Anubis - Analysis Report

Analysis Report for Scanner-9ab_2006-63.exe

MD5: 85a6c733775d2e3a75cd5565ec7085e7

Summary:

Description	Risk
Changes security settings of Internet Explorer: This system alteration could seriously affect safety surfing the World Wide Web.	medium
Performs File Modification and Destruction: The executable modifies and destructs files which are not temporary.	high
Performs Registry Activities: The executable reads and modifies register values. It also creates and monitors register keys.	low

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

Dependency overview:

Scanner-9ab_2006-63.exe C:\Scanner-9ab_2006-63.exe

Analysis reason: Primary Analysis Subject

Table of Contents:

1. General Information

Information about Anubis' invocation	
Time needed:	241 s
Report created:	09/14/09, 04:05:45 UTC
Termination reason:	Timeout
Program version:	1.72.0

1.a) - Network Activity

Unknown UDP Traffic:
From ANUBIS:1039 to 192.168.0.1:53
State: Normal establishment and termination - Transferred outbound Bytes: 35 - Transferred inbound Bytes: 197
From ANUBIS:1025 to 192.168.0.1:53
State: Normal establishment and termination - Transferred outbound Bytes: 68 - Transferred inbound Bytes: 499

2. Scanner-9ab_2006-63.exe

General information about this executable	
Analysis Reason:	Primary Analysis Subject
Filename:	Scanner-9ab_2006-63.exe
MD5:	85a6c733775d2e3a75cd5565ec7085e7
SHA-1:	7c16cb51b9aade6847ac28ea48d58da5f69a34bc
File Size:	155648
Command Line:	"C:\Scanner-9ab_2006-63.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

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\hnetcfg.dll	0x662B0000	0x00058000
C:\WINDOWS\system32\mswsock.dll	0x71A50000	0x0003F000
C:\WINDOWS\System32\wshtcpip.dll	0x71A90000	0x00008000
C:\WINDOWS\system32\WS2HELP.dll	0x71AA0000	0x00008000
C:\WINDOWS\system32\WS2_32.dll	0x71AB0000	0x00017000
C:\WINDOWS\system32\wsock32.dll	0x71AD0000	0x00009000
C:\WINDOWS\system32\sensapi.dll	0x722B0000	0x00005000
C:\WINDOWS\system32\MSCTF.dll	0x74720000	0x0004C000
C:\WINDOWS\system32\mlang.dll	0x75CF0000	0x00091000
C:\WINDOWS\system32\msimg32.dll	0x76380000	0x00005000
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

Run-time Dlls

Module Name	Base Address	Size
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\VERSION.dll	0x77C00000	0x00008000
C:\WINDOWS\system32\msvcrt.dll	0x77C10000	0x00058000
C:\WINDOWS\system32\ADVAPI32.dll	0x77DD0000	0x0009B000
C:\WINDOWS\system32\RPCRT4.dll	0x77E70000	0x00092000
C:\WINDOWS\system32\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

Ikarus Virus Scanner

Packed.Win32.Katusha (Sig-Id:32523374)

2.a) Scanner-9ab_2006-63.exe - Registry Activities

Registry Keys Created:

HKLM\Software\683C9F62757EF7BC4D6E89F74FDF91C6\

Registry Values Modified:

Key	Name	New Value
HKLM\SYSTEM\CURRENTCONTROLSET\HARDWARE PROFILES\CURRENT\Software\Microsoft\windows\CurrentVersion\Internet Settings	ProxyEnable	0
HKLM\Software\683C9F62757EF7BC4D6E89F74FDF91C6\	pcxkv	EUJ[@J>k?rF>C!!
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

Registry Values Modified:

Key	Name	New Value
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	DefaultConnectionSetti	0x3c000000030000000100000000000000000000000000000000000040000000000
HKU\S-1-5-21-842925246-1425521274-308236825-500\Software\Microsoft\windows\CurrentVersion\Internet Settings\Connections	SavedLegacySettings	0x3c000000050000000900000000000000000000000000000000000000000000000

Registry Values Read:

Key	Name	Value	Times
HKLM\HARDWARE\DESCRIPTION\System	Identifier	AT/AT COMPATIBLE	8
HKLM\HARDWARE\DESCRIPTION\System	SystemBiosVersion	0x510045004d0055002000200020002d002200031000000520065007600690	8
HKLM\SOFTWARE\CLASSES\AUTOPROXYTYPES\APPLICATION/X-INTERNET-SIGNUP	Default	0x00000000	1
HKLM\SOFTWARE\CLASSES\AUTOPROXYTYPES\APPLICATION/X-INTERNET-SIGNUP	DllFile	%SystemRoot%\system32\iedkcs32.dll	2
HKLM\SOFTWARE\CLASSES\AUTOPROXYTYPES\APPLICATION/X-INTERNET-SIGNUP	FileExtensions	.ins	2
HKLM\SOFTWARE\CLASSES\AUTOPROXYTYPES\APPLICATION/X-NS-PROXY-AUTOCONFIG	Default	0x01000000	1
HKLM\SOFTWARE\CLASSES\AUTOPROXYTYPES\APPLICATION/X-NS-PROXY-AUTOCONFIG	DllFile	%SystemRoot%\system32\jsproxy.dll	2
HKLM\SOFTWARE\CLASSES\AUTOPROXYTYPES\APPLICATION/X-NS-PROXY-AUTOCONFIG	FileExtensions	.pac;.jvs;.js	2
HKLM\SOFTWARE\CLASSES\AUTOPROXYTYPES\APPLICATION/X-NS-PROXY-AUTOCONFIG	Flags	0x01000000	1
HKLM\SOFTWARE\CLASSES\CLSID\{20D04FE0-3AEA-1069-A2D8-08002B30309D}\INPROCSERVER32		%SystemRoot%\system32\SHELL32.dll	1
HKLM\SOFTWARE\CLASSES\DIRECTORY	AlwaysShowExt		1
HKLM\SOFTWARE\CLASSES\MIME\DATABASE\CONTENT TYPE\TEXT/HTML	Extension	.htm	6
HKLM\SOFTWARE\Microsoft\CTF\SystemShared\	CUAS	0	1
HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion	InstallDate	1212451221	2

Registry Values Read:

Key	Name	Value	Times
HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\	BuildLab	2600.xpsp.080413-2111	12
HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\	CSDVersion	Service Pack 3	12
HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\	CurrentBuild	1.511.1 () (Obsolete data - do not use)	12
HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\	CurrentBuildNumber	2600	12
HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\	CurrentType	Uniprocessor Free	12
HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\	CurrentVersion	5.1	12
HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\	PathName	C:\WINDOWS	12
HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\	ProductId	76487-640-1457236-23837	12
HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\	ProductName	Microsoft Windows XP	12
HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\	RegDone		12
HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\	RegisteredOrganizatior	TU Wien, Campuslizenz	12
HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\	RegisteredOwner	Ihr Benutzername	12
HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\	SoftwareType	SYSTEM	12
HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\	SourcePath	D:\I386	12
HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\	SubVersionNumber		12
HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\	SystemRoot	C:\WINDOWS	12
HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Internet Settings	UrlEncoding	0x00000000	2
HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Internet Settings\User Agent\Post Platform	SV1		1
HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Internet Settings\User Agent\UA Tokens			1
HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Internet Settings\User Agent\UA Tokens	MSN 2.0		1
HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Internet Settings\User Agent\UA Tokens	MSN 2.5		1
HKLM\SYSTEM\CurrentControlSet\Control\Session Manager	CriticalSectionTimeout	2592000	1
HKLM\SYSTEM\CurrentControlSet\Services\NetBT\Linkage	Export	0x5c00440065007600690063006500 5c0044e00650074004200540 05f005400	1
HKLM\SYSTEM\CurrentControlSet\Services\Tcpip\Linkage	Bind	0x5c00440065007600690063006500 5c0077b00310041004400340035004200	2
HKLM\SYSTEM\CurrentControlSet\Services\Tcpip\Parameters\Interfaces\{1AD45B38-4060-4F73-BB1E-A0439A2D97EB}	DhcpServer	255.255.255.255	2
HKLM\SYSTEM\CurrentControlSet\Services\Tcpip\Parameters\Interfaces\{1AD45B38-4060-4F73-BB1E-A0439A2D97EB}	EnableDHCP	0	1
HKLM\SYSTEM\CurrentControlSet\Services\Winsock\Parameters	Transports	0x540063007000690070000000 4e00650077400420049004f00530000000000	2
HKLM\SYSTEM\Setup	OsLoaderPath	\	2
HKLM\SYSTEM\Setup	SystemPartition	\Device\HarddiskVolume1	2
HKLM\SYSTEM\Setup	SystemSetupInProgres	0	1
HKLM\Software\683C9F62757EF7BC4D6E89F74FDF91C6\	pcxkv	EUJ[@J>k?rF>C!!	8
HKLM\Software\Clients\StartMenuInternet		IEXPLORE.EXE	8

Registry Values Read:

Key	Name	Value	Times
HKLM\Software\Microsoft\Internet Explorer\Main\ FeatureControl\FEATURE_BEHAVIORS	*	1	1
HKLM\Software\Microsoft\Internet Explorer\Main\ FeatureControl\FEATURE_DISABLE_MK_PROTOCOL	*	1	1
HKLM\Software\Microsoft\Tracing	EnableConsoleTracing	0	1
HKLM\Software\Microsoft\Tracing\RASAPI32	ConsoleTracingMask	4294901760	2
HKLM\Software\Microsoft\Tracing\RASAPI32	EnableConsoleTracing	0	2
HKLM\Software\Microsoft\Tracing\RASAPI32	EnableFileTracing	0	2
HKLM\Software\Microsoft\Tracing\RASAPI32	FileDirectory	%windir%\tracing	4
HKLM\Software\Microsoft\Tracing\RASAPI32	FileTracingMask	4294901760	2
HKLM\Software\Microsoft\Tracing\RASAPI32	MaxFileSize	1048576	2
HKLM\Software\Microsoft\Windows NT\CurrentVersion\ 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	3
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	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\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
HKLM\System\CurrentControlSet\Control\Session Manager\Environment	TEMP	%SystemRoot%\TEMP	4

Registry Values Read:

Key	Name	Value	Times
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		11
HKLM\System\CurrentControlSet\Services\Tcpip\Parameters	Hostname	pc	11
HKLM\System\CurrentControlSet\Services\Tcpip\Parameters	NameServer		2
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	3
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
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

Registry Values Read:

Key	Name	Value	Times
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	1012	1
HKLM\System\CurrentControlSet\Services\WinSock2\Parameters\Protocol_Catalog9	Num_Catalog_Entries	11	1
HKLM\System\CurrentControlSet\Services\WinSock2\Parameters\Protocol_Catalog9	Serial_Access_Num	4	3
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
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

Registry Values Read:

Key	Name	Value	Times
HKLM\System\CurrentControlSet\Services\WinSock2\Parameters\Protocol_Catalog9\Catalog_Entries\000000000011	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	User Agent	Mozilla/4.0 (compatible; MSIE 6.0; Win32)	2
HKU\S-1-5-21-842925246-1425521274-308236825-500\SOFTWARE\Microsoft\Windows\CurrentVersion\Internet Settings	WarnOnPost	0x01000000	1
HKU\S-1-5-21-842925246-1425521274-308236825-500\Software\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

Registry Values Read:

Key	Name	Value	Times
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
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\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\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

Registry Values Read:

Key	Name	Value	Times
HKU\S-1-5-21-842925246-1425521274-308236825-500\Software\Microsoft\Windows\CurrentVersion\Internet Settings\ZoneMap\	IntranetName	1	3
HKU\S-1-5-21-842925246-1425521274-308236825-500\Software\Microsoft\Windows\CurrentVersion\Internet Settings\ZoneMap\	ProxyBypass	1	3
HKU\S-1-5-21-842925246-1425521274-308236825-500\Software\Microsoft\Windows\CurrentVersion\Internet Settings\ZoneMap\\ProtocolDefaults\	http	3	3
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	0x3c000000020000000900000000000000000000000000000000000000000000000000000000	4
HKU\S-1-5-21-842925246-1425521274-308236825-500\Software\Microsoft\windows\CurrentVersion\Internet Settings\Connections	SavedLegacySettings	0x3c000000040000000900000000000000000000000000000000000000000000000000000000	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		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

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	2
HKLM\System\CurrentControlSet\Services\WinSock2\Parameters\Protocol_Catalog9	0	Key Change	2

2.b) Scanner-9ab_2006-63.exe - File Activities

Files Deleted:

C:\Documents and Settings\Administrator\Local Settings\Temporary Internet Files\Content.IE5\WDUF49AN\thanks[1].htm

Files Created:

C:\Documents and Settings\Administrator\Local Settings\Temporary Internet Files\Content.IE5\WDUF49AN\pencil-netwok[1].htm
C:\Documents and Settings\Administrator\Local Settings\Temporary Internet Files\Content.IE5\WDUF49AN\thanks[1].htm
C:\Documents and Settings\Administrator\Local Settings\Temporary Internet Files\Content.IE5\WDUF49AN\thanks[2].htm

Files Read:

PIPE\lsarpc
c:\autoexec.bat

Files Modified:

C:\Documents and Settings\Administrator\Local Settings\Temporary Internet Files\Content.IE5\WDUF49AN\pencil-netwok[1].htm
C:\Documents and Settings\Administrator\Local Settings\Temporary Internet Files\Content.IE5\WDUF49AN\thanks[1].htm
C:\Documents and Settings\Administrator\Local Settings\Temporary Internet Files\Content.IE5\WDUF49AN\thanks[2].htm
Ip
MountPointManager
PIPE\lsarpc
\Device\Afd\AsyncConnectHlp
\Device\Afd\Endpoint
\Device\Ip
\Device\NetBT_Tcpip_{1AD45B38-4060-4F73-BB1E-A0439A2D97EB}
\Device\RasAcd
\Device\Tcp

File System Control Communication:

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

Device Control Communication:

File	Control Code	Times
\Device\KsecDD	0x00390008	8
IDE#CdRomQEMU_QEMU_CD-ROM_____0.9.____#4d513030303020332020202020202020202020202020#{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_GET_INFO (0x0001207B)	2
\Device\Afd\Endpoint	AFD_SET_CONTEXT (0x00012047)	26
\Device\Afd\Endpoint	AFD_BIND (0x00012003)	6
\Device\Afd\Endpoint	AFD_GET_TDI_HAND (0x00012037)	12
\Device\Afd\Endpoint	AFD_GET_SOCK_NAI (0x0001202F)	7
\Device\Afd\Endpoint	AFD_CONNECT (0x00012007)	2
\Device\Afd\Endpoint	AFD_SELECT (0x00012024)	28
\Device\Afd\Endpoint	AFD_SET_INFO (0x0001203B)	4
\Device\Tcp	0x00120003	19

Device Control Communication:

File	Control Code	Times
\Device\Ip	0x00120040	2
\Device\Ip	0x00120090	1
\Device\NetBT_Tcpip_{1AD45B38-4060-4F73-BB1E-A0439A2D97EB}	0x0021009A	1
\Device\Afd\AsyncConnectHlp	AFD_CONNECT (0x00012007)	4
\Device\Afd\Endpoint	AFD_RECV (0x00012017)	10
\Device\Afd\Endpoint	AFD_SEND (0x0001201F)	8
\Device\NetBT_Tcpip_{1AD45B38-4060-4F73-BB1E-A0439A2D97EB}	0x00210096	1
unnamed file	0x00120028	3
\Device\Afd\Endpoint	AFD_DISCONNECT (0x0001202B)	2

Memory Mapped Files:

File Name
C:\WINDOWS\System32\winrnr.dll
C:\WINDOWS\System32\wshtcpip.dll
C:\WINDOWS\WinSxS\x86_Microsoft.Windows.Common-Controls_6595b64144ccf1df_6.0.2600.5512_x-ww_35d4ce83\comctl32.dll
C:\WINDOWS\WindowsShell.Manifest
C:\WINDOWS\system32\DNSAPI.dll
C:\WINDOWS\system32\IPHLPAPI.DLL
C:\WINDOWS\system32\MSCTF.dll
C:\WINDOWS\system32\PSAPI.dll
C:\WINDOWS\system32\RASAPI32.DLL
C:\WINDOWS\system32\SETUPAPI.dll
C:\WINDOWS\system32\TAPI32.dll
C:\WINDOWS\system32\URLMON.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\hnetcfg.dll
C:\WINDOWS\system32\imm32.dll
C:\WINDOWS\system32\mlang.dll
C:\WINDOWS\system32\msimg32.dll
C:\WINDOWS\system32\mswsock.dll
C:\WINDOWS\system32\rasadhlp.dll
C:\WINDOWS\system32\rasman.dll
C:\WINDOWS\system32\rpcss.dll
C:\WINDOWS\system32\rtutils.dll
C:\WINDOWS\system32\sensapi.dll
C:\WINDOWS\system32\shell32.dll
C:\WINDOWS\system32\wininet.dll
C:\WINDOWS\system32\wsock32.dll

2.c) Scanner-9ab_2006-63.exe - Process Activities

Foreign Memory Regions Read:

Process: C:\Program Files\Messenger\msmsgs.exe
Process: C:\Scanner-9ab_2006-63.exe
Process: C:\WINDOWS\explorer.exe
Process: C:\WINDOWS\system32\cmd.exe
Process: C:\WINDOWS\system32\ctfmon.exe
Process: C:\WINDOWS\system32\lsass.exe
Process: C:\WINDOWS\system32\services.exe

Foreign Memory Regions Read:
Process: C:\WINDOWS\system32\smss.exe
Process: C:\WINDOWS\system32\spoolsv.exe
Process: C:\WINDOWS\system32\svchost.exe
Process: C:\WINDOWS\system32\winlogon.exe
Process: C:\WINDOWS\system32\wscntfy.exe
Process: C:\WINDOWS\system32\wuauclt.exe
Process: C:\nwor.exeor.exe
Process: C:\rjher.exeer.exe

2.d) Scanner-9ab_2006-63.exe - Network Activity

DNS Queries:

Name	Query Type	Query Result	Successful	Protocol
update.microsoft.com	DNS_TYPE_A		1	
wpad	DNS_TYPE_A		0	
pencil-netwok.com	DNS_TYPE_A	94.102.48.31	1	
thebigben.cn	DNS_TYPE_A	127.0.0.1	1	

HTTP Conversations:

From ANUBIS:1040 to 65.55.185.28:80 - [update.microsoft.com]
Request: GET /windowsupdate/v6/thanks.aspx
Response: 200 "OK"
Request: GET /windowsupdate/v6/thanks.aspx
Response: 200 "OK"
From ANUBIS:1041 to 94.102.48.31:80 - [pencil-netwok.com]
Request: GET /?act=fb&1=1&2=1212451221&3=5.1.3.0.2600&4=IEXPLORE.EXE&5=23&6=4&7=31&8=23&9=0&10=2006-63
Response: 200 "OK"

Unknown TCP Traffic:

From ANUBIS:1042 to 65.55.185.28:80

State: Connection established, not terminated - Transferred outbound Bytes: 212 - Transferred inbound Bytes: 2500

Data sent:

```
4745 5420 2f77 696e 646f 7773 7570 6461    GET /windowsupda
7465 2f76 362f 7468 616e 6b73 2e61 7370    te/v6/thanks.asp
7820 4854 5450 2f31 2e31 0d0a 4163 6365    x HTTP/1.1..Acce
7074 3a20 2a2f 2a0d 0a41 6363 6570 742d    pt: */*..Accept-
456e 636f 6469 6e67 3a20 677a 6970 2c20    Encoding: gzip,
6465 666c 6174 650d 0a55 7365 722d 4167    deflate..User-Ag
656e 743a 204d 6f7a 696c 6c61 2f34 2e30    ent: Mozilla/4.0
2028 636f 6d70 6174 6962 6c65 3b20 4d53     (compatible; MS
4945 2036 2e30 3b20 5769 6e64 6f77 7320    IE 6.0; Windows
4e54 2035 2e31 3b20 5356 3129 0d0a 486f    NT 5.1; SV1)..Ho
7374 3a20 7570 6461 7465 2e6d 6963 726f    st: update.micro
736f 6674 2e63 6f6d 0d0a 436f 6e6e 6563    soft.com..Connec
7469 6f6e 3a20 4b65 6570 2d41 6c69 7665    tion: Keep-Alive
0d0a 0d0a                                  ....
```

Data received:

```
4854 5450 2f31 2e31 2032 3030 204f 4b0d    HTTP/1.1 200 OK.
0a43 6163 6865 2d43 6f6e 7472 6f6c 3a20    .Cache-Control:
7072 6976 6174 650d 0a43 6f6e 7465 6e74    private..Content
2d4c 656e 6774 683a 2032 3330 380d 0a43    -Length: 2308..C
6f6e 7465 6e74 2d54 7970 653a 2074 6578    ontent-Type: tex
742f 6874 6d6c 3b20 6368 6172 7365 743d    t/html; charset=
7574 662d 380d 0a53 6572 7665 723a 204d    utf-8..Server: M
6963 726f 736f 6674 2d49 4953 2f36 2e30    icrosoft-IIS/6.0
0d0a 582d 506f 7765 7265 642d 4279 3a20    ..X-Powered-By:
4153 502e 4e45 540d 0a44 6174 653a 204d    ASP.NET..Date: M
6f6e 2c20 3134 2053 6570 2032 3030 3920    on, 14 Sep 2009
3034 3a30 323a 3436 2047 4d54 0d0a 0d0a    04:02:46 GMT....
3c68 746d 6c20 6469 723d 276c 7472 273e    <html dir='ltr'>
0a3c 6865 6164 3e0a 3c6d 6574 6120 6874    .<head>.<meta ht
```

Unknown TCP Traffic:

```
7470 2d65 7175 6976 3d22 5049 4353 2d4c    tp-equiv="PICS-L
6162 656c 2220 636f 6e74 656e 743d 2728    abel" content='(
5049 4353 2d31 2e31 2022 6874 7470 3a2f    PICS-1.1 "http:/
2f77 7777 2e72 7361 632e 6f72 672f 7261    /www.rsac.org/ra
7469 6e67 7376 3031 2e68 746d 6c22 206c    tingsv01.html" l
2067 656e 2074 7275 6520 636f 6d6d 656e     gen true commen
7420 2252 5341 4369 204e 6f72 7468 2041    t "RSACi North A
6d65 7269 6361 2053 6572 7665 7222 2062    merica Server" b
7920 2269 6e65 7440 6d69 6372 6f73 6f66    y "inet@microsof
742e 636f 6d22 206f 6e20 2231 3939 372e    t.com" on "1997.
3036 2e33 3054 3134 3a34 382d 3035 3030    06.30T14:48-0500
2220 7220 286e 2030 2073 2030 2076 2030    " r (n 0 s 0 v 0
206c 2030 2929 2720 2f3e 200a 3c6d 6574     l 0))' /> .<met
6120 6874 7470 2d65 7175 6976 3d27 436f    a http-equiv='Co
6e74 656e 742d 5479 7065 2720 636f 6e74    ntent-Type' cont
656e 743d 2774 6578 742f 6874 6d6c 3b63    ent='text/html;c
6861 7273 6574 3d77 696e 646f 7773 2d31    harset=windows-1
3235 3227 202f 3e0a 3c6d 6574 6120 6874    252' />.<meta ht
7470 2d65 7175 6976 3d27 4d53 5468 656d    tp-equiv='MSThem
6543 6f6d 7061 7469 626c 6527 2063 6f6e    eCompatible' con
7465 6e74 3d27 7965 7327 202f 3e0a 3c74    tent='yes' />.<t
6974 6c65 3e4d 6963 726f 736f 6674 2057    itle>Microsoft W
696e 646f 7773 2055 7064 6174 653c 2f74    indows Update</t
6974 6c65 3e0a 3c6c 696e 6b20 7265 6c3d    itle>.<link rel=
2773 686f 7274 6375 7420 6963 6f6e 2720    'shortcut icon'
6872 6566 3d27 7368 6172 6564 2f69 6d61    href='shared/ima
6765 732f 6261 6e6e 6572 732f 6661 7669    ges/banners/favi
636f 6e2e 6963 6f27 2074 7970 653d 2769    con.ico' type='i
6d61 6765 2f78 2d69 636f 6e27 2f3e 0a3c    mage/x-icon'/>.<
6d65 7461 206e 616d 653d 274d 5353 6d61    meta name='MSSma
7274 5461 6773 5072 6576 656e 7450 6172    rtTagsPreventPar
7369 6e67 2720 636f 6e74 656e 743d 2779    sing' content='y
6573 2720 2f3e 0a3c 6d65 7461 206e 616d    es' />.<meta nam
653d 2752 4f42 4f54 5327 2063 6f6e 7465    e='ROBOTS' conte
6e74 3d27 4e4f 494e 4445 5827 3e0a 3c21    nt='NOINDEX'>.<!
2d2d 436f 7079 7269 6768 7420 2863 2920    --Copyright (c)
4d69 6372 6f73 6f66 7420 436f 7270 6f72    Microsoft Corpor
6174 696f 6e2e 2020 416c 6c20 7269 6768    ation.  All righ
7473 2072 6573 6572 7665 642e 2d2d 3e0a    ts reserved.-->.
3c73 6372 6970 7420 6c61 6e67 7561 6765    <script language
3d27 6a61 7661 7363 7269 7074 2720 7479    ='javascript' ty
7065 3d27 7465 7874 2f6a 6176 6173 6372    pe='text/javascr
6970 7427 3e0a 7769 6e64 6f77 2e6f 6e65    ipt'>.window.one
7272 6f72 203d 206e 6577 2046 756e 6374    rror = new Funct
696f 6e28 274d 6573 7361 6765 2720 2c27    ion('Message' ,'
7355 524c 2720 2c27 734c 696e 6527 202c    sURL' ,'sLine' ,
2027 7265 7475 726e 2074 7275 653b 2729     'return true;')
0a3c 2f73 6372 6970 743e 0a3c 7363 7269    .</script>.<scri
7074 206c 616e 6775 6167 653d 274a 5363    pt language='JSc
7269 7074 2720 7479 7065 3d27 7465 7874    ript' type='text
2f6a 6176 6173 6372 6970 7427 2073 7263    /javascript' src
3d27 7368 6172 6564 2f6a 732f 7467 6172    ='shared/js/tgar
2e6a 733f 3633 3338 3834 3732 3536 3635    .js?633884725665
3738 3235 3238 273e 3c2f 7363 7269 7074    782528'></script
3e0a 3c73 6372 6970 7420 6c61 6e67 7561    >.<script langua
6765 3d27 4a53 6372 6970 7427 2074 7970    ge='JScript' typ
653d 2774 6578 742f 6a61 7661 7363 7269    e='text/javascri
7074 2720 7372 633d 2773 6861 7265 642f    pt' src='shared/
6a73 2f63 6f6e 7465 6e74 2e6a 733f 3633    js/content.js?63
3338 3834 3732 3536 3635 3738 3235 3238    3884725665782528
273e 3c2f 7363 7269 7074 3e0a 3c6c 696e    '></script>.<lin
6b20 7265 6c3d 2773 7479 6c65 5368 6565    k rel='styleshee
7427 2074 7970 653d 2774 6578 742f 6373    t' type='text/cs
7327 2068 7265 663d 2773 6861 7265 642f    s' href='shared/
6373 732f 6863 702e 6373 7327 202f 3e0a    css/hcp.css' />.
3c6c 696e 6b20 7265 6c3d 2773 7479 6c65    <link rel='style
7368 6565 7427 2074 7970 653d 2774 6578    sheet' type='tex
742f 6373 7327 2068 7265 663d 2773 6861    t/css' href='sha
7265 642f 6373 732f 636f 6e74 656e 742e    red/css/content.
6373 7327 202f 3e0a 3c73 7479 6c65 2074    css' />.<style t
7970 653d 2774 6578 742f 6373 7327 3e62    ype='text/css'>b
7574 746f 6e20 7b70 6164 6469 6e67 3a20    utton {padding:
3070 7820 3134 7078 2031 7078 2031 3470    0px 14px 1px 14p
783b 7769 6474 683a 2038 3070 783b 6865    x;width: 80px;he
6967 6874 3a20 3231 7078 3b6f 7665 7266    ight: 21px;overf
```

Unknown TCP Traffic:

```
6c6f 773a 2076 6973 6962 6c65 3b6c 696e    low: visible;lin
652d 6865 6967 6874 3a20 3135 7078 3b63    e-height: 15px;c
7572 736f                                  urso
```

Data received:

```
723a 2064 6566 6175 6c74 3b7d 3c2f 7374    r: default;}</st
796c 653e 0d0a 3c73 7479 6c65 2074 7970    yle>..<style typ
653d 2774 6578 742f 6373 7327 3e20 7461    e='text/css'> ta
626c 6520 7b20 7461 626c 652d 6c61 796f    ble { table-layo
7574 3a20 6669 7865 643b 207d 0d0a 093c    ut: fixed; }...<
2f73 7479 6c65 3e0d 0a3c 2f68 6561 643e    /style>..</head>
0909 200d 0a3c 626f 6479 2073 7479 6c65    .. ..<body style
3d22 6f76 6572 666c 6f77 3a76 6973 6962    ="overflow:visib
6c65 3b22 206f 6e6c 6f61 643d 2266 6e49    le;" onload="fnI
6e69 7428 332c 2031 3030 293b 2220 6267    nit(3, 100);" bg
636f 6c6f 723d 2277 6869 7465 2220 6c69    color="white" li
6e6b 3d22 2335 3837 6564 6322 2061 6c69    nk="#587edc" ali
6e6b 3d22 2335 3837 6564 6322 2076 6c69    nk="#587edc" vli
6e6b 3d22 2335 3837 6564 6322 3e0d 0a09    nk="#587edc">...
0d0a 093c 666f 6e74 2073 697a 653d 2233    ...<font size="3
2220 636f 6c6f 723d 2223 3538 3765 6463    " color="#587edc
223e 3c62 3e0d 0a09 0909 5468 616e 6b20    "><b>.....Thank
796f 7520 666f 7220 796f 7572 2069 6e74    you for your int
6572 6573 7420 696e 206f 6274 6169 6e69    erest in obtaini
6e67 2075 7064 6174 6573 2066 726f 6d20    ng updates from
6f75 7220 7369 7465 2e0d 0a09 093c 2f62    our site.....</b
3e3c 2f66 6f6e 743e 0d0a 093c 6272 3e0d    ></font>...<br>.
0a09 3c62 723e 0d0a 0957 696e 646f 7773    ..<br>...Windows
2055 7064 6174 6520 6973 2074 6865 206f     Update is the o
6e6c 696e 6520 6578 7465 6e73 696f 6e20    nline extension
6f66 204d 6963 726f 736f 6674 2057 696e    of Microsoft Win
646f 7773 2074 6861 7420 6865 6c70 7320    dows that helps
796f 7520 6765 7420 7468 6520 6d6f 7374    you get the most
206f 7574 206f 6620 796f 7572 2063 6f6d     out of your com
7075 7465 722e 0d0a 093c 6272 3e0d 0a09    puter....<br>...
3c62 723e 0d0a 093c 666f 6e74 2073 697a    <br>...<font siz
653d 2232 223e 0d0a 0909 466f 6c6c 6f77    e="2">....Follow
2074 6865 7365 2073 7465 7073 2074 6f20     these steps to
6163 6365 7373 2057 696e 646f 7773 2055    access Windows U
7064 6174 6520 7468 726f 7567 6820 7468    pdate through th
6520 4865 6c70 2061 6e64 2073 7570 706f    e Help and suppo
7274 2043 656e 7465 723a 0d0a 0909 3c75    rt Center:....<u
6c3e 0d0a 0909 093c 6c69 3e0d 0a09 0909    l>.....<li>.....
0943 6c69 636b 203c 623e 5374 6172 743c    .Click <b>Start<
2f62 3e2c 2061 6e64 2074 6865 6e20 636c    /b>, and then cl
6963 6b20 3c62 3e48 656c 7020 616e 6420    ick <b>Help and
7375 7070 6f72 743c 2f62 3e2e 0d0a 0909    support</b>.....
093c 6c69 3e0d 0a09 0909 0949 6620 796f    .<li>......If yo
7520 6172 6520 7275 6e6e 696e 6720 5769    u are running Wi
6e64 6f77 7320 5850 2c20 636c 6963 6b20    ndows XP, click
3c62 3e4b 6565 7020 796f 7572 2063 6f6d    <b>Keep your com
7075 7465 7220 7570 2d74 6f2d 6461 7465    puter up-to-date
2077 6974 6820 5769 6e64 6f77 7320 5570     with Windows Up
6461 7465 3c2f 623e 2e0d 0a09 0909 3c6c    date</b>......<l
693e 0d0a 0909 0909 4966 2079 6f75 2061    i>......If you a
7265 2072 756e 6e69 6e67 2061 2057 696e    re running a Win
646f 7773 2053 6572 7665 7220 3230 3033    dows Server 2003
2066 616d 696c 7920 7072 6f64 7563 742c     family product,
2063 6c69 636b 203c 623e 5769 6e64 6f77     click <b>Window
7320 5570 6461 7465 3c2f 623e 2e0d 0a09    s Update</b>....
0909 3c2f 6c69 3e0d 0a09 093c 2f75 6c3e    ..</li>....</ul>
0d0a 093c 2f66 6f6e 743e 0d0a 090d 0a09    ...</font>......
3c2f 464f 4e54 3e0d 0a09 0d0a 093c 6966    </FONT>......<if
7261 6d65 206e 616d 653d 2765 5265 706f    rame name='eRepo
7274 696e 6727 2073 7263 3d27 626c 616e    rting' src='blan
6b2e 6173 7078 2720 6e6f 7265 7369 7a65    k.aspx' noresize
2068 6569 6768 743d 2730 2720 7769 6474     height='0' widt
683d 2730 2720 7374 796c 653d 2744 4953    h='0' style='DIS
504c 4159 3a6e 6f6e 6527 3e0d 0a3c 2f62    PLAY:none'>..</b
6f64 793e 0d0a 3c2f 6874 6d6c 3e20 0d0a
```

TCP Connection Attempts:

From ANUBIS:1042 to 65.55.185.28:80

2.e) Scanner-9ab_2006-63.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
LDRMTX
ZonesCacheCounterMutex
ZonesCounterMutex
ZonesLockedCacheCounterMutex

Windows SEH exceptions:

Description	Times
Exception 0xc000001d (STATUS_ILLEGAL_INSTRUCTION) at 0x41d3b4	1
Exception 0xc0000096 (STATUS_PRIVILEGED_INSTRUCTION) at 0x4083ac	1
Exception 0xc000001d (STATUS_ILLEGAL_INSTRUCTION) at 0x408412	1