Anubis - Analysis Report

Analysis Report for Windows Loader.exe

MD5: 2c444a8bfbfc6e2c6fa4d7a7f7358d7a

Summary:

Description	Risk
Performs File Modification and Destruction: The executable modifies and destructs files which are not temporary.	low
Packed Binary: This executable is protected with a packer in order to prevent it from being reverse engineered.	medium
Performs Registry Activities: The executable creates and/or modifies registry entries.	low

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

Dependency overview:

Windows Lo.exe C:\Windows Lo.exe

Analysis reason: Primary Analysis Subject

Table of Contents:

1. General Information

Information about Anubis' invocation	
Time needed:	287 s
Report created:	12/28/12, 02:57:02 UTC
Termination reason:	Timeout
Program version:	1.76.3886

2. Windows Lo.exe

General information about this executable	
Analysis Reason:	Primary Analysis Subject
Filename:	Windows Lo.exe
MD5:	2c444a8bfbfc6e2c6fa4d7a7f7358d7a
SHA-1:	240afd1c9c258d645c2a81bf13769e0393b8caca
File Size:	3930002
Command Line:	"C:\Windows Lo.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\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\iphlpapi.dll	0x76D60000	0x00019000
C:\WINDOWS\system32\WS2_32.dll	0x71AB0000	0x00017000
C:\WINDOWS\system32\WS2HELP.dll	0x71AA0000	0x00008000
C:\WINDOWS\system32\ole32.dll	0x774E0000	0x0013D000
C:\WINDOWS\system32\OLEAUT32.dll	0x77120000	0x0008B000
C:\WINDOWS\system32\VERSION.dll	0x77C00000	0x00008000
C:\WINDOWS\system32\WINMM.dll	0x76B40000	0x0002D000

Run-time Dlls

Module Name	Base Address	Size
C:\WINDOWS\system32\xpsp2res.dll	0x011F0000	0x002C5000
C:\WINDOWS\system32\msftedit.dll	0x4B400000	0x00086000
C:\WINDOWS\WinSxS\x86_Microsoft.Windows.GdiPlus_6595b64144ccf1df_1.0.2600.5512_x-ww_dfb54e0c\Gdiplus.dll	0x4EC50000	0x001A6000
C:\WINDOWS\system32\uxtheme.dll	0x5AD70000	0x00038000
C:\WINDOWS\system32\NETAPI32.dll	0x5B860000	0x00055000
C:\WINDOWS\system32\asycfilt.dll	0x708F0000	0x00013000
C:\WINDOWS\system32\wsock32.dll	0x71AD0000	0x00009000
C:\WINDOWS\system32\RICHED32.DLL	0x732E0000	0x00005000
C:\WINDOWS\system32\MSCTF.dll	0x74720000	0x0004C000
C:\WINDOWS\system32\RICHED20.dll	0x74E30000	0x0006D000

Run-time Dlls

Module Name	Base Address	Size
C:\WINDOWS\system32\wbem\wbemsvc.dll	0x74ED0000	0x0000E000
C:\WINDOWS\system32\wbem\wbemprox.dll	0x74EF0000	0x00008000
C:\WINDOWS\system32\wbem\wbemcomn.dll	0x75290000	0x00037000
C:\WINDOWS\system32\wbem\fastprox.dll	0x75690000	0x00076000
C:\WINDOWS\system32\mlang.dll	0x75CF0000	0x00091000
C:\WINDOWS\system32\MSVCP60.dll	0x76080000	0x00065000
C:\WINDOWS\system32\NTDSAPI.dll	0x767A0000	0x00013000
C:\WINDOWS\system32\DNSAPI.dll	0x76F20000	0x00027000
C:\WINDOWS\system32\WLDAP32.dll	0x76F60000	0x0002C000
C:\WINDOWS\system32\CLBCATQ.DLL	0x76FD0000	0x0007F000
C:\WINDOWS\system32\COMRes.dll	0x77050000	0x000C5000
C:\WINDOWS\system32\SETUPAPI.dll	0x77920000	0x000F3000
C:\WINDOWS\system32\urlmon.dll	0x7E1E0000	0x000A2000

SigBuster Output

UPX V2.9-3.X SN: 1730

2.a) Windows Lo.exe - Registry Activities

Registry Keys Created:

HKLM\HARDWARE\DESCRIPTION\System\BIOS

Registry Keys Deleted:

HKLM\HARDWARE\DESCRIPTION\System\BIOS

Registry Values Modified:

Key	Name	New Value
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

Registry Values Read:

Key	Name	Value	Times
HKLM\HARDWARE\DESCRIPTION\System	SystemBiosDate	06/10/17	8
HKLM\HARDWARE\DESCRIPTION\System	SystemBiosVersion	0x510045004d0055002000200020002d002200031000000520065007600690	4
HKLM\SOFTWARE\CLASSES\APPID\{8BC3F05E-D86B-11D0-A075-00C04FB68820}	LocalService	winmgmt	1
HKLM\SOFTWARE\CLASSES\CLSID\{00021401-0000-0000-C000-000000000046}\INPROCSERVER32		shell32.dll	1
HKLM\SOFTWARE\CLASSES\CLSID\{00021401-0000-0000-C000-000000000046}\INPROCSERVER32	ThreadingModel	Apartment	1
HKLM\SOFTWARE\CLASSES\CLSID\{1B1CAD8C-2DAB-11D2-B604-00104B703EFD}\INPROCSERVER32		C:\WINDOWS\system32\wbem\fastprox.dll	1
HKLM\SOFTWARE\CLASSES\CLSID\{1B1CAD8C-2DAB-11D2-B604-00104B703EFD}\INPROCSERVER32	ThreadingModel	Both	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\{4590F812-1D3A-11D0-891F-00AA004B2E24}\INPROCSERVER32		C:\WINDOWS\system32\wbem\fastprox.dll	1
HKLM\SOFTWARE\CLASSES\CLSID\{4590F812-1D3A-11D0-891F-00AA004B2E24}\INPROCSERVER32	ThreadingModel	Both	1
HKLM\SOFTWARE\CLASSES\CLSID\{56FDF344-FD6D-11D0-958A-006097C9A090}\INPROCSERVER32		%SystemRoot%\system32\shdocvw.dll	1
HKLM\SOFTWARE\CLASSES\CLSID\{56FDF344-FD6D-11D0-958A-006097C9A090}\INPROCSERVER32	ThreadingModel	Apartment	1
HKLM\SOFTWARE\CLASSES\CLSID\{7C857801-7381-11CF-884D-00AA004B2E24}\INPROCSERVER32		C:\WINDOWS\system32\wbem\wbemsvc.dll	1
HKLM\SOFTWARE\CLASSES\CLSID\{7C857801-7381-11CF-884D-00AA004B2E24}\INPROCSERVER32	ThreadingModel	Both	1
HKLM\SOFTWARE\CLASSES\CLSID\{8BC3F05E-D86B-11D0-A075-00C04FB68820}	AppID	{8BC3F05E-D86B-11D0-A075-00C04FB68820}	1
HKLM\SOFTWARE\CLASSES\CLSID\{CB8555CC-9128-11D1-AD9B-00C04FD8FDFF}\INPROCSERVER32		C:\WINDOWS\system32\wbem\wbemprox.dll	1
HKLM\SOFTWARE\CLASSES\CLSID\{CB8555CC-9128-11D1-AD9B-00C04FD8FDFF}\INPROCSERVER32	ThreadingModel	Both	1
HKLM\SOFTWARE\CLASSES\CLSID\{D68AF00A-29CB-43FA-8504-CE99A996D9EA}\INPROCSERVER32		C:\WINDOWS\system32\wbem\fastprox.dll	1
HKLM\SOFTWARE\CLASSES\CLSID\{D68AF00A-29CB-43FA-8504-CE99A996D9EA}\INPROCSERVER32	ThreadingModel	Both	1
HKLM\SOFTWARE\CLASSES\DIRECTORY	AlwaysShowExt		1
HKLM\SOFTWARE\CLASSES\INTERFACE\{027947E1-D731-11CE-A357-000000000001}\PROXYSTUBCLSID32		{1B1CAD8C-2DAB-11D2-B604-00104B703EFD}	1
HKLM\SOFTWARE\CLASSES\INTERFACE\{1C1C45EE-4395-11D2-B60B-00104B703EFD}\PROXYSTUBCLSID32		{7C857801-7381-11CF-884D-00AA004B2E24}	1
HKLM\SOFTWARE\CLASSES\INTERFACE\{423EC01E-2E35-11D2-B604-00104B703EFD}\PROXYSTUBCLSID32		{7C857801-7381-11CF-884D-00AA004B2E24}	1
HKLM\SOFTWARE\CLASSES\INTERFACE\{9556DC99-828C-11CF-A37E-00AA003240C7}\PROXYSTUBCLSID32		{D68AF00A-29CB-43FA-8504-CE99A996D9EA}	1
HKLM\SOFTWARE\CLASSES\INTERFACE\{D4781CD6-E5D3-44DF-AD94-930EFE48A887}\PROXYSTUBCLSID32		{7C857801-7381-11CF-884D-00AA004B2E24}	1
HKLM\SOFTWARE\CLASSES\INTERFACE\{F309AD18-D86A-11D0-A075-00C04FB68820}\PROXYSTUBCLSID32		{7C857801-7381-11CF-884D-00AA004B2E24}	1
HKLM\SOFTWARE\Microsoft\CTF\SystemShared\	CUAS	0	1
HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\OEMInformation	Logo	c:\windows\oemlogo.bmp	1
HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\OEMInformation	Manufacturer	TU Wien - Campuslizenz	1
HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\OEMInformation	SupportHours	Montag bis Freitag, 8 Uhr bis 17 Uhr	1
HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\OEMInformation	SupportPhone	(01) (58801) 42002	1
HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\OEMInformation	SupportURL	http://www.zid.tuwien.ac.at/servicee/	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

Registry Values Read:

Key	Name	Value	Times
HKLM\Software\Microsoft\COM3	Com+Enabled	1	2
HKLM\Software\Microsoft\COM3	REGDBVersion	0x0b00000000000000	16
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\WBEM\CIMOM	Log File Max Size	65536	1
HKLM\Software\Microsoft\WBEM\CIMOM	Logging	1	1
HKLM\Software\Microsoft\WBEM\CIMOM	Logging Directory	C:\WINDOWS\system32\WBEM\Logs\	2
HKLM\Software\Microsoft\WBEM\CIMOM	ProcessID	680	1
HKLM\Software\Microsoft\WBEM\CIMOM	Repository Directory	%SystemRoot%\system32\WBEM\Repository	2
HKLM\Software\Microsoft\Windows NT\CurrentVersion	BuildLab	2600.xpsp.080413-2111	4
HKLM\Software\Microsoft\Windows NT\CurrentVersion	CurrentBuildNumber	2600	4
HKLM\Software\Microsoft\Windows NT\CurrentVersion	CurrentVersion	5.1	4
HKLM\Software\Microsoft\Windows NT\CurrentVersion	ProductName	Microsoft Windows XP	4
HKLM\Software\Microsoft\Windows NT\CurrentVersion\	DigitalProductId	0xa4000000030000003736343837 2d36343302d313435373233362d32333833	1
HKLM\Software\Microsoft\Windows\CurrentVersion	DevicePath	%SystemRoot%\inf	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	TransparentEnabled	1	1
HKLM\System\CurrentControlSet\Control\ComputerName\ActiveComputerName	ComputerName	PC	6
HKLM\System\CurrentControlSet\Control\MediaProperties\PrivateProperties\Joystick\Winmm	wheel	1	1
HKLM\System\CurrentControlSet\Control\Nls\Codepage	20127	c_20127.nls	2
HKLM\System\CurrentControlSet\Control\Terminal Server	TSUserEnabled	0	1
HKLM\System\CurrentControlSet\Services\LDAP	LdapClientIntegrity	1	1
HKLM\System\CurrentControlSet\Services\Tcpip\Parameters	Domain		7
HKLM\System\CurrentControlSet\Services\Tcpip\Parameters	Hostname	pc	7
HKLM\System\CurrentControlSet\Services\Tcpip\Parameters	UseDomainNameDevo	0	1
HKLM\System\CurrentControlSet\Services\WinSock2\Parameters	WinSock_Registry_Ver	2.0	2
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

Registry Values Read:

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

Registry Values Read:

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

Registry Values Read:

Key	Name	Value	Times
HKU\S-1-5-21-842925246-1425521274-308236825-500\Software\Microsoft\Windows\CurrentVersion\Explorer\Advanced	ShowSuperHidden	1	1
HKU\S-1-5-21-842925246-1425521274-308236825-500\Software\Microsoft\Windows\CurrentVersion\Explorer\Advanced	WebView	0	1
HKU\S-1-5-21-842925246-1425521274-308236825-500\Software\Microsoft\Windows\CurrentVersion\Explorer\MountPoints2\CPC\Volume\{a1094da8-30a0-11dd-817b-806d6172696f}\	Data	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	0x000000005c005c003f005c00530054004f00520041004700450023005600	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

Monitored Registry Keys:

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

2.b) Windows Lo.exe - File Activities

Files Read:

C:\WINDOWS\Registration\R00000000000b.clb
C:\WINDOWS\win.ini
C:\Windows Lo.exe
PIPE\lsarpc

Files Modified:

Ip
MountPointManager
PIPE\lsarpc
\Device\Ip
\Device\Tcp

File System Control Communication:

File	Control Code	Times
C:\Program Files\Common Files\	0x00090028	1
PIPE\lsarpc	0x0011C017	12

Device Control Communication:

File	Control Code	Times
\Device\Tcp	0x00120003	6
\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\WinSxS\x86_Microsoft.Windows.GdiPlus_6595b64144ccf1df_1.0.2600.5512_x-ww_dfb54e0c\Gdiplus.dll
C:\WINDOWS\WindowsShell.Manifest
C:\WINDOWS\system32\CLBCATQ.DLL
C:\WINDOWS\system32\COMRes.dll
C:\WINDOWS\system32\DNSAPI.dll
C:\WINDOWS\system32\MSCTF.dll
C:\WINDOWS\system32\MSVCP60.dll
C:\WINDOWS\system32\NTDSAPI.dll
C:\WINDOWS\system32\RICHED20.dll
C:\WINDOWS\system32\RICHED32.DLL
C:\WINDOWS\system32\SETUPAPI.dll
C:\WINDOWS\system32\SHELL32.dll
C:\WINDOWS\system32\WINMM.dll
C:\WINDOWS\system32\WS2HELP.dll
C:\WINDOWS\system32\WS2_32.dll
C:\WINDOWS\system32\asycfilt.dll
C:\WINDOWS\system32\imm32.dll
C:\WINDOWS\system32\iphlpapi.dll
C:\WINDOWS\system32\mlang.dll
C:\WINDOWS\system32\msftedit.dll
C:\WINDOWS\system32\rpcss.dll
C:\WINDOWS\system32\shdocvw.dll
C:\WINDOWS\system32\urlmon.dll
C:\WINDOWS\system32\uxtheme.dll
C:\WINDOWS\system32\wbem\fastprox.dll
C:\WINDOWS\system32\wbem\wbemcomn.dll
C:\WINDOWS\system32\wbem\wbemprox.dll
C:\WINDOWS\system32\wbem\wbemsvc.dll
C:\WINDOWS\system32\winlogon.exe
C:\WINDOWS\system32\wsock32.dll
C:\WINDOWS\system32\xpsp2res.dll

2.c) Windows Lo.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
WIN7LDRMU
ZonesCacheCounterMutex
ZonesCounterMutex

Mutexes Created:

ZonesLockedCacheCounterMutex

Keyboard Keys Monitored:

Virtual Key Code	Times
VK_ESCAPE (27)	3
VK_CONTROL (17)	7
VK_SHIFT (16)	7
VK_MENU (18)	7
VK_LWIN (91)	7
VK_RWIN (92)	7