Anubis - Analysis Report

Analysis Report for Portable_WINRAR_3.8.exe

MD5: ae5ee4c4c44c9f7e69979f0ca98c34e4

Summary:

Description	Risk
Changes security settings of Internet Explorer: This system alteration could seriously affect safety surfing the World Wide Web.	low
Performs Registry Activities: The executable creates and/or modifies registry entries.	low

Dependency overview:

Portable_W.exe C:\Portable_W.exe

Analysis reason: Primary Analysis Subject

Table of Contents:

1. General Information

Information about Anubis' invocation	
Time needed:	266 s
Report created:	09/25/11, 03:40:15 UTC
Termination reason:	All tracked processes have exited
Program version:	1.75.3394

2. Portable_W.exe

General information about this executable	
Analysis Reason:	Primary Analysis Subject
Filename:	Portable_W.exe
MD5:	ae5ee4c4c44c9f7e69979f0ca98c34e4
SHA-1:	29757d5bb63899a7222c2787c094da0fed44409e
File Size:	1999929
Command Line:	"C:\Portable_W.exe"
Process-status at analysis end:	dead
Exit Code:	255

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\WinSxS\X86_Microsoft.Windows.Common-Controls_6595b64144ccf1df_6.0.2600.5512_x-ww_35d4ce83\COMCTL32.DLL	0x773D0000	0x00103000
C:\WINDOWS\system32\msvcrt.dll	0x77C10000	0x00058000
C:\WINDOWS\system32\GDI32.dll	0x77F10000	0x00049000
C:\WINDOWS\system32\USER32.dll	0x7E410000	0x00091000
C:\WINDOWS\system32\SHLWAPI.dll	0x77F60000	0x00076000
C:\WINDOWS\system32\COMDLG32.DLL	0x763B0000	0x00049000
C:\WINDOWS\system32\SHELL32.dll	0x7C9C0000	0x00817000
C:\WINDOWS\system32\OLE32.DLL	0x774E0000	0x0013D000

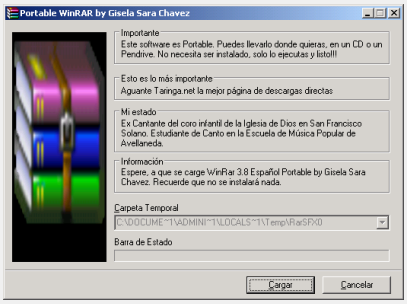
Run-time Dlls

Module Name	Base Address	Size
C:\WINDOWS\system32\xpsp2res.dll	0x00BD0000	0x002C5000
C:\WINDOWS\system32\UxTheme.dll	0x5AD70000	0x00038000
C:\WINDOWS\system32\NETAPI32.dll	0x5B860000	0x00055000
C:\WINDOWS\system32\shdoclc.dll	0x71800000	0x00088000
C:\WINDOWS\system32\WS2HELP.dll	0x71AA0000	0x00008000
C:\WINDOWS\system32\WS2_32.dll	0x71AB0000	0x00017000
C:\WINDOWS\system32\sensapi.dll	0x722B0000	0x00005000
C:\WINDOWS\system32\riched32.dll	0x732E0000	0x00005000
C:\WINDOWS\system32\msls31.dll	0x746C0000	0x00027000
C:\WINDOWS\system32\msimtf.dll	0x746F0000	0x0002A000
C:\WINDOWS\system32\MSCTF.dll	0x74720000	0x0004C000
C:\WINDOWS\system32\RICHED20.dll	0x74E30000	0x0006D000
C:\WINDOWS\system32\CRYPTUI.dll	0x754D0000	0x00080000
C:\WINDOWS\system32\MLANG.dll	0x75CF0000	0x00091000
C:\WINDOWS\system32\browseui.dll	0x75F80000	0x000FD000
C:\WINDOWS\system32\IMM32.DLL	0x76390000	0x0001D000
C:\WINDOWS\system32\USERENV.dll	0x769C0000	0x000B4000
C:\WINDOWS\system32\WINMM.dll	0x76B40000	0x0002D000

Run-time Dlls

Module Name	Base Address	Size
C:\WINDOWS\system32\PSAPI.DLL	0x76BF0000	0x0000B000
C:\WINDOWS\system32\WINTRUST.dll	0x76C30000	0x0002E000
C:\WINDOWS\system32\IMAGEHLP.dll	0x76C90000	0x00028000
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\WLDAP32.dll	0x76F60000	0x0002C000
C:\WINDOWS\system32\CLBCATQ.DLL	0x76FD0000	0x0007F000
C:\WINDOWS\system32\COMRes.dll	0x77050000	0x000C5000
C:\WINDOWS\system32\OLEAUT32.dll	0x77120000	0x0008B000
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
C:\WINDOWS\system32\VERSION.dll	0x77C00000	0x00008000
C:\WINDOWS\system32\mshtml.dll	0x7DC30000	0x002F2000
C:\WINDOWS\system32\urlmon.dll	0x7E1E0000	0x000A2000
C:\WINDOWS\system32\shdocvw.dll	0x7E290000	0x00171000

Popups

Window Name	Window Text	Screenshot	Number of Displayed Times
Portable WinRAR by Gisela Sara Chavez	&Carpeta Temporal C:\DOCUME~1\ADMINI~1\LOCALS~1\Temp\RarSFX0 C:\DOCUME~1\ADMINI~1\LOCALS~1\Temp\RarSFX0 Barra de Estado &Cargar &Cancelar Importante Este software es Portable. Puedes llevarlo donde quieras, en un CD o un Pendrive. No necesita ser instalado, solo lo ejecutas y listo!!! Esto es lo m.s importante Aguante Taringa.net la mejor p.gina de descargas directas Mi estado Ex Cantante del coro infantil de la Iglesia de Dios en San Francisco Solano. Estudiante de Canto en la Escuela de M.sica Popular de Avellaneda. Informaci.n Espere, a que se carge WinRar 3.8 Espa.ol Portable by Gisela Sara Chavez. Recuerde que no se instalar. nada.		1

2.a) Portable_W.exe - Registry Activities

Registry Values Modified:

Key	Name	New Value
HKLM\SYSTEM\CURRENTCONTROLSET\HARDWARE PROFILES\CURRENT\Software\Microsoft\windows\CurrentVersion\Internet Settings	ProxyEnable	0
HKLM\Software\Microsoft\Windows\CurrentVersion\Explorer\Shell Folders	Common 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

Registry Values Modified:

Key	Name	New Value
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	0x3c000000160000000100000000000000000000000000000000040000000000

Registry Values Read:

Key	Name	Value	Times
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
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

Registry Values Read:

Key	Name	Value	Times
HKLM\SOFTWARE\CLASSES\CLSID\{25336920-03F9-11CF-8FD0-00AA00686F13}\INPROCSERVER32		%SystemRoot%\system32\mshtml.dll	1
HKLM\SOFTWARE\CLASSES\CLSID\{25336920-03F9-11CF-8FD0-00AA00686F13}\INPROCSERVER32	ThreadingModel	Apartment	1
HKLM\SOFTWARE\CLASSES\CLSID\{25336920-03F9-11CF-8FD0-00AA00686F13}\PROGID		htmlfile	1
HKLM\SOFTWARE\CLASSES\CLSID\{3050F3BC-98B5-11CF-BB82-00AA00BDCE0B}\INPROCSERVER32		%SystemRoot%\system32\mshtml.dll	1
HKLM\SOFTWARE\CLASSES\CLSID\{3050F3BC-98B5-11CF-BB82-00AA00BDCE0B}\INPROCSERVER32	ThreadingModel	Apartment	1
HKLM\SOFTWARE\CLASSES\CLSID\{3050F406-98B5-11CF-BB82-00AA00BDCE0B}\INPROCSERVER32		%SystemRoot%\system32\mshtml.dll	2
HKLM\SOFTWARE\CLASSES\CLSID\{3050F406-98B5-11CF-BB82-00AA00BDCE0B}\INPROCSERVER32	ThreadingModel	Apartment	1
HKLM\SOFTWARE\CLASSES\CLSID\{50D5107A-D278-4871-8989-F4CEAAF59CFC}\INPROCSERVER32		C:\WINDOWS\system32\msimtf.dll	1
HKLM\SOFTWARE\CLASSES\CLSID\{50D5107A-D278-4871-8989-F4CEAAF59CFC}\INPROCSERVER32	ThreadingModel	Apartment	1
HKLM\SOFTWARE\CLASSES\CLSID\{7B8A2D94-0AC9-11D1-896C-00C04FB6BFC4}\INPROCSERVER32		C:\WINDOWS\system32\urlmon.dll	2
HKLM\SOFTWARE\CLASSES\CLSID\{7B8A2D94-0AC9-11D1-896C-00C04FB6BFC4}\INPROCSERVER32	ThreadingModel	Both	1
HKLM\SOFTWARE\CLASSES\CLSID\{8856F961-340A-11D0-A96B-00C04FD705A2}\INPROCSERVER32		C:\WINDOWS\system32\shdocvw.dll	1
HKLM\SOFTWARE\CLASSES\CLSID\{8856F961-340A-11D0-A96B-00C04FD705A2}\INPROCSERVER32	ThreadingModel	Apartment	1
HKLM\SOFTWARE\CLASSES\CLSID\{FF393560-C2A7-11CF-BFF4-444553540000}\INPROCSERVER32		%SystemRoot%\system32\shdocvw.dll	2
HKLM\SOFTWARE\CLASSES\CLSID\{FF393560-C2A7-11CF-BFF4-444553540000}\INPROCSERVER32	ThreadingModel	Apartment	1
HKLM\SOFTWARE\CLASSES\DIRECTORY	AlwaysShowExt		1
HKLM\SOFTWARE\CLASSES\DRIVE\SHELLEX\FOLDEREXTENSIONS\{FBEB8A05-BEEE-4442-804E-409D6C4515E9}	DriveMask	32	1
HKLM\SOFTWARE\CLASSES\INTERFACE\{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\SHELL.EXPLORER\CLSID		{8856F961-340A-11D0-A96B-00C04FD705A2}	1
HKLM\SOFTWARE\Classes\PROTOCOLS\Handler\about	CLSID	{3050F406-98B5-11CF-BB82-00AA00BDCE0B}	22
HKLM\SOFTWARE\Classes\PROTOCOLS\Handler\res	CLSID	{3050F3BC-98B5-11CF-BB82-00AA00BDCE0B}	2
HKLM\SOFTWARE\Microsoft\CTF\SystemShared\	CUAS	0	1

Registry Values Read:

Key	Name	Value	Times
HKLM\SOFTWARE\Microsoft\Internet Explorer\AboutURLs	blank	res://mshtml.dll/blank.htm	1
HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Internet Settings	UrlEncoding	0x00000000	4
HKLM\SYSTEM\CurrentControlSet\Control\SecurityProviders	SecurityProviders	msapsspc.dll, schannel.dll, digest.dll, msnsspc.dll	2
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\Software\Classes\CLSID\{ff393560-c2a7-11cf-bff4-444553540000}\InProcServer32		%SystemRoot%\system32\shdocvw.dll	1
HKLM\Software\Microsoft\COM3	Com+Enabled	1	2
HKLM\Software\Microsoft\COM3	REGDBVersion	0x0b00000000000000	22
HKLM\Software\Microsoft\Internet Explorer	IntegratedBrowser	1	1
HKLM\Software\Microsoft\Internet Explorer\Extensions\{08B0E5C0-4FCB-11CF-AAA5-00401C608501}	MenuText	Sun Java Console	1
HKLM\Software\Microsoft\Internet Explorer\Extensions\{08B0E5C0-4FCB-11CF-AAA5-00401C608501}	clsid	{1FBA04EE-3024-11d2-8F1F-0000F87ABD16}	1
HKLM\Software\Microsoft\Internet Explorer\Extensions\{E2E2DD38-D088-4134-82B7-F2BA38496583}	Exec	%windir%\Network Diagnostic\xpnetdiag.exe	1
HKLM\Software\Microsoft\Internet Explorer\Extensions\{E2E2DD38-D088-4134-82B7-F2BA38496583}	MenuText	@xpsp3res.dll,-20001	1
HKLM\Software\Microsoft\Internet Explorer\Extensions\{FB5F1910-F110-11D2-BB9E-00C04F795683}	ButtonText	Messenger	1
HKLM\Software\Microsoft\Internet Explorer\Extensions\{FB5F1910-F110-11D2-BB9E-00C04F795683}	Default Visible	Yes	1
HKLM\Software\Microsoft\Internet Explorer\Extensions\{FB5F1910-F110-11D2-BB9E-00C04F795683}	Exec	C:\Program Files\Messenger\msmsgs.exe	1
HKLM\Software\Microsoft\Internet Explorer\Extensions\{FB5F1910-F110-11D2-BB9E-00C04F795683}	MenuText	Windows Messenger	1
HKLM\Software\Microsoft\Internet Explorer\Extensions\{FB5F1910-F110-11d2-BB9E-00C04F795683}	clsid	{1FBA04EE-3024-11D2-8F1F-0000F87ABD16}	1
HKLM\Software\Microsoft\Internet Explorer\Extensions\{e2e2dd38-d088-4134-82b7-f2ba38496583}	clsid	{1FBA04EE-3024-11d2-8F1F-0000F87ABD16}	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\Internet Explorer\URL Compatibility\~/CONNWIZ.HTM	Compatibility Flags	4	1
HKLM\Software\Microsoft\Internet Explorer\URL Compatibility\~/CWIZINTR.HTM	Compatibility Flags	4	1
HKLM\Software\Microsoft\Internet Explorer\Version Vector	IE	6.0000	1
HKLM\Software\Microsoft\Internet Explorer\Version Vector	VML	1.0	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

Registry Values Read:

Key	Name	Value	Times
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\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\App Paths\ICWCONN1.EXE	Path	C:\Program Files\Internet Explorer\ Connection Wizard;	1
HKLM\Software\Microsoft\Windows\CurrentVersion\ Explorer\User Shell Folders	Common AppData	%ALLUSERSPROFILE%\Application Data	1
HKLM\Software\Microsoft\Windows\CurrentVersion\ Internet Settings\Accepted Documents	0	image/gif	3
HKLM\Software\Microsoft\Windows\CurrentVersion\ Internet Settings\Accepted Documents	1	image/x-xbitmap	3
HKLM\Software\Microsoft\Windows\CurrentVersion\ Internet Settings\Accepted Documents	2	image/jpeg	3
HKLM\Software\Microsoft\Windows\CurrentVersion\ Internet Settings\Accepted Documents	3	image/pjpeg	3
HKLM\Software\Microsoft\Windows\CurrentVersion\ Internet Settings\Accepted Documents	application	application/x-ms-application	3
HKLM\Software\Microsoft\Windows\CurrentVersion\ Internet Settings\Accepted Documents	flash	application/x-shockwave-flash	3
HKLM\Software\Microsoft\Windows\CurrentVersion\ Internet Settings\Accepted Documents	xaml	application/xaml+xml	3
HKLM\Software\Microsoft\Windows\CurrentVersion\ Internet Settings\Accepted Documents	xbap	application/x-ms-xbap	3
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\Microsoft\windows\CurrentVersion\ Internet Settings	UrlEncoding	0x00000000	3
HKLM\Software\Policies\Microsoft\Windows\Safer\ CodeIdentifiers	TransparentEnabled	1	1
HKLM\System\CurrentControlSet\Control\ComputerName \ActiveComputerName	ComputerName	PC	4
HKLM\System\CurrentControlSet\Control\ MediaProperties\PrivateProperties\Joystick\Winmm	wheel	1	1
HKLM\System\CurrentControlSet\Control\Nls\CodePage	950	c_950.nls	1
HKLM\System\CurrentControlSet\Control\ProductOptions	ProductType	WinNT	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
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

Registry Values Read:

Key	Name	Value	Times
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	TSUserEnabled	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	3
HKLM\System\WPA\PnP	seed	1274198464	1
HKU\S-1-5-21-842925246-1425521274-308236825-500\ Control Panel\International	NumShape	1	4
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	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\CTF\TIP\{DCBD6FA8-032F-11D3-B5B1-00C04FC324A1}\LanguageProfile\0x00000409\ {09EA4E4B-46CE-4469-B450-0DE76A435BBB}	Enable	0	1
HKU\S-1-5-21-842925246-1425521274-308236825-500\ SOFTWARE\Microsoft\CTF\TIP\{DCBD6FA8-032F-11D3-B5B1-00C04FC324A1}\LanguageProfile\0x00000c07\ {09EA4E4B-46CE-4469-B450-0DE76A435BBB}	Enable	0	1
HKU\S-1-5-21-842925246-1425521274-308236825-500\ SOFTWARE\Microsoft\Internet Explorer\Security\ P3Global	Enabled	1	1
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\Internet Explorer\Extensions\ CmdMapping	{08B0E5C0-4FCB-11C AAA5-00401C608501}	8194	1
HKU\S-1-5-21-842925246-1425521274-308236825-500\ Software\Microsoft\Internet Explorer\Extensions\ CmdMapping	{FB5F1910-F110-11d2-BB9E-00C04F795683}	8193	1
HKU\S-1-5-21-842925246-1425521274-308236825-500\ Software\Microsoft\Internet Explorer\Extensions\ CmdMapping	{e2e2dd38-d088-4134-82b7-f2ba38496583}	8192	1
HKU\S-1-5-21-842925246-1425521274-308236825-500\ Software\Microsoft\Internet Explorer\International\Scripts \3	IEFixedFontName	Courier New	2
HKU\S-1-5-21-842925246-1425521274-308236825-500\ Software\Microsoft\Internet Explorer\International\Scripts \3	IEPropFontName	Times New Roman	2
HKU\S-1-5-21-842925246-1425521274-308236825-500\ Software\Microsoft\Internet Explorer\Main	Anchor Underline	yes	1

Registry Values Read:

Key	Name	Value	Times
HKU\S-1-5-21-842925246-1425521274-308236825-500\Software\Microsoft\Internet Explorer\Main	Disable Script Debugger	yes	1
HKU\S-1-5-21-842925246-1425521274-308236825-500\Software\Microsoft\Internet Explorer\Main	Display Inline Images	yes	1
HKU\S-1-5-21-842925246-1425521274-308236825-500\Software\Microsoft\Internet Explorer\Main	Use_DlgBox_Colors	yes	1
HKU\S-1-5-21-842925246-1425521274-308236825-500\Software\Microsoft\Internet Explorer\Settings	Anchor Color	0,0,255	1
HKU\S-1-5-21-842925246-1425521274-308236825-500\Software\Microsoft\Internet Explorer\Settings	Anchor Color Visited	128,0,128	1
HKU\S-1-5-21-842925246-1425521274-308236825-500\Software\Microsoft\Internet Explorer\Settings	Use Anchor Hover Color	No	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\	ShellState	0x240000003808000000000000000000000000000010000000d0000000000	2
HKU\S-1-5-21-842925246-1425521274-308236825-500\Software\Microsoft\Windows\CurrentVersion\Explorer\Advanced	DontPrettyPath	0	1
HKU\S-1-5-21-842925246-1425521274-308236825-500\Software\Microsoft\Windows\CurrentVersion\Explorer\Advanced	Filter	0	1
HKU\S-1-5-21-842925246-1425521274-308236825-500\Software\Microsoft\Windows\CurrentVersion\Explorer\Advanced	Hidden	1	1
HKU\S-1-5-21-842925246-1425521274-308236825-500\Software\Microsoft\Windows\CurrentVersion\Explorer\Advanced	HideFileExt	0	1
HKU\S-1-5-21-842925246-1425521274-308236825-500\Software\Microsoft\Windows\CurrentVersion\Explorer\Advanced	HideIcons	0	1
HKU\S-1-5-21-842925246-1425521274-308236825-500\Software\Microsoft\Windows\CurrentVersion\Explorer\Advanced	MapNetDrvBtn	0	1
HKU\S-1-5-21-842925246-1425521274-308236825-500\Software\Microsoft\Windows\CurrentVersion\Explorer\Advanced	NoNetCrawling	1	1
HKU\S-1-5-21-842925246-1425521274-308236825-500\Software\Microsoft\Windows\CurrentVersion\Explorer\Advanced	SeparateProcess	0	1
HKU\S-1-5-21-842925246-1425521274-308236825-500\Software\Microsoft\Windows\CurrentVersion\Explorer\Advanced	ShowCompColor	1	1
HKU\S-1-5-21-842925246-1425521274-308236825-500\Software\Microsoft\Windows\CurrentVersion\Explorer\Advanced	ShowInfoTip	1	1
HKU\S-1-5-21-842925246-1425521274-308236825-500\Software\Microsoft\Windows\CurrentVersion\Explorer\Advanced	ShowSuperHidden	1	1
HKU\S-1-5-21-842925246-1425521274-308236825-500\Software\Microsoft\Windows\CurrentVersion\Explorer\Advanced	WebView	0	1
HKU\S-1-5-21-842925246-1425521274-308236825-500\Software\Microsoft\Windows\CurrentVersion\Explorer\MountPoints2\CPC\Volume\{a1094da8-30a0-11dd-817b-806d6172696f}\	Data	0x000000005c005c003f005c00490044004450023004300640052006f006d00	1
HKU\S-1-5-21-842925246-1425521274-308236825-500\Software\Microsoft\Windows\CurrentVersion\Explorer\MountPoints2\CPC\Volume\{a1094da8-30a0-11dd-817b-806d6172696f}\	Generation	1	1
HKU\S-1-5-21-842925246-1425521274-308236825-500\Software\Microsoft\Windows\CurrentVersion\Explorer\MountPoints2\CPC\Volume\{a1094daa-30a0-11dd-817b-806d6172696f}\	Data	0x000000005c005c003f005c005300540044f00520041004700450023005600	1
HKU\S-1-5-21-842925246-1425521274-308236825-500\Software\Microsoft\Windows\CurrentVersion	Generation	1	2

Registry Values Read:

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

Registry Values Read:

Key	Name	Value	Times
Internet Settings\5.0\Cache\Extensible Cache\ MSHist012011021820110219			
HKU\S-1-5-21-842925246-1425521274-308236825-500\ Software\Microsoft\Windows\CurrentVersion\ Internet Settings\5.0\Cache\Extensible Cache\ MSHist012011021820110219	CacheOptions	11	1
HKU\S-1-5-21-842925246-1425521274-308236825-500\ Software\Microsoft\Windows\CurrentVersion\ Internet Settings\5.0\Cache\Extensible Cache\ MSHist012011021820110219	CachePath	%USERPROFILE%\Local Settings\History\ History.IE5\MSHist012011021820110219\	2
HKU\S-1-5-21-842925246-1425521274-308236825-500\ Software\Microsoft\Windows\CurrentVersion\ Internet Settings\5.0\Cache\Extensible Cache\ MSHist012011021820110219	CachePrefix	:2011021820110219:	2
HKU\S-1-5-21-842925246-1425521274-308236825-500\ Software\Microsoft\Windows\CurrentVersion\ Internet Settings\5.0\Cache\Extensible Cache\ MSHist012011021820110219	CacheRepair	0	1
HKU\S-1-5-21-842925246-1425521274-308236825-500\ Software\Microsoft\Windows\CurrentVersion\Internet Settings\5.0\Cache\History	CacheLimit	8192	1
HKU\S-1-5-21-842925246-1425521274-308236825-500\ Software\Microsoft\Windows\CurrentVersion\Internet Settings\5.0\Cache\History	CachePrefix	Visited:	2
HKU\S-1-5-21-842925246-1425521274-308236825-500\ Software\Microsoft\Windows\CurrentVersion\Internet Settings\5.0\Cache\History	PerUserItem	1	1
HKU\S-1-5-21-842925246-1425521274-308236825-500\ Software\Microsoft\Windows\CurrentVersion\Internet Settings\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	1809	0	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\Shell Extensions\Cached	{FF393560-C2A7-11CF-BFF4-444553540000} {062E1261-A60E-11D0-82C2-00C(0x401	0x010000007c6c9c7c8e68fd27bdc5c801	1
HKU\S-1-5-21-842925246-1425521274-308236825-500\ Software\Microsoft\Windows\ShellNoRoam\MUICache	LangID	0x0904	1
HKU\S-1-5-21-842925246-1425521274-308236825-500\ Software\Microsoft\Windows\ShellNoRoam\MUICache\	@xpsp3res.dll,-20001	Diagnose Connection Problems...	1
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	0x3c000000300000001000000000000000 00000000000000000040000000000	2
HKU\S-1-5-21-842925246-1425521274-308236825-500\ Software\Microsoft\windows\CurrentVersion\Internet Settings\Connections	SavedLegacySettings	0x3c000000150000000100000000000000 00000000000000000040000000000	4

Registry Values Read:

Key	Name	Value	Times
HKU\S-1-5-21-842925246-1425521274-308236825-500\Software\Microsoft\windows\CurrentVersion\Internet Settings\Url History	DaysToKeep	20	1
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
HKU\S-1-5-21-842925246-1425521274-308236825-500\Volatile Environment	SESSIONNAME	Console	4
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
HKLM\Software\Microsoft\Tracing\RASAPI32	0	Attributes Change,Value Change,Security Descriptor Change	2
HKU	1	Key Change,Value Change	4

2.b) Portable_W.exe - File Activities

Files Read:

C:\Documents and Settings\Administrator\Local Settings\History\desktop.ini
C:\Portable_W.exe
C:\WINDOWS\Registration\R00000000000b.clb
C:\WINDOWS\win.ini
PIPE\lsarpc
c:\autoexec.bat

Files Modified:

MountPointManager
PIPE\lsarpc

File System Control Communication:

File	Control Code	Times
C:\Program Files\Common Files\	0x00090028	1
PIPE\lsarpc	0x0011C017	22

Device Control Communication:

File	Control Code	Times
\Device\KsecDD	0x00390008	8

Device Control Communication:

File	Control Code	Times
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:\WINDOWS\WinSxS\X86_Microsoft.Windows.Common-Controls_6595b64144ccf1df_6.0.2600.5512_x-ww_35d4ce83\COMCTL32.DLL
C:\WINDOWS\WindowsShell.Manifest
C:\WINDOWS\WindowsShell.manifest
C:\WINDOWS\system32\CLBCATQ.DLL
C:\WINDOWS\system32\COMRes.dll
C:\WINDOWS\system32\IMM32.DLL
C:\WINDOWS\system32\MLANG.dll
C:\WINDOWS\system32\MSCTF.dll
C:\WINDOWS\system32\PSAPI.DLL
C:\WINDOWS\system32\RASAPI32.DLL
C:\WINDOWS\system32\RICHED20.dll
C:\WINDOWS\system32\SETUPAPI.dll
C:\WINDOWS\system32\SHELL32.dll
C:\WINDOWS\system32\TAPI32.dll
C:\WINDOWS\system32\UxTheme.dll
C:\WINDOWS\system32\WININET.dll
C:\WINDOWS\system32\WINMM.dll
C:\WINDOWS\system32\WS2HELP.dll
C:\WINDOWS\system32\WS2_32.dll
C:\WINDOWS\system32\browseui.dll
C:\WINDOWS\system32\imm32.dll
C:\WINDOWS\system32\mshtml.dll
C:\WINDOWS\system32\msimtf.dll
C:\WINDOWS\system32\msls31.dll
C:\WINDOWS\system32\rasman.dll
C:\WINDOWS\system32\riched32.dll
C:\WINDOWS\system32\rpcss.dll
C:\WINDOWS\system32\rtutils.dll
C:\WINDOWS\system32\sensapi.dll
C:\WINDOWS\system32\shdoclc.dll
C:\WINDOWS\system32\shdocvw.dll
C:\WINDOWS\system32\urlmon.dll
C:\WINDOWS\system32\xpsp2res.dll

2.c) Portable_W.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

Mutexes Created:

ZonesCounterMutex
ZonesLockedCacheCounterMutex

Keyboard Keys Monitored:

Virtual Key Code	Times
VK_ESCAPE (27)	23
VK_SHIFT (16)	16
VK_CONTROL (17)	16
VK_MENU (18)	16
VK_LSHIFT (160)	15
VK_LCONTROL (162)	15
VK_LMENU (164)	15
VK_LBUTTON (1)	1
VK_RBUTTON (2)	1
VK_MBUTTON (4)	1