




# Anubis - Analysis Report




## **Analysis Report for Forensics100.exe**

MD5: 8c6d131f029ce24746cdee8cc196d7e1


Dependency overview:

**Forensics1.exe** C:\Forensics1.exe

Analysis reason: Primary Analysis Subject

**Explorer.EXE** C:\WINDOWS\Explorer.EXE

Analysis reason: Forensics1.exe wrote to the virtual memory of this process

**iexplore.exe** C:\Program Files\Internet Explorer\iexplore.exe

Analysis reason: Started by Explorer.EXE

## **Table of Contents:**

1. General Information.....	4
2. Forensics1.exe.....	4
a) Registry Activities.....	4
b) File Activities.....	5
c) Process Activities.....	6
3. Explorer.EXE.....	6
a) Registry Activities.....	8
b) File Activities.....	8
c) Process Activities.....	9
d) Other Activities.....	9
4. iexplore.exe.....	9
a) Registry Activities.....	10
b) File Activities.....	13
c) Network Activities.....	14



## 1. General Information

### Information about Anubis' invocation

Time needed:	249 s
Report created:	07/05/14, 03:03:06 UTC
Termination reason:	Timeout
Program version:	1.76.3886

### 1.a) - Network Activity

#### TCP Connection Attempts:

From ANUBIS:1031 to 193.95.68.245:81

## 2. Forensics1.exe

### General information about this executable

Analysis Reason:	Primary Analysis Subject
Filename:	Forensics1.exe
MD5:	8c6d131f029ce24746cdee8cc196d7e1
SHA-1:	9d558b17354052bd14d8a146f1720033ab43a8e9
File Size:	32673
Command Line:	"C:\Forensics1.exe"
Process-status at analysis end:	dead
Exit Code:	0

### Load-time DLLs

Module Name	Base Address	Size
C:\WINDOWS\system32\ntdll.dll	0x7C900000	0x000AF000
C:\WINDOWS\system32\kernel32.dll	0x7C800000	0x000F6000
C:\WINDOWS\system32\USER32.dll	0x7E410000	0x00091000
C:\WINDOWS\system32\GDI32.dll	0x77F10000	0x00049000

### Run-time DLLs

Module Name	Base Address	Size
C:\WINDOWS\system32\comctl32.dll	0x5D090000	0x0009A000
C:\WINDOWS\system32\WS2HELP.dll	0x71AA0000	0x00008000
C:\WINDOWS\system32\WS2_32.dll	0x71AB0000	0x00017000
C:\WINDOWS\system32\advpack.dll	0x75260000	0x00029000
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\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\SHLWAPI.dll	0x77F60000	0x00076000
C:\WINDOWS\system32\Secur32.dll	0x77FE0000	0x00011000
C:\WINDOWS\system32\SHELL32.dll	0x7C9C0000	0x00817000

### 2.a) Forensics1.exe - Registry Activities



## Registry Values Modified:

Key	Name	New Value
HKU\S-1-5-21-842925246-1425521274-308236825-500\Software\Microsoft\Windows\CurrentVersion\Explorer\Shell Folders	AppData	C:\Documents and Settings\Administrator\Application Data

## Registry Values Read:

Key	Name	Value	Times
HKLM\SOFTWARE\Microsoft\Active Setup\Installed Components\>{22d6f312-b0f6-11d0-94ab-0080c74c7e95}	stubpath	C:\WINDOWS\inf\unregmp2.exe /ShowWMP	2
HKLM\SOFTWARE\Microsoft\Active Setup\Installed Components\>{26923b43-4d38-484f-9b9e-de460746276c}	stubpath	%systemroot%\system32\shmigrate.exe OCInstallUserConfigIE	2
HKLM\SOFTWARE\Microsoft\Active Setup\Installed Components\>{881dd1c5-3dcf-431b-b061-f3f88e8be88a}	stubpath	%systemroot%\system32\shmigrate.exe OCInstallUserConfigOE	2
HKLM\SOFTWARE\Microsoft\Active Setup\Installed Components\{2179C5D3-EBFF-11CF-B6FD-00AA00B4E220}	stubpath		2
HKLM\SOFTWARE\Microsoft\Active Setup\Installed Components\{22d6f312-b0f6-11d0-94ab-0080c74c7e95}	stubpath		2
HKLM\SOFTWARE\Microsoft\Active Setup\Installed Components\{2C7339CF-2B09-4501-B3F3-F3508C9228ED}	stubpath	%SystemRoot%\system32\regsvr32.exe /s /n /i:/UserInstall %SystemRoot%\system32\themeui.dll	2
HKLM\SOFTWARE\Microsoft\Active Setup\Installed Components\{44BBA840-CC51-11CF-AAFA-00AA00B6015C}	stubpath	"%ProgramFiles%\Outlook Express\setup50.exe" /APP:OE /CALLER:WINNT /user /install	2
HKLM\SOFTWARE\Microsoft\Active Setup\Installed Components\{44BBA842-CC51-11CF-AAFA-00AA00B6015B}	stubpath	rundll32.exe advpack.dll,LaunchINFSection C:\WINDOWS\INF\msnetmtg.inf,NetMtg.Install.PerUserr.NT	2
HKLM\SOFTWARE\Microsoft\Active Setup\Installed Components\{4b218e3e-bc98-4770-93d3-2731b9329278}	stubpath	%SystemRoot%\System32\rundll32.exe setupapi,InstallHinfSection MarketplaceLinkInstall 896 %systemroot%\inf\ie.inf	2
HKLM\SOFTWARE\Microsoft\Active Setup\Installed Components\{5945c046-1e7d-11d1-bc44-00c04fd912be}	stubpath	rundll32.exe advpack.dll,LaunchINFSection C:\WINDOWS\INF\msmsgs.inf,BLC.QuietInstall.PerUserr	2
HKLM\SOFTWARE\Microsoft\Active Setup\Installed Components\{6BF52A52-394A-11d3-B153-00C04F79FAA6}	stubpath	rundll32.exe advpack.dll,LaunchINFSection C:\WINDOWS\INF\wmp.inf,PerUserStub	2
HKLM\SOFTWARE\Microsoft\Active Setup\Installed Components\{7790769C-0471-11d2-AF11-00C04FA35D02}	stubpath	"%ProgramFiles%\Outlook Express\setup50.exe" /APP:WAB /CALLER:WINNT /user /install	2
HKLM\SOFTWARE\Microsoft\Active Setup\Installed Components\{89820200-ECBD-11cf-8B85-00AA005B4340}	stubpath	regsvr32.exe /s /n /i:U shell32.dll	2
HKLM\SOFTWARE\Microsoft\Active Setup\Installed Components\{89820200-ECBD-11cf-8B85-00AA005B4383}	stubpath	%SystemRoot%\system32\ie4uinit.exe	2
HKLM\SYSTEM\CurrentControlSet\Control\Session Manager	CriticalSectionTimeout	2592000	1
HKLM\SYSTEM\Setup	SystemSetupInProgress	0	1
HKLM\Software\Microsoft\Windows NT\CurrentVersion\Windows	AppInit_DLLs		1
HKLM\Software\Policies\Microsoft\Windows\Safer\CodeIdentifiers	TransparentEnabled	1	1
HKLM\System\CurrentControlSet\Control\Terminal Server	TSAppCompat	0	3
HKLM\System\CurrentControlSet\Control\Terminal Server	TSUserEnabled	0	1
HKU\S-1-5-21-842925246-1425521274-308236825-500\Software\Microsoft\Windows\CurrentVersion\Explorer\User Shell Folders	AppData	%USERPROFILE%\Application Data	1

## 2.b) Forensics1.exe - File Activities

## Files Read:

C:\Forensics1.exe  
C:\WINDOWS\system32\kernel32.dll



## Files Read:

C:\WINDOWS\system32\ntdll.dll

## File System Control Communication:

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

## Device Control Communication:

File	Control Code	Times
\Device\KsecDD	0x00390008	1

## Memory Mapped Files:

File Name
C:\WINDOWS\WinSxS\x86_Microsoft.Windows.Common-Controls_6595b64144ccf1df_6.0.2600.5512_x-ww_35d4ce83\comctl32.dll
C:\WINDOWS\WindowsShell.Manifest
C:\WINDOWS\system32\SHELL32.dll
C:\WINDOWS\system32\WININET.dll
C:\WINDOWS\system32\WS2HELP.dll
C:\WINDOWS\system32\WS2_32.dll
C:\WINDOWS\system32\advpack.dll
C:\WINDOWS\system32\comctl32.dll

## 2.c) Forensics1.exe - Process Activities

## Remote Threads Created:

Affected Process
C:\WINDOWS\explorer.exe

## Foreign Memory Regions Written:

Process: C:\WINDOWS\explorer.exe

## 3. Explorer.EXE

## General information about this executable

Analysis Reason:	Forensics1.exe wrote to the virtual memory of this process
Filename:	Explorer.EXE
MD5:	12896823fb95bfb3dc9b46bcaedc9923
SHA-1:	9d2bf84874abc5b6e9a2744b7865c193c08d362f
File Size:	1033728
Command Line:	C:\WINDOWS\Explorer.EXE
Process-status at analysis end:	alive
Exit Code:	0

## Load-time DLLs

Module Name	Base Address	Size
C:\WINDOWS\system32\ntdll.dll	0x7C900000	0x000AF000
C:\WINDOWS\system32\kernel32.dll	0x7C800000	0x000F6000
C:\WINDOWS\system32\ADVAPI32.dll	0x77DD0000	0x0009B000
C:\WINDOWS\system32\RPCRT4.dll	0x77E70000	0x00092000
C:\WINDOWS\system32\Secur32.dll	0x77FE0000	0x00011000
C:\WINDOWS\system32\BROWSEUI.dll	0x75F80000	0x000FD000
C:\WINDOWS\system32\GDI32.dll	0x77F10000	0x00049000
C:\WINDOWS\system32\USER32.dll	0x7E410000	0x00091000
C:\WINDOWS\system32\msvcrt.dll	0x77C10000	0x00058000
C:\WINDOWS\system32\ole32.dll	0x774E0000	0x0013D000



## Load-time Dlls

Module Name	Base Address	Size
C:\WINDOWS\system32\SHLWAPI.dll	0x77F60000	0x00076000
C:\WINDOWS\system32\OLEAUT32.dll	0x77120000	0x0008B000
C:\WINDOWS\system32\SHDOCVW.dll	0x7E290000	0x00171000
C:\WINDOWS\system32\CRYPT32.dll	0x77A80000	0x00095000
C:\WINDOWS\system32\MSASN1.dll	0x77B20000	0x00012000
C:\WINDOWS\system32\CRYPTUI.dll	0x754D0000	0x00080000
C:\WINDOWS\system32\NETAPI32.dll	0x5B860000	0x00055000
C:\WINDOWS\system32\VERSION.dll	0x77C00000	0x00008000
C:\WINDOWS\system32\WININET.dll	0x771B0000	0x000AA000
C:\WINDOWS\system32\WINTRUST.dll	0x76C30000	0x0002E000
C:\WINDOWS\system32\IMAGEHLP.dll	0x76C90000	0x00028000
C:\WINDOWS\system32\WLDAP32.dll	0x76F60000	0x0002C000
C:\WINDOWS\system32\SHELL32.dll	0x7C9C0000	0x00817000
C:\WINDOWS\system32\UxTheme.dll	0x5AD70000	0x00038000
C:\WINDOWS\system32\ShimEng.dll	0x5CB70000	0x00026000
C:\WINDOWS\AppPatch\AcGenral.DLL	0x6F880000	0x001CA000
C:\WINDOWS\system32\WINMM.dll	0x76B40000	0x0002D000
C:\WINDOWS\system32\MSACM32.dll	0x77BE0000	0x00015000
C:\WINDOWS\system32\USERENV.dll	0x769C0000	0x000B4000
C:\WINDOWS\WinSxS\x86_Microsoft.Windows.Common-Controls_6595b64144ccf1df_6.0.2600.5512_x-ww_35d4ce83\comctl32.dll	0x773D0000	0x00103000
C:\WINDOWS\system32\comctl32.dll	0x5D090000	0x0009A000
C:\WINDOWS\system32\appHelp.dll	0x77B40000	0x00022000
C:\WINDOWS\system32\CLBCATQ.DLL	0x76FD0000	0x0007F000
C:\WINDOWS\system32\COMRes.dll	0x77050000	0x000C5000
C:\WINDOWS\System32\cscui.dll	0x77A20000	0x00054000
C:\WINDOWS\System32\CSCDLL.dll	0x76600000	0x0001D000
C:\WINDOWS\system32\themeui.dll	0x5BA60000	0x00071000
C:\WINDOWS\system32\MSIMG32.dll	0x76380000	0x00005000
C:\WINDOWS\system32\xpsp2res.dll	0x00AC0000	0x002C5000
C:\WINDOWS\system32\actxprxy.dll	0x71D40000	0x0001B000
C:\WINDOWS\system32\msutb.dll	0x5FC10000	0x00033000
C:\WINDOWS\system32\MSCTF.dll	0x74720000	0x0004C000
C:\WINDOWS\system32\urlmon.dll	0x7E1E0000	0x000A2000
C:\WINDOWS\system32\LINKINFO.dll	0x76980000	0x00008000
C:\WINDOWS\system32\ntshrui.dll	0x76990000	0x00025000
C:\WINDOWS\system32\ATL.DLL	0x76B20000	0x00011000
C:\WINDOWS\system32\rsaenh.dll	0x68000000	0x00036000
C:\WINDOWS\system32\msi.dll	0x7D1E0000	0x002BC000
C:\WINDOWS\system32\WINSTA.dll	0x76360000	0x00010000
C:\WINDOWS\system32\webcheck.dll	0x74B30000	0x00046000
C:\WINDOWS\system32\WSOCK32.dll	0x71AD0000	0x00009000
C:\WINDOWS\system32\WS2_32.dll	0x71AB0000	0x00017000
C:\WINDOWS\system32\WS2HELP.dll	0x71AA0000	0x00008000
C:\WINDOWS\system32\stobject.dll	0x76280000	0x00021000
C:\WINDOWS\system32\BatMeter.dll	0x74AF0000	0x0000A000
C:\WINDOWS\system32\POWRPROF.dll	0x74AD0000	0x00008000
C:\WINDOWS\system32\SETUPAPI.dll	0x77920000	0x000F3000
C:\WINDOWS\system32\WTSAPI32.dll	0x76F50000	0x00008000
C:\WINDOWS\system32\NETSHELL.dll	0x76400000	0x001A5000
C:\WINDOWS\system32\credui.dll	0x76C00000	0x0002E000
C:\WINDOWS\system32\dot3api.dll	0x478C0000	0x0000A000
C:\WINDOWS\system32\rtutils.dll	0x76E80000	0x0000E000
C:\WINDOWS\system32\dot3dlg.dll	0x736D0000	0x00006000
C:\WINDOWS\system32\OneX.DLL	0x5DCA0000	0x00028000
C:\WINDOWS\system32\leappcfg.dll	0x745B0000	0x00022000



## Load-time DLLs

Module Name	Base Address	Size
C:\WINDOWS\system32\MSVCP60.dll	0x76080000	0x00065000
C:\WINDOWS\system32\leappprxy.dll	0x5DCD0000	0x0000E000
C:\WINDOWS\system32\iphlpapi.dll	0x76D60000	0x00019000
C:\WINDOWS\system32\MPR.dll	0x71B20000	0x00012000
C:\WINDOWS\System32\drprov.dll	0x75F60000	0x00007000
C:\WINDOWS\System32\ntlanman.dll	0x71C10000	0x0000E000
C:\WINDOWS\System32\NETUI0.dll	0x71CD0000	0x00017000
C:\WINDOWS\System32\NETUI1.dll	0x71C90000	0x00040000
C:\WINDOWS\System32\NETRAP.dll	0x71C80000	0x00007000
C:\WINDOWS\System32\SAMLIB.dll	0x71BF0000	0x00013000
C:\WINDOWS\System32\davclnt.dll	0x75F70000	0x0000A000
C:\WINDOWS\system32\comdlg32.dll	0x763B0000	0x00049000
C:\WINDOWS\system32\MSGINA.dll	0x75970000	0x000F8000
C:\WINDOWS\system32\ODBC32.dll	0x74320000	0x0003D000
C:\WINDOWS\system32\odbcint.dll	0x01350000	0x00017000
C:\WINDOWS\system32\browseui.dll	0x71600000	0x00012000
C:\WINDOWS\system32\shdoclc.dll	0x71800000	0x00088000

### 3.a) Explorer.EXE - Registry Activities

## Registry Keys Created:

HKLM\SOFTWARE\Microsoft\Active Setup\Installed Components\{9D71D88C-C598-4935-C5D1-43AA4DB90836}

HKLM\SOFTWARE\Lame

HKU\S-1-5-21-842925246-1425521274-308236825-500\SOFTWARE\Lame

## Registry Values Modified:

Key	Name	New Value
HKLM\SOFTWARE\Lame	nck	0xed1be627b928d63274c3cd74fa935b67
HKLM\SOFTWARE\Microsoft\Active Setup\Installed Components\{9D71D88C-C598-4935-C5D1-43AA4DB90836}	stubpath	C:\Program Files\Bifrost\Lame.exe s
HKU\S-1-5-21-842925246-1425521274-308236825-500\SOFTWARE\Lame	klg	0x00

## Registry Values Read:

Key	Name	Value	Times
HKLM\SOFTWARE\Classes\HTTP\shell\open\command		"C:\Program Files\Internet Explorer\iexplore.exe" -nohome	2
HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion	ProgramFilesDir	C:\Program Files	2
HKLM\SYSTEM\WPA\MediaCenter	Installed	0	1
HKLM\System\CurrentControlSet\Control\ComputerName\ActiveComputerName	ComputerName	PC	1

### 3.b) Explorer.EXE - File Activities

## Files Created:

C:\Program Files\Bifrost

C:\Program Files\Bifrost\Lame.exe

## Files Read:

C:\WINDOWS\system32\Advapi32.dll

## Files Modified:

C:\Program Files\Bifrost\Lame.exe





## Directories Created:

C:\Program Files\Bifrost

## File System Control Communication:

File	Control Code	Times
C:\lsarpc, Flags: Named pipe	0x0011C017	3

## Memory Mapped Files:

File Name
C:\Forensics1.exe
C:\Program Files\Internet Explorer\IEXPLORE.EXE
C:\Program Files\Internet Explorer\iexplore.exe
C:\Windows\AppPatch\sysmain.sdb

### 3.c) Explorer.EXE - Process Activities

## Processes Created:

Executable	Command Line
C:\Program Files\Internet Explorer\iexplore.exe	
C:\Program Files\Internet Explorer\iexplore.exe	

## Remote Threads Created:

Affected Process
C:\Program Files\Internet Explorer\iexplore.exe

## Foreign Memory Regions Read:

Process: C:\Program Files\Internet Explorer\iexplore.exe

## Foreign Memory Regions Written:

Process: C:\Program Files\Internet Explorer\iexplore.exe

### 3.d) Explorer.EXE - Other Activities

## Mutexes Created:

lm1234

## Keyboard Keys Monitored:

Virtual Key Code	Times
VK_LBUTTON (1)	218

## 4. iexplore.exe

## General information about this executable

Analysis Reason:	Started by Explorer.EXE
Filename:	iexplore.exe
MD5:	55794b97a7faabd2910873c85274f409
SHA-1:	58e80c90bf54850b5f3ccbd8edf0877537e0ea8e
File Size:	93184
Command Line:	"C:\Program Files\Internet Explorer\iexplore.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:\Program Files\Internet Explorer\iexplore.exe	0x00400000	0x00019000
C:\WINDOWS\system32\kernel32.dll	0x7C800000	0x000F6000
C:\WINDOWS\system32\msvcrt.dll	0x77C10000	0x00058000
C:\WINDOWS\system32\USER32.dll	0x7E410000	0x00091000
C:\WINDOWS\system32\GDI32.dll	0x77F10000	0x00049000
C:\WINDOWS\system32\SHLWAPI.dll	0x77F60000	0x00076000
C:\WINDOWS\system32\ADVAPI32.dll	0x77DD0000	0x0009B000
C:\WINDOWS\system32\RPCRT4.dll	0x77E70000	0x00092000
C:\WINDOWS\system32\Secur32.dll	0x77FE0000	0x00011000
C:\WINDOWS\system32\SHDOCVW.dll	0x7E290000	0x00171000
C:\WINDOWS\system32\CRYPT32.dll	0x77A80000	0x00095000
C:\WINDOWS\system32\MSASN1.dll	0x77B20000	0x00012000
C:\WINDOWS\system32\CRYPTUI.dll	0x754D0000	0x00080000
C:\WINDOWS\system32\NETAPI32.dll	0x5B860000	0x00055000
C:\WINDOWS\system32\OLEAUT32.dll	0x77120000	0x0008B000
C:\WINDOWS\system32\ole32.dll	0x774E0000	0x0013D000
C:\WINDOWS\system32\VERSION.dll	0x77C00000	0x00008000
C:\WINDOWS\system32\WININET.dll	0x771B0000	0x000AA000
C:\WINDOWS\system32\WINTRUST.dll	0x76C30000	0x0002E000
C:\WINDOWS\system32\IMAGEHLP.dll	0x76C90000	0x00028000
C:\WINDOWS\system32\WLDAP32.dll	0x76F60000	0x0002C000
C:\WINDOWS\system32\ShimEng.dll	0x5CB70000	0x00026000
C:\WINDOWS\WinSxS\x86_Microsoft.Windows.Common-Controls_6595b64144ccf1df_6.0.2600.5512_x-ww_35d4ce83\comctl32.dll	0x773D0000	0x00103000
C:\WINDOWS\system32\RichEd20.dll	0x74E30000	0x0006D000

## Run-time DLLs

Module Name	Base Address	Size
C:\WINDOWS\system32\comctl32.dll	0x5D090000	0x0009A000
C:\WINDOWS\system32\hnetcfg.dll	0x662B0000	0x00058000
C:\WINDOWS\system32\mswsock.dll	0x71A50000	0x0003F000
C:\WINDOWS\System32\wshtcpip.dll	0x71A90000	0x00008000
C:\WINDOWS\system32\WS2HELP.dll	0x71AA0000	0x00008000
C:\WINDOWS\system32\WS2_32.dll	0x71AB0000	0x00017000
C:\WINDOWS\system32\MSCTF.dll	0x74720000	0x0004C000
C:\WINDOWS\system32\MSVFW32.dll	0x75A70000	0x00021000
C:\WINDOWS\system32\WINMM.dll	0x76B40000	0x0002D000
C:\WINDOWS\system32\SHELL32.dll	0x7C9C0000	0x00817000

#### 4.a) iexplore.exe - Registry Activities

## Registry Keys Created:

HKLM\SYSTEM\CurrentControlSet\Control\MediaResources\msvideo

## Registry Values Read:

Key	Name	Value	Times
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



## Registry Values Read:

Key	Name	Value	Times
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\Microsoft\CTF\SystemShared\	CUAS	0	1
HKLM\SYSTEM\CurrentControlSet\Control\Session Manager	CriticalSectionTimeout	2592000	1
HKLM\SYSTEM\CurrentControlSet\Services\Winsock\Parameters	Transports	0x5400630070006900700000004e00650077400420049004f005300000000000	2
HKLM\SYSTEM\Setup	SystemSetupInProgress	0	1
HKLM\SYSTEM\WPA\MediaCenter	Installed	0	1
HKLM\Software\Microsoft\Windows NT\CurrentVersion\Windows	AppInit_DLLs		1
HKLM\Software\Policies\Microsoft\Windows\Safer\CodeIdentifiers	TransparentEnabled	1	1
HKLM\System\CurrentControlSet\Control\ComputerName\ActiveComputerName	ComputerName	PC	1
HKLM\System\CurrentControlSet\Control\MediaProperties\PrivateProperties\Joystick\Winmm	wheel	1	1
HKLM\System\CurrentControlSet\Control\Terminal Server	TSAppCompat	0	1
HKLM\System\CurrentControlSet\Services\LDAP	LdapClientIntegrity	1	1
HKLM\System\CurrentControlSet\Services\Tcpip\Parameters\Winsock	HelperDllName	%SystemRoot%\System32\wshtcpip.dll	1
HKLM\System\CurrentControlSet\Services\Tcpip\Parameters\Winsock	Mapping	0x0b00000003000000020000000100000000600000002000000010000000000	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	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	StoresServiceClassInfc	0	1
HKLM\System\CurrentControlSet\Services\WinSock2\Parameters\NameSpace_Catalog5\Catalog_Entries\000000000001	SupportedNameSpace	12	1
HKLM\System\CurrentControlSet\Services\WinSock2\Parameters\NameSpace_Catalog5\Catalog_Entries\000000000001	Version	0	1
HKLM\System\CurrentControlSet\Services\WinSock2\Parameters\NameSpace_Catalog5\Catalog_Entries\000000000002	DisplayString	NTDS	4



## Registry Values Read:

Key	Name	Value	Times
HKLM\System\CurrentControlSet\Services\WinSock2\Parameters\NameSpace_Catalog5\Catalog_Entries\000000000002	Enabled	1	1
HKLM\System\CurrentControlSet\Services\WinSock2\Parameters\NameSpace_Catalog5\Catalog_Entries\000000000002	LibraryPath	%SystemRoot%\System32\winnr.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	StoresServiceClassInfc	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	StoresServiceClassInfc	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_IL	1020	1
HKLM\System\CurrentControlSet\Services\WinSock2\Parameters\Protocol_Catalog9	Num_Catalog_Entries	13	1
HKLM\System\CurrentControlSet\Services\WinSock2\Parameters\Protocol_Catalog9	Serial_Access_Num	6	2
HKLM\System\CurrentControlSet\Services\WinSock2\Parameters\Protocol_Catalog9\Catalog_Entries\000000000001	PackedCatalogItem	%SystemRoot%\system32\mswsock.	1
HKLM\System\CurrentControlSet\Services\WinSock2\Parameters\Protocol_Catalog9\Catalog_Entries\000000000002	PackedCatalogItem	%SystemRoot%\system32\mswsock.	1
HKLM\System\CurrentControlSet\Services\WinSock2\Parameters\Protocol_Catalog9\Catalog_Entries\000000000003	PackedCatalogItem	%SystemRoot%\system32\mswsock.	1
HKLM\System\CurrentControlSet\Services\WinSock2\Parameters\Protocol_Catalog9\Catalog_Entries\000000000004	PackedCatalogItem	%SystemRoot%\system32\rsvpsp.d	1
HKLM\System\CurrentControlSet\Services\WinSock2\Parameters\Protocol_Catalog9\Catalog_Entries\000000000005	PackedCatalogItem	%SystemRoot%\system32\rsvpsp.d	1
HKLM\System\CurrentControlSet\Services\WinSock2\Parameters\Protocol_Catalog9\Catalog_Entries\000000000006	PackedCatalogItem	%SystemRoot%\system32\mswsock.	1
HKLM\System\CurrentControlSet\Services\WinSock2\Parameters\Protocol_Catalog9\Catalog_Entries\000000000007	PackedCatalogItem	%SystemRoot%\system32\mswsock.	1



## Registry Values Read:

Key	Name	Value	Times
HKLM\System\CurrentControlSet\Services\WinSock2\Parameters\Protocol_Catalog9\Catalog_Entries\000000000008	PackedCatalogItem	%SystemRoot%\system32\mswsock.	1
HKLM\System\CurrentControlSet\Services\WinSock2\Parameters\Protocol_Catalog9\Catalog_Entries\000000000009	PackedCatalogItem	%SystemRoot%\system32\mswsock.	1
HKLM\System\CurrentControlSet\Services\WinSock2\Parameters\Protocol_Catalog9\Catalog_Entries\000000000010	PackedCatalogItem	%SystemRoot%\system32\mswsock.	1
HKLM\System\CurrentControlSet\Services\WinSock2\Parameters\Protocol_Catalog9\Catalog_Entries\000000000011	PackedCatalogItem	%SystemRoot%\system32\mswsock.	1
HKLM\System\CurrentControlSet\Services\WinSock2\Parameters\Protocol_Catalog9\Catalog_Entries\000000000012	PackedCatalogItem	%SystemRoot%\system32\mswsock.	1
HKLM\System\CurrentControlSet\Services\WinSock2\Parameters\Protocol_Catalog9\Catalog_Entries\000000000013	PackedCatalogItem	%SystemRoot%\system32\mswsock.	1
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

## Monitored Registry Keys:

Key Name	Watch subtree	Notify Filter	Count
HKLM\System\CurrentControlSet\Services\WinSock2\Parameters\NameSpace_Catalog5	0	Key Change	1
HKLM\System\CurrentControlSet\Services\WinSock2\Parameters\Protocol_Catalog9	0	Key Change	1

#### 4.b) iexplore.exe - File Activities

## Files Read:

C:\WINDOWS\system32\Advapi32.dll  
C:\WINDOWS\system32\avicap32.dll  
PIPE\lsarpc

## Files Modified:

PIPE\lsarpc  
\Device\Afd\Endpoint

## File System Control Communication:

File	Control Code	Times
C:\Documents and Settings\Administrator\	0x00090028	1
PIPE\lsarpc	0x0011C017	3

## Device Control Communication:

File	Control Code	Times
\Device\KsecDD	0x00390008	1
\Device\Afd\Endpoint	AFD_GET_INFO (0x0001207B)	2
\Device\Afd\Endpoint	AFD_SET_CONTEXT (0x00012047)	6
\Device\Afd\Endpoint	AFD_BIND (0x00012003)	3
\Device\Afd\Endpoint	AFD_GET_TDI_HAND (0x00012037)	9
\Device\Afd\Endpoint	AFD_CONNECT (0x00012007)	3



## Memory Mapped Files:

**File Name**

C:\WINDOWS\System32\wshtcpip.dll
C:\WINDOWS\WinSxS\x86_Microsoft.Windows.Common-Controls_6595b64144ccf1df_6.0.2600.5512_x-ww_35d4ce83\comctl32.dll
C:\WINDOWS\WindowsShell.Manifest
C:\WINDOWS\system32\MSCTF.dll
C:\WINDOWS\system32\MSVFW32.dll
C:\WINDOWS\system32\RichEd20.dll
C:\WINDOWS\system32\SHDOCVW.dll
C:\WINDOWS\system32\SHELL32.dll
C:\WINDOWS\system32\ShimEng.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\comctl32.dll
C:\WINDOWS\system32\hnetcfg.dll
C:\WINDOWS\system32\imm32.dll
C:\WINDOWS\system32\mswsock.dll
C:\Windows\AppPatch\sysmain.sdb

**4.c) iexplore.exe - Network Activity**

## TCP Connection Attempts:

From ANUBIS:1028 to 193.95.68.245:81
From ANUBIS:1029 to 193.95.68.245:81
From ANUBIS:1030 to 193.95.68.245:81