Anubis - Analysis Report

Analysis Report for [tvN]_____.E02.130712.HDTV.H264.720p-WITH.mp4.torrent.exe

MD5: 948c2abdd3d4dbea3f689432a31c33ce

International Secure Systems Lab
Vienna University of Technology , Eurecom France , UC Santa Barbara
Contact: anubis@iseclab.org

Dependency overview:

- **[tvN]_____.exe** C:\[tvN]_____.exe
  Analysis reason: Primary Analysis Subject
  - **server.exe** C:\Program Files\server.exe
    Analysis reason: Started by [tvN]_____.exe
    - **net.exe** C:\WINDOWS\system32\net.exe
      Analysis reason: Started by server.exe
      - **net1.exe** C:\WINDOWS\system32\net1.exe
        Analysis reason: Started by net.exe
        - **services.exe** C:\WINDOWS\system32\services.exe
          Analysis reason: A service was started.
  - **rundll32.exe** C:\WINDOWS\system32\rundll32.exe
    Analysis reason: Started by [tvN]_____.exe

Table of Contents:

1. General Information

Information about Anubis' invocation	
Time needed:	249 s
Report created:	07/12/13, 14:15:18 UTC
Termination reason:	Timeout
Program version:	1.76.3886

2. [tvN]_____.exe

General information about this executable	
Analysis Reason:	Primary Analysis Subject
Filename:	[tvN]_____.exe
MD5:	948c2abdd3d4dbea3f689432a31c33ce
SHA-1:	bb58fa729d6157d758468d6f07530d5d7566b584
File Size:	422570
Command Line:	"C:\[tvN]_____.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\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\ADVAPI32.dll	0x77DD0000	0x0009B000
C:\WINDOWS\system32\RPCRT4.dll	0x77E70000	0x00092000
C:\WINDOWS\system32\Secur32.dll	0x77FE0000	0x00011000
C:\WINDOWS\system32\GDI32.dll	0x77F10000	0x00049000
C:\WINDOWS\system32\USER32.dll	0x7E410000	0x00091000
C:\WINDOWS\system32\SHLWAPI.dll	0x77F60000	0x00076000
C:\WINDOWS\system32\COMDLG32.dll	0x763B0000	0x00049000
C:\WINDOWS\system32\SHELL32.dll	0x7C9C0000	0x00817000
C:\WINDOWS\system32\ole32.dll	0x774E0000	0x0013D000
C:\WINDOWS\system32\OLEAUT32.dll	0x77120000	0x0008B000

Run-time Dlls

Module Name	Base Address	Size
C:\WINDOWS\system32\UxTheme.dll	0x5AD70000	0x00038000
C:\WINDOWS\system32\netapi32.dll	0x5B860000	0x00055000
C:\WINDOWS\system32\riched32.dll	0x732E0000	0x00005000
C:\WINDOWS\system32\MSCTF.dll	0x74720000	0x0004C000
C:\WINDOWS\system32\RICHED20.dll	0x74E30000	0x0006D000
C:\WINDOWS\system32\CRYPTUI.dll	0x754D0000	0x00080000
C:\WINDOWS\system32\browseui.dll	0x75F80000	0x000FD000
C:\WINDOWS\system32\WINTRUST.dll	0x76C30000	0x0002E000
C:\WINDOWS\system32\IMAGEHLP.dll	0x76C90000	0x00028000
C:\WINDOWS\system32\WLDAP32.dll	0x76F60000	0x0002C000
C:\WINDOWS\system32\CLBCATQ.DLL	0x76FD0000	0x0007F000
C:\WINDOWS\system32\COMRes.dll	0x77050000	0x000C5000
C:\WINDOWS\system32\WININET.dll	0x771B0000	0x000AA000
C:\WINDOWS\system32\SETUPAPI.dll	0x77920000	0x000F3000
C:\WINDOWS\system32\CRYPT32.dll	0x77A80000	0x00095000
C:\WINDOWS\system32\MSASN1.dll	0x77B20000	0x00012000
C:\WINDOWS\system32\Apphelp.dll	0x77B40000	0x00022000

Run-time Dlls

Module Name	Base Address	Size
C:\WINDOWS\system32\VERSION.dll	0x77C00000	0x00008000
C:\WINDOWS\system32\urlmon.dll	0x7E1E0000	0x000A2000
C:\WINDOWS\system32\SHDOCVW.dll	0x7E290000	0x00171000

2.a) [tvN]_____.exe - Registry Activities

Registry Keys Created:

HKU\S-1-5-21-842925246-1425521274-308236825-500\Software\WinRAR SFX

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
HKU\S-1-5-21-842925246-1425521274-308236825-500\Software\Microsoft\Windows\ShellNoRoam\MUICache\	C:\Program Files\server.exe	
HKU\S-1-5-21-842925246-1425521274-308236825-500\Software\Microsoft\Windows\ShellNoRoam\MUICache\	C:\WINDOWS\system32\shell32.dll	Windows Shell Common Dll
HKU\S-1-5-21-842925246-1425521274-308236825-500\Software\WinRAR SFX	C%%Program Files	C:\Program Files

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\{00BB2763-6A77-11D0-A535-00C04FD7D062}\INPROCSERVER32		%SystemRoot%\system32\browseui.dll	2
HKLM\SOFTWARE\CLASSES\CLSID\{00BB2763-6A77-11D0-A535-00C04FD7D062}\INPROCSERVER32	ThreadingModel	Apartment	1

Registry Values Read:

Key	Name	Value	Times
HKLM\SOFTWARE\CLASSES\CLSID\{00BB2765-6A77-11D0-A535-00C04FD7D062}\INPROCSERVER32		%SystemRoot%\system32\browseui.dll	1
HKLM\SOFTWARE\CLASSES\CLSID\{00BB2765-6A77-11D0-A535-00C04FD7D062}\INPROCSERVER32	ThreadingModel	Apartment	1
HKLM\SOFTWARE\CLASSES\CLSID\{03C036F1-A186-11D0-824A-00AA005B4383}\INPROCSERVER32		%SystemRoot%\system32\browseui.dll	2
HKLM\SOFTWARE\CLASSES\CLSID\{03C036F1-A186-11D0-824A-00AA005B4383}\INPROCSERVER32	ThreadingModel	Apartment	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	3
HKLM\SOFTWARE\CLASSES\CLSID\{7B8A2D94-0AC9-11D1-896C-00C04FB6BFC4}\INPROCSERVER32	ThreadingModel	Both	1
HKLM\SOFTWARE\CLASSES\CLSID\{AEB6717E-7E19-11D0-97EE-00C04FD91972}\INPROCSERVER32		shell32.dll	2
HKLM\SOFTWARE\CLASSES\CLSID\{DD313E04-FEFF-11D1-8ECD-0000F87A470C}\INPROCSERVER32		%SystemRoot%\system32\browseui.dll	3
HKLM\SOFTWARE\CLASSES\CLSID\{DD313E04-FEFF-11D1-8ECD-0000F87A470C}\INPROCSERVER32	ThreadingModel	Both	1
HKLM\SOFTWARE\CLASSES\DIRECTORY	AlwaysShowExt		1
HKLM\SOFTWARE\CLASSES\DRIVE\SHELLEX\FOLDEREXTENSIONS\{FBEB8A05-BEEE-4442-804E-409D6C4515E9}	DriveMask	32	2
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\UNKNOWN\SHELL		openas	2
HKLM\SOFTWARE\CLASSES\UNKNOWN\SHELL\OPENAS\COMMAND		%SystemRoot%\system32\rundll32.exe %SystemRoot%\system32\shell32.dll,OpenAs_RunDLL %1	3
HKLM\SOFTWARE\Microsoft\CTF\SystemShared\	CUAS	0	1
HKLM\SYSTEM\CurrentControlSet\Control\Session Manager	CriticalSectionTimeout	2592000	1
HKLM\SYSTEM\Setup	OsLoaderPath	\	2
HKLM\SYSTEM\Setup	SystemPartition	\Device\HarddiskVolume1	2
HKLM\SYSTEM\Setup	SystemSetupInProgres	0	1
HKLM\SYSTEM\WPA\MediaCenter	Installed	0	2
HKLM\Software\Microsoft\COM3	Com+Enabled	1	2
HKLM\Software\Microsoft\COM3	REGDBVersion	0x0b00000000000000	14
HKLM\Software\Microsoft\Internet Explorer\Main\FeatureControl\FEATURE_BEHAVIORS	*	1	1
HKLM\Software\Microsoft\Internet Explorer\Main\FeatureControl\FEATURE_DISABLE_MK_PROTOCOL	*	1	1

Registry Values Read:

Key	Name	Value	Times
HKLM\Software\Microsoft\Windows NT\CurrentVersion\Windows	AppInit_DLLs		1
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	0x4100700070006c0069006300610074006669006f006e002000460069006c00	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	0x4100440045000000410044005000000042004100530000004200410053000000420041005400	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

Registry Values Read:

Key	Name	Value	Times
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
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\Terminal Server	TSAppCompat	0	1
HKLM\System\CurrentControlSet\Services\LDAP	LdapClientIntegrity	1	1
HKLM\System\CurrentControlSet\Services\Tcpip\Parameters	Domain		1
HKLM\System\CurrentControlSet\Services\Tcpip\Parameters	Hostname	pc	1
HKLM\System\Setup	SystemSetupInProgres	0	2
HKLM\System\WPA\PnP	seed	1274198464	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\Windows\CurrentVersion\Explorer\	ShellState	0x240000003808000000000000000000000000000000000010000000d0000000000	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

Registry Values Read:

Key	Name	Value	Times
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	5
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
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	Personal	%USERPROFILE%\My Documents	1
HKU\S-1-5-21-842925246-1425521274-308236825-500\Software\Microsoft\Windows\CurrentVersion\Explorer\\\UserAssist\{5E6AB780-7743-11CF-A12B-00AA004AE837}	Version	3	1
HKU\S-1-5-21-842925246-1425521274-308236825-500\Software\Microsoft\Windows\CurrentVersion\Explorer\\\UserAssist\{5E6AB780-7743-11CF-A12B-00AA004AE837}\Count	HRZR_PGYFRFFVBA	0x967c5e0e06000000	1
HKU\S-1-5-21-842925246-1425521274-308236825-500\Software\Microsoft\Windows\CurrentVersion\Explorer\\\UserAssist\{75048700-EF1F-11D0-9888-006097DEACF9}	Version	3	1
HKU\S-1-5-21-842925246-1425521274-308236825-500\Software\Microsoft\Windows\CurrentVersion\Explorer\\\UserAssist\{75048700-EF1F-11D0-9888-006097DEACF9}\Count	HRZR_PGYFRFFVBA	0xe57b5e0e05000000	1
HKU\S-1-5-21-842925246-1425521274-308236825-500\Software\Microsoft\Windows\CurrentVersion\Internet Settings\Zones\0	1806	0	1

Registry Values Read:

Key	Name	Value	Times
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
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\Explorer\Advanced	ListviewAlphaSelect	0	1
HKU\S-1-5-21-842925246-1425521274-308236825-500\software\Microsoft\Windows\CurrentVersion\Explorer\Advanced	ListviewShadow	0	1
HKU\S-1-5-21-842925246-1425521274-308236825-500\software\Microsoft\Windows\CurrentVersion\Explorer\Advanced	ListviewWatermark	1	1

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
HKU	1	Key Change,Value Change	5

2.b) [tvN]_____.exe - File Activities

Files Deleted:

C:\Program Files__tmp_rar_sfx_access_check_414171

Files Created:

C:\Program Files\2ne1.torrent
C:\Program Files__tmp_rar_sfx_access_check_414171
C:\Program Files\server.exe

Files Read:

C:\Documents and Settings\Administrator\My Documents\desktop.ini
C:\Documents and Settings\All Users\Documents\desktop.ini
C:\Program Files\server.exe
C:\WINDOWS\Registration\R00000000000b.clb
C:\WINDOWS\system32\rundll32.exe
C:\WINDOWS\win.ini
C:\[tvN]_____.exe
PIPE\lsarpc
PIPE\wkssvc

Files Modified:

C:\Program Files\2ne1.torrent
C:\Program Files\server.exe

Files Modified:
MountPointManager
PIPE\lsarpc
PIPE\wkssvc

File System Control Communication:

File	Control Code	Times
C:\Program Files\Common Files\	0x00090028	1
PIPE\wkssvc	0x0011C017	1
PIPE\lsarpc	0x0011C017	6

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

Memory Mapped Files:

File Name
C:\Program Files\server.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\Apphelp.dll
C:\WINDOWS\system32\CLBCATQ.DLL
C:\WINDOWS\system32\COMRes.dll
C:\WINDOWS\system32\MSCTF.dll
C:\WINDOWS\system32\RICHED20.dll
C:\WINDOWS\system32\SETUPAPI.dll
C:\WINDOWS\system32\SHDOCVW.dll
C:\WINDOWS\system32\SHELL32.dll
C:\WINDOWS\system32\UxTheme.dll
C:\WINDOWS\system32\WININET.dll
C:\WINDOWS\system32\browseui.dll
C:\WINDOWS\system32\imm32.dll
C:\WINDOWS\system32\riched32.dll
C:\WINDOWS\system32\rpcss.dll
C:\WINDOWS\system32\rundll32.exe
C:\WINDOWS\system32\urlmon.dll
C:\Windows\AppPatch\sysmain.sdb

2.c) [tvN]_____.exe - Process Activities

Processes Created:

Executable	Command Line
C:\Program Files\server.exe	
C:\Program Files\server.exe	"C:\Program Files\server.exe"
C:\WINDOWS\system32\rundll32.exe	
C:\WINDOWS\system32\rundll32.exe	"C:\WINDOWS\system32\rundll32.exe" C:\WINDOWS\system32\shell32.dll,OpenAs_RunDLL C:\Program Files\2ne1.torrent

Remote Threads Created:
Affected Process
C:\Program Files\server.exe
C:\WINDOWS\system32\rundll32.exe

Foreign Memory Regions Read:
Process: C:\Program Files\server.exe
Process: C:\WINDOWS\system32\rundll32.exe

Foreign Memory Regions Written:
Process: C:\Program Files\server.exe
Process: C:\WINDOWS\system32\rundll32.exe

2.d) [tvN]_____.exe - Other Activities

Mutexes Created:
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
MSCTF.Shared.MUTEX.IFG
ZonesCacheCounterMutex
ZonesCounterMutex
ZonesLockedCacheCounterMutex
_SHuassist.mtx

Keyboard Keys Monitored:	
Virtual Key Code	**Times**
VK_ESCAPE (27)	23
VK_SHIFT (16)	1

3. server.exe

General information about this executable	
Analysis Reason:	Started by [tvN]_____.exe
Filename:	server.exe
Command Line:	"C:\Program Files\server.exe"
Process-status at analysis end:	alive
Exit Code:	0

Load-time Dlls		
Module Name	**Base Address**	**Size**
C:\WINDOWS\system32\ntdll.dll	0x7C900000	0x000AF000
C:\WINDOWS\system32\kernel32.dll	0x7C800000	0x000F6000
C:\WINDOWS\system32\MSVCRT.dll	0x77C10000	0x00058000

Run-time Dlls		
Module Name	**Base Address**	**Size**
C:\WINDOWS\WinSxS\ x86_Microsoft.Windows.GdiPlus_6595b64144ccf1df_1.0.2600.5512_x-ww_dfb54e0c\ GDIPLUS.DLL	0x4EC50000	0x001A6000
C:\WINDOWS\system32\NETAPI32.DLL	0x5B860000	0x00055000
C:\WINDOWS\system32\hnetcfg.dll	0x662B0000	0x00058000

Run-time Dlls

Module Name	Base Address	Size
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\wsock32.dll	0x71AD0000	0x00009000
C:\WINDOWS\system32\sensapi.dll	0x722B0000	0x00005000
C:\WINDOWS\system32\AVICAP32.DLL	0x73B80000	0x00012000
C:\WINDOWS\system32\MSCTF.dll	0x74720000	0x0004C000
C:\WINDOWS\system32\MSVFW32.dll	0x75A70000	0x00021000
C:\WINDOWS\system32\MSVCP60.DLL	0x76080000	0x00065000
C:\WINDOWS\system32\WINSTA.dll	0x76360000	0x00010000
C:\WINDOWS\system32\USERENV.dll	0x769C0000	0x000B4000
C:\WINDOWS\system32\WINMM.dll	0x76B40000	0x0002D000
C:\WINDOWS\system32\PSAPI.DLL	0x76BF0000	0x0000B000
C:\WINDOWS\system32\IPHLPAPI.DLL	0x76D60000	0x00019000
C:\WINDOWS\system32\rtutils.dll	0x76E80000	0x0000E000
C:\WINDOWS\system32\rasman.dll	0x76E90000	0x00012000
C:\WINDOWS\system32\TAPI32.dll	0x76EB0000	0x0002F000
C:\WINDOWS\system32\RASAPI32.DLL	0x76EE0000	0x0003C000
C:\WINDOWS\system32\DNSAPI.dll	0x76F20000	0x00027000
C:\WINDOWS\system32\WTSAPI32.DLL	0x76F50000	0x00008000
C:\WINDOWS\system32\WLDAP32.dll	0x76F60000	0x0002C000
C:\WINDOWS\System32\winrnr.dll	0x76FB0000	0x00008000
C:\WINDOWS\system32\rasadhlp.dll	0x76FC0000	0x00006000
C:\WINDOWS\system32\OLEAUT32.DLL	0x77120000	0x0008B000
C:\WINDOWS\system32\WININET.DLL	0x771B0000	0x000AA000
C:\WINDOWS\WinSxS\x86_Microsoft.Windows.Common-Controls_6595b64144ccf1df_6.0.2600.5512_x-ww_35d4ce83\comctl32.dll	0x773D0000	0x00103000
C:\WINDOWS\system32\OLE32.DLL	0x774E0000	0x0013D000
C:\WINDOWS\system32\SETUPAPI.DLL	0x77920000	0x000F3000
C:\WINDOWS\system32\CRYPT32.dll	0x77A80000	0x00095000
C:\WINDOWS\system32\MSASN1.dll	0x77B20000	0x00012000
C:\WINDOWS\system32\Apphelp.dll	0x77B40000	0x00022000
C:\WINDOWS\system32\VERSION.dll	0x77C00000	0x00008000
C:\WINDOWS\system32\msv1_0.dll	0x77C70000	0x00024000
C:\WINDOWS\system32\ADVAPI32.DLL	0x77DD0000	0x0009B000
C:\WINDOWS\system32\RPCRT4.dll	0x77E70000	0x00092000
C:\WINDOWS\system32\GDI32.dll	0x77F10000	0x00049000
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\USER32.DLL	0x7E410000	0x00091000

3.a) server.exe - Registry Activities

Registry Keys Created:

HKLM\SYSTEM\CurrentControlSet\Control\MediaResources\msvideo
HKLM\SYSTEM\InfoTime

Registry Values Modified:

Key	Name	New Value
HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Run	281F20BE	C:\WINDOWS\281F20BE\svchsot.exe
HKLM\SYSTEM\CURRENTCONTROLSET\HARDWARE PROFILES\CURRENT\Software\Microsoft\windows\CurrentVersion\Internet Settings	ProxyEnable	0

Registry Values Modified:

Key	Name	New Value
HKLM\SYSTEM\InfoTime	InfoTime	20110302
HKLM\Software\Microsoft\Windows\CurrentVersion\Explorer\Shell Folders	Common AppData	C:\Documents and Settings\All Users\Application Data
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	AppData	C:\Documents and Settings\Administrator\Application Data
HKU\S-1-5-21-842925246-1425521274-308236825-500\Software\Microsoft\Windows\CurrentVersion\Explorer\Shell Folders	Cache	C:\Documents and Settings\Administrator\Local Settings\Temporary Internet Files
HKU\S-1-5-21-842925246-1425521274-308236825-500\Software\Microsoft\Windows\CurrentVersion\Explorer\Shell Folders	Cookies	C:\Documents and Settings\Administrator\Cookies
HKU\S-1-5-21-842925246-1425521274-308236825-500\Software\Microsoft\Windows\CurrentVersion\Explorer\Shell Folders	History	C:\Documents and Settings\Administrator\Local Settings\History
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\CurrentVersion\Internet Settings	MigrateProxy	1
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	0x3c000000160000000100000000000000000000000000000000000040000000000

Registry Values Read:

Key	Name	Value	Times
HKLM\HARDWARE\DESCRIPTION\System\CentralProcessor\0	~MHz	2992	1
HKLM\SOFTWARE\CLASSES\CLSID\{20D04FE0-3AEA-1069-A2D8-08002B30309D}\INPROCSERVER32		%SystemRoot%\system32\SHELL32.dll	1

Registry Values Read:

Key	Name	Value	Times
HKLM\SOFTWARE\CLASSES\DRIVE\SHELLEX\FOLDEREXTENSIONS\{FBEB8A05-BEEE-4442-804E-409D6C4515E9}	DriveMask	32	2
HKLM\SOFTWARE\Microsoft\CTF\SystemShared\	CUAS	0	1
HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion	ProductName	Microsoft Windows XP	2
HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Internet Settings	UrlEncoding	0x00000000	2
HKLM\SYSTEM\CurrentControlSet\Control\Session Manager	CriticalSectionTimeout	2592000	1
HKLM\SYSTEM\CurrentControlSet\Services\Winsock\Parameters	Transports	0x5400630070006900700000004e0065007 7400420049004f00530000000000	2
HKLM\SYSTEM\InfoTime	InfoTime	20110302	4
HKLM\SYSTEM\Setup	OsLoaderPath	\	2
HKLM\SYSTEM\Setup	SystemPartition	\Device\HarddiskVolume1	2
HKLM\SYSTEM\Setup	SystemSetupInProgres	0	1
HKLM\SYSTEM\WPA\MediaCenter	Installed	0	1
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\Rpc\SecurityService	10	secur32.dll	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\ProfileList	AllUsersProfile	All Users	2
HKLM\Software\Microsoft\Windows NT\CurrentVersion\ProfileList	DefaultUserProfile	Default User	2
HKLM\Software\Microsoft\Windows NT\CurrentVersion\ProfileList	ProfilesDirectory	%SystemDrive%\Documents and Settings	4
HKLM\Software\Microsoft\Windows NT\CurrentVersion\ProfileList\S-1-5-21-842925246-1425521274-308236825-500	ProfileImagePath	%SystemDrive%\Documents and Settings\Administrator	2
HKLM\Software\Microsoft\Windows NT\CurrentVersion\Windows	AppInit_DLLs		1
HKLM\Software\Microsoft\Windows\CurrentVersion	CommonFilesDir	C:\Program Files\Common Files	2
HKLM\Software\Microsoft\Windows\CurrentVersion	DevicePath	%SystemRoot%\inf	1
HKLM\Software\Microsoft\Windows\CurrentVersion	ProgramFilesDir	C:\Program Files	2
HKLM\Software\Microsoft\Windows\CurrentVersion\Explorer\User Shell Folders	Common AppData	%ALLUSERSPROFILE%\Application Data	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	PolicyScope	0	1
HKLM\Software\Policies\Microsoft\Windows\Safer\CodeIdentifiers	TransparentEnabled	1	2

Registry Values Read:

Key	Name	Value	Times
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
HKLM\Software\Policies\Microsoft\Windows\Safer\CodeIdentifiers\0\Paths\{dda3f824-d8cb-441b-834d-be2efd2c1a33}	SaferFlags	0	1

Registry Values Read:

Key	Name	Value	Times
HKLM\System\CurrentControlSet\Control\ComputerName\ActiveComputerName	ComputerName	PC	4
HKLM\System\CurrentControlSet\Control\Lsa\SspiCache\digest.dll	Capabilities	16464	1
HKLM\System\CurrentControlSet\Control\Lsa\SspiCache\digest.dll	Comment	Digest SSPI Authentication Package	2
HKLM\System\CurrentControlSet\Control\Lsa\SspiCache\digest.dll	Name	Digest	2
HKLM\System\CurrentControlSet\Control\Lsa\SspiCache\digest.dll	RpcId	65535	1
HKLM\System\CurrentControlSet\Control\Lsa\SspiCache\digest.dll	TokenSize	65535	1
HKLM\System\CurrentControlSet\Control\Lsa\SspiCache\digest.dll	Type	49	1
HKLM\System\CurrentControlSet\Control\Lsa\SspiCache\digest.dll	Version	1	1
HKLM\System\CurrentControlSet\Control\Lsa\SspiCache\msapsspc.dll	Capabilities	55	1
HKLM\System\CurrentControlSet\Control\Lsa\SspiCache\msapsspc.dll	Comment	DPA Security Package	2
HKLM\System\CurrentControlSet\Control\Lsa\SspiCache\msapsspc.dll	Name	DPA	2
HKLM\System\CurrentControlSet\Control\Lsa\SspiCache\msapsspc.dll	RpcId	17	1
HKLM\System\CurrentControlSet\Control\Lsa\SspiCache\msapsspc.dll	TokenSize	768	1
HKLM\System\CurrentControlSet\Control\Lsa\SspiCache\msapsspc.dll	Type	49	1
HKLM\System\CurrentControlSet\Control\Lsa\SspiCache\msapsspc.dll	Version	1	1
HKLM\System\CurrentControlSet\Control\Lsa\SspiCache\msnsspc.dll	Capabilities	55	1
HKLM\System\CurrentControlSet\Control\Lsa\SspiCache\msnsspc.dll	Comment	MSN Security Package	2
HKLM\System\CurrentControlSet\Control\Lsa\SspiCache\msnsspc.dll	Name	MSN	2
HKLM\System\CurrentControlSet\Control\Lsa\SspiCache\msnsspc.dll	RpcId	18	1
HKLM\System\CurrentControlSet\Control\Lsa\SspiCache\msnsspc.dll	TokenSize	768	1
HKLM\System\CurrentControlSet\Control\Lsa\SspiCache\msnsspc.dll	Type	49	1
HKLM\System\CurrentControlSet\Control\Lsa\SspiCache\msnsspc.dll	Version	1	1
HKLM\System\CurrentControlSet\Control\MediaProperties\PrivateProperties\Joystick\Winmm	wheel	1	1
HKLM\System\CurrentControlSet\Control\ProductOptions	ProductType	WinNT	1
HKLM\System\CurrentControlSet\Control\SecurityProviders	SecurityProviders	msapsspc.dll, schannel.dll, digest.dll, msnsspc.dll	2
HKLM\System\CurrentControlSet\Control\SecurityProviders\SaslProfiles	GSSAPI	Kerberos	1
HKLM\System\CurrentControlSet\Control\Session Manager\Environment	ComSpec	%SystemRoot%\system32\cmd.exe	4
HKLM\System\CurrentControlSet\Control\Session Manager\Environment	FP_NO_HOST_CHEC	NO	4
HKLM\System\CurrentControlSet\Control\Session Manager\Environment	NUMBER_OF_PROCE	1	4
HKLM\System\CurrentControlSet\Control\Session Manager\Environment	OS	Windows_NT	4
HKLM\System\CurrentControlSet\Control\Session Manager\Environment	PATHEXT	.COM;.EXE;.BAT;.CMD;.VBS;.VBE;.JS;.JSE;.WSF;.WSH	4
HKLM\System\CurrentControlSet\Control\Session Manager\Environment	PROCESSOR_ARCHI	x86	4

Registry Values Read:

Key	Name	Value	Times
HKLM\System\CurrentControlSet\Control\Session Manager\Environment	PROCESSOR_IDENTI	x86 Family 6 Model 3 Stepping 3, GenuineIntel	4
HKLM\System\CurrentControlSet\Control\Session Manager\Environment	PROCESSOR_LEVEL	6	4
HKLM\System\CurrentControlSet\Control\Session Manager\Environment	PROCESSOR_REVISI	0303	4
HKLM\System\CurrentControlSet\Control\Session Manager\Environment	Path	%SystemRoot%\system32;%SystemRoot%; %SystemRoot%\System32\Wbem	4
HKLM\System\CurrentControlSet\Control\Session Manager\Environment	TEMP	%SystemRoot%\TEMP	4
HKLM\System\CurrentControlSet\Control\Session Manager\Environment	TMP	%SystemRoot%\TEMP	4
HKLM\System\CurrentControlSet\Control\Session Manager\Environment	windir	%SystemRoot%	4
HKLM\System\CurrentControlSet\Control\Terminal Server	TSAppCompat	0	3
HKLM\System\CurrentControlSet\Control\Terminal Server	TSUserEnabled	0	1
HKLM\System\CurrentControlSet\Services\LDAP	LdapClientIntegrity	1	1
HKLM\System\CurrentControlSet\Services\Tcpip\ Parameters	Domain		5
HKLM\System\CurrentControlSet\Services\Tcpip\ Parameters	Hostname	pc	5
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	0x0b000000030000000200000001000000006000000020000000100000000000	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	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

Registry Values Read:

Key	Name	Value	Times
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
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

Registry Values Read:

Key	Name	Value	Times
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\Environment	TEMP	%USERPROFILE%\Local Settings\Temp	4
HKU\S-1-5-21-842925246-1425521274-308236825-500\Environment	TMP	%USERPROFILE%\Local Settings\Temp	4
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	WarnOnPost	0x01000000	1
HKU\S-1-5-21-842925246-1425521274-308236825-500\Software\Microsoft\Windows NT\CurrentVersion\Winlogon	ParseAutoexec	1	2
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	2
HKU\S-1-5-21-842925246-1425521274-308236825-500\Software\Microsoft\Windows\CurrentVersion\Explorer\MountPoints2\CPC\Volume\{a1094daa-30a0-11dd-817b-806d6172696f}\	Data	0x000000005c005c003f005c00530054004 4f005200410047004500230056 00	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	2
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
HKU\S-1-5-21-842925246-1425521274-308236825-500\Software\Microsoft\Windows\CurrentVersion\Explorer\User Shell Folders	AppData	%USERPROFILE%\Application Data	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	History	%USERPROFILE%\Local Settings\History	3
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\Internet Settings\5.0\Cache	Signature	Client UrlCache MMF Ver 5.2	2
HKU\S-1-5-21-842925246-1425521274-308236825-500\Software\Microsoft\Windows\CurrentVersion\Internet Settings\5.0\Cache\Content	CacheLimit	163410	1
HKU\S-1-5-21-842925246-1425521274-308236825-500\Software\Microsoft\Windows\CurrentVersion\Internet Settings\5.0\Cache\Content	CachePrefix		2
HKU\S-1-5-21-842925246-1425521274-308236825-500\Software\Microsoft\Windows\CurrentVersion\Internet Settings\5.0\Cache\Content	PerUserItem	1	1
HKU\S-1-5-21-842925246-1425521274-308236825-500\Software\Microsoft\Windows\CurrentVersion\Internet Settings\5.0\Cache\Cookies	CacheLimit	8192	1
HKU\S-1-5-21-842925246-1425521274-308236825-500\Software\Microsoft\Windows\CurrentVersion\Internet Settings\5.0\Cache\Cookies	CachePrefix	Cookie:	2
HKU\S-1-5-21-842925246-1425521274-308236825-500\Software\Microsoft\Windows\CurrentVersion\Internet Settings\5.0\Cache\Cookies	PerUserItem	1	1
HKU\S-1-5-21-842925246-1425521274-308236825-500\Software\Microsoft\Windows\CurrentVersion\Internet Settings\5.0\Cache\Extensible Cache\MSHist012011021720110218	CacheLimit	8192	1
HKU\S-1-5-21-842925246-1425521274-308236825-500\Software\Microsoft\Windows\CurrentVersion\Internet Settings\5.0\Cache\Extensible Cache\MSHist012011021720110218	CacheOptions	11	1
HKU\S-1-5-21-842925246-1425521274-308236825-500\Software\Microsoft\Windows\CurrentVersion\Internet Settings\5.0\Cache\Extensible Cache\MSHist012011021720110218	CachePath	%USERPROFILE%\Local Settings\History\History.IE5\MSHist012011021720110218\	2
HKU\S-1-5-21-842925246-1425521274-308236825-500\Software\Microsoft\Windows\CurrentVersion\Internet Settings\5.0\Cache\Extensible Cache\MSHist012011021720110218	CachePrefix	:2011021720110218:	2
HKU\S-1-5-21-842925246-1425521274-308236825-500\Software\Microsoft\Windows\CurrentVersion\Internet Settings\5.0\Cache\Extensible Cache\MSHist012011021720110218	CacheRepair	0	1
HKU\S-1-5-21-842925246-1425521274-308236825-500\Software\Microsoft\Windows\CurrentVersion\Internet Settings\5.0\Cache\Extensible Cache\MSHist012011021820110219	CacheLimit	8192	1
HKU\S-1-5-21-842925246-1425521274-308236825-500\Software\Microsoft\Windows\CurrentVersion\Internet Settings\5.0\Cache\Extensible Cache\MSHist012011021820110219	CacheOptions	11	1
HKU\S-1-5-21-842925246-1425521274-308236825-500\Software\Microsoft\Windows\CurrentVersion\Internet Settings\5.0\Cache\Extensible Cache\MSHist012011021820110219	CachePath	%USERPROFILE%\Local Settings\History\History.IE5\MSHist012011021820110219\	2

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	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	1
HKU\S-1-5-21-842925246-1425521274-308236825-500\Software\Microsoft\Windows\CurrentVersion\Internet Settings\ZoneMap\\ProtocolDefaults\	http	3	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\Internet Settings	MigrateProxy	1	1
HKU\S-1-5-21-842925246-1425521274-308236825-500\Software\Microsoft\windows\CurrentVersion\Internet Settings	ProxyEnable	0	1
HKU\S-1-5-21-842925246-1425521274-308236825-500\Software\Microsoft\windows\CurrentVersion\Internet Settings\Connections	DefaultConnectionSetti	0x3c000000300000001000000000000000000000000000000000000000040000000000	2
HKU\S-1-5-21-842925246-1425521274-308236825-500\Software\Microsoft\windows\CurrentVersion\Internet Settings\Connections	SavedLegacySettings	0x3c000000150000000100000000000000000000000000000000000000040000000000	4
HKU\S-1-5-21-842925246-1425521274-308236825-500\Volatile Environment	APPDATA	C:\Documents and Settings\Administrator\Application Data	4
HKU\S-1-5-21-842925246-1425521274-308236825-500\Volatile Environment	CLIENTNAME	Console	4
HKU\S-1-5-21-842925246-1425521274-308236825-500\Volatile Environment	HOMEDRIVE	C:	4
HKU\S-1-5-21-842925246-1425521274-308236825-500\Volatile Environment	HOMEPATH	\Documents and Settings\Administrator	4
HKU\S-1-5-21-842925246-1425521274-308236825-500\Volatile Environment	HOMESHARE		4
HKU\S-1-5-21-842925246-1425521274-308236825-500\Volatile Environment	LOGONSERVER	\\PC	4

Registry Values Read:

Key	Name	Value	Times
HKU\S-1-5-21-842925246-1425521274-308236825-500\Volatile Environment	SESSIONNAME	Console	4

Monitored Registry Keys:

Key Name	Watch subtree	Notify Filter	Count
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

3.b) server.exe - File Activities

Files Created:

C:\WINDOWS\281F20BE
C:\WINDOWS\281F20BE\svchsot.exe

Files Read:

PIPE\atsvc
PIPE\lsarpc
c:\autoexec.bat

Files Modified:

C:\WINDOWS\281F20BE\svchsot.exe
Ip
MountPointManager
PIPE\atsvc
PIPE\lsarpc
\Device\Afd\Endpoint
\Device\Ip
\Device\RasAcd
\Device\Tcp

Directories Created:

C:\WINDOWS\281F20BE

File System Control Communication:

File	Control Code	Times
C:\Program Files	0x00090028	1
PIPE\lsarpc	0x0011C017	106
PIPE\atsvc	0x0011C017	26

Device Control Communication:

File	Control Code	Times
\Device\KsecDD	0x00390008	8
\Device\Tcp	0x00120003	6
\Device\Afd\Endpoint	AFD_GET_INFO (0x0001207B)	2
\Device\Afd\Endpoint	AFD_SET_CONTEXT (0x00012047)	15
\Device\RasAcd	0x00F14014	2
\Device\Afd\Endpoint	AFD_BIND (0x00012003)	3

Device Control Communication:

File	Control Code	Times
\Device\Afd\Endpoint	AFD_GET_TDI_HAND (0x00012037)	6
\Device\Afd\Endpoint	AFD_CONNECT (0x00012007)	3
unnamed file	0x00120028	5
\Device\Afd\Endpoint	AFD_DISCONNECT (0x0001202B)	1
\Device\Afd\Endpoint	AFD_SELECT (0x00012024)	2
\Device\Afd\Endpoint	AFD_GET_SOCK_NAI (0x0001202F)	2
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\Afd\Endpoint	AFD_SEND (0x0001201F)	2
\Device\Afd\Endpoint	AFD_RECV (0x00012017)	2

Memory Mapped Files:

File Name
C:\Program Files\server.exe
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\WinSxS\x86_Microsoft.Windows.GdiPlus_6595b64144ccf1df_1.0.2600.5512_x-ww_dfb54e0c\GDIPLUS.DLL
C:\WINDOWS\WindowsShell.Manifest
C:\WINDOWS\system32\AVICAP32.DLL
C:\WINDOWS\system32\Apphelp.dll
C:\WINDOWS\system32\DNSAPI.dll
C:\WINDOWS\system32\IPHLPAPI.DLL
C:\WINDOWS\system32\MSCTF.dll
C:\WINDOWS\system32\MSVCP60.DLL
C:\WINDOWS\system32\MSVFW32.dll
C:\WINDOWS\system32\PSAPI.DLL
C:\WINDOWS\system32\RASAPI32.DLL
C:\WINDOWS\system32\SETUPAPI.DLL
C:\WINDOWS\system32\SHELL32.DLL
C:\WINDOWS\system32\TAPI32.dll
C:\WINDOWS\system32\URLMON.DLL
C:\WINDOWS\system32\WININET.DLL
C:\WINDOWS\system32\WINMM.dll
C:\WINDOWS\system32\WINSTA.dll
C:\WINDOWS\system32\WS2HELP.dll
C:\WINDOWS\system32\WS2_32.DLL
C:\WINDOWS\system32\WTSAPI32.DLL
C:\WINDOWS\system32\hnetcfg.dll
C:\WINDOWS\system32\imm32.dll
C:\WINDOWS\system32\msv1_0.dll
C:\WINDOWS\system32\mswsock.dll
C:\WINDOWS\system32\net.exe
C:\WINDOWS\system32\rasadhlp.dll
C:\WINDOWS\system32\rasman.dll
C:\WINDOWS\system32\rtutils.dll

Memory Mapped Files:

File Name
C:\WINDOWS\system32\sensapi.dll
C:\WINDOWS\system32\wsock32.dll
C:\Windows\AppPatch\sysmain.sdb

3.c) server.exe - Process Activities

Processes Created:

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

Remote Threads Created:

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

Foreign Memory Regions Read:

Process: C:\WINDOWS\system32\net.exe

Foreign Memory Regions Written:

Process: C:\WINDOWS\system32\net.exe

3.d) server.exe - Network Activity

DNS Queries:

Name	Query Type	Query Result	Successful	Protocol
0712.1276592227.tk	DNS_TYPE_A	199.114.246.121	YES	udp

HTTP Conversations:

From ANUBIS:1030 to 192.169.109.2:80 - [192.169.109.2]

Request: GET /0711.exe

Response: 200 "OK"

Unknown TCP Traffic:

From ANUBIS:1029 to 199.114.246.121:2012

State: Connection established, not terminated - Transferred outbound Bytes: 135 - Transferred inbound Bytes: 55

Data sent:

```
3030 3030 3030 3030 8700 0000 6001 0000    00000000....`...
789c 4b63 6060 9803 c4ac 40cc 08c4 1a5c    x.Kc``....@....\
0c0c 4c40 3a38 b5a8 2c33 3955 2120 3139    ..L@:8..,39U! 19
5bc1 9881 ee80 1944 3032 326c e086 b8eb    [......D022l....
c00a 06a6 8264 c2fa 9e00 15d7 0369 633d    .....d.......ic=
7353 7cea 5c52 d312 4b73 4af0 9aa5 ab8b    sS|.\R..KsJ.....
2926 01c4 2c0c 1037 ddbb 6dc4 6864 6068    )&..,..7..m.hd`h
a86b 60ac 6b60 a46f 686a 6564 6465 6481    .k`.k`.ohjedded.
a21e 00d3 a614 11                          .......
```

Data received:

```
0000 0000 0000                             ......
```

Data received:

```
3030 3030 3030 3030 3700 0000 1f00 0000    000000007.......
789c cbc8 2829 29b0 d2d7 37b4 34d2 3334    x...())...7.4.34
b3d4 3334 b0d4 33d2 3730 3734 d44b ad48    ..34..3.7074.K.H
6500 0085 9e07 bb                          e.......
```

TCP Connection Attempts:

From ANUBIS:1028 to 199.114.246.121:2012

3.e) server.exe - Other Activities

Mutexes Created:
0712.1276592227.tk:2012127.0.0.1:2012127.0.0.1:2012
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
ZonesCacheCounterMutex
ZonesCounterMutex
ZonesLockedCacheCounterMutex

Windows SEH exceptions:	
Description	**Times**
Exception 0xc000001d (STATUS_ILLEGAL_INSTRUCTION) at 0x100026c9	1
Exception 0xc0000096 (STATUS_PRIVILEGED_INSTRUCTION) at 0x10002768	1
Exception 0xc0000005 (STATUS_ACCESS_VIOLATION) at 0x7c80bea7	2

4. rundll32.exe

General information about this executable	
Analysis Reason:	Started by [tvN]_____.exe
Filename:	rundll32.exe
MD5:	037b1e7798960e0420003d05bb577ee6
SHA-1:	303a90020bf3beaf9acd0ea86487c853636a99a3
File Size:	33280
Command Line:	"C:\WINDOWS\system32\rundll32.exe" C:\WINDOWS\system32\shell32.dll,OpenAs_RunDLL C:\Program Files\2ne1.torrent
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\msvcrt.dll	0x77C10000	0x00058000
C:\WINDOWS\system32\GDI32.dll	0x77F10000	0x00049000
C:\WINDOWS\system32\USER32.dll	0x7E410000	0x00091000
C:\WINDOWS\system32\IMAGEHLP.dll	0x76C90000	0x00028000
C:\WINDOWS\system32\ShimEng.dll	0x5CB70000	0x00026000
C:\WINDOWS\AppPatch\AcGenral.DLL	0x6F880000	0x001CA000
C:\WINDOWS\system32\ADVAPI32.dll	0x77DD0000	0x0009B000
C:\WINDOWS\system32\RPCRT4.dll	0x77E70000	0x00092000
C:\WINDOWS\system32\Secur32.dll	0x77FE0000	0x00011000
C:\WINDOWS\system32\WINMM.dll	0x76B40000	0x0002D000
C:\WINDOWS\system32\ole32.dll	0x774E0000	0x0013D000
C:\WINDOWS\system32\OLEAUT32.dll	0x77120000	0x0008B000
C:\WINDOWS\system32\MSACM32.dll	0x77BE0000	0x00015000
C:\WINDOWS\system32\VERSION.dll	0x77C00000	0x00008000
C:\WINDOWS\system32\SHELL32.dll	0x7C9C0000	0x00817000
C:\WINDOWS\system32\SHLWAPI.dll	0x77F60000	0x00076000
C:\WINDOWS\system32\USERENV.dll	0x769C0000	0x000B4000
C:\WINDOWS\system32\UxTheme.dll	0x5AD70000	0x00038000

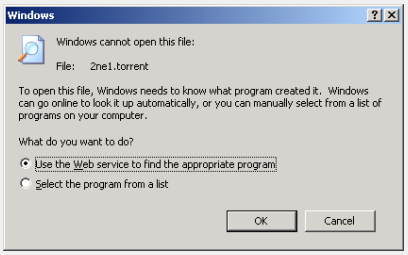
Load-time Dlls

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\comctl32.dll	0x5D090000	0x0009A000

Run-time Dlls

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

Popups

Window Name	Window Text	Screenshot	Number of Displayed Times
Windows	Windows cannot open this file: File: 2ne1.torrent To open this file, Windows needs to know what program created it. Windows can go online to look it up automatically, or you can manually select from a list of programs on your computer. What do you want to do? Use the &Web service to find the appropriate program &Select the program from a list OK Cancel		1

4.a) rundll32.exe - Registry Activities

Registry Values Read:

Key	Name	Value	Times
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	0x010000001000000002040000014000000	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	0x010000001000000011000000014000000	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	0x010000001000000055000001e000000	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	0x010000001000000002000000032000000	1
HKLM\Software\Microsoft\AudioCompressionManager\DriverCache\msacm.msadpcm	cFilterTags	0	1
HKLM\Software\Microsoft\AudioCompressionManager\DriverCache\msacm.msadpcm	cFormatTags	2	1

Registry Values Read:

Key	Name	Value	Times
HKLM\Software\Microsoft\AudioCompressionManager\DriverCache\msacm.msadpcm	fdwSupport	1	1
HKLM\Software\Microsoft\AudioCompressionManager\DriverCache\msacm.msaudio1	aFormatTagCache	0x0100000012000000600100001600000066101000001c000000	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	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	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	0x0100000010000000310000001400000	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	0x0100000010000000300100001600000	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	0x0100000010000000220000003200000	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	C:\WINDOWS\system32\iac25_32.ax	2
HKLM\Software\Microsoft\Windows NT\CurrentVersion\Drivers32	msacm.imaadpcm		3
HKLM\Software\Microsoft\Windows NT\CurrentVersion\Drivers32	msacm.l3acm		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

Registry Values Read:

Key	Name	Value	Times
HKLM\Software\Microsoft\Windows NT\CurrentVersion\Drivers32	msacm.msg723		3
HKLM\Software\Microsoft\Windows NT\CurrentVersion\Drivers32	msacm.msgsm610	msgsm32.acm	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\Windows	AppInit_DLLs		1
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
HKLM\System\CurrentControlSet\Control\Terminal Server	TSAppCompat	0	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\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

4.b) rundll32.exe - File Activities

File System Control Communication:

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

Device Control Communication:

File	Control Code	Times
\Device\KsecDD	0x00390008	8

Memory Mapped Files:

File Name
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\comctl32.dll
C:\WINDOWS\system32\imm32.dll
C:\WINDOWS\system32\rpcss.dll
C:\WINDOWS\system32\shell32.dll
C:\Windows\AppPatch\sysmain.sdb

5. net.exe

General information about this executable

Analysis Reason:	Started by server.exe
Filename:	net.exe
MD5:	fd3da8425624b98903407df608cf2c11
SHA-1:	5c7248824eef8bedf3bb7e60b9d5d4bb00d1a791
File Size:	42496
Command Line:	net start "Task Scheduler"
Process-status at analysis end:	dead
Exit Code:	2

Load-time Dlls

Module Name	Base Address	Size
C:\WINDOWS\system32\ntdll.dll	0x7C900000	0x000AF000
C:\WINDOWS\system32\kernel32.dll	0x7C800000	0x000F6000
C:\WINDOWS\system32\msvcrt.dll	0x77C10000	0x00058000
C:\WINDOWS\system32\ADVAPI32.dll	0x77DD0000	0x0009B000
C:\WINDOWS\system32\RPCRT4.dll	0x77E70000	0x00092000
C:\WINDOWS\system32\Secur32.dll	0x77FE0000	0x00011000
C:\WINDOWS\system32\NETAPI32.dll	0x5B860000	0x00055000
C:\WINDOWS\system32\MPR.dll	0x71B20000	0x00012000
C:\WINDOWS\system32\USER32.dll	0x7E410000	0x00091000
C:\WINDOWS\system32\GDI32.dll	0x77F10000	0x00049000
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

Load-time Dlls

Module Name	Base Address	Size
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

Run-time Dlls

Module Name	Base Address	Size
C:\WINDOWS\system32\Apphelp.dll	0x77B40000	0x00022000

5.a) net.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\SYSTEM\WPA\MediaCenter	Installed	0	2
HKLM\Software\Microsoft\AudioCompressionManager\DriverCache\msacm.iac2	aFormatTagCache	0x010000001000000002040000014000000	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	0x010000001000000011000000014000000	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	0x010000001000000005500000001e000000	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	0x010000001000000002000000032000000	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

Registry Values Read:

Key	Name	Value	Times
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	0x010000001000000042000000 1c000000	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	0x0100000010000000310000001 4000000	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	0x0100000010000000300100001 6000000	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	0x0100000010000000220000003 2000000	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	C:\WINDOWS\system32\iac25_32.ax	2
HKLM\Software\Microsoft\Windows NT\CurrentVersion\Drivers32	msacm.imaadpcm	imaadp32.acm	3
HKLM\Software\Microsoft\Windows NT\CurrentVersion\Drivers32	msacm.l3acm		2
HKLM\Software\Microsoft\Windows NT\CurrentVersion\Drivers32	msacm.msadpcm	msadp32.acm	3
HKLM\Software\Microsoft\Windows NT\CurrentVersion\Drivers32	msacm.msaudio1	msaud32.acm	3
HKLM\Software\Microsoft\Windows NT\CurrentVersion\Drivers32	msacm.msg711	msg711.acm	3
HKLM\Software\Microsoft\Windows NT\CurrentVersion\Drivers32	msacm.msg723	msg723.acm	3
HKLM\Software\Microsoft\Windows NT\CurrentVersion\Drivers32	msacm.msgsm610		3
HKLM\Software\Microsoft\Windows NT\CurrentVersion\Drivers32	msacm.sl_anet	sl_anet.acm	2
HKLM\Software\Microsoft\Windows NT\CurrentVersion\Drivers32	msacm.trspch		3
HKLM\Software\Microsoft\Windows NT\CurrentVersion\Drivers32	vidc.I420		2

Registry Values Read:

Key	Name	Value	Times
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\Windows	AppInit_DLLs		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

Registry Values Read:

Key	Name	Value	Times
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
HKLM\Software\Policies\Microsoft\Windows\Safer\CodeIdentifiers\0\Paths\{dda3f824-d8cb-441b-834d-be2efd2c1a33}	SaferFlags	0	1
HKLM\System\CurrentControlSet\Control\MediaProperties\PrivateProperties\Joystick\Winmm	wheel	1	1
HKLM\System\CurrentControlSet\Control\Nls\Language Groups	1	1	1
HKLM\System\CurrentControlSet\Control\Nls\Locale	00000C07	1	1
HKLM\System\CurrentControlSet\Control\ProductOptions	ProductType	WinNT	1
HKLM\System\CurrentControlSet\Control\Terminal Server	TSAppCompat	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\Shell Folders	Cache	C:\Documents and Settings\Administrator\Local Settings\Temporary Internet Files	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

Monitored Registry Keys:

Key Name	Watch subtree	Notify Filter	Count
HKLM\system\CurrentControlSet\control\NetworkProvider\HwOrder	0	Value Change	1

5.b) net.exe - File Activities

File System Control Communication:

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

Device Control Communication:

File	Control Code	Times
\Device\KsecDD	0x00390008	1

Memory Mapped Files:

File Name
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\Apphelp.dll
C:\WINDOWS\system32\MSACM32.dll
C:\WINDOWS\system32\SHELL32.dll
C:\WINDOWS\system32\ShimEng.dll
C:\WINDOWS\system32\UxTheme.dll
C:\WINDOWS\system32\WINMM.dll
C:\WINDOWS\system32\comctl32.dll
C:\WINDOWS\system32\net1.exe
C:\Windows\AppPatch\sysmain.sdb

5.c) net.exe - Process Activities

Processes Created:

Executable	Command Line
C:\WINDOWS\system32\net1.exe	
	net1 start "Task Scheduler"

Remote Threads Created:

Affected Process
C:\WINDOWS\system32\net1.exe

Foreign Memory Regions Read:

Process: C:\WINDOWS\system32\net1.exe

Foreign Memory Regions Written:

Process: C:\WINDOWS\system32\net1.exe

6. net1.exe

General information about this executable

Analysis Reason:	Started by net.exe
Filename:	net1.exe
MD5:	3f14c041342e3fba343f2a1d11e74bba
SHA-1:	4221467faee4926d692bd5ae71cf0a37f326bf42
File Size:	124928
Command Line:	net1 start "Task Scheduler"
Process-status at analysis end:	dead
Exit Code:	2

Load-time Dlls

Module Name	Base Address	Size
C:\WINDOWS\system32\ntdll.dll	0x7C900000	0x000AF000
C:\WINDOWS\system32\kernel32.dll	0x7C800000	0x000F6000
C:\WINDOWS\system32\msvcrt.dll	0x77C10000	0x00058000
C:\WINDOWS\system32\ADVAPI32.dll	0x77DD0000	0x0009B000
C:\WINDOWS\system32\RPCRT4.dll	0x77E70000	0x00092000
C:\WINDOWS\system32\Secur32.dll	0x77FE0000	0x00011000
C:\WINDOWS\system32\NETAPI32.dll	0x5B860000	0x00055000
C:\WINDOWS\system32\SAMLIB.dll	0x71BF0000	0x00013000
C:\WINDOWS\system32\USER32.dll	0x7E410000	0x00091000
C:\WINDOWS\system32\GDI32.dll	0x77F10000	0x00049000
C:\WINDOWS\system32\NTDSAPI.dll	0x767A0000	0x00013000
C:\WINDOWS\system32\DNSAPI.dll	0x76F20000	0x00027000
C:\WINDOWS\system32\WS2_32.dll	0x71AB0000	0x00017000
C:\WINDOWS\system32\WS2HELP.dll	0x71AA0000	0x00008000
C:\WINDOWS\system32\WLDAP32.dll	0x76F60000	0x0002C000
C:\WINDOWS\system32\NETRAP.dll	0x71C80000	0x00007000
C:\WINDOWS\system32\ShimEng.dll	0x5CB70000	0x00026000
C:\WINDOWS\AppPatch\AcGenral.DLL	0x6F880000	0x001CA000
C:\WINDOWS\system32\WINMM.dll	0x76B40000	0x0002D000
C:\WINDOWS\system32\ole32.dll	0x774E0000	0x0013D000
C:\WINDOWS\system32\OLEAUT32.dll	0x77120000	0x0008B000
C:\WINDOWS\system32\MSACM32.dll	0x77BE0000	0x00015000
C:\WINDOWS\system32\VERSION.dll	0x77C00000	0x00008000
C:\WINDOWS\system32\SHELL32.dll	0x7C9C0000	0x00817000
C:\WINDOWS\system32\SHLWAPI.dll	0x77F60000	0x00076000
C:\WINDOWS\system32\USERENV.dll	0x769C0000	0x000B4000
C:\WINDOWS\system32\UxTheme.dll	0x5AD70000	0x00038000
C:\WINDOWS\WinSxS\x86_Microsoft.Windows.Common-Controls_6595b64144ccf1df_6.0.2600.5512_x-ww_35d4ce83\comctl32.dll	0x773D0000	0x00103000
C:\WINDOWS\system32\comctl32.dll	0x5D090000	0x0009A000

Run-time Dlls

Module Name	Base Address	Size
C:\WINDOWS\system32\NETMSG.dll	0x71B40000	0x0002C000

6.a) net1.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\SYSTEM\WPA\MediaCenter	Installed	0	1
HKLM\Software\Microsoft\AudioCompressionManager\DriverCache\msacm.iac2	aFormatTagCache	0x0100000010000000020400001400000	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	0x0100000010000000110000001400000	1
HKLM\Software\Microsoft\AudioCompressionManager\DriverCache\msacm.imaadpcm	cFilterTags	0	1
HKLM\Software\Microsoft\AudioCompressionManager\DriverCache\msacm.imaadpcm	cFormatTags	2	1

Registry Values Read:

Key	Name	Value	Times
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	0x0100000010000000200000032000000	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	0x0100000012000000600100001600000066101000001c000000	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	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	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	0x0100000010000000310000001400000	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	0x0100000010000000300100001600000	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	0x0100000010000000220000032000000	1
HKLM\Software\Microsoft\AudioCompressionManager\DriverCache\msacm.trspch	cFilterTags	0	1
HKLM\Software\Microsoft\AudioCompressionManager\DriverCache\msacm.trspch	cFormatTags	2	1

Registry Values Read:

Key	Name	Value	Times
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	C:\WINDOWS\system32\iac25_32.ax	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		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	sl_anet.acm	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\Windows	AppInit_DLLs		1
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\Nls\Language Groups	1	1	1

Registry Values Read:

Key	Name	Value	Times
HKLM\System\CurrentControlSet\Control\Nls\Locale	00000C07	1	1
HKLM\System\CurrentControlSet\Control\ProductOptions	ProductType	WinNT	1
HKLM\System\CurrentControlSet\Control\Terminal Server	TSAppCompat	0	1
HKLM\System\CurrentControlSet\Services\LDAP	LdapClientIntegrity	1	1
HKLM\System\CurrentControlSet\Services\Tcpip\Parameters	UseDomainNameDevo	0	1
HKLM\System\Setup	SystemSetupInProgres	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\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

6.b) net1.exe - File Activities

Device Control Communication:

File	Control Code	Times
\Device\KsecDD	0x00390008	8

Memory Mapped Files:

File Name
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\DNSAPI.dll
C:\WINDOWS\system32\MSACM32.dll
C:\WINDOWS\system32\NETMSG.dll
C:\WINDOWS\system32\NETRAP.dll
C:\WINDOWS\system32\NTDSAPI.dll
C:\WINDOWS\system32\SAMLIB.dll
C:\WINDOWS\system32\SHELL32.dll
C:\WINDOWS\system32\ShimEng.dll
C:\WINDOWS\system32\UxTheme.dll
C:\WINDOWS\system32\WINMM.dll
C:\WINDOWS\system32\WS2HELP.dll
C:\WINDOWS\system32\WS2_32.dll
C:\WINDOWS\system32\comctl32.dll
C:\Windows\AppPatch\sysmain.sdb

7. services.exe

General information about this executable

Analysis Reason:	A service was started.
Filename:	services.exe
MD5:	0e776ed5f7cc9f94299e70461b7b8185
SHA-1:	cb5a33cec4c7b8ef4bd5dc8c241005b66b26cbbf
File Size:	108544
Command Line:	C:\WINDOWS\system32\services.exe
Process-status at analysis end:	alive
Exit Code:	0

Load-time Dlls

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

7.a) services.exe - Registry Activities

Registry Values Read:

Key	Name	Value	Times
HKLM\SYSTEM\CONTROLSET001\SERVICES\Schedule\Enum	0	Root\LEGACY_SCHEDULE\0000	1
HKLM\SYSTEM\CONTROLSET001\SERVICES\Schedule\Enum	Count	1	2