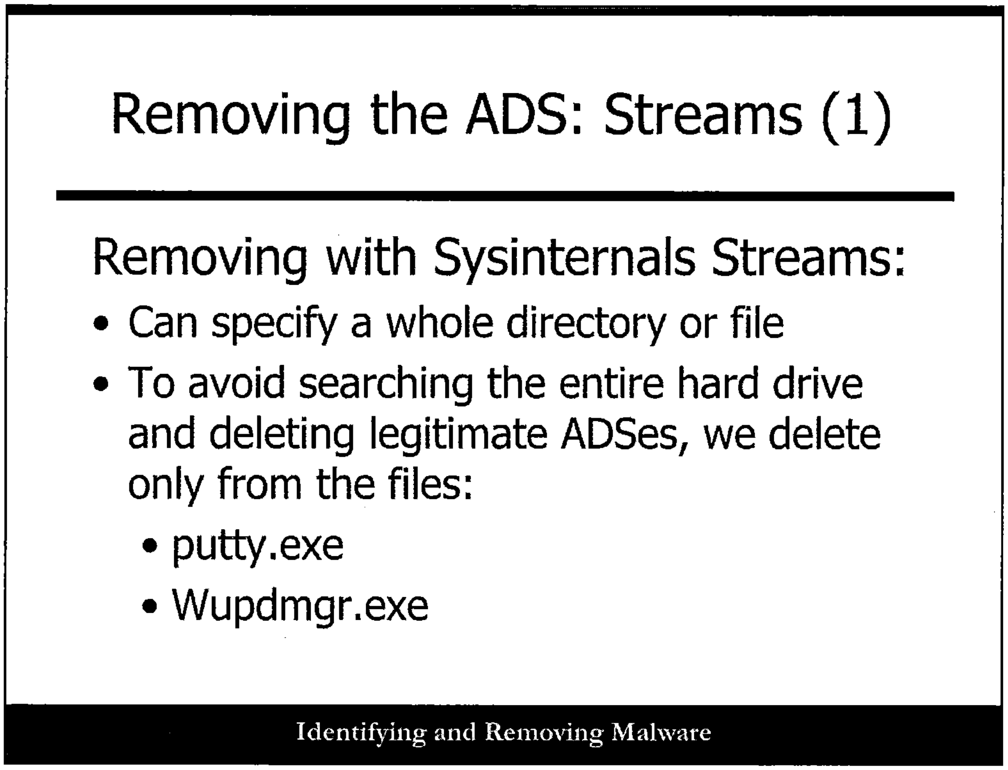
Identifying and Removing Malware

**Removing the ADS!**

Right now, you know that both ADSes are malicious or part of a malware that was installed in the system, making it safe to remove them.

Now you have two options to remove the ADSes using the same tools that you used to scan and search for ADSes on the system. These are:

- HijackThis ADS Spy
- Sysinternals Streams




**Removing the ADS: Streams (1)**

**Removing the Malicious ADS**
Using Sysinternals Streams it is quite easy to remove an ADS. You have two options to remove them:

- Remove them directly from the file.
- Scan a directory and delete all ADSes.

Because you already know the files that you want to delete the ADS from, you can simply use the path of the files to delete them. This can help avoid deleting legitimate ADSes by mistake.

## Removing the ADS: Streams (2)

### Removing with Sysinternals Streams

Streams.exe –d c:\windows\system32\putty.exe

Will search the ADS on the putty.exe file and delete it

```
C:\Users\lab01\Desktop>streams -d c:\Windows\system32\putty.exe

Streams v1.53 - Enumerate alternate NTFS data streams
Copyright (C) 1999-2005 Mark Russinovich
Sysinternals - www.sysinternals.com

c:\Windows\system32\putty.exe:
   Deleted :config2.txt:$DATA

C:\Users\lab01\Desktop>
```

Identifying and Removing Malware

**Removing the ADS: Streams (2)**

**Removing the Malicious ADS!**
Streams will use basically one command line to delete the ADS:

streams.exe -d c:\WINDOWS\system32\putty.exe

Streams v1.56 - Enumerate alternate NTFS data streams
Copyright (C) 1999-2007 Mark Russinovich
Sysinternals - www.sysinternals.com

c:\WINDOWS\system32\putty.exe:
  **Deleted :config2.txt:$DATA**

streams.exe -d c:\WINDOWS\system32\wupdmgr.exe

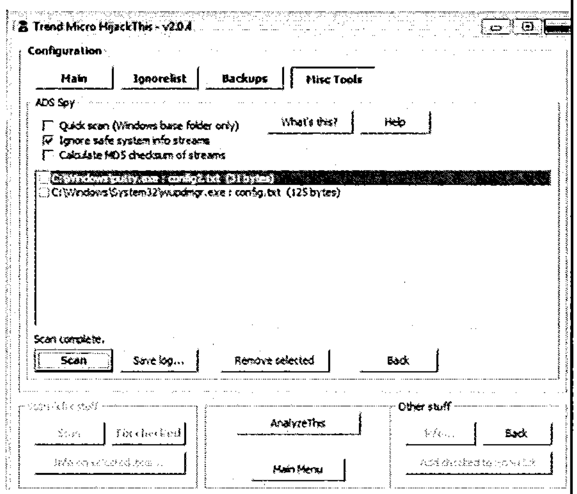
Streams v1.56 - Enumerate alternate NTFS data streams
Copyright (C) 1999-2007 Mark Russinovich
Sysinternals - www.sysinternals.com

c:\WINDOWS\system32\wupdmgr.exe:
  **Deleted :config.txt:$DATA**

# Removing the ADS: HijackThis

- Removing with HijackThis ADS Spy
  - Simple as removing BHOs
  - Select and click Remove Selected button
  - Confirm (in the latest version the confirmation pop-up is blank)

One difference from removing BHOs: deletions are permanent, no backups!




Identifying and Removing Malware

**Removing the ADS: HijackThis**

**Removing the Malicious ADS!**

Using HijackThis ADS Spy is even easier. On the report screen, you can see the ADS that HijackThis found on the system. If you check the box of any ADS and click the Remove Selected button, you will be prompted with a pop-up screen asking:

"Are you sure you want to remove the selected ADS from your system? They will be deleted permanently."

If you click Yes, you will remove all the selected ADSes.

Note: The screen shot of the HijackThis on this slide is version 1.99.1. In version 2.04 (which is the latest version and which most slides are based on), there is an error on the confirmation pop-up. It is blank, with just the Yes or No buttons.

# Identifying and Removing Malware

## Identifying and Fighting Persistent Malware

Identifying and Removing Malware

This page intentionally left blank.

# What is Persistent Malware?

- What is persistent malware?

  Malware that uses techniques to keep it running as long as possible on the system, avoiding all attempts to clean the system by removing the malicious entries or killing the process

Identifying and Removing Malware

**What is Persistent Malware?**

In this module, you learn how to identify and remove persistent malware. As you learned in previous examples, it is quite simple to remove or kill a process using either GUI or command-line tools. However, some malware has a protection mode, which prevents you from killing it.

So you may define them as a malware that uses techniques to keep it running as long as possible on the system, avoiding all attempts to clean the system by removing the malicious entries or killing the process.

## How is Persistent Malware Created?

- Our example is a Remote Administration tool (RAT). A RAT is a Backdoor trojan used to remotely control the machine.
- This one is called Ap0calypse RAT and is used by hackers to create their versions

Identifying and Removing Malware

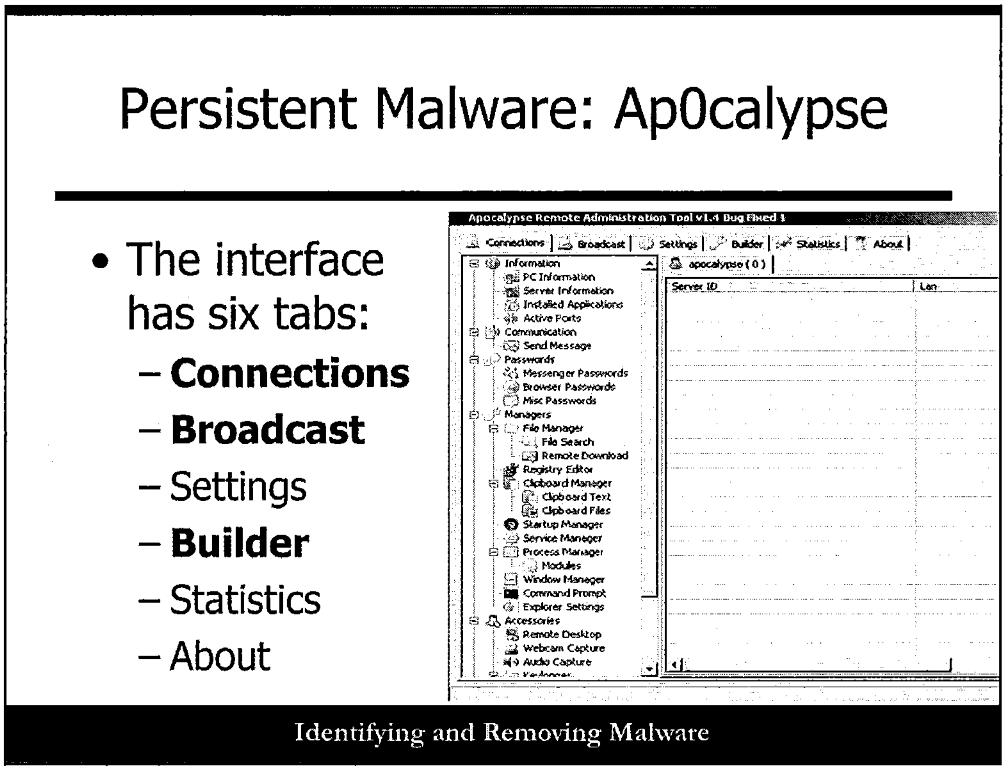
**How is Persistent Malware Created?**

Before we actually play and learn how to identify and remove the persistent malware, it is interesting to learn how the hackers actually build those pieces of software.

The persistent malware is a RAT, which stands for Remote Administration Tool. In other words, it is a backdoor that can give the hacker remote access to the system.

RATs are the preferred method used by APT groups, and most of the recent public target attacks used one or another common RAT, such as Poison Ivy or DarkCommet used in the latest attacks in Syria at the end of 2012.

The RAT that we build is called Ap0calypse RAT and is the latest "stable" version released as the time of this writing.




**Persistent Malware: Ap0calypse**

The main interface of the Ap0calypse RAT has six tabs:

- Connections
- Broadcast
- Settings
- Builder
- Statistics
- About

We focus on Connections, Broadcast, and Builder tabs, which are more what we are looking for.

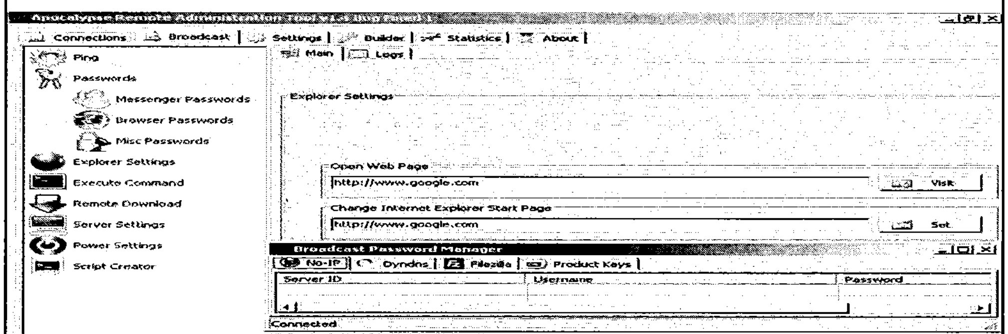
Settings and Statistics tabs are more related to the server side of the RAT, than the client.

The About tab has the description of it, with this information:

Using: Borland™ Delphi® 7
Compiled at: 02:09 AM Saturday 29 August, 2009
Coded In TURKEY

# Persistent Malware: Ap0calypse Server

- Broadcast allows the hacker to execute commands, retrieve passwords, and change settings




Identifying and Removing Malware

**Persistent Malware: Ap0calypse Server**

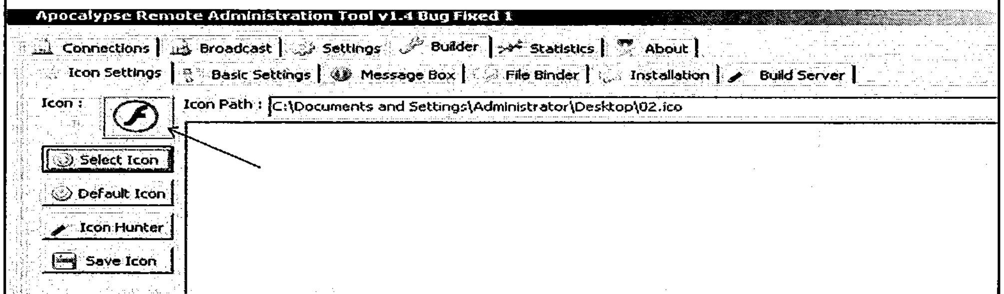
The Broadcast tab has several options that allow the hacker to push instructions and commands to all the clients that it has connected to its server.

These options are

- Ping
- Password (which allows it to get passwords from Messenger, Browser, No-IP, DynDNS, Filezilla, and also Product Keys)
- Change Explorer Settings, like the Internet Explorer Start Page, and open a specific web page
- Execute Commands on the client machine
- Change some server settings
- Power Settings
- Script Creator

# Persistent Malware: Ap0calypse Builder (1)

- The Builder tab allows the hacker to customize his new malware, first by selecting the icon to be used (in this case, an icon used by Flash files)




Identifying and Removing Malware

**Persistent Malware: Ap0calypse Builder (1)**

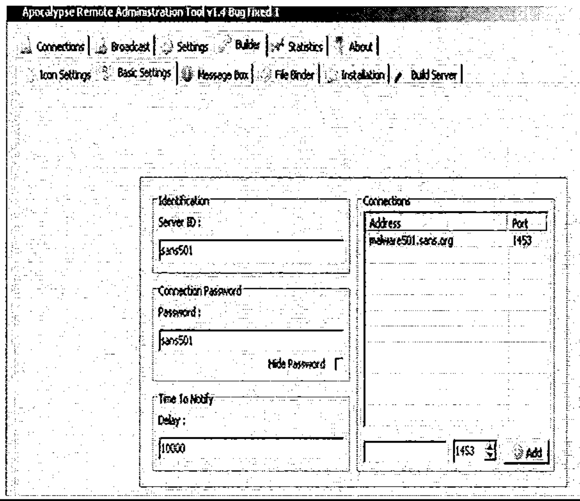
The sample application that has the server options and settings also allows the hacker to build its own customized client version.

The builder has several subtabs. The first subtab is Icon Settings, which allows the hacker to change the icon that will be used by its backdoor executable.

In the example, you use an icon that is used by Adobe Flash applications.

# Persistent Malware: Ap0calypse Builder (2)

- The hacker can then customize things like Server ID, Password, and the server/port to which it should connect




Identifying and Removing Malware

**Persistent Malware: Ap0calypse Builder (2)**

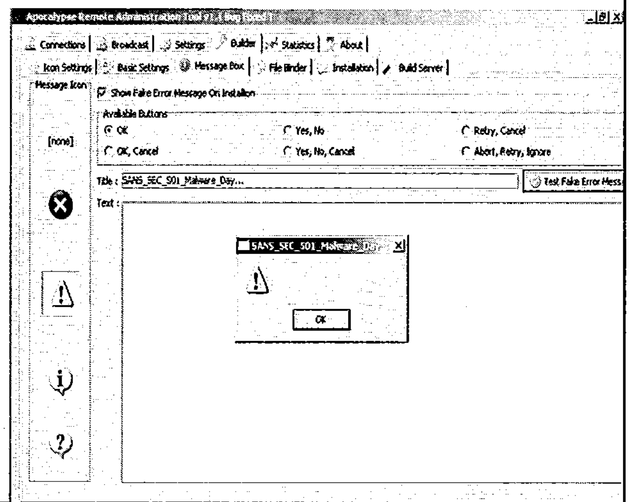
The Basic Settings subtab enables the hacker to configure options for the server that it will connect when executed on the victim machine.

For example, it is possible to define a Connection Password, which in this case is sans501, and the address which the server will be installed and the port number.

In this case, the address is malware501.sans.org and the port is 1453. (Note that this is not a valid address.)

# Persistent Malware: Ap0calypse Builder (3)

- The Builder also allows the option to create fake deceptive messages when executing the malware




Identifying and Removing Malware

**Persistent Malware: Ap0calypse Builder (3)**

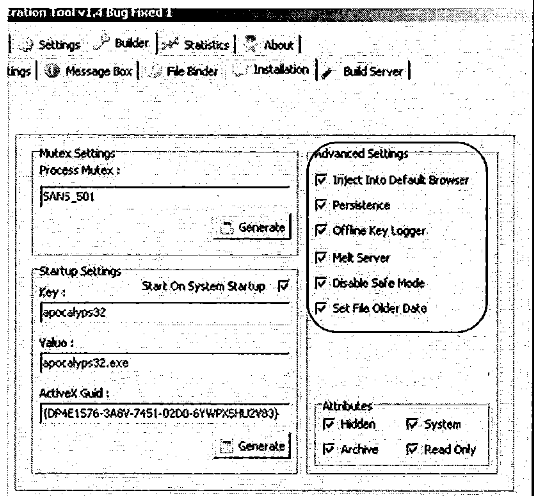
On the Message Box subtab, it is possible to configure a fake message to be shown when the malware runs on the system.

This message is sometimes used to make the user believe that maybe the application was corrupt and didn't work, so that in the background the malware can run and with no worries about the user being suspicious, because apparently the application didn't run correctly.

In the example, you selected the Attention message icon with the message SANS_SEC_501_Malware_Day.

# Persistent Malware: Ap0calypse Builder (4)

- The Advanced settings show the main options for persistence, such as Inject into the Browser and a Watchdog option, called Persistence, as well




Identifying and Removing Malware

**Persistent Malware: Ap0calypse Builder (4)**
On the Installation subtab, there is a box called Advanced Settings.

In this box, it is possible to select which Advanced options you will use to build the malware.

The options are:

- **Inject Into Default Browser**: This option will make the malware run in a more stealthy mode because the malware will not be seen on the process list, but will run as an injected code into the system browser, such as IE or Firefox. In this way, you can see the browser doing the malicious activities and not the executable.
- **Persistence**: This option creates a "watchdog" mode, which monitors when the process is running and the Registry entries are in place. This makes it much harder to remove it from the system.
- **Offline Key Logger**: This means that even if the client is not connected to the server, the key logger will be running.
- **Melt Server**: This is an option that makes the executable disappear after run.

- **Disable Safe Mode**

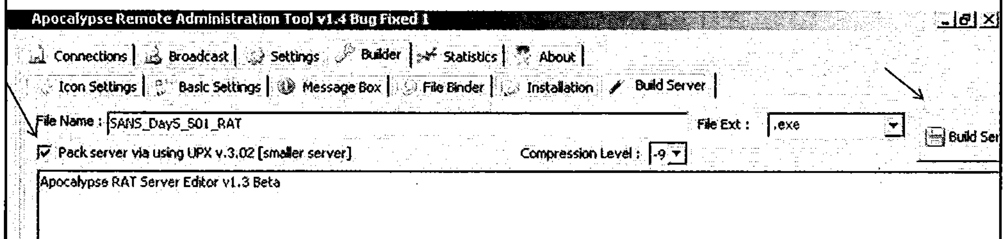
  This option disables the Windows Safe Mode. Some tools and techniques to remove malware require that you enter into Windows Safe Mode. When checking this option, the Safe Mode will not exist anymore.

- **Set File Older Date**

  This option sets the file to an older date than the date it was copied/installed. One of the techniques used to find out if new files are installed on the computer is using a simple Dir /O:d. This command lists all files and sort by date, which makes it easy to spot new files added to the folder, especially the Windows and Windows\System32 folders.

# Persistent Malware: Ap0calypse Builder (5)

- After the options are selected, the tab Build Server is used to define the filename used and the option to apply a packer (UPX) to make it smaller and attempt to bypass some antivirus




Identifying and Removing Malware

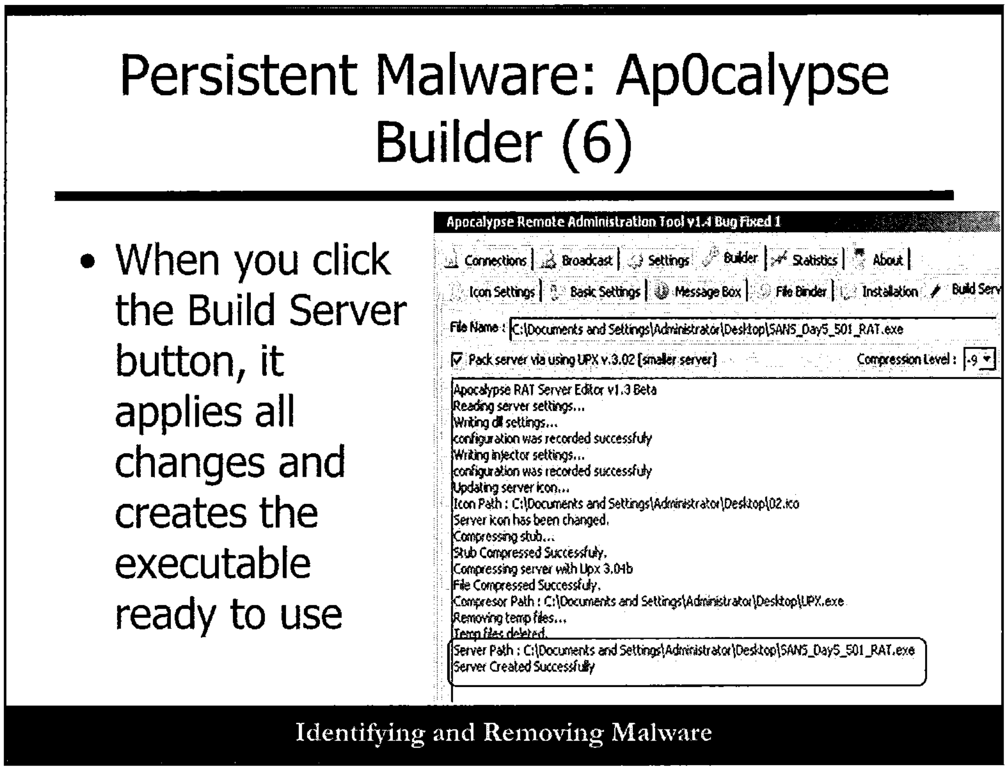
**Persistent Malware: Ap0calypse Builder (5)**

The last step to build the malware is to select the name that will be used by it and if you want to pack it.

If you decide to pack it, it uses the UPX packer. This is generally used to try to bypass antivirus and to make it a smaller size.

Although most modern antivirus can unpack UPX, it is still a valid technique.

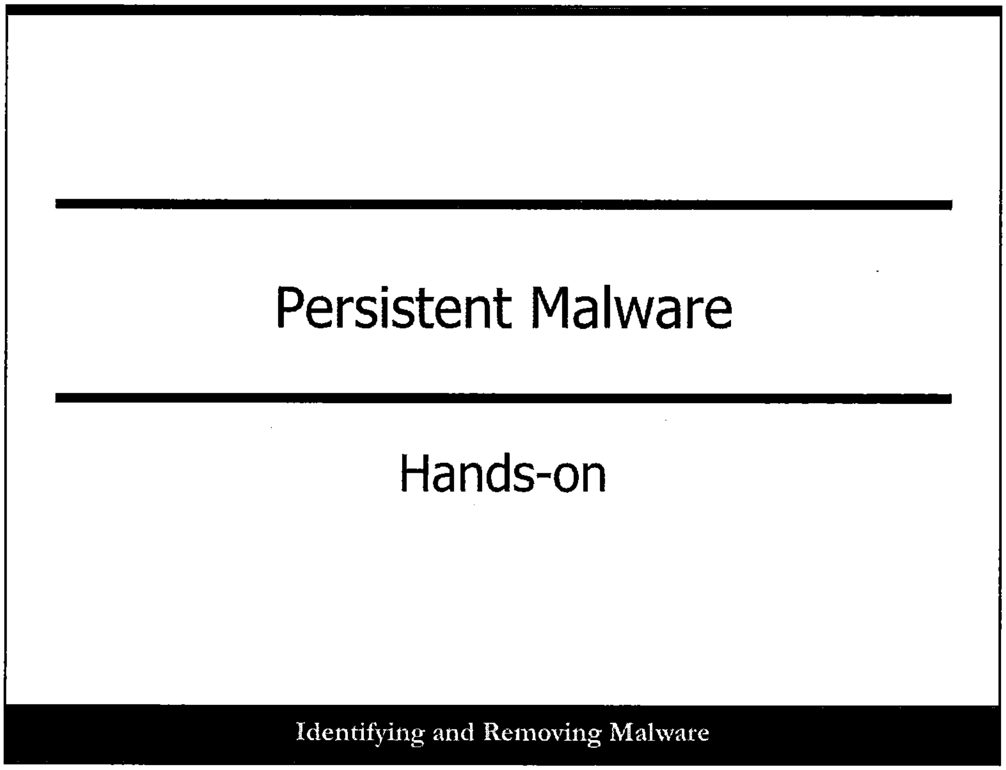
When ready, you just need to click the Build Server to create the customized version.




**Persistent Malware: Ap0calypse Builder (6)**

When you click the Build Server button, the builder creates a customized executable.

With no errors, the message box shows that the server was created successfully.



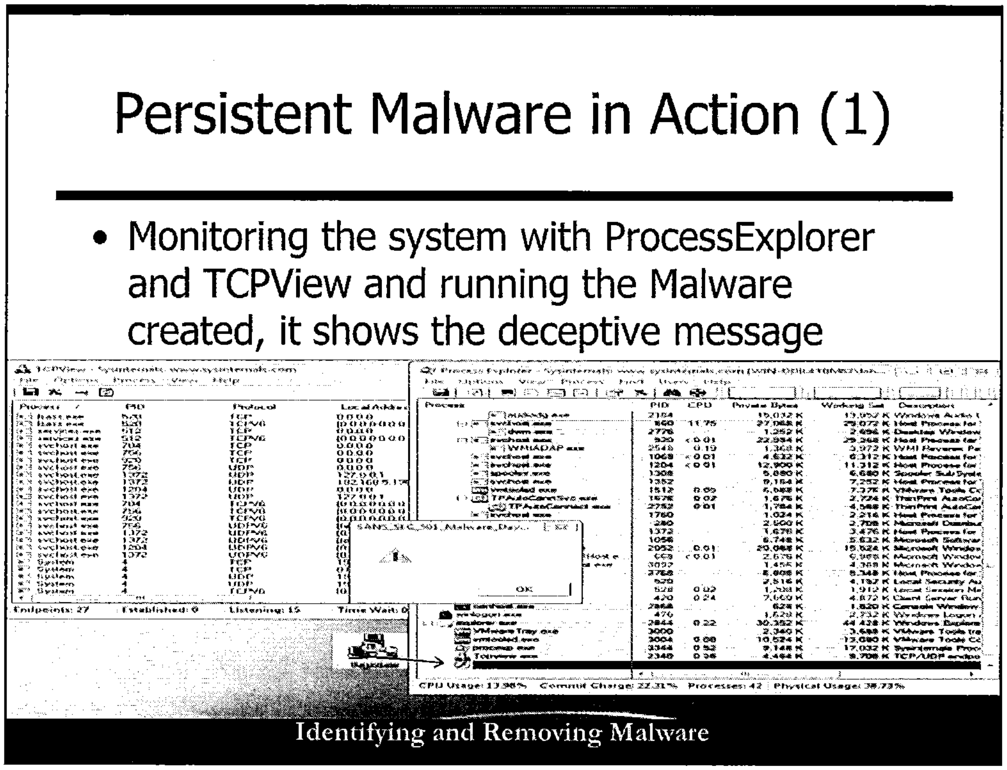

**Hands-on**

To start the "Persistent Malware Hands-On" section, you need to revert to our VM Image and run the course.exe file again.

On the RAT Malware part, start with the following steps:

1. Revert the VMware Windows 7 image to the Snapshot Clean7:
   VM -> Snapshot -> Select Clean7
2. Open the folder Course on the VMware Windows 7 Desktop.
3. Open the Part9 folder.
4. Copy HijackThis.exe, Processexp.exe, and Tcpview.exe to the desktop. This can be done by right-clicking and selecting Copy and going to the desktop and right-clicking and selecting Paste.
5. Double-click the SANS_Day5_501_RAT.exe file.

Now, continue to follow the slides doing the same on the VMware Windows 7 image.




**Persistent Malware in Action (1)**

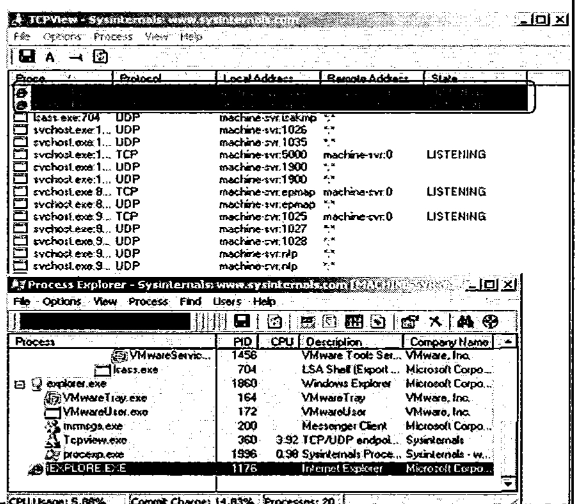
Monitor the system with Microsoft Sysinternals Process Explorer and TCPView. Run both tools as Administrator and arrange them in a way that it will be possible to see both running.

> Now that they are running, let's run the RAT Backdoor trojan. It creates a folder called SANS_Day5_501_RAT.
>
> Double-click the folder, and it opens the folder.
>
> Now right-click the file SANS_Day5_501_RAT.exe and select Run as Administrator.

Notice that when we run it, the fake warning message appears. On Process Explorer it is also be possible to see that it is running.

# Persistent Malware in Action (2)

- After you click OK, you can see that the process disappears from the process list
- You can see an Internet Explorer process trying to access a remote address at port 1453



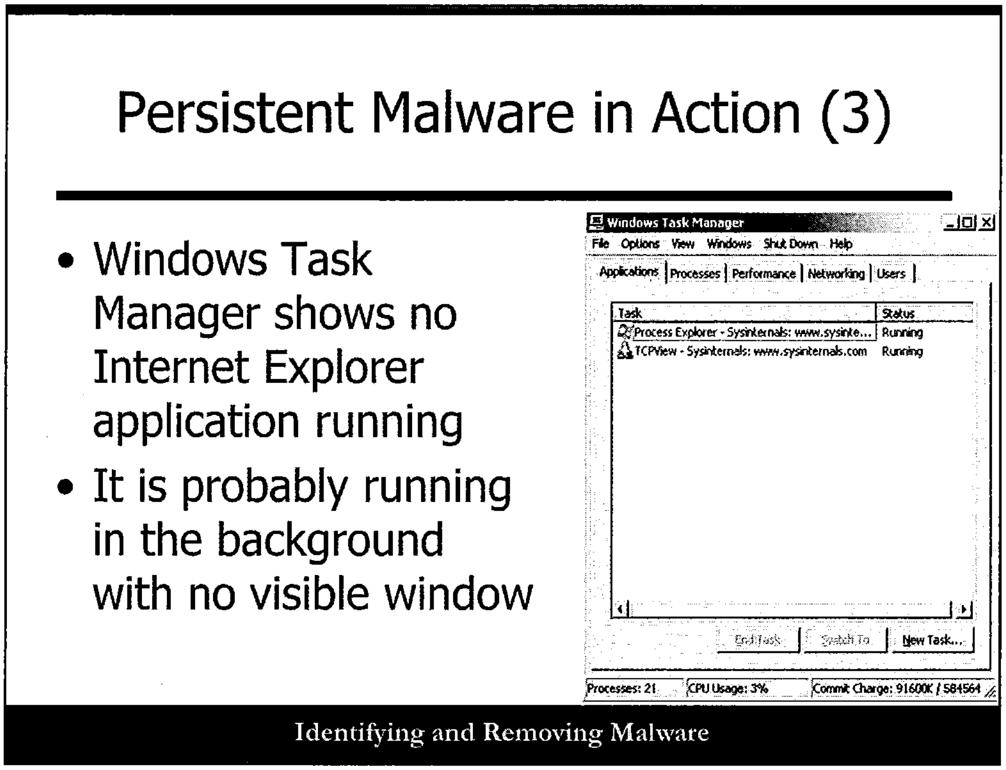

Identifying and Removing Malware

**Persistent Malware in Action (2)**

After you click the OK button on the fake warning message, you can see that the SANS_Day5_501_RAT.exe exits, but a new process starts, the Internet Explorer process.

If the system can resolve domains, you also notice that it tries to connect to the remote server on port 1453.

If your VM image cannot resolve domains, you cannot see this part, but you will still see the Internet Explorer process.

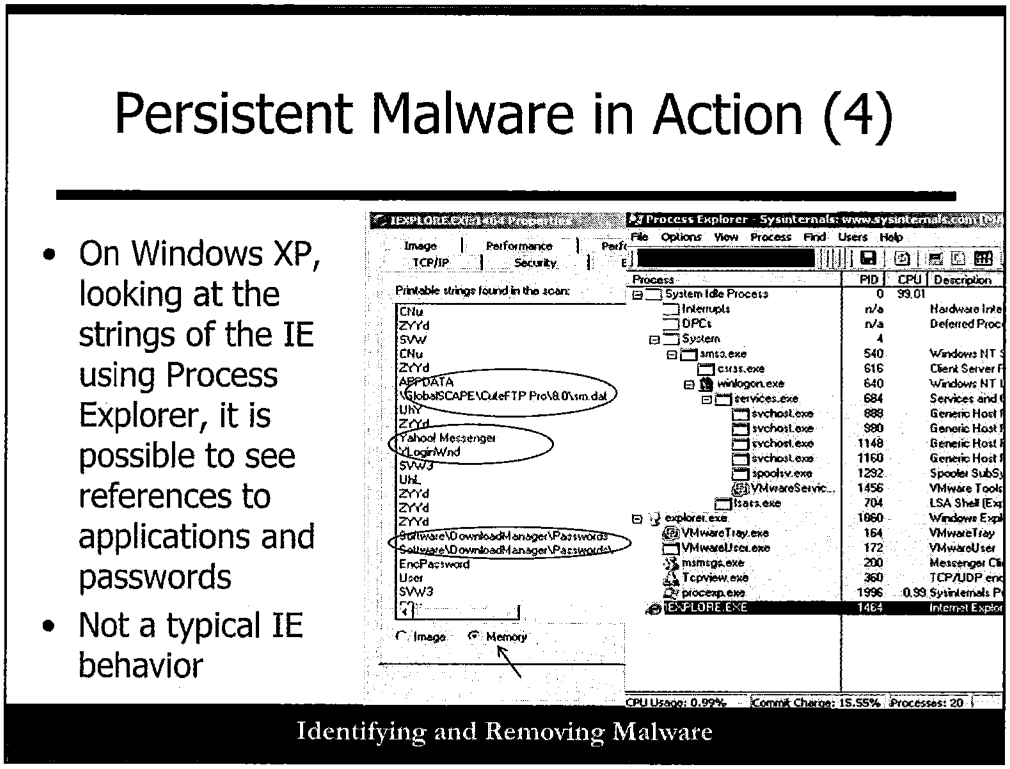



**Persistent Malware in Action (3)**

You can now open Windows Task Manager (using the shortcut Ctrl+Shift+ESC keys).

On the Applications tab it is possible to see only two windows, Process Explorer and TCPView. Remember that the applications tab shows the processes that are in the foreground, that means, with Windows. So, why would an Internet Explorer process, which is an Internet browser, not have a visible window?

That means that it is running in the background and with no visible window, which is highly suspicious.




**Persistent Malware in Action (4)**

We already know that Process Explorer offers an option to check the strings of any given process, being the strings from the image file on disk, or on memory, which is always useful when dealing with a packed malware.

If you come across this malware on Windows XP, it is possible to see some interesting strings. In Process Explorer, double-click the Internet Explorer process and click the Strings tab. At the bottom of the Strings window, be sure to select the Memory option.

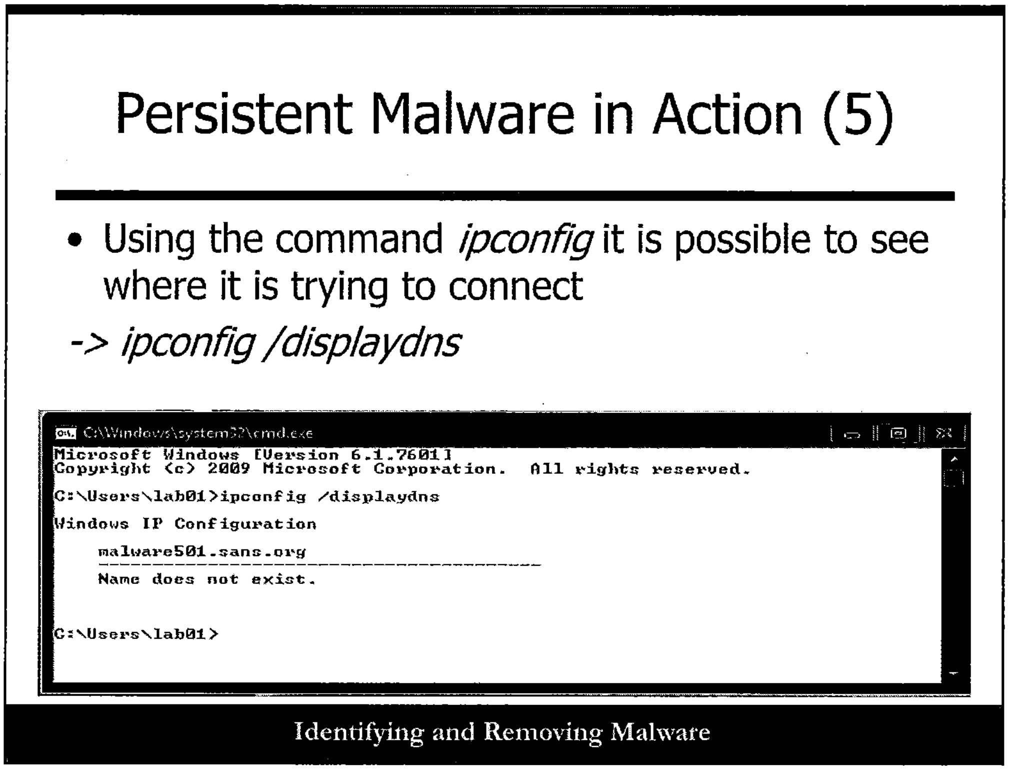
If you go through all the strings, you find some strings that are not part of a "clean" Internet Explorer process, such the following:

APPDATA
**\GlobalSCAPE\CuteFTP Pro\8.0\sm.dat**
UhY
ZYYd
**Yahoo! Messenger**
**YLoginWnd**
SVW3
UhL
ZYYd
ZYYd
ZYYd

**Software\DownloadManager\Passwords**
**Software\DownloadManager\Passwords**
**EncPassword**
**User**

During the previous phase, you saw that the Ap0calypse RAT gathered passwords from different applications, such as Messenger, FTP clients, and so on. Here, it is clear.

Also, in Advanced Settings, there was an option called Inject Code into Default Browser. This option was created to inject the malicious code into the browser, so it could run in stealth mode, exactly what you see here.




**Persistent Malware in Action (5)**

Another way to verify where the malware is trying to connect or even which domains it queried before is by using the ipconfig command.

Open a DOS prompt.
-> Click Start; then click Run, type **CMD,** and press Enter.

On the DOS prompt, type **ipconfig** and Press Enter.
The output is the common output that shows the IP information for the interfaces installed.

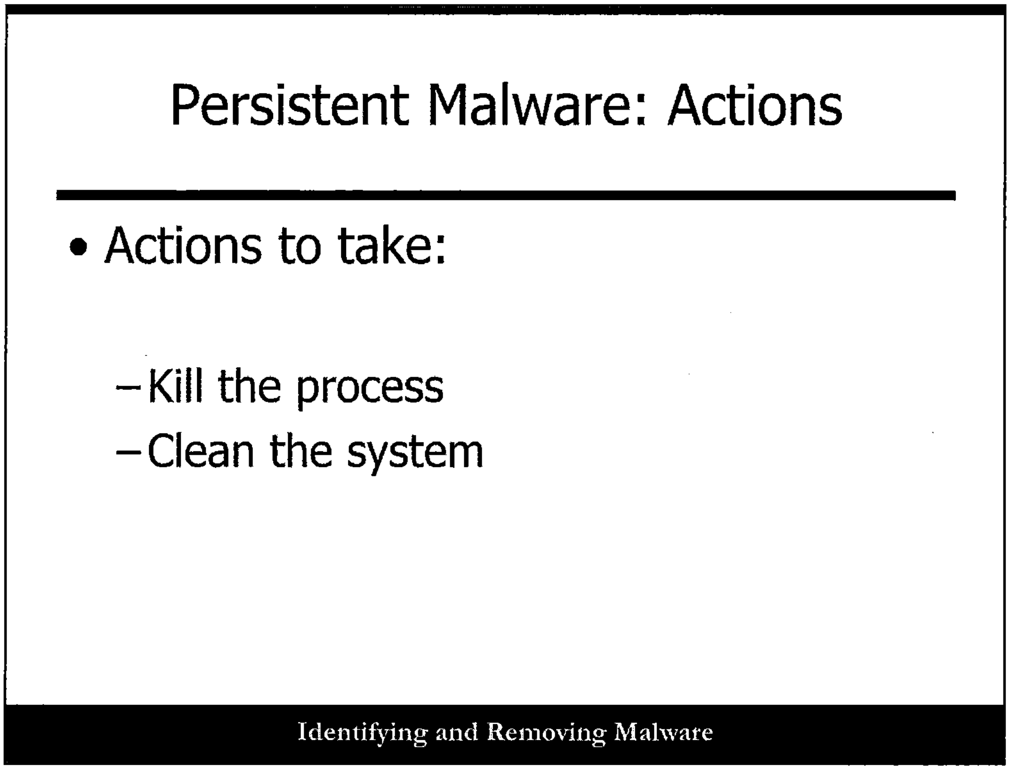
An additional switch that can be used with ipconfig is the option to display the DNS cache on the machine. This is done via the command: ipconfig /displaydns

```
C:\Windows\system32>ipconfig /displaydns

Windows IP Configuration

    malware501.sans.org
    ----------------------------------------
    Name does not exist.
```

Again, this information is shown only if the VM can resolve names.




**Persistent Malware: Actions**

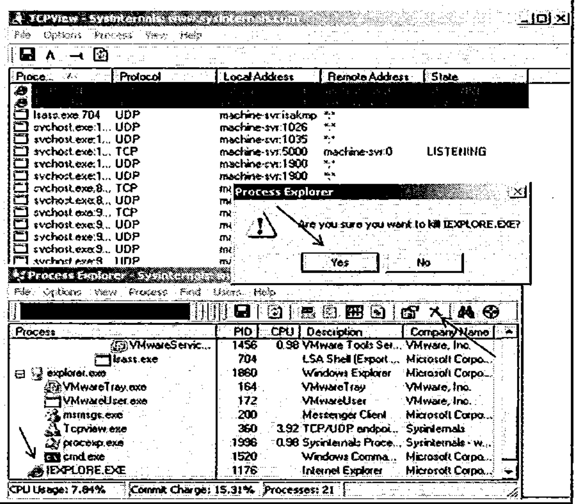
Now that we have the malware installed on the system, we need to get rid of it.

Our suggested actions will be:

- Kill the process.
- Clean the system.

# Persistent Malware: Process Explorer

- Highlighting the process and clicking X button lets you kill it




Identifying and Removing Malware

**Persistent Malware: Process Explorer**

The first step is to kill the process via Process Explorer. As you saw on previous modules, Process Explorer can kill any process simply by clicking to highlight it and then pressing the X button. After that, it will ask for confirmation.

In this case, let's try it with the Internet Explorer process.

Click once on it in Process Explorer, so it will be highlighted. Then, click the red X button. When the confirmation pop-up appears, just click the Yes button.

## Persistent Malware: Cleaning Problems (1)

- Problem:
  - As soon as you kill Internet Explorer with the injected malware, it restarts. This is part of the "watchdog" persistent method
  - This happens if you try with ProcessExplorer, Windows Task Manager, or even with WMIC

Identifying and Removing Malware

**Persistent Malware: Cleaning Problems (1)**

As noted, Process Explorer kills the Internet Explorer, but just after that a new Internet Explorer shows up there again. (Please note that you may notice different behavior in Windows 7 32 bit and Windows 7 64 bit)

This is part of the "watchdog" persistent method used by the Ap0calypse RAT.

This is not a defect of Process Explorer. You can try it with Process Explorer, Windows Task Manager or even via command line with WMIC. All these behave the same.

You can go ahead and open Windows Task Manager again and try it.

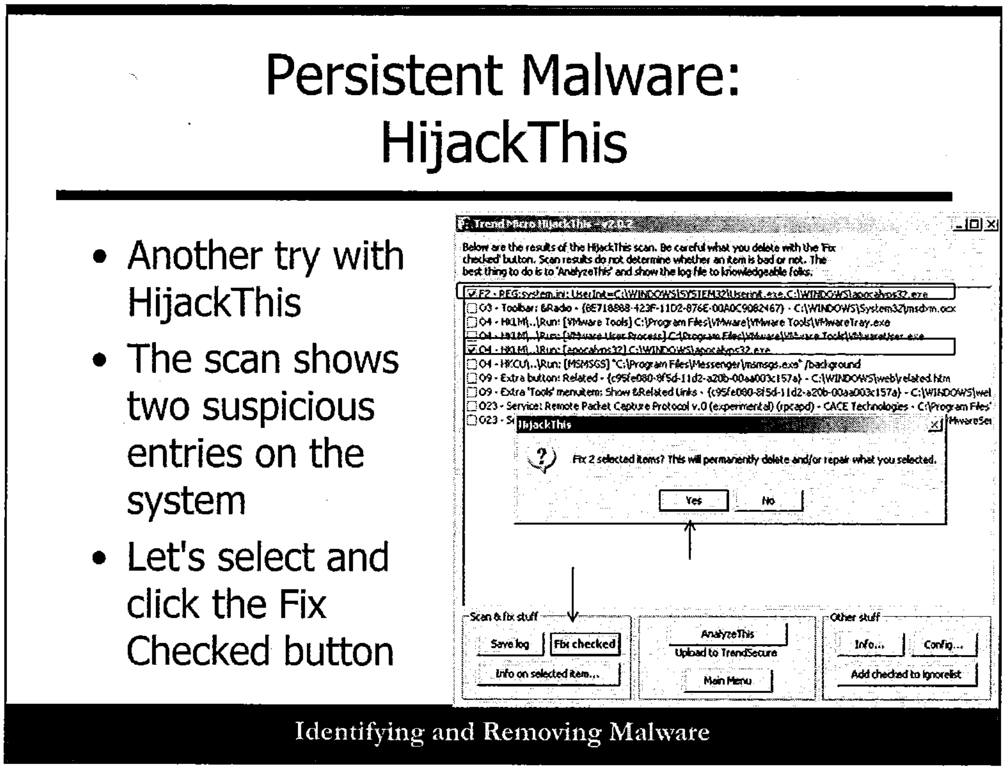
To open it, use the shortcut Ctrl+Shift+ESC key. Then click the Process tab, locate the Internet Explorer process, and click the End Process button.

Another option, via WMIC:

Open a DOS Prompt window and type:

-> wmic process list brief <- this will list the processes running and the respective Process ID number (PID). The PID will be necessary to kill the process.

-> wmic process <PID_Number> delete <- this will actually kill the process, but as noted, you can list the processes again and it will be there.




**Persistent Malware: HijackThis**

We already tried to kill the process using several methods, but the watchdog method prevents it.

Now, you will make another attempt with the HijackThis tool and see what else can you find on this process.

Let's run HijackThis and scan the system. This can be done by double-clicking the HijackThis.exe application that was copied to the desktop.

When you double-click it, you can select the option Do a System Scan Only. The output will be quite close to this:

F2 - REG:system.ini: UserInit=C:\WINDOWS\system32\userinit.exe,C:\WINDOWS\apocalyps32.exe

O3 - Toolbar: &Radio - {8E718888-423F-11D2-876E-00A0C9082467} – C:\WINDOWS\System32\msdxm.ocx

O4 - HKLM\..\Run: [VMware Tools] C:\Program Files\VMware\VMware Tools\VMwareTray.exe

O4 - HKLM\..\Run: [VMware User Process] C:\Program Files\VMware\VMware Tools\VMwareUser.exe

O4 - HKLM\..\Run: [apocalyps32] C:\WINDOWS\apocalyps32.exe

O4 - HKCU\..\Run: [MSMSGS] "C:\Program Files\Messenger\msmsgs.exe" /background

O9 - Extra button: Related - {c95fe080-8f5d-11d2-a20b-00aa003c157a} – C:\WINDOWS\web\related.htm

O9 - Extra 'Tools' menuitem: Show &Related Links - {c95fe080-8f5d-11d2-a20b-00aa003c157a} – C:\WINDOWS\web\related.htm

O23 - Service: Remote Packet Capture Protocol v.0 (experimental) (rpcapd) - CACE Technologies – C:\Program Files\WinPcap\rpcapd.exe

O23 - Service: VMware Tools Service (VMTools) - VMware, Inc. - C:\Program Files\VMware\VMware Tools\VMwareService.exe

You can now try to select and fix the suspicious Ap0calyps32.exe entries. Select the two/three entries and click the Fix Checked button.

In theory, it cleans those entries.

## Persistent Malware: Cleaning Problems (2)

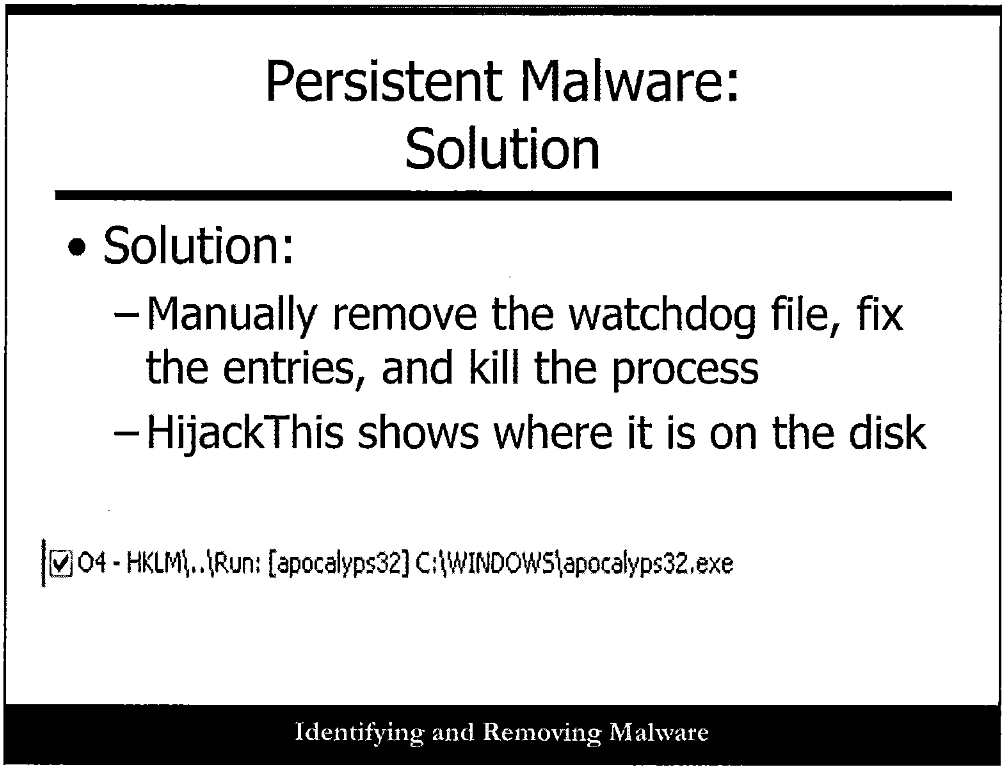
- Problem 2:
  - Another scan with HijackThis shows that the entries that were removed were added again
  - The "watchdog" process is preventing us from removing it

Identifying and Removing Malware

**Persistent Malware: Cleaning Problems (2)**

Another problem with the cleaning…

As you rescan with HijackThis, you can see that the results are not good. As soon as it removes it, the watchdog mechanism adds them again.




**Persistent Malware: Solution**

Because the watchdog mechanism prevents us from removing the entries and killing the process, we need to follow with another approach.

Remember that this malware also disables the Windows Safe Mode, so you cannot reboot the system and enter into Safe Mode to try something else. The approach now is to manually remove the watchdog file.

One good thing in the HijackThis scan result is that we were able to see where it is located:

**O4 - HKLM\..\Run: [apocalyps32] C:\WINDOWS\apocalyps32.exe**

## Persistent Malware: Removing the Watchdog

*-> C:\>move c:\windows\apocalyps32.exe c:\virus.ex_*

The reason for using move instead of Del is that with move you can send this file to your antivirus later.

Now it is time to kill the process and fix the entries

Identifying and Removing Malware

**Persistent Malware: Removing the Watchdog**

There may be several ways to do so. The easiest way is simply to open Windows Explorer in that location and drag the file to some other place.

Another way is simply to open a DOS prompt window and do it by hand.

Open the DOS prompt:

> Click Start, click Run, and type **CMD**. Right-click the CMD.EXE, select Run as Administrator, and press Enter.

Now let's move the files to C:\:

```
-> C:\>move c:\windows\apocalyps32.exe c:\virus.ex_
```

Instead of Move, you could simply use Del and remove the file. The reason to use Move instead of Del is to preserve the file and move it to another location on the disk. In this way, it will be possible to send the file to the antivirus for analysis.

After you are done with this step, it will finally be time to kill the process and fix the entries.

# Persistent Malware: Killing the Process

- The process can be terminated with either Windows Task Manager or repeating the same step with Process Explorer
- A CLI version with WMIC would also works:
  - > *c:\wmic process list brief* <- to get the PID (process ID)
  - > *c:\wmic process <PID> delete*

  Deleting instance \\MACHINE\ROOT\CIMV2:Win32_Process.Handle="<PID>"
  Instance deletion successful.

Identifying and Removing Malware

**Persistent Malware: Killing the Process**

The process now can be killed using any tool, from WMIC, to Windows Task Manager or Process Explorer.

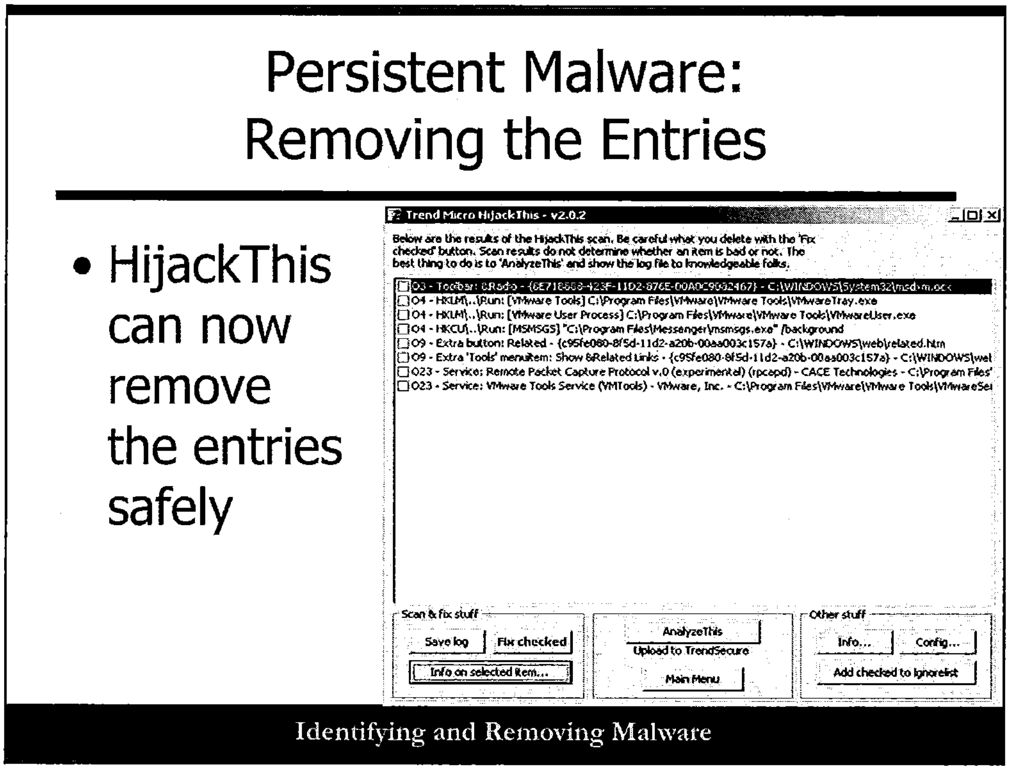
Using the command line with WMIC, open the DOS prompt:

-> Click on Start, then click on Run and type CMD. Press Enter.

-> c:\wmic process list brief <- to list and get the PID (process ID)

-> c:\wmic process <PID> delete

Repeat the process listing step to verify that this time it killed the process.

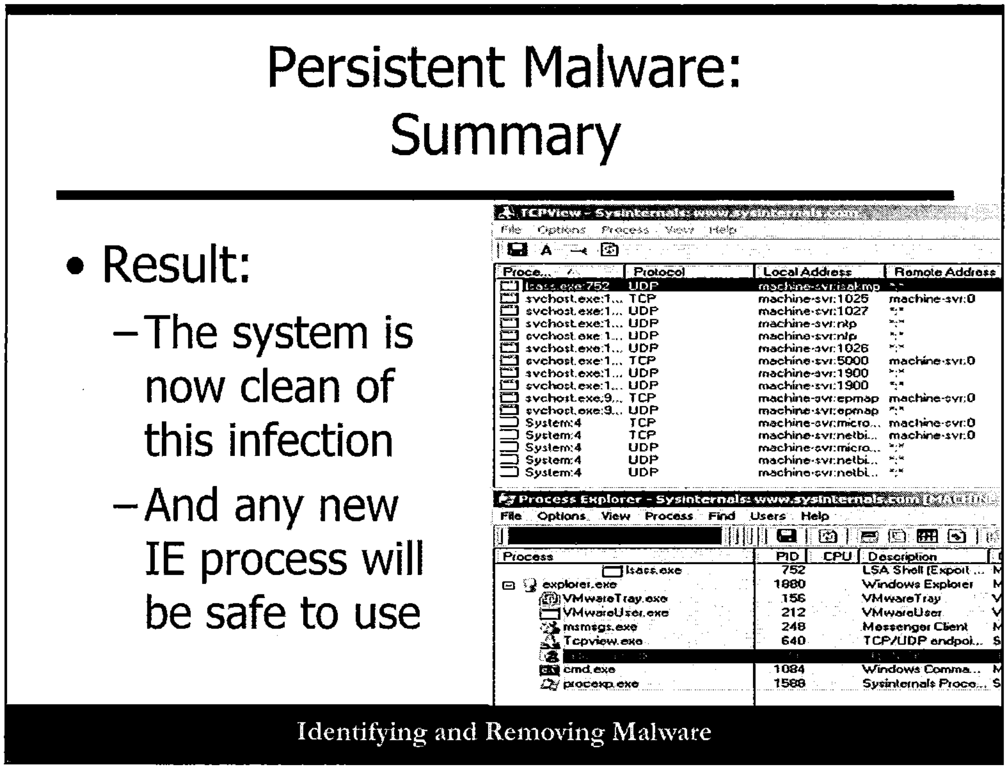



**Persistent Malware: Removing the Entries**

Now that we removed the watchdog file and killed the process, we can delete the entries.

Just run HijackThis scan again, select the entries to be fixed, and click the Fix Checked button.

Rescan and you see that this time, they have been removed.




**Persistent Malware: Summary**

Because you removed the watchdog file, killed the process, and removed the malicious entries, the view of Process Explorer will be almost the same as on the slide. You got rid of the infection and have a clean system.

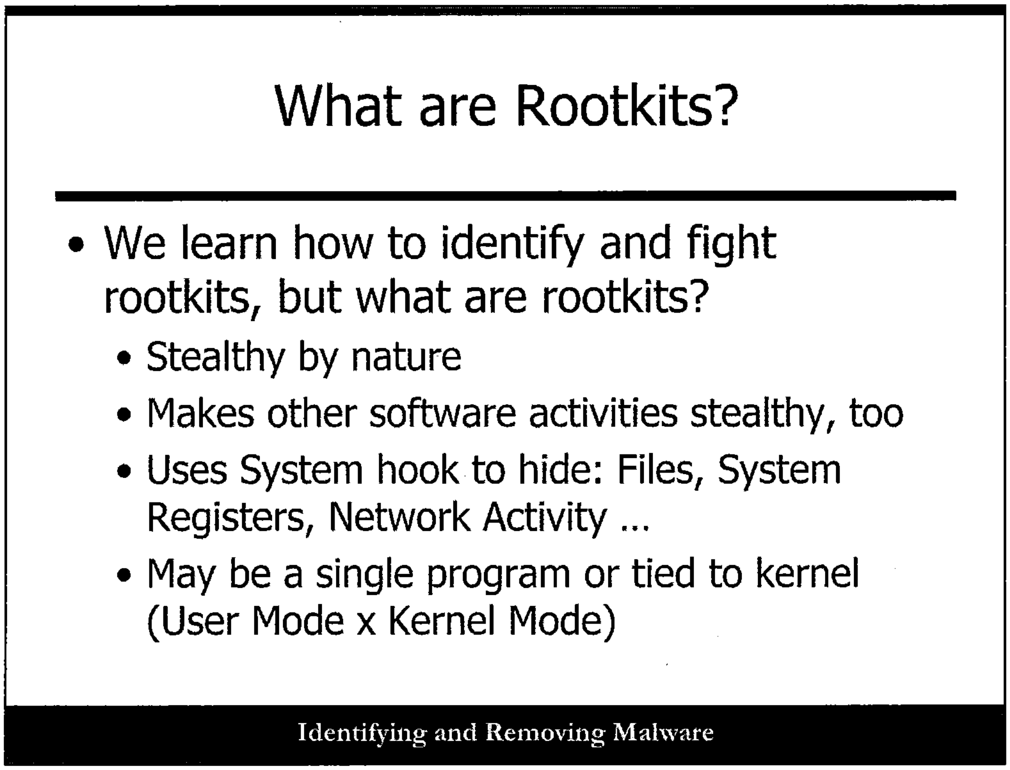
You can now safely start a new Internet Explorer process with no risk of infection.

## Identifying and Removing Malware

## Identifying and Fighting Rootkits

Identifying and Removing Malware

This page intentionally left blank.




**What are Rootkits?**

You will probably find several definitions of rootkits. My definition is that a rootkit is some piece of software whose purpose is to hide activities on the user's machine.

Wikipedia[1] defines a rootkit as:

"A rootkit is a general description of a set of programs which work to subvert control of an operating system from its legitimate operators. Usually, a rootkit will obscure its installation and attempt to prevent its removal through a subversion of standard system security. Techniques used to accomplish this can include concealing running processes, files or system data from the operating system. Rootkits have their origin in benign applications, but in recent years have been used increasingly by malware to help intruders maintain access to systems while avoiding detection. Rootkits exist for a variety of operating systems, such as Microsoft Windows, Mac OS X, Linux, and Solaris. Rootkits often modify parts of the operating system or install themselves as drivers or kernel modules."

Examples of such activities could be

Hide files

- Hide Registry entries
- Hide network activity

In this way, the rootkit can hide software such as a keylogger that can save the keys typed by a user to a file and send the file to a remote host, or create a backdoor in the system, allowing hackers to get into the machine in an "invisible" way.

One thing to notice is that rootkits are usually loaded as device drivers (files with .sys extension), so most of the time you can notice an .exe and .sys as part of the rootkit schema.

There are several types of rootkits, but we focus on the most common ones:

- User Mode Rootkit
- Kernel Mode Rootkit

Find more information at this Wikipedia reference on rootkits: http://en.wikipedia.org/wiki/Rootkit.

# Rootkits: User Mode

Three types of rootkits:

- User mode rootkits
  - More common
  - Hook into user/application space
  - Intercepts calls and returns rootkit modified information
  - Easier to implement for malware author

Identifying and Removing Malware

**Rootkits: User Mode**

**User Mode Versus Kernel Mode**

Most applications work in user mode and can be visible to anyone. User mode rootkits are rootkits that do not modify the kernel but only other user applications. They usually run as a separate thread inside an application.

The user mode rootkits will usually hook into user/application space to intercept system calls and then return the information filtered as wanted by the hacker.

The most used techniques implemented by user mode rootkits are:

- Intercept calls to an API
- Patch an API

For example:

You want to see the contents of a directory (the files within a folder …).

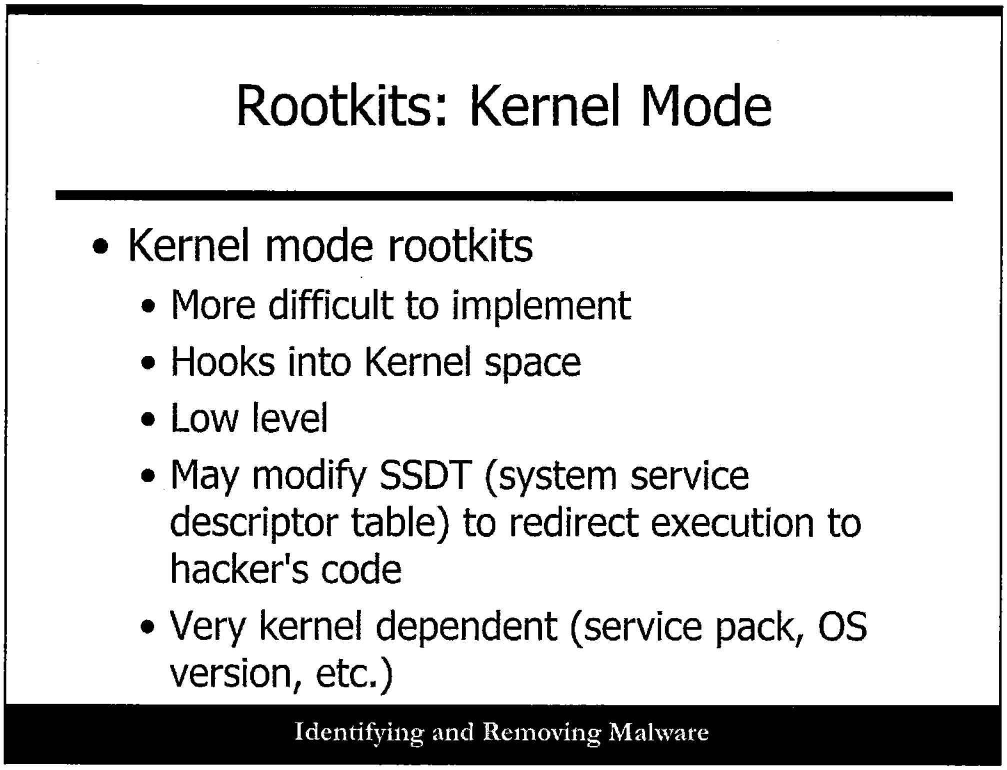
Explorer will call the following APIs:

FindFirstFile
FindNextFile

Those APIs are located in the ADVAPI32.DLL. The rootkit will find the APIs in the ADVAPI32.DLL and modify them so that when Windows Explorer calls the DLL, the execution will be redirected to the rootkit. The rootkit will then modify the results before returning them back to Windows Explorer. The modification can be anything, like hiding all files that start with rk*. In this way, if the rootkit files are in that folder and start with rk*, they will not appear inside the folder!

Although simpler to uncover than kernel mode rootkits, the user mode rootkits have the advantage of being easier to implement because they will not be dependent on kernel specifics.

An example of a User Mode Rootkit is the Hacker Defender Rootkit.




**Rootkits: Kernel Mode**

Kernel mode rootkits are a little more complex than user mode rootkits.

Basically, they play with the hooks in kernel space and at a low level. You can think of kernel mode rootkits as applications that can hide from any user-mode program. Because the kernel is the most important and privileged part of the operating system and the rootkit will be running in kernel space, kernels also have control of the operating system.

Like user mode rootkits, those in kernel mode try to find a way to intercept the various calls and requests the user and system make. They can return any information they want, but in a more powerful way, because they can now intercept native API calls and manipulate some kernel mode data structures.

One of the techniques used by kernel mode rootkits is hooking into the system service descriptor table (SSDT) too, for example, hide a process from the kernel's list of active processes.

The main problem with kernel mode rootkits is that they are kernel-dependent, which means that although one may work in Windows 2000, for example, it may not work in Windows XP, Windows 2003, or even in a different Service Pack level for the same operating system.

Examples of Kernel Mode rootkits are

- NtRootkit
- HE4Rootkit
- Cutwail

The Cutwail Trojan is part of the Cutwail botnet, which was one of the most prevalent botnets in the last quarter of 2009.

## Rootkits: MBR

- MBR Rootkits:
  - Technique where the rootkit replaces the MBR (Master Boot Record)
  - Common in DOS era
  - On rise since 2007
  - Makes current anti-rootkit tools useless
  - Common examples: Stoned Bootkit, MebRoot, and TDSS/TDL3/TDL4

Identifying and Removing Malware

**Rootkits: MBR**

The Master Boot Record (MBR) is the first section of the disk, and the rootkit takes advantage of this to write its code in a way that it can be loaded on the early stage of the operating system boot process.

This technique was quite common during the DOS era but became in disuse until 2007 when the first actual malware was spotted.

Because it's the nature of the rootkit to hook onto the system before the OS loads, it can hide from many applications, including some antivirus and anti-rootkits.

Common examples of those malware are MebRoot, Sinowal, and TDSS. In 2009, researcher Peter Kleissner released his own version called Stoned Bootkit, of which he made the source code available in 2010.

In 2011 and 2012, the most common MBR rootkit was from the TDSS family, downloading additional malware to the machine.

## Are Rootkits Malicious?

- Are all rootkits malicious?
  - Yes!
- But ...
- What about Sony DRM's 2005?
  "It was just Xtended Copy Protection ..."
- What about Sony USB Stick hidden files in 2007?
  "Ooops, we did it again ..."

Identifying and Removing Malware

**Are Rootkits Malicious?**

Although you may find some people that defend some types of rootkits, I can't see software that tries to hide aspects of an application in the OS as something benign. In 2005, we had a clear case of how things can go wrong when you try to implement a rootkit in a system, obviously without the user's agreement.

In October 31, 2005, Mark Russinovich, from SysInternals, revealed details of Sony's extended copy protection (XCP) digital rights management (DRM) application that it used on its audio CDs. The XCP was a rootkit that was designed to hide any files, Registry keys, and processes starting with the string $sys$ so that they could hide the XCP application.

A series of problems resulted:

- It was installed even before the EULA was presented to the user.
- Removal/uninstall could cause serious problems with Windows drives.
- Any malware writer could write his malware to start with the name beginning with the string $sys$ and be hidden by Sony's XCP application.

In 2007, the F-Secure Blog reported that three models of Sony USB stick drives with fingerprint capabilities were using rootkit techniques. The fingerprint reader software was installing a device driver that would hide a folder in the same way as rootkits! Bad? You bet! Now any malware writer could include those files in their malware and it would be hidden in the operating system.

## Rootkits: Our Approach

- Examples on Windows 7
- Also examples on Windows XP
  - Still a large market share
  - More rootkits for Win XP
  - More anti-rootkit tools for Win XP
- Hands-on using Windows 7 32-bit

Identifying and Removing Malware

**Rootkits: Our Approach**

This course material was updated to cover Windows 7; although Windows XP still has a large market share, its EOL (End of Life) is now a reality. Another point is that although most companies decided to keep Windows XP instead of updating to Windows Vista, the adoption of Windows 7 is a common point for most companies and the end user.

Because we still have a large base of Windows XP users out there, we cover the rootkits and anti-rootkit tools that exist for Windows XP; however, the hands-on is only for Windows 7.

Also, on Windows 64-bit OSes (both XP and 7), Microsoft incorporated Patch Guard (Kernel Patch Protection), which prevents a lot of rootkits from working properly because they can no longer patch the Kernel.

# Rootkits and Anti-Rootkits

## Windows XP: Examples

Identifying and Removing Malware

Although the training material is based on Windows 7, we decided to include this subsection of Tools specifically for Windows XP. The reason, as explained before, is there is still a large user base of Windows XP in both the corporate and end user worlds.

The following slides contain tools that are needed to fight rootkits on Windows XP systems, but that don't work on Windows 7. There few examples of rootkits that work on Windows 7, and the same applies for the anti-rootkit tools. Most of the tools from Anti-Virus and Security companies will not work under Windows 7 and 8.

If you want to practice these examples on a Windows XP system, we included the file badkits.zip in the "Part 7" folder that you can use later.

## Rootkits: XP Example

- In the following example, we examine a machine that acts strangely
- Identify/verify malicious activity with Windows tools

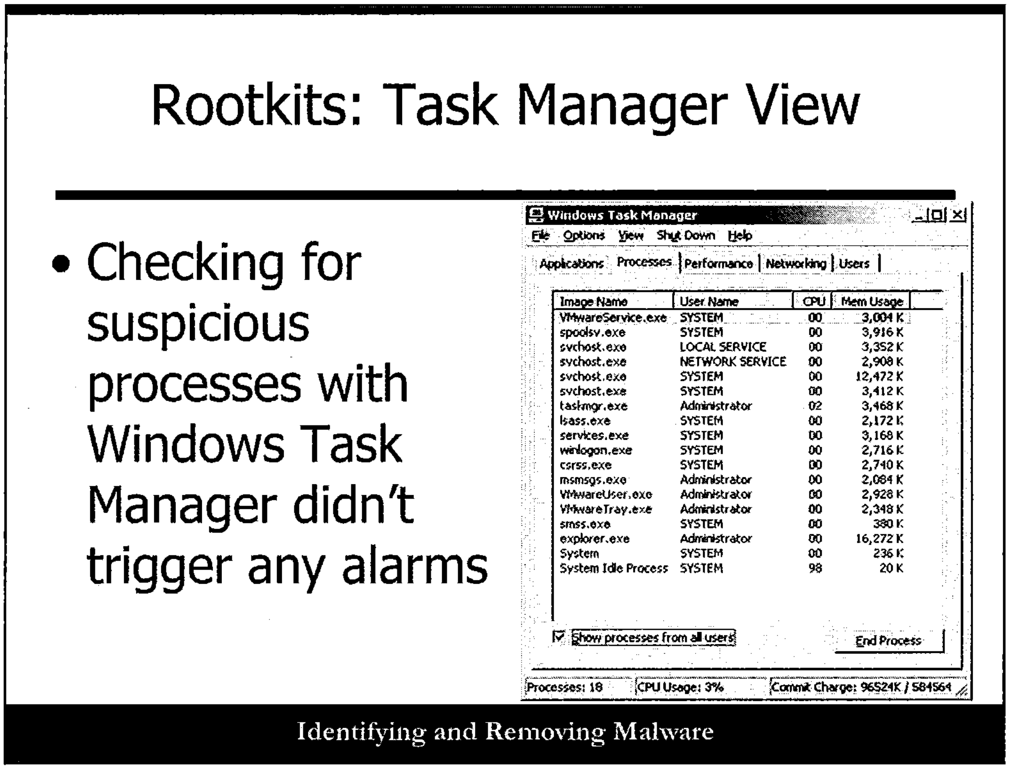
Identifying and Removing Malware

**Rootkits: Live Example**

**Our Learning Example**

In the learning example with rootkits is the following scenario: A machine was working okay, but the Incident Response Team identified that something was not quite right. That's not exactly the best thing to hear, because no details were provided, yet we have to figure it out.

First, try to identify if something is wrong using tools such as Task Manager, Process Explorer, and TCPView.




**Rootkits: TaskManager View**

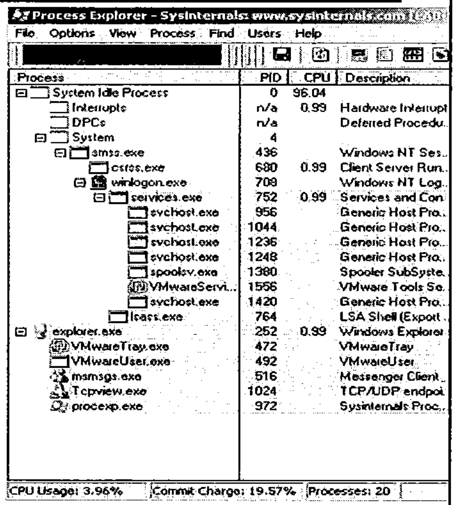
**Using Task Manager**
The first thing to do is use Windows Task Manager and visually try to identify anything that could be considered suspicious and any process that would not fit in the machine configuration.

This is obviously not an easy task because a machine can have hundreds of processes and you may not always know each of the processes, and because a malicious process can choose a deceptive name to avoid visual detection.

In this case, nothing triggers the "visual radar."

# Rootkits: Process Explorer View

- Using Process Explorer to look for suspicious processes didn't help either




Identifying and Removing Malware

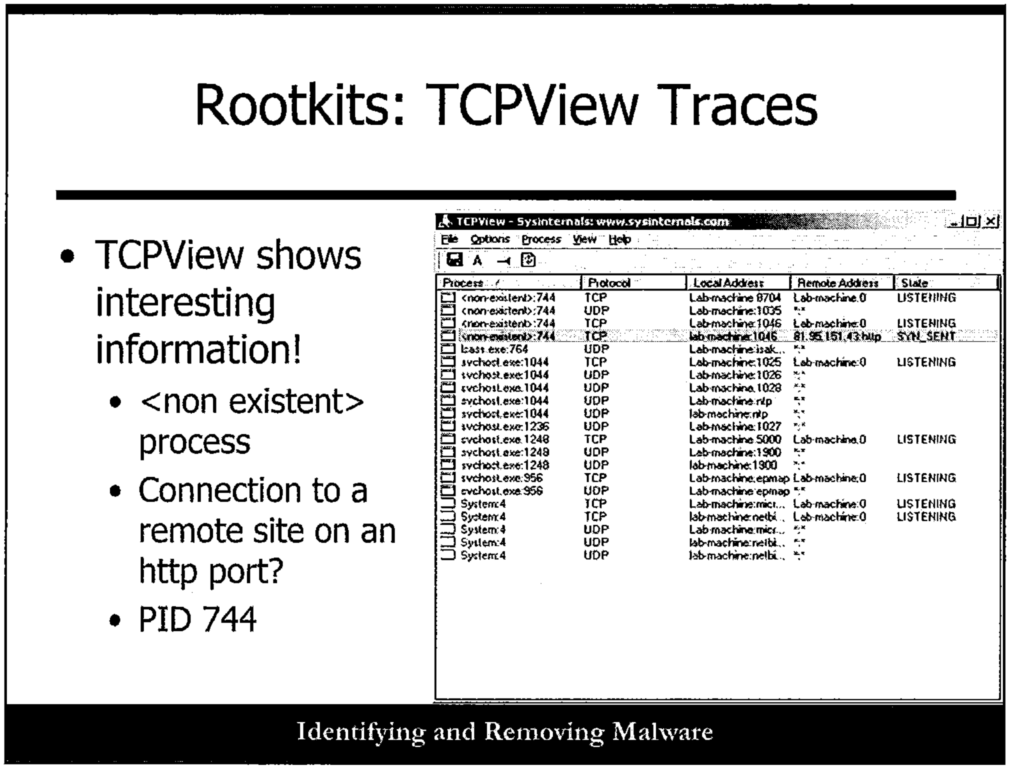
**Rootkits: Process Explorer View**

**Using Sysinternals' Process Explorer**

We already tried to identify possible suspicious processes or services with Windows Task Manager, but we didn't have any luck. Now we will try to see the same processes and services with Microsoft Sysinternals tool Process Explorer.

Process Explorer can give a much more complete view of the processes and services on the machine, including the description of the process and service.

| Process | PID | CPU | Description | Company Name |
|---|---|---|---|---|
| System Idle Process | 0 | 98.02 | | |
| Interrupts | n/a | | Hardware Interrupts | |
| DPCs | n/a | | Deferred Procedure Calls | |




**Rootkits: TCPView Traces**

**Using Sysinternals TCPView**

Because we already tried to get information with Windows Task Manager and Process Explorer and could not identify any suspicious processes or services, we can now try to use another well-known Sysinternals tool: TCPView.

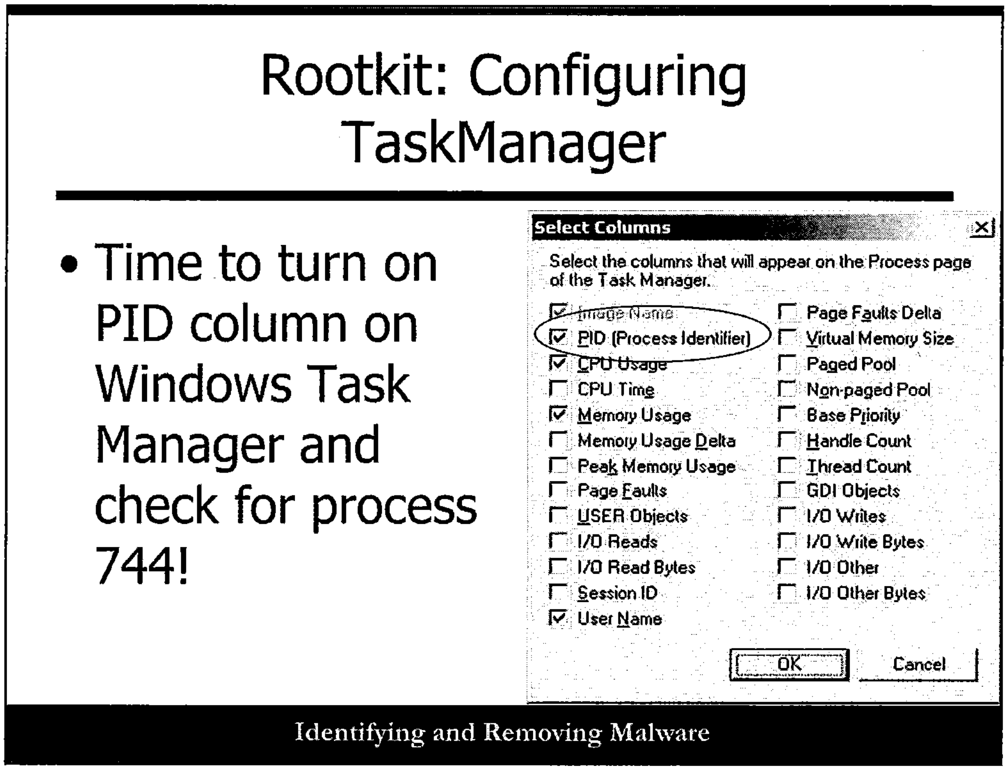
This time, we get at least some suspicious activities.

TCPView shows a bunch of connections initiated by a <non-existent> process, which has a PID of 744 to a remote server on port 80. So how can a non-existent process have a process ID associated with it?

| Process | Protocol | Local Address | Remote Address | State |
|---|---|---|---|---|
| <non-existent>:744 | UDP | Lab-machine:1075 | *:* | |
| <non-existent>:744 | TCP | Lab-machine:1046 | Lab-machine:0 | LISTENING |
| <non-existent>:744 | TCP | lab-machine:1046 | 81.95.151.43:http | SYN_SENT |

| | | | | |
|---|---|---|---|---|
| **lsass.exe:764** | **UDP** | **Lab-machine:isakmp** | *:* | |
| svchost.exe:1044 | TCP | Lab-machine:1025 | Lab-machine:0 | LISTENING |
| svchost.exe:1044 | UDP | Lab-machine:1026 | *:* | |
| svchost.exe:1044 | UDP | Lab-machine:1028 | *:* | |
| svchost.exe:1044 | UDP | Lab-machine:ntp | *:* | |
| svchost.exe:1044 | UDP | lab-machine:ntp | *:* | |
| svchost.exe:1236 | UDP | Lab-machine:1027 | *:* | |
| svchost.exe:1248 | TCP | Lab-machine:5000 | Lab-machine:0 | LISTENING |
| svchost.exe:1248 | UDP | Lab-machine:1900 | *:* | |
| svchost.exe:1248 | UDP | lab-machine:1900 | *:* | |
| svchost.exe:956 | TCP | Lab-machine:epmap | Lab-machine:0 | LISTENING |
| svchost.exe:956 | UDP | Lab-machine:epmap | *:* | |
| System:4 | TCP | Lab-machine:microsoft-ds | Lab-machine:0 | LISTENING |
| System:4 | TCP | lab-machine:netbios-ssn | Lab-machine:0 | LISTENING |
| System:4 | UDP | Lab-machine:microsoft-ds | *:* | |
| System:4 | UDP | lab-machine:netbios-ns | *:* | |
| System:4 | UDP | lab-machine:netbios-dgm | *:* | |

But who is PID 744?




**Rootkit: Configuring TaskManager**

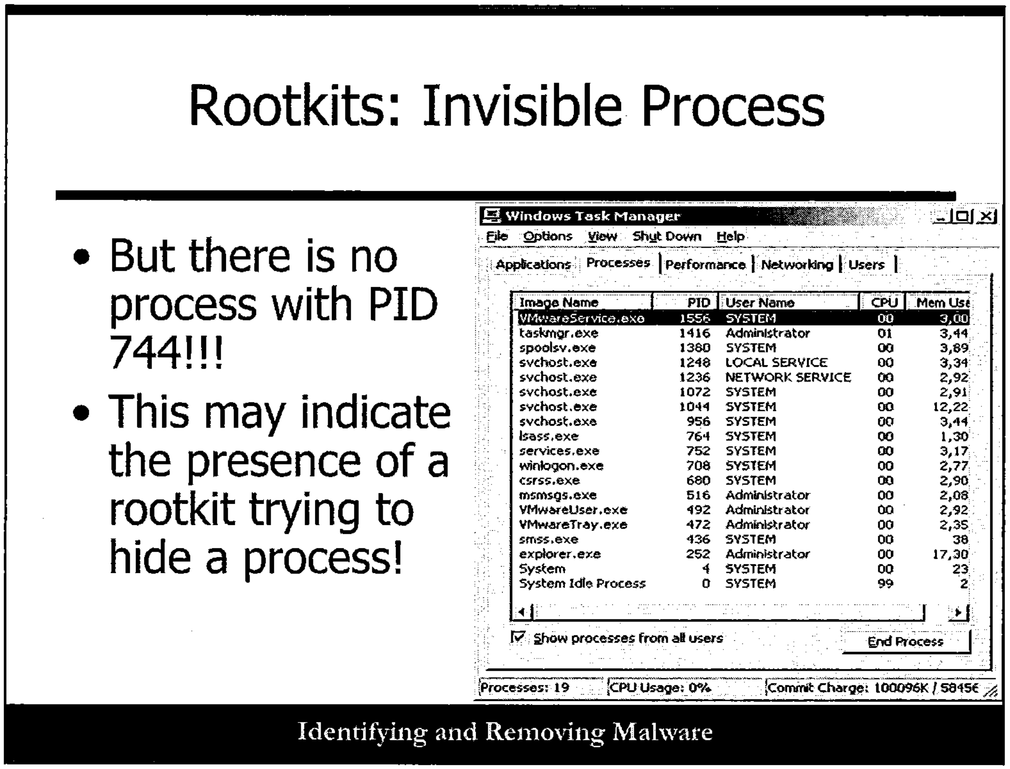
**Windows TaskManager**

By default, Windows Task Manager shows only the following fields on the Process tab:

- Image Name
- User Name
- CPU
- Mem Usage

To see the process ID is important in an attempt to identify a possibly strange process.

To enable the view of Process ID (PID), you need to go to View->Select Columns option on the Task Manager menu and check the PID (Process Identifier) box.




**Rootkits: Invisible Process**

**Windows Task Manager**

After enabling the option to see the PIDs of all processes, we can check again in the list of processes and see if a program is running with a PID of 744.

Unfortunately, there is no process with PID 744. This fact makes it even more suspicious because we know that "something" is running in our machine. We also know that it has a PID associated with it, but we cannot see it on Windows Task Manager.

This can indicate that something is trying to hide this process from us and can imply the presence of a rootkit in our system.

# Identifying and Fighting Rootkits (1)

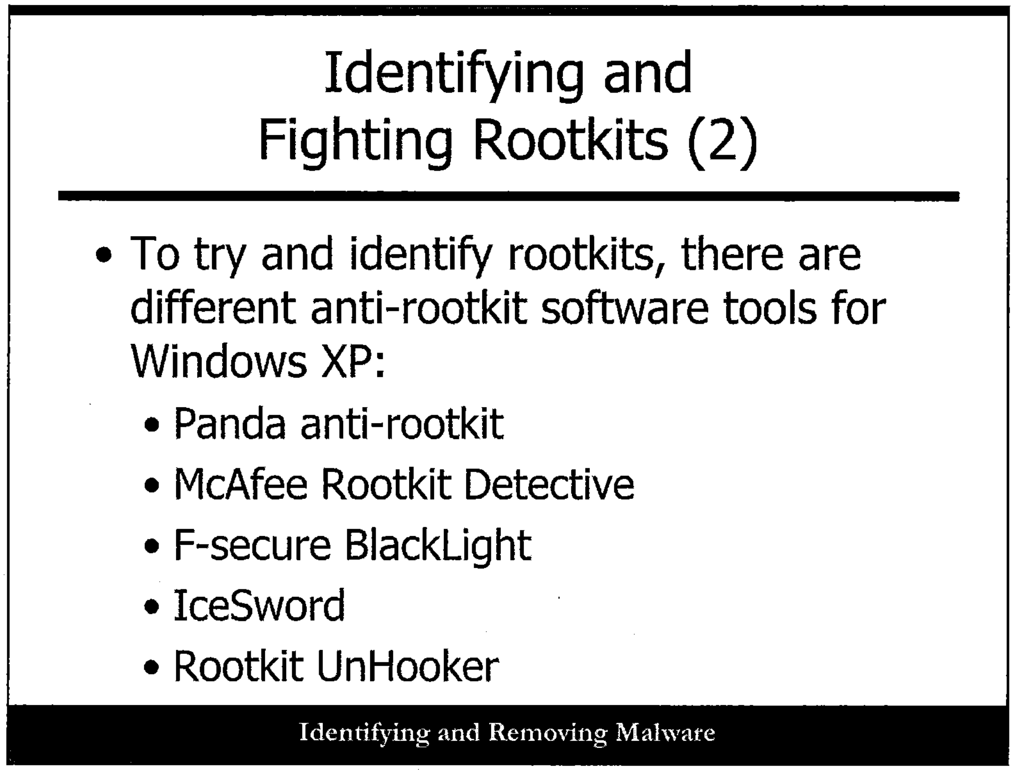
- Summary
  - Process Explorer doesn't show anything suspicious
  - TaskManager doesn't show anything either
  - TCPView shows a suspicious <non-existent> process trying to connect to a remote host with a PID that doesn't "exist"

Identifying and Removing Malware

**Identifying and Fighting Rootkits (1)**

**Summary**
At this point, we already have some interesting information about what could be happening in the machine:

- We could not identify any suspicious process or service using TaskManager.
- We could not identify any suspicious process or service using Process Explorer.
- TCPView shows a suspicious <non-existent> process trying to access a remote host on port 80.
- This <non-existent> process has a PID associated with it.
- Task Manager does not show any process with the same PID as the one found by TCPView.




**Identifying and Fighting Rootkits (2)**

**Anti-Rootkit Tools**

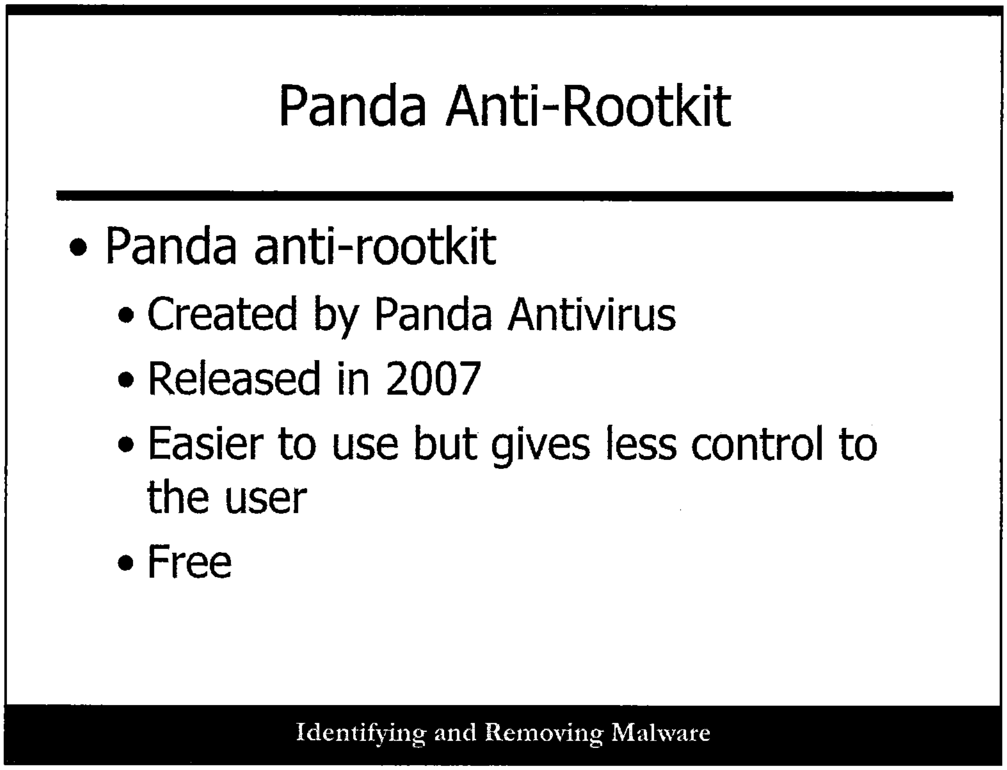
Because we have identified that something is trying to hide activities in our machine, we may believe that it could be a rootkit. Fighting rootkits can be a hard task, but fortunately we have some good and freely available external tools to help with this task.

In this step, you learn how to use five different anti-rootkit software tools to help us identify possible rootkits on Windows XP systems.

These tools are:

- Panda anti-rootkit
- McAfee Rootkit Detective
- F-Secure BlackLight
- IceSword
- Rootkit UnHooker

One great advantage of these programs is you don't have to install them on the computer; you just run them.



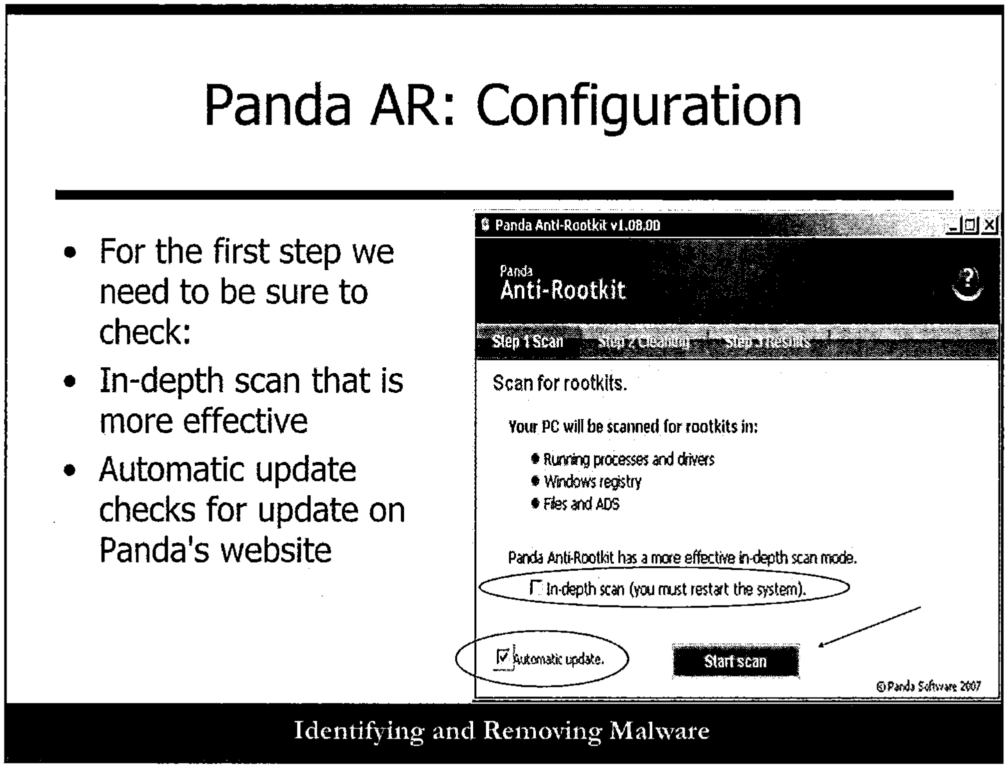

**Panda Anti-Rootkit**

The Panda anti-rootkit software was developed by the Spanish Antivirus vendor Panda Security.

It was released in 2007, and while a good product at the time, it had a problem. When it detected a rootkit, and didn't know which one it was, it would not remove it. Later versions fixed that, and now it can remove all rootkits, both known and unknown.

The Panda anti-rootkit is one of the easiest to use and is quite informative about the actions it will take. However, it gives less control to the user when tuning for extra functionality. It is available to anyone for free and can be downloaded at http://acs.pandasoftware.com/marketing/promo/en/antirootkit.exe.




**Panda AR: Configuration**

**Panda Anti-Rootkit**

After downloading the Panda anti-rootkit software, it is easy to get started with it. By just double-clicking the program icon and accepting the license agreement, it opens a window. Here, you have two options to select before starting the scan on the system to look for rootkits:

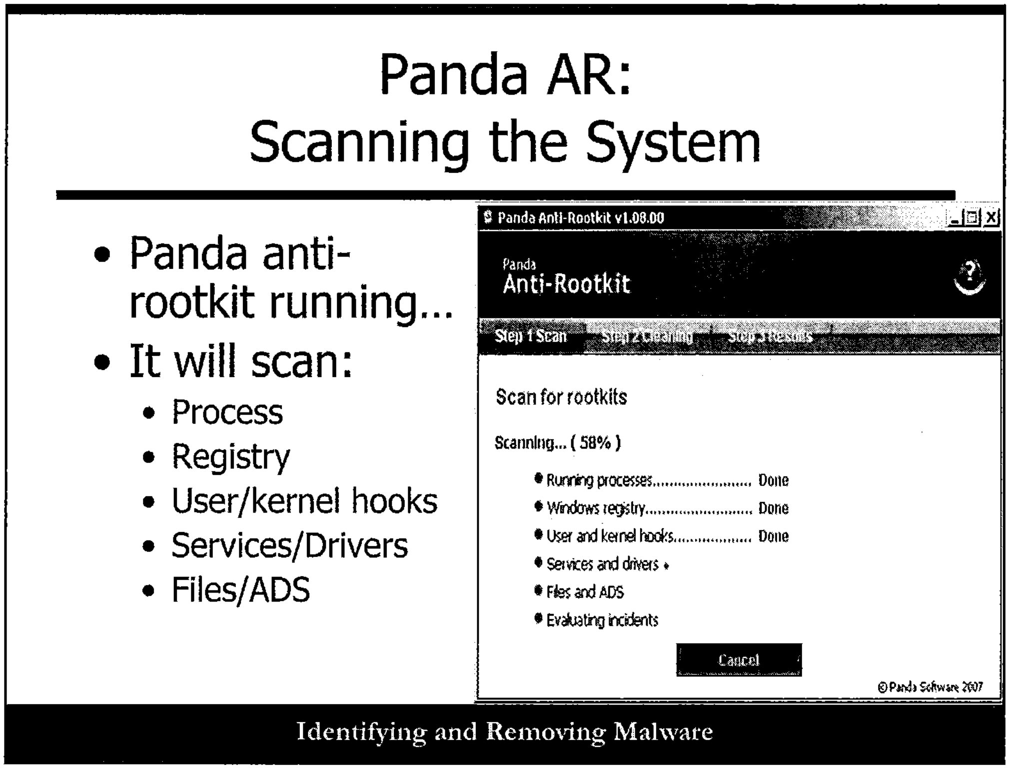
- Check the box for an in-depth scan.

  When enabling this option it use a more in-depth approach. It has the disadvantage of having to restart the computer if you check it. Right after the restart the scan will start. The in-depth mode allows Panda software to control the computer so that the presence of a rootkit will not impede the detection and removal process. That is why the computer restart is needed.

- Enable automatic update.

  This is recommended if your machine is connected to the Internet because it goes to the Panda website and looks for product updates such as additional new rootkits signatures.

In our example, we will not check the box for an in-depth scan.

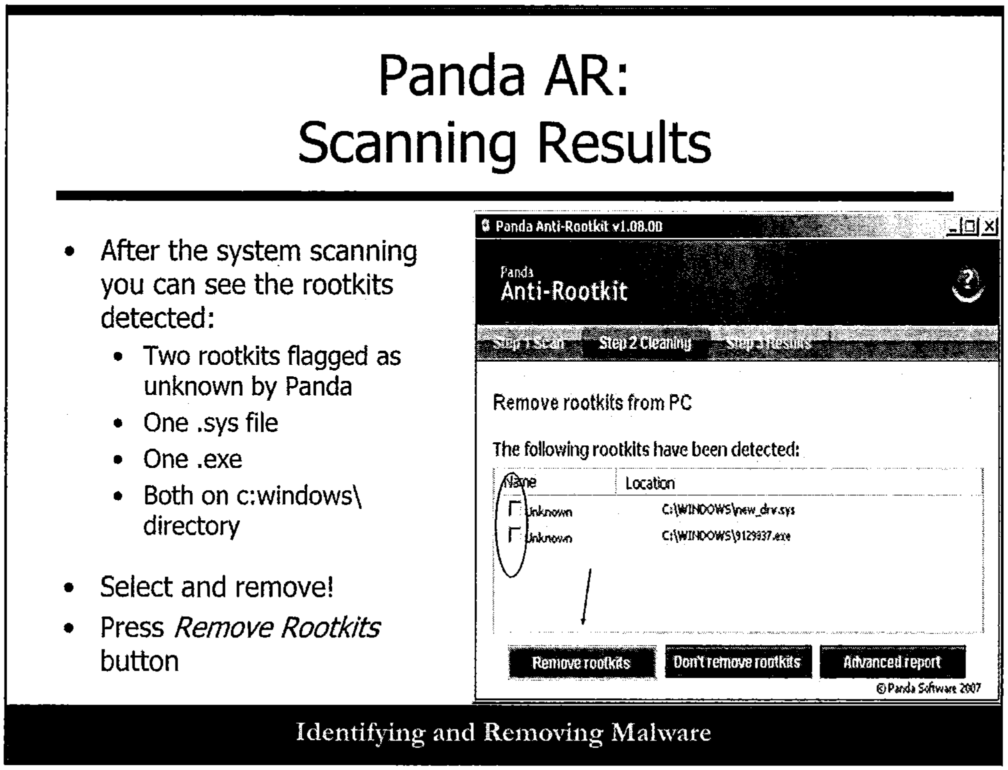



**Panda AR: Scanning the System**

**Panda Anti-Rootkit**
The Panda anti-rootkit starts as soon as we press the Start Scan button.

Using either the regular or the in-depth option, it will scan:

- Running processes
- Windows Registry
- User and Kernel hooks (for detecting user mode and kernel mode rootkits)
- Services and drivers
- Files and ADS (Alternate Data Streams)
- Check the system for things that it believes to be rootkit-related




**Panda AR: Scanning Results**

**Panda Anti-Rootkit**

When the system scan is over, it shows you a report. In our case it displayed a screen indicating that some rootkits were detected. Because it has a database of known rootkits, it also tries to give the name of the rootkits. If it is something that it is not in their database, it presents the rootkit as unknown.

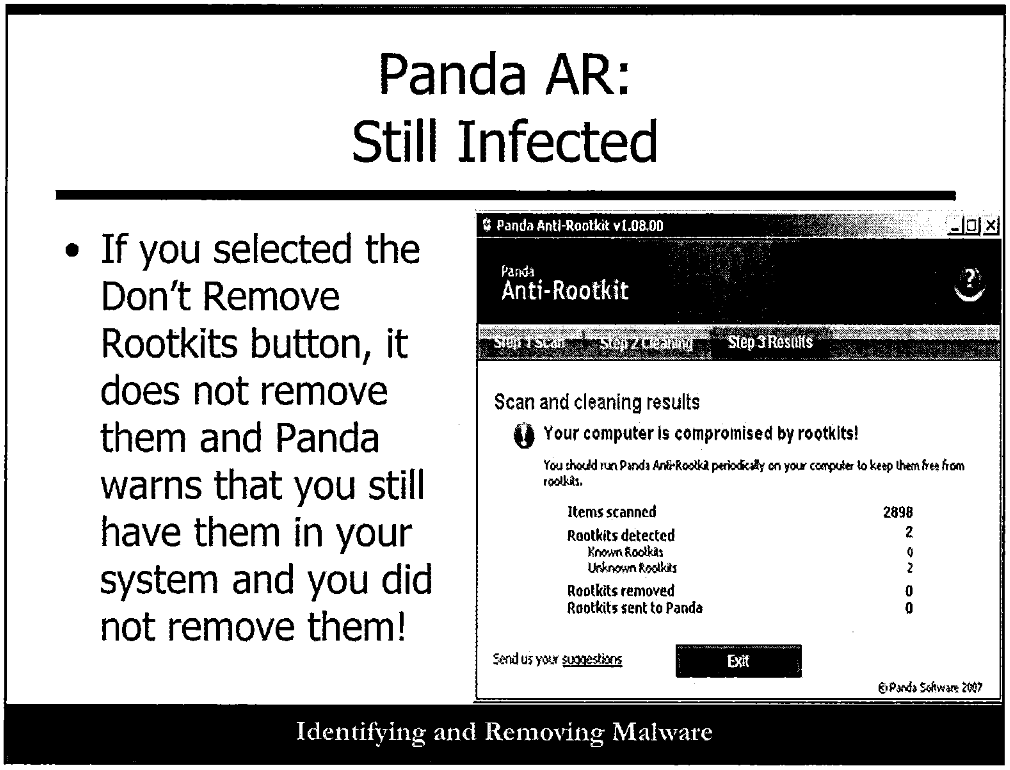
From our case, it detected:

C:\windows\new_drv.sys
C:\windows\9129837.exe

So, we have one .sys and one .exe file, and both are in the Windows directory.

Because Panda identified them as rootkits, we should remove them from our system, and it is pretty easy to do so:

- Select the boxes of the presented rootkits.
- Click the Remove Rootkits button.




**Panda AR: Still Infected**

**Panda Anti-Rootkit**

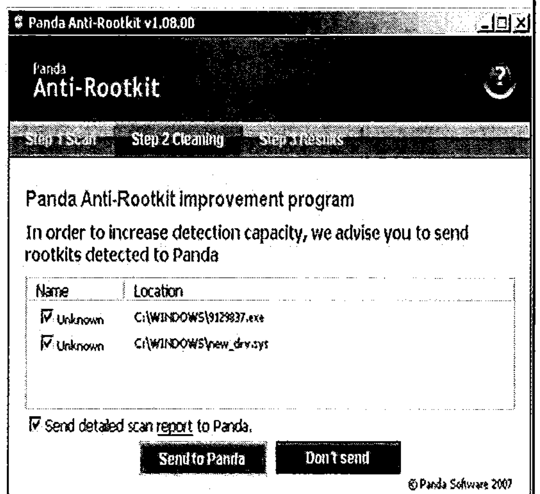
While looking for signs of system compromise and the presence of malicious software installed on the computer, you may not want to modify the system in any way. You may need to find out if something is, in fact, wrong with the system, yet still need to preserve the computer in its original state to allow for appropriate forensic examinations.

So, if you run the Panda anti-rootkit, and find some rootkits, but you don't want to remove them from the system, you can select the Don't Remove Rootkits button.

After you select the Don't Remove Rootkits button, Panda presents another screen warning that you are still infected with some rootkits and that you didn't remove them.

# Panda AR:
# Submitting the Sample

- After checking the rootkit components to be removed, you can also select to send the information to Panda. Panda anti-rootkit improvement program is optional



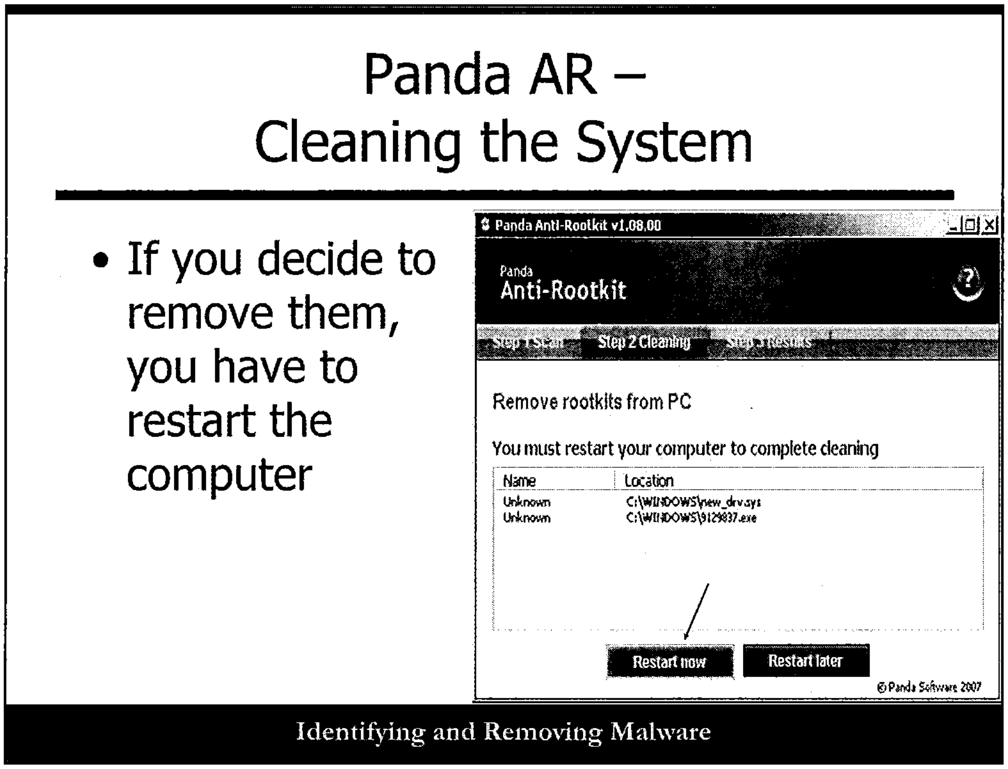

Identifying and Removing Malware

**Panda AR: Submitting the Sample**

**Panda Anti-Rootkit**

After we check the rootkits and click the Remove Rootkits button, we will be presented with another screen. This one asks if we want to send the detected rootkits to Panda so that it can improve its database of known rootkits; this is optional. If you decide to share your findings with Panda, just click the Send to Panda button. If you don't want to share the information with Panda, click the Don't send button.

Note that not sending the samples to Panda does not prevent you from continuing to use the program to remove rootkits.

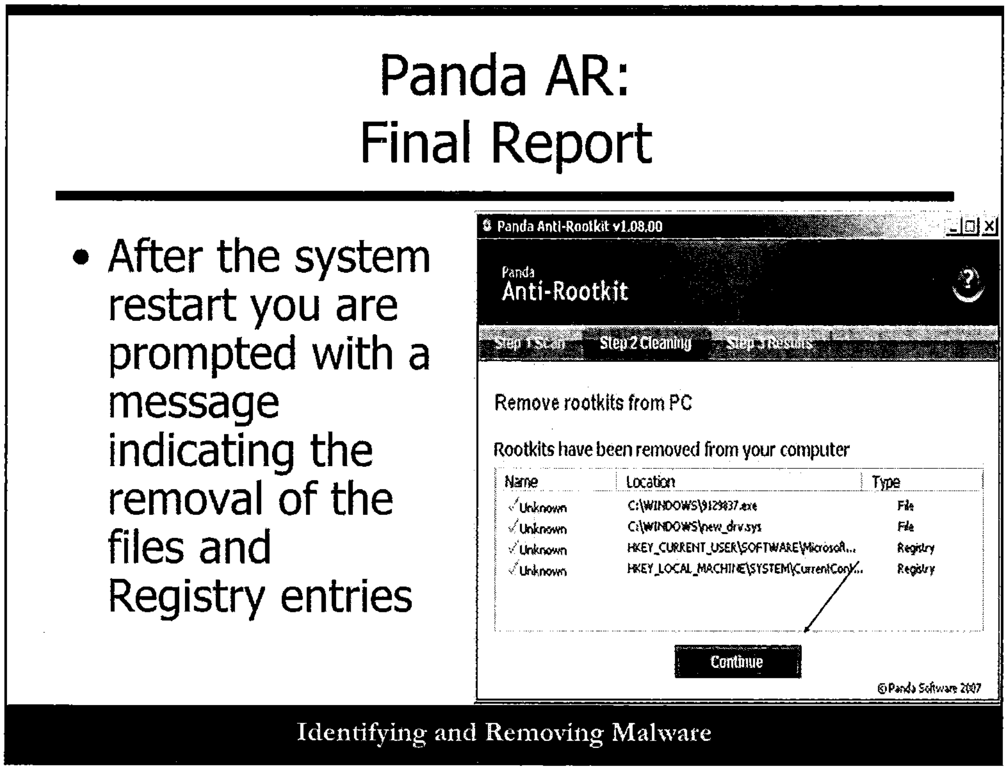



**Panda AR: Cleaning the System**

**Panda Anti-Rootkit**

Upon discovery of the rootkit, a screen appears indicating the presence of the rootkits discovered. We were given the option to remove them and to send the samples to Panda. Either way, we will be presented with another window that shows the rootkit components we selected for removal, and it asks us to restart the computer so that it can complete the cleaning process.

At this point we have the option to restart the computer right away by pressing the Restart Now button, or delay the restart by pressing the Restart Later button. It is strongly recommended that we restart the computer as soon as we find the rootkits. The restart removes the rootkit and prevents the rootkit software from continuing its malicious activities.




**Panda AR: Final Report**

**Panda Anti-Rootkit**

When our system reboots and we log in again, we will be presented with a screen displaying a message that the rootkits have been removed from our computer.

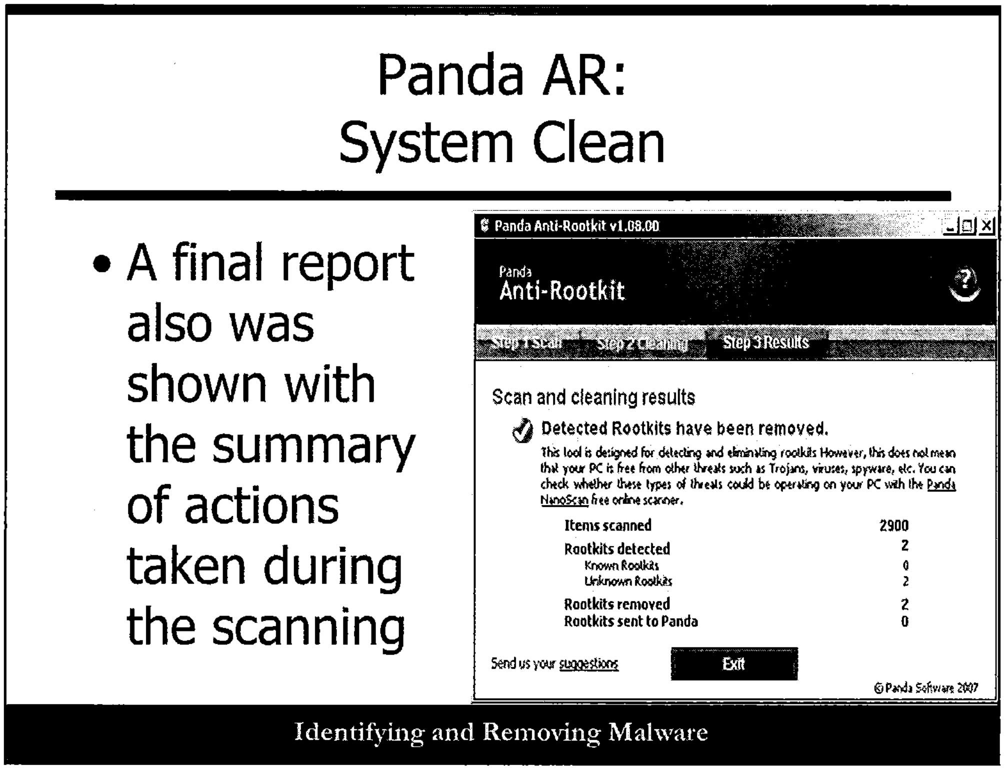
It also shows which files and Registry entries were removed from the system:

- The files:

  C:\WINDOWS\new_drv.sys
  C:\WINDOWS\9129837.exe

- The Registry keys and values:

  SYSTEM\CurrentControlSet\Services\new_drv "ImagePath";
  SOFTWARE\Microsoft\Windows\CurrentVersion\Run "ttool"



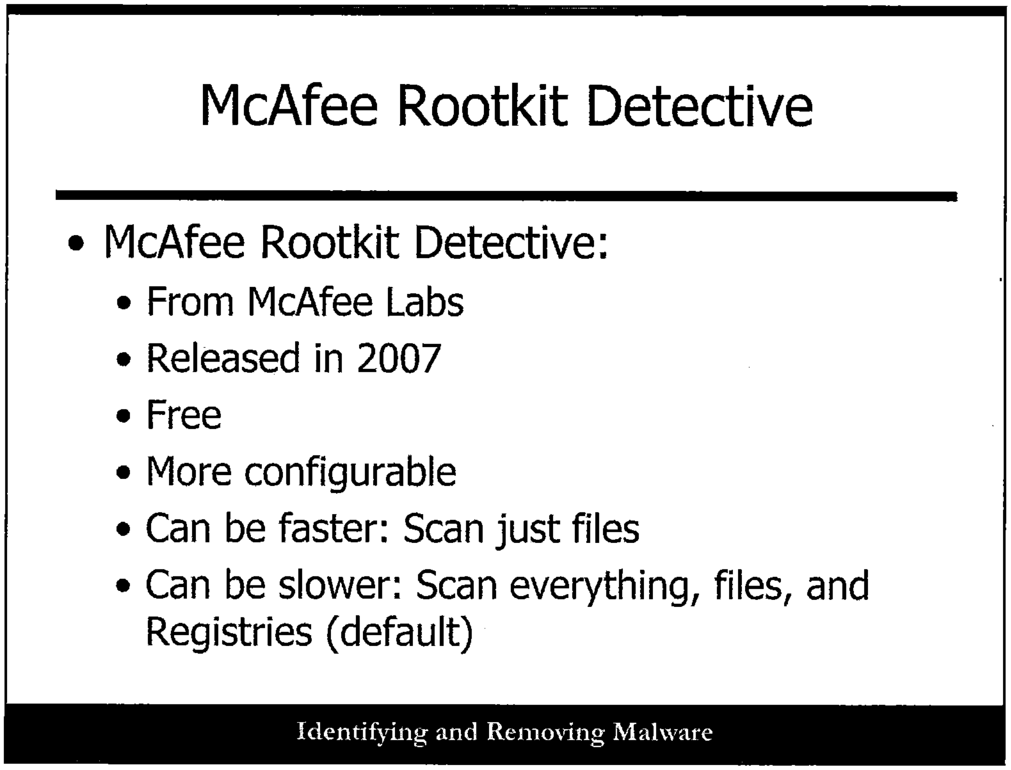

**Panda AR: System Clean**

**Panda Anti-Rootkit**

After clicking the Continue button from the last screen, we will be presented with a final report. The report specifies all the actions performed by the anti-rootkit program:

| | |
|---|---|
| The number of items scanned: | 2900 |
| The number of rootkits detected: | 2 |
| Known rootkits: | 0 |
| Unknown rootkits: | 2 |
| Rootkits removed: | 2 |
| Rootkits sent to Panda: | 0 |

After this we can safely click the Exit button because our system is now free from rootkits!




**McAfee Rootkit Detective**

The McAfee Rootkit Detective anti-rootkit application was developed by the McAfee Labs and was released in 2007. As with most anti-rootkit applications it is also freely available to the general public and can be downloaded at http://download.nai.com/products/tools/foundstone/mcafeerootkitdetective.zip.

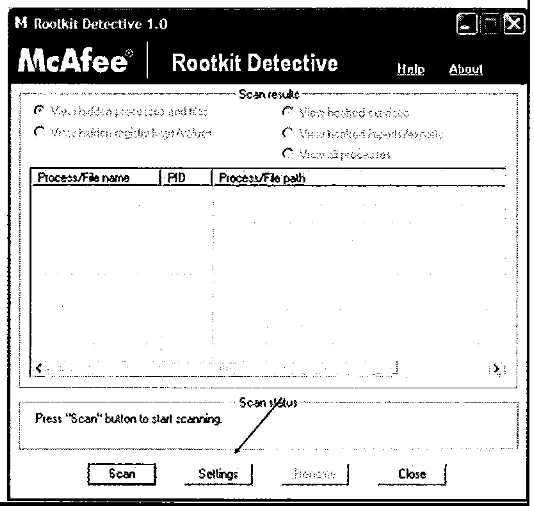
The McAfee program gives you more control over what the application should or should not do. McAfee has an option to access its settings. Because of this option it is more configurable, making it faster or slower depending of the configuration adopted.

In our example, we use the default configuration.

Please note that McAfee recently released a command-line version of the tool, focused only on ZeroAccess and TDSS rootkits, called rootkitremover, that can be downloaded at http://www.mcafee.com/us/downloads/free-tools/rootkitremover.aspx.

## McAfee Detective: Configuration (1)

- On the main screen of Rootkit Detective, you can choose to do a System scan or check the settings
- The settings page defines if you want it faster or slower



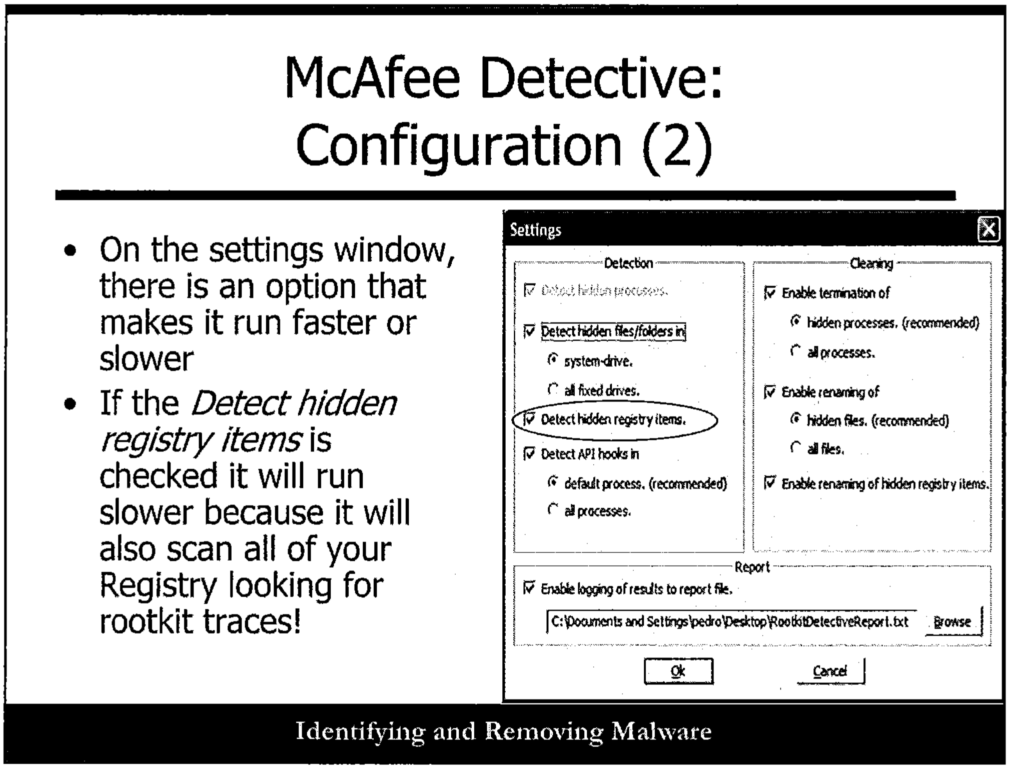

Identifying and Removing Malware

**McAfee Detective: Configuration (1)**

**McAfee Rootkit Detective**

When starting McAfee Rootkit Detective, you can see the main window where you either start the scan right away by clicking the Scan button or you check and define its settings.

Right now we will check the settings by clicking the Settings button.



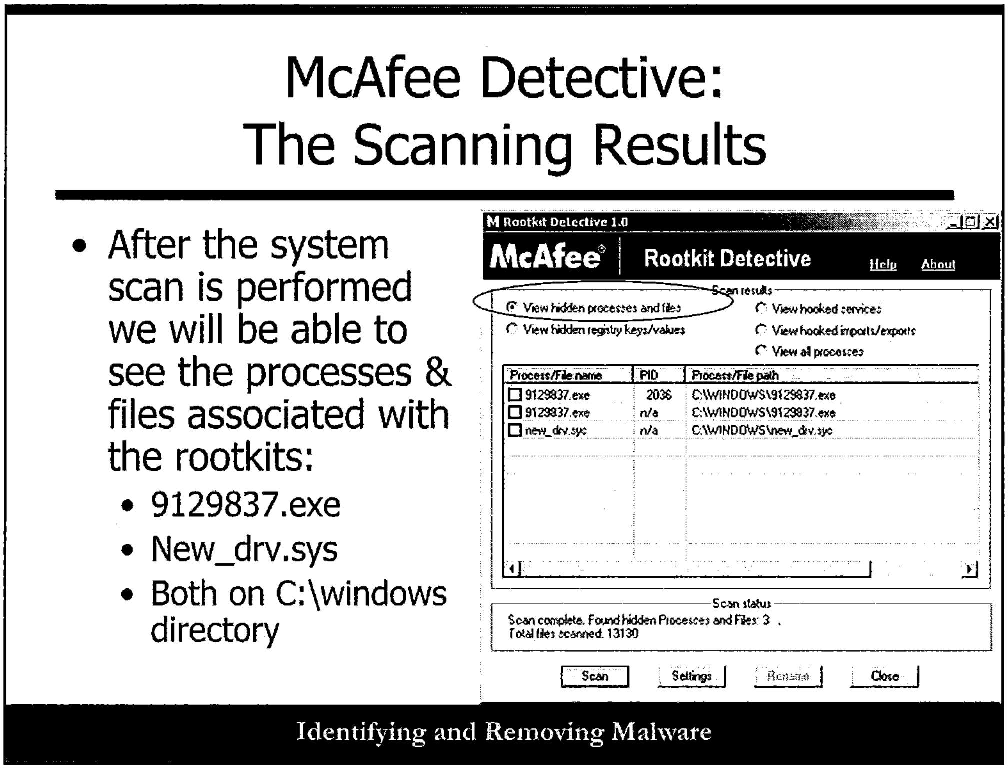

**McAfee Detective: Configuration (2)**

**McAfee Rootkit Detective**

Because we decided to click the Settings button, we will be presented with the configuration screen. This screen has some options that you can select that define the way it will:

- Detect (scan the system to try to identify possible rootkits)
- Clean (how it will remove the malicious processes)
- Report (the logging file)

One option in particular can make it perform better; it is the Detect hidden Registry items in the detection section. By default it is checked and will scan the Registry looking for, as the name indicates, hidden Registry items. In some cases it will make the software perform slower than usual but it is safer to leave it checked because it will run a more in-depth scan.




**McAfee Detective: The Scanning Results**

**McAfee Rootkit Detective**

As soon as the scan completes, it returns to the main screen. Here you can see the results of the scan and additional information.

The regular report shows the hidden process and files:

C:\WINDOWS\9129837.exe
C:\WINDOWS\new_drv.sys

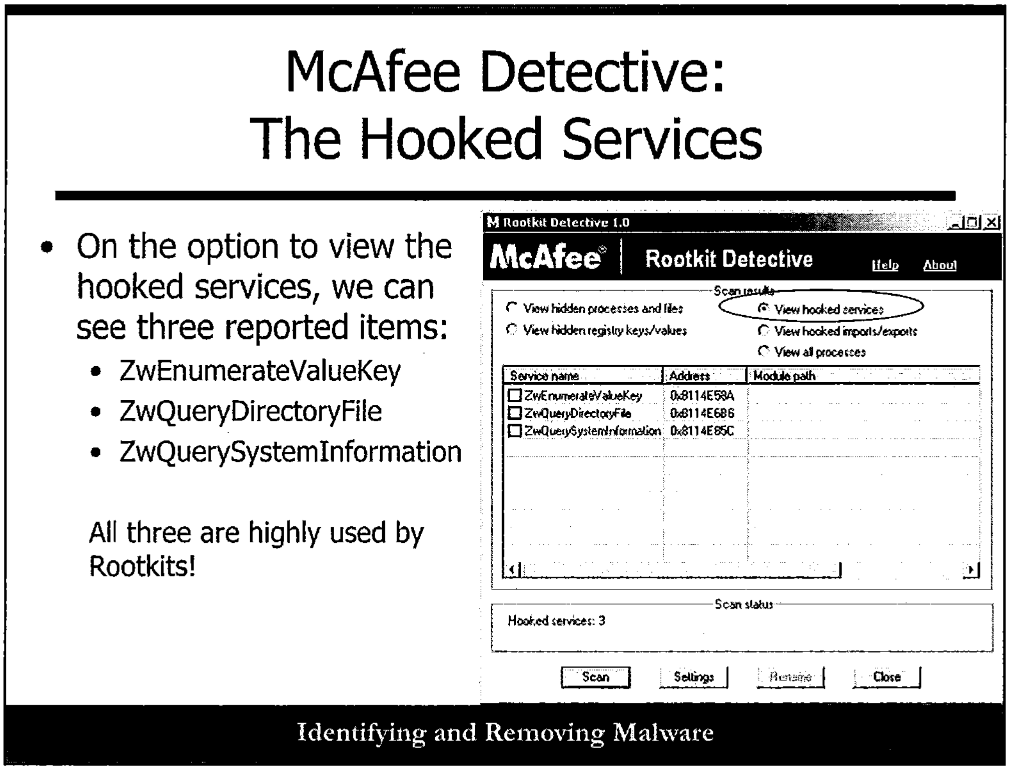
You can also select other options provided by the program:

- **View hidden processes and files**: This is the default view.
- **View hidden Registry keys/values**: Use this to see the Registry related to the rootkit.
- **View the hooked services**: Use this to see the type of hooks used by the rootkit.
- **View hooked imports/exports:** Use this to see the import and exported resources.

The log generated gives even more information about the files and processes that are hidden:

- **Object-Type**: Process
- **Object-Name**: 9129837.exe
- **Pid**: 2006
- **Object-Path**: C:\WINDOWS\9129837.exe
- **Status**: Hidden

Object-Type: File/Folder
Object-Name: new_drv.sys
Pid: n/a
Object-Path: C:\WINDOWS\new_drv.sys
Status: Hidden




**McAfee Detective: The Hooked Services**

**McAfee Rootkit Detective**

Looking at the scan results, we found two rootkit components, so we already know that our machine is infected with rootkits. We can continue with the process of cleaning or try to get more information about them. Another nice source of information is the option to see the hooked services, which we will check.

Clicking the View hooked services, we can see three hooked services:

- ZwEnumerateValueKey
- ZwQueryDirectoryFile
- ZwQuerySystemInformation

By just checking the function names, we cannot tell if Zw* functions are kernel mode functions. This may indicate that the rootkit that is installed in our machine is a kernel mode rootkit. There could be user mode applications that call Zw* functions in the same way that kernel mode applications call Zw* functions. With the function names alone, it is not possible to determine whether we are dealing with a kernel mode or user mode rootkit.

So how can we get more information about the kind of rootkit that is installed in our machine?

According to the log generated by McAfee Rootkit Detective:

Object-Type: SSDT-hook
Object-Name: ZwEnumerateValueKey

Object-Type: SSDT-hook

Object-Name: ZwQueryDirectoryFile (More information about it can be found at https://msdn.microsoft.com/en-us/library/windows/hardware/ff567047.)

Object-Type: SSDT-hook

Object-Name: ZwQuerySystemInformation

This means that these functions are of the SSDT-hook object type. The System Service Descriptor Table (SSDT) is a kernel structure that has all the addresses of all system function calls. If the rootkit can modify this table, it will have the power to redirect the execution to another piece of code. This code then can do whatever it wants, such as removing itself from a process enumeration request so that it will not be easily detected.

## McAfee Detective: Checking the Processes (1)

- Another nice option from McAfee Rootkit Detective is the TaskManager style tool:
  - The View All Processes option

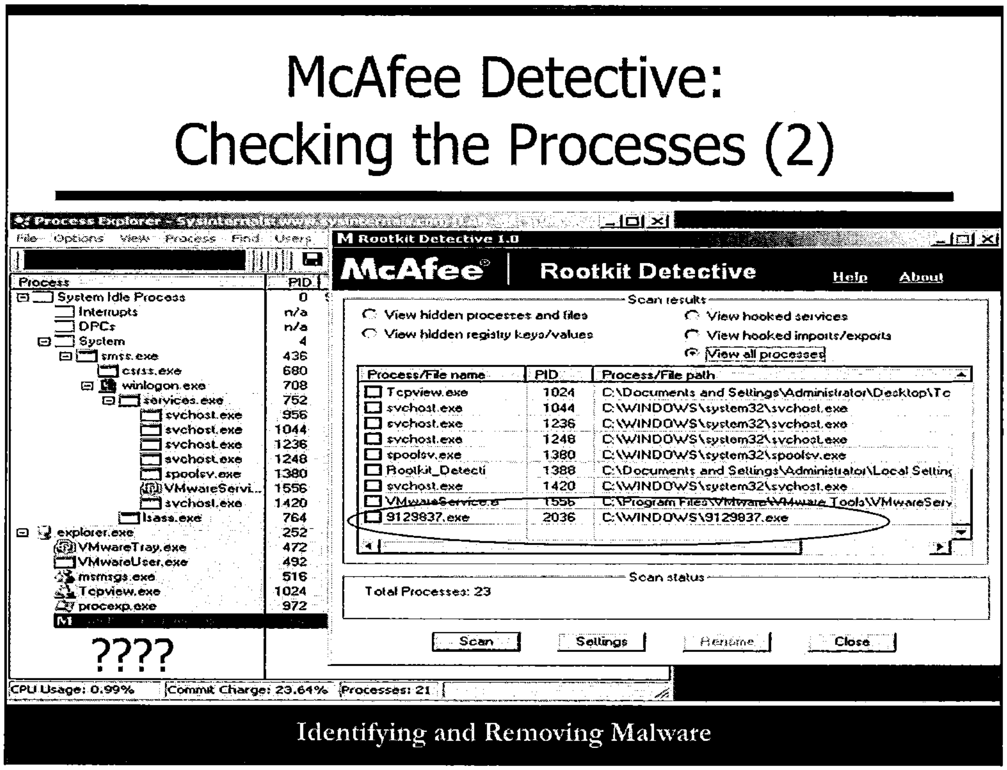
It can reveal processes that are not visible to either Windows TaskManager or Process Explorer

Identifying and Removing Malware

**McAfee Detective: Checking the Processes (1)**

**McAfee Rootkit Detective**

The lack of information regarding the process that is hidden by the rootkit is really frustrating. Tools such as Windows Task Manager and SysInternals Process Explorer will not show the process to us. Another nice option from the McAfee product is a Task Manager-like tool, which can be accessed through the option View all Processes.




**McAfee Detective: Checking the Processes (2)**

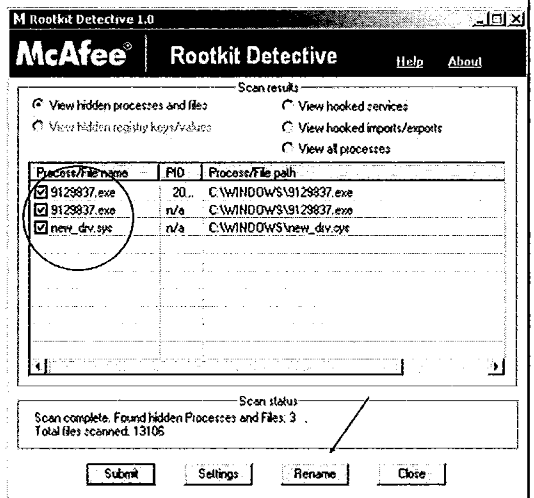
**McAfee Rootkit Detective**

When you click the option View All Processes, you can see a list of the running processes and services on the machine.

This time, you can see the process **9129837.exe**, previously identified as a rootkit by the McAfee application. In the same window, you can see the Process Explorer window, which does NOT show this process.

# McAfee Detective: Cleaning the System

- Now that we know the rootkit components it is time to get rid of them
- To accomplish this we have to mark the rootkit components and click on the Rename button
- This will rename them, restart the system, and save the files for you




Identifying and Removing Malware

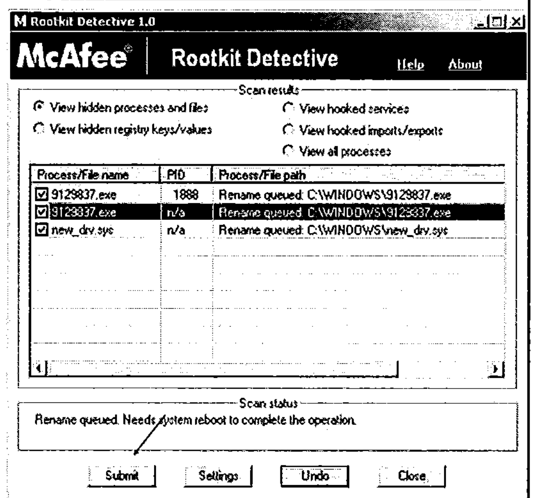
**McAfee Detective: Cleaning the System**

**McAfee Rootkit Detective**

After we got all the information regarding the rootkit, it is time to start the cleaning process. Instead of having a Remove Rootkit button, McAfee Detective has a Rename button. This means we have to check the rootkit components that we want to get rid of and then click the Rename button. In this way, McAfee Detective does not delete the files. Instead, when you restart the computer they will not be active but will still be in the same directories with a .ren (from renamed) extension. This allows you to share it with security companies or save them for more in-depth research.

# McAfee Detective: Submitting the Suspicious Samples (1)

- Now that we have selected the files, we also have the option to submit them to McAfee AvertLabs so that it can research and add into its database
- Just click the Submit button

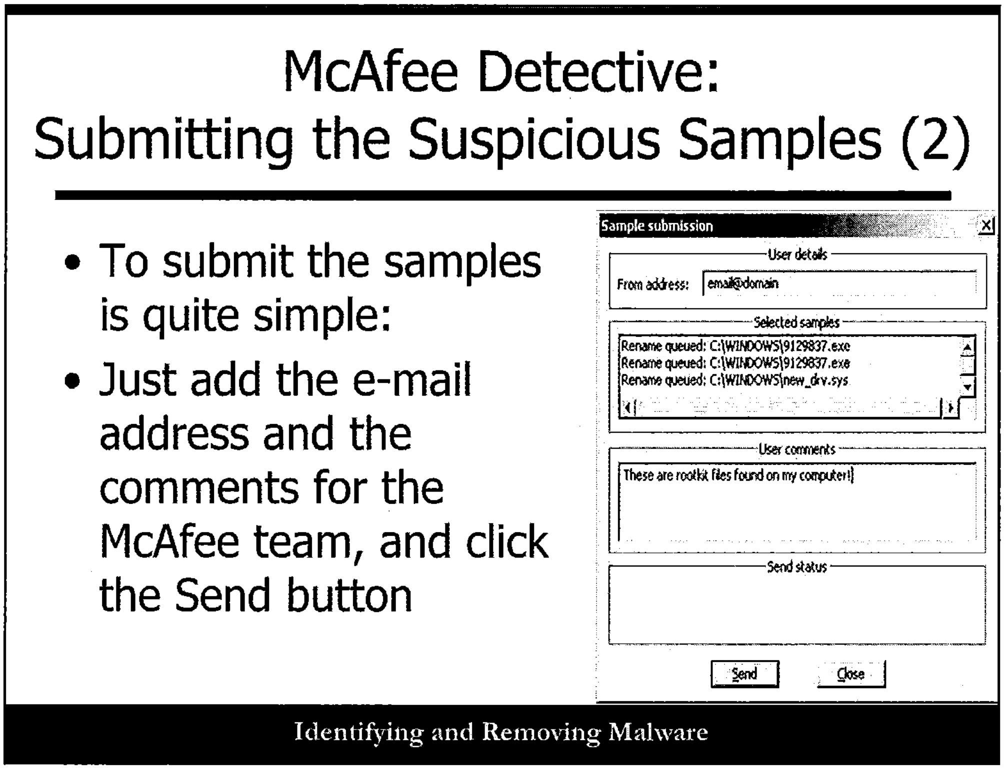



Identifying and Removing Malware

**McAfee Detective: Submitting the Suspicious Samples (1)**

**McAfee Rootkit Detective**

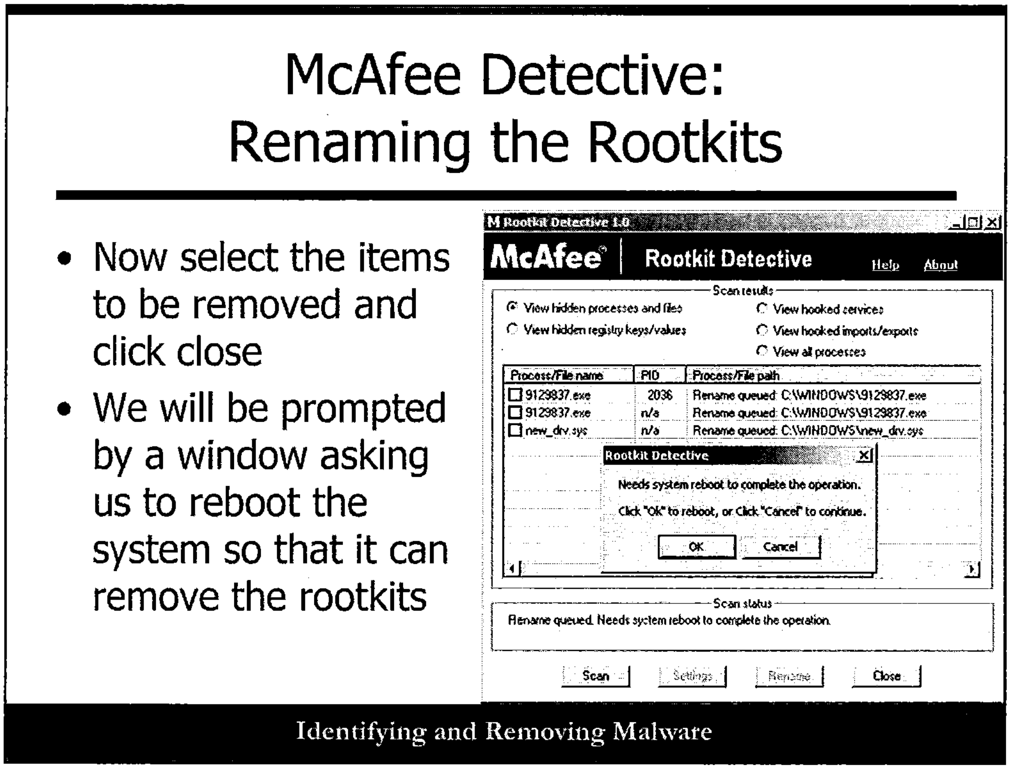
As with many anti-rootkit applications, we can submit the rootkit components to McAfee AvertLabs, so it can research and add it to its database. To do so we just need to click the Submit button.




**McAfee Detective: Submitting the Suspicious Samples (2)**

**McAfee Rootkit Detective**

When we click the Submit button, we are presented with another window where we can fill in some information, such as our e-mail address. (This enables you to receive a response from McAfee about the files sent.) Also fill in any additional information that you think could be useful for the researchers, such as which behavior you noticed. In our case, we could include that it was a hidden file and had network connections. Then we can just click the Send button to submit the information to McAfee.




**McAfee Detective: Renaming the Rootkits**

**McAfee Rootkit Detective**

We already decided to remove the malware from our machine, so we have to check the components and click the Rename button. A pop-up window asks if we want to reboot the system now, by clicking the OK button, or later by clicking the Cancel button.

As usual, unless we have a reason to keep the computer with the rootkits installed, we are strongly advised to reboot it right away to remove them from our system.

# F-Secure BlackLight: Rootkit Eliminator

- The first functional anti-rootkit
- Released in 2005 as Beta
- Faster, but scan has less options ...
- Free
- Provided as Legacy only, to Windows XP

Identifying and Removing Malware

**F-Secure BlackLight: Rootkit Eliminator**

The Finnish antivirus company, F-Secure, was one of the original innovators of anti-rootkit software. In 2005, it released the first beta version of its anti-rootkit product called F-Secure BlackLight (Rootkit Eliminator). It was one of the first functional anti-rootkit programs!

As with most anti-rootkit software, it is also free and publicly available at their website at ftp://ftp.f-secure.com/anti-virus/tools/fsbl.exe.

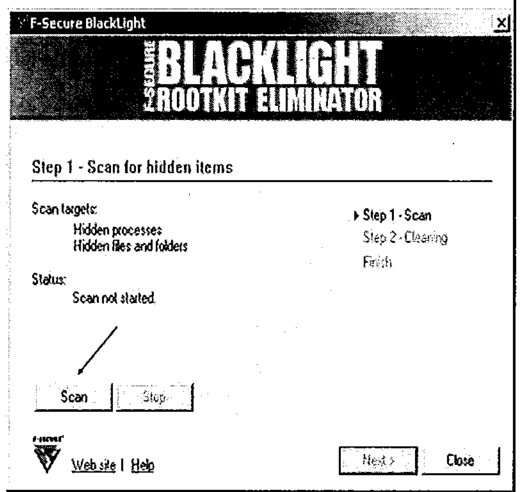
Although free, it has an annoying expiration date. Every once in a while, you have to go to its website and download a new version with a new expiration date.

As with some other anti-rootkit products, it doesn't offer many options to the user to configure it. Another characteristic of this product is that it is quite fast when compared to other products. The increased speed is because they don't do Registry scanning.

# F-Secure BlackLight: Scanning the System

- The F-Secure Blacklight has a simple interface and doesn't offer many options

- Faster, but it scans only for files, not for Registry entries



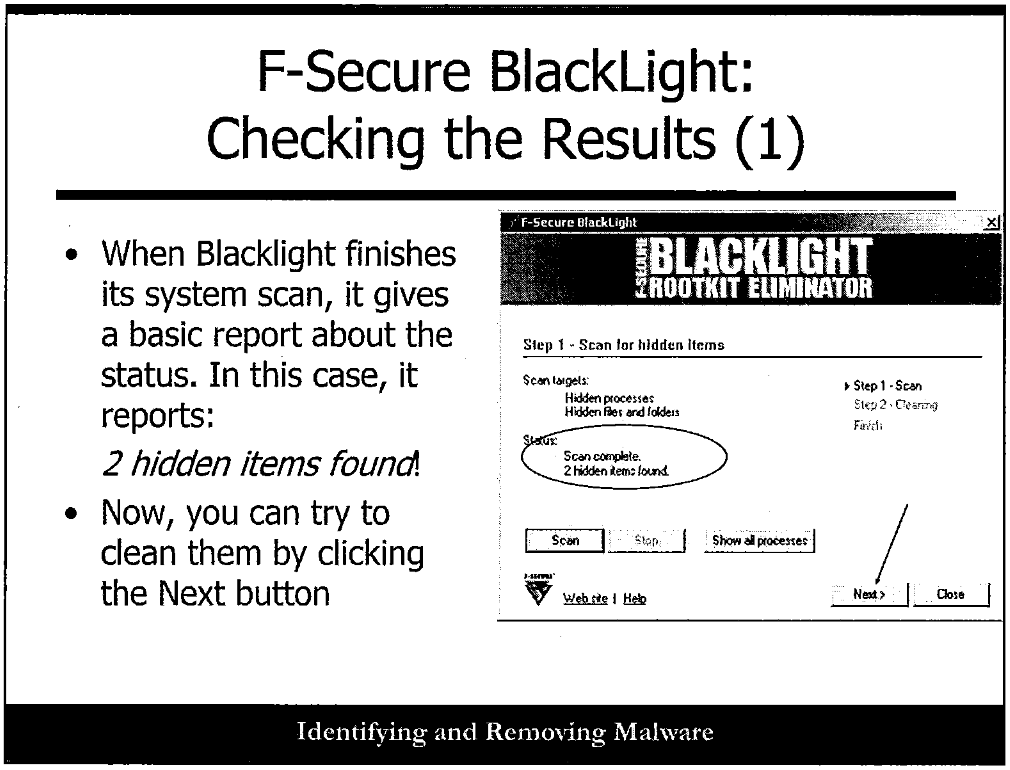

Identifying and Removing Malware

**F-Secure BlackLight: Scanning the System**

After we accept the license agreement from F-Secure, we will be prompted with the product main interface that is quite clean and simple. We basically just have two options:

Click Scan button to start the system scan.
Click Close button to exit.

Because we want to search our computer for the presence of a rootkit, we click the Scan button to continue.

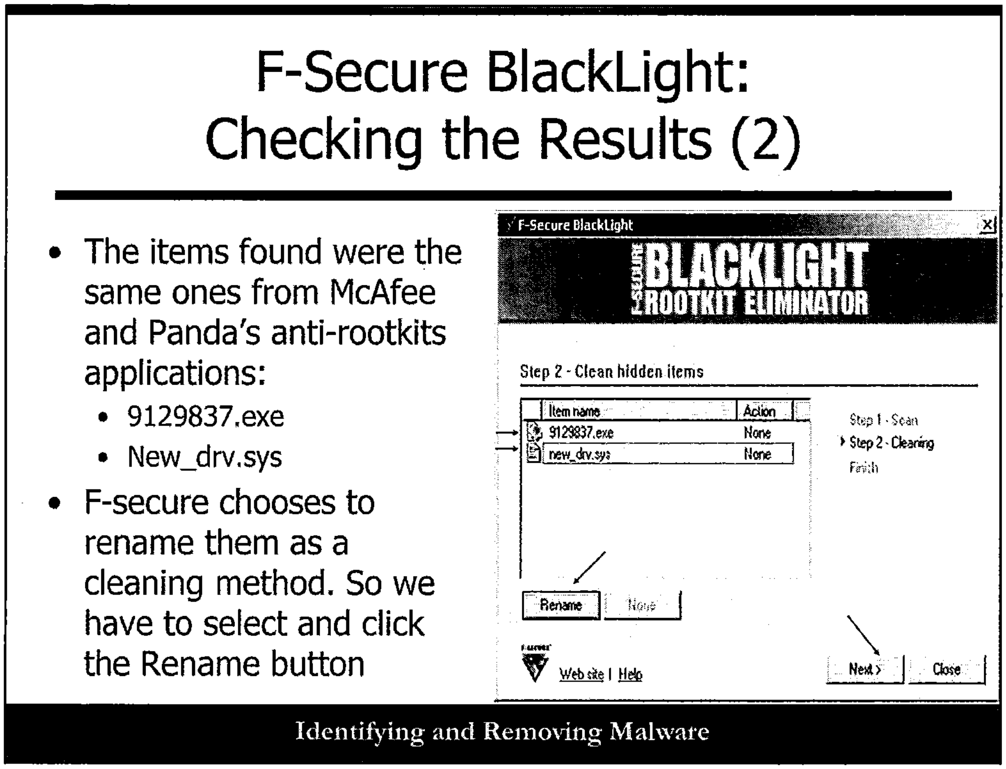



**F-Secure BlackLight: Checking the Results (1)**

When F-Secure Blacklight finishes the system scan, it goes directly to the report screen where it shows the status:

Scan complete
2 hidden items found

Now that we are sure our computer has two hidden items, it is time to start the cleaning process by clicking the Next button.




**F-Secure BlackLight: Checking the Results (2)**

The cleaning method adopted by F-Secure is the same used by McAfee Rootkit Detective. It renames the files after a reboot so that it deactivates the rootkit but keeps the files so that you can share them or research them deeper.

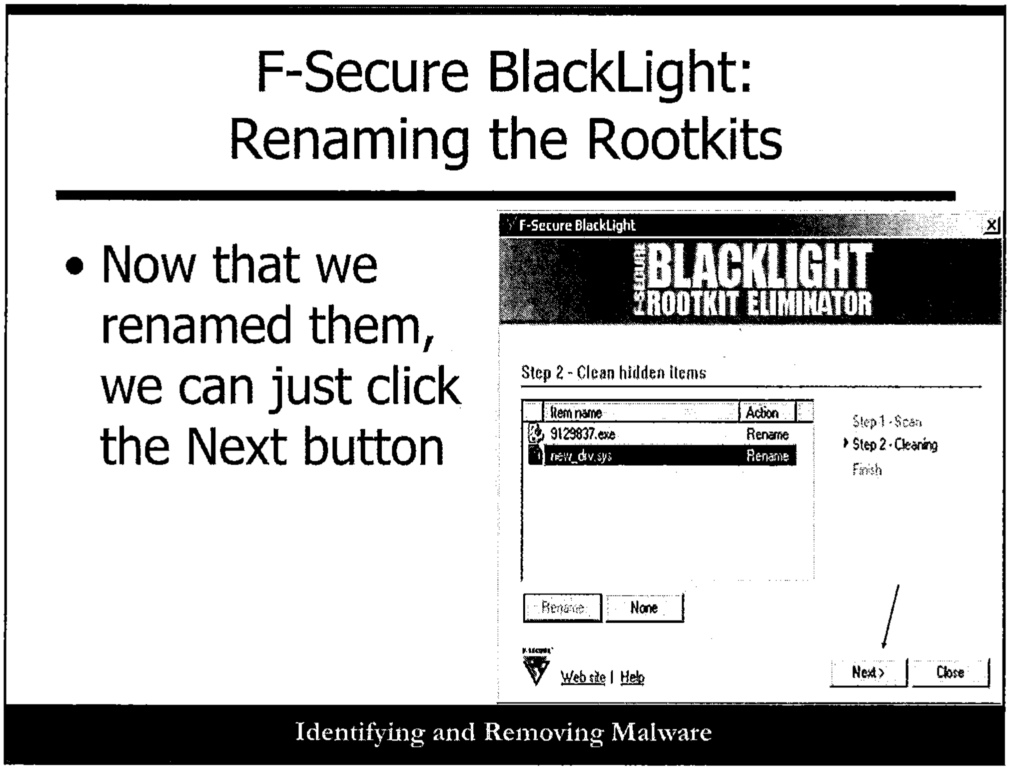
F-Secure Blacklight found the same two files as Panda and McAfee:

- C:\WINDOWS\9129837.exe
- C:\WINDOWS\new_drv.sys

As you can see from the log file:

08/17/07 11:53:45 [Info]: Hidden process: C:\WINDOWS\9129837.exe
08/17/07 11:53:52 [Info]: Hidden file: C:\WINDOWS\9129837.exe
08/17/07 11:53:52 [Info]: Hidden file: c:\WINDOWS\new_drv.sys

So we have to select the files and click the Rename button.



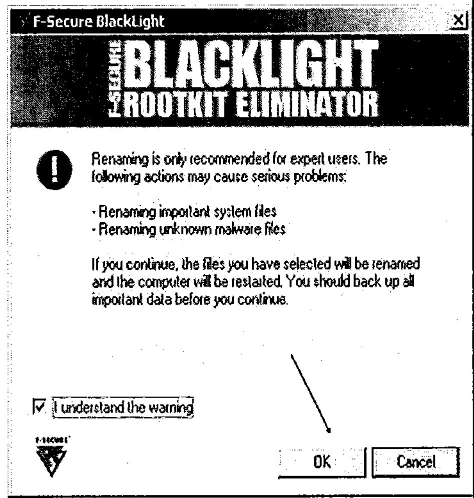

**F-Secure Blacklight: Renaming the Rootkits**

Note the rootkit components now show the word **Rename** in the action column.

The last step of the F-Secure BlackLight cleaning procedure after renaming the files is to continue by clicking the Next button. This reboots the system to clean up the rootkit files and processes.

## F-Secure BlackLight: Renaming the Rootkits (2)

- Accept F-Secure's warning about the procedure
- Click OK to restart the computer
- Files are renamed to make them unusable




Identifying and Removing Malware

**F-Secure BlackLight: Renaming the Rootkits (2)**

Before F-Secure BlackLight starts the shutdown process, it prompts with a last warning and asks for confirmation that you understand the warning. To continue we have to check the box I Understand the Warning, and then click the OK button.

The reason for this warning is that any application using a rootkit technique will be renamed, making the application unusable.

## Anti-Rootkits: Advanced Tools

- The tools used so far are great for fast detection of Rootkits
- However, they offer little/no option for more in-depth check
- IceSword and Rootkit UnHooker give plenty of information and actionable options

Identifying and Removing Malware

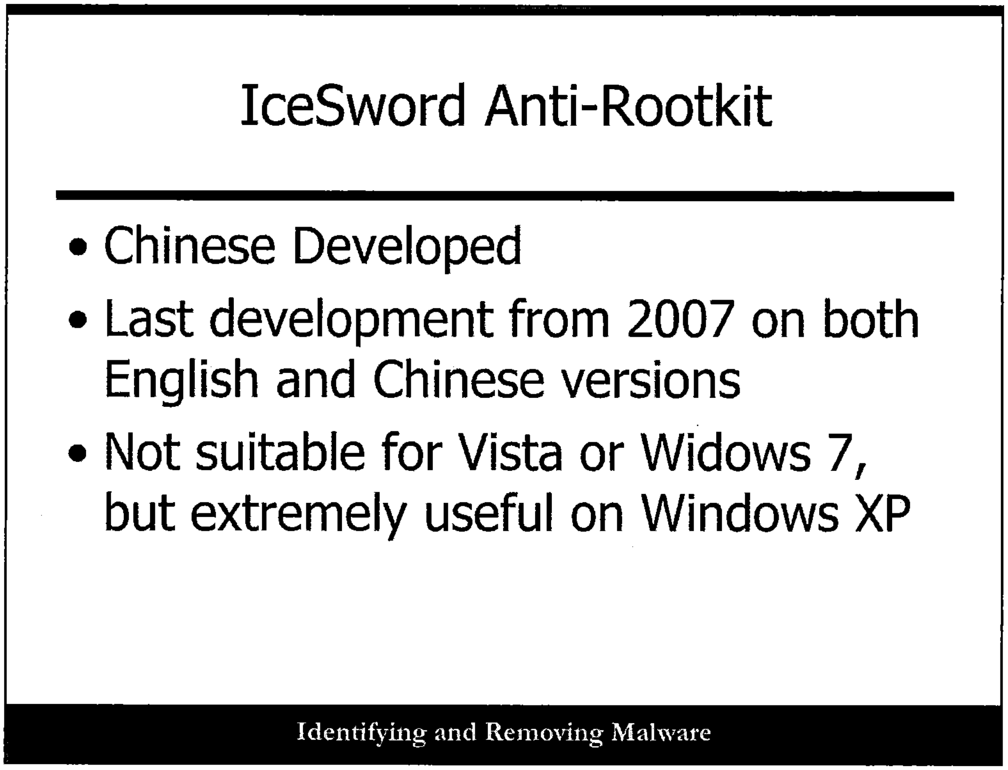
**Anti-Rootkits: Advanced Tools**

The Panda, McAfee, and F-Secure anti-rootkit tools are great tools, but they are restrictive about what they can do. They are basically point-and-shoot rootkit scanners. The McAfee tool still offers more options, such as renaming the files hidden by the rootkits, but that's it.

Sometimes, you need additional options when trying to identify and remove malware on the machine.

On the following slides, you will be introduced to some basic usage of two tools that offers more control on what you can do when you suspect you have a rootkit on the machine.

These are powerful tools that should be handled carefully to avoid system crashes.

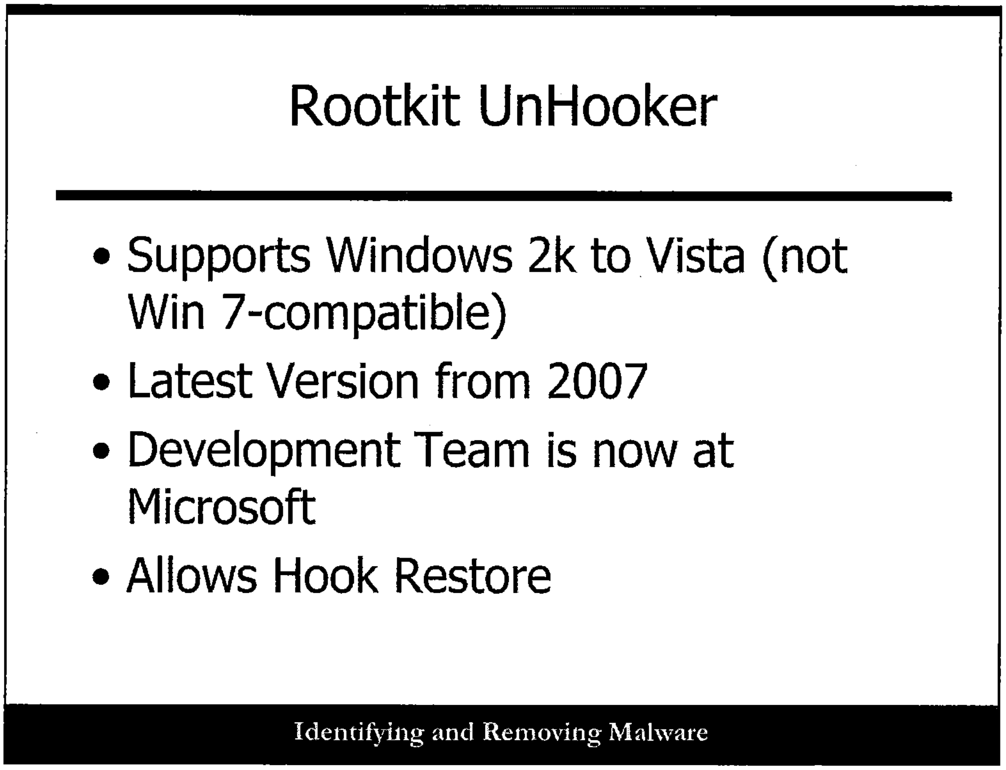



**IceSword Anti-Rootkit**

The IceSword tool is a powerful tool that enables you to inspect

- Kernel Modules
- BHO
- SPI
- SSDT
- Scan Modules
- Explorer-like view of files, even files hidden by rootkits

It can be downloaded at http://www.antirootkit.com/software/IceSword.htm.




**Rootkit UnHooker**

Like various anti-rootkit tools, the Rootkit Unhooker was developed by a group of users that are not publicly known.

The latest version is 3.7.300.509, which added support to Vista OS in 2007. The latest news about the development group is that it moved to Microsoft and no longer supports it. However, it is still one of the best anti-rootkit tools available.

From the website, the features described are:

- SSDT Hooks Detection and Restoring
- Shadow SSDT Hooks Detection and Restoring
- Hidden Processes Detection/Terminating/Dumping
- Hidden Drivers Detection and Dumping
- Hidden Files Detection/Copying/Deleting
- Code Hooks Detection and Restoring
- Report Generation

It can be downloaded at http://www.antirootkit.com/software/RootKit-Unhooker.htm.

## Advanced Rootkits and Anti-Rootkits

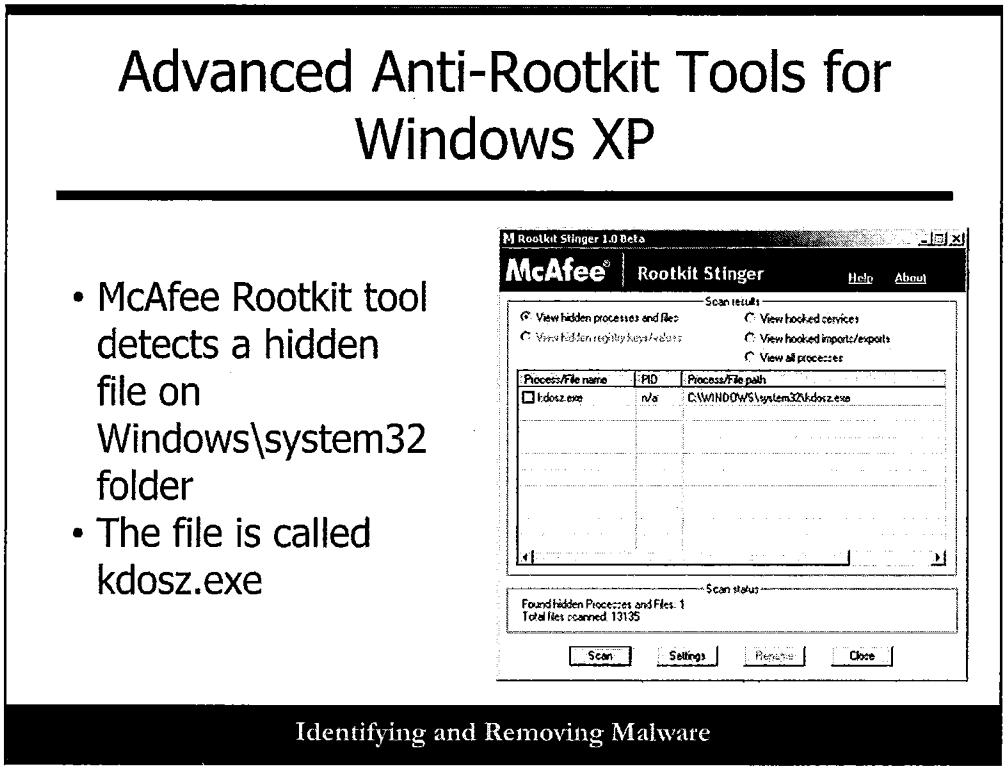
### Windows XP: Examples

Identifying and Removing Malware

Although our training material is based on Windows 7, we decided to include this subsection of tools specifically for Windows XP. The reason, as explained before, is that there is still a large user base of Windows XP in both the corporate and end-user world.

The following slides contain tools that are needed to fight rootkits on Windows XP systems, but don't work on Windows 7. Although we find few examples of rootkits that work on Windows 7, the same applies for the anti-rootkit tools. Most of the tools from antivirus and security companies will not work under Windows 7 and 8.

If you want to practice these examples on a Windows XP system, we included the file badkits2.zip in the Part 7 folder that you can use later.




**Advanced Anti-Rootkit Tools for Windows XP**

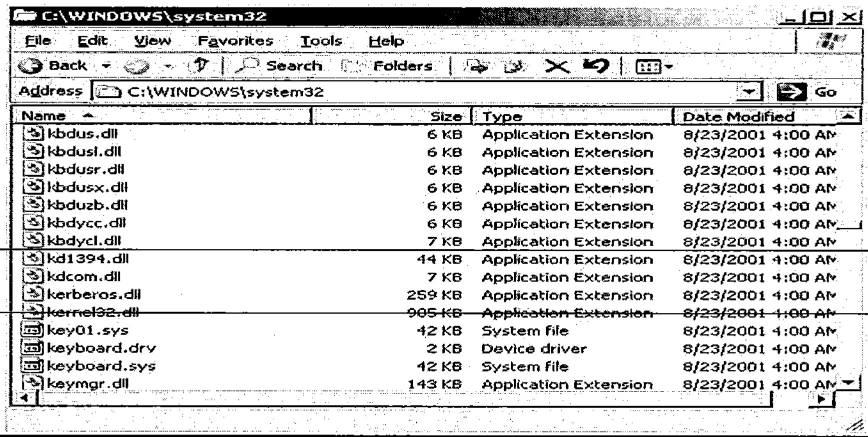
When we run the file, we can first run the McAfee tool to check the results. In this case, it shows that there is a hidden file on the Windows\System32 folder called kdosz.exe.

Because the malware uses a random name every time it runs, you may notice a different filename in your exercise.

Now, let's confirm it uses Windows Explorer.

# Advanced Anti-Rootkit Tools: Using Windows Explorer

The file is hidden by the rootkit and **not** viewable on Explorer




Identifying and Removing Malware

**Advanced Anti-Rootkit Tools: Using Windows Explorer**

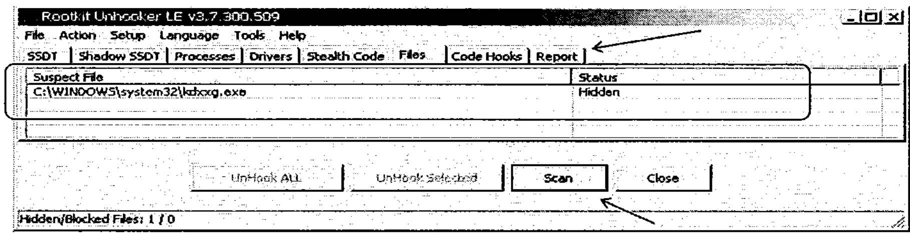
As you can see on this slide, there is no file called kdosz.exe on our Windows\System32 folder because it is hidden by the rootkit.

For this lab, you have to check in the Windows\System32 folder for the filename that was detected with the McAfee tool because the name will change.

Now, let's check Rootkit UnHooker and see what we can do.

# Advanced Anti-Rootkit Tools: Rootkit UnHooker

Opening Rootkit UnHooker and going to the File tab and selecting SCAN shows our hidden file.




Going to the "Report" tab and pressing the Scan button lets you scan all options.

Identifying and Removing Malware

**Advanced Anti-Rootkit Tools: Rootkit UnHooker**

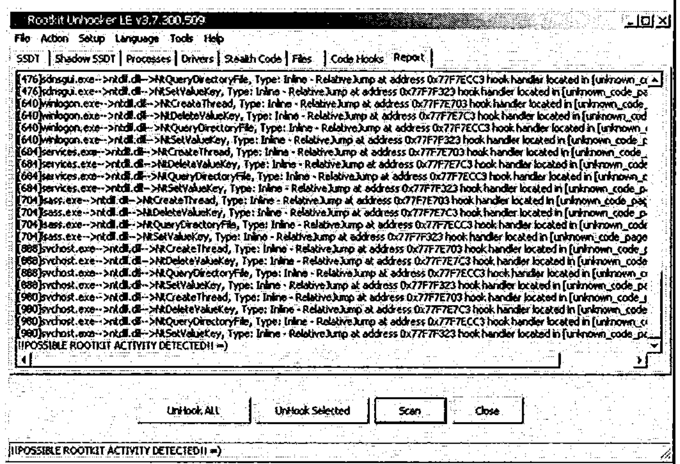
When we open Rootkit UnHooker, we can go to the File tab and ask for a Scan.

The result reveals the "suspect file" (the executable under the C:\Windows\system32\ folder) and the status, in this case Hidden.

Instead of going to each tab for a Scan, we can now go to the Report and ask for a scan to reveal a more complete view of the system.

## Advanced Anti-Rootkit Tools: Rootkit UnHooker (2)

- On the report tab, it is possible to run a scan
- The report shows a warning about rootkit infection
- Also, shows the hooks made by the rootkit to hide the file




Identifying and Removing Malware

**Advanced Anti-Rootkit Tools: Rootkit UnHooker (2)**

The Report tab is useful to have a broad view of the system, and in the end it may even warn on what it suspects. In our case, after the scan it shows the hidden file and all Hooks that it found.

The warning is also clear: POSSIBLE ROOTKIT ACTIVITY DETECTED.

The functions for hooked are basically the following four:

- NtQueryDirectoryFile
- NtSetValueKey
- NtCreateThread
- NtDeleteValueKey

The hooks are always the same on the report, in most of the running process. In this case, it is fairly safe to assume the consequences to force the unhook, using the option Code Hooks.

Advanced Anti-Rootkit Tools: Rootkit UnHooker (3)

- To UnHook the functions that prevent us from seeing the malware, we have to:
  - Go to the Code Hooks tab
  - Scan again
  - Select UnHook ALL button

Identifying and Removing Malware

**Advanced Anti-Rootkit Tools: Rootkit UnHooker (3)**

On the Report tab, it was possible to see the hooks that were preventing us from seeing the malware on Windows Explorer.

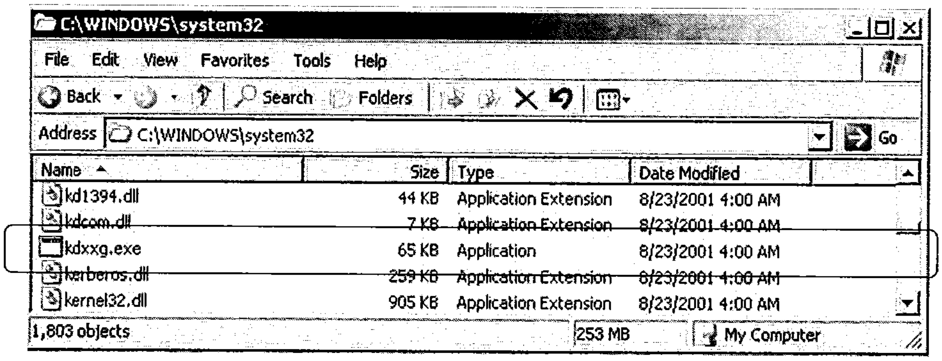
Now, we can UnHook them. To do this, we go to the Code Hooks tab, and click the Scan button again.

After it is done with the scan, we can simply click the UnHook ALL button because in this case all hooks are related to the Rootkit. There may be some cases in which you may go and manually select the hooks where you want to do the Unhook.

When we click the Unhook button, we will be warned that in some cases, when you unhook a function, the system may become unstable and you may get a BSOD (the infamous Blue Screen of Death).

# Advanced Anti-Rootkit Tools: Rootkit UnHooker (4)

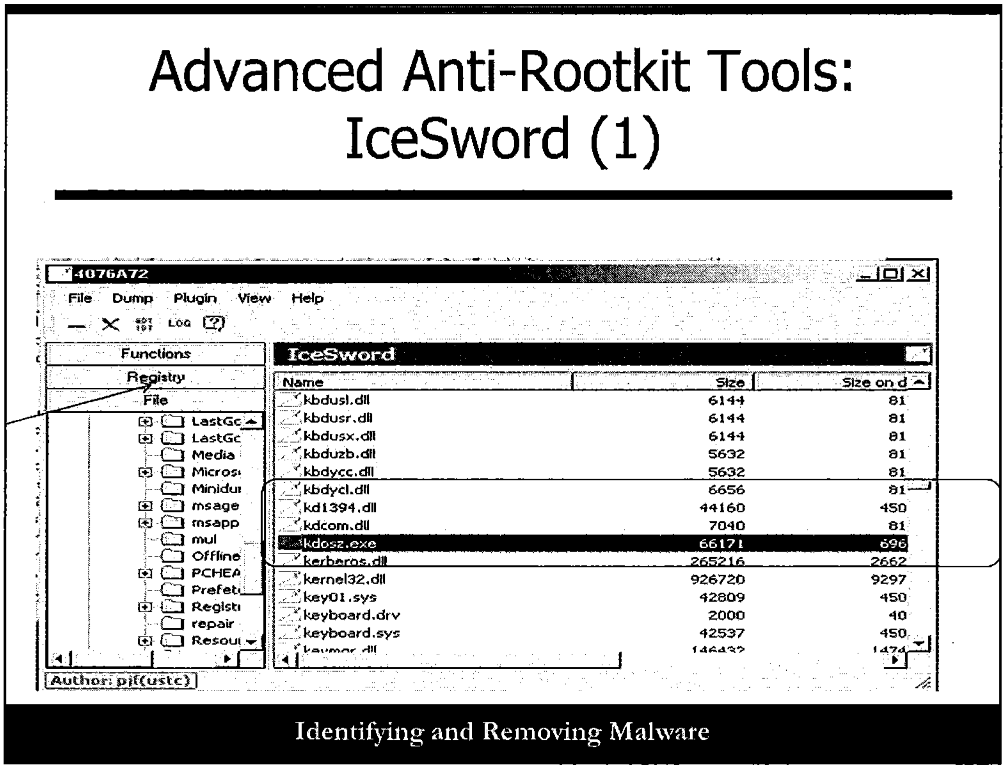
After the UnHook, we can now see our hidden file on Explorer!




Identifying and Removing Malware

**Advanced Anti-Rootkit Tools: Rootkit UnHooker (4)**

After the UnHook, if we go back to Windows Explorer, we have a nice surprise. Go to Tools and select Refresh. We can now see the file(s); this previously was only possible with other tools!

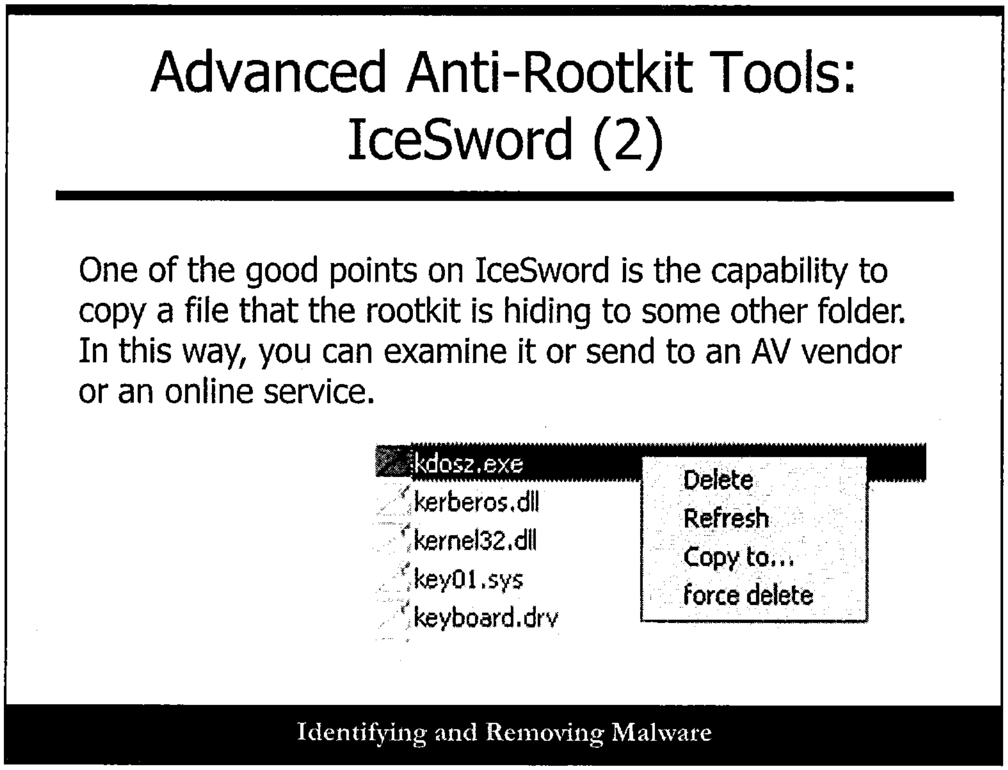



**Advanced Anti-Rootkit Tools: IceSword (1)**

This is another example of a great tool that works only on Windows XP. The following slides use the same badkits2.zip rootkit file used to create the previous slides.

After the badkits2 is executed, extract the IceSword122.zip and open IceSword.exe; then select the File section on the left panel.

Selecting our local driver C: and going to the Windows\System32 folder, it reveals a nice surprise: It is possible to see our hidden malware on the Windows\System32 folder.




**Advanced Anti-Rootkit Tools: IceSword (2)**

We now know that IceSword can show us the file that is hidden by the rootkit.

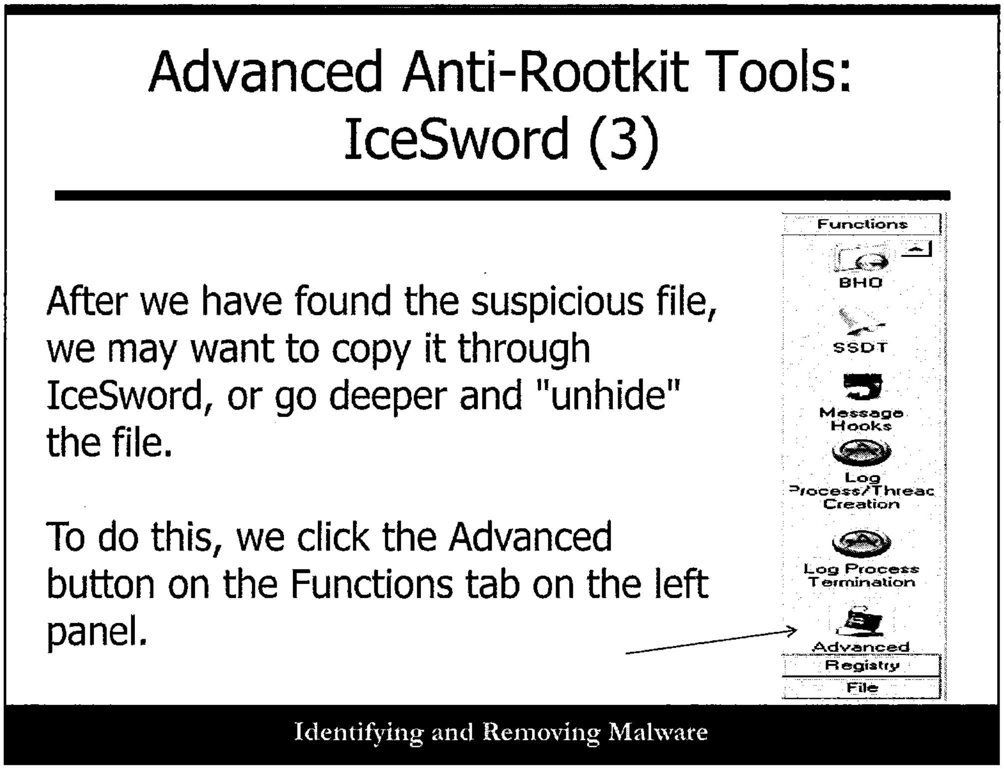
That is already a good thing. Now, another good thing from this tool is the ability to Copy the file to another location on the hard drive.

This is useful because sometimes we want to send this suspicious file to our antivirus vendor, simply run it on one online service that offers a Sandbox, or just run several AV and see how they detect this suspicious file.

This is accomplished on IceSword by right-clicking the file and choosing the Copy to option.

The right-click also offers the following options:

- Delete
- Refresh
- Copy to …
- Force delete

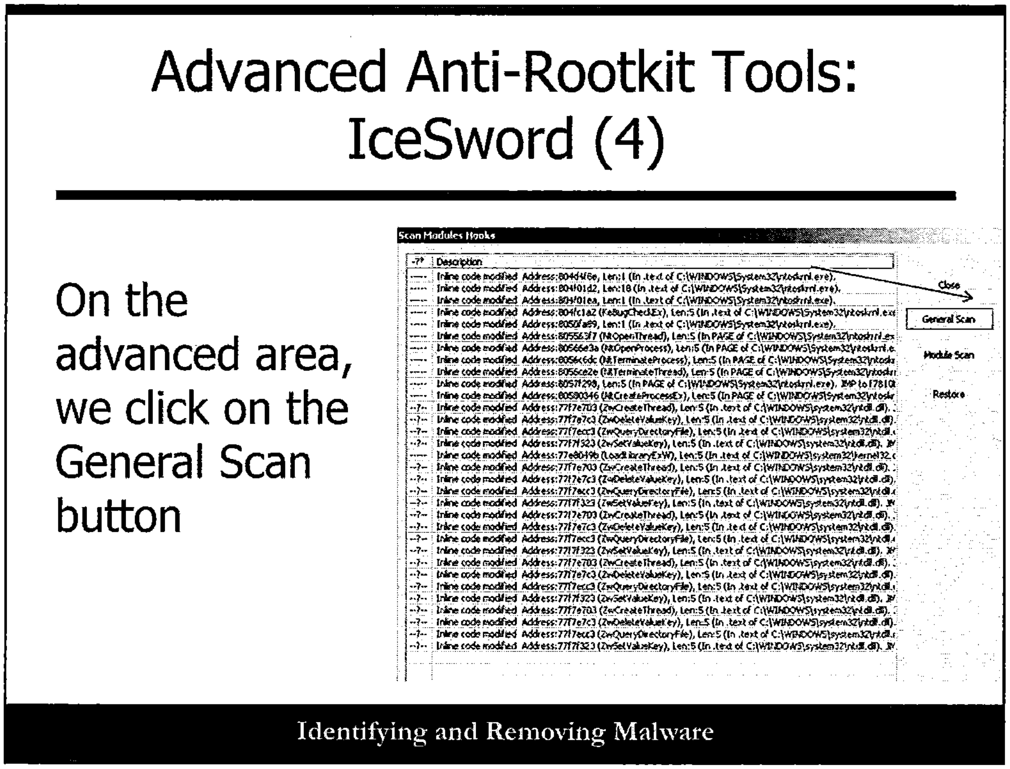



**Advanced Anti-Rootkit Tools: IceSword (3)**

As mentioned before, IceSword is powerful and has several functions.

Because we know that we have a hidden file on our system, it would be nice to find the hooks associated with it.

The Advanced button helps with this, by offering the option to scan the system.




**Advanced Anti-Rootkit Tools: IceSword (4)**

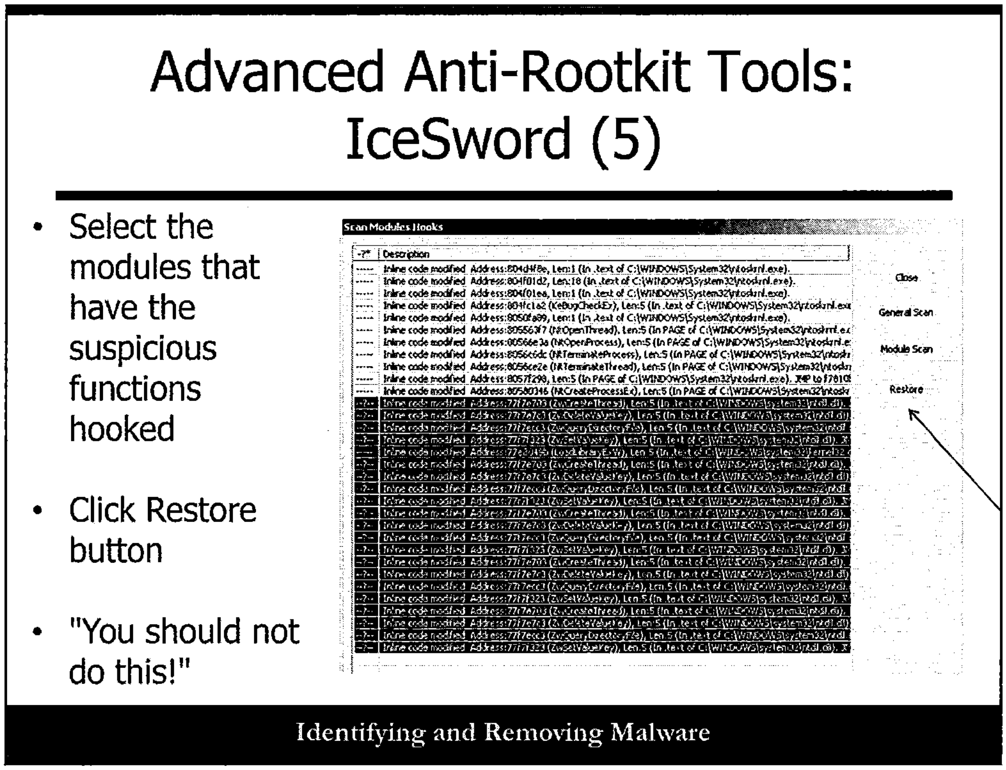
When we go to the advanced area, we can scan the system by pressing the General Scan button.

The results come up quite fast and show the hooked functions.

In this case:

- ZwQueryDirectoryFile
- ZwCreateThread
- ZwDeleteValueKey
- ZwSetValueKey

Does this sound similar to Rootkit UnHooker? ☺




**Advanced Anti-Rootkit Tools: IceSword (5)**

We can now select the hooked functions by clicking them and holding the Shift key.

After we select all hooks of interest, we can press the Restore button.

You will see a warning window, with the message: "You should not do this!" ☺ This is because in some cases, if we do something wrong (unhook something critical), we may get a BSOD.

Go ahead and restore the Hooks and see if we can now see the hidden file in Windows Explorer.

# Identifying and Fighting Rootkits (1)

- Caveats:
  - Beware when cleaning the machine with anti-rootkit tools
  - Some Rootkits may hide in legitimate processes like iexplore or winlogon.exe
  - Removing legitimate files may result in failure to boot or failure of the system to run correctly

Identifying and Removing Malware

**Identifying and Fighting Rootkits (1)**

Following are some caveats:

- Beware when "cleaning" the machine with anti-rootkit products; some rootkits may be tricky to remove.

- Some rootkits may hide in legitimate processes such as Internet Explorer (iexplore.exe) and winlogon.exe. Removing legitimate files may result in failure to boot or failure to run correctly. In those cases, it is recommended to follow these actions:

  - Get a more verbose program to check the hook and device drivers related to the legitimate application.
  - Boot in safe-mode to allow you to manually delete the malicious device driver (preferably using CLI tools).
  - Restart the system and run the anti-rootkit application again.

# Identifying and Fighting Rootkits (2)

- Last tip:
  - When dealing with Rootkits, if you are unsure about the cleaning operation, make a backup of your files and rebuild the machine from scratch

Identifying and Removing Malware

**Identifying and Fighting Rootkits (2)**

**Last Tip**

Although we identified this rootkit in our machine, and safely removed/renamed them, in some cases it may not be possible or it may be too complex to do so without causing harm to the computer. If you are unsure about cleaning the rootkit, back up the important files instead and rebuild the machine from scratch. Be careful, as some malicious files may still be hiding in the data you are about to back up.

Therefore, it's better to restore your system from a known clean previous backup if you have one.

And remember, removing legitimate files may result in failure to boot or failure to run correctly.

# Rootkits and Anti-Rootkits

## Windows 7 Hands-on
## Part 1

Identifying and Removing Malware

**Rootkits and Anti-Rootkits**
On the rootkits and anti-rootkits part, we start with the following steps:

1. Revert the VMware Windows 7 image to the Snapshot Clean7:
   VM -> Snapshot -> Select Clean7
2. Open the folder Course on the VMware Windows 7 Desktop.
3. Open the Part7 folder.
4. Copy TDSSKiller.exe, mbr.exe and sanitySetup.exe to your desktop.
5. Double-click the SanitySetup.exe file and click the Next button on the instructions screens to complete the installation.
6. Right-click the badkit.zip file and select Extract All. Enter the **training** password when asked.
7. Double-click the new created folder.
8. Copy the badkit.exe to the desktop.
9. Now, right-click the badkit.exe file and select Run as Administrator.

Continue to follow the slides doing the same on your VMware Windows 7 image.

**LEGACY INFO**: If you plan to do this exercise on a Windows XP machine, you need to check: If the machine is on Service Pack1 or less, you need to install the Service Pack2, WindowsXP-KB835935-SP2-ENU.exe. This process can take up to 20 minutes depending on your system. Restart your Windows XP (on VM) after the SP2 installation. Take a new snapshot, called SP2, so we can revert later.

# Rootkits: Win 7 Example

- In the following example we examine a machine that is acting strangely
- Identify/verify malicious activity with Windows tools

Identifying and Removing Malware

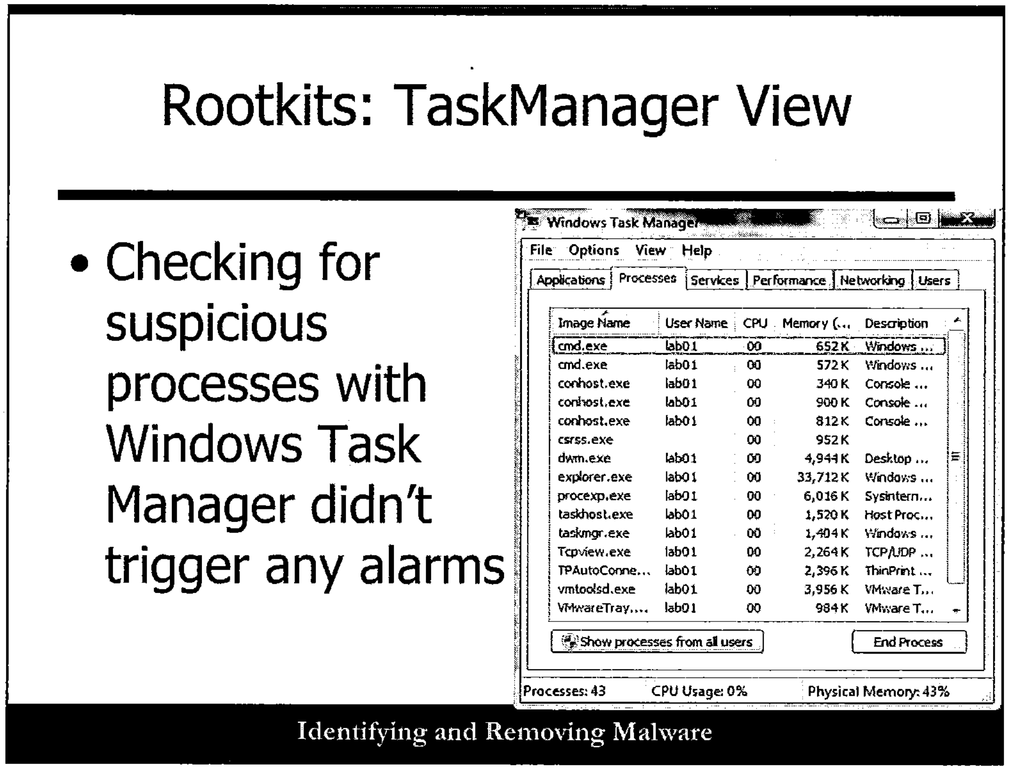
**Rootkits: Live Example**

**Our Learning Example**

In our learning example with Rootkits, we have the following scenario:

A machine was working okay, but the Incident Response Team identified that something was not quite right. That's not exactly the best thing to hear because no details were provided, yet we have to figure it out.

First, we try to identify if something is wrong using some of the tools that we learned about so far such as Task Manager, Process Explorer, and TCPView.



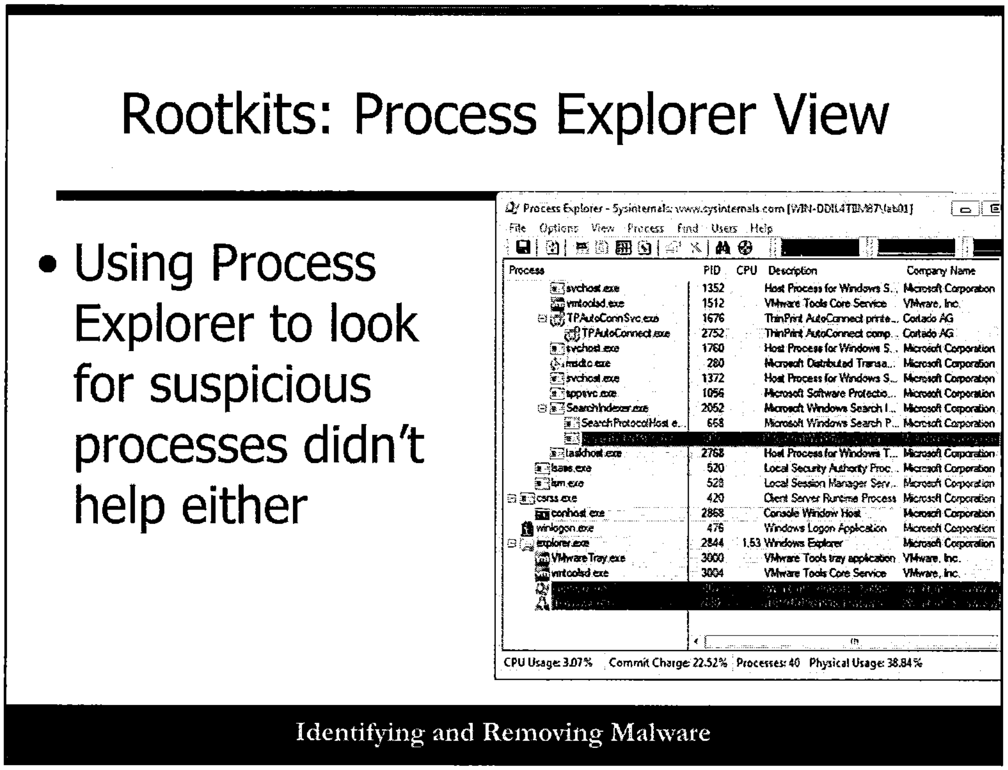

**Rootkits: TaskManager View**

**Using TaskManager**

The first thing we can do is use Windows TaskManager and visually try to identify anything that could be considered suspicious, any process that would not fit in the machine configuration.

This is obviously not an easy task because a machine can have hundreds of processes, and you may not always know each of the processes, and because a malicious process could choose a deceptive name to avoid visual detection.

In our case, we could not see anything that triggered our "visual radar."




**Rootkits: Process Explorer View**

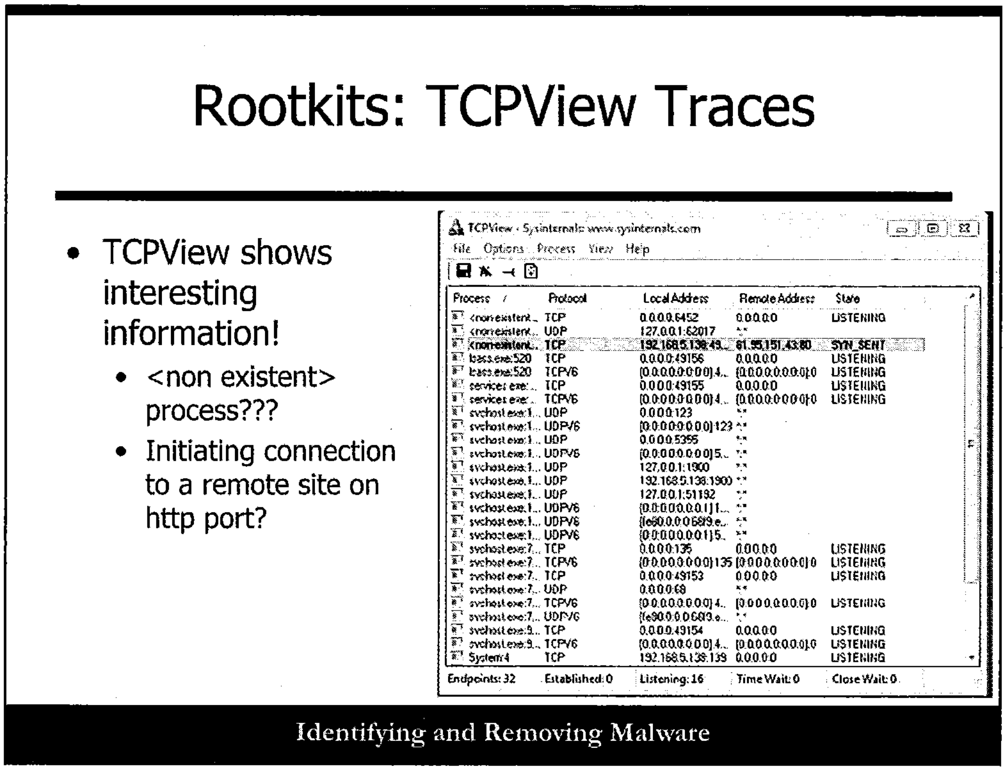
**Using Sysinternals' Process Explorer**

We already tried to identify possible suspicious processes or services with Windows Task Manager, but we didn't have any luck. Now we try to see the same processes and services with Microsoft Sysinternals tool Process Explorer.

Process Explorer can give a much more complete view of the processes and services on the machine, including the description of the process and service.

As you can see, you cannot spot any suspicious activities or processes.

| Process | PID | CPU | Description | Company Name |
|---|---|---|---|---|
| System Idle Process | 0 | 98.02 | | |
| Interrupts | n/a | | Hardware Interrupts | |
| DPCs | n/a | | Deferred Procedure Calls | |




**Rootkits: TCPView Traces**

**Using Sysinternals TCPView**

Because we already tried to get information with Windows Task Manager and Process Explorer, and could not identify any suspicious processes or services, we can now try to use another well-known Sysinternals tool: TCPView.

This time we got at least some suspicious activities.

TCPView shows a bunch of connections initiated by a <non-existent> process, to a remote server on port 80.

| **Process** | **Protocol** | **Local Address** | **Remote Address** | **State** |
|---|---|---|---|---|
| <non-existent>:744 | UDP | Lab-machine:1075 | *:* | |
| <non-existent>:744 | TCP | Lab-machine:1046 | Lab-machine:0 | LISTENING |
| <non-existent>:744 | TCP | lab-machine:1046 | 81.95.151.43:http | SYN_SENT |

# Rootkits: SanityCheck (1)

- Works on different versions of Windows, including 7, 8, and Server 2012
- Works on x32 and x64
- Great to "assist," not to "Fix"

Identifying and Removing Malware

**Rootkits: SanityCheck (1)**

The tool SanityCheck works great in different versions of Windows, including Windows 7. Before you start to use it, you need to have it installed in the system.

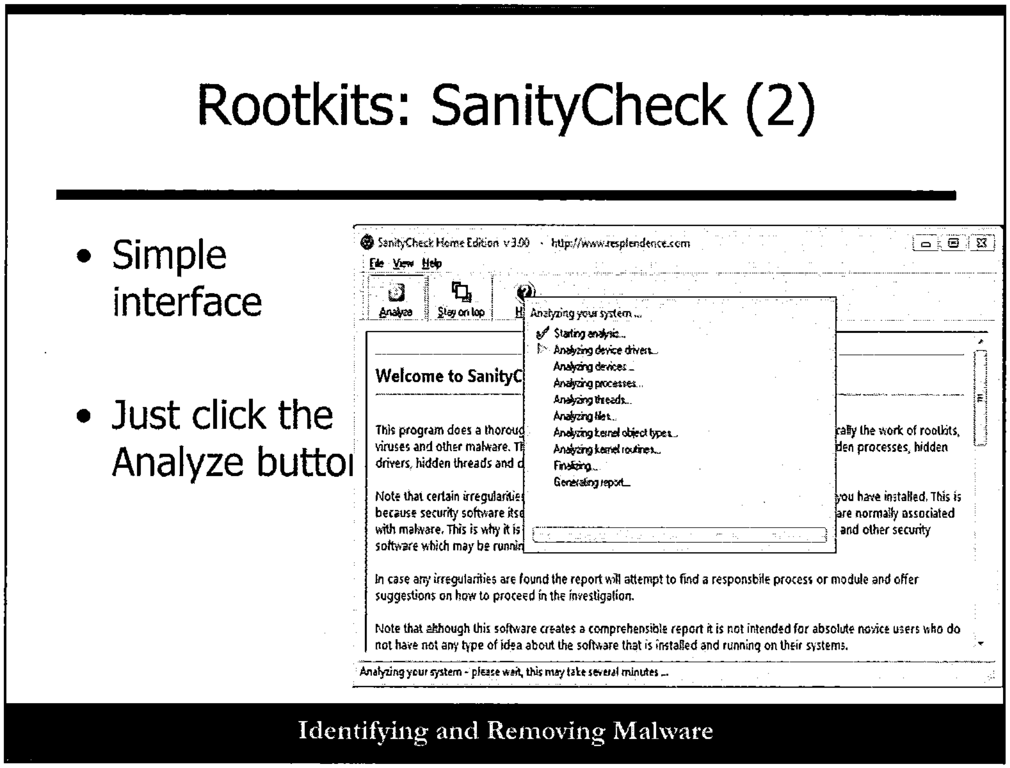
It is a great tool to assist to you in identifying suspicious rootkit activities; however, it does not fix them.

It can be downloaded at http://www.resplendence.com/download/sanitySetup.exe.

The installation is simple; just double-click it and follow the default options. Remember to check the box that creates a desktop icon, on the screen called Select Additional Tasks.

The last screen during installation lets you launch the tool after the Setup Wizard finishes. That's okay; just click Finish.

Before the tool actually starts, it asks if you want to change certain Registry settings to improve detection. Because we don't want to mess with the Registry, select No.

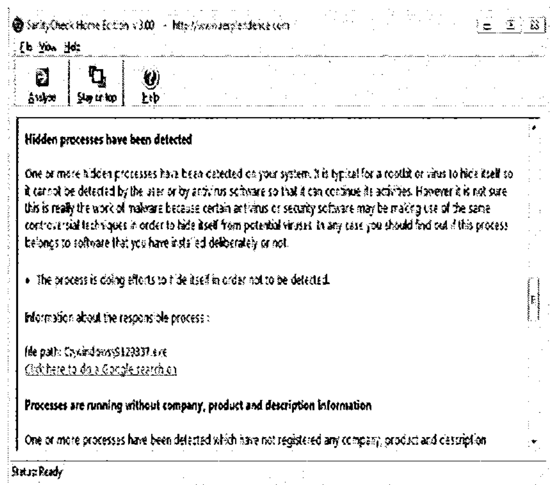



**Rootkits: SanityCheck (2)**

The SanityCheck interface is simple. We just need to click the Analyze button and wait for the results.

# Rootkits: SanityCheck (3)

- The result shows a hidden process detected running in the system
- This is a good indication that a rootkit is installed
- Now we need to find the driver that is preventing us to see and kill the process to clean our system




Identifying and Removing Malware

**Rootkits: SanityCheck (3)**

After the scan finishes, it shows you the results when you scroll down the main window.

On the results, you can see that it detected a hidden process running on the system, called 9129837.exe. This is a good indication that there is a rootkit on the system that is intercepting the system calls and preventing a process to display.

This is usually done by a low-level system driver installed in the system. To clean our system, we need to see the process. To see the process we need to delete what is preventing Windows to show it.

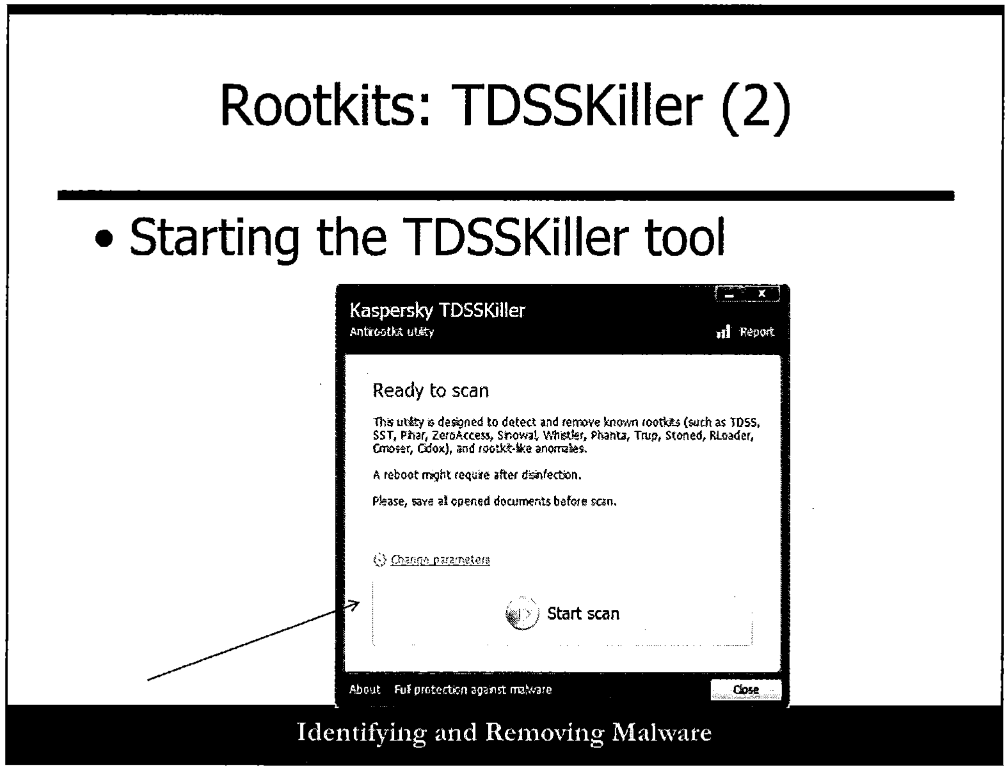
# Rootkits: TDSSKiller (1)

- Kaspersky TDSSKiller
  - Developed by AV Kaspersky in 2009
  - Clear UI (command line available)
  - Supports 32 and 64 bits

Identifying and Removing Malware

**Rootkits: TDSSKiller (1)**

TDSSKiller, developed by the AV vendor Kaspersky, can be downloaded at http://support.kaspersky.com/downloads/utils/tdsskiller.exe. It is a simple, yet powerful application, and it runs smoothly on Windows 7, both 32- and 64-bit.

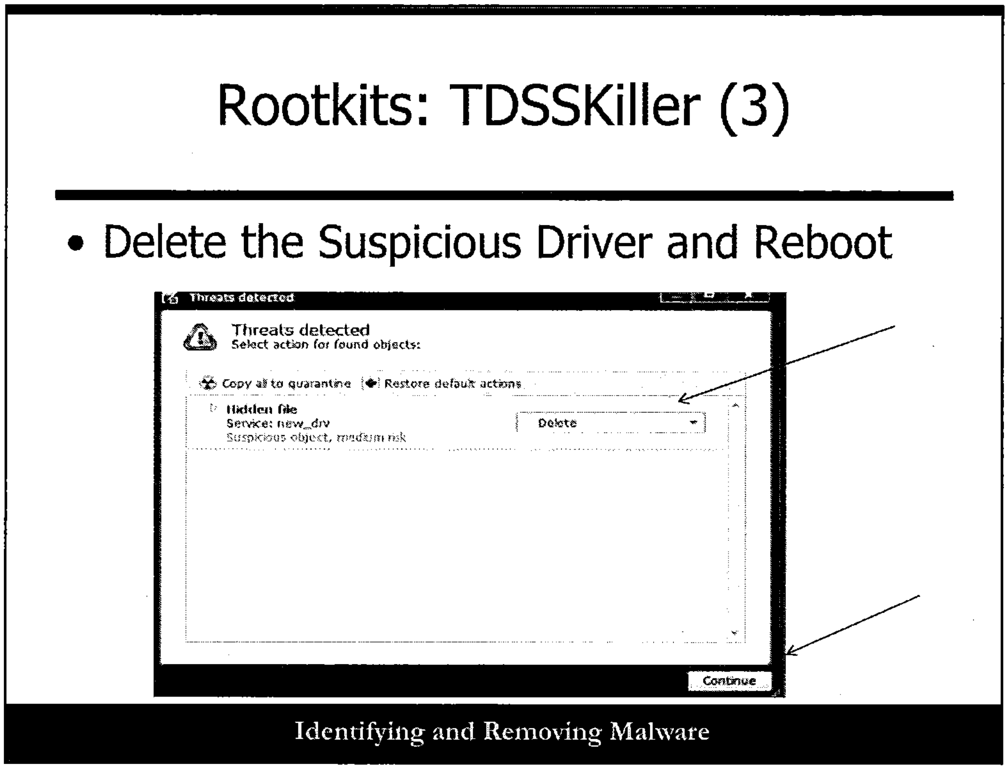



**Rootkits: TDSSKiller (2)**

To start the TDSSKiller tool, simply double-click it on the tdsskiller.exe on your desktop.

The application opens and asks if you want to Start the Scan right away, or if you want to customize it. The tool offers you the option to select which objects you want to scan, such as System Memory, Services and Drivers, Boot Sectors and Loaded Modules. By default the first three are checked to be scanned and in general you should be okay.

P.S. The tool also offers some options that enable you to run on the command line. Typing **tdsskiller.exe –h** shows all available options.




**Rootkits: TDSSKiller (3)**

As you can see, the slide shows that the TDSSKiller found a threat. It is a hidden file that works as a service, with the name new_drv.

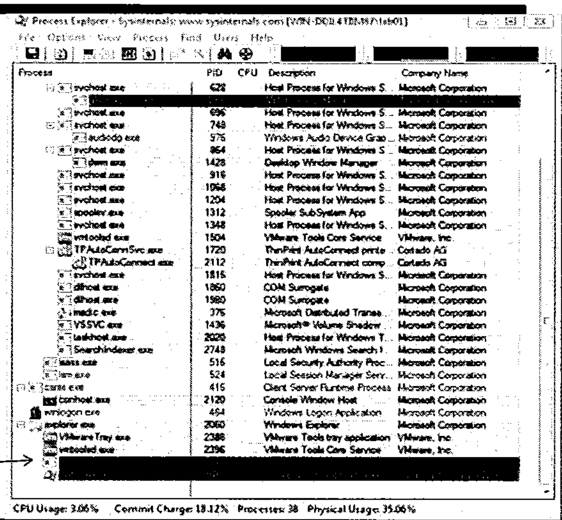
TDSSKiller offers three options for the suspicious hidden file: Skip, Copy to Quarantine, and Delete.

Now let's delete the suspicious driver and reboot the system.

Note that on 64-bit Windows 7, after running TDSSKiller, new_drv is not detected, but 9129837 exists on the machine and may be running.

## Rootkits: Process Explorer (1)

- Now you can see the process running!
- It is time to remove it from the system



Identifying and Removing Malware

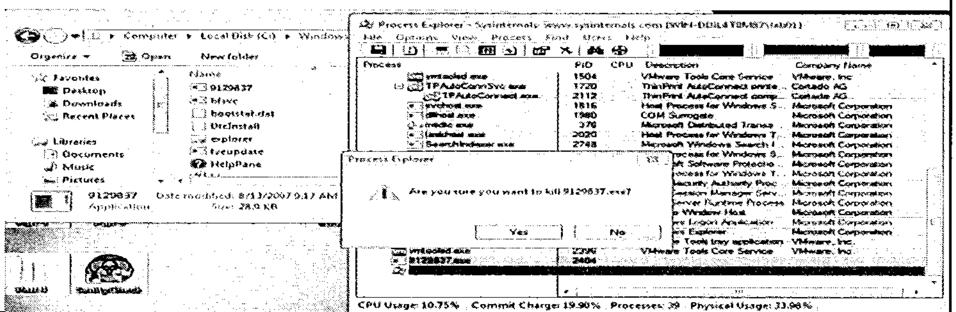
**Rootkits: Process Explorer (1)**

After the system reboot, open Process Explorer again. Notice that now you can see the malicious process running.

It is good because to remove it from the system, we need to kill it first.

# Rootkits: Process Explorer (2)

- Before we delete the file from c:\windows, we need first to make sure it is not running
- On Process Explorer, kill the process 9129837.exe so that you can delete the file from the Windows folder



Identifying and Removing Malware

**Rootkits: Process Explorer (2)**

To remove the malware from the system, you can just go to the Windows folder and delete it; however, if you try to delete it with the malicious process still running, Windows will not let you do it.

So, first you need to kill the malicious process. Because you have Process Explorer running, you can just click it and select Kill Process. Process Explorer shows a confirmation window. Just click Yes.

Then you can delete the file from the Windows folder, either by going there with Windows Explorer or via command line.

# Rootkits and Anti-Rootkits

## Windows 7 Hands-on
## Part 2

Identifying and Removing Malware

**Rootkits and Anti-Rootkits**
On the rootkits and anti-rootkits part, we start with the following steps:

1. Revert the VMware Windows 7 image to the Snapshot Clean7:
   VM -> Snapshot -> Select Clean7
2. Open the folder Course on the VMware Windows 7 Desktop.
3. Open the Part7 folder.
4. Copy TDSSKiller.exe and mbr.exe to your desktop.
5. Double-click the badkit3.zip file, copy the badkit3.exe to Desktop, and enter the **training** password. Then, right-click the file and select Run as Administrator.

Now, continue to follow the slides doing the same on your VMware Windows 7 image.

Note: On Windows 64 bit you may experience BSOD (Blue Screen of Death) due some attempted actions performed by the rootkit.

LEGACY INFO: If you plan to do this exercise on a Windows XP machine, you need to check if the machine is on Service Pack1 or less; you will need to install the Service Pack2, WindowsXP-KB835935-SP2-ENU.exe. This process can take up to 20 minutes depending on your system. Restart your Windows XP (on VM) after the SP2 installation. Take a new snapshot, called SP2, so we can revert later.

## Fighting MBR Rootkits (1)

- GMER MBR
  - Developed in 2008
  - Command-line tool, no UI
- Kaspersky TDSSKiller
  - Developed by AV Kaspersky in 2009
  - Clear UI (command line available)
  - Supports 32 and 64 bits

Identifying and Removing Malware

**Fighting MBR Rootkits (1)**

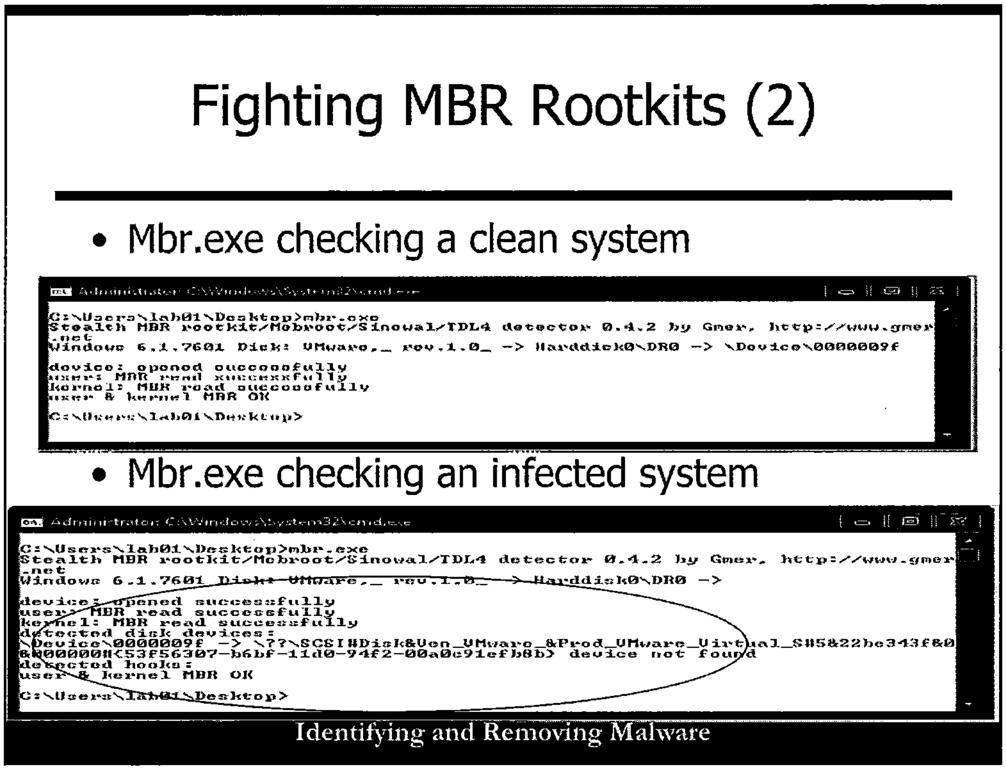
For MBR rootkits, we use two different tools:

- MBR, developed by GMER, which can be downloaded at http://www2.gmer.net/mbr/mbr.exe.
- TDSSKiller, developed by the AV vendor Kaspersky, which can be downloaded here at http://support.kaspersky.com/downloads/utils/tdsskiller.exe.

The good thing is that you have a choice because one is a console application, which means that you can run from the command line, and the other offers a nice and clean graphical interface.

Both will also generate a log file:

- mbr.log for the MBR GMER tool
- TDSSKiller_<tool_version>_<date>_<time>.txt




**Fighting MBR Rootkits (2)**

Open the cmd.exe as Administrator.

Now, go to the desktop where you put the mbr.exe tool:

-> cd \Users\<your username>\Desktop

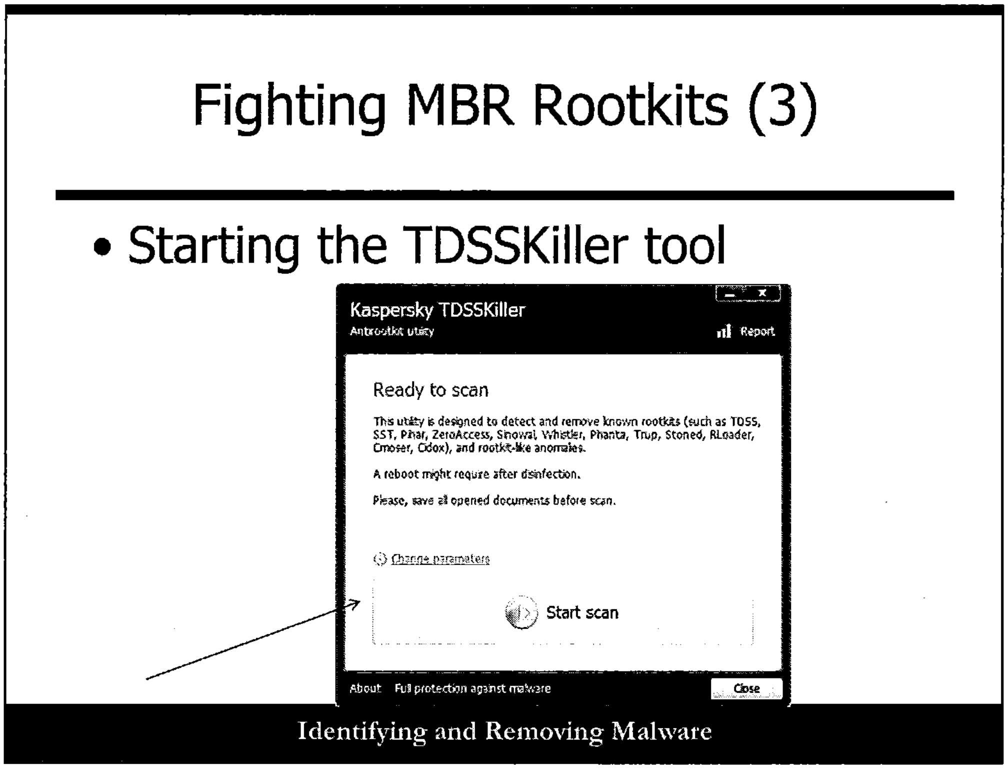
Run the mbr.exe tool:

-> mbr.exe

The good thing about this tool is that even if it doesn't show a clear message of a system being infected, it helps to spot issues on the MBR, such as an infection for an unknown variant that infects the system MBR.

The first screen shot shows the tool running on a clean system. The second one shows it running on a system already infected. It is possible to see that even it didn't display the Infected message; it throws some errors that mean that something is wrong and needs a need investigation.

For this reason, we now use the Kaspersky TDSSKiller tool in the next step.




**Fighting MBR Rootkits (3)**

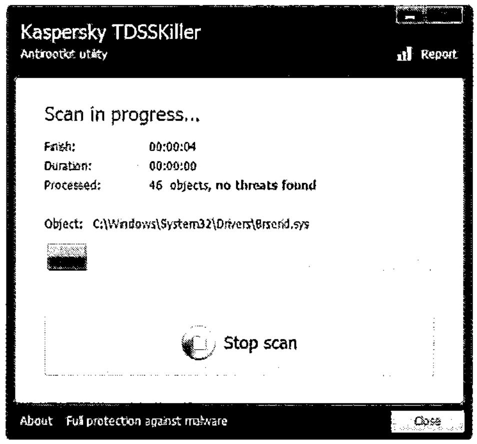
To start the TDSSKiller tool, simply right-click and select Run as Administrator.

The application opens and asks if you want to Start the Scan right away, or if you want to customize it. The tool offers you the option to select which objects you want to scan, like System Memory, Services and Drivers, Boot Sectors, and Loaded Modules. By default the first three are checked to be scanned and in general you should be okay.

The tool also offers some options that allow you to run it on the command line. Typing **tdsskiller.exe –h** shows all available options.

# Fighting MBR Rootkits (4)

The tool will run and show the status while scanning



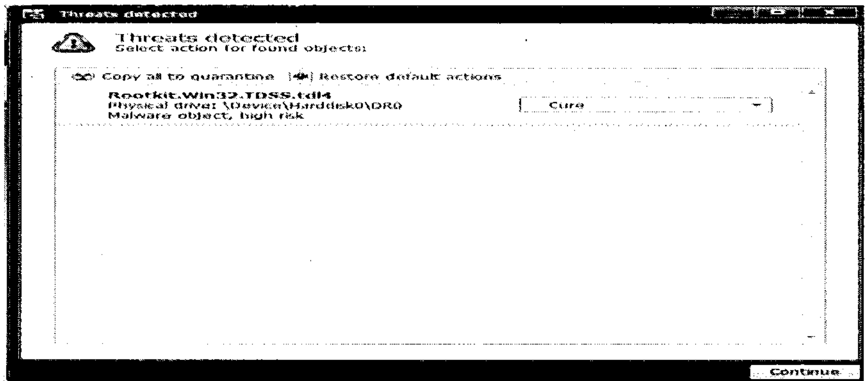

Identifying and Removing Malware

**Fighting MBR Rootkits (4)**

When the tool is running, you can see the scan progress and maybe the number of threats found.

# Fighting MBR Rootkits (5)

- TDSSKiller reports the type of threat found, TLD3, TLD4, and so on



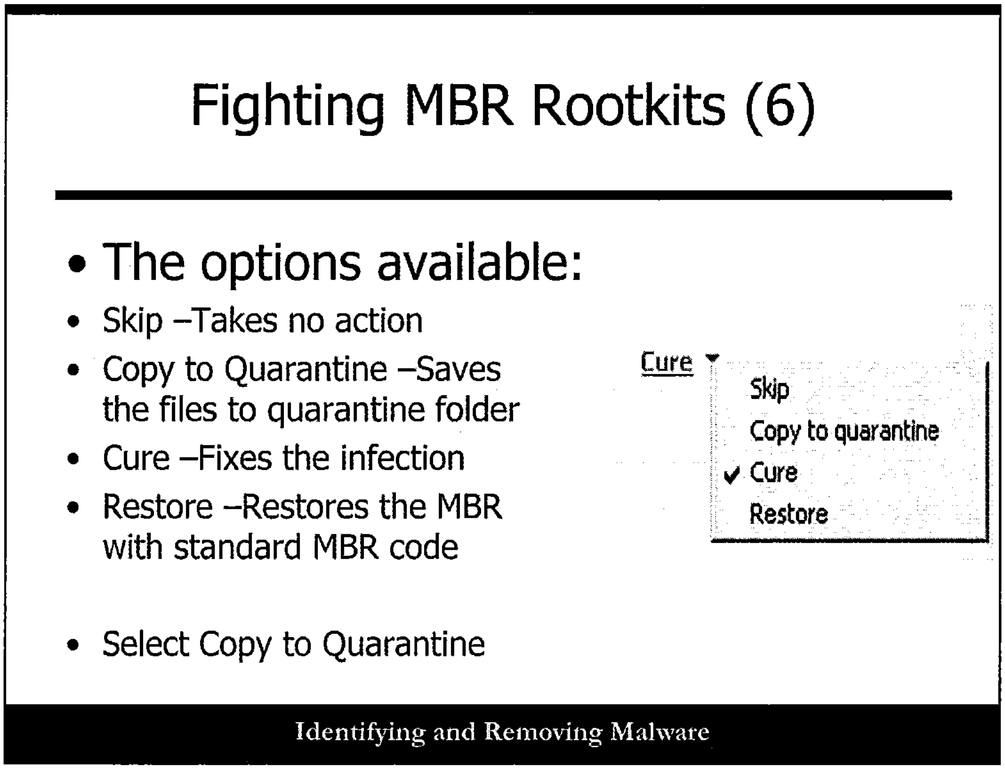

Identifying and Removing Malware

**Fighting MBR Rootkits (5)**

After it finishes the scan, the next window shows the results.

In this case, you see that it detected as Rootkit.Win32.TDSS.tdl4.

Now, you can select if you want to continue or explore more options.




**Fighting MBR Rootkits (6)**

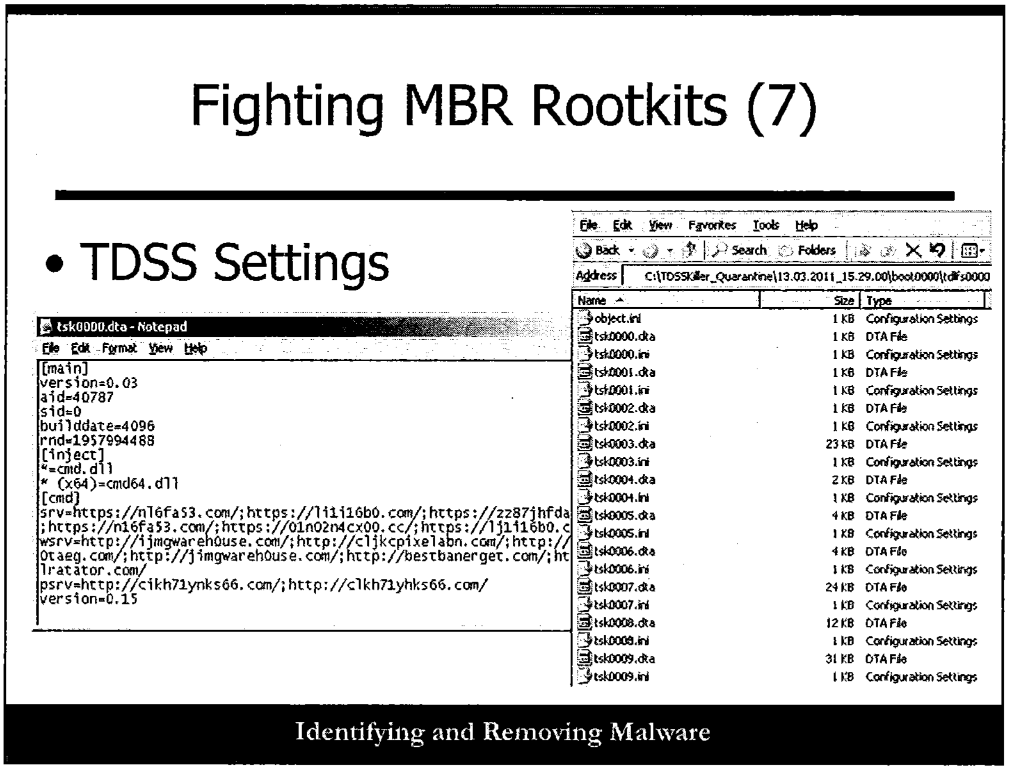
When an infection is found, the tool offer the following options:

- **Skip**: Takes no action and just report
- **Copy to Quarantine**: Removes the infection and copies the files, which includes the binary PE file to **C:\TDSSKiller_Quarantine**: You can use these files to submit to your AV vendor or get more information.
- **Cure**: Removes the infection on the MBR
- **Restore**: Writes standard clean MBR code and overwrites the infected one

For now, choose the Copy to Quarantine option and click Continue.

An example of good usage of the Quarantine folder is to gather information about the remote sites the malware connects to.

On the following pages, learn how to find this information.




**Fighting MBR Rootkits (7)**

Now that we saved the files on the Quarantine folder, we can open it in Windows Explorer.

1. Open the Quarantine folder at C:\TDSSKiller_Quarantine.
2. Open the subfolder that is the in the format <date>_<time>.
3. Open the subfolder boot0000.
4. Open the subfolder tdlfs0000 (this is the TDL file system).
5. Open the file tsk0000.dta (select Notepad to open it).

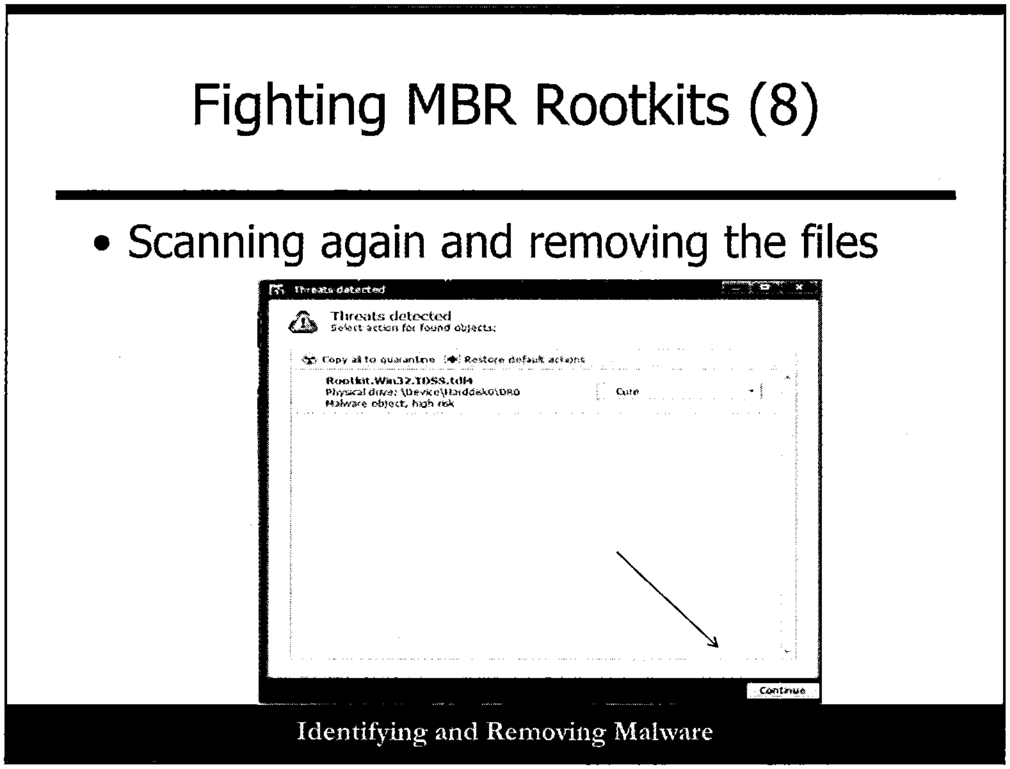
This file contains some configuration settings used by the malware, which includes the websites it connects to:

srv=https://nl6fa53.com/;https://li1i16b0.com/;https://zz87jhfda88.com/;https://n16fa53.com/;https://01n02n4cx00.cc/;https://lj1i16b0.com/

wsrv=http://ijmgwareh0use.com/;http://cljkcpixelabn.com/;http://thynksn0taeg.com/;http://jimgwareh0use.com/;http://bestbanerget.com/;http://pxlratator.com/

psrv=http://cikh71ynks66.com/;http://clkh71yhks66.com/

Note that when you select Copy to Quarantine, it does not remove the malware, so you need to run the scan again.




**Fighting MBR Rootkits (8)**

Now run the scan again, but this time, do not change the settings, so it removes the malware, but only after the reboot.

To complete the cleaning, you need to restart the computer.

# Identifying and Removing Malware

## Cloud-Based Tools

Identifying and Removing Malware

This page intentionally left blank.

## Cloud-based Tools

- Tools that need to reach out to external servers to be fully functional:
  - Team Cymru WinMHR
  - CrowdStrike CrowdInspect
  - Process Explorer (!)

*Make sure this is okay with your company policy for incident/malware handling.

Identifying and Removing Malware

**Cloud-based Tools**

In the Malware Day of SANS 501, you use different tools to deal with different types of malware. The good thing about these tools is that they work independently regardless if you connect to the Internet.

During some malware investigation you may need to work with some machines that are not online anymore. However, on most cases you will find the infected machine and start to work on it while it is still online.

Some of the tools presented on this section use the Internet to help you during your investigation by checking external sites for indicators that can help you identify the infection.

However, for some companies the fact that you will be checking files or even hashes against an external server is considered a violation of the Malware/Incident Handling policy, so be sure to check before add these tools to your kit.

# Team Cymru WinMHR (1)

- Free tool
- Developed by the nonprofit organization Team Cymru
- Checks the running processes and files against the Malware Hash Registry database of files and antivirus detection
- Supports Windows XP Sp3, Vista, and 7
- Does NOT remove the malware

Identifying and Removing Malware

**Team Cymru WinMHR (1)**

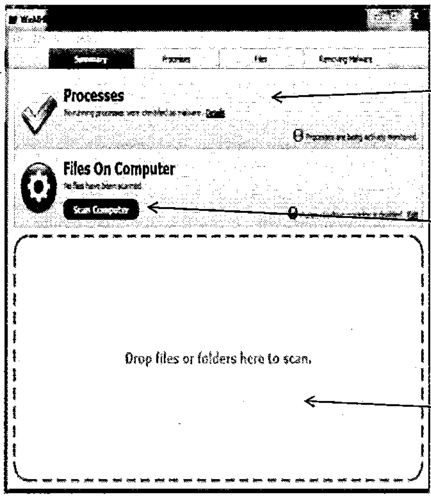
The WinMHR is an application developed by the Team Cymru, a nonprofit organization that specializes in Internet Security research.

This tool checks the running processes and the files on the system against a large database of known bad files and presents the results and alerts.

Although it can be used to detect malware running on the system, it will not remove it. This is still a job for your End Point Anti-Malware solution.

It can be downloaded at http://www.team-cymru.org/Services/MHR/WinMHR/.

# Team Cymru WinMHR (2)




- When the application starts it automatically checks the processes running
- To start a new file scan, the user just needs to click the Scan Computer button
- It also presents a screen where the user can just drop suspicious files

Identifying and Removing Malware

**Team Cymru WinMHR**

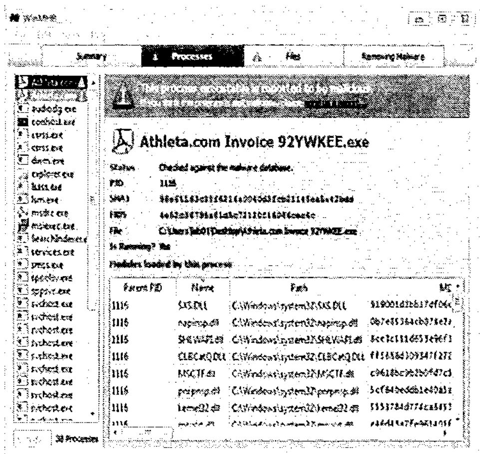
When you run the application for the first time, it goes through all the steps to install a regular application, including a EULA agreement.

After it is installed, and running, it will scan all processes running and give you an immediate response.

For files, the user has two options:

1. Do a complete scan; just press the Scan Computer button. Depending on your computer it may take between 1 to 5 minutes to complete the scan.
2. Do a scan on specific files, by just dropping them in the "Drop Files or Folders Here to Scan" section of the application.

# Team Cymru WinMHR (3)



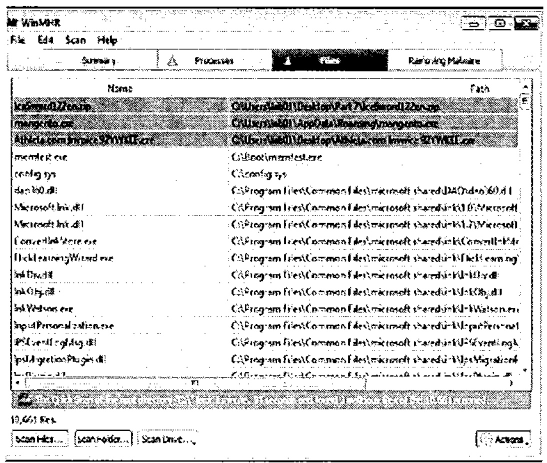

- When WinMHR finds a suspicious process, it marks it and displays a few more details about the malicious process
- It also offers a view of all modules that were loaded with the process

Identifying and Removing Malware

**Team Cymru WinMHR**

If the tool finds a suspicious process, it displays an alert highlighting them. By clicking any of the suspicious processes, it is possible to get more information about it, including the hashes and the current modules loaded by this process.

# Team Cymru WinMHR (4)



- When WinMHR finds suspicious files, it marks them orange and displays them in the beginning of the report
- By right-clicking it, it is possible to go straight to the folder and then perform additional tasks like delete or copy

Identifying and Removing Malware

**Team Cymru WinMHR**

When the tool finds suspicious files, it acts almost like on the suspicious process part. It also highlights them with the orange color and displays them on the top of the report to make it easy to identify them.

After it is identified you can perform additional tasks, such as right-click and go to the folder where the file is, and either delete, copy, or quarantine the file for further analysis.

# CrowdStrike CrowdInspect (1)

- Free tool
- Created by the CrowdStrike company as a tool to help inspect the running processes against different databases of malicious indicators, such as WoT, MHR, and VirusTotal
- Supports Windows XP, Vista, and 7

Identifying and Removing Malware

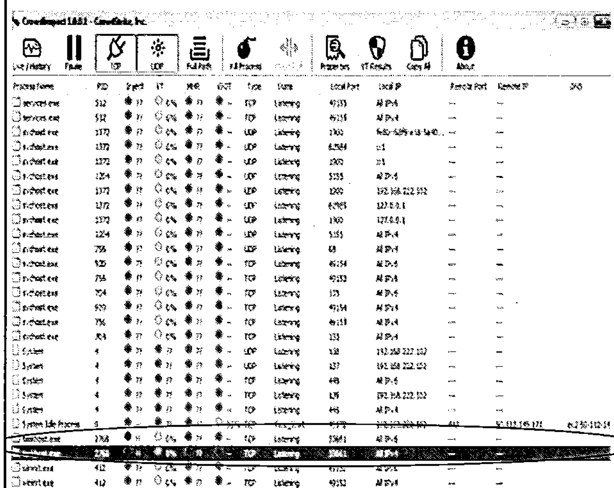
**CrowdStrike CrowdInspect (1)**

The CrowdInspect tool was created by the CrowdStrike company as a tool to assist on investigations by inspecting the running processes against different databases of malicious indicators, such as WoT (Web of Trust), MHR (Malware Hash Registry), and VirusTotal.

It supports most of the Windows OSs including Windows XP.

It can be downloaded at http://www.crowdstrike.com/crowdinspect/index.html.

# CrowdStrike CrowdInspect (2)



In this case, CrowdInspect detected that the process taskhost.exe has malicious code injected into it.

VirusTotal reports green status for the file.

This means that while the file is legit, the malicious code is running as a remote thread in the legit taskhost process.

The next step is to find the process and remove it before it is loaded into the legit process

Identifying and Removing Malware

**CrowdStrike CrowdInspect (2)**

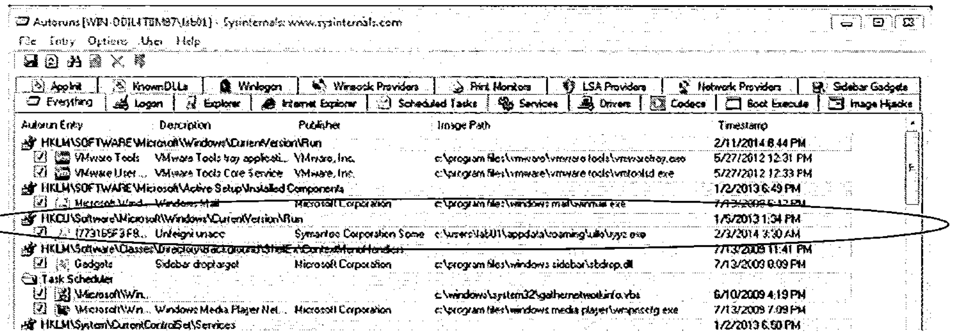
This screen shot shows the CrowdInspect tool in action. We can see that it is showing all running processes. For the process TaskHost.exe it shows a Red ball on the Inject column. This means that the tool detected that there is a malicious code that was injected into this process. MHR (Malware Hash Database) and WoT (Web of Trust) show no sign of this file, which can be a good signal. However, VirusTotal shows a Green ball for the taskhost.exe file.

This behavior means that the taskhost.exe is a legit file in the system. It also means that it is a legit process running in the system, which contains malicious code injected into it.

Sometimes, when a malware runs, it injects its code into a legit process and then copies itself to another location and exits. When the malware analyst is checking the list of process he won't notice anything suspicious.

The next step is to find the malicious file that is injecting its code into the legit processes. As usual, the malware needs to find a persistence method to ensure it can inject its code again when the computer restarts. So we need to check all autorun files against possible malicious ones.

# Microsoft Autoruns



And here it is! A file that has a random *Description* name, a suspicious Publisher name, and an even more suspicious filename/location.

Identifying and Removing Malware

**Microsoft Autoruns**

By running Microsoft Autoruns, it is easy to find the malicious file. Checking the Registry key that the malware usually uses to ensure persistence, you can see a file with suspicious characteristics:

- **Description name**: "Unfeigni unacc"
- **Published name**: "Symantec Corporation Some"
- **Image path**: c:\users\lab01\appdata\roaming\ullo\ryyz.exe

By removing this key and removing the file, you can ensure that the malware does not restart and does not inject its code again in the legit processes.

## Microsoft Process Explorer (1)

- Same old process Explorer that we already know
- Since version 16, released on January 2014, it included a cloud capability:
  - Checks a single file or all files and loaded DLLs against VirusTotal database and highlights the results

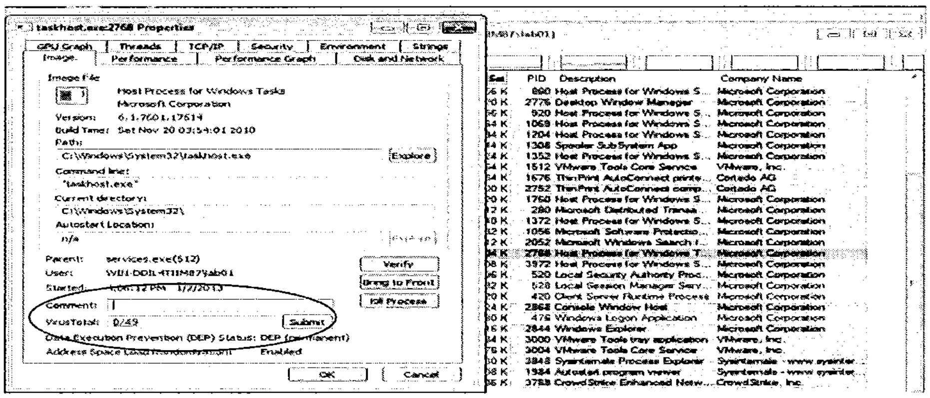
Identifying and Removing Malware

**Microsoft Process Explorer (1)**

It is the same Process Explorer that we used on previous sections of this course; however since the version 16, which was released on January 2014, it included an integration with VirusTotal. It is now possible to check a single file or all running processes and the loaded DLLs against the VirusTotal database.

Note that Process Explorer will NOT send the file to VirusTotal, but just check the file hash.

# Microsoft Process Explorer (2)



In our case, we can see that VirusTotal does not detect taskhost.exe, which is good since is a legit file from Microsoft.



**Microsoft Process Explorer (2)**

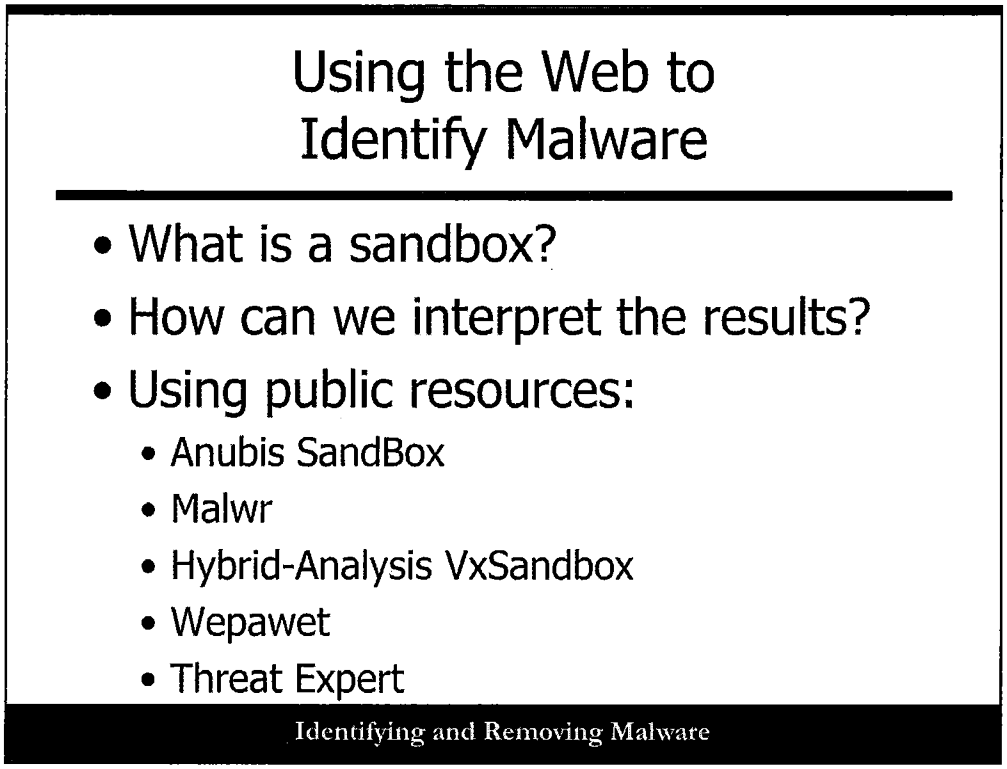
By double-clicking any process, the tool now shows a field called VirusTotal, with a Submit button. When you click this button, Process Explorer checks the hash of the image file against the VirusTotal database and reports the findings. For the taskhost.exe file, it returned that it found 0 detections among the 42 different antimalware engines at VirusTotal. In this case, it is a good thing because you already know that this is a legit Microsoft file.

## Identifying and Removing Malware

## Using the Web to Identify Malware

Identifying and Removing Malware

This page intentionally left blank.




**Using the Web to Identify Malware**

**Our Module**

In this module, you learn how to use the Web to get help when everything else fails. When you have a strange binary on your hands and you have no clue what it is, whether it is malicious, and/or whether it works alone or with other malicious software, the Web can help.

First, you learn about the sandbox technology. Then, you learn how to use three different publicly available sandboxes on the Internet. Finally, how can you interpret the results/reports generated to help us to clean our machines?

The five public sandboxes used with different malware follow:

- Anubis Sandbox
- Malwr
- Norman Sandbox
- Wepawet
- ThreatExpert

Because sandbox technologies are quite popular, other options are available. The following are included here for your reference:

- JSUnpack: Created by Blake Hartstein (Jsunpack.jeek.org)
- Eureka: Sandbox (http://eureka.cyber-ta.org/)

## What is a Sandbox?

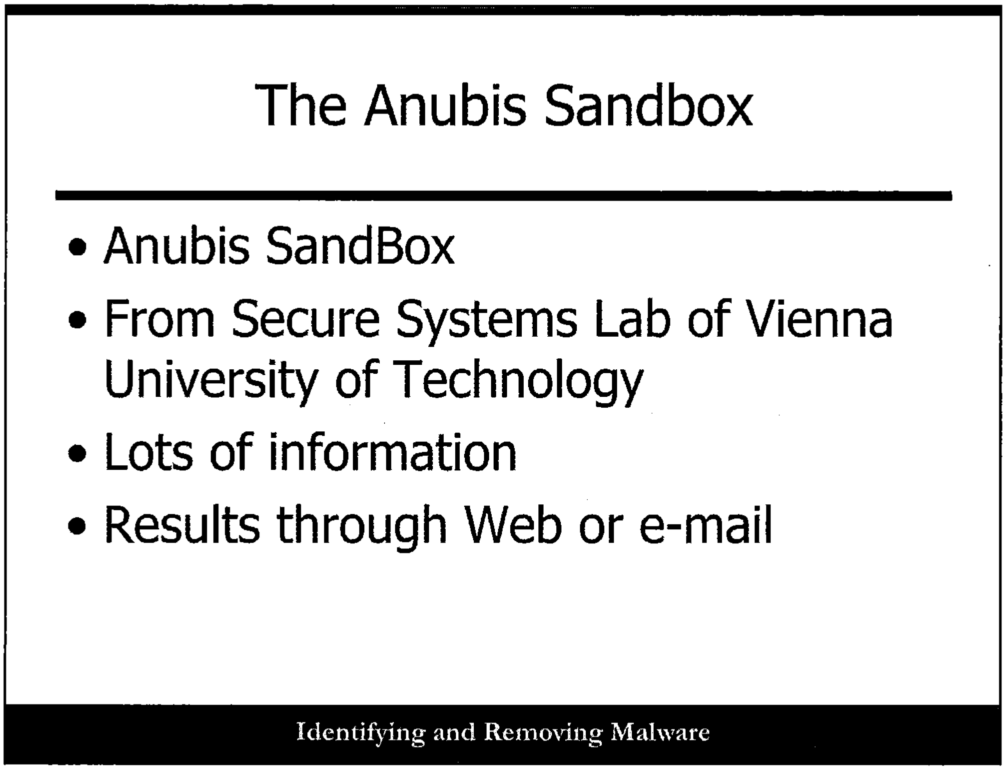
- What is a sandbox?

A basic explanation: A machine on which you can execute suspicious code and applications and watch for analysis results without risking your own environment

Identifying and Removing Malware

**What is a Sandbox?**

A sandbox in the computer environment is a quite recent term that is being adopted by computer security and research companies. The basic idea is that if you need to analyze the behavior of a piece of code or a program in a controlled environment and without endangering your own computer environment, you can use a sandbox. So you may run it within the sandbox and watch for changes to the system, network activities, and files added or modified to get a better view of the malware behavior and its capabilities.




**The Anubis Sandbox**

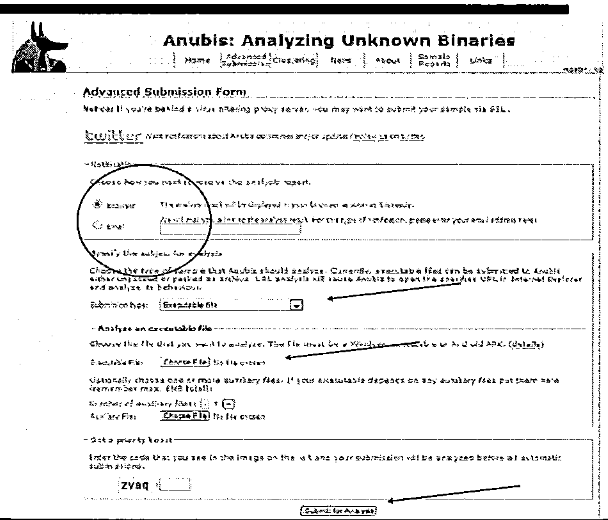
The Anubis Sandbox is an interesting project from the Secure Systems Lab at the Vienna University of Technology. Its sandbox, which is publicly available, provides a lot of information regarding the sample submitted to them, as you can see in the next slides.

This has good and bad sides:

- The bad side is the amount of information can confuse some people who are not security specialists.
- The good side is you have a more complete view of the malware activities, which can help you trace it in your own machine.

# Anubis Sandbox: Uploading (1)

- Simple steps:
- Choose if you want the report in the browser or to receive a link by e-mail
- Select if it's a file or URL
- Select the file and send




Identifying and Removing Malware

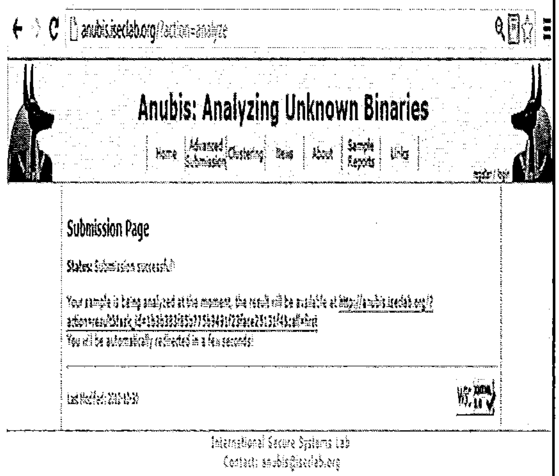
**Anubis Sandbox: Uploading (1)**

Getting started with Anubis Sandbox is quite easy. First, we need to point our browser to it. It can be reached at http://anubis.iseclab.org/.

On the first page, you have to select if you want to see the report in the browser or just receive an e-mail with the link that contains the report. Then, select if you want to submit a file or a URL. Finally, select the file you want to submit and type in the captcha code to get a higher priority for the analysis. Then, click the Submit button.

# Anubis Sandbox: Uploading (2)

- The report is generated
- It gives you an estimated time to completion
- You can click directly on the link provided or wait for automatic redirection



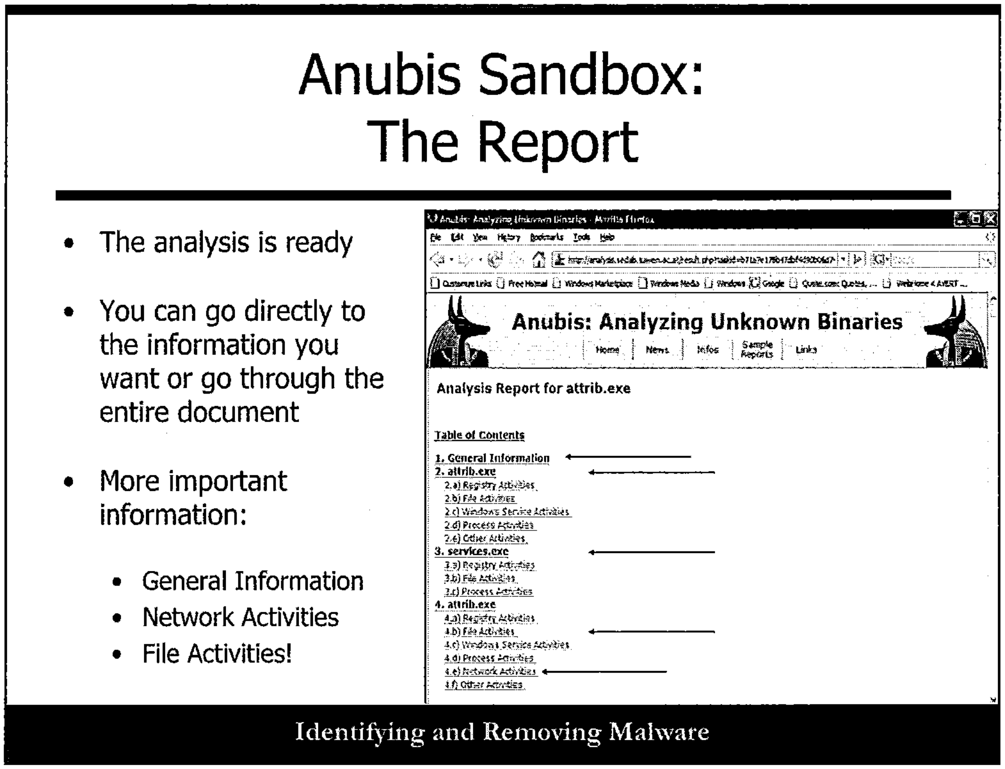

Identifying and Removing Malware

**Anubis Sandbox: Uploading (2)**

When we decide to submit a file to Anubis, it shows a status page with an estimated time to complete the task. In our case, it is approximately 2 minutes.

Right now you have two options:

- Click the link provided and wait for the results.
- Wait on this screen for the results because it refreshes automatically.




**Anubis Sandbox: The Report**

When the analysis is done, you will be presented with another window with all of the results.

First, you will be shown an index of the results. The index generally is divided into:

- General Information
- Processes involved

For each process involved, you have a lot of information, such as:

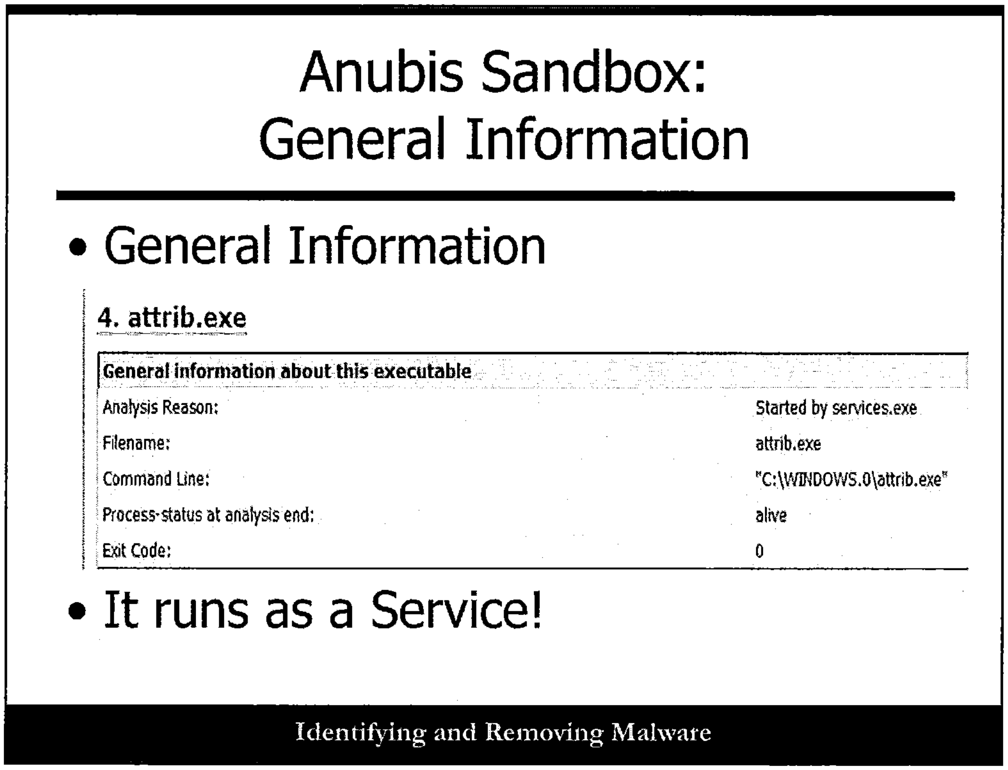
- Registry Activities
- File Activities
- Windows Services Activities
- Process Activities
- Network Activities
- Other Activities

For the purpose of trying to identify malware in your machine, the most interesting information that you can get is

- General Information
- File Activities
- Network Activities

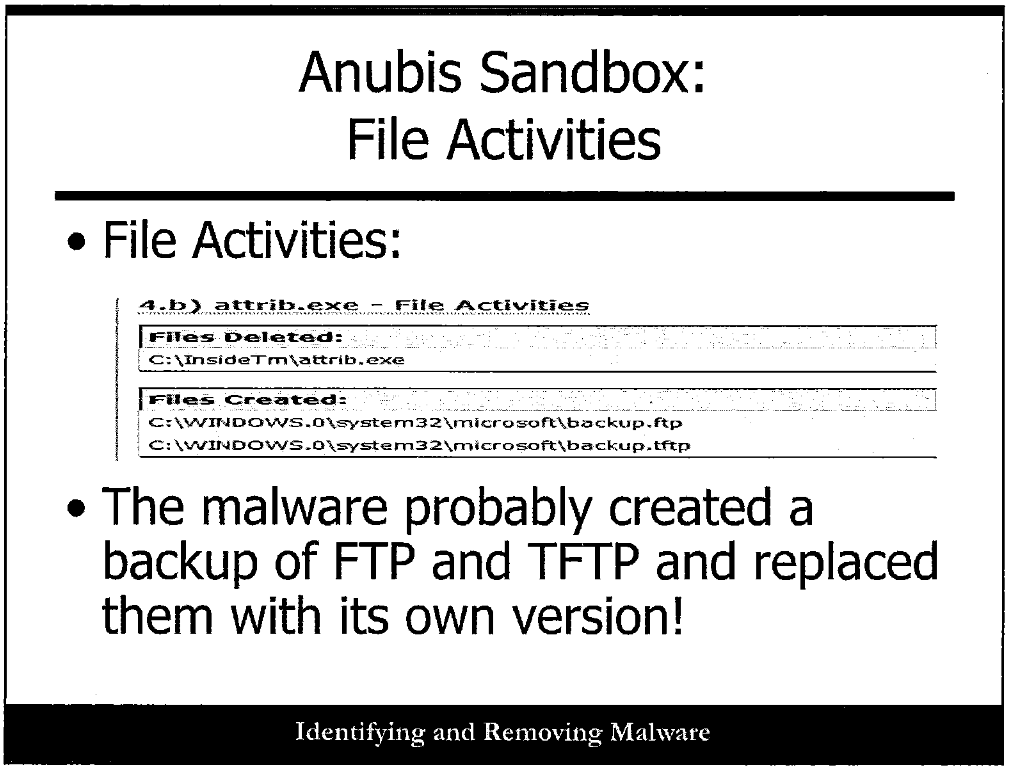
Under network activities, you can identify what kind of malware it is, such as spyware, downloader, Bot, etc.

Under file activities, you can identify the files that were created on the system and then look for them on our own machines!




**Anubis Sandbox: General Information**

The first essential information that we get is from the General Information: section. It says that it runs as a service and not as a regular process. That is good information because when you start to look for it in your system, you will not look for a process but rather for a system service.



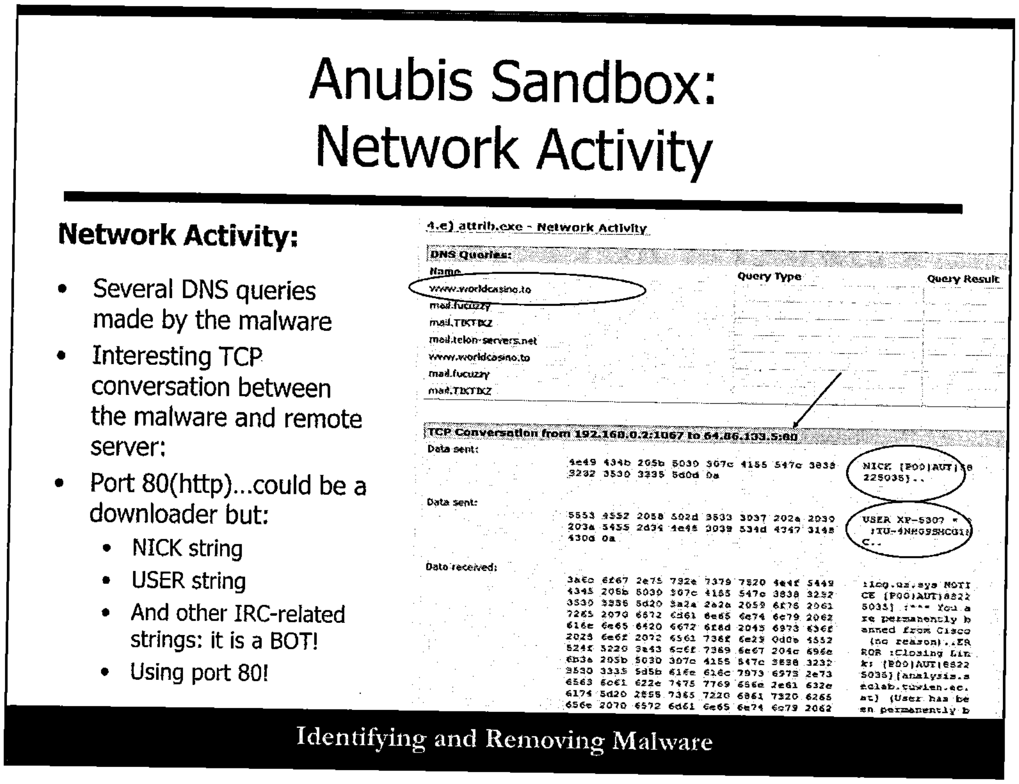

**Anubis Sandbox: File Activities**

Under the File Activities section, you can see interesting information about the file we submitted: attrib.exe

1. It deletes itself from the running directory, and as you already know, it runs as a service.
2. It creates two files on the system:

- Backup.ftp
- Backup.tftp

The two files then replace the existing legitimate files (ftp.exe and tftp.exe) with its own version, which may be specially crafted for the malware's purpose.




**Anubis Sandbox: Network Activity**

The next section that we visit is network activity. This section also reveals some important information for our analysis. It shows several DNS queries that were made by the malicious software and some interesting network traffic. It is a TCP connection from the local host to a remote server on port 80.

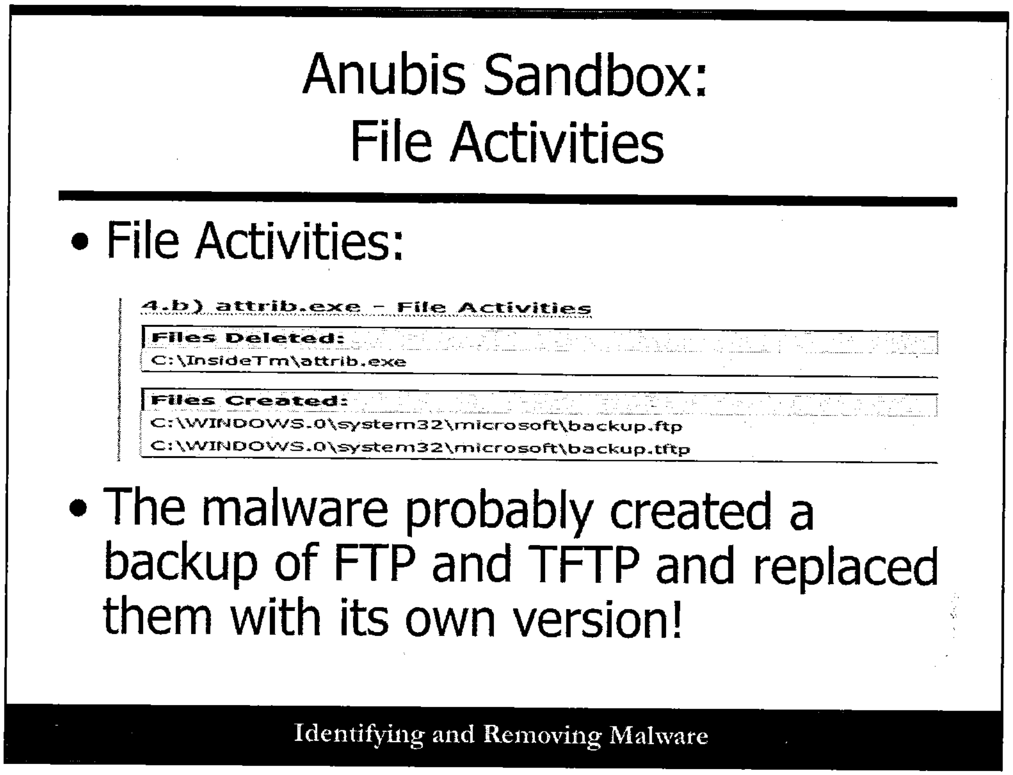
At first it could indicate access to a web server, maybe to download additional software, maybe to get a configuration file, or even to post information from the machine.

The nice thing about Anubis is that it also provides the packet dump of the network traffic in both HEX and ASCII formats. Thanks to that, it is possible to see it is not HTTP traffic but IRC (Internet Relay Chat) traffic.

On the ASCII portion of the packet, can notice the regular Bot/botnet strings:

- NICK
- USER
- Other server-side IRC strings

So now we know what this malware is; it is a BOT that is using port 80.



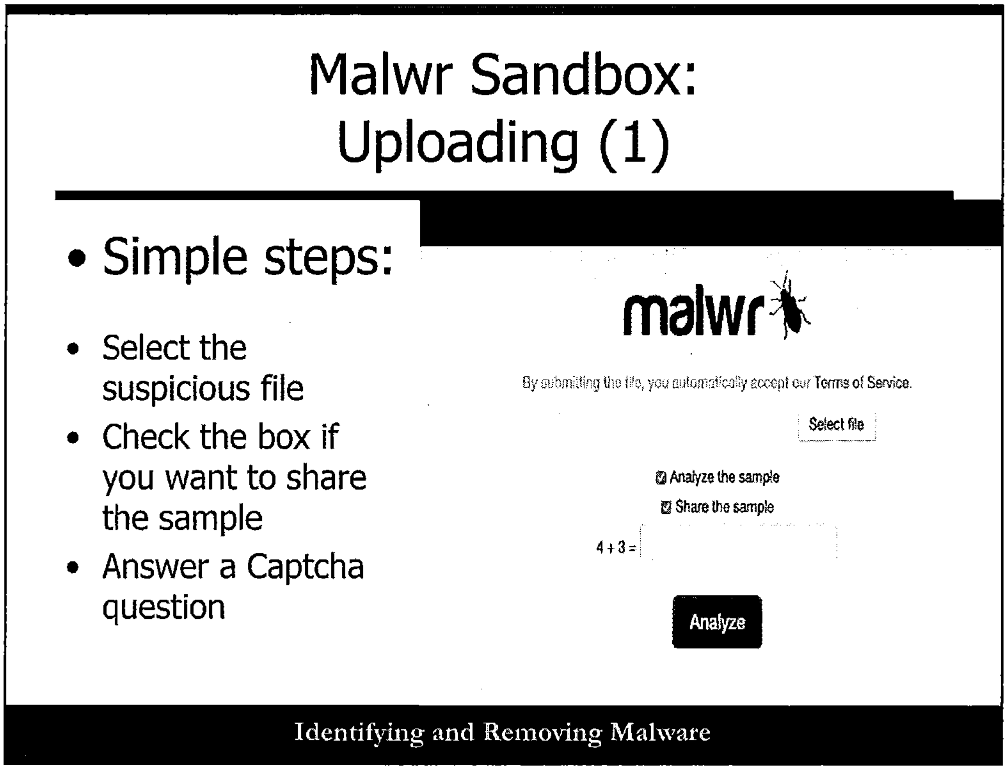

**Anubis Sandbox: File Activities**

Under the File Activities section, you can see interesting information about the file we submitted: attrib.exe

1. It deletes itself from the running directory, and as you already know, it runs as a service.
2. It creates two files on the system:

   - Backup.ftp
   - Backup.tftp

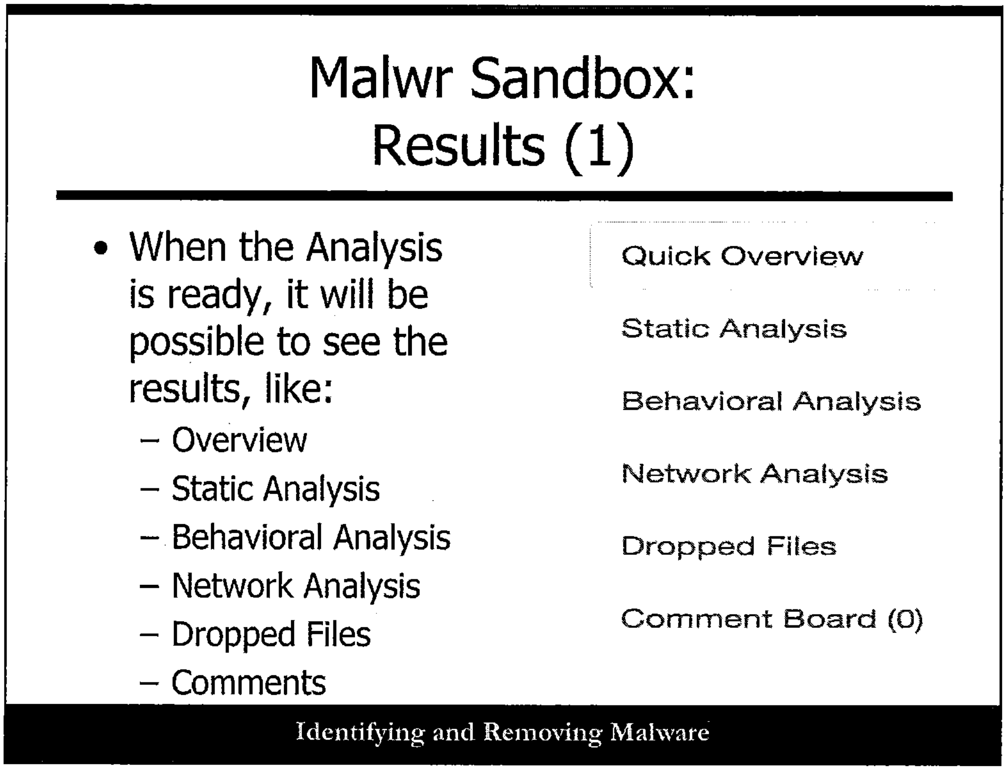
The two files then replace the existing legitimate files (ftp.exe and tftp.exe) with its own version, which may be specially crafted for the malware's purpose.




**GFI Sandbox ThreatTrack- Uploading (1)**

The web interface of the Malwr Sandbox can be accessed at https://malwr.com/submission/.

The process to submit a sample to Malwr is simple. It requires the user to select the file and to answer a captcha question. You also have the option to check a box to indicate you want to share the sample.




**Malwr Sandbox: Uploading (1)**

The Malwr Sandbox provides a nice list of results per sample submitted, such as:

- **Overview**: Shows information about the submission, a summary of the findings, some screen shots captured, and basic network information, such as hosts connected
- **Static Analysis**: Shows information about the file sections, imports. and strings
- **Behavioral Analysis**: Shows information about the processes and Registries involved in the malware execution
- **Network Analysis**: Shows information about the network connections involved during the malware execution
- **Dropped Files**: Shows information about all files dropped by the original file during the malware execution
- **Comments**: Shows any comments that a user may have posted related to the sample

# Malwr Sandbox: Results (2)

The Quick Overview part of the report already gives almost all information needed to understand the threat

**Signatures**

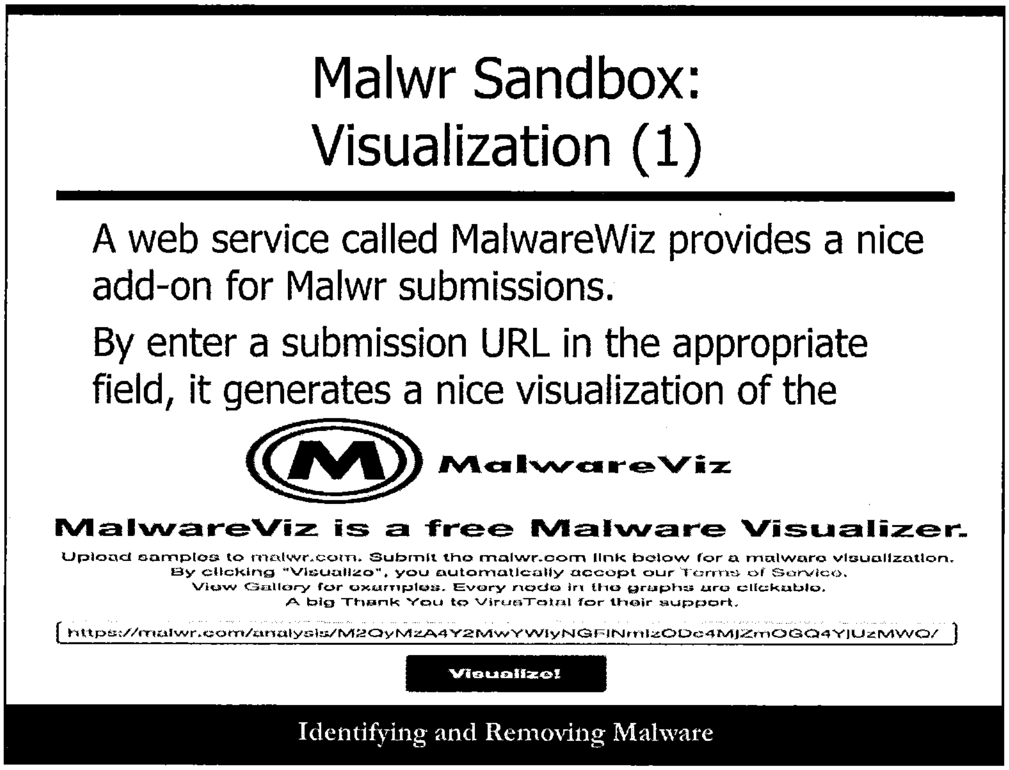
- File has been identified by at least one AntiVirus on VirusTotal as malicious
- The binary likely contains encrypted or compressed data.
- The executable is compressed using UPX
- Tries to unhook Windows functions monitored by Cuckoo
- Collects information to fingerprint the system (MachineGuid, DigitalProductId, SystemBiosDate)
- Creates a slightly modified copy of itself
- Installs itself for autorun at Windows startup

Identifying and Removing Malware

**Malwr Sandbox: Results (2)**

Even if you feel that you don't fully understand other sections of the results, such as the Static Analysis, you can get plenty of good information on the Quick Overview section of the results page.

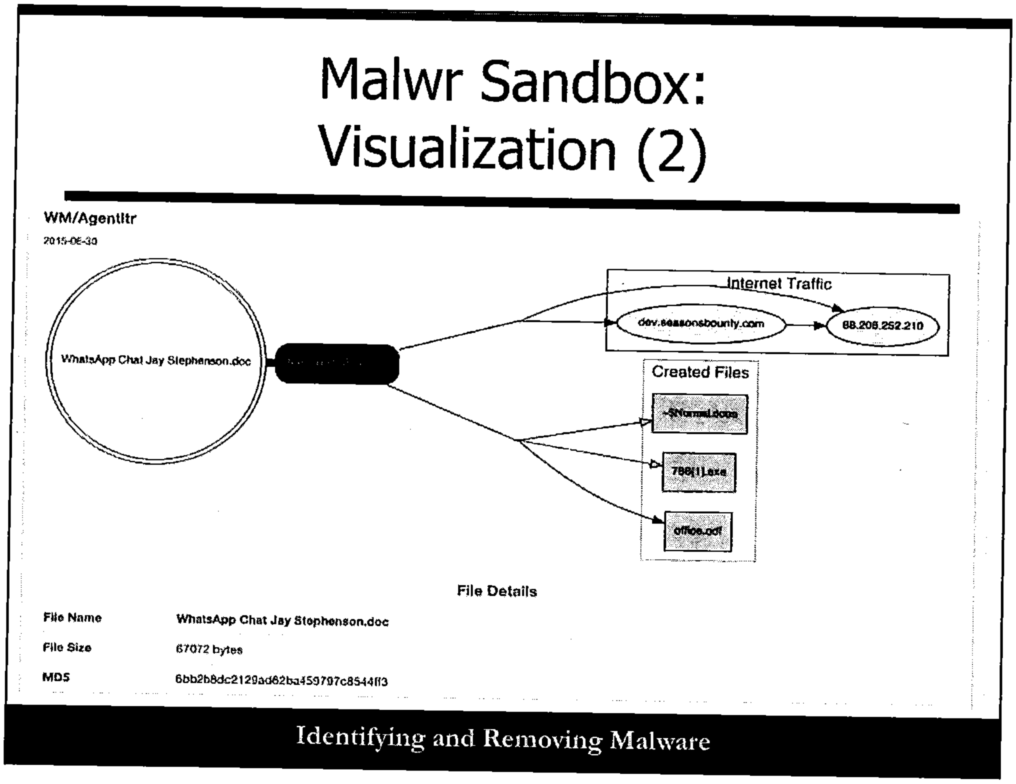
For this example, it tells you that the file was detected by at least one antivirus, that it creates a modified copy of itself, and that it installs itself for autorun at Windows startup, which as we saw previously, it is a bad sign.




**Malwr Sandbox: Visualization (1)**

A web service called MalwareViz recently released an interesting add-on for the submissions made to Malwr Sandbox. When you get to your analysis page, you can copy the analysis URL and go to its website and generate a nice visualization.

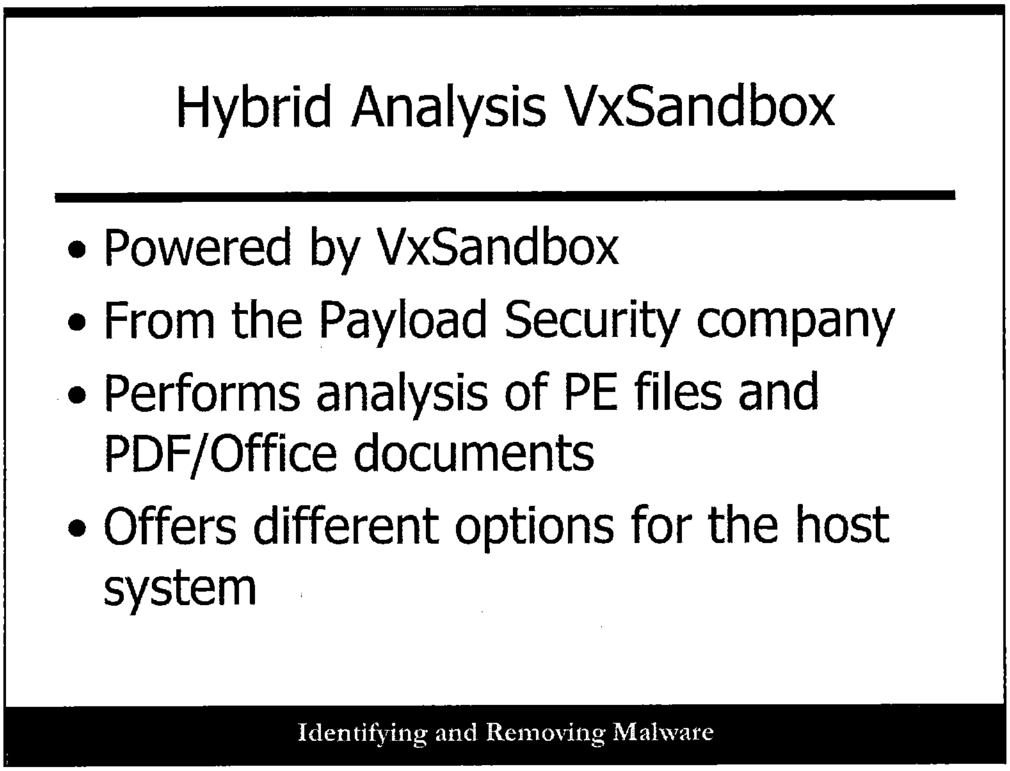
The website is https://www.malwareviz.com/.




### Malwr Sandbox: Visualization (2)

For this example a file called WhatsApp Chat Jay Stephenson.doc was submitted to Malwr. When copying and pasting the URL in Following are a couple of interesting points:

- An Antivirus detects it as WM/Agent!tr.
- At least 28 antiviruses detect it.
- The Document file drops an executable named 786[1].exe.
- A network connection is generated to dev[.]seasonsbounty[.]com, which resolves to IP 88[.]208[.]252[.]210.




**Hybrid Analysis: VxSandbox**

The Hybrid Analysis service is powered by VxSandbox, from the Payload Security company.

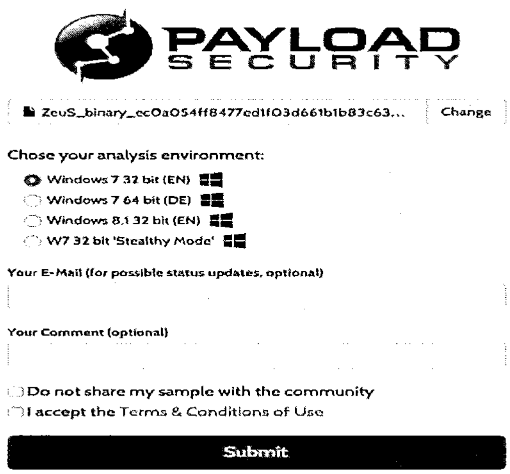
The site is https://www.hybrid-analysis.com/.

It can perform analysis on different types of files, such as PE files (Exe and DLL), and document files, such as PDF and Microsoft Office documents.

It also offers a nice feature to provide different versions of Windows to execute the malware.

# Hybrid Analysis VxSandbox: Submission (1)

- The main page of Hybrid Analysis allows you to:
  - Search past analysis
  - Submit a new file
  - Enter an e-mail to receive the report



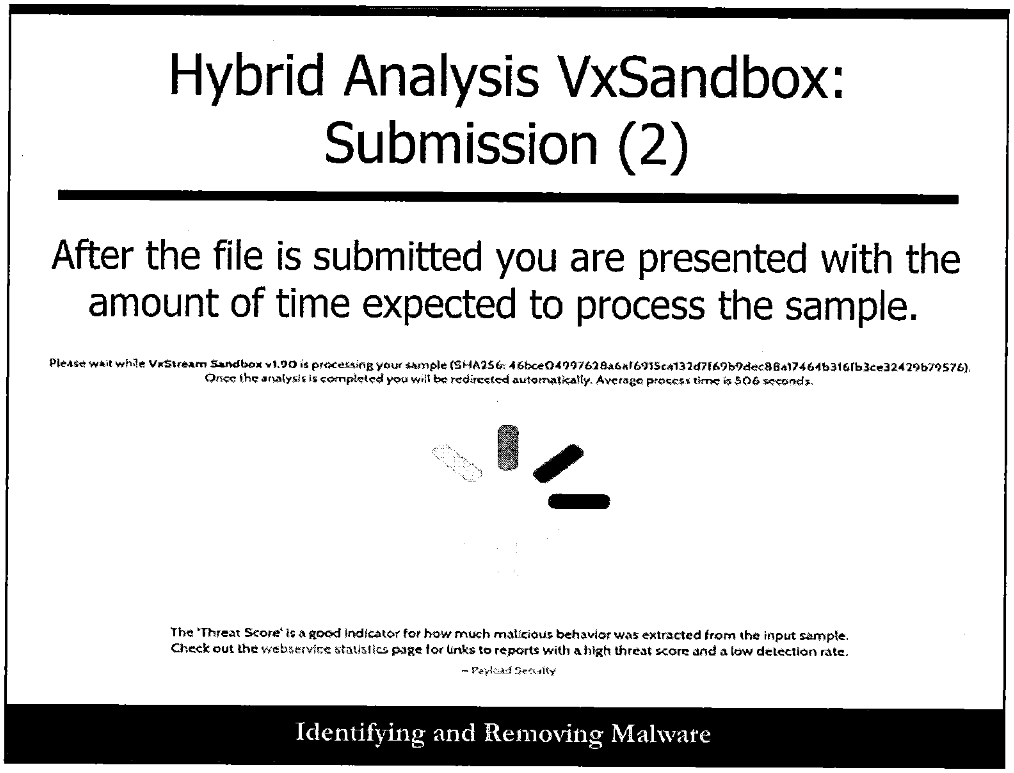

Identifying and Removing Malware

**Hybrid Analysis VxSandbox: Submission (1)**

The usage Hybrid Analysis is quite intuitive. It can be found at https://www.hybrid-analysis.com/.

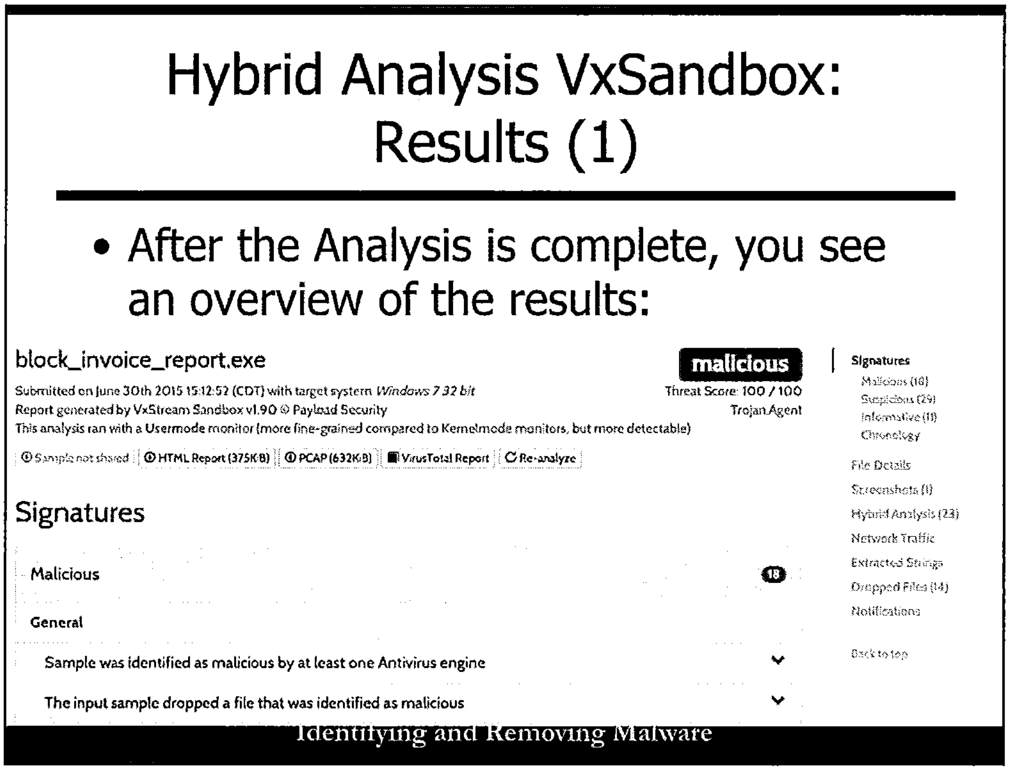
The main sandbox page also offers two other interesting features:

- An option to select the version of Windows system to run each file. Currently it allows you to select Windows 7 32 and 64 bit and Windows 8.1 32 bit.
- An option to search for strings that may be on a report generated by any of the files received, like an IP address, or a domain.




### Hybrid Analysis VxSandbox: Submission (2)

Right after you submit a file, you are presented with information about files in the queue and the estimated time to process your sample. On your example, it shows that the average process time is currently 506 seconds (about 8 minutes).




**Hybrid Analysis: Results (1)**

The result from the analysis provides a comprehensive view of the malware.

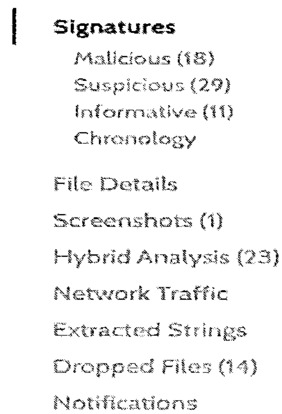
As on other sandbox products, you can have most of the information on the overview/summary page.

In this case, you can see that the system classifies it as Malicious with a ThreatScore of 100 out of 100 (maximum score).

The "Signatures" section contains different information that can help easily identify malicious characteristics on the file and help identify behaviors that you can use to look for the malware on other machines.

# Hybrid Analysis VxSandbox: Results (2)

- The analysis also shows:
  - The detection according AV
  - Threat Score
  - Option to Download the PCAP for analysis
  - Behavior Signatures
  - Screen Shots
  - Network Traffic




Identifying and Removing Malware

**Hybrid Analysis: Results (2)**

The analysis result also provides you with more options to understand the malware capabilities:

- VirusTotal report
- Screen shots
- Static and behavioral analysis
- Network traffic
- Dropped files
- PCAP for analysis

# Wepawet

- Wepawet Analysis
- Developed by the Computer Security Lab on the University of California in Santa Barbara in 2008
- Performs PDF/JavaScript and Flash files analysis
- Results through Web

Identifying and Removing Malware

**Wepawet**

Wepawet Analysis is a fairly new tool on the malware analysis game.

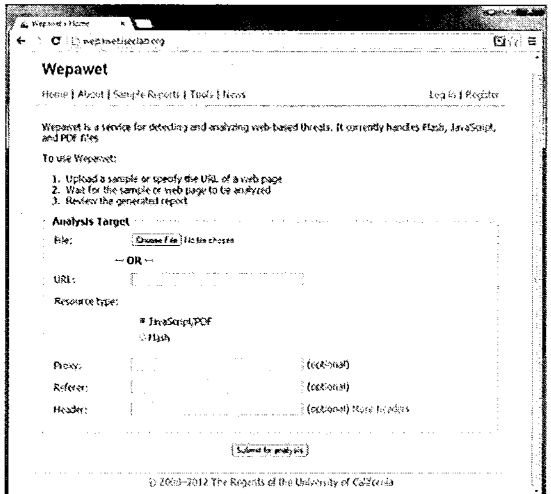
It was developed by the Computer Security Lab at the University of California in Santa Barbara, and it was publicly released in 2008.

The good thing about it is one of the unique free services that performs PDF/JavaScript and Flash analysis.

The results display through the web and not by e-mail.

# Wepawet: Resources

- The main page of Wepawet allows you to:
  - Select the file or URL where the file is
  - Select the file type you want to analyze, being a Flash or Javascript/PDF file




Identifying and Removing Malware

**Wepawet: Resources**

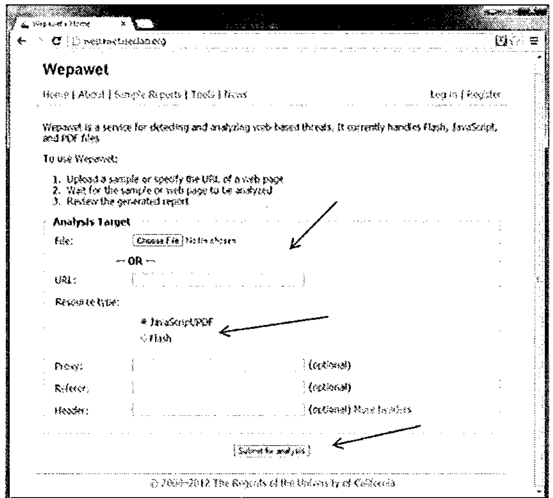
The main page of Wepawet enables you to select if you want it to analyze a file from a URL or to upload a file from your hard drive.

Then, you have to specify if it is a PDF or JavaScript file or if it is a Flash file.

The site is http://wepawet.iseclab.org.

## Wepawet: Uploading (1)

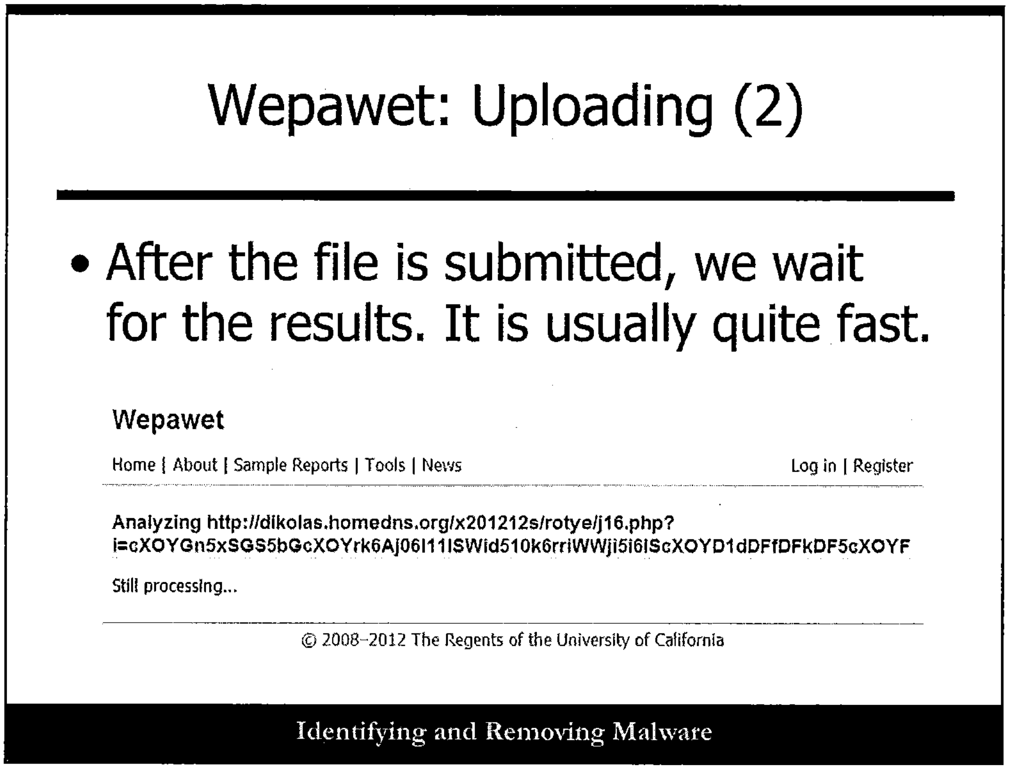
- Simple step:
  - Select the file/URL
  - Select the file type
  - Submit




Identifying and Removing Malware

**Wepawet: Uploading (1)**

The uploading process is quite straightforward, you just have to select the type and click the Submit button.



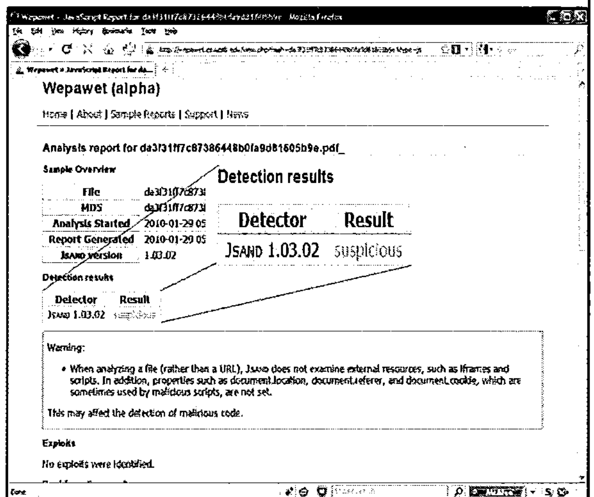

**Wepawet: Uploading (2)**

If everything is okay, the next screen is the one that shows that the file/URL is being analyzed.

It is usually quite fast to process the files, so it will not take much time on this screen and will redirect to the analysis page.

# Wepawet: Analysis (1)

- The Analysis is ready and shows:
  - Basic results as suspicious or not
  - Exploits-related
  - Deobfuscation
  - Network Activity
  - Shellcode
  - URL



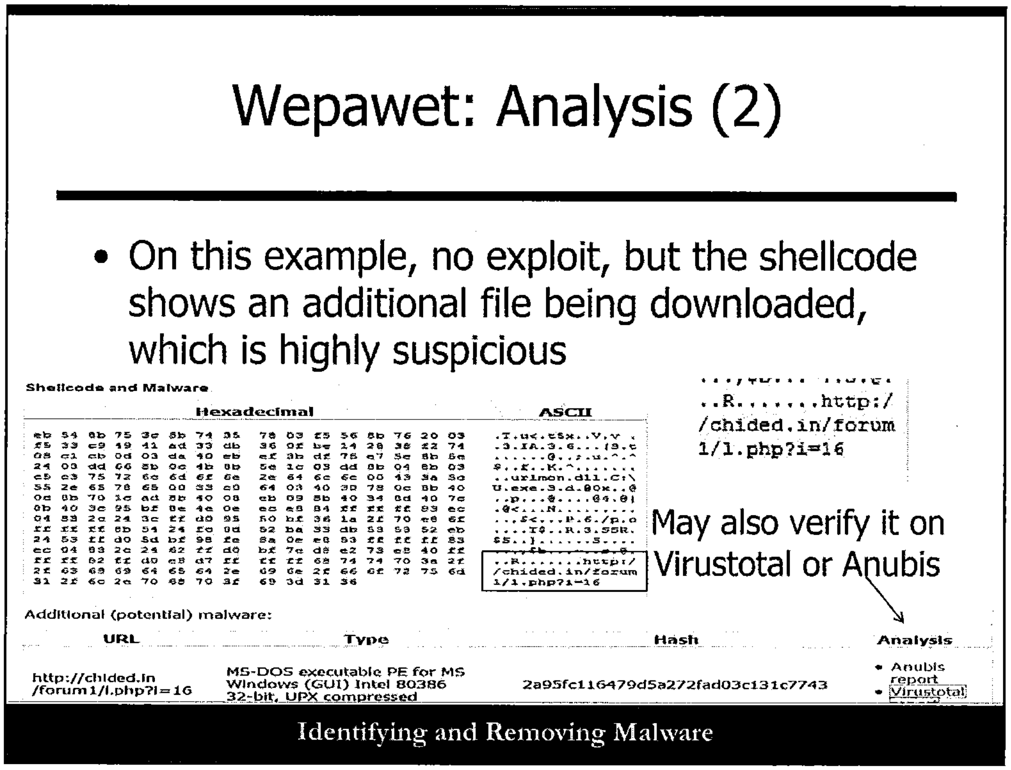

Identifying and Removing Malware

**Wepawet: Analysis (1)**

The analysis shows:

- Basic results, as Suspicious or Malicious
- Any exploits found on the file
- Deobfuscates any part that includes obfuscated strings
- Any network activity
- Shellcode that may be present on the file
- URLs found during the analysis

This example is from a malicious PDF file. The basic result shows it as Suspicious.




**Wepawet: Analysis (2)**

The slide shows the continuation of the analysis of the same PDF file.

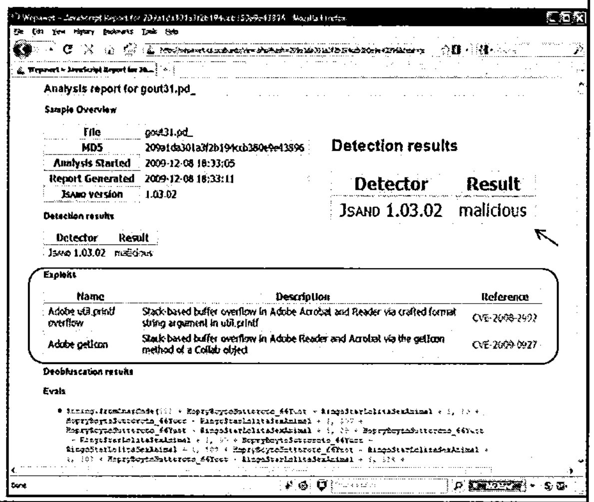
It shows that it found a URL present on this file that can lead to another file, which is an MS-DOS executable PE for Windows.

It also shows that it was compressed with the UPX packer.

Now, you would have the option to use that URL and get the file, but it already did it. It has also sent it to VirusTotal to check how the antivirus vendors are detecting it and even provides a direct link for the analysis.

# Wepawet: Analysis (3)

- This second example shows a PDF file with two exploits being used, which definitely makes it malicious




Identifying and Removing Malware

**Wepawet Analysis (3)**

Another example from a malicious PDF file sent to Wepawet.

This time, the basic analysis shows it as Malicious.

It also shows that it found two PDF exploits on that file.

- One from 2008 (with CVE number 2008-2992) called Adobe util.printf
- One from 2009 (CVE number 2009-0927) called Adobe GetIcon

# Threat Expert

- Created by PCTools
- Acquired by Symantec in 2008
- Offers a detailed report

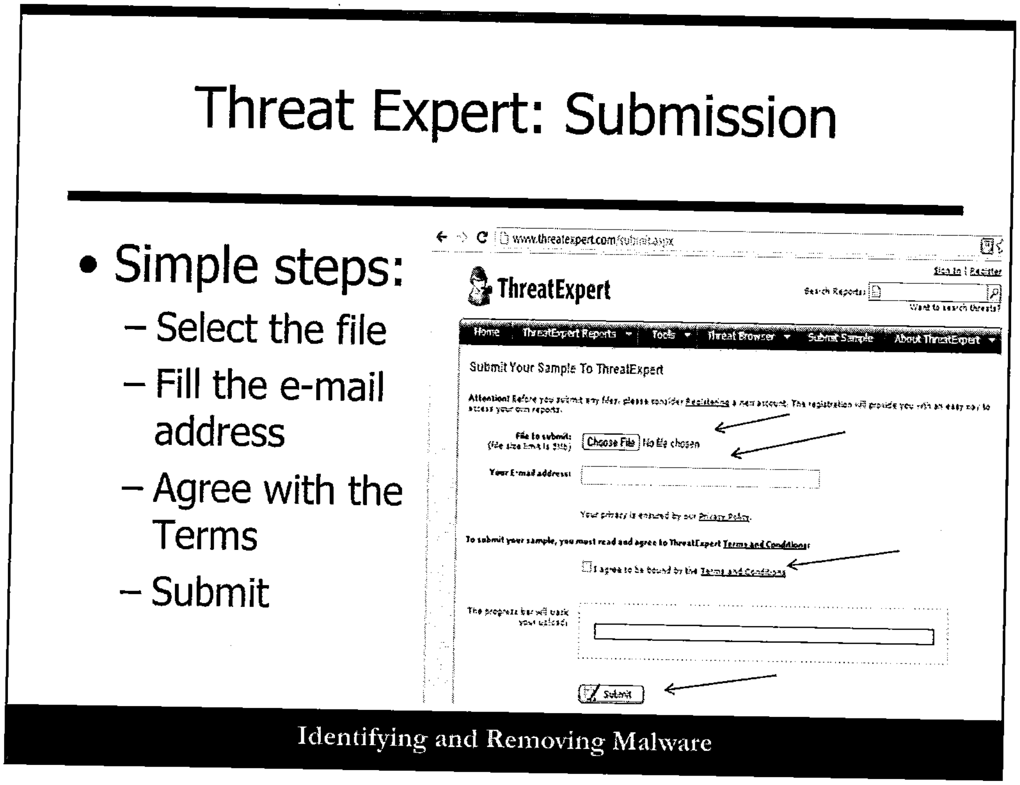
Identifying and Removing Malware

**Threat Expert**

Threat Expert is another public/online sandbox that offers a detailed report with the analysis performed.

It was created by the former security company PCTools, that was acquired by Symantec in 2008.

It allows you to submit and see the results online, and if you create an account, you can track your submissions online.




**Threat Expert: Submission**

The submission process is simple. The URL is http://www.threatexpert.com/submit.aspx.

When there, the user just has to select the file, fill in the e-mail address, and agree with the Terms and Conditions.

# Threat Expert: Results

- The results contains:
  - Static info, Summary, Network and System modifications

**ThreatExpert**

Visit ThreatExpert web site | Close Report

**Submission Summary:**

- Submission details:
  - Submission received: 5 October 2012, 09:25:57
  - Processing time: 9 min 7 sec
  - Submitted sample:
    - File MD5: 0x6B375FD700CF95DAD00EC1B432F94670
    - File SHA-1: 0x408D5A3F4A6D9543EDD9DEB7730A10F17E0B8FDC
    - Filesize: 475,136 bytes
    - Alias:

Identifying and Removing Malware

**Threat Expert: Results**

The Threat Expert report page contains a lot of useful information that can be used to search for common IOCs (Indicators of Compromise) in your environment:

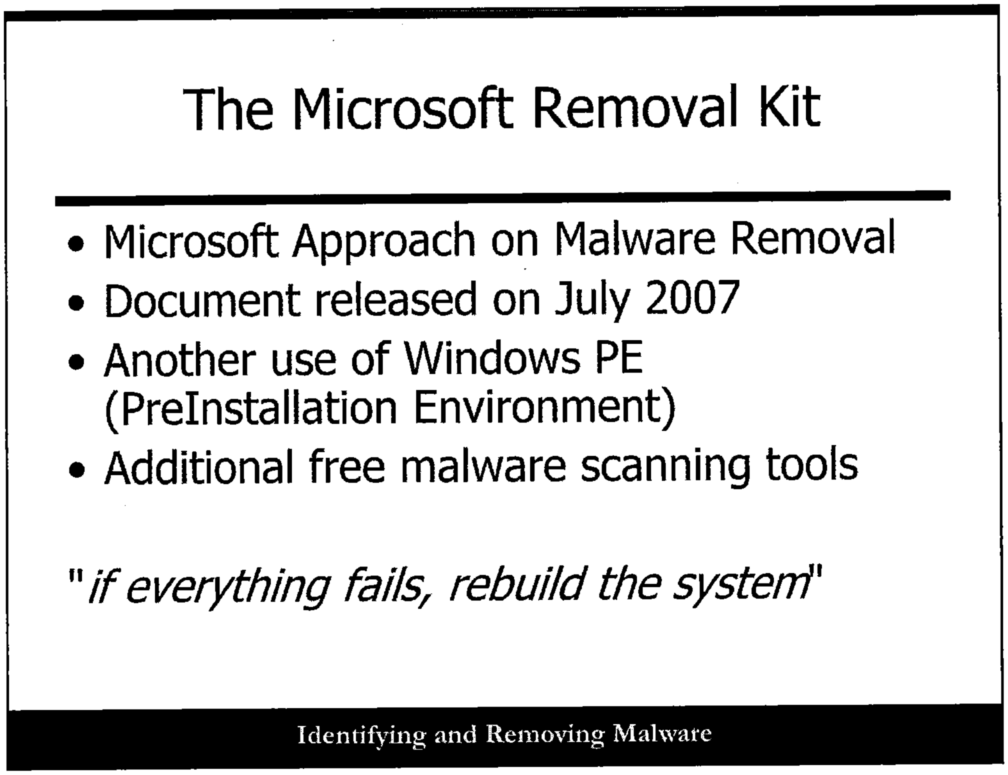
- Summary
- AV Detection
- Network Connections
- File Created/Modified
- Possible Country of Origin

Identifying and Removing Malware

The Microsoft Approach
MS Malware Removal
Starter Kit

Identifying and Removing Malware

This page intentionally left blank.




**The Microsoft Removal Kit**

The Microsoft Malware Removal Kit is a document, released in 2007, that explains the basics of malware and shows another use of the Windows PE (PreInstallation Environment). By adding some free malware scanning tools like antivirus and antispyware, it creates a rescue bootable CD-ROM.

As we will see, all the analysis done in the system using the Windows PE CD-ROM is considered an offline analysis because the real windows machine is off and we are just checking the hard-disk for malware traces.

Of course, it is another attempt to get rid of malware from the system, but removing files in an offline system may cause damage to your OS, so we will also learn what to do when everything fails.

# The Microsoft Document

- The document is split into five sections:
  - Overview
  - Planning Your Response
  - How to Determine if You Have a Problem
  - Dealing with an Infection
  - Summary

Identifying and Removing Malware

**The Microsoft Document**

The Microsoft Malware Removal Kit is a document that offers the following sections:

- **Overview**: This is the phase that resumes what a malware is and how it can get into the machine.
- **Planning Your Response**: This section shows an example of a basic response plan, like:

1. "A staff member calls an in-house support resource after noticing something strange appears on her computer screen."
2. "The support resource checks the computer and calls a support number."
3. "A support technician responds to complete a short diagnostic test, and then either cleans or rebuilds the system depending on the severity of the problem."

SANS offers a nice course called Hacker Techniques, Exploits & Incident Handling – SEC 504, the first part of the course looks at the Incident Handling Step-by-Step model.

More information can be found at http://www.sans.org/training/description.php?tid=243.

This section also explains how to build a special Windows PE CD-ROM to use for offline scanning.

- **How to Determine if You Have a Problem**: This section explains how to check for signs that your computer is infected with malicious software.
- **Dealing with an Infection**: This section explains the need of using online and offline scanning tools, and the usage of the Windows PE CD-ROM built in section "Planning Your Response."
- **Summary**: This is a short explanation about the needs of a Malware Removal Kit document.

# Our Approach (1)

- In the Planning Your Response phase, you:
  - Gather information from the machine
    - We already know how to do that
  - Do a live investigation
    - We also know how to perform these actions
  - Create a special Windows PE CD-ROM for offline investigation
    - We will focus here
- We already have knowledge about live, or online, investigation

Identifying and Removing Malware

**Our Approach (1)**

Our approach is based on the Microsoft document on Malware Removal Kit. We focus on Section 2 ("Planning Your Response") and Section 4 ("Dealing with Infection"). This is because Section 2 explains how to perform both Live and Offline Analysis, building the special Windows PE CD-ROM. Section 4 explains the need to use both online and offline scanning.

In this course, you have already learned how to identify and remove malware from Live (or online) machines and why the focus now is on offline analysis.

# Our Approach (2)

Our approach is to adapt the MS view in a more technical way to deal with offline investigation!

- What we will see:
  - How to include additional tools we will put in the bootable live Windows PE CD-ROM
  - Build a Windows PE CD-ROM with offline malware analysis tools
  - Run them on a system!

Identifying and Removing Malware

**Our Approach (2)**

Because we focus on the offline analysis part of the Microsoft document, we adapt it to our needs by including additional tools on the bootable CD-ROM, and how to actually build the CD-ROM.

## Why Offline Analysis (1)

- You will be sure that no malware will be active, hidden, or not
- You will be able to remove/delete malware components that install as critical components, preventing them to be removed when the system is on, such as:
  - Drivers
    - Some rootkits .sys files
  - DLLs
    - Some DLLs injected into running processes

Identifying and Removing Malware

**Why Offline Analysis (1)**

Offline Analysis is an important phase when trying to identify and remove malware because some malware can use stealthy techniques.

When doing offline analysis you can remove/delete malware components that are not possible when the system is on because of some techniques used by the malware. Because the original system is off, the techniques based on kernel hooks or some call interception will not work, so you can see and remove the component.

Some examples of such components are:

- **Drivers**: Some rootkits use .sys driver files, so even if you can see it, you cannot remove it from live systems.
- **DLLs**: Some DLLs injected on processes and services such as Winlogon.exe and Svchost.exe may be too hard to remove on online systems but quite simple when offline.

# Why Offline Analysis (2)

- When performing offline analysis, you can run security applications that may be disabled to run by malware/rootkits that you were unable to find/remove, such as:
  - Antivirus
  - Anti-SpyWare
- In this way, you have a high probability to find and safely remove them

Identifying and Removing Malware

**Why Offline Analysis (2)**

Another reason to perform offline scanning is some malware can prevent security tools from running and consequently finding the malware, such as antivirus and antispyware software, so when offline you can bypass this restriction and run some of the tools which included on the Live CD-ROM.

# Building the Removal Kit (1)

- First Step:
  - Download the component needed to build our Live CD-ROM:
    - Windows Automated Installation Kit (AIK)
  - Burn a DVD with the image downloaded

Identifying and Removing Malware

**Building the Removal Kit (1)**

The first thing you need to know before building the kit is you need a blank DVD and a blank CD. The reason is that to start with the process, you have to download a 900mb image file, the Windows Automated Installation Kit, and burn it to the DVD blank media.

When the DVD burning process is ready, you can re-insert the DVD into the reader.

You can download it at:

Pre-reqs:

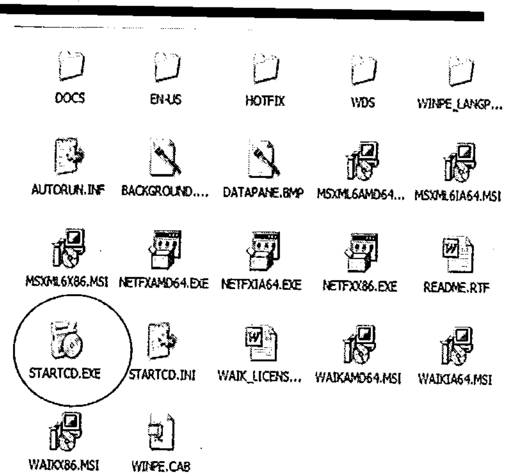
- https://technet.microsoft.com/en-us/library/dn293200.aspx
- http://go.microsoft.com/fwlink/?LinkId=76343
- http://go.microsoft.com/fwlink/?LinkId=79533

AIK:

- http://www.microsoft.com/en-us/download/details.aspx?id=5753

# Building the Removal Kit (2)

- You should see the following folders on the newly created DVD
- Run StartCd.exe from the DVD and install the Automated Installation Kit (needed to build our PE CD-ROM)




Identifying and Removing Malware

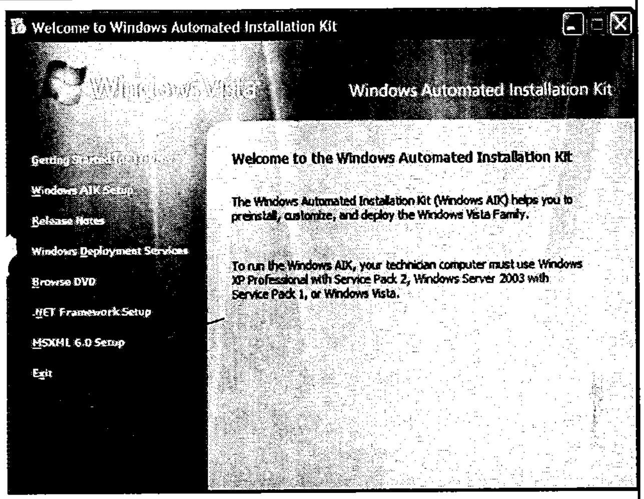
**Building the Removal Kit (2)**

When you re-insert the DVD in the drive, you can open it with Windows Explorer. The screen shot on the slide shows the contents from the DVD.

To install the Windows Automated Installation Kit, you need to double-click the StartCD.exe file.

# Building the Removal Kit (3)

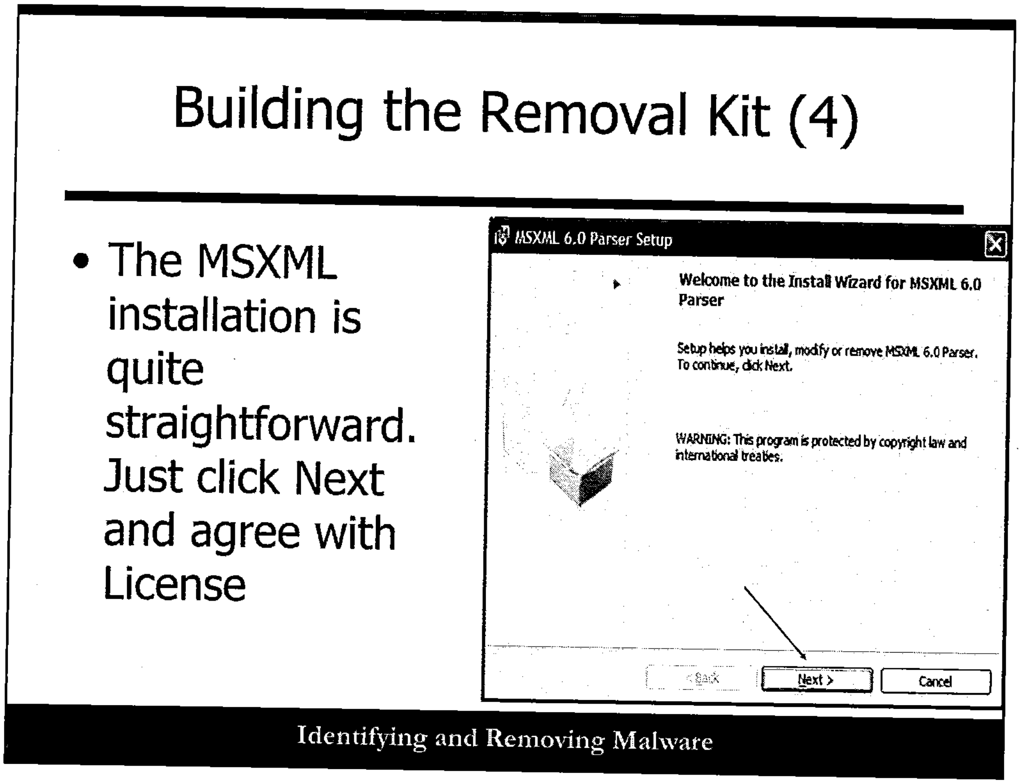
- We need to install the MSXML 6.0 first, so select the MSXML 6.0 Setup option




Identifying and Removing Malware

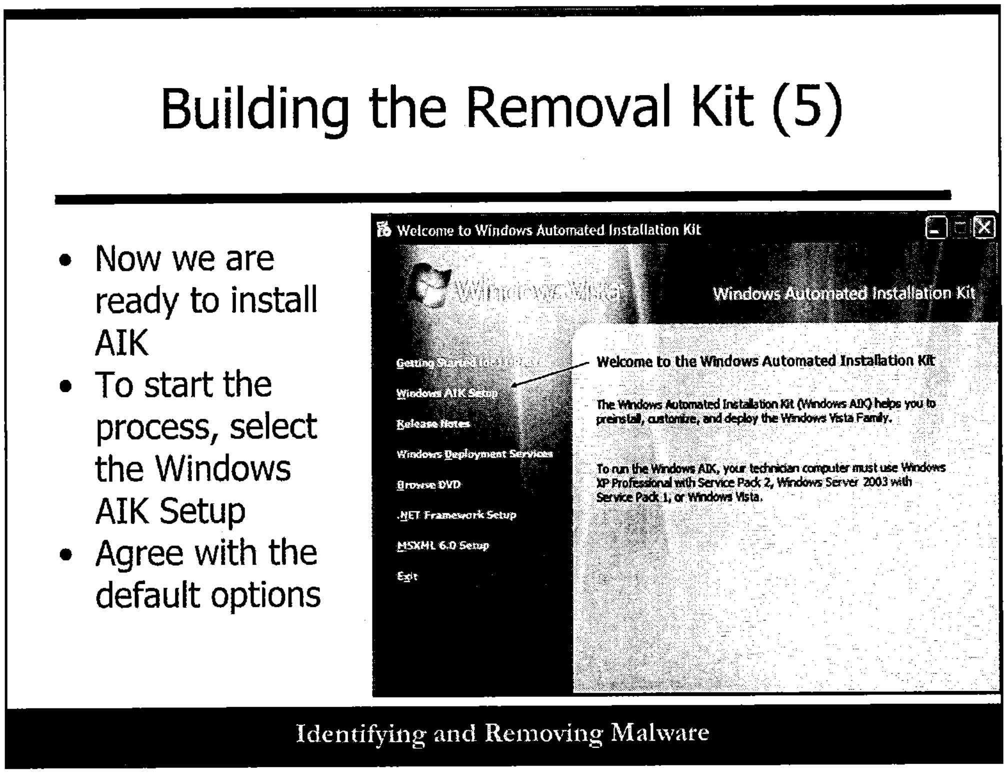
**Building the Removal Kit (3)**

When you double-click the StartCD, another window appears with some option. The first thing you need to do is to install the MSXML by selecting the MSXML 6.0 Setup.




**Building the Removal Kit (4)**

The MSXML installation is quite straightforward. To install it, just click the Next button and agree with the License, and the installation will be ready soon.



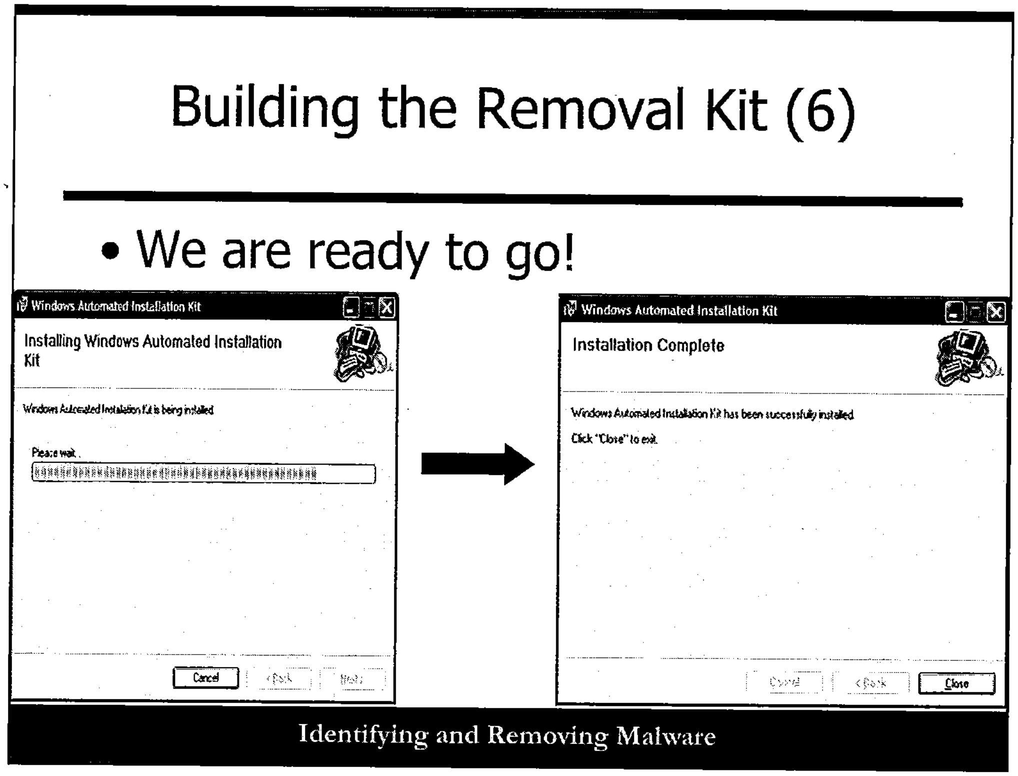

**Building the Removal Kit (5)**

**AIK**

Because we've already installed the MSXML, we are now ready to install the actual AIK.

We just have to select the Windows AIK setup option in the same way we chose the MSXML 6.0 Setup.

After that, we agree with the licensing and default options.



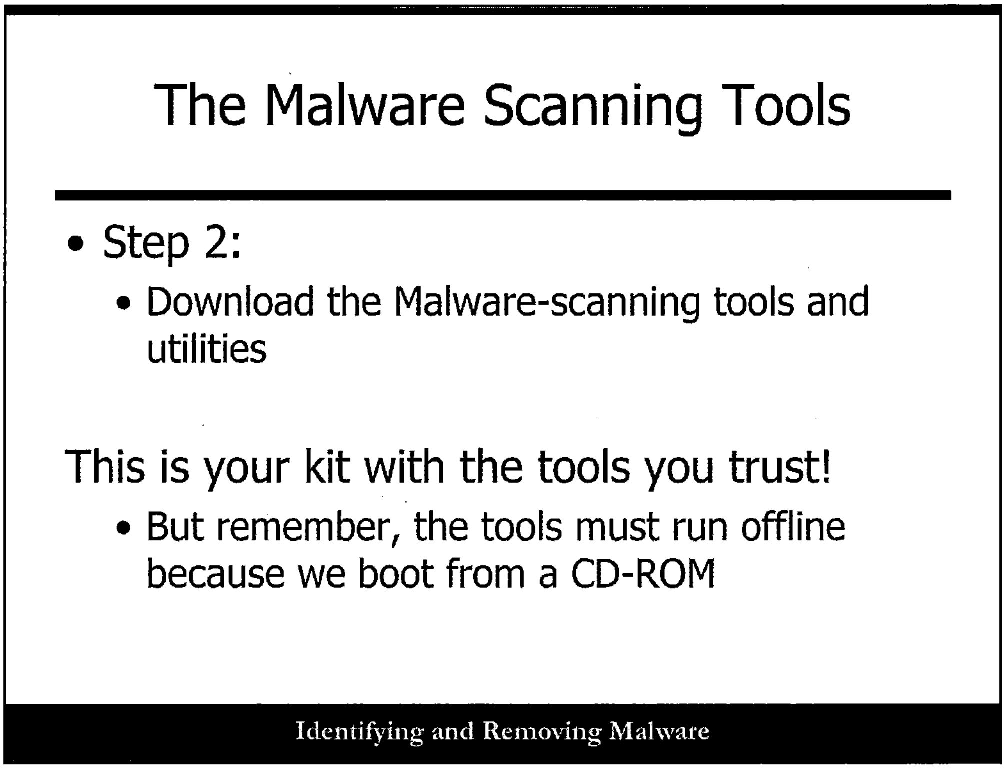

**Building the Removal Kit (6)**

The installation process is quite simple, and after we accept the default options, it will install quite quickly.

When ready, it gives you the message:

"Windows Automated Installation Kit has been successfully installed"

Just click the Close button for now.




**The Malware Scanning Tools**

Step 2 is to download the malware scanning tools and utilities. This will be used to build your tool kit, which you will use when doing an offline scanning.

We can separate it into two different tool kit sections:

- The tools recommended by Microsoft
- The additional tools that you trust and know how to use

When composing your personal tool kit, remember that all tools must be able to run offline.

## MS Suggested Tools

- Tools recommended by Microsoft:
  - avast! Virus Cleaner from Alwil Software
  - McAfee AVERT Stinger, a stand-alone virus scanner from McAfee
  - Malicious Software Removal Tool from Microsoft
  - Spybot: Search & Destroy from Spybot Search and Destroy
  - Drive Manager from the Freeware Utilities by Alex Nolan website
  - System Spec from the Freeware Utilities by Alex Nolan

Identifying and Removing Malware

**MS Suggested Tools**

Microsoft recommends its own selection of tools to build the tool kit to be used on the offline scanning:

avast! Virus Cleaner from Alwil Software.

- It is a special standalone version from the Avast Anti-Virus that is aimed to remove selected viruses from the machine.
- According the Avast Website: "avast! Virus Cleaner is available free for every user. This tool will help you remove selected worm infections from your computer."
- It can be downloaded for free at http://www.avast.com/eng/down_cleaner.html.

McAfee AVERT Stinger, a standalone virus scanner from McAfee.

- It is another standalone tool to remove selected malware, according McAfee's website:
- "Stinger is a stand-alone utility used to detect and remove specific viruses. It is not a substitute for full anti-virus protection, but rather a tool to assist administrators and users when dealing with an infected system."
- It can be downloaded for free at http://vil.nai.com/vil/stinger/.

Malicious Software Removal Tool from Microsoft.

- The Microsoft version of the standalone virus remover is the Microsoft Software Removal tool. It also checks for specific viruses on the machine.

- "The Microsoft Windows Malicious Software Removal Tool checks computers running Windows XP, Windows 2000, and Windows Server 2003 for infections by specific, prevalent malicioussoftware—including Blaster, Sasser, and Mydoom—and helps remove any infection found. When the detection and removal process is complete, the tool displays a report describing the outcome, including which, if any, malicious software was detected and removed."
- It can be downloaded for free at http://www.microsoft.com/security/malwareremove/default.mspx.

Spybot: Search & Destroy from Spybot Search and Destroy.

- Spyboy SD is a commercial tool, which offers a free version of its antispyware product. The disadvantage of the usage of Spybot is that you have to install it first on the machine that you will do the offline scan, so it can download the updated signature database. Then, when booting with our special Windows PE, Spybot will use the downloaded signature database file to scan the system.
- It can be downloaded for free at http://www.spybot.info/en/download/index.html.

Drive Manager from the Freeware Utilities by Alex Nolan website.

- This tool can be used to get information about the storage devices connected to the system.
- It can be downloaded for free at http://www.alexnolan.net/software/driveman.htm.

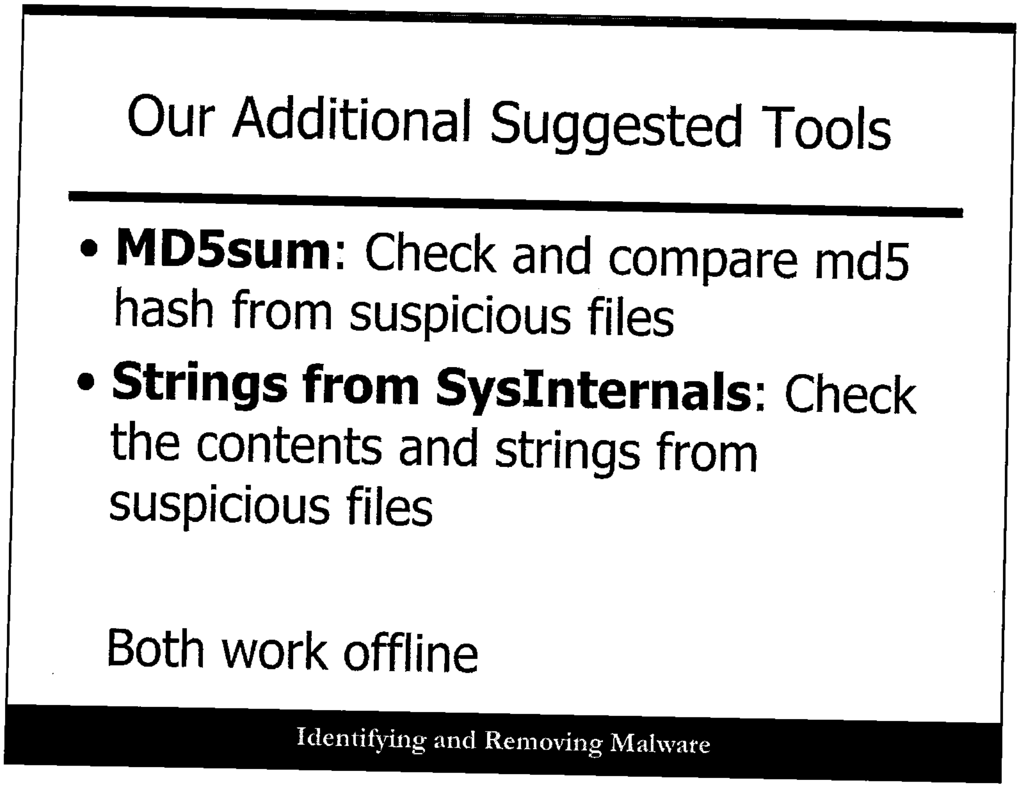
System Spec from the Freeware Utilities by Alex Nolan

- This tool can be used to get system information from the machine you are scanning. It gives most of the information you can get from Computer Management when the system is online.
- It can be downloaded for free at http://www.alexnolan.net/software/sysspec.htm.

Note: Download these tools to a single directory, to make it easy for our next step, when we will create our WinPE CD-ROM.

For clarity, following is the complete list of URLs:

- http://www.avast.com/eng/down_cleaner.html
- http://vil.nai.com/vil/stinger/
- http://www.microsoft.com/security/malwareremove/default.mspx
- http://www.spybot.info/en/download/index.html
- http://www.alexnolan.net/software/driveman.htm
- http://www.alexnolan.net/software/sysspec.htm




**Our Additional Suggested Tools**

As stated before, you can also include your own set of tools (if they work offline). Our additional suggested tools are

- **MD5sum**: Can be used to generate md5 hash from the file, so you can compare it to a clean file. It can be downloaded for free at http://www.etree.org/cgi bin/counter.cgi/software/md5sum.exe.
- **MS SysInternals Strings**: You can use to generate strings from suspicious files and try to identify packers and malware known strings, like from bots, for example. It can be downloaded for free at http://download.sysinternals.com/files/Strings.zip. In addition, you may want to download the RAR extraction tool from http://www.rarlabs.com/rar/rarx371.exe.

**Note**: When you download the strings file, it will be zipped. You will have to extract it to a folder. The .exe file is the one you will move to the tools directory when creating the WinPE CD-ROM.

# Building the Removal Kit

- Step 1: Download the Components
- Step 2: Download the tools
- Step 3: Create the Malware Removal Starter Kit CD-ROM
  - These are actually 13 sub-steps to run (described on your notes!)

Identifying and Removing Malware

**Building the Removal Kit**

To start the following steps, you must be logged in with an Administrator privileged account.
The substeps are strongly based on Microsoft Document, with our comments and examples.

1. Click Start, Programs, Microsoft Windows AIK, and then Windows PE Tools Command Prompt.

If you are running Windows Vista on your computer, right-click Windows PE Tools Command Prompt, click Run as administrator, and then click Continue.

2. At the command prompt, type the following and then press ENTER to create a copy of the x86 image of Windows PE and set up a working folder directory on your computer:

    ***copype x86 c:\WinPE***

If successful, you should see the following message:

Success

*Updating path to include peimg, oscdimg, imagex*

*C:\Program Files\Windows AIK\Tools\PETools*
*C:\Program Files\Windows AIK\Tools\PETools\..\x86*

3. If you are not already there, go to the newly created directory:

```
Cd c:\winpe
```

4. At the command prompt in the new directory c:\WinPE, type the following and then press Enter to mount the WinPE.wim image so that you can change it:

```
imagex /mountrw winpe.wim 1 c:\WinPE\Mount
```

You should see the following message:

```
C:\winpe>imagex /mountrw winpe.wim 1 c:\WinPE\Mount
```

*ImageX Tool for Windows*
*Copyright (C) Microsoft Corp. 1981-2005. All rights reserved.*

*Mounting (RW): [C:\winpe\winpe.wim, 1] ->*
*[c:\WinPE\Mount]*

*Successfully mounted image (RW).*

5. At the command prompt, type the following and then press Enter to access the following Registry subkey:

(The font size may break into two lines, but it is just one command line.)

```
reg load HKLM\_WinPE_SYSTEM
c:\WinPE\Mount\windows\system32\config\system
```

6. At the command prompt, type the following and then press Enter to create a 96MB disk cache of RAM:

(The font size may break into two lines, but it is just one command line.)

```
reg add HKLM\_WinPE_SYSTEM\ControlSet001\Services\FBWF /v
WinPECacheThreshold /t REG_DWORD /d 96 /f
```

7. At the command prompt, type the following and then press Enter to exit this Registry key:

```
reg unload HKLM\_WinPE_SYSTEM
```

8. Create a directory for the malware-scanning tools under the Mount folder. (For example, you could use the name "Tools" for this folder.)

```
mkdir c:\WinPE\mount\Tools
```

9. Copy the tool files that you downloaded in Task 2 to the tools directory that you just created. Example:

```
copy <tools from the Task 2 directory> c:\WinPE\mount\Tools
```

**You can also use Windows Explorer to do this task!**

10. At the command prompt, type the following, press Enter, type Yes, and press ENTER again to continue the process:

```
peimg /prep c:\WinPE\Mount
```

You should see the following message on your system:

*Preinstallation Environment Image Setup Tool for Windows*
*Copyright (C) Microsoft Corporation. All rights reserved.*

*The /prep command will permanently modify a Windows PE image, so that it can no longer be serviced. This means that operations including:*

- *Installing or uninstalling optional features*
- *Applying hotfixes or other servicing packages*
- *Installing language packs*

*Will not be possible on the prepared image.*

*To continue, enter "yes". Any other input will exit the program.*

*Continue? Yes*
*[==========================100,0%==========================]*
*PEIMG completed the operation successfully.*

11. At the command prompt, type the following and then press Enter to save your changes:

```
imagex /unmount c:\WinPE\Mount /commit
```

You should see the following message on your system:

*ImageX Tool for Windows*
*Copyright (C) Microsoft Corp. 1981-2005. All rights reserved.*

*Unmounting: [c:\WinPE\Mount]...*

*Successfully unmounted image.*

12. At the command prompt, copy the following, press Enter, and then type Yes to overwrite the existing file:

```
copy c:\WinPE\WinPE.wim c:\winpe\ISO\sources\boot.wim
```

13. At the command prompt, type the following and then press Enter to create an .iso file of the Windows PE image:

(The font size may break into two lines, but it is just one command line.)

```
oscdimg -n -bc:\WinPE\etfsboot.com c:\WinPE\ISO
c:\WinPE\WinPE_Tools.iso
```

The message indicates that it was successful. Please note that the number of files may vary depending on the tools you include. In my case I didn't include Spybot Search & Destroy because it would require it to be installed on the machine; we will do the offline analysis and in most cases we will not be able to install additional software in the infected machine.

*OSCDIMG 2.45 CD-ROM and DVD-ROM Premastering Utility*
*Copyright (C) Microsoft, 1993-2000. All rights reserved.*
*For Microsoft internal use only.*

*Scanning source tree complete (17 files in 8 directories)*

*Computing directory information complete*

*Image file is 205975552 bytes*

*Writing 17 files in 8 directories to c:\WinPE\WinPE_Tools.iso*

*100% complete*

*Final image file is 205975552 bytes*

*Done.*

14. The previous step created an ISO image for us. We will burn the .iso file located at c:\WinPE\WinPE_Tools.iso to a CD-ROM.

# Booting with Windows PE

- Step 4: Use the Malware Removal Starter Kit to scan your computer
  - It is time to boot your system with the newly created Windows PE CD-ROM
  - Ensure that your BIOS is set to boot from CD-ROM!

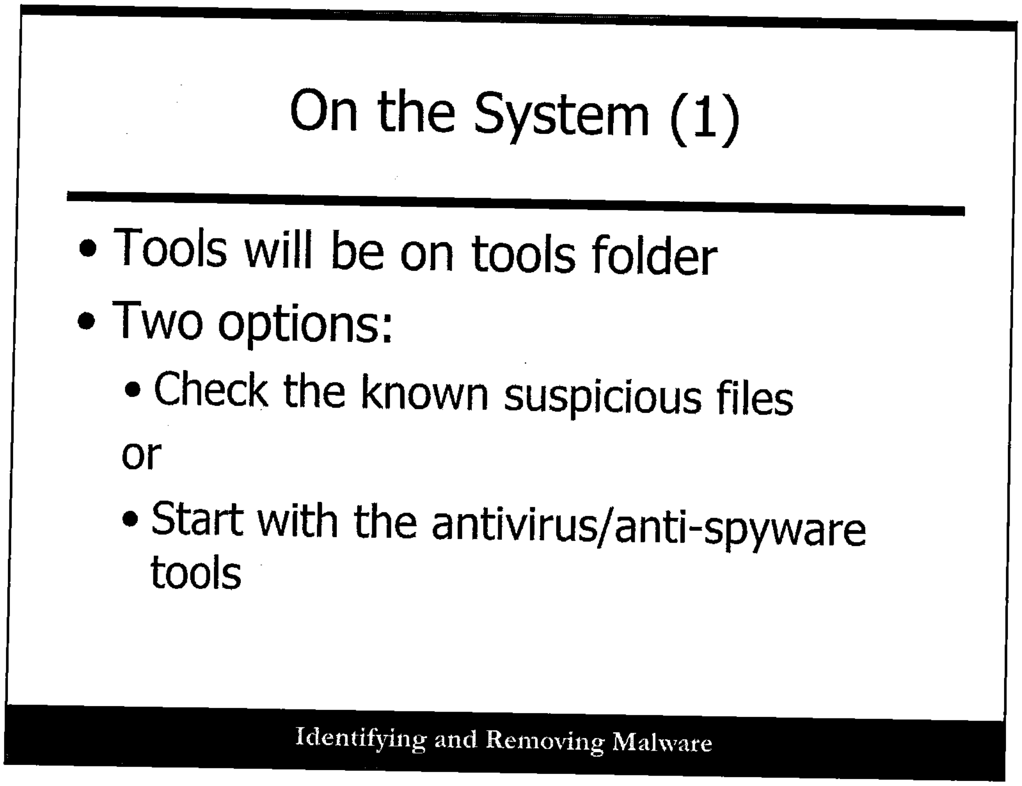
Identifying and Removing Malware

**Booting with Windows PE**

Some BIOSes are already set to put the CD-ROM boot in first place, followed by hard disk and other medias.

You may need to consult your BIOS documentation for instructions on how to change the settings for Boot preferences.

If your computer is already set to check CD-ROM first, you may be asked to press Enter to boot from the CD-ROM and then start the Windows PE.




**On the System (1)**

When you first start on Windows PE, you are presented with a DOS Prompt window in folder x:\windows\system32.

Your tools are in folder x:\tools; then, you have to change directories:

```
X:\windows\system32\cd x:\tools
```

This sends you to the Tools folders, where you can find all the tools that you included in the previous step.

## On the System (2)

- Check the known suspicious files
  - This option is for when you already found suspicious files during the online analysis but could not delete them
  - Now you can find and delete them!

Identifying and Removing Malware

**On the System (2)**

Now that you have access to the offline system, you can go after the suspicious files that you found during an online analysis but were unable to delete/remove them because of a malware trick.

When the boot process is finished, you will be in a DOS prompt window on drive X:, but you can easily go through the actual hard drives and find the suspicious file and try to delete it.

A simple command: cd c:\ will take you to the drive C:\ and then you can navigate to any folder.

# On the System (3)

- All tools will be on X: drive in folder tools
- Check your USB pen-drive drive letter with Drive Manager tool, from X:\tools

Identifying and Removing Malware

**On the System (3)**

As you already explained, you will be prompted to a DOS window on the X:\windows\system32\ folder. The tools you put on will be in X:\tools; you can just cd x:\tools.

If during the boot process you inserted your pen-drive, you can find it. Usually the system will assign the letter E: for it, but you might need to check it with the Drive Manager tool.

# On the System (4)

- Using the AV/AS tools in offline mode:
  - This option is useful when you've already tried everything possible to uncover malicious files on a live system
  - It runs some antivirus and anti-spyware tools, looking for suspicious file/threats
  - This helps because some malware prevents them from running on live systems

Identifying and Removing Malware

**On the System (4)**

You probably want to use the antivirus/antispyware tools, such as the Avast and McAfee Stinger, so they can scan the system looking for malicious software.

Some of these tools are set to scan C:\, which is usually the common root drive for Windows systems, but you might want to use DriveMan.exe to see all disk drives on the system, and maybe reconfigure the scan tools to also check for additional drives.

## Cleaning the System

- When your tools detect something malicious, you have a chance to remove it
- Remember that removing legitimate files may result in failure to boot or failure to run correctly

Identifying and Removing Malware

**Cleaning the System**

When you decide to run an antivirus/antispyware, you must know that some of them will automatically remove the virus from the system.

The Avast Cleaner will proceed in this way, but McAfee Stinger offers you four options on virus detection:

- **Report Only**: Reports only the virus detection on the screen
- **Repair**: Tries to repair the virus infection
- **Rename**: Renames the infected file
- **Delete**: Deletes the infected file from the system

The default option is to repair the virus infection.

Remember that removing legitimate files may result in failure to boot or failure to run correctly.

Note: In some cases, it is not safe to remove a malware file if the changes made by it are not remediated as well. For example, the malware could have been acting as an LSP, removing it without reassigning the order in the Registry keys would lead to a loss of network connectivity. The same goes for other malware that hooks the initialization chain, which without removal of all artifacts, may lead to an unbootable system. Therefore, it's better to rename the file so that you can revert the changes if necessary.

Restoring the System (1)

- In case of failure, to restart the system after removing files during the offline scan, you have two options:
  - Restore the system
  - Rebuild the system

Identifying and Removing Malware

**Restoring the System (1)**

When you decide to remove some files, you might affect your system in a way to prevent it from restarting properly. When that occurs, you have two options:

- Restore the system.
- Rebuild the system.

We see both options in detail on the following pages.

## Restoring the System (2)

- In some situations, Windows creates Snapshots of "safe" configurations, so if your system is booting, you may have a chance to restore it to a last good state
- If it doesn't boot, you can also try to restore from the command prompt

Identifying and Removing Malware

**Restoring the System (2)**

The first option is the System Restore. Windows usually creates snapshots of safe configurations and calls them restore points. In case something goes wrong you can choose to restore the system configuration to one of those safe restore points.

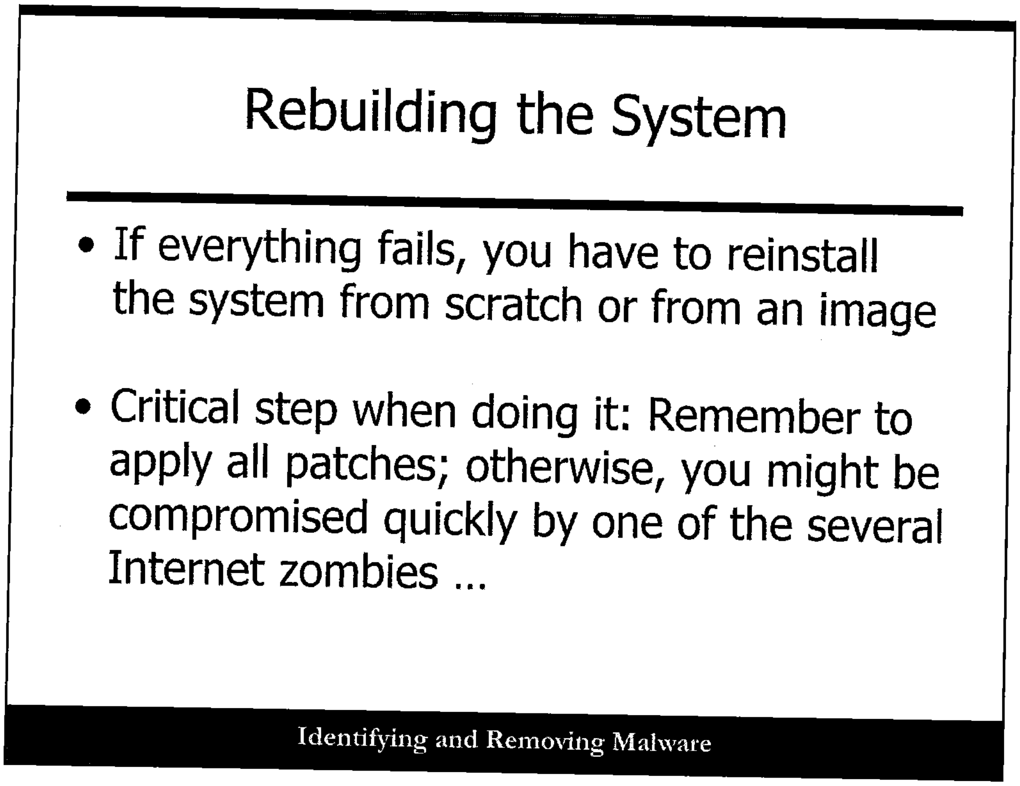
If you can boot the system, you can locate the system restore points by following these steps:

1. Log on to Windows as Administrator.
2. Click Start, point to All Programs, point to Accessories, point to System Tools, and then click System Restore. System Restore starts.
3. On the Welcome to System Restore page, click Restore my computer to an earlier time (if it is not already selected), and then click Next.
4. On the Select a Restore Point page, click the most recent system checkpoint in the On this list, click a restore point list, and then click Next.
   A System Restore message may appear that lists configuration changes that System Restore will make. Click OK.
5. On the Confirm Restore Point Selection page, click Next. System Restore restores the previous Windows XP configuration, and then restarts the computer.
6. Log on to the computer as Administrator. The System Restore Restoration Complete page appears.
7. Click OK.

If you cannot log correctly, boot the system. You can try to restore the system using the command prompt instructions:

1. Restart your computer, and then press F8 during the initial startup to start your computer in Safe Mode with a command prompt.
2. Log on to your computer with an administrator account or with an account that has administrator credentials.
3. Type the following command at a command prompt, and then press Enter:
   **%systemroot%\system32\restore\rstrui.exe**
4. Follow the instructions that appear on the screen to restore your computer to an earlier state.

http://support.microsoft.com/kb/306084/
http://support.microsoft.com/kb/304449/

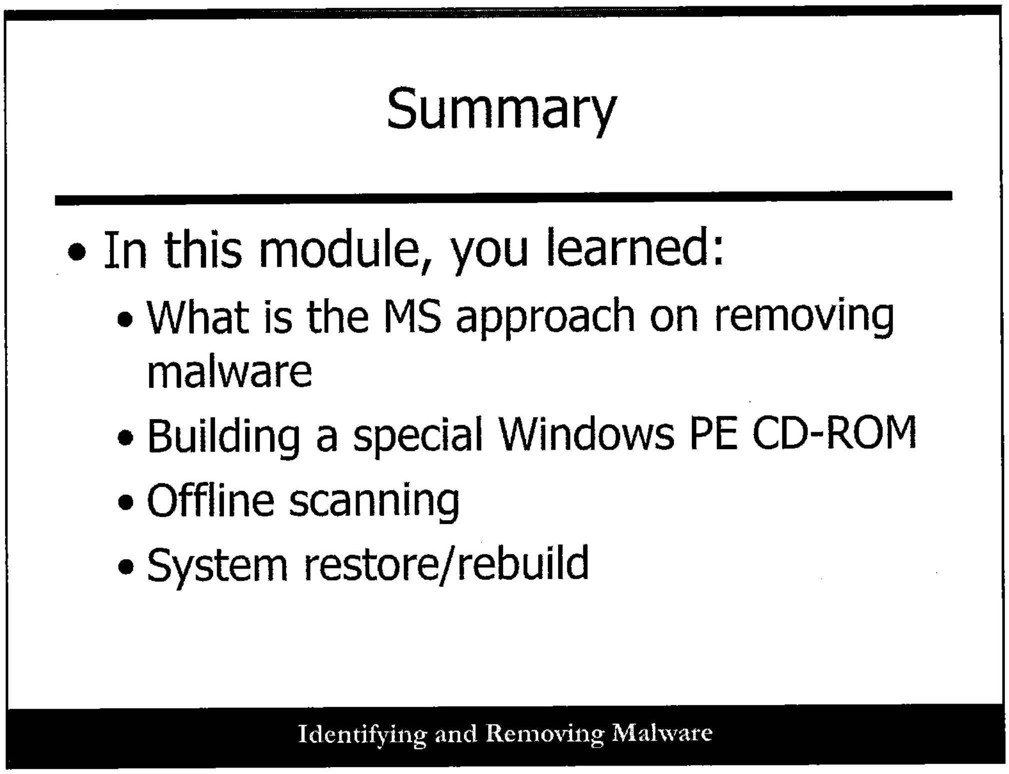



**Rebuilding the System**

When everything fails, and not even a system restore solves the problem, the only way to follow is to rebuild the system.

Some companies have hard-disk imaging software and that makes the work faster.

If you are not in this category, you have to install it from scratch. In this case, a critical step is to apply the security patches as soon as possible; otherwise, you may be compromised fast by one of the several Internet zombies that keeps scanning the Internet looking for vulnerable (unpatched) machines.




**Summary**

In this module, you learned about the MS approach for malware removal. You also learned how to build a custom Windows PE CD-ROM that can be used for attempts to identify and remove malware on an offline system, using both commercial free tools and going directly to suspicious files that might may have been found during live analysis.

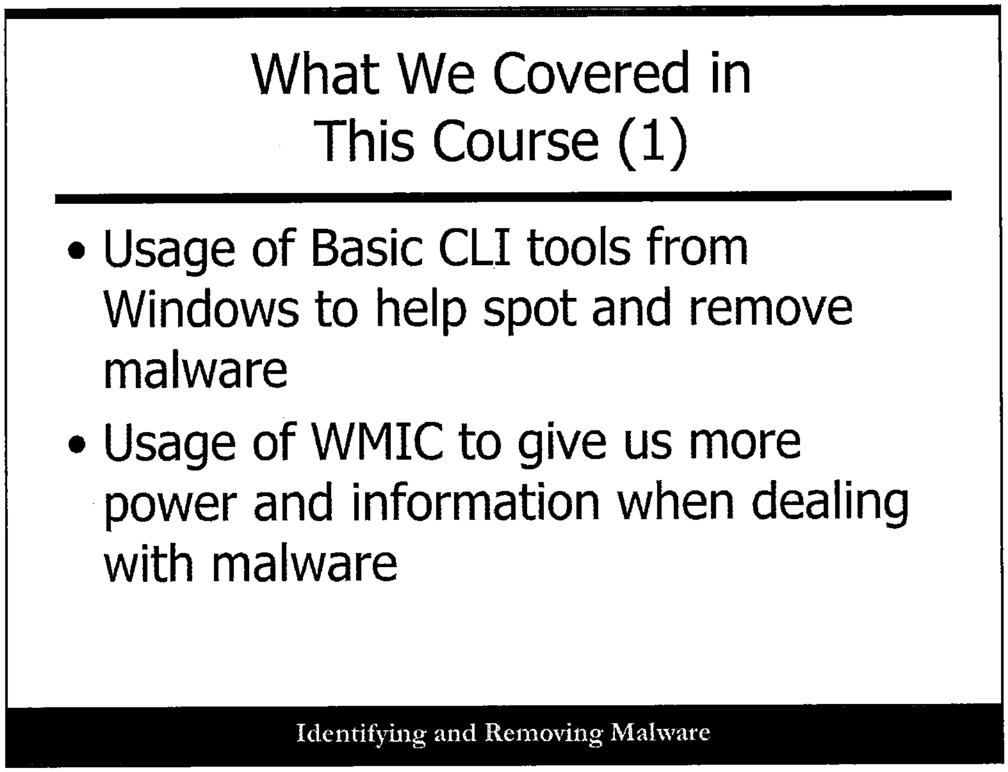
Also, if we accidentally remove a critical file, and the system refuses to behave normally, you learned how to use a Windows feature, called system restore, so you can go back to the last known good configuration. And if even that doesn't work, you learned that the best solution would be to reinstall the system from scratch.

# Identifying and Removing Malware

## Summary

Identifying and Removing Malware

This page intentionally left blank.




**What We Covered in This Course (1)**

During this course, you learned how to use the DOS prompt to get the most from already known tools, such as DIR and Netstat, which help identify and remove malware from the system. You also learned about the advanced command-line tool, WMIC, which enables us to query the system for more complete information and to terminate processes and services that may be used by malware.

## What We Covered in This Course (2)

- Usage of HijackThis tools in different scenarios
- Usage of MS Sysinternals Process Explorer and TCPView to identify and remove malware
- Understanding BHOs and how to use ListDLLs and HijackThis to deal with them

Identifying and Removing Malware

**What We Covered in This Course (2)**

We first used a Swiss knife tool called HijackThis, which enables you to do a system scan, clean malware traces, terminate malware processes, and identify auto-loading applications.

We also introduced the Microsoft Sysinternals Suite, which contains a lot of tools. We started with Process Explorer, an advanced version of Windows Task Manager, and then we covered TCPView, which can be also compared with the Netstat tool.

The malicious usage of DLLs as BHO was also explained, as well the introduction of MS Sysinternals ListDLLs to deal with them.

## What We Covered in This Course (3)

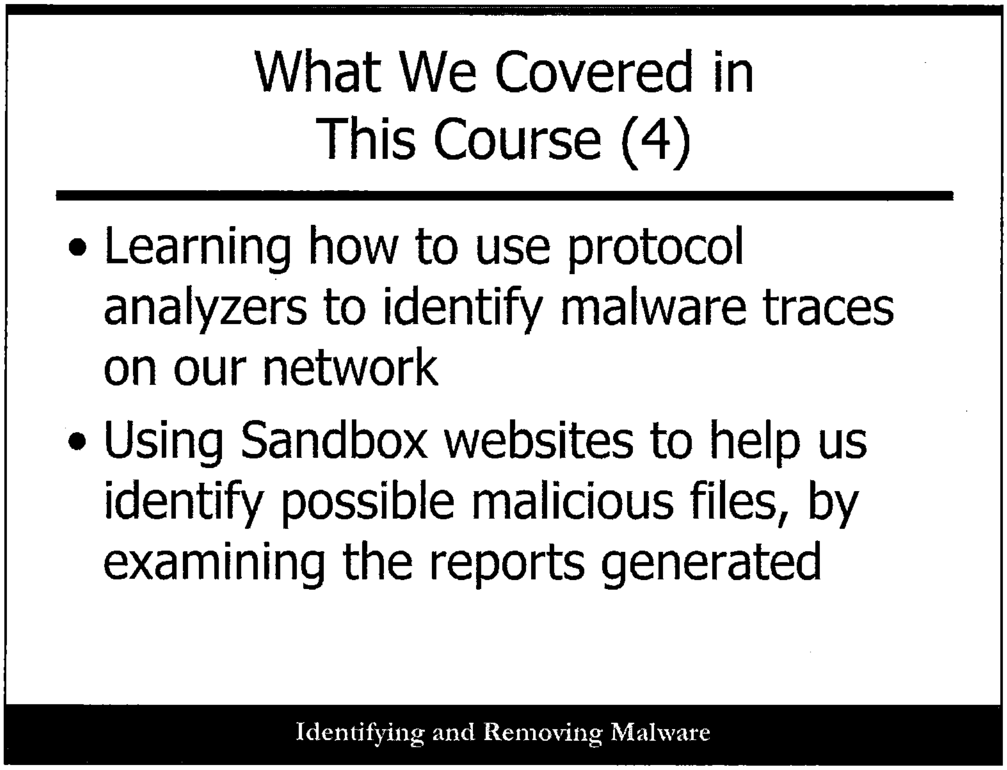
- Understanding ADS and how to get information about them
- Examining rootkits and anti-rootkits technologies
- Dealing with persistent malware
- Analyzing different types of malware

Identifying and Removing Malware

**What We Covered in This Course (3)**

Alternate data streams were covered, as well as the tools that can be used to identify and remove them from our system.

You learned about rootkit and anti-rootkit technologies, such as the tools that can be used to identify rootkit presence and how to use the anti-rootkit tools to remove them from our system.




**What We Covered in This Course (4)**

Identifying the presence of malware in the network can help a lot to improve defenses. You learned how to use a protocol analyzer tool, Wireshark, to identify the network traces left by malware, so you could better understand the purpose of it.

The Sandbox technologies were also explained and you learned how to use them to identify if a suspicious file is malicious by observing the reports generated.

# What We Covered in This Course (5)

- How to build a special version of Windows PE, used on Microsoft Malware Removal Kit, and how to use it



**What We Covered in This Course (5)**

In this course, you learned how to build a special version of Microsoft Windows PE, which is used on the Microsoft Malware Removal Kit with tools for an offline scan on the machine.

You also learned how you can use the kit to detect additional malicious software.

# Hands-on Answers

Identifying and Removing Malware

This page intentionally left blank.

# Lab 1: Part 1

## Answers

Identifying and Removing Malware

1) How many files were added to the directory?

Files/directories that are created as a result of running cli.exe:
C:\WINDOWS\system32\0wned.log
C:\WINDOWS\system32\Badfile1.exe

Hidden files:
C:\WINDOWS\system32\inetsrv\smc.exe

2) Are any of them running?

Process that is running: smc.exe

3) Can you identify any network connections associated with those files?

Using Netstat with the parameters –ano, it is possible to identify some network connections and the process ID of each one. Because the malware rotates between a list of hard-coded IPs, you may notice different IPs being checked, such as 173.194.43.43 and 37.59.41.117.

4) How can you kill that connection?

On the previous question, you were able to see the SMC.exe process making network connections.
Our material shows examples of using taskkill.exe /IM malware.exe, but in this case you can notice that using only the parameter /IM won't kill the process smc.exe.
Sometimes you might need to force the kill. This can be done by adding the parameter /F to the command line.

# Lab 2: Part 2

## Answers

Identifying and Removing Malware

1. How can you start WMIC console?

    Open the command line and type **wmic.**

2. List all processes in a brief way. Which command did you use?

```
wmic:root\cli>process list brief
```

3. List all instances of malware.exe processes. Which command did you use?

```
wmic:root\cli>process where name='malware.exe' list brief
```

4. Use WMIC to kill all processes of name malware.exe.

```
wmic:root\cli>process <PID> delete
```

5. Check if malware.exe or any suspicious file is configured to start when the computer reboots. Tip: Check the startup list.

```
wmic:root\cli>startup list full
```

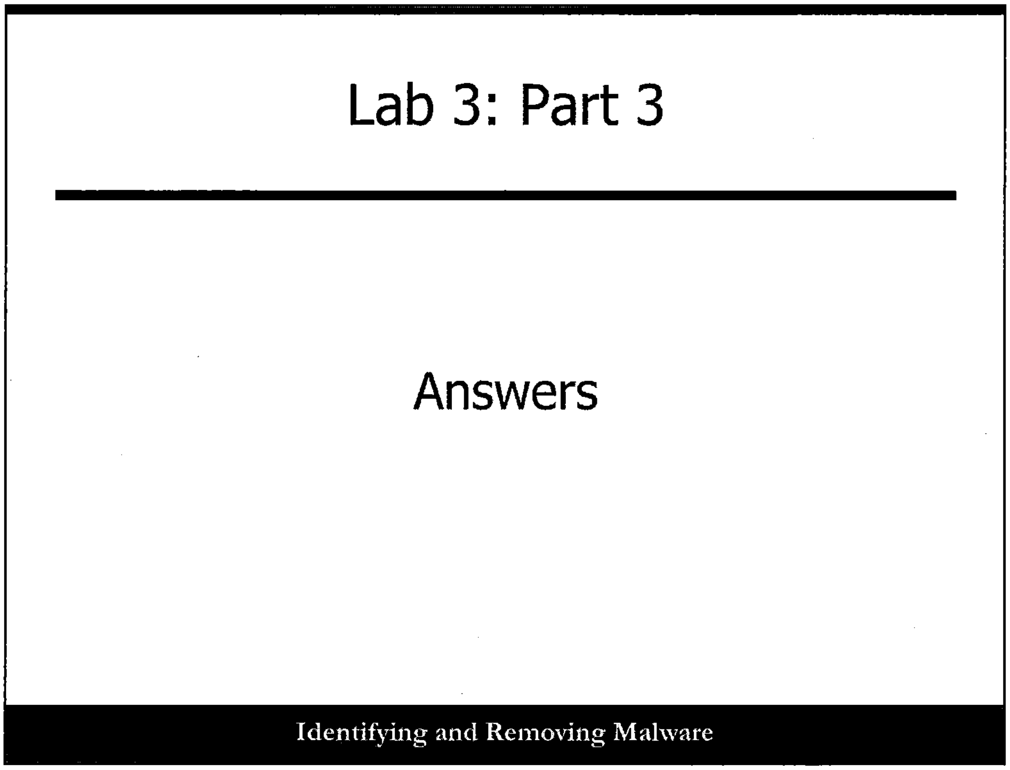
```
This command will show a list of the files; notice the My_love.exe
file.
```

6. Generate the list of all processes that start on boot time in the HTML format and open with IE.

    Wmic startup list full /format:hform : startup.html

7. List all services and see if malware.exe or any suspicious file is running as a service.

    Using the process described, malware.exe is not shown, but it is possible to see My_Love.exe.




This lab has the following questions:

1. What do you see when you click "Do a system scan only?" Take note of anything suspicious that will be loaded at boot time.

2. If a suspicious process is running, try to kill/terminate it. Describe the process used to kill the suspicious process using HijackThis.

3. If the process was successfully terminated, it is time to remove the malicious registry entries. Using the HijackThis tool, which function will allow you to remove the entries?

Because this is an interactive lab, the answers are included in the slides following the original Hands-On questions.

# Lab 4: Part 4

## Answers

Identifying and Removing Malware

1. Do you see any suspicious activity on the machine using both Process Explorer and TCPView?

   If you keep TCPView open for a few moments, you will notice the machine attempting to connect to a remote website.

2. Which remote ports are involved?

   Port 80

3. Is it using any method to ensure that it will be loaded at boot time?

   Yes, by running HijackThis, it is possible to see it being loaded with an Autorun Registry key (HKLM\Software\Microsoft\Windows\CurrentVersion\Run).

4. What can you use to clean its traces?

   HijackThis can delete it by checking the box that it is and selecting the Fix button. However, in some cases you need to make sure that the malware is not running. The solution in this case is to rename the malware on this folder, reboot the system, and then run HijackThis to fix it.

5. Which folder is the suspicious file installed in?

   On Windows 7, it is installed in the c:\Users\<username logged>\AppData\Roaming\<random name folder>\.

6. Can you delete it?

With TCPView, you notice that the malware is making connections, but the process that is doing it is not the malware process. It is a Windows process called TaskHost.exe. (Note that you might observe different behaviors on Windows 7 32-bit and Windows 7 64-bit.)
This means that the malware injected its code into a legit Windows process to make it harder for the analyst to find it.

With the tools provided in the folder, you can find the autostart mechanism and the folder where it is located.

After you delete it, try to run the HijackTools and remove the autorun entry. Then, scan again.

7. Did the Autorun entry get removed?

No, which means that you need to reboot the system first.

Now reboot the system and try to remove the Autorun entry again.

# Lab 5: Part 6

## Answers

Identifying and Removing Malware

Because this is an interactive lab, the answers are included in the slides following the original Hands-on questions.

## Lab 6: Part 9

Answers

Identifying and Removing Malware

Because this is an interactive lab, the answers are included in the slides following the original Hands-on questions.

# Lab 7: Part 7

## Answers

Identifying and Removing Malware

Because this is an interactive lab, the answers are included in the slides following the original Hands-on questions.

Remember that Rootkit_Detective, Panda anti-rootkit, and rku37300509 from the Part 7 course files do not run on Windows 7. They are included to help you create your arsenal of tools, which may run on different Windows versions.

# Lab 8: Part 7

## Answers

Identifying and Removing Malware

Because this is an interactive lab, the answers are included in the slides following the original Hands-on questions.