



# Global Information Assurance Certification Paper

Copyright SANS Institute  
Author Retains Full Rights

This paper is taken from the GIAC directory of certified professionals. Reposting is not permitted without express written permission.

## Interested in learning more?

Check out the list of upcoming events offering  
"Security Essentials: Network, Endpoint, and Cloud (Security 401)"  
at <http://www.giac.org/registration/gsec>

# **Trench Warfare with Malware**

**Methods and tools for system administrators dealing with  
Viruses, Worms, & Spyware.**

David Warde  
GSEC GIAC Security Essentials Certification, ver 1.4c  
April 6, 2005

## TABLE OF CONTENTS

<a href="#"><u>Abstract</u></a>	3
<a href="#"><u>How to use this document</u></a>	3
<a href="#"><u>Introduction</u></a>	4
<a href="#"><u>The Roadmap</u></a>	4
<a href="#"><u>Anti-virus</u></a>	5
<a href="#"><u>Updated Anti-virus</u></a>	5
<a href="#"><u>Advanced AV options</u></a>	6
<a href="#"><u>Heuristic Scanning –</u></a>	6
<a href="#"><u>ADS Scanning</u></a>	6
<a href="#"><u>AV Boot Diskette</u></a>	7
<a href="#"><u>2<sup>nd</sup> AV Vendor Solution</u></a>	7
<a href="#"><u>Standalone AV products</u></a>	7
<a href="#"><u>Mcafee Stinger</u></a>	7
<a href="#"><u>Microsoft Malicious Software Removal Tool</u></a>	7
<a href="#"><u>AntiSpyware</u></a>	8
<a href="#"><u>Microsoft AntiSpyware (Giant)</u></a>	8
<a href="#"><u>SpyBot Search &amp; Destroy</u></a>	9
<a href="#"><u>Multiple Anti-SpyWare solutions</u></a>	9
<a href="#"><u>Process Monitoring Utilities</u></a>	9
<a href="#"><u>Windows Task Manager</u></a>	9
<a href="#"><u>Limitations of Task Manager</u></a>	11
<a href="#"><u>TUT The Ultimate Troubleshooter</u></a>	12
<a href="#"><u>Monitoring suspicious Network Connections</u></a>	14
<a href="#"><u>Desktop Firewalls</u></a>	14
<a href="#"><u>Netstat –nao</u></a>	14
<a href="#"><u>Patch It!</u></a>	15
<a href="#"><u>The File System</u></a>	15
<a href="#"><u>Windows Find</u></a>	16
<a href="#"><u>Data Integrity Solutions</u></a>	16
<a href="#"><u>Vendor File Lists</u></a>	16
<a href="#"><u>Conclusion</u></a>	17
<a href="#"><u>Appendix A: References</u></a>	18
<a href="#"><u>Appendix B: Troubleshooting Checklist</u></a>	19

## Abstract

This paper describes tools and methods for diagnosing a computer system that is exhibiting symptoms of an infection of malicious software, or malware that is not immediately identified by your existing anti-virus or even anti-spyware software.

This paper is focused on tools and methods for isolating the problem until one of several things happens:

1. The vendor releases an updated signature to identify and remove the malware.
2. A decision is made to rebuild or restore the system. That may be the proper course of action, provided you are prepared.
3. The guilty file(s) are located, though the malware may still be unidentified. Typically the file would be handed off for more advanced study.

There are situations that fall short of a criminal investigation where you must still persevere and identify an infected file. One good example would be the early stages of an outbreak when you wish to get a sample to your anti-virus vendor.

## How to use this document

The intended audience is a system administrator in any organization large or small, business or academic institution. It is assumed that you have experience installing and configuring software for the Windows platform; therefore there is no time or space spent here with installation screen shots.

The best use of this document depends on your circumstances. I believe it is a useful resource for preparing for an outbreak in advance. However, if this paper somehow finds it's way into your hands while you are dealing with an outbreak, you may still be able to make immediate use of the checklist in appendix B. The paper and references can be read at length afterward. You should assemble a toolkit by downloading the available tools and burning them to a CD and/or storing them online where they may be readily accessed. The CD should be updated regularly. Having the tools on a CD may be very helpful if the system has been removed from the network to prevent further spread of the threat. Kevin Liston, one of the handlers of the Internet Storm Center, referred to this as a "Goodie Basket for Grandma"<sup>1</sup> in one of his diaries.

It is not the goal of this paper to instruct you in how to reverse engineer malicious software, nor is that within my own skill set. I do not address advanced forensics in this paper or provide direction for situations where

---

<sup>1</sup> <http://isc.sans.org/diary.php?date=2005-01-10>

criminal activity is indicated. In that case you will want to obtain and comply with your organization's Incident Response Plan.

## Introduction

In his 1957 B-Movie classic "The DI", Jack Webb of TV's Dragnet plays a Marine Corp Drill Instructor. In one classic scene, Webb faces off two inches from a poor recruits face, and as only Jack Webb can he belts out "If you were completely surrounded this morning by an enemy force of 500 men, what would you do?" At the top of his lungs, the recruit shouts back the only answer acceptable to the DI, "Kill them, SIR!!"

System administrators today often find themselves in situation that feel like that miserable recruit. Outgunned and outnumbered by constantly evolving threats our own expectations and the expectations of the organizations we serve are that we will somehow find a way to "Kill them, Sir!"

Network Magazine recently polled their readers and the results were instructive. "93 percent of respondents said spyware was a serious problem, even though nearly 100 percent had anti-virus software installed." <sup>2</sup> Anti-Spyware software has emerged to deal with the problem but the best of breed can still miss one quarter of the known threats. There are occasions where neither your anti-virus nor your anti-spyware is able to quickly identify the culprit. The behavior of the system however, clearly indicates that malicious software has made its way on to your system.

These situations come to the administrator's attention via a variety of ways. The company's intrusion detection system picks up traffic indicating a problem with the system. The firewall logs may indicate a large number of packet drops pattern from the computer. The network management team notices increased traffic from their NMS console. Perhaps the user calls the help desk to report a problem with the system, the system is unusually slow or that they were attempting to browse to a particular web site and were redirected to another site.

## The Roadmap

Our discussion of methodology begins with current anti-virus software. Advanced AV options such as heuristic scanning and scanning for alternate data streams are then discussed. Utilizing a second vendor's AV solution will

<sup>2</sup> [The Battle for the Desktop Rages On](http://www.networkmagazine.com/shared/article/showArticle.ihtml;jsessionid=MOGPXFLYJ2Z1UQSNDBCSKH0CJUMEKJVN?articleId=60401607&classroom=), Network Magazine, Mar 05 p.25

sometimes produce results, as vendor's time to produce signatures can vary. Many AV vendors provide standalone or online scanners that can be used to fill in the gaps.

In most situations, if AV software hasn't identified the threat, it probably cannot until the vendor produces the signature update. In other situations, the AV software will not alert you because it is looking for viruses and worms and not spyware, rootkits, backdoors, etc.

Anti-Spyware is coming into maturity, but by most accounts not fast enough. The Microsoft AntiSpyware (Giant) product is discussed as well as SpyBot Search & Destroy. There are an ever-growing number of commercial solutions available. Checkout the comparison on <http://anti-spyware-review.toptenreviews.com/>, which reviews 10 commercial anti-spyware products.

Traditional signature based security solutions are seriously limited in their ability to detect and stop evolving threats. When both AV and Anti-Spyware have failed to identify what is plaguing your system, it is important to isolate the process or executable(s) responsible.

We will deal with the capabilities and limitations of the built in Windows Task Manager and one alternative to Task Manager. Process oriented tools can provide great insight into what is happening on your system. Several now incorporate knowledge bases to tell you more about processes and executables. They tell you where in the directory the executable process loaded from compared to where it usually loads from, giving additional clues as to whether a process is legitimate or suspect.

Next we discuss monitoring of network connections with desktop firewalls and the netstat command. Finally we have a quick word about data integrity solutions and vendor file lists. Appendix A contains a list of references and Appendix B features a simple checklist.

## **Anti-virus**

### ***Updated Anti-virus***

It goes without saying the AV solution needs to be updated regularly, especially when searching a suspect system. Not long ago, monthly or weekly anti-virus updates were sufficient intervals to provide adequate protection. Daily updates are usually the norm. Hourly updates are now configurable with some anti-virus products, including ClamWin, the open source anti-virus solution.

In my recent experience, updating the AV signatures has not usually changed

the results; that is the evil code is not suddenly identified. But updating does work often enough, and with the update mechanisms that are now available we would be fools to run with AV signatures that are more than a day old.

## ***Advanced AV options***

### **Heuristic Scanning –**

Heuristic scanning methods are supposed to detect new or unknown viruses, viruses for which no signature exists. In this mode, the software is looking for activity that is typical of viruses, rather than matching bits of code against its signature database. Unfortunately there is a price to pay in system performance and this approach may result in more false positives. As a result, AV solutions frequently ship with heuristic scanning turned off. Turning on heuristic scanning may require admin privileges.

I recommend reading Stan Miastkowski's [Step-By-Step: Set Anti-virus Software for Maximum Protection](http://www.pcworld.com/howto/article/0,aid,106718,pq,1,00.asp). Though it is two years old, it is still a valuable guide for configuring anti-virus software.

<http://www.pcworld.com/howto/article/0,aid,106718,pq,1,00.asp>

### **ADS Scanning**

Alternate Data Streams are a feature of the NTFS file system that serves several legitimate purposes. The NTFS file system uses ADS to store summary data about files, including title, subject and author. A thumbnail image of a graphics file is stored in ADS. ADS is also used by the NTFS to provide storage volume support for Macintosh systems.

They can also be used to hide files from the user. The windows notepad application can write to ADS, and can read from it as well. Notepad is only useful if you know the exact name of the stream you are looking for. And it has obvious limitations with reading executables, which can also be hidden in a stream.

For an overview of ADS, you may wish to wade into "Alternate Data Streams: Out of the Shadows and into the Light" by Ryan L. Means. Means provides a very thorough technical treatment of ADS, and features the results of his evaluation of several freeware scanning tools. This white paper is available at the SANS reading room at <http://www.sans.org/rr/whitepapers/honors/1503.php>

ADS Scanning is included with most commercial Anti-virus software, though it may be deactivated by default. As with heuristic scanning, activating ADS scanning may require admin privileges.

There is one certain way to “scrub” a file to insure that no ADS remains. Copy the file by whatever means to a FAT volume. The FAT volume has no ADS capability so the streams just wind up in the bit bucket. If the file previously had an ADS payload, then a change in behavior should result. This method does not scale very nicely and would only be practical where the administrator has isolated the problem to a small number of files.

### **AV Boot Diskette**

If you are going to utilize a boot diskette to clean a system, make sure that you update the AV signatures first, on a clean system, before making the boot diskette. Certain viruses and worms can be very tricky to clear off your system. Miss one registry entry and it will load up again into memory. By booting and running the AV from the floppy you stop the code from loading into memory from the hard drive.

### **2<sup>nd</sup> AV Vendor Solution**

Rinse and Repeat as above. On any given point and time, a given vendor's anti-virus product may beat it's competitors with a new virus signature; the following week the competition may beat them. The differential between vendors was once measured in days or weeks, but is now more frequently a matter of a few hours. Remember also that many virus/worms also have the capability to “morph” or mutate.

### **Standalone AV products**

You may not have the option of installing a second vendor's anti-virus solution, either because you do not have a license or you cannot afford the delay. There are also issues that can arise when trying to run two fully installed products. A standalone package from an AV vendor may solve this problem.

### **Mcafee Stinger**

This free product scans for a limited number of signatures. It is more effective if you have a clue what virus or worm you are looking for. The list changes frequently so check the McAfee web site first to see if your suspect is included in the signatures.

“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. Stinger utilizes next generation scan engine technology, including process scanning, digitally signed DAT files, and scan performance optimizations.” <http://vil.nai.com/vil/stinger/>

### **Microsoft Malicious Software Removal Tool**



Microsoft has a standalone tool cleverly named “The Microsoft Windows Malicious Software Removal Tool”. My own efforts to convert that into a catchy acronym failed. In my opinion Microsoft needs to take a cue from McAfee and come up with a zippier name. Maybe crusher or thwacker are still available. As with McAfee’s Stinger, the Microsoft tool addresses the most prevalent current threats and it changes at least monthly to coincide with the monthly patch release cycle. So you will want to revisit the site and update before using the tool.

<http://support.microsoft.com/?id=890830>

- This Microsoft Knowledge Base article, KB 890830, will be updated with information for each monthly release so that the number of the relevant article remains the same. The name of the file will be changed to reflect the tool version. For example, the file name of the January 2005 version is Windows-KB890830-ENU.exe and the file name of the February 2005 version is Windows-KB890830-V1.1-ENU.exe
- This cumulative tool currently removes the following as of February, 2005

Win32/Beberew January 2005 (V 1.0) Moderate  
 Win32/Doomjuice January 2005 (V 1.0) Low  
 Win32/Gaobot January 2005 (V 1.0) Moderate  
 Win32/MSBlast January 2005 (V 1.0) Moderate  
 Win32/Mydoom January 2005 (V 1.0) Moderate  
 Win32/Nachi January 2005 (V 1.0) Moderate  
 Win32/Sasser January 2005 (V 1.0) Moderate  
 Win32/Zindos January 2005 (V 1.0) Low  
 Win32/Korgo February 2005 (V 1.1) Moderate  
 Win32/Netsky February 2005 (V 1.1) Moderate  
 Win32/Randex February 2005 (V 1.1) Moderate  
 Win32/Zafi February 2005 (V 1.1) Moderate

- <http://www.microsoft.com/technet/security/tools/default.mspx>

You need only download and run the utility. Administrator privileges are required to run. The tool does not require installation or configuration. It will run and by default find and remove all the malicious software on its list. There are command line options for help and for a “/q” option to run in quiet mode; no user interface is displayed in quiet mode.

## AntiSpyware

### ***Microsoft AntiSpyware (Giant)***

Microsoft acquired Giant AntiSpyware in January. Giant had been rated tops overall in October 2004 by independent Virus researcher Eric Howes. Howe and other professionals recommend using multiple vendor products, as the best still missed about 25% of the threats.

Microsoft’s Anti-Spyware is a Beta1 product, but Microsoft is making it available free of charge now. Microsoft announced that they will continue to provide the

product free of charge, and will soon announce their strategy for supporting enterprise clients. It is unknown whether enterprise tools for managing the solution will likewise be free of charge. The product can be downloaded at:

<http://www.microsoft.com/athome/security/spyware/software/default.msp>  
[X](#)

### **SpyBot Search & Destroy**

SpyBot Search & Destroy is a freeware tool written by Patrick Michael Kolla, <http://www.safer-networking.org/en/download/>.

The license permits you to download and use it with no qualifiers on whether that use is limited to home, academia, or business. Kolla does accept donations to support his work.

SpyBot S&D has multiple components. First there is the on demand scanner, which scans the system for spyware, and removes components matching it's database of known spyware. Removal of some spyware components can cause applications to stop functioning. SpyBot S&D does a good job of warning the user of this, and a recovery function is available to restore the application functionality. One drawback with the product is the lack of an automated update mechanism. The user must manually update the product.

SpyBot S&D also features two resident levels of protection, one of which is a browser helper for Internet Explorer which blocks the download of known malicious files. The other resident component is called Tea Timer, which monitors system processes and certain critical registry keys, and will stop suspicious changes.

### **Multiple Anti-SpyWare solutions**

Running two or more anti-spyware solutions will increase the odds of detecting spyware. In the conclusion to his research in October 2004, Eric Howes writes:

*"No single anti-spyware scanner removes everything. Even the best-performing anti-spyware scanner in these tests missed fully one quarter of the 'critical' files and Registry entries. It is better to use two or more anti-spyware scanners in combination, as one will often detect and remove things that others do not."*

<http://spywarewarrior.com/asw-test-guide.htm#conclusions>

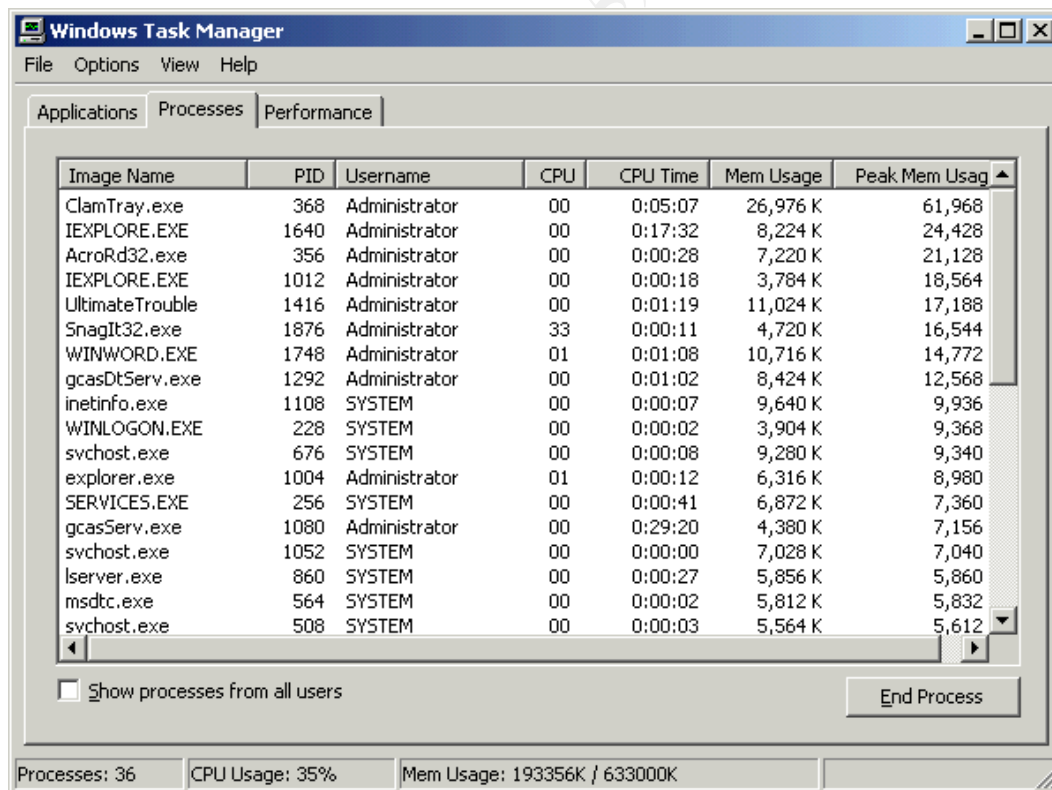
## Process Monitoring Utilities

### Windows Task Manager

At some time, you will reach that frustrating point at which neither the Anti-virus or Anti-SpyWare is able to identify whatever may be on the system, even after updating and trying another vendor's product. Perhaps it is a "zero-day" exploit, or a morph of a virus for which no signatures have been produced yet. For whatever reason, your existing security utilities aren't able to identify anything, but you suspect or know your system is infected with something.

Taskman, the built in Windows task manager, can be very useful in identifying processes that are consuming heavy system resources, and which may lead to the cause of your trouble.

Most Windows administrators have probably used this utility at some point. There are a number of parameters monitored by default and others can be selected depending on your objective.



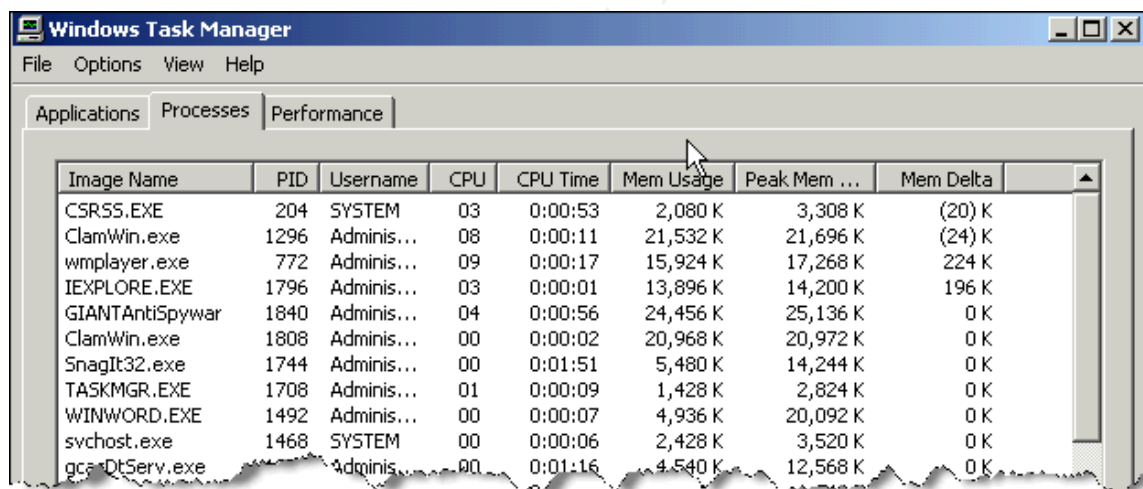
There are a variety of ways to sort the view on Task Manager including Image Name, Process ID (PID), CPU, CPU Time, and Mem Usage. There are additional columns which can be selected for viewing and sorting. You should

experiment with the various views to see what stands out.

Some bits of malware code may manifest themselves by consuming memory or CPU cycles. Though a process may not be the current top entry under “CPU” it may appear at the top when you sort by “CPU Time”. The miscreant process may not be consuming memory at the time, however if you sort by “Peak Mem Usage”, you may spot your culprit.

The “Username” and “Peak Mem Usage” columns are not in the default view and must be selected by the *View | Select Columns* menu path.

When using taskman, beware of the “background noise” of other processes. In the example above you can see that the top consumers of system resources are known entities, ClamTray.exe, Iexplore.exe, AcroRd32.exe, and Iexplore.exe again. The view is sorted by “Peak Mem Usage”, and the point is you should close whatever you don’t need to make it easier to spot your process. And yes, I was running as administrator on my isolated system; (bad security man!)



The screenshot shows the Windows Task Manager Performance tab. The table displays the following data:

Image Name	PID	Username	CPU	CPU Time	Mem Usage	Peak Mem ...	Mem Delta
CSRSS.EXE	204	SYSTEM	03	0:00:53	2,080 K	3,308 K	(20) K
ClamWin.exe	1296	Adminis...	08	0:00:11	21,532 K	21,696 K	(24) K
wmplayer.exe	772	Adminis...	09	0:00:17	15,924 K	17,268 K	224 K
IEXPLORE.EXE	1796	Adminis...	03	0:00:01	13,896 K	14,200 K	196 K
GIANTAntiSpywar	1840	Adminis...	04	0:00:56	24,456 K	25,136 K	0 K
ClamWin.exe	1808	Adminis...	00	0:00:02	20,968 K	20,972 K	0 K
SnagIt32.exe	1744	Adminis...	00	0:01:51	5,480 K	14,244 K	0 K
TASKMGR.EXE	1708	Adminis...	01	0:00:09	1,428 K	2,824 K	0 K
WINWORD.EXE	1492	Adminis...	00	0:00:07	4,936 K	20,092 K	0 K
svchost.exe	1468	SYSTEM	00	0:00:06	2,428 K	3,520 K	0 K
gcadtserv.exe		Adminis...	00	0:01:16	4,540 K	12,568 K	0 K

One more column deserves a special mention, the “Mem Delta” column shown at the extreme right. This column shows the memory usage change from one sample period to another. The processes in the two top rows have just given memory back, displayed in parentheses. The next two processes have added memory.

The system here has been made more active by rapidly opening and shutting applications in order to demonstrate the memory usage, but in an actual situation it would be more advantageous to shut down everything that is not needed so that the computer is in a quiescent state. With the system in a quiet state, processes which are grabbing and releasing memory should be more noticeable.

## Limitations of Task Manager

The main limitation of taskman is that it will not help you determine whether processes are legitimate or not.

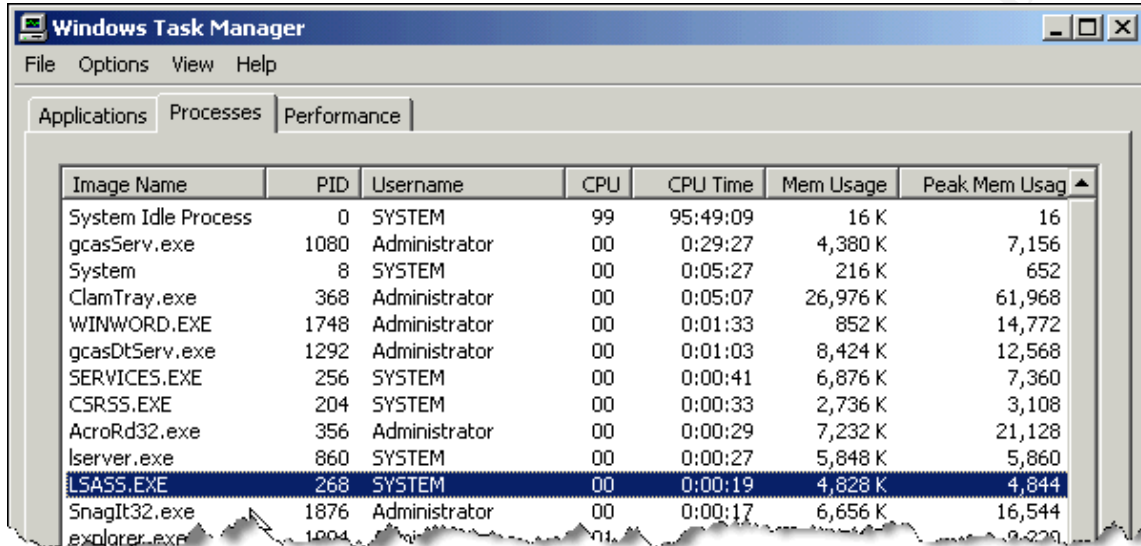


Image Name	PID	Username	CPU	CPU Time	Mem Usage	Peak Mem Usage
System Idle Process	0	SYSTEM	99	95:49:09	16 K	16
gcasServ.exe	1080	Administrator	00	0:29:27	4,380 K	7,156
System	8	SYSTEM	00	0:05:27	216 K	652
ClamTray.exe	368	Administrator	00	0:05:07	26,976 K	61,968
WINWORD.EXE	1748	Administrator	00	0:01:33	852 K	14,772
gcasDtServ.exe	1292	Administrator	00	0:01:03	8,424 K	12,568
SERVICES.EXE	256	SYSTEM	00	0:00:41	6,876 K	7,360
CSRSS.EXE	204	SYSTEM	00	0:00:33	2,736 K	3,108
AcroRd32.exe	356	Administrator	00	0:00:29	7,232 K	21,128
lsrvr.exe	860	SYSTEM	00	0:00:27	5,848 K	5,860
LSASS.EXE	268	SYSTEM	00	0:00:19	4,828 K	4,844
Snagit32.exe	1876	Administrator	00	0:00:17	6,656 K	16,544
explorer.exe	1004	Administrator	00	0:00:17	9,220 K	9,220

The taskman screenshot above shows the view sorted by CPU Time. This system in my lab is not heavily utilized and the top user of CPU Time is the System Idle Process. The “LSASS.EXE” process near the bottom is highlighted. It is not at the top of any resource category but I chose it for another reason. LSASS is the Local System Authentication Server.

Prior to the outbreak of the Sasser worm most system administrators probably had no clue what this process did. To be frank, if it had never become the target for an exploit I might have reached retirement age without knowing its purpose. Imagine that it is the fourth week of April 2004, at the onset of outbreak of the Sasser worm. If you were looking at taskman at that time, odds are you would have noticed something out of the ordinary with LSASS.EXE. Taskman doesn't tell you anything about the vendor or the purpose of the process. The Process ID of 268 and Username of SYSTEM are insufficient to determine whether it is legitimate.

What is required is a utility that will tell the administrator more about the processes running on your system. There are several promising utilities that make up for the lack of information provided by the Task Manager. These utilities give additional capabilities including an embedded knowledge base that is displayed in one of the windows.

## TUT The Ultimate Troubleshooter

The Ultimate Troubleshooter, as implied, is positioned as a troubleshooting tool. It is a task manager on steroids if you will.

TUT displays much more detailed information about most of the executable processes running on your system. It comes with knowledgebase that gives you context-based advice; the knowledgebase knows where most tasks are supposed to run from.

The evaluation product will not display the entire knowledgebase; you have to purchase the product (\$29) for that. However, you can access the same information online during the evaluation at the vendor's web site.

[http://www.answersthatwork.com/Tasklist\\_pages/tasklist.htm](http://www.answersthatwork.com/Tasklist_pages/tasklist.htm)

The following is an excerpt from the online tasklist with information about the LSASS.EXE process:

<b>Lsasrv</b> <b>Lsass</b>	Lsasrv.exe <b>(???)</b>	You have the <b>W32.Mydoom.AG@mm \ W32/Mydoom.af@MM \ WORM_SWASH.A</b> virus.
<b>Lsass (1)</b>	Lsass.exe <b>(Microsoft)</b>	Windows NT4/2000/XP/2003 only. LSASS is the Local Security Authentication Server. It verifies the validity of user logons to your PC/Server (in technical jargon : it generates the process that is responsible for authenticating users for the Winlogon service).  <b>Recommendation :</b> An integral part of the operating system, leave alone provided that its full path as shown in <a href="#">The Ultimate Troubleshooter</a> is either <u>C:\WinNT\System32\LSASS.exe</u> (Windows 2000) or <u>C:\Windows\System32\LSASS.exe</u> (Windows XP/2003). If the path is anything else then you may have a virus (see below).
<b>Lsass (2)</b>	Lsass.exe <b>(???)</b>	If the full path to this program as shown in <a href="#">The Ultimate Troubleshooter</a> is <b>not</b> <u>C:\WinNT\System32\LSASS.exe</u> (Windows 2000) or <u>C:\Windows\System32\LSASS.exe</u> (Windows XP, 2003), then you have the <b>W32.Nimos.Worm</b> virus or some other virus.  <b>Recommendation :</b> Make sure you have up-to-date reputable antivirus software and then reboot your PC into Safe Mode and run a full virus scan.
<b>Lsasss</b>	Lsasss.exe <b>(???)</b>	You have the <b>W32.Sasser.E.Worm</b> virus.

In the graphic above, there are four references to LSASS. The knowledgebase gives the possible paths for the legitimate path for the LSAS service. In the first example the executable referenced is "lsasrv.exe" which is actually the executable for a MyDoom version. The next two entries have the correct executable name. The proper path is either C:\WinNT\System32\LSASS.exe or



C:\Windows\System32\LSASS.exe. If the process loads from another location the KB advises that the system probably has the Nimos or another virus. The last entry likewise has a misspelled executable, but the third “s” is just the sort of detail you would miss in a hurry. The KB indicates this is Sasser.E.

## Monitoring suspicious Network Connections

### **Desktop Firewalls**

Desktop firewalls can help in the prevention of an exploit against your system and in the spread of that exploit to other systems, provided they are not vulnerable to exploit themselves. As with AV software, desktop firewalls are already the target of code that will attempt to turn off well-known security software.

In a recent Network magazine poll, 36.8% of respondents were running third party personal firewalls and 46.5% of respondents were currently running Windows XP SP2 firewall.<sup>3</sup> The wording of the question was “What security software programs do you currently run on your desktop or laptop PCs?” Multiple responses were allowed, so you need to be careful not to read into those figures and assume that three quarters of desktops are protected by desktop firewalls. Again, the results say that n% of respondents have this or that firewall deployed. They do NOT mean that 72% of desktops are covered by desktop firewalls.

Odds are that if you are dealing with a malware infection, you probably don’t have a desktop firewall available to help do a post mortem. Ideally desktop firewalls would be ubiquitous and in a troubleshooting scenario, it is possible that the desktop firewall logs may point to suspicious network connections.

If there is no desktop firewall already installed, why not do it now? I would try practically anything to find the source of the problem including downloading and installing a desktop firewall. If the product will install you may be able to use it to monitor for rogue network connection attempts that will lead you to your enemy.

### **Netstat –nao**

Windows systems administrators should be familiar with this utility which has been around for a while. Beginning with Windows XP a new option was added. By entering the command “netstat –nao” in a command shell network connections can be monitored and what is new is that they are now traceable to

<sup>3</sup> The Battle for the Desktop Rages On, Network Magazine, Mar 05 p.25  
<http://www.networkmagazine.com/shared/article/showArticle.ihtml;jsessionid=MOGPXFLYJ2Z1UQSNDBCSKH0CJUMEKJVN?articleId=60401607&classroom=>

the process ID. In the following screen shot the command is “netstat –nao 30”, which will also cause the connection list to update every 30 seconds.

```

C:\>netstat -nao 30
Active Connections

```

Proto	Local Address	Foreign Address	State	PID
TCP	0.0.0.0:135	0.0.0.0:0	LISTENING	1920
TCP	0.0.0.0:445	0.0.0.0:0	LISTENING	4
TCP	127.0.0.1:1025	0.0.0.0:0	LISTENING	676
TCP	169.254.83.199:139	0.0.0.0:0	LISTENING	4
TCP	192.168.1.103:139	0.0.0.0:0	LISTENING	4
UDP	0.0.0.0:445	***		4
UDP	0.0.0.0:500	***		1692
UDP	0.0.0.0:1046	***		296
UDP	0.0.0.0:1078	***		296
UDP	0.0.0.0:4500	***		1692
UDP	127.0.0.1:103	***		1000

This means that you can monitor a suspicious network connection and link it to the process Id. This information can be used together with the task manager or an alternative system to identify processes that are attempting to access the network.

In a practical situation an administrator would probably start with a suspicious process from task manager and then check netstat –nao to see if there are network connections that are owned by that PID.

The opposite approach of starting with the network connection could also be taken, as long as all unnecessary applications were shut down to achieve a relatively quiescent state.

## Patch It!

Patching is more of a proactive, preventative measure than a remediation action. It is definitely one of the best preventative actions you can take and should be part of your after action plan.

However, many administrators have been able to stop worms by applying patches on computer systems. I have observed this myself and corroborated with other administrators. An executable component may still be left behind in multiple locations with registry keys to execute it. However if the code is dependent on an exploit to run with elevated privileges, the patch may effectively neuter the exploit. The safe bet of course is rebuild the system, restore data from a trusted backup, and then apply patches. But patching may enable you to check the spread of an outbreak until there is time for rebuilding.



## The File System

When dealing with a system that is acting abnormally, it is helpful to determine if system files have been added, modified, or replaced.

### ***Windows Find***

The Windows “Find” function can be used to look for recently added files that may coincide with the onset of strange behavior associated with your infection. This approach generally works better with servers in a controlled environment than on a user’s workstation, unless your organization has done a real good job of locking them down. For some further tips on behavior based anti-virus work, check out Robert B. Fried’s practical, [A System Administrator’s Guide to Implementing Various Anti-Virus Mechanisms](http://www.sans.org/rr/whitepapers/malicious/43.php) available at the Sans Reading Room.<sup>4</sup>

If a data integrity solution has been used to baseline the system then the task is much easier. Without a data integrity solution, you may be able to determine the authenticity of a particular file using vendor file lists.

### ***Data Integrity Solutions***

A Data Integrity Assurance solution is the most certain way to tell if a file or system has been compromised. The common denominator of these is that cryptographic hashes are run against your important system and data files so you have a baseline to compare them against in order to verify a file’s integrity.

Commercial solutions such as Tripwire have demonstrated their effectiveness and are used by many organizations. They are more prevalent in large enterprises due to their cost and overhead to manage. Another obvious factor is they are of no value after an infection if the solution was not in place prior to such infection

### ***Vendor File Lists***

In order to determine if a file has been modified you can go to some vendor sites and look up the details of the file in question. This solution is far from foolproof. If the vendor does not have file checksums but only file size and date, you cannot say for certain that the file is unaltered, and would be advised to either replace the file or rebuild the system.

Many software vendors do provide checksums for their installation packages, if not a file-by-file list. If Microsoft provides itemized lists of files with checksums, I have not found them.

---

<sup>4</sup> <http://www.sans.org/rr/whitepapers/malicious/43.php>

You usually find MS file lists in a knowledgebase article on Technet, such as the following. <http://support.microsoft.com/?kbid=310504> That particular list is file list 1 of 2, and it only applies to Internet Explorer 6.0. If you have patched or upgraded, then this particular list will be useless to you. You have to dive into the details of each upgrade or patch.

## Conclusion

In IT administration there are situations that fall somewhere between the option of “just rebuild it” on one hand and a full-blown computer forensics investigation on the other. The IT world eagerly waits for anti-spyware solutions to reach maturity, particularly in their support of the enterprise customer. At that point who knows what new threats we will be dealing with. In the meantime, it is my hope that the tools and methods outlined in this paper will add value in the effort to isolate bits of malicious software.

© SANS Institute 2000 - 2005, Author retains full rights.

## Appendix A: References

A Goodie Basket for Grandma,  
Kevin Liston Sans ISC handler

<http://isc.sans.org/diary.php?date=2005-01-10>

Step-By-Step: Set Antivirus Software for Maximum Protection

<http://www.pcworld.com/howto/article/0,aid,106718,pg,1,00.asp>

Anti-Spyware Software Review – Ten commercial ASW products reviewed.

<http://anti-spyware-review.toptenreviews.com/>

"Alternate Data Streams: Out of the Shadows and into the Light" by Ryan L. Means

<http://www.sans.org/rr/whitepapers/honors/1503.php>

McAfee Stinger – Stand Alone anti-virus tool

<http://vil.nai.com/vil/stinger/>

Microsoft Windows Malicious Software Removal Tool

<http://support.microsoft.com/?id=890830>

Microsoft AntiSpyware (Giant)

<http://www.microsoft.com/athome/security/spyware/software/default.mspix>

SpyBot Search & Destroy

<http://www.safer-networking.org/en/download/>

Spyware Warrior Web Site

<http://spywarewarrior.com/>

The Ultimate Troubleshooter

[http://www.answersthatwork.com/TUT\\_pages/TUT\\_information.htm](http://www.answersthatwork.com/TUT_pages/TUT_information.htm)

A System Administrator's Guide to Implementing Various Anti-Virus Mechanisms Robert B. Fried, GIAC Practical Assignment. Sans Reading Room.

<http://www.sans.org/rr/whitepapers/malicious/43.php>

The Battle for the Desktop Rages On, Network Magazine, Mar 05 p. 25

<http://www.networkmagazine.com/shared/article/showArticle.jhtml;jsessionid=M0GPXFLYJ2Z1UQSNDBCSKH0CJUMKJVN?articleId=60401607&classroom=>

## Appendix B: Troubleshooting Checklist

Category	Method or Tool	Complete
<b>Anti-virus</b>		
	Update signatures	
	Heuristic Scanning	
	ADS Scanning	
	"Scrub" file with FAT drive	
	2 <sup>nd</sup> Anti-virus Vendor	
<b>Standalone AV</b>		
	Mcafee Stinger	
	MS Malicious Software Removal Tool	
<b>AntiSpyware</b>		
	Microsoft AntiSpyware	
	SpyBot S&D	
<b>Process Monitoring</b>		
	Windows Task Manager	
	TUT The Ultimate Troubleshooter	
	Wintasks 5 Professional	
<b>Network Connection Monitoring</b>		
	Desktop Firewall	
	Netstat -nao	
<b>Patching</b>		
<b>File Integrity Assurance</b>		
	Windows "Find" recently added files	
	Data Integrity Solution	
	Vendor File Lists	