Anubis - Analysis Report

Analysis Report for http://www.colorblender.com/

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:

iexplore.exe C:\Programme\Internet Explorer\iexplore.exe

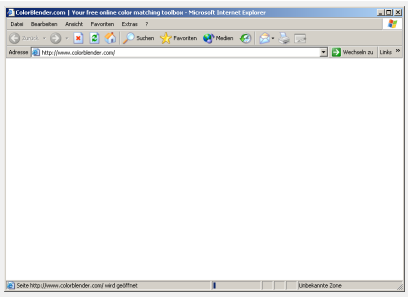
Analysis reason: Primary Analysis Subject

Table of Contents:

1. General Information

Information about Anubis' invocation	
Time needed:	230 s
Report created:	07/12/09, 09:22:34 UTC
Termination reason:	All tracked processes have exited
Program version:	1.70.0

Popups

Process	Window Name	Window Text	Screenshot	Number of Displayed Times
IEXPLORE.EXE	http://www.colorblender.(- Microsoft Internet Explorer	Links http://www.colorblender.com/ http://www.colorblender.com/ Seite http://www.colorblender.com/ wird ge.ffnet		1

1.a) - Network Activity

Unknown UDP Traffic:

From ANUBIS:1026 to 192.168.0.1:53
State: Normal establishment and termination - Transferred outbound Bytes: 127 - Transferred inbound Bytes: 909

2. iexplore.exe

General information about this executable	
Analysis Reason:	Primary Analysis Subject
Filename:	iexplore.exe
Command Line:	"C:\Programme\Internet Explorer\iexplore.exe" http://www.colorblender.com/
Process-status at analysis end:	dead
Exit Code:	0

Load-time Dlls

Module Name	Base Address	Size
C:\WINDOWS\System32\ntdll.dll	0x77F40000	0x000B0000
C:\WINDOWS\system32\kernel32.dll	0x77E40000	0x000F7000
C:\WINDOWS\system32\msvcrt.dll	0x77BE0000	0x00053000
C:\WINDOWS\system32\USER32.dll	0x77D10000	0x0008D000
C:\WINDOWS\system32\GDI32.dll	0x77C40000	0x00040000
C:\WINDOWS\system32\ADVAPI32.dll	0x77DA0000	0x0009A000
C:\WINDOWS\system32\RPCRT4.dll	0x77C90000	0x00075000
C:\WINDOWS\system32\SHLWAPI.dll	0x772A0000	0x00063000
C:\WINDOWS\System32\SHDOCVW.dll	0x76970000	0x00149000
C:\WINDOWS\WinSxS\x86_Microsoft.Windows.Common-Controls_6595b64144ccf1df_6.0.0.0_x-ww_1382d70a\comctl32.dll	0x71950000	0x000E4000

Run-time Dlls

Module Name	Base Address	Size
C:\WINDOWS\System32\wsock32.dll	0x00C40000	0x00009000
C:\WINDOWS\System32\WS2_32.dll	0x00C50000	0x00015000
C:\WINDOWS\System32\WS2HELP.dll	0x00C70000	0x00008000
C:\WINDOWS\System32\wshtcpip.dll	0x00C80000	0x00008000

Run-time Dlls

Module Name	Base Address	Size
C:\WINDOWS\system32\mswsock.dll	0x00EA0000	0x0003C000
C:\WINDOWS\System32\UxTheme.dll	0x5B0F0000	0x00034000
C:\Programme\Java\jre1.6.0_07\bin\ssv.dll	0x6D7C0000	0x0007B000
C:\WINDOWS\System32\NETAPI32.dll	0x71BA0000	0x0004F000
C:\WINDOWS\System32\browselc.dll	0x723C0000	0x00013000
C:\WINDOWS\System32\MSLS31.DLL	0x74640000	0x00027000
C:\WINDOWS\System32\msimtf.dll	0x74670000	0x00029000
C:\WINDOWS\System32\MSCTF.dll	0x746A0000	0x0004B000
C:\WINDOWS\System32\mlang.dll	0x746F0000	0x0008F000
C:\WINDOWS\System32\mshtml.dll	0x74790000	0x002AD000
C:\WINDOWS\system32\USERENV.dll	0x75A10000	0x000A5000
C:\WINDOWS\System32\jscript.dll	0x75BF0000	0x00091000
C:\WINDOWS\system32\appHelp.dll	0x75EE0000	0x0001D000
C:\WINDOWS\System32\BROWSEUI.dll	0x75F20000	0x000FC000
C:\WINDOWS\system32\urlmon.dll	0x76090000	0x00078000
C:\WINDOWS\system32\shdoclc.dll	0x76110000	0x0008E000
C:\WINDOWS\system32\WININET.dll	0x761A0000	0x00098000
C:\WINDOWS\system32\MSASN1.dll	0x76240000	0x0000F000
C:\WINDOWS\system32\CRYPT32.dll	0x76260000	0x0008B000
C:\WINDOWS\System32\IMM32.DLL	0x76330000	0x0001A000
C:\WINDOWS\System32\CSCDLL.dll	0x765A0000	0x0001B000
C:\WINDOWS\System32\cscui.dll	0x765C0000	0x00050000
C:\WINDOWS\System32\SETUPAPI.dll	0x76620000	0x000E5000
C:\WINDOWS\System32\shfolder.dll	0x76730000	0x00008000
C:\WINDOWS\System32\WINMM.dll	0x76AF0000	0x0002D000
C:\WINDOWS\System32\rtutils.dll	0x76E40000	0x0000D000
C:\WINDOWS\System32\rasman.dll	0x76E50000	0x00011000
C:\WINDOWS\System32\TAPI32.dll	0x76E70000	0x0002A000
C:\WINDOWS\System32\RASAPI32.DLL	0x76EA0000	0x00037000
C:\WINDOWS\System32\DNSAPI.dll	0x76EE0000	0x00025000
C:\WINDOWS\system32\WLDAP32.dll	0x76F20000	0x0002D000
C:\WINDOWS\System32\Secur32.dll	0x76F50000	0x00010000
C:\WINDOWS\System32\winrnr.dll	0x76F70000	0x00007000
C:\WINDOWS\System32\rasadhlp.dll	0x76F80000	0x00005000
C:\WINDOWS\System32\CLBCATQ.DLL	0x76F90000	0x00078000
C:\WINDOWS\System32\COMRes.dll	0x77010000	0x000D3000
C:\WINDOWS\system32\OLEAUT32.dll	0x770F0000	0x0008B000
C:\WINDOWS\system32\ole32.dll	0x77180000	0x0011A000
C:\WINDOWS\system32\comctl32.dll	0x77310000	0x0008B000
C:\WINDOWS\system32\SHELL32.dll	0x773A0000	0x007FE000
C:\WINDOWS\system32\VERSION.dll	0x77BD0000	0x00007000
C:\Programme\Java\jre1.6.0_07\bin\MSVCR71.dll	0x7C340000	0x00056000

2.a) iexplore.exe - Registry Activities

Registry Keys Created:

HKU\S-1-5-21-1343024091-1292428093-1606980848-500\Software\Microsoft\Windows\ShellNoRoam\\BagMRU
HKU\S-1-5-21-1343024091-1292428093-1606980848-500\Software\Microsoft\Windows\ShellNoRoam\MUICache
HKU\S-1-5-21-1343024091-1292428093-1606980848-500\Software\Microsoft\Windows\ShellNoRoam\\BagMRU\0
HKU\S-1-5-21-1343024091-1292428093-1606980848-500\Software\Microsoft\Windows\ShellNoRoam\\Bags
HKU\S-1-5-21-1343024091-1292428093-1606980848-500\Software\Microsoft\Windows\ShellNoRoam\\Bags\1
HKU\S-1-5-21-1343024091-1292428093-1606980848-500\Software\Microsoft\Windows\ShellNoRoam\\Bags\1\Shell

Registry Keys Deleted:

HKU\S-1-5-21-1343024091-1292428093-1606980848-500\Software\Microsoft\Windows\ShellNoRoam\\MUICache

Registry Keys Deleted:

HKU\S-1-5-21-1343024091-1292428093-1606980848-500\Software\Microsoft\Windows\ShellNoRoam\\DUIBags\ShellFolders\ {F3364BA0-65B9-11CE-A9BA-00AA004AE837}
HKU\S-1-5-21-1343024091-1292428093-1606980848-500\Software\Microsoft\Windows\ShellNoRoam\\DUIBags\ShellFolders\ {7007ACC7-3202-11D1-AAD2-00805FC1270E}
HKU\S-1-5-21-1343024091-1292428093-1606980848-500\Software\Microsoft\Windows\ShellNoRoam\\DUIBags\ShellFolders\ {21EC2020-3AEA-1069-A2DD-08002B30309D}
HKU\S-1-5-21-1343024091-1292428093-1606980848-500\Software\Microsoft\Windows\ShellNoRoam\\DUIBags\ShellFolders\ {20D04FE0-3AEA-1069-A2D8-08002B30309D}
HKU\S-1-5-21-1343024091-1292428093-1606980848-500\Software\Microsoft\Windows\ShellNoRoam\\DUIBags\ShellFolders
HKU\S-1-5-21-1343024091-1292428093-1606980848-500\Software\Microsoft\Windows\ShellNoRoam\\DUIBags
HKU\S-1-5-21-1343024091-1292428093-1606980848-500\Software\Microsoft\Windows\ShellNoRoam\\Bags\7\Shell
HKU\S-1-5-21-1343024091-1292428093-1606980848-500\Software\Microsoft\Windows\ShellNoRoam\\Bags\7
HKU\S-1-5-21-1343024091-1292428093-1606980848-500\Software\Microsoft\Windows\ShellNoRoam\\Bags\6\Shell
HKU\S-1-5-21-1343024091-1292428093-1606980848-500\Software\Microsoft\Windows\ShellNoRoam\\Bags\6
HKU\S-1-5-21-1343024091-1292428093-1606980848-500\Software\Microsoft\Windows\ShellNoRoam\\Bags\5\Shell
HKU\S-1-5-21-1343024091-1292428093-1606980848-500\Software\Microsoft\Windows\ShellNoRoam\\Bags\5
HKU\S-1-5-21-1343024091-1292428093-1606980848-500\Software\Microsoft\Windows\ShellNoRoam\\Bags\4\Shell
HKU\S-1-5-21-1343024091-1292428093-1606980848-500\Software\Microsoft\Windows\ShellNoRoam\\Bags\4
HKU\S-1-5-21-1343024091-1292428093-1606980848-500\Software\Microsoft\Windows\ShellNoRoam\\Bags\3\Shell
HKU\S-1-5-21-1343024091-1292428093-1606980848-500\Software\Microsoft\Windows\ShellNoRoam\\Bags\3
HKU\S-1-5-21-1343024091-1292428093-1606980848-500\Software\Microsoft\Windows\ShellNoRoam\\Bags\2\Shell
HKU\S-1-5-21-1343024091-1292428093-1606980848-500\Software\Microsoft\Windows\ShellNoRoam\\Bags\2
HKU\S-1-5-21-1343024091-1292428093-1606980848-500\Software\Microsoft\Windows\ShellNoRoam\\Bags\1\Shell
HKU\S-1-5-21-1343024091-1292428093-1606980848-500\Software\Microsoft\Windows\ShellNoRoam\\Bags\1
HKU\S-1-5-21-1343024091-1292428093-1606980848-500\Software\Microsoft\Windows\ShellNoRoam\\Bags
HKU\S-1-5-21-1343024091-1292428093-1606980848-500\Software\Microsoft\Windows\ShellNoRoam\\BagMRU\2
HKU\S-1-5-21-1343024091-1292428093-1606980848-500\Software\Microsoft\Windows\ShellNoRoam\\BagMRU\1
HKU\S-1-5-21-1343024091-1292428093-1606980848-500\Software\Microsoft\Windows\ShellNoRoam\\BagMRU\0\2
HKU\S-1-5-21-1343024091-1292428093-1606980848-500\Software\Microsoft\Windows\ShellNoRoam\\BagMRU\0\1
HKU\S-1-5-21-1343024091-1292428093-1606980848-500\Software\Microsoft\Windows\ShellNoRoam\\BagMRU\0\0\0
HKU\S-1-5-21-1343024091-1292428093-1606980848-500\Software\Microsoft\Windows\ShellNoRoam\\BagMRU\0\0
HKU\S-1-5-21-1343024091-1292428093-1606980848-500\Software\Microsoft\Windows\ShellNoRoam\\BagMRU\0
HKU\S-1-5-21-1343024091-1292428093-1606980848-500\Software\Microsoft\Windows\ShellNoRoam\\BagMRU

Registry Values Deleted:

Key	Name
HKU\S-1-5-21-1343024091-1292428093-1606980848-500\Software\Microsoft\Windows\ ShellNoRoam	

Registry Values Modified:

Key	Name	New Value
HKU\S-1-5-21-1343024091-1292428093-1606980848-500\Software\ Microsoft\Windows\ShellNoRoam		
HKU\S-1-5-21-1343024091-1292428093-1606980848-500\Software\ Microsoft\Windows\ShellNoRoam\MUICache	LangID	0x0704
HKU\S-1-5-21-1343024091-1292428093-1606980848-500\Software\ Microsoft\Windows\ShellNoRoam\\BagMRU	0	0x14001f0080531c87a0426910a2ea08002 2b30309d0000
HKU\S-1-5-21-1343024091-1292428093-1606980848-500\Software\ Microsoft\Windows\ShellNoRoam\\BagMRU\0	NodeSlot	1
HKU\S-1-5-21-1343024091-1292428093-1606980848-500\Software\ Microsoft\Windows\ShellNoRoam\\Bags\1\Shell	Address	4294967295
HKU\S-1-5-21-1343024091-1292428093-1606980848-500\Software\ Microsoft\Windows\ShellNoRoam\\Bags\1\Shell	Buttons	4294967295
HKU\S-1-5-21-1343024091-1292428093-1606980848-500\Software\ Microsoft\Windows\ShellNoRoam\\Bags\1\Shell	FFlags	0
HKU\S-1-5-21-1343024091-1292428093-1606980848-500\Software\ Microsoft\Windows\ShellNoRoam\\Bags\1\Shell	HotKey	0
HKU\S-1-5-21-1343024091-1292428093-1606980848-500\Software\ Microsoft\Windows\ShellNoRoam\\Bags\1\Shell	Links	4294967295

Registry Values Modified:

Key	Name	New Value
HKU\S-1-5-21-1343024091-1292428093-1606980848-500\Software\Microsoft\Windows\ShellNoRoam\\Bags\1\Shell	MaxPos800x600(1).x	4294967295
HKU\S-1-5-21-1343024091-1292428093-1606980848-500\Software\Microsoft\Windows\ShellNoRoam\\Bags\1\Shell	MaxPos800x600(1).y	4294967295
HKU\S-1-5-21-1343024091-1292428093-1606980848-500\Software\Microsoft\Windows\ShellNoRoam\\Bags\1\Shell	MinPos800x600(1).x	4294967295
HKU\S-1-5-21-1343024091-1292428093-1606980848-500\Software\Microsoft\Windows\ShellNoRoam\\Bags\1\Shell	MinPos800x600(1).y	4294967295
HKU\S-1-5-21-1343024091-1292428093-1606980848-500\Software\Microsoft\Windows\ShellNoRoam\\Bags\1\Shell	Rev	0
HKU\S-1-5-21-1343024091-1292428093-1606980848-500\Software\Microsoft\Windows\ShellNoRoam\\Bags\1\Shell	ShowCmd	1
HKU\S-1-5-21-1343024091-1292428093-1606980848-500\Software\Microsoft\Windows\ShellNoRoam\\Bags\1\Shell	Status	4294967295
HKU\S-1-5-21-1343024091-1292428093-1606980848-500\Software\Microsoft\Windows\ShellNoRoam\\Bags\1\Shell	WFlags	0
HKU\S-1-5-21-1343024091-1292428093-1606980848-500\Software\Microsoft\Windows\ShellNoRoam\\Bags\1\Shell	WinPos800x600(1).bot	570
HKU\S-1-5-21-1343024091-1292428093-1606980848-500\Software\Microsoft\Windows\ShellNoRoam\\Bags\1\Shell	WinPos800x600(1).left	0
HKU\S-1-5-21-1343024091-1292428093-1606980848-500\Software\Microsoft\Windows\ShellNoRoam\\Bags\1\Shell	WinPos800x600(1).righ	800
HKU\S-1-5-21-1343024091-1292428093-1606980848-500\Software\Microsoft\Windows\ShellNoRoam\\Bags\1\Shell	WinPos800x600(1).top	0

Registry Values Read:

Key	Name	Value	Times
HKLM\SYSTEM\CurrentControlSet\Control\Session Manager	CriticalSectionTimeout	2592000	1
HKLM\SYSTEM\CurrentControlSet\Services\Winsock\Parameters	Transports	0x5400630070006900700000004e0065007 7400420049004f00530000000000	2
HKLM\SYSTEM\Setup	OsLoaderPath	\	2
HKLM\SYSTEM\Setup	SystemPartition	\Device\HarddiskVolume1	2
HKLM\Software\Microsoft\Internet Explorer\URL Compatibility\~/CONNWIZ.HTM	Compatibility Flags	4	1
HKLM\Software\Microsoft\Internet Explorer\URL Compatibility\~/CWIZINTR.HTM	Compatibility Flags	4	1
HKLM\Software\Microsoft\Windows\CurrentVersion	DevicePath	%SystemRoot%\inf	1
HKLM\Software\Microsoft\Windows\CurrentVersion\App Paths\ICWCONN1.EXE	Path	C:\Programme\Internet Explorer\Connection Wizard;	1
HKLM\Software\Microsoft\Windows\CurrentVersion\Setup	DriverCachePath	%SystemRoot%\Driver Cache	2
HKLM\Software\Microsoft\Windows\CurrentVersion\Setup	ServicePackSourcePat	D:\	2
HKLM\Software\Microsoft\Windows\CurrentVersion\Setup	SourcePath	D:\	2
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\WPA\PnP	seed	3051945280	1
HKLM\System\CurrentControlSet\Services\LDAP	LdapClientIntegrity	1	1
HKLM\System\CurrentControlSet\Services\Tcpip\Parameters	UseDomainNameDevo	1	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

Registry Values Read:

Key	Name	Value	Times
HKU\ S-1-5-21-1343024091-1292428093-1606980848-500\ Keyboard Layout\Toggle	Language Hotkey	1	2
HKU\ S-1-5-21-1343024091-1292428093-1606980848-500\ Keyboard Layout\Toggle	Layout Hotkey	2	2
HKU\ S-1-5-21-1343024091-1292428093-1606980848-500\ Software\Microsoft\Windows\CurrentVersion\Explorer\ User Shell Folders	Local Settings	%USERPROFILE%\Lokale Einstellungen	1
HKU\ S-1-5-21-1343024091-1292428093-1606980848-500\ Software\Microsoft\Windows\CurrentVersion\Explorer\ User Shell Folders	Personal	%USERPROFILE%\Eigene Dateien	1
HKU\ S-1-5-21-1343024091-1292428093-1606980848-500\ Software\Microsoft\Windows\ShellNoRoam	TU-D8OIR705F1MD	TU-D8OIR705F1MD	1

2.b) iexplore.exe - File Activities

Files Deleted:

C:\Dokumente und Einstellungen\Administrator\Lokale Einstellungen\Temporary Internet Files\Content.IE5\C4ESWJ2L\urchin[1].js
C:\Dokumente und Einstellungen\Administrator\Lokale Einstellungen\Temporary Internet Files\Content.IE5\YIQUT0RH\show_ads[1].js

Files Created:

C:\Dokumente und Einstellungen\Administrator\Cookies\administrator@colorblender[1].txt
C:\Dokumente und Einstellungen\Administrator\Lokale Einstellungen\Temporary Internet Files\Content.IE5\C4ESWJ2L\bluecurve[1].css
C:\Dokumente und Einstellungen\Administrator\Lokale Einstellungen\Temporary Internet Files\Content.IE5\C4ESWJ2L\tabs[1].gif
C:\Dokumente und Einstellungen\Administrator\Lokale Einstellungen\Temporary Internet Files\Content.IE5\C4ESWJ2L\urchin[1].js
C:\Dokumente und Einstellungen\Administrator\Lokale Einstellungen\Temporary Internet Files\Content.IE5\CHT2SY0U\blendercore[1].asp
C:\Dokumente und Einstellungen\Administrator\Lokale Einstellungen\Temporary Internet Files\Content.IE5\CHT2SY0U\colorblender[1]
C:\Dokumente und Einstellungen\Administrator\Lokale Einstellungen\Temporary Internet Files\Content.IE5\CHT2SY0U\colorblender[1].gif
C:\Dokumente und Einstellungen\Administrator\Lokale Einstellungen\Temporary Internet Files\Content.IE5\OTAFWPMF\backdrop[1].gif
C:\Dokumente und Einstellungen\Administrator\Lokale Einstellungen\Temporary Internet Files\Content.IE5\OTAFWPMF\colorblender[1].css
C:\Dokumente und Einstellungen\Administrator\Lokale Einstellungen\Temporary Internet Files\Content.IE5\OTAFWPMF\grred[1].gif
C:\Dokumente und Einstellungen\Administrator\Lokale Einstellungen\Temporary Internet Files\Content.IE5\YIQUT0RH\show_ads[1].js
C:\Dokumente und Einstellungen\Administrator\Lokale Einstellungen\Temporary Internet Files\Content.IE5\YIQUT0RH\show_ads[2].js
C:\Dokumente und Einstellungen\Administrator\Lokale Einstellungen\Temporary Internet Files\Content.IE5\YIQUT0RH\urchin[1].js

Files Read:

C:\Dokumente und Einstellungen\Administrator\Lokale Einstellungen\Temporary Internet Files\Content.IE5\C4ESWJ2L\bluecurve[1].css
C:\Dokumente und Einstellungen\Administrator\Lokale Einstellungen\Temporary Internet Files\Content.IE5\OTAFWPMF\colorblender[1].css
C:\Dokumente und Einstellungen\Administrator\Lokale Einstellungen\Temporary Internet Files\Content.IE5\YIQUT0RH\show_ads[2].js
C:\Dokumente und Einstellungen\Administrator\Lokale Einstellungen\Temporary Internet Files\Content.IE5\YIQUT0RH\urchin[1].js

Files Modified:

C:\Dokumente und Einstellungen\Administrator\Cookies\administrator@colorblender[1].txt
C:\Dokumente und Einstellungen\Administrator\Lokale Einstellungen\Temporary Internet Files\Content.IE5\C4ESWJ2L\bluecurve[1].css
C:\Dokumente und Einstellungen\Administrator\Lokale Einstellungen\Temporary Internet Files\Content.IE5\C4ESWJ2L\tabs[1].gif
C:\Dokumente und Einstellungen\Administrator\Lokale Einstellungen\Temporary Internet Files\Content.IE5\C4ESWJ2L\urchin[1].js
C:\Dokumente und Einstellungen\Administrator\Lokale Einstellungen\Temporary Internet Files\Content.IE5\CHT2SY0U\blendercore[1].asp
C:\Dokumente und Einstellungen\Administrator\Lokale Einstellungen\Temporary Internet Files\Content.IE5\CHT2SY0U\colorblender[1]
C:\Dokumente und Einstellungen\Administrator\Lokale Einstellungen\Temporary Internet Files\Content.IE5\CHT2SY0U\colorblender[1].gif
C:\Dokumente und Einstellungen\Administrator\Lokale Einstellungen\Temporary Internet Files\Content.IE5\OTAFWPMF\backdrop[1].gif
C:\Dokumente und Einstellungen\Administrator\Lokale Einstellungen\Temporary Internet Files\Content.IE5\OTAFWPMF\colorblender[1].css
C:\Dokumente und Einstellungen\Administrator\Lokale Einstellungen\Temporary Internet Files\Content.IE5\OTAFWPMF\grred[1].gif
C:\Dokumente und Einstellungen\Administrator\Lokale Einstellungen\Temporary Internet Files\Content.IE5\YIQUT0RH\show_ads[1].js

Files Modified:

C:\Dokumente und Einstellungen\Administrator\Lokale Einstellungen\Temporary Internet Files\Content.IE5\YIQUT0RH\show_ads[2].js
C:\Dokumente und Einstellungen\Administrator\Lokale Einstellungen\Temporary Internet Files\Content.IE5\YIQUT0RH\urchin[1].js
C:\WINDOWS\Debug\UserMode\userenv.log
\Device\Afd\Endpoint

Device Control Communication:

File	Control Code	Times
\Device\KsecDD	0x00390008	8

Memory Mapped Files:

File Name
C:\Programme\Java\jre1.6.0_07\bin\MSVCR71.dll
C:\Programme\Java\jre1.6.0_07\bin\ssv.dll
C:\WINDOWS\System32\BROWSEUI.dll
C:\WINDOWS\System32\CLBCATQ.DLL
C:\WINDOWS\System32\COMRes.dll
C:\WINDOWS\System32\CSCDLL.dll
C:\WINDOWS\System32\DNSAPI.dll
C:\WINDOWS\System32\IMM32.DLL
C:\WINDOWS\System32\MSCTF.dll
C:\WINDOWS\System32\MSLS31.DLL
C:\WINDOWS\System32\NETAPI32.dll
C:\WINDOWS\System32\RASAPI32.DLL
C:\WINDOWS\System32\SETUPAPI.dll
C:\WINDOWS\System32\Secur32.dll
C:\WINDOWS\System32\TAPI32.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\browselc.dll
C:\WINDOWS\System32\cscui.dll
C:\WINDOWS\System32\jscript.dll
C:\WINDOWS\System32\mlang.dll
C:\WINDOWS\System32\msimtf.dll
C:\WINDOWS\System32\rasadhlp.dll
C:\WINDOWS\System32\rasman.dll
C:\WINDOWS\System32\rtutils.dll
C:\WINDOWS\System32\shdoclc.dll
C:\WINDOWS\System32\shfolder.dll
C:\WINDOWS\System32\winrnr.dll
C:\WINDOWS\System32\wshtcpip.dll
C:\WINDOWS\System32\wsock32.dll
C:\WINDOWS\system32\WININET.dll
C:\WINDOWS\system32\mswsock.dll
C:\WINDOWS\system32\shdoclc.dll
C:\WINDOWS\system32\urlmon.dll

2.d) iexplore.exe - Network Activity

DNS Queries:

Name	Query Type	Query Result	Successful	Protocol
www.colorblender.com	DNS_TYPE_A	66.226.89.239	1	
www.google-analytics.com	DNS_TYPE_A		1	
pagead2.googlesyndication.	DNS_TYPE_A		1	

HTTP Conversations:
From ANUBIS:1034 to 66.226.89.239:80 - [www.colorblender.com]
Request: GET /
Response: 200 "OK"
Request: GET /js/range.js
Response: 404 "Not Found"
Request: GET /js/timer.js
Response: 404 "Not Found"
Request: GET /js/slider.js
Response: 404 "Not Found"
Request: GET /css/bluecurve/bluecurve.css
Response: 200 "OK"
Request: GET /colorblender.css
Response: 200 "OK"
Request: GET /colorblender.gif
Response: 200 "OK"
Request: GET /backdrop.gif
Response: 200 "OK"
Request: GET /blendercore.asp
Response: 200 "OK"
Request: GET /tabs.gif
Response: 200 "OK"
Request: GET /grred.gif
Response: 200 "OK"
From ANUBIS:1039 to 74.125.87.100:80 - [www.google-analytics.com]
Request: GET /urchin.js
Response: 200 "OK"
From ANUBIS:1040 to 74.125.87.164:80 - [pagead2.googlesyndication.com]
Request: GET /pagead/show_ads.js
Response: 200 "OK"

TCP Connection Attempts:
From ANUBIS:1035 to 66.226.89.239:80
From ANUBIS:1036 to 66.226.89.239:80
From ANUBIS:1037 to 66.226.89.239:80
From ANUBIS:1038 to 66.226.89.239:80

2.e) iexplore.exe - Other Activities

Mutexes Created:
MSCTF.Shared.MUTEX.AFF
MSCTF.TimListMUTEX.
MSUIM.Assembly.Mutex
MSUIM.GlobalCompartment.Mutex
MSUIM.GlobalLangBarEventSink.Mutex
MSUIM.Layouts.Mutex
MSUIM.MarshalInterfaceMutex.TMD
ZonesCacheCounterMutex
ZonesCounterMutex
_SHuassist.mtx

Keyboard Keys Monitored:

Virtual Key Code	Times
VK_CONTROL (17)	37
VK_ESCAPE (27)	23
VK_LBUTTON (1)	75
VK_SHIFT (16)	37

Keyboard Keys Monitored:

Virtual Key Code	Times
VK_MENU (18)	36
VK_LSHIFT (160)	23
VK_LCONTROL (162)	23
VK_LMENU (164)	23
VK_RBUTTON (2)	13
VK_MBUTTON (4)	13

Windows SEH exceptions:

Description	Times
Exception 0x6a6 at 0x77e4d756	103