Anubis - Analysis Report

Analysis Report for Shipping_Label_USPS.exe

MD5: 96255178f15033362c81fb6d9b9c3ce4

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
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:

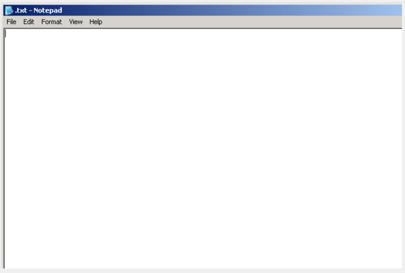
- **Shipping_L.exe** C:\Shipping_L.exe
  Analysis reason: Primary Analysis Subject
  - **Shipping_L.exe** C:\Shipping_L.exe
    Analysis reason: Started by Shipping_L.exe
    - **svchost.exe** svchost.exe
      Analysis reason: Started by Shipping_L.exe
      - **NOTEPAD.EXE** C:\WINDOWS\system32\NOTEPAD.EXE
        Analysis reason: Started by svchost.exe
      - **hhdtdvkc.exe** C:\Documents and Settings\Administrator\Local Settings\Application Data\hhdtdvkc.exe
        Analysis reason: Started by svchost.exe

Table of Contents:

1. General Information

Information about Anubis' invocation	
Time needed:	248 s
Report created:	11/02/12, 17:11:00 UTC
Termination reason:	Timeout
Program version:	1.76.3886

Popups

Process	Window Name	Window Text	Screenshot	Number of Displayed Times
notepad.exe	Untitled - Notepad			1

2. Shipping_L.exe

General information about this executable	
Analysis Reason:	Primary Analysis Subject
Filename:	Shipping_L.exe
Command Line:	"C:\Shipping_L.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\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\comdlg32.dll	0x763B0000	0x00049000
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\SHLWAPI.dll	0x77F60000	0x00076000
C:\WINDOWS\system32\SHELL32.dll	0x7C9C0000	0x00817000
C:\WINDOWS\system32\ole32.dll	0x774E0000	0x0013D000

2.a) Shipping_L.exe - Registry Activities

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	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) Shipping_L.exe - File Activities

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:\Shipping_L.exe
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

2.c) Shipping_L.exe - Process Activities

Processes Created:

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

Remote Threads Created:

Affected Process
C:\Shipping_L.exe

Foreign Memory Regions Read:

Process: C:\Shipping_L.exe

Foreign Memory Regions Written:

Process: C:\Shipping_L.exe

3. Shipping_L.exe

General information about this executable

Analysis Reason:	Started by Shipping_L.exe
Filename:	Shipping_L.exe
MD5:	96255178f15033362c81fb6d9b9c3ce4
SHA-1:	757422f38739c0e0032d1f5534d4a46b328379cd
File Size:	57344
Command Line:	C:\Shipping_L.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

Run-time Dlls

Module Name	Base Address	Size
C:\WINDOWS\system32\Apphelp.dll	0x77B40000	0x00022000
C:\WINDOWS\system32\VERSION.dll	0x77C00000	0x00008000
C:\WINDOWS\system32\ADVAPI32.DLL	0x77DD0000	0x0009B000
C:\WINDOWS\system32\RPCRT4.dll	0x77E70000	0x00092000
C:\WINDOWS\system32\Secur32.dll	0x77FE0000	0x00011000

3.a) Shipping_L.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
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

Registry Values Read:

Key	Name	Value	Times
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
HKLM\Software\Policies\Microsoft\Windows\Safer\CodeIdentifiers\0\Paths\{dda3f824-d8cb-441b-834d-be2efd2c1a33}	SaferFlags	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

3.b) Shipping_L.exe - File Activities

Files Read:

C:\Shipping_L.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\system32\svchost.exe
C:\Windows\AppPatch\sysmain.sdb

3.c) Shipping_L.exe - Process Activities

Processes Created:

Executable	Command Line
C:\WINDOWS\system32\svchost.exe	
	svchost.exe

Remote Threads Created:

Affected Process
C:\WINDOWS\system32\svchost.exe

Foreign Memory Regions Read:
Process: C:\WINDOWS\system32\svchost.exe

Foreign Memory Regions Written:
Process: C:\WINDOWS\system32\svchost.exe

4. svchost.exe

General information about this executable	
Analysis Reason:	Started by Shipping_L.exe
Filename:	svchost.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\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\WS2_32.dll	0x71AB0000	0x00017000
C:\WINDOWS\system32\WS2HELP.dll	0x71AA0000	0x00008000
C:\WINDOWS\system32\urlmon.dll	0x7E1E0000	0x000A2000
C:\WINDOWS\system32\WININET.dll	0x771B0000	0x000AA000
C:\WINDOWS\system32\CRYPT32.dll	0x77A80000	0x00095000
C:\WINDOWS\system32\MSASN1.dll	0x77B20000	0x00012000
C:\WINDOWS\system32\MSCTF.dll	0x74720000	0x0004C000
C:\WINDOWS\system32\netapi32.dll	0x5B860000	0x00055000
C:\WINDOWS\system32\appHelp.dll	0x77B40000	0x00022000
C:\WINDOWS\system32\CLBCATQ.DLL	0x76FD0000	0x0007F000
C:\WINDOWS\system32\COMRes.dll	0x77050000	0x000C5000
C:\WINDOWS\system32\shdocvw.dll	0x7E290000	0x00171000
C:\WINDOWS\system32\CRYPTUI.dll	0x754D0000	0x00080000
C:\WINDOWS\system32\WINTRUST.dll	0x76C30000	0x0002E000
C:\WINDOWS\system32\IMAGEHLP.dll	0x76C90000	0x00028000
C:\WINDOWS\system32\WLDAP32.dll	0x76F60000	0x0002C000
C:\WINDOWS\system32\RichEd20.dll	0x74E30000	0x0006D000
C:\WINDOWS\system32\SETUPAPI.dll	0x77920000	0x000F3000
C:\WINDOWS\System32\mswsock.dll	0x71A50000	0x0003F000

Load-time Dlls

Module Name	Base Address	Size
C:\WINDOWS\system32\DNSAPI.dll	0x76F20000	0x00027000
C:\WINDOWS\System32\winrnr.dll	0x76FB0000	0x00008000
C:\WINDOWS\system32\rasadhlp.dll	0x76FC0000	0x00006000
C:\WINDOWS\system32\wsock32.dll	0x71AD0000	0x00009000
C:\WINDOWS\system32\RASAPI32.DLL	0x76EE0000	0x0003C000
C:\WINDOWS\system32\rasman.dll	0x76E90000	0x00012000
C:\WINDOWS\system32\TAPI32.dll	0x76EB0000	0x0002F000
C:\WINDOWS\system32\rtutils.dll	0x76E80000	0x0000E000
C:\WINDOWS\system32\sensapi.dll	0x722B0000	0x00005000
C:\WINDOWS\system32\hnetcfg.dll	0x662B0000	0x00058000
C:\WINDOWS\System32\wshtcpip.dll	0x71A90000	0x00008000
C:\WINDOWS\system32\mlang.dll	0x75CF0000	0x00091000

4.a) svchost.exe - Registry Activities

Registry Keys Created:
HKLM\Software\Microsoft\DownloadManager

Registry Values Modified:

Key	Name	New Value
HKLM\SYSTEM\CURRENTCONTROLSET\HARDWARE PROFILES\CURRENT\Software\Microsoft\windows\CurrentVersion\Internet Settings	ProxyEnable	0
HKLM\Software\Microsoft\Windows\CurrentVersion\Explorer\Shell Folders	Common Desktop	C:\Documents and Settings\All Users\Desktop
HKLM\Software\Microsoft\Windows\CurrentVersion\Explorer\Shell Folders	Common Documents	C:\Documents and Settings\All Users\Documents
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\MountPoints2\{a1094da8-30a0-11dd-817b-806d6172696f}\	BaseClass	Drive
HKU\S-1-5-21-842925246-1425521274-308236825-500\Software\Microsoft\Windows\CurrentVersion\Explorer\MountPoints2\{a1094daa-30a0-11dd-817b-806d6172696f}\	BaseClass	Drive
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

Registry Values Modified:

Key	Name	New Value
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	Desktop	C:\Documents and Settings\Administrator\Desktop
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
HKU\S-1-5-21-842925246-1425521274-308236825-500\Software\Microsoft\Windows\CurrentVersion\Explorer\Shell Folders	Local AppData	C:\Documents and Settings\Administrator\Local Settings\Application Data
HKU\S-1-5-21-842925246-1425521274-308236825-500\Software\Microsoft\Windows\CurrentVersion\Explorer\Shell Folders	Personal	C:\Documents and Settings\Administrator\My Documents
HKU\S-1-5-21-842925246-1425521274-308236825-500\Software\Microsoft\Windows\CurrentVersion\Internet Settings\ZoneMap\	IntranetName	1
HKU\S-1-5-21-842925246-1425521274-308236825-500\Software\Microsoft\Windows\CurrentVersion\Internet Settings\ZoneMap\	ProxyBypass	1
HKU\S-1-5-21-842925246-1425521274-308236825-500\Software\Microsoft\Windows\CurrentVersion\Internet Settings\ZoneMap\	UNCAsIntranet	1
HKU\S-1-5-21-842925246-1425521274-308236825-500\Software\Microsoft\Windows\ShellNoRoam\MUICache\	C:\Documents and Settings\Administrator\Local Settings\Application Data\hhdtdvkc.exe	hhdtdvkc
HKU\S-1-5-21-842925246-1425521274-308236825-500\Software\Microsoft\Windows\ShellNoRoam\MUICache\	C:\WINDOWS\system32\NOTEPAD.E	Notepad
HKU\S-1-5-21-842925246-1425521274-308236825-500\Software\Microsoft\windows\CurrentVersion\Internet Settings	ProxyEnable	0
HKU\S-1-5-21-842925246-1425521274-308236825-500\Software\Microsoft\windows\CurrentVersion\Internet Settings\Connections	SavedLegacySettings	0x3c000000160000000100000000000000000000000000000000040000000000

Registry Values Read:

Key	Name	Value	Times
HKLM\SOFTWARE\CLASSES\.ASP		aspfile	2
HKLM\SOFTWARE\CLASSES\.BAT		batfile	2
HKLM\SOFTWARE\CLASSES\.CER		CERFile	2
HKLM\SOFTWARE\CLASSES\.CHM		chm.file	2
HKLM\SOFTWARE\CLASSES\.CMD		cmdfile	2
HKLM\SOFTWARE\CLASSES\.COM		comfile	2
HKLM\SOFTWARE\CLASSES\.CPL		cplfile	2
HKLM\SOFTWARE\CLASSES\.CRT		CERFile	2
HKLM\SOFTWARE\CLASSES\.EXE		exefile	4
HKLM\SOFTWARE\CLASSES\.HLP		hlpfile	1
HKLM\SOFTWARE\CLASSES\.HTA		htafile	1
HKLM\SOFTWARE\CLASSES\.INF		inffile	1
HKLM\SOFTWARE\CLASSES\.INS		x-internet-signup	1
HKLM\SOFTWARE\CLASSES\.ISP		x-internet-signup	1
HKLM\SOFTWARE\CLASSES\.ITS		ITS File	1
HKLM\SOFTWARE\CLASSES\.JS		JSFile	1
HKLM\SOFTWARE\CLASSES\.JSE		JSEFile	1
HKLM\SOFTWARE\CLASSES\.LNK		lnkfile	1
HKLM\SOFTWARE\CLASSES\.MSC		MSCFile	1
HKLM\SOFTWARE\CLASSES\.MSI		Msi.Package	1
HKLM\SOFTWARE\CLASSES\.MSP		Msi.Patch	1
HKLM\SOFTWARE\CLASSES\.PIF		piffile	1
HKLM\SOFTWARE\CLASSES\.PRF		prffile	1
HKLM\SOFTWARE\CLASSES\.REG		regfile	1
HKLM\SOFTWARE\CLASSES\.SCF		SHCmdFile	1
HKLM\SOFTWARE\CLASSES\.SCR		scrfile	1
HKLM\SOFTWARE\CLASSES\.SCT		scriptletfile	1
HKLM\SOFTWARE\CLASSES\.SHB		DocShortcut	1
HKLM\SOFTWARE\CLASSES\.SHS		ShellScrap	1

Registry Values Read:

Key	Name	Value	Times
HKLM\SOFTWARE\CLASSES\.TXT		txtfile	4
HKLM\SOFTWARE\CLASSES\.TXT	PerceivedType	text	1
HKLM\SOFTWARE\CLASSES\.URL		InternetShortcut	1
HKLM\SOFTWARE\CLASSES\.VBE		VBEFile	1
HKLM\SOFTWARE\CLASSES\.VBS		VBSFile	1
HKLM\SOFTWARE\CLASSES\.WSC		scriptletfile	1
HKLM\SOFTWARE\CLASSES\.WSF		WSFFile	1
HKLM\SOFTWARE\CLASSES\.WSH		WSHFile	1
HKLM\SOFTWARE\CLASSES\CLSID\{20D04FE0-3AEA-1069-A2D8-08002B30309D}\INPROCSERVER32		%SystemRoot%\system32\SHELL32.dll	1
HKLM\SOFTWARE\CLASSES\CLSID\{7B8A2D94-0AC9-11D1-896C-00C04FB6BFC4}\INPROCSERVER32		C:\WINDOWS\system32\urlmon.dll	2
HKLM\SOFTWARE\CLASSES\CLSID\{7B8A2D94-0AC9-11D1-896C-00C04FB6BFC4}\INPROCSERVER32	ThreadingModel	Both	1
HKLM\SOFTWARE\CLASSES\CLSID\{871C5380-42A0-1069-A2EA-08002B30309D}\INPROCSERVER32		%SystemRoot%\system32\shdocvw.dll	2
HKLM\SOFTWARE\CLASSES\CLSID\{871C5380-42A0-1069-A2EA-08002B30309D}\INPROCSERVER32	ThreadingModel	Apartment	1
HKLM\SOFTWARE\CLASSES\CLSID\{871C5380-42A0-1069-A2EA-08002B30309D}\SHELLFOLDER	WantsParseDisplayNa		1
HKLM\SOFTWARE\CLASSES\CLSID\{AEB6717E-7E19-11D0-97EE-00C04FD91972}\INPROCSERVER32		shell32.dll	2
HKLM\SOFTWARE\CLASSES\DIRECTORY	AlwaysShowExt		1
HKLM\SOFTWARE\CLASSES\DRIVE\SHELLEX\FOLDEREXTENSIONS\{FBEB8A05-BEEE-4442-804E-409D6C4515E9}	DriveMask	32	3
HKLM\SOFTWARE\CLASSES\EXEFILE\SHELL\OPEN\COMMAND		"%1" %*	2
HKLM\SOFTWARE\CLASSES\INTERFACE\{000214E6-0000-0000-C000-000000000046}\PROXYSTUBCLSID32		{bf50b68e-29b8-4386-ae9c-9734d5117cd5}	1
HKLM\SOFTWARE\CLASSES\INTERFACE\{79EAC9C4-BAF9-11CE-8C82-00AA004BA90B}\PROXYSTUBCLSID32		{B8DA6310-E19B-11D0-933C-00A0C90DCAA9}	1
HKLM\SOFTWARE\CLASSES\INTERFACE\{93F2F68C-1D1B-11D3-A30E-00C04F79ABD1}\PROXYSTUBCLSID32		{bf50b68e-29b8-4386-ae9c-9734d5117cd5}	1
HKLM\SOFTWARE\CLASSES\INTERFACE\{B722BCCB-4E68-101B-A2BC-00AA00404770}\PROXYSTUBCLSID32		{B8DA6310-E19B-11D0-933C-00A0C90DCAA9}	1
HKLM\SOFTWARE\CLASSES\INTERFACE\{EAB22AC1-30C1-11CF-A7EB-0000C05BAE0B}\TYPELIB		{EAB22AC0-30C1-11CF-A7EB-0000C05BAE0B}	1
HKLM\SOFTWARE\CLASSES\TXTFILE	EditFlags	65536	1
HKLM\SOFTWARE\CLASSES\TXTFILE\SHELL\OPEN\COMMAND		%SystemRoot%\system32\NOTEPAD.EXE %1	4
HKLM\SOFTWARE\Microsoft\CTF\SystemShared\	CUAS	0	1
HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Internet Settings	UrlEncoding	0x00000000	2
HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Internet Settings\5.0\User Agent\Post Platform	.NET CLR 1.1.4322		1
HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Internet Settings\5.0\User Agent\Post Platform	.NET CLR 2.0.50727		1
HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Internet Settings\5.0\User Agent\Post Platform	.NET CLR 3.0.04506.30		1
HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Internet Settings\5.0\User Agent\Post Platform	.NET CLR 3.0.04506.648		1

Registry Values Read:

Key	Name	Value	Times
HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Internet Settings\5.0\User Agent\Post Platform	.NET CLR 3.5.21022		1
HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Internet Settings\5.0\User Agent\Post Platform	.NET4.0C		1
HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Internet Settings\5.0\User Agent\Post Platform	.NET4.0E		1
HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Internet Settings\User Agent\Post Platform	SV1		1
HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Internet Settings\User Agent\UA Tokens			1
HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Internet Settings\User Agent\UA Tokens	MSN 2.0		1
HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Internet Settings\User Agent\UA Tokens	MSN 2.5		1
HKLM\SYSTEM\CurrentControlSet\Control\Session Manager	CriticalSectionTimeout	2592000	1
HKLM\SYSTEM\CurrentControlSet\Services\Winsock\Parameters	Transports	0x5400630070006900700000004e00650074004200490004f00530000000000	2
HKLM\SYSTEM\Setup	OsLoaderPath	\	2
HKLM\SYSTEM\Setup	SystemPartition	\Device\HarddiskVolume1	2
HKLM\SYSTEM\Setup	SystemSetupInProgres	0	1
HKLM\SYSTEM\WPA\MediaCenter	Installed	0	3
HKLM\Software\Classes\CLSID\{871c5380-42a0-1069-a2ea-08002b30309d}\InProcServer32		%SystemRoot%\system32\shdocvw.dll	1
HKLM\Software\Microsoft\AudioCompressionManager\DriverCache\msacm.iac2	aFormatTagCache	0x01000000100000000204000014000000	1
HKLM\Software\Microsoft\AudioCompressionManager\DriverCache\msacm.iac2	cFilterTags	0	1
HKLM\Software\Microsoft\AudioCompressionManager\DriverCache\msacm.iac2	cFormatTags	2	1
HKLM\Software\Microsoft\AudioCompressionManager\DriverCache\msacm.iac2	fdwSupport	1	1
HKLM\Software\Microsoft\AudioCompressionManager\DriverCache\msacm.imaadpcm	aFormatTagCache	0x01000000100000001100000014000000	1
HKLM\Software\Microsoft\AudioCompressionManager\DriverCache\msacm.imaadpcm	cFilterTags	0	1
HKLM\Software\Microsoft\AudioCompressionManager\DriverCache\msacm.imaadpcm	cFormatTags	2	1
HKLM\Software\Microsoft\AudioCompressionManager\DriverCache\msacm.imaadpcm	fdwSupport	1	1
HKLM\Software\Microsoft\AudioCompressionManager\DriverCache\msacm.l3acm	aFormatTagCache	0x0100000010000000550000001e000000	1
HKLM\Software\Microsoft\AudioCompressionManager\DriverCache\msacm.l3acm	cFilterTags	0	1
HKLM\Software\Microsoft\AudioCompressionManager\DriverCache\msacm.l3acm	cFormatTags	2	1
HKLM\Software\Microsoft\AudioCompressionManager\DriverCache\msacm.l3acm	fdwSupport	1	1
HKLM\Software\Microsoft\AudioCompressionManager\DriverCache\msacm.msadpcm	aFormatTagCache	0x01000000100000000200000032000000	1
HKLM\Software\Microsoft\AudioCompressionManager\DriverCache\msacm.msadpcm	cFilterTags	0	1
HKLM\Software\Microsoft\AudioCompressionManager\DriverCache\msacm.msadpcm	cFormatTags	2	1
HKLM\Software\Microsoft\AudioCompressionManager\DriverCache\msacm.msadpcm	fdwSupport	1	1
HKLM\Software\Microsoft\AudioCompressionManager\DriverCache\msacm.msaudio1	aFormatTagCache	0x0100000012000000060010000160000006610100001c000000	1
HKLM\Software\Microsoft\AudioCompressionManager\DriverCache\msacm.msaudio1	cFilterTags	0	1
HKLM\Software\Microsoft\AudioCompressionManager\DriverCache\msacm.msaudio1	cFormatTags	3	1

Registry Values Read:

Key	Name	Value	Times
HKLM\Software\Microsoft\AudioCompressionManager\DriverCache\msacm.msaudio1	fdwSupport	1	1
HKLM\Software\Microsoft\AudioCompressionManager\DriverCache\msacm.msg711	aFormatTagCache	0x0100000010000000060000001200000000700000012000000	1
HKLM\Software\Microsoft\AudioCompressionManager\DriverCache\msacm.msg711	cFilterTags	0	1
HKLM\Software\Microsoft\AudioCompressionManager\DriverCache\msacm.msg711	cFormatTags	3	1
HKLM\Software\Microsoft\AudioCompressionManager\DriverCache\msacm.msg711	fdwSupport	1	1
HKLM\Software\Microsoft\AudioCompressionManager\DriverCache\msacm.msg723	aFormatTagCache	0x01000000100000004200000001c000000	1
HKLM\Software\Microsoft\AudioCompressionManager\DriverCache\msacm.msg723	cFilterTags	0	1
HKLM\Software\Microsoft\AudioCompressionManager\DriverCache\msacm.msg723	cFormatTags	2	1
HKLM\Software\Microsoft\AudioCompressionManager\DriverCache\msacm.msg723	fdwSupport	1	1
HKLM\Software\Microsoft\AudioCompressionManager\DriverCache\msacm.msgsm610	aFormatTagCache	0x01000000100000003100000014000000	1
HKLM\Software\Microsoft\AudioCompressionManager\DriverCache\msacm.msgsm610	cFilterTags	0	1
HKLM\Software\Microsoft\AudioCompressionManager\DriverCache\msacm.msgsm610	cFormatTags	2	1
HKLM\Software\Microsoft\AudioCompressionManager\DriverCache\msacm.msgsm610	fdwSupport	1	1
HKLM\Software\Microsoft\AudioCompressionManager\DriverCache\msacm.sl_anet	aFormatTagCache	0x01000000100000003001000016000000	1
HKLM\Software\Microsoft\AudioCompressionManager\DriverCache\msacm.sl_anet	cFilterTags	0	1
HKLM\Software\Microsoft\AudioCompressionManager\DriverCache\msacm.sl_anet	cFormatTags	2	1
HKLM\Software\Microsoft\AudioCompressionManager\DriverCache\msacm.sl_anet	fdwSupport	1	1
HKLM\Software\Microsoft\AudioCompressionManager\DriverCache\msacm.trspch	aFormatTagCache	0x01000000100000002200000032000000	1
HKLM\Software\Microsoft\AudioCompressionManager\DriverCache\msacm.trspch	cFilterTags	0	1
HKLM\Software\Microsoft\AudioCompressionManager\DriverCache\msacm.trspch	cFormatTags	2	1
HKLM\Software\Microsoft\AudioCompressionManager\DriverCache\msacm.trspch	fdwSupport	1	1
HKLM\Software\Microsoft\COM3	Com+Enabled	1	4
HKLM\Software\Microsoft\COM3	REGDBVersion	0x0b00000000000000	4
HKLM\Software\Microsoft\Internet Explorer\Main\FeatureControl\FEATURE_BEHAVIORS	*	1	1
HKLM\Software\Microsoft\Internet Explorer\Main\FeatureControl\FEATURE_DISABLE_MK_PROTOCOL	*	1	1
HKLM\Software\Microsoft\Tracing	EnableConsoleTracing	0	1
HKLM\Software\Microsoft\Tracing\RASAPI32	ConsoleTracingMask	4294901760	2
HKLM\Software\Microsoft\Tracing\RASAPI32	EnableConsoleTracing	0	2
HKLM\Software\Microsoft\Tracing\RASAPI32	EnableFileTracing	0	2
HKLM\Software\Microsoft\Tracing\RASAPI32	FileDirectory	%windir%\tracing	4
HKLM\Software\Microsoft\Tracing\RASAPI32	FileTracingMask	4294901760	2
HKLM\Software\Microsoft\Tracing\RASAPI32	MaxFileSize	1048576	2
HKLM\Software\Microsoft\Windows NT\CurrentVersion\Drivers32	midimapper		2
HKLM\Software\Microsoft\Windows NT\CurrentVersion\Drivers32	msacm.iac2		2
HKLM\Software\Microsoft\Windows NT\CurrentVersion\Drivers32	msacm.imaadpcm		3
HKLM\Software\Microsoft\Windows NT\CurrentVersion\Drivers32	msacm.l3acm		2

Registry Values Read:

Key	Name	Value	Times
HKLM\Software\Microsoft\Windows NT\CurrentVersion\Drivers32	msacm.msadpcm		3
HKLM\Software\Microsoft\Windows NT\CurrentVersion\Drivers32	msacm.msaudio1		3
HKLM\Software\Microsoft\Windows NT\CurrentVersion\Drivers32	msacm.msg711		3
HKLM\Software\Microsoft\Windows NT\CurrentVersion\Drivers32	msacm.msg723		3
HKLM\Software\Microsoft\Windows NT\CurrentVersion\Drivers32	msacm.msgsm610		3
HKLM\Software\Microsoft\Windows NT\CurrentVersion\Drivers32	msacm.sl_anet		2
HKLM\Software\Microsoft\Windows NT\CurrentVersion\Drivers32	msacm.trspch		3
HKLM\Software\Microsoft\Windows NT\CurrentVersion\Drivers32	vidc.I420		2
HKLM\Software\Microsoft\Windows NT\CurrentVersion\Drivers32	vidc.M261		2
HKLM\Software\Microsoft\Windows NT\CurrentVersion\Drivers32	vidc.M263		2
HKLM\Software\Microsoft\Windows NT\CurrentVersion\Drivers32	vidc.cvid		2
HKLM\Software\Microsoft\Windows NT\CurrentVersion\Drivers32	vidc.iv31		2
HKLM\Software\Microsoft\Windows NT\CurrentVersion\Drivers32	vidc.iv32		2
HKLM\Software\Microsoft\Windows NT\CurrentVersion\Drivers32	vidc.iv41		2
HKLM\Software\Microsoft\Windows NT\CurrentVersion\Drivers32	vidc.iv50		1
HKLM\Software\Microsoft\Windows NT\CurrentVersion\Drivers32	vidc.iyuv		2
HKLM\Software\Microsoft\Windows NT\CurrentVersion\Drivers32	vidc.mrle		2
HKLM\Software\Microsoft\Windows NT\CurrentVersion\Drivers32	vidc.msvc		2
HKLM\Software\Microsoft\Windows NT\CurrentVersion\Drivers32	vidc.uyvy		2
HKLM\Software\Microsoft\Windows NT\CurrentVersion\Drivers32	vidc.yuy2		2
HKLM\Software\Microsoft\Windows NT\CurrentVersion\Drivers32	vidc.yvu9		2
HKLM\Software\Microsoft\Windows NT\CurrentVersion\Drivers32	vidc.yvyu		2
HKLM\Software\Microsoft\Windows NT\CurrentVersion\Drivers32	wavemapper		2
HKLM\Software\Microsoft\Windows NT\CurrentVersion\ProfileList\S-1-5-21-842925246-1425521274-308236825-500	CentralProfile		1
HKLM\Software\Microsoft\Windows NT\CurrentVersion\ProfileList\S-1-5-21-842925246-1425521274-308236825-500	Flags	0	1
HKLM\Software\Microsoft\Windows NT\CurrentVersion\ProfileList\S-1-5-21-842925246-1425521274-308236825-500	ProfileImagePath	%SystemDrive%\Documents and Settings\Administrator	1
HKLM\Software\Microsoft\Windows NT\CurrentVersion\ProfileList\S-1-5-21-842925246-1425521274-308236825-500	ProfileLoadTimeHigh	30136624	1
HKLM\Software\Microsoft\Windows NT\CurrentVersion\ProfileList\S-1-5-21-842925246-1425521274-308236825-500	ProfileLoadTimeLow	3900495046	1
HKLM\Software\Microsoft\Windows NT\CurrentVersion\ProfileList\S-1-5-21-842925246-1425521274-308236825-500	State	256	1

Registry Values Read:

Key	Name	Value	Times
HKLM\Software\Microsoft\Windows\CurrentVersion	DevicePath	%SystemRoot%\inf	1
HKLM\Software\Microsoft\Windows\CurrentVersion	ProgramFilesDir	C:\Program Files	1
HKLM\Software\Microsoft\Windows\CurrentVersion\Explorer\FileAssociation	CutList	0x4100700070006c006900630061007400669006f006e002000460069006c00	4
HKLM\Software\Microsoft\Windows\CurrentVersion\Explorer\ShellExecuteHooks	{AEB6717E-7E19-11d0		2
HKLM\Software\Microsoft\Windows\CurrentVersion\Explorer\User Shell Folders	Common Desktop	%ALLUSERSPROFILE%\Desktop	1
HKLM\Software\Microsoft\Windows\CurrentVersion\Explorer\User Shell Folders	Common Documents	%ALLUSERSPROFILE%\Documents	1
HKLM\Software\Microsoft\Windows\CurrentVersion\Setup	DriverCachePath	%SystemRoot%\Driver Cache	2
HKLM\Software\Microsoft\Windows\CurrentVersion\Setup	LogLevel	0	2
HKLM\Software\Microsoft\Windows\CurrentVersion\Setup	ServicePackCachePath	c:\windows\ServicePackFiles\ServicePackCache	2
HKLM\Software\Microsoft\Windows\CurrentVersion\Setup	ServicePackSourcePat	D:\	2
HKLM\Software\Microsoft\Windows\CurrentVersion\Setup	SourcePath	D:\	2
HKLM\Software\Policies\Microsoft\Windows\Safer\CodeIdentifiers	AuthenticodeEnabled	0	1
HKLM\Software\Policies\Microsoft\Windows\Safer\CodeIdentifiers	DefaultLevel	262144	1
HKLM\Software\Policies\Microsoft\Windows\Safer\CodeIdentifiers	ExecutableTypes	0x4100440045000000410044005000000042004100530000004200410054 00	2
HKLM\Software\Policies\Microsoft\Windows\Safer\CodeIdentifiers	PolicyScope	0	1
HKLM\Software\Policies\Microsoft\Windows\Safer\CodeIdentifiers	TransparentEnabled	1	4
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

Registry Values Read:

Key	Name	Value	Times
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
HKLM\Software\Policies\Microsoft\Windows\Safer\CodeIdentifiers\0\Paths\{dda3f824-d8cb-441b-834d-be2efd2c1a33}	SaferFlags	0	1
HKLM\System\CurrentControlSet\Control\ComputerName\ActiveComputerName	ComputerName	PC	2
HKLM\System\CurrentControlSet\Control\MediaProperties\PrivateProperties\Joystick\Winmm	wheel	1	1
HKLM\System\CurrentControlSet\Control\ProductOptions	ProductType	WinNT	1
HKLM\System\CurrentControlSet\Services\LDAP	LdapClientIntegrity	1	2
HKLM\System\CurrentControlSet\Services\Tcpip\Parameters	Domain		7
HKLM\System\CurrentControlSet\Services\Tcpip\Parameters	Hostname	pc	7
HKLM\System\CurrentControlSet\Services\Tcpip\Parameters	UseDomainNameDevo	0	1
HKLM\System\CurrentControlSet\Services\Tcpip\Parameters\Winsock	HelperDllName	%SystemRoot%\System32\wshtcpip.dll	1
HKLM\System\CurrentControlSet\Services\Tcpip\Parameters\Winsock	Mapping	0x0b0000000300000002000000010000000600000002000000010000000000	1
HKLM\System\CurrentControlSet\Services\Tcpip\Parameters\Winsock	MaxSockaddrLength	16	1
HKLM\System\CurrentControlSet\Services\Tcpip\Parameters\Winsock	MinSockaddrLength	16	1
HKLM\System\CurrentControlSet\Services\Tcpip\Parameters\Winsock	UseDelayedAcceptanc	0	1
HKLM\System\CurrentControlSet\Services\WinSock2\Parameters	WinSock_Registry_Ver	2.0	4
HKLM\System\CurrentControlSet\Services\WinSock2\Parameters\NameSpace_Catalog5	Num_Catalog_Entries	3	1
HKLM\System\CurrentControlSet\Services\WinSock2\Parameters\NameSpace_Catalog5	Serial_Access_Num	4	2
HKLM\System\CurrentControlSet\Services\WinSock2\Parameters\NameSpace_Catalog5\Catalog_Entries\000000000001	DisplayString	Tcpip	4
HKLM\System\CurrentControlSet\Services\WinSock2\Parameters\NameSpace_Catalog5\Catalog_Entries\000000000001	Enabled	1	1
HKLM\System\CurrentControlSet\Services\WinSock2\Parameters\NameSpace_Catalog5\Catalog_Entries\000000000001	LibraryPath	%SystemRoot%\System32\mswsock.dll	2

Registry Values Read:

Key	Name	Value	Times
HKLM\System\CurrentControlSet\Services\WinSock2\Parameters\NameSpace_Catalog5\Catalog_Entries\000000000001	ProviderId	0x409d05229e7ecf11ae5a00aa00a7112b	1
HKLM\System\CurrentControlSet\Services\WinSock2\Parameters\NameSpace_Catalog5\Catalog_Entries\000000000001	StoresServiceClassInfo	0	1
HKLM\System\CurrentControlSet\Services\WinSock2\Parameters\NameSpace_Catalog5\Catalog_Entries\000000000001	SupportedNameSpace	12	1
HKLM\System\CurrentControlSet\Services\WinSock2\Parameters\NameSpace_Catalog5\Catalog_Entries\000000000001	Version	0	1
HKLM\System\CurrentControlSet\Services\WinSock2\Parameters\NameSpace_Catalog5\Catalog_Entries\000000000002	DisplayString	NTDS	4
HKLM\System\CurrentControlSet\Services\WinSock2\Parameters\NameSpace_Catalog5\Catalog_Entries\000000000002	Enabled	1	1
HKLM\System\CurrentControlSet\Services\WinSock2\Parameters\NameSpace_Catalog5\Catalog_Entries\000000000002	LibraryPath	%SystemRoot%\System32\winrnr.dll	2
HKLM\System\CurrentControlSet\Services\WinSock2\Parameters\NameSpace_Catalog5\Catalog_Entries\000000000002	ProviderId	0xee37263b80e5cf11a55500c04fd8d4ac	1
HKLM\System\CurrentControlSet\Services\WinSock2\Parameters\NameSpace_Catalog5\Catalog_Entries\000000000002	StoresServiceClassInfo	0	1
HKLM\System\CurrentControlSet\Services\WinSock2\Parameters\NameSpace_Catalog5\Catalog_Entries\000000000002	SupportedNameSpace	32	1
HKLM\System\CurrentControlSet\Services\WinSock2\Parameters\NameSpace_Catalog5\Catalog_Entries\000000000002	Version	0	1
HKLM\System\CurrentControlSet\Services\WinSock2\Parameters\NameSpace_Catalog5\Catalog_Entries\000000000003	DisplayString	Network Location Awareness (NLA) Namespace	4
HKLM\System\CurrentControlSet\Services\WinSock2\Parameters\NameSpace_Catalog5\Catalog_Entries\000000000003	Enabled	1	1
HKLM\System\CurrentControlSet\Services\WinSock2\Parameters\NameSpace_Catalog5\Catalog_Entries\000000000003	LibraryPath	%SystemRoot%\System32\mswsock.dll	2
HKLM\System\CurrentControlSet\Services\WinSock2\Parameters\NameSpace_Catalog5\Catalog_Entries\000000000003	ProviderId	0x3a244266a83ba64abaa52e0bd71fdd83	1
HKLM\System\CurrentControlSet\Services\WinSock2\Parameters\NameSpace_Catalog5\Catalog_Entries\000000000003	StoresServiceClassInfo	0	1
HKLM\System\CurrentControlSet\Services\WinSock2\Parameters\NameSpace_Catalog5\Catalog_Entries\000000000003	SupportedNameSpace	15	1
HKLM\System\CurrentControlSet\Services\WinSock2\Parameters\NameSpace_Catalog5\Catalog_Entries\000000000003	Version	0	1
HKLM\System\CurrentControlSet\Services\WinSock2\Parameters\Protocol_Catalog9	Next_Catalog_Entry_ID	1020	1
HKLM\System\CurrentControlSet\Services\WinSock2\Parameters\Protocol_Catalog9	Num_Catalog_Entries	13	1
HKLM\System\CurrentControlSet\Services\WinSock2\Parameters\Protocol_Catalog9	Serial_Access_Num	6	2
HKLM\System\CurrentControlSet\Services\WinSock2\Parameters\Protocol_Catalog9\Catalog_Entries\000000000001	PackedCatalogItem	%SystemRoot%\system32\mswsock.	1
HKLM\System\CurrentControlSet\Services\WinSock2\Parameters\Protocol_Catalog9\Catalog_Entries\000000000002	PackedCatalogItem	%SystemRoot%\system32\mswsock.	1

Registry Values Read:

Key	Name	Value	Times
HKLM\System\CurrentControlSet\Services\WinSock2\Parameters\Protocol_Catalog9\Catalog_Entries\000000000003	PackedCatalogItem	%SystemRoot%\system32\mswsock.	1
HKLM\System\CurrentControlSet\Services\WinSock2\Parameters\Protocol_Catalog9\Catalog_Entries\000000000004	PackedCatalogItem	%SystemRoot%\system32\rsvpsp.d	1
HKLM\System\CurrentControlSet\Services\WinSock2\Parameters\Protocol_Catalog9\Catalog_Entries\000000000005	PackedCatalogItem	%SystemRoot%\system32\rsvpsp.d	1
HKLM\System\CurrentControlSet\Services\WinSock2\Parameters\Protocol_Catalog9\Catalog_Entries\000000000006	PackedCatalogItem	%SystemRoot%\system32\mswsock.	1
HKLM\System\CurrentControlSet\Services\WinSock2\Parameters\Protocol_Catalog9\Catalog_Entries\000000000007	PackedCatalogItem	%SystemRoot%\system32\mswsock.	1
HKLM\System\CurrentControlSet\Services\WinSock2\Parameters\Protocol_Catalog9\Catalog_Entries\000000000008	PackedCatalogItem	%SystemRoot%\system32\mswsock.	1
HKLM\System\CurrentControlSet\Services\WinSock2\Parameters\Protocol_Catalog9\Catalog_Entries\000000000009	PackedCatalogItem	%SystemRoot%\system32\mswsock.	1
HKLM\System\CurrentControlSet\Services\WinSock2\Parameters\Protocol_Catalog9\Catalog_Entries\000000000010	PackedCatalogItem	%SystemRoot%\system32\mswsock.	1
HKLM\System\CurrentControlSet\Services\WinSock2\Parameters\Protocol_Catalog9\Catalog_Entries\000000000011	PackedCatalogItem	%SystemRoot%\system32\mswsock.	1
HKLM\System\CurrentControlSet\Services\WinSock2\Parameters\Protocol_Catalog9\Catalog_Entries\000000000012	PackedCatalogItem	%SystemRoot%\system32\mswsock.	1
HKLM\System\CurrentControlSet\Services\WinSock2\Parameters\Protocol_Catalog9\Catalog_Entries\000000000013	PackedCatalogItem	%SystemRoot%\system32\mswsock.	1
HKLM\System\Setup	SystemSetupInProgres	0	4
HKLM\System\WPA\PnP	seed	1274198464	1
HKU\S-1-5-21-842925246-1425521274-308236825-500\Keyboard Layout\Toggle	Language Hotkey	1	2
HKU\S-1-5-21-842925246-1425521274-308236825-500\Keyboard Layout\Toggle	Layout Hotkey	2	2
HKU\S-1-5-21-842925246-1425521274-308236825-500\SOFTWARE\Microsoft\Windows\CurrentVersion\Internet Settings	EnableHttp1_1	1	1
HKU\S-1-5-21-842925246-1425521274-308236825-500\SOFTWARE\Microsoft\Windows\CurrentVersion\Internet Settings	EnableNegotiate	1	1
HKU\S-1-5-21-842925246-1425521274-308236825-500\SOFTWARE\Microsoft\Windows\CurrentVersion\Internet Settings	MimeExclusionListForC	multipart/mixed multipart/x-mixed-replace multipart/x-byteranges	4
HKU\S-1-5-21-842925246-1425521274-308236825-500\SOFTWARE\Microsoft\Windows\CurrentVersion\Internet Settings	User Agent	Mozilla/4.0 (compatible; MSIE 6.0; Win32)	2
HKU\S-1-5-21-842925246-1425521274-308236825-500\SOFTWARE\Microsoft\Windows\CurrentVersion\Internet Settings	WarnOnPost	0x01000000	1
HKU\S-1-5-21-842925246-1425521274-308236825-500\Software\K-Dat	AutoRefresh	0	1
HKU\S-1-5-21-842925246-1425521274-308236825-500\Software\K-Dat	DefaultAction	2	1
HKU\S-1-5-21-842925246-1425521274-308236825-500\Software\K-Sig	ConfirmDownloadsInCl	0	1
HKU\S-1-5-21-842925246-1425521274-308236825-500\Software\K-Sig	SendDirectlyToClient	1	1
HKU\S-1-5-21-842925246-1425521274-308236825-500\Software\K-Sig	SleepBeforePassing	10	1
HKU\S-1-5-21-842925246-1425521274-308236825-500\Software\K-Sig	UseAlternateMethod	1	1

Registry Values Read:

Key	Name	Value	Times
HKU\S-1-5-21-842925246-1425521274-308236825-500\Software\KLExtensions	AddToMainMenu	1	1
HKU\S-1-5-21-842925246-1425521274-308236825-500\Software\KLExtensions	AskExit	0	1
HKU\S-1-5-21-842925246-1425521274-308236825-500\Software\KLExtensions	ChangeDownloadMenu	1	1
HKU\S-1-5-21-842925246-1425521274-308236825-500\Software\KLExtensions	ChangeToolbarBehave	0	1
HKU\S-1-5-21-842925246-1425521274-308236825-500\Software\Microsoft\Multimedia\Audio	SystemFormats	CD Quality,Radio Quality,Telephone Quality	1
HKU\S-1-5-21-842925246-1425521274-308236825-500\Software\Microsoft\Windows\CurrentVersion\Explorer\	ShellState	0x24000000380800000000000000000000000000000001000000 0d0000000000	2
HKU\S-1-5-21-842925246-1425521274-308236825-500\Software\Microsoft\Windows\CurrentVersion\Explorer\Advanced	DontPrettyPath	0	1
HKU\S-1-5-21-842925246-1425521274-308236825-500\Software\Microsoft\Windows\CurrentVersion\Explorer\Advanced	Filter	0	1
HKU\S-1-5-21-842925246-1425521274-308236825-500\Software\Microsoft\Windows\CurrentVersion\Explorer\Advanced	Hidden	1	1
HKU\S-1-5-21-842925246-1425521274-308236825-500\Software\Microsoft\Windows\CurrentVersion\Explorer\Advanced	HideFileExt	0	1
HKU\S-1-5-21-842925246-1425521274-308236825-500\Software\Microsoft\Windows\CurrentVersion\Explorer\Advanced	HideIcons	0	1
HKU\S-1-5-21-842925246-1425521274-308236825-500\Software\Microsoft\Windows\CurrentVersion\Explorer\Advanced	MapNetDrvBtn	0	1
HKU\S-1-5-21-842925246-1425521274-308236825-500\Software\Microsoft\Windows\CurrentVersion\Explorer\Advanced	NoNetCrawling	1	1
HKU\S-1-5-21-842925246-1425521274-308236825-500\Software\Microsoft\Windows\CurrentVersion\Explorer\Advanced	SeparateProcess	0	1
HKU\S-1-5-21-842925246-1425521274-308236825-500\Software\Microsoft\Windows\CurrentVersion\Explorer\Advanced	ShowCompColor	1	1
HKU\S-1-5-21-842925246-1425521274-308236825-500\Software\Microsoft\Windows\CurrentVersion\Explorer\Advanced	ShowInfoTip	1	1
HKU\S-1-5-21-842925246-1425521274-308236825-500\Software\Microsoft\Windows\CurrentVersion\Explorer\Advanced	ShowSuperHidden	1	1
HKU\S-1-5-21-842925246-1425521274-308236825-500\Software\Microsoft\Windows\CurrentVersion\Explorer\Advanced	WebView	0	1
HKU\S-1-5-21-842925246-1425521274-308236825-500\Software\Microsoft\Windows\CurrentVersion\Explorer\MountPoints2\CPC\Volume\{a1094da8-30a0-11dd-817b-806d6172696f}\	Data	0x000000005c005c003f005c00490044004450023004300640052006f006d00	1
HKU\S-1-5-21-842925246-1425521274-308236825-500\Software\Microsoft\Windows\CurrentVersion\Explorer\MountPoints2\CPC\Volume\{a1094da8-30a0-11dd-817b-806d6172696f}\	Generation	1	1
HKU\S-1-5-21-842925246-1425521274-308236825-500\Software\Microsoft\Windows\CurrentVersion\Explorer\MountPoints2\CPC\Volume\{a1094daa-30a0-11dd-817b-806d6172696f}\	Data	0x000000005c005c003f005c005300540044f00520041004700450023005600	1
HKU\S-1-5-21-842925246-1425521274-308236825-500\Software\Microsoft\Windows\CurrentVersion\Explorer\MountPoints2\CPC\Volume\{a1094daa-30a0-11dd-817b-806d6172696f}\	Generation	1	7
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

Registry Values Read:

Key	Name	Value	Times
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	Desktop	%USERPROFILE%\Desktop	1
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\Explorer\User Shell Folders	Local AppData	%USERPROFILE%\Local Settings\Application Data	1
HKU\S-1-5-21-842925246-1425521274-308236825-500\Software\Microsoft\Windows\CurrentVersion\Explorer\User Shell Folders	Local Settings	%USERPROFILE%\Local Settings	1
HKU\S-1-5-21-842925246-1425521274-308236825-500\Software\Microsoft\Windows\CurrentVersion\Explorer\User Shell Folders	Personal	%USERPROFILE%\My Documents	2
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

Registry Values Read:

Key	Name	Value	Times
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\Internet Settings\5.0\Cache\Extensible Cache\MSHist012011021820110219	CachePrefix	:2011021820110219:	2
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
HKU\S-1-5-21-842925246-1425521274-308236825-500\Software\Microsoft\Windows\CurrentVersion\Internet Settings\ZoneMap\	ProxyBypass	1	2
HKU\S-1-5-21-842925246-1425521274-308236825-500\Software\Microsoft\Windows\CurrentVersion\Internet Settings\ZoneMap\\ProtocolDefaults\	http	3	2
HKU\S-1-5-21-842925246-1425521274-308236825-500\Software\Microsoft\Windows\CurrentVersion\Internet Settings\Zones\0	1806	0	1
HKU\S-1-5-21-842925246-1425521274-308236825-500\Software\Microsoft\Windows\CurrentVersion\Internet Settings\Zones\0	Flags	33	2
HKU\S-1-5-21-842925246-1425521274-308236825-500\Software\Microsoft\Windows\CurrentVersion\Internet Settings\Zones\1	Flags	219	2
HKU\S-1-5-21-842925246-1425521274-308236825-500\Software\Microsoft\Windows\CurrentVersion\Internet Settings\Zones\2	Flags	71	2
HKU\S-1-5-21-842925246-1425521274-308236825-500\Software\Microsoft\Windows\CurrentVersion\Internet Settings\Zones\3	1A10	1	1
HKU\S-1-5-21-842925246-1425521274-308236825-500\Software\Microsoft\Windows\CurrentVersion\Internet Settings\Zones\3	Flags	1	2
HKU\S-1-5-21-842925246-1425521274-308236825-500\Software\Microsoft\Windows\CurrentVersion\Internet Settings\Zones\4	Flags	3	2
HKU\S-1-5-21-842925246-1425521274-308236825-500\Software\Microsoft\Windows\CurrentVersion\Run	CTFMON.EXE	C:\WINDOWS\system32\ctfmon.exe	2
HKU\S-1-5-21-842925246-1425521274-308236825-500\Software\Microsoft\Windows\CurrentVersion\Run	MSMSGS	"C:\Program Files\Messenger\msmsgs.exe" /background	2
HKU\S-1-5-21-842925246-1425521274-308236825-500\Software\Microsoft\Windows\CurrentVersion\Shell Extensions\Cached	{871C5380-42A0-1069-A2EA-08002B30309D} {000214E6-0000-0000-C000-000000000046} 0x401	0x010000007c6c9c7cc0da56ab0ac5c801	1
HKU\S-1-5-21-842925246-1425521274-308236825-500\Software\Microsoft\Windows\ShellNoRoam\MUICache	LangID	0x0904	1
HKU\S-1-5-21-842925246-1425521274-308236825-500\Software\Microsoft\windows\CurrentVersion\Internet Settings\Connections	DefaultConnectionSetti	0x3c00000003000000010000000000000000000000000000000000000040000000000	2

Registry Values Read:

Key	Name	Value	Times
HKU\S-1-5-21-842925246-1425521274-308236825-500\Software\Microsoft\windows\CurrentVersion\Internet Settings\Connections	SavedLegacySettings	0x3c00000015000000010000000000000000000000000000000004000000000000	2

Monitored Registry Keys:

Key Name	Watch subtree	Notify Filter	Count
HKLM\Software\Classes	1	Key Change,Value Change	6
HKLM\Software\Classes\CLSID	1	Key Change,Value Change	4
HKLM\Software\Microsoft\COM3	1	Key Change,Value Change	12
HKLM\Software\Microsoft\Tracing\RASAPI32	0	Attributes Change,Value Change,Security Descriptor Change	2
HKLM\System\CurrentControlSet\Services\WinSock2\Parameters\NameSpace_Catalog5	0	Key Change	1
HKLM\System\CurrentControlSet\Services\WinSock2\Parameters\Protocol_Catalog9	0	Key Change	1
HKU	1	Key Change,Value Change	6

4.b) svchost.exe - File Activities

Files Created:

C:\Documents and Settings\Administrator\Local Settings\Application Data\hhdtdvkc.exe
C:\Documents and Settings\Administrator\Local Settings\Temporary Internet Files\Content.IE5\WDUF49AN\43d982be5107d1b8de698e16759b9956[1].exe
C:\Program Files\Common Files\.txt

Files Read:

C:\Documents and Settings\Administrator\Local Settings\Application Data\hhdtdvkc.exe
C:\Documents and Settings\Administrator\Local Settings\Temporary Internet Files\Content.IE5\WDUF49AN\43d982be5107d1b8de698e16759b9956[1].exe
C:\Documents and Settings\Administrator\My Documents\desktop.ini
C:\Documents and Settings\All Users\Documents\desktop.ini
C:\WINDOWS\Registration\R00000000000b.clb
C:\WINDOWS\system32\NOTEPAD.EXE
PIPE\lsarpc
PIPE\wkssvc

Files Modified:

C:\Documents and Settings\Administrator\Local Settings\Application Data\hhdtdvkc.exe
C:\Documents and Settings\Administrator\Local Settings\Temporary Internet Files\Content.IE5\WDUF49AN\43d982be5107d1b8de698e16759b9956[1].exe
C:\Program Files\Common Files\.txt
MountPointManager
PIPE\lsarpc
PIPE\wkssvc
\Device\Afd\AsyncConnectHlp
\Device\Afd\Endpoint
\Device\RasAcd

File System Control Communication:

File	Control Code	Times
C:\Program Files\Common Files\	0x00090028	1
PIPE\wkssvc	0x0011C017	1
PIPE\lsarpc	0x0011C017	9

Device Control Communication:

File	Control Code	Times
\Device\KsecDD	0x00390008	8
IDE#CdRomQEMU_QEMU_CD-ROM________________________0.9.____#4d513030303020332020202020202020200202020#{53f5630d-b6bf-11d0-94f2-00a0c91efb8b}	0x004D0008	1
MountPointManager	0x006D0008	2
STORAGE#Volume#1&30a96598&0&SignatureB15FB15FOffset7E00Length13F2918000#{53f5630d-b6bf-11d0-94f2-00a0c91efb8b}	0x004D0008	1
MountPointManager	0x006D0034	4
\Device\RasAcd	0x00F14014	1
\Device\Afd\Endpoint	AFD_GET_INFO (0x0001207B)	2
\Device\Afd\Endpoint	AFD_SET_CONTEXT (0x00012047)	16
\Device\Afd\Endpoint	AFD_BIND (0x00012003)	3
\Device\Afd\Endpoint	AFD_GET_TDI_HAND (0x00012037)	6
\Device\Afd\Endpoint	AFD_GET_SOCK_NAI (0x0001202F)	4
\Device\Afd\Endpoint	AFD_CONNECT (0x00012007)	2
unnamed file	0x00120028	3
\Device\Afd\Endpoint	AFD_SEND (0x0001201F)	18
\Device\Afd\Endpoint	AFD_RECV (0x00012017)	97
\Device\Afd\Endpoint	AFD_SET_INFO (0x0001203B)	4
\Device\Afd\Endpoint	AFD_SELECT (0x00012024)	42
\Device\Afd\Endpoint	AFD_DISCONNECT (0x0001202B)	2
\Device\Afd\AsyncConnectHlp	AFD_CONNECT (0x00012007)	1

Memory Mapped Files:

File Name
C:\Documents and Settings\Administrator\Local Settings\Application Data\hhdtdvkc.exe
C:\WINDOWS\AppPatch\AcGenral.DLL
C:\WINDOWS\System32\mswsock.dll
C:\WINDOWS\System32\winrnr.dll
C:\WINDOWS\System32\wshtcpip.dll
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\CLBCATQ.DLL
C:\WINDOWS\system32\COMRes.dll
C:\WINDOWS\system32\DNSAPI.dll
C:\WINDOWS\system32\MSACM32.dll
C:\WINDOWS\system32\MSCTF.dll
C:\WINDOWS\system32\NOTEPAD.EXE
C:\WINDOWS\system32\RASAPI32.DLL
C:\WINDOWS\system32\RichEd20.dll
C:\WINDOWS\system32\SETUPAPI.dll
C:\WINDOWS\system32\SHELL32.dll
C:\WINDOWS\system32\ShimEng.dll
C:\WINDOWS\system32\TAPI32.dll
C:\WINDOWS\system32\UxTheme.dll
C:\WINDOWS\system32\WININET.dll
C:\WINDOWS\system32\WINMM.dll

Memory Mapped Files:

File Name
C:\WINDOWS\system32\WS2HELP.dll
C:\WINDOWS\system32\WS2_32.dll
C:\WINDOWS\system32\comctl32.dll
C:\WINDOWS\system32\hnetcfg.dll
C:\WINDOWS\system32\imm32.dll
C:\WINDOWS\system32\mlang.dll
C:\WINDOWS\system32\notepad.exe
C:\WINDOWS\system32\rasadhlp.dll
C:\WINDOWS\system32\rasman.dll
C:\WINDOWS\system32\rpcss.dll
C:\WINDOWS\system32\rtutils.dll
C:\WINDOWS\system32\sensapi.dll
C:\WINDOWS\system32\shdocvw.dll
C:\WINDOWS\system32\urlmon.dll
C:\WINDOWS\system32\wsock32.dll
C:\Windows\AppPatch\sysmain.sdb

4.c) svchost.exe - Process Activities

Processes Created:

Executable	Command Line
C:\WINDOWS\system32\NOTEPAD.EXE	
C:\WINDOWS\system32\NOTEPAD.EXE	"C:\WINDOWS\system32\NOTEPAD.EXE" C:\Program Files\Common Files\.txt
C:\Documents and Settings\Administrator \Local Settings\Application Data\hhdtdvkc.exe	
C:\Documents and Settings\Administrator \Local Settings\Application Data\hhdtdvkc.exe	"C:\Documents and Settings\Administrator\Local Settings\Application Data\hhdtdvkc.exe"

Remote Threads Created:

Affected Process
C:\WINDOWS\system32\NOTEPAD.EXE
C:\Documents and Settings\Administrator\Local Settings\Application Data\hhdtdvkc.exe

Foreign Memory Regions Read:

Process: C:\Documents and Settings\Administrator\Local Settings\Application Data\hhdtdvkc.exe
Process: C:\WINDOWS\system32\NOTEPAD.EXE

Foreign Memory Regions Written:

Process: C:\Documents and Settings\Administrator\Local Settings\Application Data\hhdtdvkc.exe
Process: C:\WINDOWS\system32\NOTEPAD.EXE

4.d) svchost.exe - Network Activity

HTTP Conversations:

From ANUBIS:1028 to 217.160.236.108:84 - [217.160.236.108:84]
Request: GET /69cde37319E9AD1D8B59022C3F75A2D11FCE400505CAAFAD1C476EF025D7D41E16204D7DB9464A55036151A1062ABAFE6FD464C96AB4AF
Response: 200 "OK"
From ANUBIS:1030 to 217.160.236.108:84 - [217.160.236.108:84]
Request: GET //get/43d982be5107d1b8de698e16759b9956.exe
Response: 200 "OK"

5. NOTEPAD.EXE

General information about this executable

Analysis Reason:	Started by svchost.exe
Filename:	NOTEPAD.EXE
MD5:	5e28284f9b5f9097640d58a73d38ad4c
SHA-1:	7a90f8b051bc82cc9cadbcc9ba345ced02891a6c
File Size:	69120
Command Line:	"C:\WINDOWS\system32\NOTEPAD.EXE" C:\Program Files\Common Files\.txt
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\NOTEPAD.EXE	0x01000000	0x00014000
C:\WINDOWS\system32\kernel32.dll	0x7C800000	0x000F6000
C:\WINDOWS\system32\comdlg32.dll	0x763B0000	0x00049000
C:\WINDOWS\system32\ADVAPI32.dll	0x77DD0000	0x0009B000
C:\WINDOWS\system32\RPCRT4.dll	0x77E70000	0x00092000
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\SHELL32.dll	0x7C9C0000	0x00817000
C:\WINDOWS\system32\WINSPOOL.DRV	0x73000000	0x00026000
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\USERENV.dll	0x769C0000	0x000B4000
C:\WINDOWS\system32\UxTheme.dll	0x5AD70000	0x00038000

Run-time Dlls

Module Name	Base Address	Size
C:\WINDOWS\system32\MSCTF.dll	0x74720000	0x0004C000

5.a) NOTEPAD.EXE - Registry Activities

Registry Values Modified:

Key	Name	New Value
HKU\S-1-5-21-842925246-1425521274-308236825-500\Software\Microsoft\Notepad	StatusBar	0
HKU\S-1-5-21-842925246-1425521274-308236825-500\Software\Microsoft\Notepad	fMLE_is_broken	0
HKU\S-1-5-21-842925246-1425521274-308236825-500\Software\Microsoft\Notepad	fSaveWindowPositions	0
HKU\S-1-5-21-842925246-1425521274-308236825-500\Software\Microsoft\Notepad	fWrap	0
HKU\S-1-5-21-842925246-1425521274-308236825-500\Software\Microsoft\Notepad	iMarginBottom	2500
HKU\S-1-5-21-842925246-1425521274-308236825-500\Software\Microsoft\Notepad	iMarginLeft	2000
HKU\S-1-5-21-842925246-1425521274-308236825-500\Software\Microsoft\Notepad	iMarginRight	2000

Registry Values Modified:

Key	Name	New Value
HKU\S-1-5-21-842925246-1425521274-308236825-500\Software\Microsoft\Notepad	iMarginTop	2500
HKU\S-1-5-21-842925246-1425521274-308236825-500\Software\Microsoft\Notepad	iPointSize	100
HKU\S-1-5-21-842925246-1425521274-308236825-500\Software\Microsoft\Notepad	iWindowPosDX	768
HKU\S-1-5-21-842925246-1425521274-308236825-500\Software\Microsoft\Notepad	iWindowPosDY	536
HKU\S-1-5-21-842925246-1425521274-308236825-500\Software\Microsoft\Notepad	iWindowPosX	133
HKU\S-1-5-21-842925246-1425521274-308236825-500\Software\Microsoft\Notepad	iWindowPosY	127
HKU\S-1-5-21-842925246-1425521274-308236825-500\Software\Microsoft\Notepad	lfCharSet	0
HKU\S-1-5-21-842925246-1425521274-308236825-500\Software\Microsoft\Notepad	lfClipPrecision	2
HKU\S-1-5-21-842925246-1425521274-308236825-500\Software\Microsoft\Notepad	lfEscapement	0
HKU\S-1-5-21-842925246-1425521274-308236825-500\Software\Microsoft\Notepad	lfFaceName	Lucida Console
HKU\S-1-5-21-842925246-1425521274-308236825-500\Software\Microsoft\Notepad	lfItalic	0
HKU\S-1-5-21-842925246-1425521274-308236825-500\Software\Microsoft\Notepad	lfOrientation	0
HKU\S-1-5-21-842925246-1425521274-308236825-500\Software\Microsoft\Notepad	lfOutPrecision	1
HKU\S-1-5-21-842925246-1425521274-308236825-500\Software\Microsoft\Notepad	lfPitchAndFamily	49
HKU\S-1-5-21-842925246-1425521274-308236825-500\Software\Microsoft\Notepad	lfQuality	2
HKU\S-1-5-21-842925246-1425521274-308236825-500\Software\Microsoft\Notepad	lfStrikeOut	0
HKU\S-1-5-21-842925246-1425521274-308236825-500\Software\Microsoft\Notepad	lfUnderline	0
HKU\S-1-5-21-842925246-1425521274-308236825-500\Software\Microsoft\Notepad	lfWeight	400
HKU\S-1-5-21-842925246-1425521274-308236825-500\Software\Microsoft\Notepad	szHeader	&f
HKU\S-1-5-21-842925246-1425521274-308236825-500\Software\Microsoft\Notepad	szTrailer	Page &p

Registry Values Read:

Key	Name	Value	Times
HKLM\SOFTWARE\CLASSES\.TXT		txtfile	1
HKLM\SOFTWARE\CLASSES\.TXT	PerceivedType	text	1
HKLM\SOFTWARE\CLASSES\CLSID\{20D04FE0-3AEA-1069-A2D8-08002B30309D}\INPROCSERVER32		%SystemRoot%\system32\SHELL32.dll	1
HKLM\SOFTWARE\CLASSES\DIRECTORY	AlwaysShowExt		1
HKLM\SOFTWARE\CLASSES\DRIVE\SHELLEX\FOLDEREXTENSIONS\{FBEB8A05-BEEE-4442-804E-409D6C4515E9}	DriveMask	32	1
HKLM\SOFTWARE\Microsoft\CTF\SystemShared\	CUAS	0	1
HKLM\SYSTEM\CurrentControlSet\Control\Session Manager	CriticalSectionTimeout	2592000	1
HKLM\SYSTEM\Setup	SystemSetupInProgres	0	1
HKLM\SYSTEM\WPA\MediaCenter	Installed	0	1
HKLM\Software\Microsoft\AudioCompressionManager\DriverCache\msacm.iac2	aFormatTagCache	0x01000000100000000204000014000000	1
HKLM\Software\Microsoft\AudioCompressionManager\DriverCache\msacm.iac2	cFilterTags	0	1

Registry Values Read:

Key	Name	Value	Times
HKLM\Software\Microsoft\AudioCompressionManager\DriverCache\msacm.iac2	cFormatTags	2	1
HKLM\Software\Microsoft\AudioCompressionManager\DriverCache\msacm.iac2	fdwSupport	1	1
HKLM\Software\Microsoft\AudioCompressionManager\DriverCache\msacm.imaadpcm	aFormatTagCache	0x01000000100000001100000014000000	1
HKLM\Software\Microsoft\AudioCompressionManager\DriverCache\msacm.imaadpcm	cFilterTags	0	1
HKLM\Software\Microsoft\AudioCompressionManager\DriverCache\msacm.imaadpcm	cFormatTags	2	1
HKLM\Software\Microsoft\AudioCompressionManager\DriverCache\msacm.imaadpcm	fdwSupport	1	1
HKLM\Software\Microsoft\AudioCompressionManager\DriverCache\msacm.l3acm	aFormatTagCache	0x0100000010000000550000001e000000	1
HKLM\Software\Microsoft\AudioCompressionManager\DriverCache\msacm.l3acm	cFilterTags	0	1
HKLM\Software\Microsoft\AudioCompressionManager\DriverCache\msacm.l3acm	cFormatTags	2	1
HKLM\Software\Microsoft\AudioCompressionManager\DriverCache\msacm.l3acm	fdwSupport	1	1
HKLM\Software\Microsoft\AudioCompressionManager\DriverCache\msacm.msadpcm	aFormatTagCache	0x01000000100000000200000032000000	1
HKLM\Software\Microsoft\AudioCompressionManager\DriverCache\msacm.msadpcm	cFilterTags	0	1
HKLM\Software\Microsoft\AudioCompressionManager\DriverCache\msacm.msadpcm	cFormatTags	2	1
HKLM\Software\Microsoft\AudioCompressionManager\DriverCache\msacm.msadpcm	fdwSupport	1	1
HKLM\Software\Microsoft\AudioCompressionManager\DriverCache\msacm.msaudio1	aFormatTagCache	0x010000001200000060010000160000006610100001c000000	1
HKLM\Software\Microsoft\AudioCompressionManager\DriverCache\msacm.msaudio1	cFilterTags	0	1
HKLM\Software\Microsoft\AudioCompressionManager\DriverCache\msacm.msaudio1	cFormatTags	3	1
HKLM\Software\Microsoft\AudioCompressionManager\DriverCache\msacm.msaudio1	fdwSupport	1	1
HKLM\Software\Microsoft\AudioCompressionManager\DriverCache\msacm.msg711	aFormatTagCache	0x010000001000000006000000120000000700000012000000	1
HKLM\Software\Microsoft\AudioCompressionManager\DriverCache\msacm.msg711	cFilterTags	0	1
HKLM\Software\Microsoft\AudioCompressionManager\DriverCache\msacm.msg711	cFormatTags	3	1
HKLM\Software\Microsoft\AudioCompressionManager\DriverCache\msacm.msg711	fdwSupport	1	1
HKLM\Software\Microsoft\AudioCompressionManager\DriverCache\msacm.msg723	aFormatTagCache	0x0100000010000000420000001c000000	1
HKLM\Software\Microsoft\AudioCompressionManager\DriverCache\msacm.msg723	cFilterTags	0	1
HKLM\Software\Microsoft\AudioCompressionManager\DriverCache\msacm.msg723	cFormatTags	2	1
HKLM\Software\Microsoft\AudioCompressionManager\DriverCache\msacm.msg723	fdwSupport	1	1
HKLM\Software\Microsoft\AudioCompressionManager\DriverCache\msacm.msgsm610	aFormatTagCache	0x01000000100000003100000014000000	1
HKLM\Software\Microsoft\AudioCompressionManager\DriverCache\msacm.msgsm610	cFilterTags	0	1
HKLM\Software\Microsoft\AudioCompressionManager\DriverCache\msacm.msgsm610	cFormatTags	2	1
HKLM\Software\Microsoft\AudioCompressionManager\DriverCache\msacm.msgsm610	fdwSupport	1	1
HKLM\Software\Microsoft\AudioCompressionManager\DriverCache\msacm.sl_anet	aFormatTagCache	0x01000000100000003001000016000000	1
HKLM\Software\Microsoft\AudioCompressionManager\DriverCache\msacm.sl_anet	cFilterTags	0	1

Registry Values Read:

Key	Name	Value	Times
HKLM\Software\Microsoft\AudioCompressionManager\DriverCache\msacm.sl_anet	cFormatTags	2	1
HKLM\Software\Microsoft\AudioCompressionManager\DriverCache\msacm.sl_anet	fdwSupport	1	1
HKLM\Software\Microsoft\AudioCompressionManager\DriverCache\msacm.trspch	aFormatTagCache	0x01000000100000002200000032000000	1
HKLM\Software\Microsoft\AudioCompressionManager\DriverCache\msacm.trspch	cFilterTags	0	1
HKLM\Software\Microsoft\AudioCompressionManager\DriverCache\msacm.trspch	cFormatTags	2	1
HKLM\Software\Microsoft\AudioCompressionManager\DriverCache\msacm.trspch	fdwSupport	1	1
HKLM\Software\Microsoft\Windows NT\CurrentVersion\Drivers32	midimapper		2
HKLM\Software\Microsoft\Windows NT\CurrentVersion\Drivers32	msacm.iac2		2
HKLM\Software\Microsoft\Windows NT\CurrentVersion\Drivers32	msacm.imaadpcm		3
HKLM\Software\Microsoft\Windows NT\CurrentVersion\Drivers32	msacm.l3acm	C:\WINDOWS\system32\l3codeca.acm	2
HKLM\Software\Microsoft\Windows NT\CurrentVersion\Drivers32	msacm.msadpcm	msadp32.acm	3
HKLM\Software\Microsoft\Windows NT\CurrentVersion\Drivers32	msacm.msaudio1		3
HKLM\Software\Microsoft\Windows NT\CurrentVersion\Drivers32	msacm.msg711	msg711.acm	3
HKLM\Software\Microsoft\Windows NT\CurrentVersion\Drivers32	msacm.msg723		3
HKLM\Software\Microsoft\Windows NT\CurrentVersion\Drivers32	msacm.msgsm610		3
HKLM\Software\Microsoft\Windows NT\CurrentVersion\Drivers32	msacm.sl_anet		2
HKLM\Software\Microsoft\Windows NT\CurrentVersion\Drivers32	msacm.trspch	tssoft32.acm	3
HKLM\Software\Microsoft\Windows NT\CurrentVersion\Drivers32	vidc.I420		2
HKLM\Software\Microsoft\Windows NT\CurrentVersion\Drivers32	vidc.M261		2
HKLM\Software\Microsoft\Windows NT\CurrentVersion\Drivers32	vidc.M263		2
HKLM\Software\Microsoft\Windows NT\CurrentVersion\Drivers32	vidc.cvid		2
HKLM\Software\Microsoft\Windows NT\CurrentVersion\Drivers32	vidc.iv31		2
HKLM\Software\Microsoft\Windows NT\CurrentVersion\Drivers32	vidc.iv32		2
HKLM\Software\Microsoft\Windows NT\CurrentVersion\Drivers32	vidc.iv41		2
HKLM\Software\Microsoft\Windows NT\CurrentVersion\Drivers32	vidc.iv50		1
HKLM\Software\Microsoft\Windows NT\CurrentVersion\Drivers32	vidc.iyuv		2
HKLM\Software\Microsoft\Windows NT\CurrentVersion\Drivers32	vidc.mrle		2
HKLM\Software\Microsoft\Windows NT\CurrentVersion\Drivers32	vidc.msvc		2
HKLM\Software\Microsoft\Windows NT\CurrentVersion\Drivers32	vidc.uyvy		2
HKLM\Software\Microsoft\Windows NT\CurrentVersion\Drivers32	vidc.yuy2		2
HKLM\Software\Microsoft\Windows NT\CurrentVersion\Drivers32	vidc.yvu9		2
HKLM\Software\Microsoft\Windows NT\CurrentVersion\Drivers32	vidc.yvyu		2

Registry Values Read:

Key	Name	Value	Times
HKLM\Software\Microsoft\Windows NT\CurrentVersion\Drivers32	wavemapper		2
HKLM\Software\Policies\Microsoft\Windows\Safer\CodeIdentifiers	TransparentEnabled	1	1
HKLM\System\CurrentControlSet\Control\MediaProperties\PrivateProperties\Joystick\Winmm	wheel	1	1
HKLM\System\CurrentControlSet\Control\ProductOptions	ProductType	WinNT	1
HKU\S-1-5-21-842925246-1425521274-308236825-500\Keyboard Layout\Toggle	Language Hotkey	1	4
HKU\S-1-5-21-842925246-1425521274-308236825-500\Keyboard Layout\Toggle	Layout Hotkey	2	4
HKU\S-1-5-21-842925246-1425521274-308236825-500\Software\Microsoft\Multimedia\Audio	SystemFormats	CD Quality,Radio Quality,Telephone Quality	1
HKU\S-1-5-21-842925246-1425521274-308236825-500\Software\Microsoft\Notepad	StatusBar	0	1
HKU\S-1-5-21-842925246-1425521274-308236825-500\Software\Microsoft\Notepad	fMLE_is_broken	0	1
HKU\S-1-5-21-842925246-1425521274-308236825-500\Software\Microsoft\Notepad	fSaveWindowPositions	0	1
HKU\S-1-5-21-842925246-1425521274-308236825-500\Software\Microsoft\Notepad	fWrap	0	1
HKU\S-1-5-21-842925246-1425521274-308236825-500\Software\Microsoft\Notepad	iMarginBottom	2500	1
HKU\S-1-5-21-842925246-1425521274-308236825-500\Software\Microsoft\Notepad	iMarginLeft	2000	1
HKU\S-1-5-21-842925246-1425521274-308236825-500\Software\Microsoft\Notepad	iMarginRight	2000	1
HKU\S-1-5-21-842925246-1425521274-308236825-500\Software\Microsoft\Notepad	iMarginTop	2500	1
HKU\S-1-5-21-842925246-1425521274-308236825-500\Software\Microsoft\Notepad	iPointSize	100	1
HKU\S-1-5-21-842925246-1425521274-308236825-500\Software\Microsoft\Notepad	iWindowPosDX	768	1
HKU\S-1-5-21-842925246-1425521274-308236825-500\Software\Microsoft\Notepad	iWindowPosDY	536	1
HKU\S-1-5-21-842925246-1425521274-308236825-500\Software\Microsoft\Notepad	iWindowPosX	133	1
HKU\S-1-5-21-842925246-1425521274-308236825-500\Software\Microsoft\Notepad	iWindowPosY	127	1
HKU\S-1-5-21-842925246-1425521274-308236825-500\Software\Microsoft\Notepad	lfCharSet	0	1
HKU\S-1-5-21-842925246-1425521274-308236825-500\Software\Microsoft\Notepad	lfClipPrecision	2	1
HKU\S-1-5-21-842925246-1425521274-308236825-500\Software\Microsoft\Notepad	lfEscapement	0	1
HKU\S-1-5-21-842925246-1425521274-308236825-500\Software\Microsoft\Notepad	lfFaceName	Lucida Console	1
HKU\S-1-5-21-842925246-1425521274-308236825-500\Software\Microsoft\Notepad	lfItalic	0	1
HKU\S-1-5-21-842925246-1425521274-308236825-500\Software\Microsoft\Notepad	lfOrientation	0	1
HKU\S-1-5-21-842925246-1425521274-308236825-500\Software\Microsoft\Notepad	lfOutPrecision	1	1
HKU\S-1-5-21-842925246-1425521274-308236825-500\Software\Microsoft\Notepad	lfPitchAndFamily	49	1
HKU\S-1-5-21-842925246-1425521274-308236825-500\Software\Microsoft\Notepad	lfQuality	2	1
HKU\S-1-5-21-842925246-1425521274-308236825-500\Software\Microsoft\Notepad	lfStrikeOut	0	1
HKU\S-1-5-21-842925246-1425521274-308236825-500\Software\Microsoft\Notepad	lfUnderline	0	1
HKU\S-1-5-21-842925246-1425521274-308236825-500\Software\Microsoft\Notepad	lfWeight	400	1

Registry Values Read:

Key	Name	Value	Times
HKU\S-1-5-21-842925246-1425521274-308236825-500\Software\Microsoft\Notepad	szHeader	&f	1
HKU\S-1-5-21-842925246-1425521274-308236825-500\Software\Microsoft\Notepad	szTrailer	Page &p	1
HKU\S-1-5-21-842925246-1425521274-308236825-500\Software\Microsoft\Windows\CurrentVersion\Explorer\	ShellState	0x240000003808000000000000000000000000000000000100000000d0000000000	2
HKU\S-1-5-21-842925246-1425521274-308236825-500\Software\Microsoft\Windows\CurrentVersion\Explorer\Advanced	DontPrettyPath	0	1
HKU\S-1-5-21-842925246-1425521274-308236825-500\Software\Microsoft\Windows\CurrentVersion\Explorer\Advanced	Filter	0	1
HKU\S-1-5-21-842925246-1425521274-308236825-500\Software\Microsoft\Windows\CurrentVersion\Explorer\Advanced	Hidden	1	1
HKU\S-1-5-21-842925246-1425521274-308236825-500\Software\Microsoft\Windows\CurrentVersion\Explorer\Advanced	HideFileExt	0	1
HKU\S-1-5-21-842925246-1425521274-308236825-500\Software\Microsoft\Windows\CurrentVersion\Explorer\Advanced	HideIcons	0	1
HKU\S-1-5-21-842925246-1425521274-308236825-500\Software\Microsoft\Windows\CurrentVersion\Explorer\Advanced	MapNetDrvBtn	0	1
HKU\S-1-5-21-842925246-1425521274-308236825-500\Software\Microsoft\Windows\CurrentVersion\Explorer\Advanced	NoNetCrawling	1	1
HKU\S-1-5-21-842925246-1425521274-308236825-500\Software\Microsoft\Windows\CurrentVersion\Explorer\Advanced	SeparateProcess	0	1
HKU\S-1-5-21-842925246-1425521274-308236825-500\Software\Microsoft\Windows\CurrentVersion\Explorer\Advanced	ShowCompColor	1	1
HKU\S-1-5-21-842925246-1425521274-308236825-500\Software\Microsoft\Windows\CurrentVersion\Explorer\Advanced	ShowInfoTip	1	1
HKU\S-1-5-21-842925246-1425521274-308236825-500\Software\Microsoft\Windows\CurrentVersion\Explorer\Advanced	ShowSuperHidden	1	1
HKU\S-1-5-21-842925246-1425521274-308236825-500\Software\Microsoft\Windows\CurrentVersion\Explorer\Advanced	WebView	0	1
HKU\S-1-5-21-842925246-1425521274-308236825-500\Software\Microsoft\Windows\CurrentVersion\Explorer\User Shell Folders	Local Settings	%USERPROFILE%\Local Settings	1
HKU\S-1-5-21-842925246-1425521274-308236825-500\Software\Microsoft\Windows\CurrentVersion\Explorer\User Shell Folders	Personal	%USERPROFILE%\My Documents	1
HKU\S-1-5-21-842925246-1425521274-308236825-500\Software\Microsoft\Windows\CurrentVersion\Explorer\User Shell Folders	Recent	%USERPROFILE%\Recent	1

5.b) NOTEPAD.EXE - File Activities

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:\Program Files\Common Files\.txt
C:\WINDOWS\AppPatch\AcGenral.DLL
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\MSACM32.dll
C:\WINDOWS\system32\MSCTF.dll
C:\WINDOWS\system32\SHELL32.dll
C:\WINDOWS\system32\ShimEng.dll
C:\WINDOWS\system32\UxTheme.dll
C:\WINDOWS\system32\WINMM.dll
C:\WINDOWS\system32\WINSPOOL.DRV
C:\WINDOWS\system32\imm32.dll
C:\Windows\AppPatch\sysmain.sdb

6. hhdtdvkc.exe

General information about this executable

Analysis Reason:	Started by svchost.exe
Filename:	hhdtdvkc.exe
MD5:	076327601597d04320191864f10d7f99
SHA-1:	41736a4f2d2672ed1e289d6647bbc51146c9bbd2
File Size:	539136
Command Line:	"C:\Documents and Settings\Administrator\Local Settings\Application Data\hhdtdvkc.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

Run-time Dlls

Module Name	Base Address	Size
C:\WINDOWS\system32\xpsp2res.dll	0x012F0000	0x002C5000
C:\WINDOWS\system32\WINHTTP.dll	0x4D4F0000	0x00059000
C:\WINDOWS\system32\netapi32.dll	0x5B860000	0x00055000
C:\WINDOWS\system32\COMCTL32.dll	0x5D090000	0x0009A000
C:\WINDOWS\system32\hnetcfg.dll	0x662B0000	0x00058000
C:\WINDOWS\system32\mswsock.dll	0x71A50000	0x0003F000
C:\WINDOWS\System32\wshtcpip.dll	0x71A90000	0x00008000
C:\WINDOWS\system32\WS2HELP.dll	0x71AA0000	0x00008000
C:\WINDOWS\system32\ws2_32.dll	0x71AB0000	0x00017000
C:\WINDOWS\system32\MSCTF.dll	0x74720000	0x0004C000
C:\WINDOWS\system32\MSIMG32.dll	0x76380000	0x00005000
C:\WINDOWS\system32\COMDLG32.dll	0x763B0000	0x00049000
C:\WINDOWS\system32\USERENV.dll	0x769C0000	0x000B4000
C:\WINDOWS\system32\Winmm.dll	0x76B40000	0x0002D000
C:\WINDOWS\system32\PSAPI.DLL	0x76BF0000	0x0000B000
C:\WINDOWS\system32\DNSAPI.dll	0x76F20000	0x00027000
C:\WINDOWS\system32\rasadhlp.dll	0x76FC0000	0x00006000
C:\WINDOWS\system32\CLBCATQ.DLL	0x76FD0000	0x0007F000
C:\WINDOWS\system32\COMRes.dll	0x77050000	0x000C5000
C:\WINDOWS\system32\OLEAUT32.dll	0x77120000	0x0008B000

Run-time Dlls

Module Name	Base Address	Size
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\SETUPAPI.dll	0x77920000	0x000F3000
C:\WINDOWS\system32\VERSION.dll	0x77C00000	0x00008000
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
C:\WINDOWS\system32\urlmon.dll	0x7E1E0000	0x000A2000
C:\WINDOWS\system32\SXS.DLL	0x7E720000	0x000B0000

6.a) hhdtdvkc.exe - Registry Activities

Registry Values Modified:

Key	Name	New Value
HKLM\Software\Microsoft\Windows\CurrentVersion\Explorer\Shell Folders	Common Desktop	C:\Documents and Settings\All Users\Desktop
HKLM\Software\Microsoft\Windows\CurrentVersion\Explorer\Shell Folders	Common Documents	C:\Documents and Settings\All Users\Documents
HKU\S-1-5-21-842925246-1425521274-308236825-500\Software\Microsoft\Windows\CurrentVersion\Explorer\MountPoints2\{a1094da8-30a0-11dd-817b-806d6172696f}\	BaseClass	Drive
HKU\S-1-5-21-842925246-1425521274-308236825-500\Software\Microsoft\Windows\CurrentVersion\Explorer\MountPoints2\{a1094daa-30a0-11dd-817b-806d6172696f}\	BaseClass	Drive
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	Desktop	C:\Documents and Settings\Administrator\Desktop
HKU\S-1-5-21-842925246-1425521274-308236825-500\Software\Microsoft\Windows\CurrentVersion\Explorer\Shell Folders	Personal	C:\Documents and Settings\Administrator\My Documents
HKU\S-1-5-21-842925246-1425521274-308236825-500\Software\Microsoft\Windows\CurrentVersion\Internet Settings\ZoneMap\	IntranetName	1
HKU\S-1-5-21-842925246-1425521274-308236825-500\Software\Microsoft\Windows\CurrentVersion\Internet Settings\ZoneMap\	ProxyBypass	1
HKU\S-1-5-21-842925246-1425521274-308236825-500\Software\Microsoft\Windows\CurrentVersion\Internet Settings\ZoneMap\	UNCAsIntranet	1

Registry Values Read:

Key	Name	Value	Times
HKLM\SOFTWARE\CLASSES\.ASP		aspfile	1
HKLM\SOFTWARE\CLASSES\.BAT		batfile	1
HKLM\SOFTWARE\CLASSES\.CER		CERFile	1
HKLM\SOFTWARE\CLASSES\.CHM		chm.file	1
HKLM\SOFTWARE\CLASSES\.CMD		cmdfile	1
HKLM\SOFTWARE\CLASSES\.COM		comfile	1
HKLM\SOFTWARE\CLASSES\.CPL		cplfile	1
HKLM\SOFTWARE\CLASSES\.CRT		CERFile	1
HKLM\SOFTWARE\CLASSES\.EXE		exefile	3
HKLM\SOFTWARE\CLASSES\CLSID\{00020420-0000-0000-C000-000000000046}\INPROCSERVER32		oleaut32.dll	1
HKLM\SOFTWARE\CLASSES\CLSID\{00020420-0000-0000-C000-000000000046}\INPROCSERVER32	ThreadingModel	Both	1

Registry Values Read:

Key	Name	Value	Times
HKLM\SOFTWARE\CLASSES\CLSID\{00020424-0000-0000-C000-000000000046}\INPROCSERVER32		oleaut32.dll	1
HKLM\SOFTWARE\CLASSES\CLSID\{00020424-0000-0000-C000-000000000046}\INPROCSERVER32	ThreadingModel	Both	1
HKLM\SOFTWARE\CLASSES\CLSID\{20D04FE0-3AEA-1069-A2D8-08002B30309D}\INPROCSERVER32		%SystemRoot%\system32\SHELL32.dll	1
HKLM\SOFTWARE\CLASSES\CLSID\{7B8A2D94-0AC9-11D1-896C-00C04FB6BFC4}\INPROCSERVER32		C:\WINDOWS\system32\urlmon.dll	2
HKLM\SOFTWARE\CLASSES\CLSID\{7B8A2D94-0AC9-11D1-896C-00C04FB6BFC4}\INPROCSERVER32	ThreadingModel	Both	1
HKLM\SOFTWARE\CLASSES\CLSID\{9BA05972-F6A8-11CF-A442-00A0C90A8F39}\INPROCSERVER32		%SystemRoot%\system32\shdocvw.dll	1
HKLM\SOFTWARE\CLASSES\CLSID\{AEB6717E-7E19-11D0-97EE-00C04FD91972}\INPROCSERVER32		shell32.dll	1
HKLM\SOFTWARE\CLASSES\CLSID\{B196B286-BAB4-101A-B69C-00AA00341D07}\INPROCSERVER32		oleaut32.dll	1
HKLM\SOFTWARE\CLASSES\CLSID\{B196B286-BAB4-101A-B69C-00AA00341D07}\INPROCSERVER32	ThreadingModel	Both	1
HKLM\SOFTWARE\CLASSES\DIRECTORY	AlwaysShowExt		1
HKLM\SOFTWARE\CLASSES\DRIVE\SHELLEX\FOLDEREXTENSIONS\{FBEB8A05-BEEE-4442-804E-409D6C4515E9}	DriveMask	32	1
HKLM\SOFTWARE\CLASSES\INTERFACE\{00020400-0000-0000-C000-000000000046}\PROXYSTUBCLSID32		{00020420-0000-0000-C000-000000000046}	1
HKLM\SOFTWARE\CLASSES\INTERFACE\{85CB6900-4D95-11CF-960C-0080C7F4EE85}\PROXYSTUBCLSID32		{00020424-0000-0000-C000-000000000046}	3
HKLM\SOFTWARE\CLASSES\INTERFACE\{85CB6900-4D95-11CF-960C-0080C7F4EE85}\TYPELIB		{EAB22AC0-30C1-11CF-A7EB-0000C05BAE0B}	2
HKLM\SOFTWARE\CLASSES\INTERFACE\{85CB6900-4D95-11CF-960C-0080C7F4EE85}\TYPELIB	Version	1.1	2
HKLM\SOFTWARE\CLASSES\INTERFACE\{B196B284-BAB4-101A-B69C-00AA00341D07}\PROXYSTUBCLSID32		{B196B286-BAB4-101A-B69C-00AA00341D07}	1
HKLM\SOFTWARE\CLASSES\INTERFACE\{B196B286-BAB4-101A-B69C-00AA00341D07}\PROXYSTUBCLSID32		{B196B286-BAB4-101A-B69C-00AA00341D07}	1
HKLM\SOFTWARE\CLASSES\TYPELIB\{00020430-0000-0000-C000-000000000046}\2.0\0\WIN32		C:\WINDOWS\system32\stdole2.tlb	1
HKLM\SOFTWARE\CLASSES\TYPELIB\{EAB22AC0-30C1-11CF-A7EB-0000C05BAE0B}\1.1\0\WIN32		C:\WINDOWS\system32\shdocvw.dll	2
HKLM\SOFTWARE\Microsoft\CTF\SystemShared\	CUAS	0	1
HKLM\SOFTWARE\Microsoft\Internet Explorer	Version	6.0.2900.5512	8
HKLM\SYSTEM\CurrentControlSet\Control\Session Manager	CriticalSectionTimeout	2592000	1
HKLM\SYSTEM\CurrentControlSet\Services\Winsock\Parameters	Transports	0x5400630070006900700000004e0065007 7400420049004f0053000000000000	2
HKLM\SYSTEM\Setup	OsLoaderPath	\	2
HKLM\SYSTEM\Setup	SystemPartition	\Device\HarddiskVolume1	2
HKLM\SYSTEM\Setup	SystemSetupInProgres	0	1
HKLM\Software\Microsoft\COM3	Com+Enabled	1	2
HKLM\Software\Microsoft\COM3	REGDBVersion	0x0b00000000000000	10
HKLM\Software\Microsoft\Internet Explorer\Main\FeatureControl\FEATURE_BEHAVIORS	*	1	1

Registry Values Read:

Key	Name	Value	Times
HKLM\Software\Microsoft\Internet Explorer\Main\FeatureControl\FEATURE_DISABLE_MK_PROTOCOL	*	1	1
HKLM\Software\Microsoft\Windows NT\CurrentVersion\ProfileList	AllUsersProfile	All Users	2
HKLM\Software\Microsoft\Windows NT\CurrentVersion\ProfileList	ProfilesDirectory	%SystemDrive%\Documents and Settings	2
HKLM\Software\Microsoft\Windows\CurrentVersion	DevicePath	%SystemRoot%\inf	1
HKLM\Software\Microsoft\Windows\CurrentVersion\Explorer\ShellExecuteHooks	{AEB6717E-7E19-11d(		1
HKLM\Software\Microsoft\Windows\CurrentVersion\Explorer\User Shell Folders	Common Desktop	%ALLUSERSPROFILE%\Desktop	1
HKLM\Software\Microsoft\Windows\CurrentVersion\Explorer\User Shell Folders	Common Documents	%ALLUSERSPROFILE%\Documents	1
HKLM\Software\Microsoft\Windows\CurrentVersion\Setup	DriverCachePath	%SystemRoot%\Driver Cache	2
HKLM\Software\Microsoft\Windows\CurrentVersion\Setup	LogLevel	0	2
HKLM\Software\Microsoft\Windows\CurrentVersion\Setup	ServicePackCachePatł	c:\windows\ServicePackFiles\ServicePackCache	2
HKLM\Software\Microsoft\Windows\CurrentVersion\Setup	ServicePackSourcePat	D:\	2
HKLM\Software\Microsoft\Windows\CurrentVersion\Setup	SourcePath	D:\	2
HKLM\Software\Policies\Microsoft\Windows\Safer\CodeIdentifiers	TransparentEnabled	1	2
HKLM\System\CurrentControlSet\Control\ComputerName\ActiveComputerName	ComputerName	PC	3
HKLM\System\CurrentControlSet\Control\MediaProperties\PrivateProperties\Joystick\Winmm	wheel	1	1
HKLM\System\CurrentControlSet\Control\ProductOptions	ProductType	WinNT	1
HKLM\System\CurrentControlSet\Services\Tcpip\Parameters	Domain		3
HKLM\System\CurrentControlSet\Services\Tcpip\Parameters	Hostname	pc	3
HKLM\System\CurrentControlSet\Services\Tcpip\Parameters	UseDomainNameDevo	0	1
HKLM\System\CurrentControlSet\Services\Tcpip\Parameters\Winsock	HelperDllName	%SystemRoot%\System32\wshtcpip.dll	1
HKLM\System\CurrentControlSet\Services\Tcpip\Parameters\Winsock	Mapping	0x0b0000000300000002000000010000000 0600000002000000010000000000	1
HKLM\System\CurrentControlSet\Services\Tcpip\Parameters\Winsock	MaxSockaddrLength	16	1
HKLM\System\CurrentControlSet\Services\Tcpip\Parameters\Winsock	MinSockaddrLength	16	1
HKLM\System\CurrentControlSet\Services\Tcpip\Parameters\Winsock	UseDelayedAcceptanc	0	1
HKLM\System\CurrentControlSet\Services\WinSock2\Parameters	WinSock_Registry_Ver	2.0	4
HKLM\System\CurrentControlSet\Services\WinSock2\Parameters\NameSpace_Catalog5	Num_Catalog_Entries	3	1
HKLM\System\CurrentControlSet\Services\WinSock2\Parameters\NameSpace_Catalog5	Serial_Access_Num	4	2
HKLM\System\CurrentControlSet\Services\WinSock2\Parameters\NameSpace_Catalog5\Catalog_Entries\000000000001	DisplayString	Tcpip	4
HKLM\System\CurrentControlSet\Services\WinSock2\Parameters\NameSpace_Catalog5\Catalog_Entries\000000000001	Enabled	1	1
HKLM\System\CurrentControlSet\Services\WinSock2\Parameters\NameSpace_Catalog5\Catalog_Entries\000000000001	LibraryPath	%SystemRoot%\System32\mswsock.dll	2
HKLM\System\CurrentControlSet\Services\WinSock2\Parameters\NameSpace_Catalog5\Catalog_Entries\000000000001	ProviderId	0x409d05229e7ecf11ae5a00aa00a7112b	1
HKLM\System\CurrentControlSet\Services\WinSock2\Parameters\NameSpace_Catalog5\Catalog_Entries\000000000001	StoresServiceClassInfc	0	1

Registry Values Read:

Key	Name	Value	Times
HKLM\System\CurrentControlSet\Services\WinSock2\Parameters\NameSpace_Catalog5\Catalog_Entries\000000000001	SupportedNameSpace	12	1
HKLM\System\CurrentControlSet\Services\WinSock2\Parameters\NameSpace_Catalog5\Catalog_Entries\000000000001	Version	0	1
HKLM\System\CurrentControlSet\Services\WinSock2\Parameters\NameSpace_Catalog5\Catalog_Entries\000000000002	DisplayString	NTDS	4
HKLM\System\CurrentControlSet\Services\WinSock2\Parameters\NameSpace_Catalog5\Catalog_Entries\000000000002	Enabled	1	1
HKLM\System\CurrentControlSet\Services\WinSock2\Parameters\NameSpace_Catalog5\Catalog_Entries\000000000002	LibraryPath	%SystemRoot%\System32\winrnr.dll	2
HKLM\System\CurrentControlSet\Services\WinSock2\Parameters\NameSpace_Catalog5\Catalog_Entries\000000000002	ProviderId	0xee37263b80e5cf11a55500c04fd8d4ac	1
HKLM\System\CurrentControlSet\Services\WinSock2\Parameters\NameSpace_Catalog5\Catalog_Entries\000000000002	StoresServiceClassInfo	0	1
HKLM\System\CurrentControlSet\Services\WinSock2\Parameters\NameSpace_Catalog5\Catalog_Entries\000000000002	SupportedNameSpace	32	1
HKLM\System\CurrentControlSet\Services\WinSock2\Parameters\NameSpace_Catalog5\Catalog_Entries\000000000002	Version	0	1
HKLM\System\CurrentControlSet\Services\WinSock2\Parameters\NameSpace_Catalog5\Catalog_Entries\000000000003	DisplayString	Network Location Awareness (NLA) Namespace	4
HKLM\System\CurrentControlSet\Services\WinSock2\Parameters\NameSpace_Catalog5\Catalog_Entries\000000000003	Enabled	1	1
HKLM\System\CurrentControlSet\Services\WinSock2\Parameters\NameSpace_Catalog5\Catalog_Entries\000000000003	LibraryPath	%SystemRoot%\System32\mswsock.dll	2
HKLM\System\CurrentControlSet\Services\WinSock2\Parameters\NameSpace_Catalog5\Catalog_Entries\000000000003	ProviderId	0x3a244266a83ba64abaa52e0bd71fdd83	1
HKLM\System\CurrentControlSet\Services\WinSock2\Parameters\NameSpace_Catalog5\Catalog_Entries\000000000003	StoresServiceClassInfo	0	1
HKLM\System\CurrentControlSet\Services\WinSock2\Parameters\NameSpace_Catalog5\Catalog_Entries\000000000003	SupportedNameSpace	15	1
HKLM\System\CurrentControlSet\Services\WinSock2\Parameters\NameSpace_Catalog5\Catalog_Entries\000000000003	Version	0	1
HKLM\System\CurrentControlSet\Services\WinSock2\Parameters\Protocol_Catalog9	Next_Catalog_Entry_ID	1020	1
HKLM\System\CurrentControlSet\Services\WinSock2\Parameters\Protocol_Catalog9	Num_Catalog_Entries	13	1
HKLM\System\CurrentControlSet\Services\WinSock2\Parameters\Protocol_Catalog9	Serial_Access_Num	6	2
HKLM\System\CurrentControlSet\Services\WinSock2\Parameters\Protocol_Catalog9\Catalog_Entries\000000000001	PackedCatalogItem	%SystemRoot%\system32\mswsock.	1
HKLM\System\CurrentControlSet\Services\WinSock2\Parameters\Protocol_Catalog9\Catalog_Entries\000000000002	PackedCatalogItem	%SystemRoot%\system32\mswsock.	1
HKLM\System\CurrentControlSet\Services\WinSock2\Parameters\Protocol_Catalog9\Catalog_Entries\000000000003	PackedCatalogItem	%SystemRoot%\system32\mswsock.	1
HKLM\System\CurrentControlSet\Services\WinSock2\Parameters\Protocol_Catalog9\Catalog_Entries\000000000004	PackedCatalogItem	%SystemRoot%\system32\rsvpsp.d	1

Registry Values Read:

Key	Name	Value	Times
HKLM\System\CurrentControlSet\Services\WinSock2\Parameters\Protocol_Catalog9\Catalog_Entries\000000000005	PackedCatalogItem	%SystemRoot%\system32\rsvpsp.d	1
HKLM\System\CurrentControlSet\Services\WinSock2\Parameters\Protocol_Catalog9\Catalog_Entries\000000000006	PackedCatalogItem	%SystemRoot%\system32\mswsock.	1
HKLM\System\CurrentControlSet\Services\WinSock2\Parameters\Protocol_Catalog9\Catalog_Entries\000000000007	PackedCatalogItem	%SystemRoot%\system32\mswsock.	1
HKLM\System\CurrentControlSet\Services\WinSock2\Parameters\Protocol_Catalog9\Catalog_Entries\000000000008	PackedCatalogItem	%SystemRoot%\system32\mswsock.	1
HKLM\System\CurrentControlSet\Services\WinSock2\Parameters\Protocol_Catalog9\Catalog_Entries\000000000009	PackedCatalogItem	%SystemRoot%\system32\mswsock.	1
HKLM\System\CurrentControlSet\Services\WinSock2\Parameters\Protocol_Catalog9\Catalog_Entries\000000000010	PackedCatalogItem	%SystemRoot%\system32\mswsock.	1
HKLM\System\CurrentControlSet\Services\WinSock2\Parameters\Protocol_Catalog9\Catalog_Entries\000000000011	PackedCatalogItem	%SystemRoot%\system32\mswsock.	1
HKLM\System\CurrentControlSet\Services\WinSock2\Parameters\Protocol_Catalog9\Catalog_Entries\000000000012	PackedCatalogItem	%SystemRoot%\system32\mswsock.	1
HKLM\System\CurrentControlSet\Services\WinSock2\Parameters\Protocol_Catalog9\Catalog_Entries\000000000013	PackedCatalogItem	%SystemRoot%\system32\mswsock.	1
HKLM\System\Setup	SystemSetupInProgres	0	3
HKLM\System\WPA\PnP	seed	1274198464	1
HKU\S-1-5-21-842925246-1425521274-308236825-500\Keyboard Layout\Toggle	Language Hotkey	1	2
HKU\S-1-5-21-842925246-1425521274-308236825-500\Keyboard Layout\Toggle	Layout Hotkey	2	2
HKU\S-1-5-21-842925246-1425521274-308236825-500\Software\Microsoft\Windows\CurrentVersion\Explorer\	ShellState	0x24000000380800000000000000000000000000000010000000d0000000000	2
HKU\S-1-5-21-842925246-1425521274-308236825-500\Software\Microsoft\Windows\CurrentVersion\Explorer\Advanced	DontPrettyPath	0	1
HKU\S-1-5-21-842925246-1425521274-308236825-500\Software\Microsoft\Windows\CurrentVersion\Explorer\Advanced	Filter	0	1
HKU\S-1-5-21-842925246-1425521274-308236825-500\Software\Microsoft\Windows\CurrentVersion\Explorer\Advanced	Hidden	1	1
HKU\S-1-5-21-842925246-1425521274-308236825-500\Software\Microsoft\Windows\CurrentVersion\Explorer\Advanced	HideFileExt	0	1
HKU\S-1-5-21-842925246-1425521274-308236825-500\Software\Microsoft\Windows\CurrentVersion\Explorer\Advanced	HideIcons	0	1
HKU\S-1-5-21-842925246-1425521274-308236825-500\Software\Microsoft\Windows\CurrentVersion\Explorer\Advanced	MapNetDrvBtn	0	1
HKU\S-1-5-21-842925246-1425521274-308236825-500\Software\Microsoft\Windows\CurrentVersion\Explorer\Advanced	NoNetCrawling	1	1
HKU\S-1-5-21-842925246-1425521274-308236825-500\Software\Microsoft\Windows\CurrentVersion\Explorer\Advanced	SeparateProcess	0	1
HKU\S-1-5-21-842925246-1425521274-308236825-500\Software\Microsoft\Windows\CurrentVersion\Explorer\Advanced	ShowCompColor	1	1
HKU\S-1-5-21-842925246-1425521274-308236825-500\Software\Microsoft\Windows\CurrentVersion\Explorer\Advanced	ShowInfoTip	1	1

Registry Values Read:

Key	Name	Value	Times
HKU\S-1-5-21-842925246-1425521274-308236825-500\Software\Microsoft\Windows\CurrentVersion\Explorer\Advanced	ShowSuperHidden	1	1
HKU\S-1-5-21-842925246-1425521274-308236825-500\Software\Microsoft\Windows\CurrentVersion\Explorer\Advanced	WebView	0	1
HKU\S-1-5-21-842925246-1425521274-308236825-500\Software\Microsoft\Windows\CurrentVersion\Explorer\MountPoints2\CPC\Volume\{a1094da8-30a0-11dd-817b-806d6172696f}\	Data	0x000000005c005c003f005c004900440044500230043006400520006f006d00	1
HKU\S-1-5-21-842925246-1425521274-308236825-500\Software\Microsoft\Windows\CurrentVersion\Explorer\MountPoints2\CPC\Volume\{a1094da8-30a0-11dd-817b-806d6172696f}\	Generation	1	1
HKU\S-1-5-21-842925246-1425521274-308236825-500\Software\Microsoft\Windows\CurrentVersion\Explorer\MountPoints2\CPC\Volume\{a1094daa-30a0-11dd-817b-806d6172696f}\	Data	0x000000005c005c003f005c005300540044f00520041004700450023005600	1
HKU\S-1-5-21-842925246-1425521274-308236825-500\Software\Microsoft\Windows\CurrentVersion\Explorer\MountPoints2\CPC\Volume\{a1094daa-30a0-11dd-817b-806d6172696f}\	Generation	1	5
HKU\S-1-5-21-842925246-1425521274-308236825-500\Software\Microsoft\Windows\CurrentVersion\Explorer\User Shell Folders	Cache	%USERPROFILE%\Local Settings\Temporary Internet Files	1
HKU\S-1-5-21-842925246-1425521274-308236825-500\Software\Microsoft\Windows\CurrentVersion\Explorer\User Shell Folders	Cookies	%USERPROFILE%\Cookies	1
HKU\S-1-5-21-842925246-1425521274-308236825-500\Software\Microsoft\Windows\CurrentVersion\Explorer\User Shell Folders	Desktop	%USERPROFILE%\Desktop	1
HKU\S-1-5-21-842925246-1425521274-308236825-500\Software\Microsoft\Windows\CurrentVersion\Explorer\User Shell Folders	Local Settings	%USERPROFILE%\Local Settings	1
HKU\S-1-5-21-842925246-1425521274-308236825-500\Software\Microsoft\Windows\CurrentVersion\Explorer\User Shell Folders	Personal	%USERPROFILE%\My Documents	2
HKU\S-1-5-21-842925246-1425521274-308236825-500\Software\Microsoft\Windows\CurrentVersion\Internet Settings\Zones\0	1806	0	1
HKU\S-1-5-21-842925246-1425521274-308236825-500\Software\Microsoft\Windows\CurrentVersion\Internet Settings\Zones\0	Flags	33	2
HKU\S-1-5-21-842925246-1425521274-308236825-500\Software\Microsoft\Windows\CurrentVersion\Internet Settings\Zones\1	Flags	219	2
HKU\S-1-5-21-842925246-1425521274-308236825-500\Software\Microsoft\Windows\CurrentVersion\Internet Settings\Zones\2	Flags	71	2
HKU\S-1-5-21-842925246-1425521274-308236825-500\Software\Microsoft\Windows\CurrentVersion\Internet Settings\Zones\3	Flags	1	2
HKU\S-1-5-21-842925246-1425521274-308236825-500\Software\Microsoft\Windows\CurrentVersion\Internet Settings\Zones\4	Flags	3	2

Monitored Registry Keys:

Key Name	Watch subtree	Notify Filter	Count
HKLM\Software\Classes	1	Key Change,Value Change	3
HKLM\Software\Classes\CLSID	1	Key Change,Value Change	2
HKLM\Software\Microsoft\COM3	1	Key Change,Value Change	6
HKLM\System\CurrentControlSet\Services\WinSock2\Parameters\NameSpace_Catalog5	0	Key Change	1
HKLM\System\CurrentControlSet\Services\WinSock2\Parameters\Protocol_Catalog9	0	Key Change	1

Monitored Registry Keys:

Key Name	Watch subtree	Notify Filter	Count
HKU	1	Key Change,Value Change	3

6.b) hhdtdvkc.exe - File Activities

Files Created:

C:\DOCUME~1\ADMINI~1\LOCALS~1\Temp\6e5edb2dda4421f5.exe

Files Read:

C:\Documents and Settings\Administrator\Local Settings\Application Data\hhdtdvkc.exe
C:\Documents and Settings\Administrator\My Documents\desktop.ini
C:\Documents and Settings\All Users\Documents\desktop.ini
C:\WINDOWS\Registration\R00000000000b.clb
C:\WINDOWS\system32\shdocvw.dll
C:\WINDOWS\system32\stdole2.tlb
PIPE\lsarpc
PIPE\wkssvc

Files Modified:

C:\DOCUME~1\ADMINI~1\LOCALS~1\Temp\6e5edb2dda4421f5.exe
MountPointManager
PIPE\lsarpc
PIPE\wkssvc
\Device\Afd\AsyncConnectHlp
\Device\Afd\Endpoint
\Device\RasAcd

File System Control Communication:

File	Control Code	Times
C:\Program Files\Common Files	0x00090028	1
PIPE\lsarpc	0x0011C017	24
PIPE\wkssvc	0x0011C017	1

Device Control Communication:

File	Control Code	Times
\Device\KsecDD	0x00390008	8
\Device\Afd\Endpoint	AFD_GET_INFO (0x0001207B)	2
\Device\Afd\Endpoint	AFD_SET_CONTEXT (0x00012047)	14
\Device\Afd\Endpoint	AFD_BIND (0x00012003)	2
\Device\Afd\Endpoint	AFD_GET_TDI_HAND (0x00012037)	4
\Device\Afd\Endpoint	AFD_GET_SOCK_NAI (0x0001202F)	2
\Device\Afd\Endpoint	AFD_SET_INFO (0x0001203B)	10
\Device\Afd\AsyncConnectHlp	AFD_CONNECT (0x00012007)	2
\Device\Afd\Endpoint	AFD_SELECT (0x00012024)	2
unnamed file	0x00120028	2
\Device\Afd\Endpoint	AFD_SEND (0x0001201F)	2
\Device\Afd\Endpoint	AFD_RECV (0x00012017)	39

Device Control Communication:

File	Control Code	Times
HKLM\Software\Classes\CLSID\{B196B286-BAB4-101A-B69C-00AA00341D07}	0x00120028	2
IDE#CdRomQEMU_QEMU_CD-ROM_______________________0.9.____#4d5130303030203320202020202020200202020#{53f5630d-b6bf-11d0-94f2-00a0c91efb8b}	0x004D0008	1
MountPointManager	0x006D0008	2
STORAGE#Volume#1&30a96598&0&SignatureB15FB15FOffset7E00Length13F2918000#{53f5630d-b6bf-11d0-94f2-00a0c91efb8b}	0x004D0008	1
MountPointManager	0x006D0034	4

Memory Mapped Files:

File Name
C:\WINDOWS\System32\wshtcpip.dll
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\CLBCATQ.DLL
C:\WINDOWS\system32\COMCTL32.dll
C:\WINDOWS\system32\COMRes.dll
C:\WINDOWS\system32\DNSAPI.dll
C:\WINDOWS\system32\MSCTF.dll
C:\WINDOWS\system32\MSIMG32.dll
C:\WINDOWS\system32\PSAPI.DLL
C:\WINDOWS\system32\SETUPAPI.dll
C:\WINDOWS\system32\SHELL32.dll
C:\WINDOWS\system32\SXS.DLL
C:\WINDOWS\system32\WINHTTP.dll
C:\WINDOWS\system32\WS2HELP.dll
C:\WINDOWS\system32\Winmm.dll
C:\WINDOWS\system32\hnetcfg.dll
C:\WINDOWS\system32\imm32.dll
C:\WINDOWS\system32\mswsock.dll
C:\WINDOWS\system32\rasadhlp.dll
C:\WINDOWS\system32\rpcss.dll
C:\WINDOWS\system32\shdocvw.dll
C:\WINDOWS\system32\stdole2.tlb
C:\WINDOWS\system32\urlmon.dll
C:\WINDOWS\system32\winlogon.exe
C:\WINDOWS\system32\ws2_32.dll
C:\WINDOWS\system32\xpsp2res.dll

6.c) hhdtdvkc.exe - Network Activity

DNS Queries:

Name	Query Type	Query Result	Successful	Protocol
fihjh.ibbuhnw.tk	DNS_TYPE_A	5.104.106.56	YES	udp

HTTP Conversations:

From ANUBIS:1031 to 175.41.29.179:80 - [175.41.29.179]
Request: GET /api/urls/?ts=aecf5081&affid=70300
Response: 200 "OK"
From ANUBIS:1032 to 5.104.106.56:80 - [fihjh.ibbuhnw.tk]
Request: GET /update.exe?ts=aecf5081&affid=7030
Response: 200 "OK"

6.d) hhdtdvkc.exe - Other Activities

Mutexes Created:
69D5070F3703E373000069D49D40E9C3
CTF.Asm.MutexDefaultS-1-5-21-842925246-1425521274-308236825-500
CTF.Compart.MutexDefaultS-1-5-21-842925246-1425521274-308236825-500
CTF.LBES.MutexDefaultS-1-5-21-842925246-1425521274-308236825-500
CTF.Layouts.MutexDefaultS-1-5-21-842925246-1425521274-308236825-500
CTF.TMD.MutexDefaultS-1-5-21-842925246-1425521274-308236825-500
CTF.TimListCache.FMPDefaultS-1-5-21-842925246-1425521274-308236825-500MUTEX.DefaultS-1-5-21-842925246-1425521274-308236825-500
ZonesCacheCounterMutex
ZonesCounterMutex
ZonesLockedCacheCounterMutex

Windows SEH exceptions:

Description	Times
Exception 0xc0000005 (STATUS_ACCESS_VIOLATION) at 0x40a650	1
Exception 0xc000001d (STATUS_ILLEGAL_INSTRUCTION) at 0x43b32e	1
Exception 0xc000001d (STATUS_ILLEGAL_INSTRUCTION) at 0x43b675	1
Exception 0xc0000096 (STATUS_PRIVILEGED_INSTRUCTION) at 0x43b3d6	1