Anubis - Analysis Report

Analysis Report for file.exe

MD5: 0f37839f48f7fc77e6d50e14657fb96e

Summary:

Description	Risk
Write to foreign memory areas: This executable tampers with the execution of another process.	high
Performs File Modification and Destruction: The executable modifies and destructs files which are not temporary.	low
AV Hit: This executable is detected by an antivirus software.	high
Packed Binary: This executable is protected with a packer in order to prevent it from being reverse engineered.	medium
Autostart capabilities: This executable registers processes to be executed at system start. This could result in unwanted actions to be performed automatically.	medium
Changes security settings of Internet Explorer: This system alteration could seriously affect safety surfing the World Wide Web.	low
Spawns Processes: The executable produces processes during the execution.	low
Execution did not terminate correctly: The executable crashed.	medium
Performs Registry Activities: The executable creates and/or modifies registry entries.	low

Dependency overview:

- **file.exe** C:\file.exe
  Analysis reason: Primary Analysis Subject
  - **Explorer.EXE** C:\WINDOWS\Explorer.EXE
    Analysis reason: file.exe wrote to the virtual memory of this process
  - **winlogon.exe** \??\C:\WINDOWS\system32\winlogon.exe
    Analysis reason: file.exe wrote to the virtual memory of this process
  - **services.exe** C:\WINDOWS\system32\services.exe
    Analysis reason: file.exe wrote to the virtual memory of this process
  - **lsass.exe** C:\WINDOWS\system32\lsass.exe
    Analysis reason: file.exe wrote to the virtual memory of this process
  - **svchost.exe** C:\WINDOWS\system32\svchost.exe
    Analysis reason: file.exe wrote to the virtual memory of this process
  - **svchost.exe** C:\WINDOWS\system32\svchost.exe
    Analysis reason: file.exe wrote to the virtual memory of this process
  - **svchost.exe** C:\WINDOWS\System32\svchost.exe
    Analysis reason: file.exe wrote to the virtual memory of this process
  - **svchost.exe** C:\WINDOWS\system32\svchost.exe
    Analysis reason: file.exe wrote to the virtual memory of this process
  - **svchost.exe** C:\WINDOWS\system32\svchost.exe
    Analysis reason: file.exe wrote to the virtual memory of this process
  - **spoolsv.exe** spoolsv.exe
    Analysis reason: file.exe wrote to the virtual memory of this process
  - **mscorsvw.exe** C:\WINDOWS\Microsoft.NET\Framework\v4.0.30319\mscorsvw.exe
    Analysis reason: file.exe wrote to the virtual memory of this process
  - **wuauclt.exe** C:\WINDOWS\system32\wuauclt.exe
    Analysis reason: file.exe wrote to the virtual memory of this process
  - **ctfmon.exe** C:\WINDOWS\system32\ctfmon.exe
    Analysis reason: file.exe wrote to the virtual memory of this process
  - **msmsgs.exe** C:\Program Files\Messenger\msmsgs.exe
    Analysis reason: file.exe wrote to the virtual memory of this process
  - **reader_sl.exe** C:\Program Files\Adobe\Reader 8.0\Reader\reader_sl.exe
    Analysis reason: file.exe wrote to the virtual memory of this process
  - **alg.exe** C:\WINDOWS\System32\alg.exe
    Analysis reason: file.exe wrote to the virtual memory of this process
  - **wscntfy.exe** wscntfy.exe
    Analysis reason: file.exe wrote to the virtual memory of this process
  - **drlwszvxbeo.exe** C:\Program Files\Common Files\drlwszvxbeo.exe
    Analysis reason: file.exe wrote to the virtual memory of this process
  - **kxuckd.exe** C:\Program Files\Common Files\kxuckd.exe
    Analysis reason: file.exe wrote to the virtual memory of this process
  - **cleansweep.exe** C:\cleansweep.exe\cleansweep.exe
    Analysis reason: Started by file.exe

Table of Contents:

1. General Information

Information about Anubis' invocation	
Time needed:	251 s
Report created:	08/12/11, 18:52:35 UTC
Termination reason:	Timeout
Program version:	1.75.3394

1.a) - Network Activity

DNS Queries:

Name	Query Type	Query Result	Successful	Protocol
freeways.in	DNS_TYPE_A		0	udp

TCP Connection Attempts:

From ANUBIS:1028 to 213.155.29.144:444

2. file.exe

General information about this executable	
Analysis Reason:	Primary Analysis Subject
Filename:	file.exe
MD5:	0f37839f48f7fc77e6d50e14657fb96e
SHA-1:	35698c61ad232ff90c5812372d23971118ea37cd
File Size:	82432
Command Line:	"C:\file.exe"
Process-status at analysis end:	dead
Exit Code:	0

Load-time Dlls

Module Name	Base Address	Size
C:\WINDOWS\system32\ntdll.dll	0x7C900000	0x000AF000
C:\WINDOWS\system32\kernel32.dll	0x7C800000	0x000F6000
C:\WINDOWS\system32\GDI32.dll	0x77F10000	0x00049000
C:\WINDOWS\system32\USER32.dll	0x7E410000	0x00091000

Run-time Dlls

Module Name	Base Address	Size
C:\WINDOWS\system32\Apphelp.dll	0x77B40000	0x00022000
C:\WINDOWS\system32\ADVAPI32.DLL	0x77DD0000	0x0009B000
C:\WINDOWS\system32\RPCRT4.dll	0x77E70000	0x00092000
C:\WINDOWS\system32\Secur32.dll	0x77FE0000	0x00011000

Ikarus Virus Scanner

Trojan-Spy.Win32.SpyEyes (Sig-Id:1342409)

2.a) file.exe - Registry Activities

Registry Values Read:

Key	Name	Value	Times
HKLM\SYSTEM\WPA\MediaCenter	Installed	0	1
HKLM\Software\Policies\Microsoft\Windows\Safer\CodeIdentifiers	AuthenticodeEnabled	0	1
HKLM\Software\Policies\Microsoft\Windows\Safer\CodeIdentifiers	DefaultLevel	262144	1

Registry Values Read:

Key	Name	Value	Times
HKLM\Software\Policies\Microsoft\Windows\Safer\CodeIdentifiers	PolicyScope	0	1
HKLM\Software\Policies\Microsoft\Windows\Safer\CodeIdentifiers	TransparentEnabled	1	2
HKLM\Software\Policies\Microsoft\Windows\Safer\CodeIdentifiers\0\Hashes\{349d35ab-37b5-462f-9b89-edd5fbde1328}	HashAlg	32771	1
HKLM\Software\Policies\Microsoft\Windows\Safer\CodeIdentifiers\0\Hashes\{349d35ab-37b5-462f-9b89-edd5fbde1328}	ItemData	0x5eab304f957a49896a006c1c31154015	1
HKLM\Software\Policies\Microsoft\Windows\Safer\CodeIdentifiers\0\Hashes\{349d35ab-37b5-462f-9b89-edd5fbde1328}	ItemSize	779	1
HKLM\Software\Policies\Microsoft\Windows\Safer\CodeIdentifiers\0\Hashes\{349d35ab-37b5-462f-9b89-edd5fbde1328}	SaferFlags	0	1
HKLM\Software\Policies\Microsoft\Windows\Safer\CodeIdentifiers\0\Hashes\{7fb9cd2e-3076-4df9-a57b-b813f72dbb91}	HashAlg	32771	1
HKLM\Software\Policies\Microsoft\Windows\Safer\CodeIdentifiers\0\Hashes\{7fb9cd2e-3076-4df9-a57b-b813f72dbb91}	ItemData	0x67b0d48b343a3fd3bce9dc646704f394	1
HKLM\Software\Policies\Microsoft\Windows\Safer\CodeIdentifiers\0\Hashes\{7fb9cd2e-3076-4df9-a57b-b813f72dbb91}	ItemSize	517	1
HKLM\Software\Policies\Microsoft\Windows\Safer\CodeIdentifiers\0\Hashes\{7fb9cd2e-3076-4df9-a57b-b813f72dbb91}	SaferFlags	0	1
HKLM\Software\Policies\Microsoft\Windows\Safer\CodeIdentifiers\0\Hashes\{81d1fe15-dd9d-4762-b16d-7c29ddecae3f}	HashAlg	32771	1
HKLM\Software\Policies\Microsoft\Windows\Safer\CodeIdentifiers\0\Hashes\{81d1fe15-dd9d-4762-b16d-7c29ddecae3f}	ItemData	0x327802dcfef8c893dc8ab006dd847d1d	1
HKLM\Software\Policies\Microsoft\Windows\Safer\CodeIdentifiers\0\Hashes\{81d1fe15-dd9d-4762-b16d-7c29ddecae3f}	ItemSize	918	1
HKLM\Software\Policies\Microsoft\Windows\Safer\CodeIdentifiers\0\Hashes\{81d1fe15-dd9d-4762-b16d-7c29ddecae3f}	SaferFlags	0	1
HKLM\Software\Policies\Microsoft\Windows\Safer\CodeIdentifiers\0\Hashes\{94e3e076-8f53-42a5-8411-085bcc18a68d}	HashAlg	32771	1
HKLM\Software\Policies\Microsoft\Windows\Safer\CodeIdentifiers\0\Hashes\{94e3e076-8f53-42a5-8411-085bcc18a68d}	ItemData	0xbd9a2adb42ebd8560e250e4df8162f67	1
HKLM\Software\Policies\Microsoft\Windows\Safer\CodeIdentifiers\0\Hashes\{94e3e076-8f53-42a5-8411-085bcc18a68d}	ItemSize	229	1
HKLM\Software\Policies\Microsoft\Windows\Safer\CodeIdentifiers\0\Hashes\{94e3e076-8f53-42a5-8411-085bcc18a68d}	SaferFlags	0	1
HKLM\Software\Policies\Microsoft\Windows\Safer\CodeIdentifiers\0\Hashes\{dc971ee5-44eb-4fe4-ae2e-b91490411bfc}	HashAlg	32771	1
HKLM\Software\Policies\Microsoft\Windows\Safer\CodeIdentifiers\0\Hashes\{dc971ee5-44eb-4fe4-ae2e-b91490411bfc}	ItemData	0x386b085f84ecf669d36b956a22c01e80	1
HKLM\Software\Policies\Microsoft\Windows\Safer\CodeIdentifiers\0\Hashes\{dc971ee5-44eb-4fe4-ae2e-b91490411bfc}	ItemSize	370	1
HKLM\Software\Policies\Microsoft\Windows\Safer\CodeIdentifiers\0\Hashes\{dc971ee5-44eb-4fe4-ae2e-b91490411bfc}	SaferFlags	0	1
HKLM\Software\Policies\Microsoft\Windows\Safer\CodeIdentifiers\0\Paths\{dda3f824-d8cb-441b-834d-be2efd2c1a33}	ItemData	%HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\Shell Folders\Cache%OLK*	1

Registry Values Read:

Key	Name	Value	Times
HKLM\Software\Policies\Microsoft\Windows\Safer\CodeIdentifiers\0\Paths\{dda3f824-d8cb-441b-834d-be2efd2c1a33}	SaferFlags	0	1
HKLM\System\CurrentControlSet\Control\Terminal Server	TSUserEnabled	0	1
HKU\S-1-5-21-842925246-1425521274-308236825-500\Software\Microsoft\Windows\CurrentVersion\Explorer\Shell Folders	Cache	C:\Documents and Settings\Administrator\Local Settings\Temporary Internet Files	1

2.b) file.exe - File Activities

Files Created:

C:\cleansweep.exe
C:\cleansweep.exe\cleansweep.exe
C:\cleansweep.exe\config.bin

Files Modified:

C:\cleansweep.exe\cleansweep.exe
C:\cleansweep.exe\config.bin

Directories Created:

C:\cleansweep.exe

File System Control Communication:

File	Control Code	Times
C:\Program Files\Common Files\	0x00090028	1

Memory Mapped Files:

File Name
C:\WINDOWS\system32\Apphelp.dll
C:\Windows\AppPatch\sysmain.sdb
C:\cleansweep.exe\cleansweep.exe
C:\file.exe
\systemroot\system32\kernel32.dll
\systemroot\system32\ntdll.dll
\systemroot\system32\user32.dll

2.c) file.exe - Process Activities

Processes Created:

Executable	Command Line
C:\cleansweep.exe\cleansweep.exe	
C:\cleansweep.exe\cleansweep.exe	

Remote Threads Created:

Affected Process
C:\cleansweep.exe\cleansweep.exe

Foreign Memory Regions Read:

Process: C:\cleansweep.exe\cleansweep.exe

Foreign Memory Regions Written:

Process: C:\Program Files\Adobe\Reader 8.0\Reader\reader_sl.exe
Process: C:\Program Files\Common Files\drlwszvxbeo.exe

Foreign Memory Regions Written:
Process: C:\Program Files\Common Files\kxuckd.exe
Process: C:\Program Files\Messenger\msmsgs.exe
Process: C:\WINDOWS\Microsoft.NET\Framework\v4.0.30319\mscorsvw.exe
Process: C:\WINDOWS\explorer.exe
Process: C:\WINDOWS\system32\alg.exe
Process: C:\WINDOWS\system32\ctfmon.exe
Process: C:\WINDOWS\system32\lsass.exe
Process: C:\WINDOWS\system32\services.exe
Process: C:\WINDOWS\system32\spoolsv.exe
Process: C:\WINDOWS\system32\svchost.exe
Process: C:\WINDOWS\system32\winlogon.exe
Process: C:\WINDOWS\system32\wscntfy.exe
Process: C:\WINDOWS\system32\wuauclt.exe
Process: C:\cleansweep.exe\cleansweep.exe
Process: C:\file.exe

3. Explorer.EXE

General information about this executable	
Analysis Reason:	file.exe wrote to the virtual memory of this process
Filename:	Explorer.EXE
MD5:	12896823fb95bfb3dc9b46bcaedc9923
SHA-1:	9d2bf84874abc5b6e9a2744b7865c193c08d362f
File Size:	1033728
Command Line:	C:\WINDOWS\Explorer.EXE
Process-status at analysis end:	alive
Exit Code:	0

Load-time Dlls

Module Name	Base Address	Size
C:\WINDOWS\system32\ntdll.dll	0x7C900000	0x000AF000
C:\WINDOWS\system32\kernel32.dll	0x7C800000	0x000F6000
C:\WINDOWS\system32\ADVAPI32.dll	0x77DD0000	0x0009B000
C:\WINDOWS\system32\RPCRT4.dll	0x77E70000	0x00092000
C:\WINDOWS\system32\Secur32.dll	0x77FE0000	0x00011000
C:\WINDOWS\system32\BROWSEUI.dll	0x75F80000	0x000FD000
C:\WINDOWS\system32\GDI32.dll	0x77F10000	0x00049000
C:\WINDOWS\system32\USER32.dll	0x7E410000	0x00091000
C:\WINDOWS\system32\msvcrt.dll	0x77C10000	0x00058000
C:\WINDOWS\system32\ole32.dll	0x774E0000	0x0013D000
C:\WINDOWS\system32\SHLWAPI.dll	0x77F60000	0x00076000
C:\WINDOWS\system32\OLEAUT32.dll	0x77120000	0x0008B000
C:\WINDOWS\system32\SHDOCVW.dll	0x7E290000	0x00171000
C:\WINDOWS\system32\CRYPT32.dll	0x77A80000	0x00095000
C:\WINDOWS\system32\MSASN1.dll	0x77B20000	0x00012000
C:\WINDOWS\system32\CRYPTUI.dll	0x754D0000	0x00080000
C:\WINDOWS\system32\NETAPI32.dll	0x5B860000	0x00055000
C:\WINDOWS\system32\VERSION.dll	0x77C00000	0x00008000
C:\WINDOWS\system32\WININET.dll	0x771B0000	0x000AA000
C:\WINDOWS\system32\WINTRUST.dll	0x76C30000	0x0002E000
C:\WINDOWS\system32\IMAGEHLP.dll	0x76C90000	0x00028000
C:\WINDOWS\system32\WLDAP32.dll	0x76F60000	0x0002C000
C:\WINDOWS\system32\SHELL32.dll	0x7C9C0000	0x00817000
C:\WINDOWS\system32\UxTheme.dll	0x5AD70000	0x00038000
C:\WINDOWS\system32\ShimEng.dll	0x5CB70000	0x00026000
C:\WINDOWS\AppPatch\AcGenral.DLL	0x6F880000	0x001CA000

Load-time Dlls

Module Name	Base Address	Size
C:\WINDOWS\system32\WINMM.dll	0x76B40000	0x0002D000
C:\WINDOWS\system32\MSACM32.dll	0x77BE0000	0x00015000
C:\WINDOWS\system32\USERENV.dll	0x769C0000	0x000B4000
C:\WINDOWS\WinSxS\x86_Microsoft.Windows.Common-Controls_6595b64144ccf1df_6.0.2600.5512_x-ww_35d4ce83\comctl32.dll	0x773D0000	0x00103000
C:\WINDOWS\system32\comctl32.dll	0x5D090000	0x0009A000
C:\WINDOWS\system32\appHelp.dll	0x77B40000	0x00022000
C:\WINDOWS\system32\CLBCATQ.DLL	0x76FD0000	0x0007F000
C:\WINDOWS\system32\COMRes.dll	0x77050000	0x000C5000
C:\WINDOWS\System32\cscui.dll	0x77A20000	0x00054000
C:\WINDOWS\System32\CSCDLL.dll	0x76600000	0x0001D000
C:\WINDOWS\system32\themeui.dll	0x5BA60000	0x00071000
C:\WINDOWS\system32\MSIMG32.dll	0x76380000	0x00005000
C:\WINDOWS\system32\xpsp2res.dll	0x00AC0000	0x002C5000
C:\WINDOWS\system32\actxprxy.dll	0x71D40000	0x0001B000
C:\WINDOWS\system32\msutb.dll	0x5FC10000	0x00033000
C:\WINDOWS\system32\MSCTF.dll	0x74720000	0x0004C000
C:\WINDOWS\system32\urlmon.dll	0x7E1E0000	0x000A2000
C:\WINDOWS\system32\LINKINFO.dll	0x76980000	0x00008000
C:\WINDOWS\system32\ntshrui.dll	0x76990000	0x00025000
C:\WINDOWS\system32\ATL.DLL	0x76B20000	0x00011000
C:\WINDOWS\system32\rsaenh.dll	0x68000000	0x00036000
C:\WINDOWS\system32\msi.dll	0x7D1E0000	0x002BC000
C:\WINDOWS\system32\WINSTA.dll	0x76360000	0x00010000
C:\WINDOWS\system32\webcheck.dll	0x74B30000	0x00046000
C:\WINDOWS\system32\WSOCK32.dll	0x71AD0000	0x00009000
C:\WINDOWS\system32\WS2_32.dll	0x71AB0000	0x00017000
C:\WINDOWS\system32\WS2HELP.dll	0x71AA0000	0x00008000
C:\WINDOWS\system32\stobject.dll	0x76280000	0x00021000
C:\WINDOWS\system32\BatMeter.dll	0x74AF0000	0x0000A000
C:\WINDOWS\system32\POWRPROF.dll	0x74AD0000	0x00008000
C:\WINDOWS\system32\SETUPAPI.dll	0x77920000	0x000F3000
C:\WINDOWS\system32\WTSAPI32.dll	0x76F50000	0x00008000
C:\WINDOWS\system32\NETSHELL.dll	0x76400000	0x001A5000
C:\WINDOWS\system32\credui.dll	0x76C00000	0x0002E000
C:\WINDOWS\system32\dot3api.dll	0x478C0000	0x0000A000
C:\WINDOWS\system32\rtutils.dll	0x76E80000	0x0000E000
C:\WINDOWS\system32\dot3dlg.dll	0x736D0000	0x00006000
C:\WINDOWS\system32\OneX.DLL	0x5DCA0000	0x00028000
C:\WINDOWS\system32\eappcfg.dll	0x745B0000	0x00022000
C:\WINDOWS\system32\MSVCP60.dll	0x76080000	0x00065000
C:\WINDOWS\system32\eappprxy.dll	0x5DCD0000	0x0000E000
C:\WINDOWS\system32\iphlpapi.dll	0x76D60000	0x00019000
C:\WINDOWS\system32\MPR.dll	0x71B20000	0x00012000
C:\WINDOWS\System32\drprov.dll	0x75F60000	0x00007000
C:\WINDOWS\System32\ntlanman.dll	0x71C10000	0x0000E000
C:\WINDOWS\System32\NETUI0.dll	0x71CD0000	0x00017000
C:\WINDOWS\System32\NETUI1.dll	0x71C90000	0x00040000
C:\WINDOWS\System32\NETRAP.dll	0x71C80000	0x00007000
C:\WINDOWS\System32\SAMLIB.dll	0x71BF0000	0x00013000
C:\WINDOWS\System32\davclnt.dll	0x75F70000	0x0000A000
C:\WINDOWS\system32\comdlg32.dll	0x763B0000	0x00049000
C:\WINDOWS\system32\MSGINA.dll	0x75970000	0x000F8000
C:\WINDOWS\system32\ODBC32.dll	0x74320000	0x0003D000
C:\WINDOWS\system32\odbcint.dll	0x01350000	0x00017000
C:\WINDOWS\system32\browselc.dll	0x71600000	0x00012000

Load-time Dlls		
Module Name	**Base Address**	**Size**
C:\WINDOWS\system32\shdoclc.dll	0x71800000	0x00088000

3.a) Explorer.EXE - Registry Activities

Registry Values Modified:		
Key	**Name**	**New Value**
HKU\S-1-5-21-842925246-1425521274-308236825-500\SOFTWARE\MICROSOFT\WINDOWS\CURRENTVERSION\RUN	cleansweep.exe	C:\cleansweep.exe\cleansweep.exe

3.b) Explorer.EXE - File Activities

Device Control Communication:		
File	**Control Code**	**Times**
unnamed file	0x00228144	1

Memory Mapped Files:
File Name
\systemroot\system32\advapi32.dll
\systemroot\system32\kernel32.dll
\systemroot\system32\ntdll.dll

3.c) Explorer.EXE - Process Activities

Remote Threads Created:
Affected Process
C:\WINDOWS\system32\winlogon.exe
C:\WINDOWS\system32\services.exe
C:\WINDOWS\system32\lsass.exe
C:\WINDOWS\system32\svchost.exe
C:\WINDOWS\system32\svchost.exe
C:\WINDOWS\system32\svchost.exe
C:\WINDOWS\system32\svchost.exe
C:\WINDOWS\system32\svchost.exe

Foreign Memory Regions Written:
Process: C:\WINDOWS\system32\lsass.exe
Process: C:\WINDOWS\system32\services.exe
Process: C:\WINDOWS\system32\spoolsv.exe
Process: C:\WINDOWS\system32\svchost.exe
Process: C:\WINDOWS\system32\winlogon.exe

3.d) Explorer.EXE - Other Activities

Mutexes Created:
__CLEANSWEEP__

Keyboard Keys Monitored:	
Virtual Key Code	**Times**
VK_LBUTTON (1)	96

4. winlogon.exe

General information about this executable	
Analysis Reason:	file.exe wrote to the virtual memory of this process

General information about this executable

Filename:	winlogon.exe
Command Line:	winlogon.exe
Process-status at analysis end:	alive
Exit Code:	0

Load-time Dlls

Module Name	Base Address	Size
C:\WINDOWS\system32\ntdll.dll	0x7C900000	0x000AF000
C:\WINDOWS\system32\kernel32.dll	0x7C800000	0x000F6000
C:\WINDOWS\system32\ADVAPI32.dll	0x77DD0000	0x0009B000
C:\WINDOWS\system32\RPCRT4.dll	0x77E70000	0x00092000
C:\WINDOWS\system32\Secur32.dll	0x77FE0000	0x00011000
C:\WINDOWS\system32\AUTHZ.dll	0x776C0000	0x00012000
C:\WINDOWS\system32\msvcrt.dll	0x77C10000	0x00058000
C:\WINDOWS\system32\CRYPT32.dll	0x77A80000	0x00095000
C:\WINDOWS\system32\MSASN1.dll	0x77B20000	0x00012000
C:\WINDOWS\system32\USER32.dll	0x7E410000	0x00091000
C:\WINDOWS\system32\GDI32.dll	0x77F10000	0x00049000
C:\WINDOWS\system32\NDdeApi.dll	0x75940000	0x00008000
C:\WINDOWS\system32\PROFMAP.dll	0x75930000	0x0000A000
C:\WINDOWS\system32\NETAPI32.dll	0x5B860000	0x00055000
C:\WINDOWS\system32\USERENV.dll	0x769C0000	0x000B4000
C:\WINDOWS\system32\PSAPI.DLL	0x76BF0000	0x0000B000
C:\WINDOWS\system32\REGAPI.dll	0x76BC0000	0x0000F000
C:\WINDOWS\system32\SETUPAPI.dll	0x77920000	0x000F3000
C:\WINDOWS\system32\VERSION.dll	0x77C00000	0x00008000
C:\WINDOWS\system32\WINSTA.dll	0x76360000	0x00010000
C:\WINDOWS\system32\WINTRUST.dll	0x76C30000	0x0002E000
C:\WINDOWS\system32\IMAGEHLP.dll	0x76C90000	0x00028000
C:\WINDOWS\system32\WS2_32.dll	0x71AB0000	0x00017000
C:\WINDOWS\system32\WS2HELP.dll	0x71AA0000	0x00008000
C:\WINDOWS\system32\MSGINA.dll	0x75970000	0x000F8000
C:\WINDOWS\system32\COMCTL32.dll	0x5D090000	0x0009A000
C:\WINDOWS\system32\ODBC32.dll	0x74320000	0x0003D000
C:\WINDOWS\system32\comdlg32.dll	0x763B0000	0x00049000
C:\WINDOWS\system32\SHELL32.dll	0x7C9C0000	0x00817000
C:\WINDOWS\system32\SHLWAPI.dll	0x77F60000	0x00076000
C:\WINDOWS\WinSxS\x86_Microsoft.Windows.Common-Controls_6595b64144ccf1df_6.0.2600.5512_x-ww_35d4ce83\comctl32.dll	0x773D0000	0x00103000
C:\WINDOWS\system32\odbcint.dll	0x00930000	0x00017000
C:\WINDOWS\system32\SHSVCS.dll	0x776E0000	0x00023000
C:\WINDOWS\system32\sfc.dll	0x76BB0000	0x00005000
C:\WINDOWS\system32\sfc_os.dll	0x76C60000	0x0002A000
C:\WINDOWS\system32\ole32.dll	0x774E0000	0x0013D000
C:\WINDOWS\system32\Apphelp.dll	0x77B40000	0x00022000
C:\WINDOWS\system32\WINSCARD.DLL	0x723D0000	0x0001C000
C:\WINDOWS\system32\WTSAPI32.dll	0x76F50000	0x00008000
C:\WINDOWS\system32\WINMM.dll	0x76B40000	0x0002D000
C:\WINDOWS\system32\uxtheme.dll	0x5AD70000	0x00038000
C:\WINDOWS\system32\cscdll.dll	0x76600000	0x0001D000
C:\WINDOWS\System32\dimsntfy.dll	0x47020000	0x00008000
C:\WINDOWS\system32\WlNotify.dll	0x75950000	0x0001A000
C:\WINDOWS\system32\MPR.dll	0x71B20000	0x00012000
C:\WINDOWS\system32\WINSPOOL.DRV	0x73000000	0x00026000
C:\WINDOWS\system32\rsaenh.dll	0x68000000	0x00036000
C:\WINDOWS\system32\SAMLIB.dll	0x71BF0000	0x00013000
C:\WINDOWS\system32\sxs.dll	0x7E720000	0x000B0000

Load-time Dlls		
Module Name	**Base Address**	**Size**
C:\WINDOWS\system32\msv1_0.dll	0x77C70000	0x00024000
C:\WINDOWS\system32\iphlpapi.dll	0x76D60000	0x00019000
C:\WINDOWS\system32\wldap32.dll	0x76F60000	0x0002C000
C:\WINDOWS\system32\cscui.dll	0x77A20000	0x00054000
C:\WINDOWS\system32\xpsp2res.dll	0x01760000	0x002C5000
C:\WINDOWS\system32\NTMARTA.DLL	0x77690000	0x00021000
C:\WINDOWS\system32\COMRes.dll	0x77050000	0x000C5000
C:\WINDOWS\system32\OLEAUT32.dll	0x77120000	0x0008B000
C:\WINDOWS\system32\CLBCATQ.DLL	0x76FD0000	0x0007F000

4.a) winlogon.exe - File Activities

Memory Mapped Files:
File Name
\systemroot\system32\ntdll.dll

5. services.exe

General information about this executable	
Analysis Reason:	file.exe wrote to the virtual memory of this process
Filename:	services.exe
MD5:	0e776ed5f7cc9f94299e70461b7b8185
SHA-1:	cb5a33cec4c7b8ef4bd5dc8c241005b66b26cbbf
File Size:	108544
Command Line:	C:\WINDOWS\system32\services.exe
Process-status at analysis end:	alive
Exit Code:	0

Load-time Dlls		
Module Name	**Base Address**	**Size**
C:\WINDOWS\system32\ntdll.dll	0x7C900000	0x000AF000
C:\WINDOWS\system32\kernel32.dll	0x7C800000	0x000F6000
C:\WINDOWS\system32\ADVAPI32.dll	0x77DD0000	0x0009B000
C:\WINDOWS\system32\RPCRT4.dll	0x77E70000	0x00092000
C:\WINDOWS\system32\Secur32.dll	0x77FE0000	0x00011000
C:\WINDOWS\system32\msvcrt.dll	0x77C10000	0x00058000
C:\WINDOWS\system32\NCObjAPI.DLL	0x5F770000	0x0000C000
C:\WINDOWS\system32\MSVCP60.dll	0x76080000	0x00065000
C:\WINDOWS\system32\SCESRV.dll	0x7DBD0000	0x00051000
C:\WINDOWS\system32\AUTHZ.dll	0x776C0000	0x00012000
C:\WINDOWS\system32\USER32.dll	0x7E410000	0x00091000
C:\WINDOWS\system32\GDI32.dll	0x77F10000	0x00049000
C:\WINDOWS\system32\USERENV.dll	0x769C0000	0x000B4000
C:\WINDOWS\system32\umpnpmgr.dll	0x7DBA0000	0x00021000
C:\WINDOWS\system32\WINSTA.dll	0x76360000	0x00010000
C:\WINDOWS\system32\NETAPI32.dll	0x5B860000	0x00055000
C:\WINDOWS\system32\ShimEng.dll	0x5CB70000	0x00026000
C:\WINDOWS\AppPatch\AcAdProc.dll	0x47260000	0x0000F000
C:\WINDOWS\system32\Apphelp.dll	0x77B40000	0x00022000
C:\WINDOWS\system32\VERSION.dll	0x77C00000	0x00008000
C:\WINDOWS\system32\eventlog.dll	0x77B70000	0x00011000
C:\WINDOWS\system32\PSAPI.DLL	0x76BF0000	0x0000B000
C:\WINDOWS\system32\WS2_32.dll	0x71AB0000	0x00017000
C:\WINDOWS\system32\WS2HELP.dll	0x71AA0000	0x00008000
C:\WINDOWS\system32\wtsapi32.dll	0x76F50000	0x00008000

5.a) services.exe - File Activities

Memory Mapped Files:

File Name
\systemroot\system32\ntdll.dll

6. lsass.exe

General information about this executable

Analysis Reason:	file.exe wrote to the virtual memory of this process
Filename:	lsass.exe
MD5:	bf2466b3e18e970d8a976fb95fc1ca85
SHA-1:	de5a73cbb5f51f64c53fb4277ef2c23e70db123f
File Size:	13312
Command Line:	C:\WINDOWS\system32\lsass.exe
Process-status at analysis end:	alive
Exit Code:	0

Load-time Dlls

Module Name	Base Address	Size
C:\WINDOWS\system32\ntdll.dll	0x7C900000	0x000AF000
C:\WINDOWS\system32\kernel32.dll	0x7C800000	0x000F6000
C:\WINDOWS\system32\ADVAPI32.dll	0x77DD0000	0x0009B000
C:\WINDOWS\system32\RPCRT4.dll	0x77E70000	0x00092000
C:\WINDOWS\system32\Secur32.dll	0x77FE0000	0x00011000
C:\WINDOWS\system32\LSASRV.dll	0x75730000	0x000B5000
C:\WINDOWS\system32\MPR.dll	0x71B20000	0x00012000
C:\WINDOWS\system32\USER32.dll	0x7E410000	0x00091000
C:\WINDOWS\system32\GDI32.dll	0x77F10000	0x00049000
C:\WINDOWS\system32\MSASN1.dll	0x77B20000	0x00012000
C:\WINDOWS\system32\msvcrt.dll	0x77C10000	0x00058000
C:\WINDOWS\system32\NETAPI32.dll	0x5B860000	0x00055000
C:\WINDOWS\system32\NTDSAPI.dll	0x767A0000	0x00013000
C:\WINDOWS\system32\DNSAPI.dll	0x76F20000	0x00027000
C:\WINDOWS\system32\WS2_32.dll	0x71AB0000	0x00017000
C:\WINDOWS\system32\WS2HELP.dll	0x71AA0000	0x00008000
C:\WINDOWS\system32\WLDAP32.dll	0x76F60000	0x0002C000
C:\WINDOWS\system32\SAMLIB.dll	0x71BF0000	0x00013000
C:\WINDOWS\system32\SAMSRV.dll	0x74440000	0x0006A000
C:\WINDOWS\system32\cryptdll.dll	0x76790000	0x0000C000
C:\WINDOWS\system32\ShimEng.dll	0x5CB70000	0x00026000
C:\WINDOWS\AppPatch\AcGenral.DLL	0x6F880000	0x001CA000
C:\WINDOWS\system32\WINMM.dll	0x76B40000	0x0002D000
C:\WINDOWS\system32\ole32.dll	0x774E0000	0x0013D000
C:\WINDOWS\system32\OLEAUT32.dll	0x77120000	0x0008B000
C:\WINDOWS\system32\MSACM32.dll	0x77BE0000	0x00015000
C:\WINDOWS\system32\VERSION.dll	0x77C00000	0x00008000
C:\WINDOWS\system32\SHELL32.dll	0x7C9C0000	0x00817000
C:\WINDOWS\system32\SHLWAPI.dll	0x77F60000	0x00076000
C:\WINDOWS\system32\USERENV.dll	0x769C0000	0x000B4000
C:\WINDOWS\system32\UxTheme.dll	0x5AD70000	0x00038000
C:\WINDOWS\WinSxS\x86_Microsoft.Windows.Common-Controls_6595b64144ccf1df_6.0.2600.5512_x-ww_35d4ce83\comctl32.dll	0x773D0000	0x00103000
C:\WINDOWS\system32\comctl32.dll	0x5D090000	0x0009A000
C:\WINDOWS\system32\msprivs.dll	0x4D200000	0x0000E000
C:\WINDOWS\system32\kerberos.dll	0x71CF0000	0x0004C000
C:\WINDOWS\system32\msv1_0.dll	0x77C70000	0x00024000
C:\WINDOWS\system32\iphlpapi.dll	0x76D60000	0x00019000

Load-time Dlls		
Module Name	**Base Address**	**Size**
C:\WINDOWS\system32\netlogon.dll	0x744B0000	0x00065000
C:\WINDOWS\system32\w32time.dll	0x767C0000	0x0002C000
C:\WINDOWS\system32\MSVCP60.dll	0x76080000	0x00065000
C:\WINDOWS\system32\schannel.dll	0x767F0000	0x00027000
C:\WINDOWS\system32\CRYPT32.dll	0x77A80000	0x00095000
C:\WINDOWS\system32\wdigest.dll	0x74380000	0x0000F000
C:\WINDOWS\system32\rsaenh.dll	0x68000000	0x00036000
C:\WINDOWS\system32\scecli.dll	0x74410000	0x0002F000
C:\WINDOWS\system32\SETUPAPI.dll	0x77920000	0x000F3000
C:\WINDOWS\system32\ipsecsvc.dll	0x743E0000	0x0002F000
C:\WINDOWS\system32\AUTHZ.dll	0x776C0000	0x00012000
C:\WINDOWS\system32\oakley.DLL	0x75D90000	0x000D0000
C:\WINDOWS\system32\WINIPSEC.DLL	0x74370000	0x0000B000
C:\WINDOWS\system32\mswsock.dll	0x71A50000	0x0003F000
C:\WINDOWS\system32\hnetcfg.dll	0x662B0000	0x00058000
C:\WINDOWS\System32\wshtcpip.dll	0x71A90000	0x00008000
C:\WINDOWS\system32\dssenh.dll	0x68100000	0x00026000
C:\WINDOWS\system32\pstorsvc.dll	0x743A0000	0x0000B000
C:\WINDOWS\system32\psbase.dll	0x743C0000	0x0001B000

6.a) lsass.exe - Registry Activities

Registry Values Read:			
Key	**Name**	**Value**	**Times**
HKLM\SECURITY\Policy\SecDesc		0x0100048098000000a8000000000000001 1400000002008400060000000100	2

6.b) lsass.exe - File Activities

Files Read:
C:\lsass, Flags: Named pipe

Files Modified:
C:\lsass, Flags: Named pipe

File System Control Communication:		
File	**Control Code**	**Times**
C:\lsass, Flags: Named pipe	0x00110004	4
C:\lsass, Flags: Named pipe	0x00110008	2
C:\lsass, Flags: Named pipe	0x00110024	4
C:\lsass, Flags: Named pipe	0x0011001C	8

Memory Mapped Files:
File Name
\systemroot\system32\ntdll.dll

7. svchost.exe

General information about this executable	
Analysis Reason:	file.exe wrote to the virtual memory of this process
Filename:	svchost.exe
MD5:	27c6d03bcdb8cfeb96b716f3d8be3e18
SHA-1:	49083ae3725a0488e0a8fbbe1335c745f70c4667
File Size:	14336

General information about this executable

Command Line:	C:\WINDOWS\system32\svchost -k DcomLaunch
Process-status at analysis end:	alive
Exit Code:	0

Load-time Dlls

Module Name	Base Address	Size
C:\WINDOWS\system32\ntdll.dll	0x7C900000	0x000AF000
C:\WINDOWS\system32\kernel32.dll	0x7C800000	0x000F6000
C:\WINDOWS\system32\ADVAPI32.dll	0x77DD0000	0x0009B000
C:\WINDOWS\system32\RPCRT4.dll	0x77E70000	0x00092000
C:\WINDOWS\system32\Secur32.dll	0x77FE0000	0x00011000
C:\WINDOWS\system32\ShimEng.dll	0x5CB70000	0x00026000
C:\WINDOWS\AppPatch\AcGenral.DLL	0x6F880000	0x001CA000
C:\WINDOWS\system32\USER32.dll	0x7E410000	0x00091000
C:\WINDOWS\system32\GDI32.dll	0x77F10000	0x00049000
C:\WINDOWS\system32\WINMM.dll	0x76B40000	0x0002D000
C:\WINDOWS\system32\ole32.dll	0x774E0000	0x0013D000
C:\WINDOWS\system32\msvcrt.dll	0x77C10000	0x00058000
C:\WINDOWS\system32\OLEAUT32.dll	0x77120000	0x0008B000
C:\WINDOWS\system32\MSACM32.dll	0x77BE0000	0x00015000
C:\WINDOWS\system32\VERSION.dll	0x77C00000	0x00008000
C:\WINDOWS\system32\SHELL32.dll	0x7C9C0000	0x00817000
C:\WINDOWS\system32\SHLWAPI.dll	0x77F60000	0x00076000
C:\WINDOWS\system32\USERENV.dll	0x769C0000	0x000B4000
C:\WINDOWS\system32\UxTheme.dll	0x5AD70000	0x00038000
C:\WINDOWS\WinSxS\x86_Microsoft.Windows.Common-Controls_6595b64144ccf1df_6.0.2600.5512_x-ww_35d4ce83\comctl32.dll	0x773D0000	0x00103000
C:\WINDOWS\system32\comctl32.dll	0x5D090000	0x0009A000
C:\WINDOWS\system32\NTMARTA.DLL	0x77690000	0x00021000
C:\WINDOWS\system32\SAMLIB.dll	0x71BF0000	0x00013000
C:\WINDOWS\system32\WLDAP32.dll	0x76F60000	0x0002C000
c:\windows\system32\rpcss.dll	0x76A80000	0x00064000
c:\windows\system32\WS2_32.dll	0x71AB0000	0x00017000
c:\windows\system32\WS2HELP.dll	0x71AA0000	0x00008000
C:\WINDOWS\system32\xpsp2res.dll	0x005F0000	0x002C5000
C:\WINDOWS\system32\CLBCATQ.DLL	0x76FD0000	0x0007F000
C:\WINDOWS\system32\COMRes.dll	0x77050000	0x000C5000
c:\windows\system32\termsrv.dll	0x760F0000	0x00053000
c:\windows\system32\ICAAPI.dll	0x74F70000	0x00006000
c:\windows\system32\SETUPAPI.dll	0x77920000	0x000F3000
C:\WINDOWS\system32\WINTRUST.dll	0x76C30000	0x0002E000
C:\WINDOWS\system32\CRYPT32.dll	0x77A80000	0x00095000
C:\WINDOWS\system32\MSASN1.dll	0x77B20000	0x00012000
C:\WINDOWS\system32\IMAGEHLP.dll	0x76C90000	0x00028000
c:\windows\system32\AUTHZ.dll	0x776C0000	0x00012000
c:\windows\system32\mstlsapi.dll	0x75110000	0x0001F000
c:\windows\system32\ACTIVEDS.dll	0x77CC0000	0x00032000
c:\windows\system32\adsldpc.dll	0x76E10000	0x00025000
C:\WINDOWS\system32\NETAPI32.dll	0x5B860000	0x00055000
c:\windows\system32\ATL.DLL	0x76B20000	0x00011000
C:\WINDOWS\system32\REGAPI.dll	0x76BC0000	0x0000F000
C:\WINDOWS\system32\rsaenh.dll	0x68000000	0x00036000
C:\WINDOWS\system32\Apphelp.dll	0x77B40000	0x00022000

7.a) svchost.exe - File Activities

Memory Mapped Files:
File Name
\systemroot\system32\ntdll.dll

8. svchost.exe

General information about this executable	
Analysis Reason:	file.exe wrote to the virtual memory of this process
Filename:	svchost.exe
Command Line:	C:\WINDOWS\system32\svchost -k rpcss
Process-status at analysis end:	alive
Exit Code:	0

Load-time Dlls

Module Name	Base Address	Size
C:\WINDOWS\system32\ntdll.dll	0x7C900000	0x000AF000
C:\WINDOWS\system32\kernel32.dll	0x7C800000	0x000F6000
C:\WINDOWS\system32\ADVAPI32.dll	0x77DD0000	0x0009B000
C:\WINDOWS\system32\RPCRT4.dll	0x77E70000	0x00092000
C:\WINDOWS\system32\Secur32.dll	0x77FE0000	0x00011000
C:\WINDOWS\system32\ShimEng.dll	0x5CB70000	0x00026000
C:\WINDOWS\AppPatch\AcGenral.DLL	0x6F880000	0x001CA000
C:\WINDOWS\system32\USER32.dll	0x7E410000	0x00091000
C:\WINDOWS\system32\GDI32.dll	0x77F10000	0x00049000
C:\WINDOWS\system32\WINMM.dll	0x76B40000	0x0002D000
C:\WINDOWS\system32\ole32.dll	0x774E0000	0x0013D000
C:\WINDOWS\system32\msvcrt.dll	0x77C10000	0x00058000
C:\WINDOWS\system32\OLEAUT32.dll	0x77120000	0x0008B000
C:\WINDOWS\system32\MSACM32.dll	0x77BE0000	0x00015000
C:\WINDOWS\system32\VERSION.dll	0x77C00000	0x00008000
C:\WINDOWS\system32\SHELL32.dll	0x7C9C0000	0x00817000
C:\WINDOWS\system32\SHLWAPI.dll	0x77F60000	0x00076000
C:\WINDOWS\system32\USERENV.dll	0x769C0000	0x000B4000
C:\WINDOWS\system32\UxTheme.dll	0x5AD70000	0x00038000
C:\WINDOWS\WinSxS\x86_Microsoft.Windows.Common-Controls_6595b64144ccf1df_6.0.2600.5512_x-ww_35d4ce83\comctl32.dll	0x773D0000	0x00103000
C:\WINDOWS\system32\comctl32.dll	0x5D090000	0x0009A000
c:\windows\system32\rpcss.dll	0x76A80000	0x00064000
c:\windows\system32\WS2_32.dll	0x71AB0000	0x00017000
c:\windows\system32\WS2HELP.dll	0x71AA0000	0x00008000
C:\WINDOWS\system32\xpsp2res.dll	0x005F0000	0x002C5000
C:\WINDOWS\system32\rsaenh.dll	0x68000000	0x00036000
C:\WINDOWS\system32\mswsock.dll	0x71A50000	0x0003F000
C:\WINDOWS\system32\hnetcfg.dll	0x662B0000	0x00058000
C:\WINDOWS\System32\wshtcpip.dll	0x71A90000	0x00008000
C:\WINDOWS\system32\DNSAPI.dll	0x76F20000	0x00027000
C:\WINDOWS\system32\iphlpapi.dll	0x76D60000	0x00019000
C:\WINDOWS\System32\winrnr.dll	0x76FB0000	0x00008000
C:\WINDOWS\system32\WLDAP32.dll	0x76F60000	0x0002C000
C:\WINDOWS\system32\rasadhlp.dll	0x76FC0000	0x00006000
C:\WINDOWS\system32\CLBCATQ.DLL	0x76FD0000	0x0007F000
C:\WINDOWS\system32\COMRes.dll	0x77050000	0x000C5000

8.a) svchost.exe - File Activities

Memory Mapped Files:

File Name
\systemroot\system32\ntdll.dll

9. svchost.exe

General information about this executable

Analysis Reason:	file.exe wrote to the virtual memory of this process
Filename:	svchost.exe
Command Line:	C:\WINDOWS\System32\svchost.exe -k netsvcs
Process-status at analysis end:	alive
Exit Code:	0

Load-time Dlls

Module Name	Base Address	Size
C:\WINDOWS\system32\ntdll.dll	0x7C900000	0x000AF000
C:\WINDOWS\system32\kernel32.dll	0x7C800000	0x000F6000
C:\WINDOWS\system32\ADVAPI32.dll	0x77DD0000	0x0009B000
C:\WINDOWS\system32\RPCRT4.dll	0x77E70000	0x00092000
C:\WINDOWS\system32\Secur32.dll	0x77FE0000	0x00011000
C:\WINDOWS\System32\ShimEng.dll	0x5CB70000	0x00026000
C:\WINDOWS\AppPatch\AcGenral.DLL	0x6F880000	0x001CA000
C:\WINDOWS\system32\USER32.dll	0x7E410000	0x00091000
C:\WINDOWS\system32\GDI32.dll	0x77F10000	0x00049000
C:\WINDOWS\System32\WINMM.dll	0x76B40000	0x0002D000
C:\WINDOWS\system32\ole32.dll	0x774E0000	0x0013D000
C:\WINDOWS\system32\msvcrt.dll	0x77C10000	0x00058000
C:\WINDOWS\system32\OLEAUT32.dll	0x77120000	0x0008B000
C:\WINDOWS\System32\MSACM32.dll	0x77BE0000	0x00015000
C:\WINDOWS\system32\VERSION.dll	0x77C00000	0x00008000
C:\WINDOWS\system32\SHELL32.dll	0x7C9C0000	0x00817000
C:\WINDOWS\system32\SHLWAPI.dll	0x77F60000	0x00076000
C:\WINDOWS\system32\USERENV.dll	0x769C0000	0x000B4000
C:\WINDOWS\System32\UxTheme.dll	0x5AD70000	0x00038000
C:\WINDOWS\WinSxS\x86_Microsoft.Windows.Common-Controls_6595b64144ccf1df_6.0.2600.5512_x-ww_35d4ce83\comctl32.dll	0x773D0000	0x00103000
C:\WINDOWS\system32\comctl32.dll	0x5D090000	0x0009A000
C:\WINDOWS\System32\NTMARTA.DLL	0x77690000	0x00021000
C:\WINDOWS\System32\SAMLIB.dll	0x71BF0000	0x00013000
C:\WINDOWS\system32\WLDAP32.dll	0x76F60000	0x0002C000
C:\WINDOWS\System32\xpsp2res.dll	0x005B0000	0x002C5000
c:\windows\system32\shsvcs.dll	0x776E0000	0x00023000
C:\WINDOWS\System32\WINSTA.dll	0x76360000	0x00010000
C:\WINDOWS\system32\NETAPI32.dll	0x5B860000	0x00055000
C:\WINDOWS\System32\rsaenh.dll	0x68000000	0x00036000
c:\windows\system32\dhcpcsvc.dll	0x7D4B0000	0x00022000
c:\windows\system32\DNSAPI.dll	0x76F20000	0x00027000
c:\windows\system32\WS2_32.dll	0x71AB0000	0x00017000
c:\windows\system32\WS2HELP.dll	0x71AA0000	0x00008000
c:\windows\system32\iphlpapi.dll	0x76D60000	0x00019000
c:\windows\system32\wzcsvc.dll	0x7DB10000	0x0008C000
c:\windows\system32\rtutils.dll	0x76E80000	0x0000E000
c:\windows\system32\WMI.dll	0x76D30000	0x00004000
C:\WINDOWS\system32\CRYPT32.dll	0x77A80000	0x00095000
C:\WINDOWS\system32\MSASN1.dll	0x77B20000	0x00012000
c:\windows\system32\EapolQec.dll	0x72810000	0x0000B000
c:\windows\system32\ATL.DLL	0x76B20000	0x00011000

Load-time Dlls

Module Name	Base Address	Size
c:\windows\system32\QUtil.dll	0x726C0000	0x00016000
c:\windows\system32\MSVCP60.dll	0x76080000	0x00065000
c:\windows\system32\dot3api.dll	0x478C0000	0x0000A000
c:\windows\system32\WTSAPI32.dll	0x76F50000	0x00008000
c:\windows\system32\ESENT.dll	0x606B0000	0x0010D000
C:\WINDOWS\System32\CLBCATQ.DLL	0x76FD0000	0x0007F000
C:\WINDOWS\System32\COMRes.dll	0x77050000	0x000C5000
C:\WINDOWS\System32\rastls.dll	0x76B70000	0x00027000
C:\WINDOWS\system32\CRYPTUI.dll	0x754D0000	0x00080000
C:\WINDOWS\system32\WININET.dll	0x771B0000	0x000AA000
C:\WINDOWS\system32\WINTRUST.dll	0x76C30000	0x0002E000
C:\WINDOWS\system32\IMAGEHLP.dll	0x76C90000	0x00028000
C:\WINDOWS\System32\MPRAPI.dll	0x76D40000	0x00018000
C:\WINDOWS\System32\ACTIVEDS.dll	0x77CC0000	0x00032000
C:\WINDOWS\System32\adsldpc.dll	0x76E10000	0x00025000
C:\WINDOWS\System32\SETUPAPI.dll	0x77920000	0x000F3000
C:\WINDOWS\System32\RASAPI32.dll	0x76EE0000	0x0003C000
C:\WINDOWS\System32\rasman.dll	0x76E90000	0x00012000
C:\WINDOWS\System32\TAPI32.dll	0x76EB0000	0x0002F000
C:\WINDOWS\System32\SCHANNEL.dll	0x767F0000	0x00027000
C:\WINDOWS\System32\WinSCard.dll	0x723D0000	0x0001C000
C:\WINDOWS\System32\PSAPI.DLL	0x76BF0000	0x0000B000
C:\WINDOWS\System32\raschap.dll	0x76BD0000	0x00016000
C:\WINDOWS\system32\msv1_0.dll	0x77C70000	0x00024000
c:\windows\system32\schedsvc.dll	0x77300000	0x00033000
c:\windows\system32\NTDSAPI.dll	0x767A0000	0x00013000
C:\WINDOWS\System32\MSIDLE.DLL	0x74F50000	0x00005000
c:\windows\system32\audiosrv.dll	0x708B0000	0x0000D000
c:\windows\system32\wkssvc.dll	0x76E40000	0x00023000
c:\windows\system32\qmgr.dll	0x5B9F0000	0x0006B000
C:\WINDOWS\system32\MPR.dll	0x71B20000	0x00012000
c:\windows\system32\SHFOLDER.dll	0x76780000	0x00009000
c:\windows\system32\WINHTTP.dll	0x4D4F0000	0x00059000
C:\WINDOWS\system32\mswsock.dll	0x71A50000	0x0003F000
C:\WINDOWS\System32\hnetcfg.dll	0x662B0000	0x00058000
C:\WINDOWS\System32\wshtcpip.dll	0x71A90000	0x00008000
c:\windows\system32\cryptsvc.dll	0x76CE0000	0x00012000
c:\windows\system32\certcli.dll	0x77B90000	0x00032000
c:\windows\system32\dmserver.dll	0x74F90000	0x00009000
c:\windows\system32\ersvc.dll	0x74F80000	0x00009000
c:\windows\system32\es.dll	0x77710000	0x00042000
c:\windows\pchealth\helpctr\binaries\pchsvc.dll	0x74F40000	0x0000C000
c:\windows\system32\srvsvc.dll	0x75090000	0x0001A000
c:\windows\system32\netman.dll	0x77D00000	0x00033000
c:\windows\system32\netshell.dll	0x76400000	0x001A5000
c:\windows\system32\credui.dll	0x76C00000	0x0002E000
c:\windows\system32\dot3dlg.dll	0x736D0000	0x00006000
c:\windows\system32\OneX.DLL	0x5DCA0000	0x00028000
c:\windows\system32\eappcfg.dll	0x745B0000	0x00022000
c:\windows\system32\eappprxy.dll	0x5DCD0000	0x0000E000
c:\windows\system32\WZCSAPI.DLL	0x73030000	0x00010000
c:\windows\system32\srsvc.dll	0x751A0000	0x0002E000
c:\windows\system32\POWRPROF.dll	0x74AD0000	0x00008000
c:\windows\system32\sens.dll	0x722D0000	0x0000D000
c:\windows\system32\seclogon.dll	0x73D20000	0x00008000
c:\windows\system32\trkwks.dll	0x75070000	0x00019000

Load-time Dlls

Module Name	Base Address	Size
c:\windows\system32\w32time.dll	0x767C0000	0x0002C000
c:\windows\system32\wbem\wmisvc.dll	0x59490000	0x00028000
C:\WINDOWS\system32\VSSAPI.DLL	0x753E0000	0x0006D000
c:\windows\system32\wuauserv.dll	0x50000000	0x00005000
C:\WINDOWS\system32\wuaueng.dll	0x50040000	0x001D9000
C:\WINDOWS\System32\WINSPOOL.DRV	0x73000000	0x00026000
C:\WINDOWS\System32\Cabinet.dll	0x75150000	0x00013000
C:\WINDOWS\System32\mspatcha.dll	0x600A0000	0x0000B000
c:\windows\system32\wscsvc.dll	0x4C0A0000	0x00017000
c:\windows\system32\msi.dll	0x7D1E0000	0x002BC000
C:\WINDOWS\system32\wbem\wbemcomn.dll	0x75290000	0x00037000
C:\WINDOWS\System32\winrnr.dll	0x76FB0000	0x00008000
C:\WINDOWS\System32\rasadhlp.dll	0x76FC0000	0x00006000
C:\WINDOWS\System32\sfc.dll	0x76BB0000	0x00005000
C:\WINDOWS\System32\sfc_os.dll	0x76C60000	0x0002A000
c:\windows\system32\browser.dll	0x76DA0000	0x00016000
C:\WINDOWS\system32\Apphelp.dll	0x77B40000	0x00022000
C:\WINDOWS\System32\SXS.DLL	0x7E720000	0x000B0000
C:\WINDOWS\system32\comsvcs.dll	0x76620000	0x0013C000
C:\WINDOWS\system32\colbact.DLL	0x75130000	0x00014000
C:\WINDOWS\system32\MTXCLU.DLL	0x750F0000	0x00013000
C:\WINDOWS\system32\WSOCK32.dll	0x71AD0000	0x00009000
C:\WINDOWS\System32\CLUSAPI.DLL	0x76D10000	0x00012000
C:\WINDOWS\System32\RESUTILS.DLL	0x750B0000	0x00012000
c:\windows\system32\ipnathlp.dll	0x66460000	0x00055000
c:\windows\system32\AUTHZ.dll	0x776C0000	0x00012000
C:\WINDOWS\system32\upnp.dll	0x76DE0000	0x00024000
C:\WINDOWS\system32\SSDPAPI.dll	0x74F00000	0x0000C000
C:\WINDOWS\System32\Wbem\wbemcore.dll	0x762C0000	0x00085000
C:\WINDOWS\System32\Wbem\esscli.dll	0x75310000	0x0003F000
C:\WINDOWS\System32\Wbem\FastProx.dll	0x75690000	0x00076000
C:\WINDOWS\system32\wbem\wbemsvc.dll	0x74ED0000	0x0000E000
C:\WINDOWS\system32\wbem\wmiutils.dll	0x75020000	0x0001B000
C:\WINDOWS\system32\wbem\repdrvfs.dll	0x75200000	0x0002F000
C:\WINDOWS\system32\wbem\wmiprvsd.dll	0x597F0000	0x0006D000
C:\WINDOWS\system32\NCObjAPI.DLL	0x5F770000	0x0000C000
C:\WINDOWS\system32\wbem\wbemess.dll	0x75390000	0x00046000
C:\WINDOWS\system32\wups2.dll	0x50F00000	0x0000D000
C:\WINDOWS\system32\wbem\ncprov.dll	0x5F740000	0x0000E000
C:\WINDOWS\System32\RASDLG.dll	0x768D0000	0x000A4000
C:\WINDOWS\System32\dssenh.dll	0x68100000	0x00026000
C:\WINDOWS\system32\wuapi.dll	0x506A0000	0x0008E000

9.a) svchost.exe - Registry Activities

Registry Values Modified:

Key	Name	New Value
HKLM\SOFTWARE\MICROSOFT\WINDOWS NT\CURRENTVERSION\PREFETCHER	LastTraceFailure	4
HKLM\SOFTWARE\MICROSOFT\WINDOWS NT\CURRENTVERSION\PREFETCHER	TracesProcessed	11
HKLM\SOFTWARE\MICROSOFT\WINDOWS NT\CURRENTVERSION\PREFETCHER	TracesSuccessful	6

Registry Values Read:

Key	Name	Value	Times
HKLM\System\CurrentControlSet\Control\ComputerName\ActiveComputerName	ComputerName	PC	1

9.b) svchost.exe - File Activities

Files Read:

C:\cleansweep.exe\config.bin

Files Modified:

\Device\Afd\Endpoint
\Device\RasAcd

Device Control Communication:

File	Control Code	Times
\Device\Afd\Endpoint	AFD_SET_CONTEXT (0x00012047)	2
\Device\RasAcd	0x00F14014	1
\Device\Afd\Endpoint	AFD_BIND (0x00012003)	1
\Device\Afd\Endpoint	AFD_GET_TDI_HAND (0x00012037)	1
\Device\Afd\Endpoint	AFD_CONNECT (0x00012007)	1

Memory Mapped Files:

File Name
\systemroot\system32\kernel32.dll
\systemroot\system32\ntdll.dll
\systemroot\system32\ws2_32.dll

9.c) svchost.exe - Network Activity

DNS Queries:

Name	Query Type	Query Result	Successful	Protocol
213.155.29.144	DNS_TYPE_A	213.155.29.144	YES	

10. svchost.exe

General information about this executable

Analysis Reason:	file.exe wrote to the virtual memory of this process
Filename:	svchost.exe
Command Line:	C:\WINDOWS\system32\svchost.exe -k NetworkService
Process-status at analysis end:	alive
Exit Code:	0

Load-time Dlls

Module Name	Base Address	Size
C:\WINDOWS\system32\ntdll.dll	0x7C900000	0x000AF000
C:\WINDOWS\system32\kernel32.dll	0x7C800000	0x000F6000
C:\WINDOWS\system32\ADVAPI32.dll	0x77DD0000	0x0009B000
C:\WINDOWS\system32\RPCRT4.dll	0x77E70000	0x00092000
C:\WINDOWS\system32\Secur32.dll	0x77FE0000	0x00011000
C:\WINDOWS\system32\ShimEng.dll	0x5CB70000	0x00026000
C:\WINDOWS\AppPatch\AcGenral.DLL	0x6F880000	0x001CA000

Load-time Dlls

Module Name	Base Address	Size
C:\WINDOWS\system32\USER32.dll	0x7E410000	0x00091000
C:\WINDOWS\system32\GDI32.dll	0x77F10000	0x00049000
C:\WINDOWS\system32\WINMM.dll	0x76B40000	0x0002D000
C:\WINDOWS\system32\ole32.dll	0x774E0000	0x0013D000
C:\WINDOWS\system32\msvcrt.dll	0x77C10000	0x00058000
C:\WINDOWS\system32\OLEAUT32.dll	0x77120000	0x0008B000
C:\WINDOWS\system32\MSACM32.dll	0x77BE0000	0x00015000
C:\WINDOWS\system32\VERSION.dll	0x77C00000	0x00008000
C:\WINDOWS\system32\SHELL32.dll	0x7C9C0000	0x00817000
C:\WINDOWS\system32\SHLWAPI.dll	0x77F60000	0x00076000
C:\WINDOWS\system32\USERENV.dll	0x769C0000	0x000B4000
C:\WINDOWS\system32\UxTheme.dll	0x5AD70000	0x00038000
C:\WINDOWS\WinSxS\x86_Microsoft.Windows.Common-Controls_6595b64144ccf1df_6.0.2600.5512_x-ww_35d4ce83\comctl32.dll	0x773D0000	0x00103000
C:\WINDOWS\system32\comctl32.dll	0x5D090000	0x0009A000
c:\windows\system32\dnsrslvr.dll	0x76770000	0x0000D000
c:\windows\system32\DNSAPI.dll	0x76F20000	0x00027000
c:\windows\system32\WS2_32.dll	0x71AB0000	0x00017000
c:\windows\system32\WS2HELP.dll	0x71AA0000	0x00008000
c:\windows\system32\iphlpapi.dll	0x76D60000	0x00019000
C:\WINDOWS\system32\rsaenh.dll	0x68000000	0x00036000
C:\WINDOWS\system32\mswsock.dll	0x71A50000	0x0003F000
C:\WINDOWS\system32\hnetcfg.dll	0x662B0000	0x00058000
C:\WINDOWS\System32\wshtcpip.dll	0x71A90000	0x00008000

10.a) svchost.exe - File Activities

Memory Mapped Files:

File Name
\systemroot\system32\ntdll.dll

11. svchost.exe

General information about this executable

Analysis Reason:	file.exe wrote to the virtual memory of this process
Filename:	svchost.exe
Command Line:	C:\WINDOWS\system32\svchost.exe -k LocalService
Process-status at analysis end:	alive
Exit Code:	0

Load-time Dlls

Module Name	Base Address	Size
C:\WINDOWS\system32\ntdll.dll	0x7C900000	0x000AF000
C:\WINDOWS\system32\kernel32.dll	0x7C800000	0x000F6000
C:\WINDOWS\system32\ADVAPI32.dll	0x77DD0000	0x0009B000
C:\WINDOWS\system32\RPCRT4.dll	0x77E70000	0x00092000
C:\WINDOWS\system32\Secur32.dll	0x77FE0000	0x00011000
C:\WINDOWS\system32\ShimEng.dll	0x5CB70000	0x00026000
C:\WINDOWS\AppPatch\AcGenral.DLL	0x6F880000	0x001CA000
C:\WINDOWS\system32\USER32.dll	0x7E410000	0x00091000
C:\WINDOWS\system32\GDI32.dll	0x77F10000	0x00049000
C:\WINDOWS\system32\WINMM.dll	0x76B40000	0x0002D000
C:\WINDOWS\system32\ole32.dll	0x774E0000	0x0013D000
C:\WINDOWS\system32\msvcrt.dll	0x77C10000	0x00058000
C:\WINDOWS\system32\OLEAUT32.dll	0x77120000	0x0008B000

Load-time Dlls		
Module Name	**Base Address**	**Size**
C:\WINDOWS\system32\MSACM32.dll	0x77BE0000	0x00015000
C:\WINDOWS\system32\VERSION.dll	0x77C00000	0x00008000
C:\WINDOWS\system32\SHELL32.dll	0x7C9C0000	0x00817000
C:\WINDOWS\system32\SHLWAPI.dll	0x77F60000	0x00076000
C:\WINDOWS\system32\USERENV.dll	0x769C0000	0x000B4000
C:\WINDOWS\system32\UxTheme.dll	0x5AD70000	0x00038000
C:\WINDOWS\WinSxS\x86_Microsoft.Windows.Common-Controls_6595b64144ccf1df_6.0.2600.5512_x-ww_35d4ce83\comctl32.dll	0x773D0000	0x00103000
C:\WINDOWS\system32\comctl32.dll	0x5D090000	0x0009A000
C:\WINDOWS\system32\NTMARTA.DLL	0x77690000	0x00021000
C:\WINDOWS\system32\SAMLIB.dll	0x71BF0000	0x00013000
C:\WINDOWS\system32\WLDAP32.dll	0x76F60000	0x0002C000
C:\WINDOWS\system32\xpsp2res.dll	0x005B0000	0x002C5000
c:\windows\system32\lmhsvc.dll	0x74C40000	0x00006000
c:\windows\system32\iphlpapi.dll	0x76D60000	0x00019000
c:\windows\system32\WS2_32.dll	0x71AB0000	0x00017000
c:\windows\system32\WS2HELP.dll	0x71AA0000	0x00008000
c:\windows\system32\webclnt.dll	0x5A6E0000	0x00015000
C:\WINDOWS\system32\WININET.dll	0x771B0000	0x000AA000
C:\WINDOWS\system32\CRYPT32.dll	0x77A80000	0x00095000
C:\WINDOWS\system32\MSASN1.dll	0x77B20000	0x00012000
C:\WINDOWS\system32\wsock32.dll	0x71AD0000	0x00009000
c:\windows\system32\regsvc.dll	0x76AF0000	0x00012000
c:\windows\system32\ssdpsrv.dll	0x765E0000	0x00014000
C:\WINDOWS\system32\hnetcfg.dll	0x662B0000	0x00058000
C:\WINDOWS\system32\CLBCATQ.DLL	0x76FD0000	0x0007F000
C:\WINDOWS\system32\COMRes.dll	0x77050000	0x000C5000
C:\WINDOWS\system32\mswsock.dll	0x71A50000	0x0003F000
C:\WINDOWS\System32\wshtcpip.dll	0x71A90000	0x00008000

11.a) svchost.exe - File Activities

Memory Mapped Files:
File Name
\systemroot\system32\ntdll.dll

12. spoolsv.exe

General information about this executable	
Analysis Reason:	file.exe wrote to the virtual memory of this process
Filename:	spoolsv.exe
Process-status at analysis end:	alive
Exit Code:	0

Load-time Dlls		
Module Name	**Base Address**	**Size**
C:\WINDOWS\system32\ntdll.dll	0x7C900000	0x000AF000

13. mscorsvw.exe

General information about this executable	
Analysis Reason:	file.exe wrote to the virtual memory of this process
Filename:	mscorsvw.exe
MD5:	c5a75eb48e2344abdc162bda79e16841
SHA-1:	ed4851c89bc80c7a38960bc14686513ac1b3fb47

General information about this executable	
File Size:	130384
Command Line:	C:\WINDOWS\Microsoft.NET\Framework\v4.0.30319\mscorsvw.exe
Process-status at analysis end:	alive
Exit Code:	0

Load-time Dlls

Module Name	Base Address	Size
C:\WINDOWS\system32\ntdll.dll	0x7C900000	0x000AF000
C:\WINDOWS\system32\kernel32.dll	0x7C800000	0x000F6000
C:\WINDOWS\system32\MSVCR100_CLR0400.dll	0x79060000	0x000BE000
C:\WINDOWS\system32\ADVAPI32.dll	0x77DD0000	0x0009B000
C:\WINDOWS\system32\RPCRT4.dll	0x77E70000	0x00092000
C:\WINDOWS\system32\Secur32.dll	0x77FE0000	0x00011000
C:\WINDOWS\system32\USER32.dll	0x7E410000	0x00091000
C:\WINDOWS\system32\GDI32.dll	0x77F10000	0x00049000
C:\WINDOWS\system32\mscoree.dll	0x79000000	0x0004A000
C:\WINDOWS\system32\ole32.dll	0x774E0000	0x0013D000
C:\WINDOWS\system32\msvcrt.dll	0x77C10000	0x00058000
C:\WINDOWS\system32\OLEAUT32.dll	0x77120000	0x0008B000
C:\WINDOWS\Microsoft.NET\Framework\v4.0.30319\mscorsvc.dll	0x608D0000	0x00054000
C:\WINDOWS\Microsoft.NET\Framework\v4.0.30319\fusion.dll	0x604A0000	0x0000C000
C:\WINDOWS\Microsoft.NET\Framework\v4.0.30319\mscoreei.dll	0x603B0000	0x00066000
C:\WINDOWS\system32\SHLWAPI.dll	0x77F60000	0x00076000
C:\WINDOWS\system32\msidle.dll	0x74F50000	0x00005000
C:\WINDOWS\system32\Wtsapi32.dll	0x76F50000	0x00008000
C:\WINDOWS\system32\WINSTA.dll	0x76360000	0x00010000
C:\WINDOWS\system32\NETAPI32.dll	0x5B860000	0x00055000
C:\WINDOWS\system32\powrprof.dll	0x74AD0000	0x00008000

13.a) mscorsvw.exe - File Activities

Files Read:

PIPE\lsarpc

Files Modified:

PIPE\lsarpc

File System Control Communication:

File	Control Code	Times
PIPE\lsarpc	0x0011C017	6

14. wuauclt.exe

General information about this executable	
Analysis Reason:	file.exe wrote to the virtual memory of this process
Filename:	wuauclt.exe
MD5:	62bb79160f86cd962f312c68c6239bfd
SHA-1:	c2de8148e1a8e8f097e3a40232ddb04efd0a7cc6
File Size:	53472
Command Line:	"C:\WINDOWS\system32\wuauclt.exe" /RunStoreAsComServer Local \[2a8]SUSDSf0c7666bfc54a04ca39ec51a6dc8d2fd
Process-status at analysis end:	alive
Exit Code:	0

Load-time Dlls

Module Name	Base Address	Size
C:\WINDOWS\system32\ntdll.dll	0x7C900000	0x000AF000
C:\WINDOWS\system32\kernel32.dll	0x7C800000	0x000F6000
C:\WINDOWS\system32\msvcrt.dll	0x77C10000	0x00058000
C:\WINDOWS\system32\ole32.dll	0x774E0000	0x0013D000
C:\WINDOWS\system32\ADVAPI32.dll	0x77DD0000	0x0009B000
C:\WINDOWS\system32\RPCRT4.dll	0x77E70000	0x00092000
C:\WINDOWS\system32\Secur32.dll	0x77FE0000	0x00011000
C:\WINDOWS\system32\GDI32.dll	0x77F10000	0x00049000
C:\WINDOWS\system32\USER32.dll	0x7E410000	0x00091000
C:\WINDOWS\system32\OLEAUT32.dll	0x77120000	0x0008B000
C:\WINDOWS\system32\SHLWAPI.dll	0x77F60000	0x00076000
C:\WINDOWS\system32\ShimEng.dll	0x5CB70000	0x00026000
C:\WINDOWS\AppPatch\AcGenral.DLL	0x6F880000	0x001CA000
C:\WINDOWS\system32\WINMM.dll	0x76B40000	0x0002D000
C:\WINDOWS\system32\MSACM32.dll	0x77BE0000	0x00015000
C:\WINDOWS\system32\VERSION.dll	0x77C00000	0x00008000
C:\WINDOWS\system32\SHELL32.dll	0x7C9C0000	0x00817000
C:\WINDOWS\system32\USERENV.dll	0x769C0000	0x000B4000
C:\WINDOWS\system32\UxTheme.dll	0x5AD70000	0x00038000
C:\WINDOWS\WinSxS\x86_Microsoft.Windows.Common-Controls_6595b64144ccf1df_6.0.2600.5512_x-ww_35d4ce83\comctl32.dll	0x773D0000	0x00103000
C:\WINDOWS\system32\wuaueng.dll	0x50040000	0x001D9000
C:\WINDOWS\system32\WS2_32.dll	0x71AB0000	0x00017000
C:\WINDOWS\system32\WS2HELP.dll	0x71AA0000	0x00008000
C:\WINDOWS\system32\ESENT.dll	0x606B0000	0x0010D000
C:\WINDOWS\system32\WTSAPI32.dll	0x76F50000	0x00008000
C:\WINDOWS\system32\WINSTA.dll	0x76360000	0x00010000
C:\WINDOWS\system32\NETAPI32.dll	0x5B860000	0x00055000
C:\WINDOWS\system32\WINSPOOL.DRV	0x73000000	0x00026000
C:\WINDOWS\system32\IPHLPAPI.DLL	0x76D60000	0x00019000
C:\WINDOWS\system32\WINHTTP.dll	0x4D4F0000	0x00059000
C:\WINDOWS\system32\WINTRUST.dll	0x76C30000	0x0002E000
C:\WINDOWS\system32\CRYPT32.dll	0x77A80000	0x00095000
C:\WINDOWS\system32\MSASN1.dll	0x77B20000	0x00012000
C:\WINDOWS\system32\IMAGEHLP.dll	0x76C90000	0x00028000
C:\WINDOWS\system32\Cabinet.dll	0x75150000	0x00013000
C:\WINDOWS\system32\mspatcha.dll	0x600A0000	0x0000B000
C:\WINDOWS\system32\xpsp2res.dll	0x00B30000	0x002C5000
C:\WINDOWS\system32\CLBCATQ.DLL	0x76FD0000	0x0007F000
C:\WINDOWS\system32\COMRes.dll	0x77050000	0x000C5000
C:\WINDOWS\system32\wups2.dll	0x50F00000	0x0000D000

15. ctfmon.exe

General information about this executable

Analysis Reason:	file.exe wrote to the virtual memory of this process
Filename:	ctfmon.exe
MD5:	5f1d5f88303d4a4dbc8e5f97ba967cc3
SHA-1:	99cb7370f16773c8e2d0c86fe805ec638ab126e9
File Size:	15360
Command Line:	"C:\WINDOWS\system32\ctfmon.exe"
Process-status at analysis end:	alive
Exit Code:	0

Load-time Dlls		
Module Name	**Base Address**	**Size**
C:\WINDOWS\system32\ntdll.dll	0x7C900000	0x000AF000
C:\WINDOWS\system32\kernel32.dll	0x7C800000	0x000F6000
C:\WINDOWS\system32\msvcrt.dll	0x77C10000	0x00058000
C:\WINDOWS\system32\ADVAPI32.dll	0x77DD0000	0x0009B000
C:\WINDOWS\system32\RPCRT4.dll	0x77E70000	0x00092000
C:\WINDOWS\system32\Secur32.dll	0x77FE0000	0x00011000
C:\WINDOWS\system32\USER32.dll	0x7E410000	0x00091000
C:\WINDOWS\system32\GDI32.dll	0x77F10000	0x00049000
C:\WINDOWS\system32\MSCTF.dll	0x74720000	0x0004C000
C:\WINDOWS\system32\MSUTB.dll	0x5FC10000	0x00033000
C:\WINDOWS\system32\ShimEng.dll	0x5CB70000	0x00026000
C:\WINDOWS\AppPatch\AcGenral.DLL	0x6F880000	0x001CA000
C:\WINDOWS\system32\WINMM.dll	0x76B40000	0x0002D000
C:\WINDOWS\system32\ole32.dll	0x774E0000	0x0013D000
C:\WINDOWS\system32\OLEAUT32.dll	0x77120000	0x0008B000
C:\WINDOWS\system32\MSACM32.dll	0x77BE0000	0x00015000
C:\WINDOWS\system32\VERSION.dll	0x77C00000	0x00008000
C:\WINDOWS\system32\SHELL32.dll	0x7C9C0000	0x00817000
C:\WINDOWS\system32\SHLWAPI.dll	0x77F60000	0x00076000
C:\WINDOWS\system32\USERENV.dll	0x769C0000	0x000B4000
C:\WINDOWS\system32\UxTheme.dll	0x5AD70000	0x00038000
C:\WINDOWS\WinSxS\x86_Microsoft.Windows.Common-Controls_6595b64144ccf1df_6.0.2600.5512_x-ww_35d4ce83\comctl32.dll	0x773D0000	0x00103000

15.a) ctfmon.exe - Registry Activities

Monitored Registry Keys:			
Key Name	**Watch subtree**	**Notify Filter**	**Count**
HKU\S-1-5-21-842925246-1425521274-308236825-Software\Microsoft\Windows\CurrentVersion\Run	1	Key Change,Value Change	1

16. msmsgs.exe

General information about this executable	
Analysis Reason:	file.exe wrote to the virtual memory of this process
Filename:	msmsgs.exe
MD5:	3e930c641079443d4de036167a69caa2
SHA-1:	ac40479e28fb680aff76e41fa14ebe18b3392629
File Size:	1695232
Command Line:	"C:\Program Files\Messenger\msmsgs.exe" /background
Process-status at analysis end:	alive
Exit Code:	0

Load-time Dlls		
Module Name	**Base Address**	**Size**
C:\WINDOWS\system32\ntdll.dll	0x7C900000	0x000AF000
C:\WINDOWS\system32\kernel32.dll	0x7C800000	0x000F6000
C:\WINDOWS\system32\msvcrt.dll	0x77C10000	0x00058000
C:\WINDOWS\system32\ADVAPI32.dll	0x77DD0000	0x0009B000
C:\WINDOWS\system32\RPCRT4.dll	0x77E70000	0x00092000
C:\WINDOWS\system32\Secur32.dll	0x77FE0000	0x00011000
C:\WINDOWS\system32\GDI32.dll	0x77F10000	0x00049000
C:\WINDOWS\system32\USER32.dll	0x7E410000	0x00091000
C:\WINDOWS\system32\WSOCK32.dll	0x71AD0000	0x00009000

Load-time Dlls

Module Name	Base Address	Size
C:\WINDOWS\system32\WS2_32.dll	0x71AB0000	0x00017000
C:\WINDOWS\system32\WS2HELP.dll	0x71AA0000	0x00008000
C:\WINDOWS\system32\ole32.dll	0x774E0000	0x0013D000
C:\WINDOWS\system32\OLEAUT32.dll	0x77120000	0x0008B000
C:\WINDOWS\WinSxS\X86_Microsoft.Windows.Common-Controls_6595b64144ccf1df_6.0.2600.5512_x-ww_35d4ce83\COMCTL32.dll	0x773D0000	0x00103000
C:\WINDOWS\system32\SHLWAPI.dll	0x77F60000	0x00076000
C:\WINDOWS\system32\comdlg32.dll	0x763B0000	0x00049000
C:\WINDOWS\system32\SHELL32.dll	0x7C9C0000	0x00817000
C:\WINDOWS\system32\VERSION.dll	0x77C00000	0x00008000
C:\WINDOWS\system32\WINMM.dll	0x76B40000	0x0002D000
C:\WINDOWS\WinSxS\x86_Microsoft.Windows.GdiPlus_6595b64144ccf1df_1.0.2600.5512_x-ww_dfb54e0c\gdiplus.dll	0x4EC50000	0x001A6000
C:\WINDOWS\system32\MSIMG32.dll	0x76380000	0x00005000
C:\WINDOWS\system32\NETAPI32.dll	0x5B860000	0x00055000
C:\WINDOWS\system32\WININET.dll	0x771B0000	0x000AA000
C:\WINDOWS\system32\CRYPT32.dll	0x77A80000	0x00095000
C:\WINDOWS\system32\MSASN1.dll	0x77B20000	0x00012000
C:\WINDOWS\system32\cryptdll.dll	0x76790000	0x0000C000
C:\WINDOWS\system32\iphlpapi.dll	0x76D60000	0x00019000
C:\WINDOWS\system32\XPOB2RES.DLL	0x10000000	0x0006C000
C:\WINDOWS\system32\CLBCATQ.DLL	0x76FD0000	0x0007F000
C:\WINDOWS\system32\COMRes.dll	0x77050000	0x000C5000
C:\WINDOWS\system32\xpsp2res.dll	0x00890000	0x002C5000
C:\WINDOWS\system32\MSCTF.dll	0x74720000	0x0004C000
C:\WINDOWS\system32\SXS.DLL	0x7E720000	0x000B0000
C:\WINDOWS\system32\es.dll	0x77710000	0x00042000
C:\WINDOWS\system32\wtsapi32.dll	0x76F50000	0x00008000
C:\WINDOWS\system32\WINSTA.dll	0x76360000	0x00010000
C:\WINDOWS\system32\credui.dll	0x76C00000	0x0002E000

17. reader_sl.exe

General information about this executable

Analysis Reason:	file.exe wrote to the virtual memory of this process
Filename:	reader_sl.exe
MD5:	54c88bfbd055621e2306534f445c0c8d
SHA-1:	960a171e826c077187fe634103874644327a6110
File Size:	40048
Command Line:	"C:\Program Files\Adobe\Reader 8.0\Reader\reader_sl.exe"
Process-status at analysis end:	alive
Exit Code:	0

Load-time Dlls

Module Name	Base Address	Size
C:\WINDOWS\system32\ntdll.dll	0x7C900000	0x000AF000
C:\WINDOWS\system32\kernel32.dll	0x7C800000	0x000F6000
C:\WINDOWS\system32\USER32.dll	0x7E410000	0x00091000
C:\WINDOWS\system32\GDI32.dll	0x77F10000	0x00049000
C:\WINDOWS\system32\ADVAPI32.dll	0x77DD0000	0x0009B000
C:\WINDOWS\system32\RPCRT4.dll	0x77E70000	0x00092000
C:\WINDOWS\system32\Secur32.dll	0x77FE0000	0x00011000
C:\WINDOWS\system32\SHELL32.dll	0x7C9C0000	0x00817000
C:\WINDOWS\system32\msvcrt.dll	0x77C10000	0x00058000
C:\WINDOWS\system32\SHLWAPI.dll	0x77F60000	0x00076000

Load-time Dlls

Module Name	Base Address	Size
C:\WINDOWS\WinSxS\x86_Microsoft.VC80.CRT_1fc8b3b9a1e18e3b_8.0.50727.1433_x-ww_5cf844d2\MSVCP80.dll	0x7C420000	0x00087000
C:\WINDOWS\WinSxS\x86_Microsoft.VC80.CRT_1fc8b3b9a1e18e3b_8.0.50727.1433_x-ww_5cf844d2\MSVCR80.dll	0x78130000	0x0009B000
C:\WINDOWS\WinSxS\x86_Microsoft.Windows.Common-Controls_6595b64144ccf1df_6.0.2600.5512_x-ww_35d4ce83\comctl32.dll	0x773D0000	0x00103000
C:\WINDOWS\system32\comctl32.dll	0x5D090000	0x0009A000
C:\WINDOWS\system32\MSCTF.dll	0x74720000	0x0004C000

18. alg.exe

General information about this executable

Analysis Reason:	file.exe wrote to the virtual memory of this process
Filename:	alg.exe
MD5:	8c515081584a38aa007909cd02020b3d
SHA-1:	ef5728c819f466bfe56c36bc9db3fac004ef3d50
File Size:	44544
Command Line:	C:\WINDOWS\System32\alg.exe
Process-status at analysis end:	alive
Exit Code:	0

Load-time Dlls

Module Name	Base Address	Size
C:\WINDOWS\system32\ntdll.dll	0x7C900000	0x000AF000
C:\WINDOWS\system32\kernel32.dll	0x7C800000	0x000F6000
C:\WINDOWS\system32\msvcrt.dll	0x77C10000	0x00058000
C:\WINDOWS\System32\ATL.DLL	0x76B20000	0x00011000
C:\WINDOWS\system32\USER32.dll	0x7E410000	0x00091000
C:\WINDOWS\system32\GDI32.dll	0x77F10000	0x00049000
C:\WINDOWS\system32\ADVAPI32.dll	0x77DD0000	0x0009B000
C:\WINDOWS\system32\RPCRT4.dll	0x77E70000	0x00092000
C:\WINDOWS\system32\Secur32.dll	0x77FE0000	0x00011000
C:\WINDOWS\system32\ole32.dll	0x774E0000	0x0013D000
C:\WINDOWS\system32\OLEAUT32.dll	0x77120000	0x0008B000
C:\WINDOWS\System32\WSOCK32.dll	0x71AD0000	0x00009000
C:\WINDOWS\System32\WS2_32.dll	0x71AB0000	0x00017000
C:\WINDOWS\System32\WS2HELP.dll	0x71AA0000	0x00008000
C:\WINDOWS\System32\MSWSOCK.DLL	0x71A50000	0x0003F000
C:\WINDOWS\System32\ShimEng.dll	0x5CB70000	0x00026000
C:\WINDOWS\AppPatch\AcGenral.DLL	0x6F880000	0x001CA000
C:\WINDOWS\System32\WINMM.dll	0x76B40000	0x0002D000
C:\WINDOWS\System32\MSACM32.dll	0x77BE0000	0x00015000
C:\WINDOWS\system32\VERSION.dll	0x77C00000	0x00008000
C:\WINDOWS\system32\SHELL32.dll	0x7C9C0000	0x00817000
C:\WINDOWS\system32\SHLWAPI.dll	0x77F60000	0x00076000
C:\WINDOWS\system32\USERENV.dll	0x769C0000	0x000B4000
C:\WINDOWS\System32\UxTheme.dll	0x5AD70000	0x00038000
C:\WINDOWS\WinSxS\x86_Microsoft.Windows.Common-Controls_6595b64144ccf1df_6.0.2600.5512_x-ww_35d4ce83\comctl32.dll	0x773D0000	0x00103000
C:\WINDOWS\system32\comctl32.dll	0x5D090000	0x0009A000
C:\WINDOWS\System32\CLBCATQ.DLL	0x76FD0000	0x0007F000
C:\WINDOWS\System32\COMRes.dll	0x77050000	0x000C5000
C:\WINDOWS\System32\xpsp2res.dll	0x00600000	0x002C5000
C:\WINDOWS\system32\hnetcfg.dll	0x662B0000	0x00058000
C:\WINDOWS\System32\wshtcpip.dll	0x71A90000	0x00008000

19. wscntfy.exe

General information about this executable	
Analysis Reason:	file.exe wrote to the virtual memory of this process
Filename:	wscntfy.exe
Process-status at analysis end:	alive
Exit Code:	0

Load-time Dlls

Module Name	Base Address	Size
C:\WINDOWS\system32\ntdll.dll	0x7C900000	0x000AF000

20. drlwszvxbeo.exe

General information about this executable	
Analysis Reason:	file.exe wrote to the virtual memory of this process
Filename:	drlwszvxbeo.exe
MD5:	ec95a4d3adc866c53bfafc3ba177d905
SHA-1:	78d7358cebb7681ba22b1ec453eb98308eadd619
File Size:	1256684
Command Line:	"C:\Program Files\Common Files\drlwszvxbeo.exe"
Process-status at analysis end:	alive
Exit Code:	0

Load-time Dlls

Module Name	Base Address	Size
C:\WINDOWS\system32\ntdll.dll	0x7C900000	0x000AF000
C:\WINDOWS\system32\kernel32.dll	0x7C800000	0x000F6000
C:\WINDOWS\system32\ADVAPI32.DLL	0x77DD0000	0x0009B000
C:\WINDOWS\system32\RPCRT4.dll	0x77E70000	0x00092000
C:\WINDOWS\system32\Secur32.dll	0x77FE0000	0x00011000
C:\WINDOWS\system32\msvcrt.dll	0x77C10000	0x00058000
C:\WINDOWS\system32\PSAPI.DLL	0x76BF0000	0x0000B000

Program output

Stdout:	. . . . .

21. kxuckd.exe

General information about this executable	
Analysis Reason:	file.exe wrote to the virtual memory of this process
Filename:	kxuckd.exe
MD5:	ed22e108cca63fab4ad592f04b117289
SHA-1:	a11b96e200594f19b8e67af04797b61267710fec
File Size:	327901
Command Line:	"C:\Program Files\Common Files\kxuckd.exe"
Process-status at analysis end:	alive
Exit Code:	0

Load-time Dlls

Module Name	Base Address	Size
C:\WINDOWS\system32\ntdll.dll	0x7C900000	0x000AF000
C:\WINDOWS\system32\kernel32.dll	0x7C800000	0x000F6000
C:\WINDOWS\system32\ADVAPI32.dll	0x77DD0000	0x0009B000
C:\WINDOWS\system32\RPCRT4.dll	0x77E70000	0x00092000

Load-time Dlls

Module Name	Base Address	Size
C:\WINDOWS\system32\Secur32.dll	0x77FE0000	0x00011000
C:\WINDOWS\WinSxS\x86_Microsoft.Windows.Common-Controls_6595b64144ccf1df_6.0.2600.5512_x-ww_35d4ce83\COMCTL32.dll	0x773D0000	0x00103000
C:\WINDOWS\system32\msvcrt.dll	0x77C10000	0x00058000
C:\WINDOWS\system32\GDI32.dll	0x77F10000	0x00049000
C:\WINDOWS\system32\USER32.dll	0x7E410000	0x00091000
C:\WINDOWS\system32\SHLWAPI.dll	0x77F60000	0x00076000
C:\WINDOWS\system32\comdlg32.dll	0x763B0000	0x00049000
C:\WINDOWS\system32\SHELL32.dll	0x7C9C0000	0x00817000
C:\WINDOWS\system32\MPR.dll	0x71B20000	0x00012000
C:\WINDOWS\system32\ole32.dll	0x774E0000	0x0013D000
C:\WINDOWS\system32\OLEAUT32.dll	0x77120000	0x0008B000
C:\WINDOWS\system32\VERSION.dll	0x77C00000	0x00008000
C:\WINDOWS\system32\WINMM.dll	0x76B40000	0x0002D000
C:\WINDOWS\system32\WSOCK32.dll	0x71AD0000	0x00009000
C:\WINDOWS\system32\WS2_32.dll	0x71AB0000	0x00017000
C:\WINDOWS\system32\WS2HELP.dll	0x71AA0000	0x00008000
C:\WINDOWS\system32\uxtheme.dll	0x5AD70000	0x00038000
C:\WINDOWS\system32\SETUPAPI.dll	0x77920000	0x000F3000
C:\WINDOWS\system32\MSCTF.dll	0x74720000	0x0004C000

SigBuster Output

UPX All_Versions SN:1634

22. cleansweep.exe

General information about this executable

Analysis Reason:	Started by file.exe
Filename:	cleansweep.exe
MD5:	0f37839f48f7fc77e6d50e14657fb96e
SHA-1:	35698c61ad232ff90c5812372d23971118ea37cd
File Size:	82432
Command Line:	"C:\cleansweep.exe\cleansweep.exe"
Process-status at analysis end:	dead
Exit Code:	0

Load-time Dlls

Module Name	Base Address	Size
C:\WINDOWS\system32\ntdll.dll	0x7C900000	0x000AF000
C:\WINDOWS\system32\kernel32.dll	0x7C800000	0x000F6000
C:\WINDOWS\system32\GDI32.dll	0x77F10000	0x00049000
C:\WINDOWS\system32\USER32.dll	0x7E410000	0x00091000

Run-time Dlls

Module Name	Base Address	Size
C:\WINDOWS\system32\comctl32.dll	0x5D090000	0x0009A000
C:\WINDOWS\system32\WS2HELP.dll	0x71AA0000	0x00008000
C:\WINDOWS\system32\WS2_32.dll	0x71AB0000	0x00017000
C:\WINDOWS\system32\OLEAUT32.dll	0x77120000	0x0008B000
C:\WINDOWS\system32\WININET.dll	0x771B0000	0x000AA000
C:\WINDOWS\WinSxS\x86_Microsoft.Windows.Common-Controls_6595b64144ccf1df_6.0.2600.5512_x-ww_35d4ce83\comctl32.dll	0x773D0000	0x00103000
C:\WINDOWS\system32\ole32.dll	0x774E0000	0x0013D000
C:\WINDOWS\system32\CRYPT32.dll	0x77A80000	0x00095000

Run-time Dlls

Module Name	Base Address	Size
C:\WINDOWS\system32\MSASN1.dll	0x77B20000	0x00012000
C:\WINDOWS\system32\msvcrt.dll	0x77C10000	0x00058000
C:\WINDOWS\system32\ADVAPI32.dll	0x77DD0000	0x0009B000
C:\WINDOWS\system32\RPCRT4.dll	0x77E70000	0x00092000
C:\WINDOWS\system32\SHLWAPI.dll	0x77F60000	0x00076000
C:\WINDOWS\system32\Secur32.dll	0x77FE0000	0x00011000
C:\WINDOWS\system32\SHELL32.dll	0x7C9C0000	0x00817000

Ikarus Virus Scanner

Trojan-Spy.Win32.SpyEyes (Sig-Id:1342409)

22.a) cleansweep.exe - Registry Activities

Registry Values Modified:

Key	Name	New Value
HKLM\Software\Microsoft\Windows\CurrentVersion\Internet Settings\Cache\Paths	Directory	C:\Documents and Settings\Administrator\Local Settings\Temporary Internet Files\Content.IE5
HKLM\Software\Microsoft\Windows\CurrentVersion\Internet Settings\Cache\Paths	Paths	4
HKLM\Software\Microsoft\Windows\CurrentVersion\Internet Settings\Cache\Paths\Path1	CacheLimit	40852
HKLM\Software\Microsoft\Windows\CurrentVersion\Internet Settings\Cache\Paths\Path1	CachePath	C:\Documents and Settings\Administrator\Local Settings\Temporary Internet Files\Content.IE5\Cache1
HKLM\Software\Microsoft\Windows\CurrentVersion\Internet Settings\Cache\Paths\Path2	CacheLimit	40852
HKLM\Software\Microsoft\Windows\CurrentVersion\Internet Settings\Cache\Paths\Path2	CachePath	C:\Documents and Settings\Administrator\Local Settings\Temporary Internet Files\Content.IE5\Cache2
HKLM\Software\Microsoft\Windows\CurrentVersion\Internet Settings\Cache\Paths\Path3	CacheLimit	40852
HKLM\Software\Microsoft\Windows\CurrentVersion\Internet Settings\Cache\Paths\Path3	CachePath	C:\Documents and Settings\Administrator\Local Settings\Temporary Internet Files\Content.IE5\Cache3
HKLM\Software\Microsoft\Windows\CurrentVersion\Internet Settings\Cache\Paths\Path4	CacheLimit	40852
HKLM\Software\Microsoft\Windows\CurrentVersion\Internet Settings\Cache\Paths\Path4	CachePath	C:\Documents and Settings\Administrator\Local Settings\Temporary Internet Files\Content.IE5\Cache4
HKU\S-1-5-21-842925246-1425521274-308236825-500\Software\Microsoft\Windows\CurrentVersion\Explorer\Shell Folders	AppData	C:\Documents and Settings\Administrator\Application Data
HKU\S-1-5-21-842925246-1425521274-308236825-500\Software\Microsoft\Windows\CurrentVersion\Explorer\Shell Folders	Cache	C:\Documents and Settings\Administrator\Local Settings\Temporary Internet Files
HKU\S-1-5-21-842925246-1425521274-308236825-500\Software\Microsoft\Windows\CurrentVersion\Explorer\Shell Folders	Cookies	C:\Documents and Settings\Administrator\Cookies
HKU\S-1-5-21-842925246-1425521274-308236825-500\Software\Microsoft\Windows\CurrentVersion\Explorer\Shell Folders	History	C:\Documents and Settings\Administrator\Local Settings\History

Registry Values Read:

Key	Name	Value	Times
HKLM\SYSTEM\CurrentControlSet\Control\Session Manager	CriticalSectionTimeout	2592000	1
HKLM\SYSTEM\Setup	SystemSetupInProgres	0	1
HKLM\Software\Policies\Microsoft\Windows\Safer\CodeIdentifiers	TransparentEnabled	1	1
HKLM\System\CurrentControlSet\Control\Terminal Server	TSUserEnabled	0	1
HKLM\System\Setup	SystemSetupInProgres	0	1

Registry Values Read:

Key	Name	Value	Times
HKU\S-1-5-21-842925246-1425521274-308236825-500\Software\Microsoft\Windows\CurrentVersion\Explorer\User Shell Folders	AppData	%USERPROFILE%\Application Data	1
HKU\S-1-5-21-842925246-1425521274-308236825-500\Software\Microsoft\Windows\CurrentVersion\Explorer\User Shell Folders	Cache	%USERPROFILE%\Local Settings\Temporary Internet Files	3
HKU\S-1-5-21-842925246-1425521274-308236825-500\Software\Microsoft\Windows\CurrentVersion\Explorer\User Shell Folders	Cookies	%USERPROFILE%\Cookies	3
HKU\S-1-5-21-842925246-1425521274-308236825-500\Software\Microsoft\Windows\CurrentVersion\Explorer\User Shell Folders	History	%USERPROFILE%\Local Settings\History	3
HKU\S-1-5-21-842925246-1425521274-308236825-500\Software\Microsoft\Windows\CurrentVersion\Internet Settings\5.0\Cache	Signature	Client UrlCache MMF Ver 5.2	2
HKU\S-1-5-21-842925246-1425521274-308236825-500\Software\Microsoft\Windows\CurrentVersion\Internet Settings\5.0\Cache\Content	CacheLimit	163410	1
HKU\S-1-5-21-842925246-1425521274-308236825-500\Software\Microsoft\Windows\CurrentVersion\Internet Settings\5.0\Cache\Content	CachePrefix		2
HKU\S-1-5-21-842925246-1425521274-308236825-500\Software\Microsoft\Windows\CurrentVersion\Internet Settings\5.0\Cache\Content	PerUserItem	1	1
HKU\S-1-5-21-842925246-1425521274-308236825-500\Software\Microsoft\Windows\CurrentVersion\Internet Settings\5.0\Cache\Cookies	CacheLimit	8192	1
HKU\S-1-5-21-842925246-1425521274-308236825-500\Software\Microsoft\Windows\CurrentVersion\Internet Settings\5.0\Cache\Cookies	CachePrefix	Cookie:	2
HKU\S-1-5-21-842925246-1425521274-308236825-500\Software\Microsoft\Windows\CurrentVersion\Internet Settings\5.0\Cache\Cookies	PerUserItem	1	1
HKU\S-1-5-21-842925246-1425521274-308236825-500\Software\Microsoft\Windows\CurrentVersion\Internet Settings\5.0\Cache\Extensible Cache\MSHist012011021720110218	CacheLimit	8192	1
HKU\S-1-5-21-842925246-1425521274-308236825-500\Software\Microsoft\Windows\CurrentVersion\Internet Settings\5.0\Cache\Extensible Cache\MSHist012011021720110218	CacheOptions	11	1
HKU\S-1-5-21-842925246-1425521274-308236825-500\Software\Microsoft\Windows\CurrentVersion\Internet Settings\5.0\Cache\Extensible Cache\MSHist012011021720110218	CachePath	%USERPROFILE%\Local Settings\History\History.IE5\MSHist012011021720110218\	2
HKU\S-1-5-21-842925246-1425521274-308236825-500\Software\Microsoft\Windows\CurrentVersion\Internet Settings\5.0\Cache\Extensible Cache\MSHist012011021720110218	CachePrefix	:2011021720110218:	2
HKU\S-1-5-21-842925246-1425521274-308236825-500\Software\Microsoft\Windows\CurrentVersion\Internet Settings\5.0\Cache\Extensible Cache\MSHist012011021720110218	CacheRepair	0	1
HKU\S-1-5-21-842925246-1425521274-308236825-500\Software\Microsoft\Windows\CurrentVersion\Internet Settings\5.0\Cache\Extensible Cache\MSHist012011021820110219	CacheLimit	8192	1
HKU\S-1-5-21-842925246-1425521274-308236825-500\Software\Microsoft\Windows\CurrentVersion\Internet Settings\5.0\Cache\Extensible Cache\MSHist012011021820110219	CacheOptions	11	1
HKU\S-1-5-21-842925246-1425521274-308236825-500\Software\Microsoft\Windows\CurrentVersion\Internet Settings\5.0\Cache\Extensible Cache\MSHist012011021820110219	CachePath	%USERPROFILE%\Local Settings\History\History.IE5\MSHist012011021820110219\	2
HKU\S-1-5-21-842925246-1425521274-308236825-500\Software\Microsoft\Windows\CurrentVersion\	CachePrefix	:2011021820110219:	2

Registry Values Read:

Key	Name	Value	Times
Internet Settings\5.0\Cache\Extensible Cache\ MSHist012011021820110219			
HKU\S-1-5-21-842925246-1425521274-308236825-500\ Software\Microsoft\Windows\CurrentVersion\ Internet Settings\5.0\Cache\Extensible Cache\ MSHist012011021820110219	CacheRepair	0	1
HKU\S-1-5-21-842925246-1425521274-308236825-500\ Software\Microsoft\Windows\CurrentVersion\Internet Settings\5.0\Cache\History	CacheLimit	8192	1
HKU\S-1-5-21-842925246-1425521274-308236825-500\ Software\Microsoft\Windows\CurrentVersion\Internet Settings\5.0\Cache\History	CachePrefix	Visited:	2
HKU\S-1-5-21-842925246-1425521274-308236825-500\ Software\Microsoft\Windows\CurrentVersion\Internet Settings\5.0\Cache\History	PerUserItem	1	1

22.b) cleansweep.exe - File Activities

Files Deleted:

C:\Documents and Settings\Administrator\Application Data\Mozilla\Firefox\Profiles\a3n0yopb.default\cookies.sqlite
C:\Documents and Settings\Administrator\Application Data\Mozilla\Firefox\Profiles\a3n0yopb.default\cookies.sqlite-journal
C:\Documents and Settings\Administrator\Cookies\administrator@adobe[1].txt
C:\Documents and Settings\Administrator\Cookies\administrator@google[1].txt
C:\Documents and Settings\Administrator\Cookies\administrator@java[1].txt
C:\Documents and Settings\Administrator\Cookies\administrator@promotion.adobe[1].txt
C:\Documents and Settings\Administrator\Cookies\administrator@sun[1].txt
C:\Documents and Settings\Administrator\Cookies\administrator@walkernews[1].txt

Files Read:

C:\Documents and Settings\Administrator\Application Data\Mozilla\Firefox\profiles.ini
C:\cleansweep.exe\config.bin

File System Control Communication:

File	Control Code	Times
C:\Program Files\Common Files\	0x00090028	1

Device Control Communication:

File	Control Code	Times
\Device\KsecDD	0x00390008	1

Memory Mapped Files:

File Name
C:\WINDOWS\WinSxS\x86_Microsoft.Windows.Common-Controls_6595b64144ccf1df_6.0.2600.5512_x-ww_35d4ce83\comctl32.dll
C:\WINDOWS\WindowsShell.Manifest
C:\WINDOWS\system32\SHELL32.dll
C:\WINDOWS\system32\WININET.dll
C:\WINDOWS\system32\WS2HELP.dll
C:\WINDOWS\system32\WS2_32.dll
C:\WINDOWS\system32\comctl32.dll
\systemroot\system32\kernel32.dll
\systemroot\system32\msvcrt.dll
\systemroot\system32\ntdll.dll
\systemroot\system32\user32.dll

22.c) cleansweep.exe - Process Activities

Remote Threads Created:

Affected Process

C:\WINDOWS\explorer.exe

Foreign Memory Regions Read:

Process: C:\WINDOWS\explorer.exe

Foreign Memory Regions Written:

Process: C:\WINDOWS\explorer.exe