Anubis - Analysis Report

Analysis Report for 43854473

MD5: 53fea0377fa2b3448b1b0de521631334

Summary:

Description	Risk
Write to foreign memory areas: This executable tampers with the execution of another process.	high
Performs File Modification and Destruction: The executable modifies and destructs files which are not temporary.	low
AV Hit: This executable is detected by an antivirus software.	high
Autostart capabilities: This executable registers processes to be executed at system start. This could result in unwanted actions to be performed automatically.	medium
Performs Registry Activities: The executable creates and/or modifies registry entries.	low

Dependency overview:

- **43854473.exe** C:\43854473.exe
  - Analysis reason: Primary Analysis Subject
  - **Explorer.EXE** C:\WINDOWS\Explorer.EXE
    - Analysis reason: 43854473.exe wrote to the virtual memory of this process
  - **ctfmon.exe** C:\WINDOWS\system32\ctfmon.exe
    - Analysis reason: 43854473.exe wrote to the virtual memory of this process

Table of Contents:

1. General Information.... 4
2. 43854473.exe.... 4
   a) Registry Activities.... 4
   b) File Activities.... 5
   c) Process Activities.... 5
3. Explorer.EXE.... 5
   a) Registry Activities.... 7
   b) File Activities.... 10
   c) Network Activities.... 11
   d) Other Activities.... 11
4. ctfmon.exe.... 11
   a) Registry Activities.... 11
   b) Process Activities.... 12

1. General Information

Information about Anubis' invocation	
Time needed:	253 s
Report created:	04/20/11, 13:25:11 UTC
Termination reason:	Timeout
Program version:	1.75.3394

2. 43854473.exe

General information about this executable	
Analysis Reason:	Primary Analysis Subject
Filename:	43854473.exe
MD5:	53fea0377fa2b3448b1b0de521631334
SHA-1:	0dc9b9b72c3537c5d9ad03ae5828c46cbadebd0f
File Size:	89600
Command Line:	"C:\43854473.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

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\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\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\user32.dll	0x7E410000	0x00091000

Ikarus Virus Scanner

P2P-Worm.Win32.Palevo (Sig-Id:465868)

2.a) 43854473.exe - Registry Activities

Registry Values Read:

Key	Name	Value	Times
HKLM\SYSTEM\CurrentControlSet\Control\Session Manager	CriticalSectionTimeout	2592000	1
HKLM\SYSTEM\Setup	SystemSetupInProgres	0	1

Registry Values Read:

Key	Name	Value	Times
HKLM\Software\Policies\Microsoft\Windows\Safer\CodeIdentifiers	TransparentEnabled	1	1
HKLM\System\CurrentControlSet\Control\Terminal Server	TSUserEnabled	0	1

2.b) 43854473.exe - File Activities

Files Created:

C:\RECYCLER\S-1-5-21-8884004121-5077429001-432226802-9869
C:\RECYCLER\S-1-5-21-8884004121-5077429001-432226802-9869\Desktop.ini

Files Modified:

C:\RECYCLER\S-1-5-21-8884004121-5077429001-432226802-9869\Desktop.ini

Directories Created:

C:\RECYCLER\S-1-5-21-8884004121-5077429001-432226802-9869

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\WS2HELP.dll
C:\WINDOWS\system32\comctl32.dll
C:\WINDOWS\system32\shell32.dll
C:\WINDOWS\system32\wininet.dll
C:\WINDOWS\system32\ws2_32.dll

2.c) 43854473.exe - Process Activities

Remote Threads Created:

Affected Process
C:\WINDOWS\explorer.exe
C:\WINDOWS\system32\ctfmon.exe

Foreign Memory Regions Written:

Process: C:\WINDOWS\explorer.exe
Process: C:\WINDOWS\system32\ctfmon.exe

3. Explorer.EXE

General information about this executable

Analysis Reason:	43854473.exe wrote to the virtual memory of this process
Filename:	Explorer.EXE
MD5:	12896823fb95bfb3dc9b46bcaedc9923
SHA-1:	9d2bf84874abc5b6e9a2744b7865c193c08d362f

General information about this executable

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
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

Load-time Dlls

Module Name	Base Address	Size
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\eappcfg.dll	0x745B0000	0x00022000
C:\WINDOWS\system32\MSVCP60.dll	0x76080000	0x00065000
C:\WINDOWS\system32\eappprxy.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\browselc.dll	0x71600000	0x00012000
C:\WINDOWS\system32\shdoclc.dll	0x71800000	0x00088000

Run-time Dlls

Module Name	Base Address	Size
C:\WINDOWS\system32\hnetcfg.dll	0x662B0000	0x00058000
C:\WINDOWS\system32\mswsock.dll	0x71A50000	0x0003F000
C:\WINDOWS\System32\wshtcpip.dll	0x71A90000	0x00008000
C:\WINDOWS\system32\DNSAPI.dll	0x76F20000	0x00027000
C:\WINDOWS\System32\winrnr.dll	0x76FB0000	0x00008000
C:\WINDOWS\system32\rasadhlp.dll	0x76FC0000	0x00006000

3.a) Explorer.EXE - Registry Activities

Registry Values Modified:

Key	Name	New Value
HKU\S-1-5-21-842925246-1425521274-308236825-500\Software\Microsoft\Windows\CurrentVersion\Run	Windows Video Drivers	C:\RECYCLER\S-1-5-21-8884004121-5077429001-432226802-9869\winlogon.exe

Registry Values Read:

Key	Name	Value	Times
HKLM\SYSTEM\CurrentControlSet\Services\Winsock\Parameters	Transports	0x540063007000690070000000 4e0065007 7400420049004f00530000000000	2

Registry Values Read:

Key	Name	Value	Times
HKLM\System\CurrentControlSet\Services\Tcpip\Parameters	Domain		2
HKLM\System\CurrentControlSet\Services\Tcpip\Parameters	Hostname	pc	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	2
HKLM\System\CurrentControlSet\Services\WinSock2\Parameters\NameSpace_Catalog5\Catalog_Entries\000000000001	DisplayString	Tcpip	4
HKLM\System\CurrentControlSet\Services\WinSock2\Parameters\NameSpace_Catalog5\Catalog_Entries\000000000001	Enabled	1	1
HKLM\System\CurrentControlSet\Services\WinSock2\Parameters\NameSpace_Catalog5\Catalog_Entries\000000000001	LibraryPath	%SystemRoot%\System32\mswsock.dll	2
HKLM\System\CurrentControlSet\Services\WinSock2\Parameters\NameSpace_Catalog5\Catalog_Entries\000000000001	ProviderId	0x409d05229e7ecf11ae5a00aa00a7112b	1
HKLM\System\CurrentControlSet\Services\WinSock2\Parameters\NameSpace_Catalog5\Catalog_Entries\000000000001	StoresServiceClassInfo	0	1
HKLM\System\CurrentControlSet\Services\WinSock2\Parameters\NameSpace_Catalog5\Catalog_Entries\000000000001	SupportedNameSpace	12	1
HKLM\System\CurrentControlSet\Services\WinSock2\Parameters\NameSpace_Catalog5\Catalog_Entries\000000000001	Version	0	1
HKLM\System\CurrentControlSet\Services\WinSock2\Parameters\NameSpace_Catalog5\Catalog_Entries\000000000002	DisplayString	NTDS	4
HKLM\System\CurrentControlSet\Services\WinSock2\Parameters\NameSpace_Catalog5\Catalog_Entries\000000000002	Enabled	1	1
HKLM\System\CurrentControlSet\Services\WinSock2\Parameters\NameSpace_Catalog5\Catalog_Entries\000000000002	LibraryPath	%SystemRoot%\System32\winrnr.dll	2
HKLM\System\CurrentControlSet\Services\WinSock2\Parameters\NameSpace_Catalog5\Catalog_Entries\000000000002	ProviderId	0xee37263b80e5cf11a55500c04fd8d4ac	1
HKLM\System\CurrentControlSet\Services\WinSock2\Parameters\NameSpace_Catalog5\Catalog_Entries\000000000002	StoresServiceClassInfo	0	1
HKLM\System\CurrentControlSet\Services\WinSock2\Parameters\NameSpace_Catalog5\Catalog_Entries\000000000002	SupportedNameSpace	32	1
HKLM\System\CurrentControlSet\Services\WinSock2\Parameters\NameSpace_Catalog5\Catalog_Entries\000000000002	Version	0	1

Registry Values Read:

Key	Name	Value	Times
HKLM\System\CurrentControlSet\Services\WinSock2\Parameters\NameSpace_Catalog5\Catalog_Entries\000000000003	DisplayString	Network Location Awareness (NLA) Namespace	4
HKLM\System\CurrentControlSet\Services\WinSock2\Parameters\NameSpace_Catalog5\Catalog_Entries\000000000003	Enabled	1	1
HKLM\System\CurrentControlSet\Services\WinSock2\Parameters\NameSpace_Catalog5\Catalog_Entries\000000000003	LibraryPath	%SystemRoot%\System32\mswsock.dll	2
HKLM\System\CurrentControlSet\Services\WinSock2\Parameters\NameSpace_Catalog5\Catalog_Entries\000000000003	ProviderId	0x3a244266a83ba64abaa52e0bd71fdd83	1
HKLM\System\CurrentControlSet\Services\WinSock2\Parameters\NameSpace_Catalog5\Catalog_Entries\000000000003	StoresServiceClassInfo	0	1
HKLM\System\CurrentControlSet\Services\WinSock2\Parameters\NameSpace_Catalog5\Catalog_Entries\000000000003	SupportedNameSpace	15	1
HKLM\System\CurrentControlSet\Services\WinSock2\Parameters\NameSpace_Catalog5\Catalog_Entries\000000000003	Version	0	1
HKLM\System\CurrentControlSet\Services\WinSock2\Parameters\Protocol_Catalog9	Next_Catalog_Entry_ID	1020	1
HKLM\System\CurrentControlSet\Services\WinSock2\Parameters\Protocol_Catalog9	Num_Catalog_Entries	13	1
HKLM\System\CurrentControlSet\Services\WinSock2\Parameters\Protocol_Catalog9	Serial_Access_Num	6	2
HKLM\System\CurrentControlSet\Services\WinSock2\Parameters\Protocol_Catalog9\Catalog_Entries\000000000001	PackedCatalogItem	%SystemRoot%\system32\mswsock.	1
HKLM\System\CurrentControlSet\Services\WinSock2\Parameters\Protocol_Catalog9\Catalog_Entries\000000000002	PackedCatalogItem	%SystemRoot%\system32\mswsock.	1
HKLM\System\CurrentControlSet\Services\WinSock2\Parameters\Protocol_Catalog9\Catalog_Entries\000000000003	PackedCatalogItem	%SystemRoot%\system32\mswsock.	1
HKLM\System\CurrentControlSet\Services\WinSock2\Parameters\Protocol_Catalog9\Catalog_Entries\000000000004	PackedCatalogItem	%SystemRoot%\system32\rsvpsp.d	1
HKLM\System\CurrentControlSet\Services\WinSock2\Parameters\Protocol_Catalog9\Catalog_Entries\000000000005	PackedCatalogItem	%SystemRoot%\system32\rsvpsp.d	1
HKLM\System\CurrentControlSet\Services\WinSock2\Parameters\Protocol_Catalog9\Catalog_Entries\000000000006	PackedCatalogItem	%SystemRoot%\system32\mswsock.	1
HKLM\System\CurrentControlSet\Services\WinSock2\Parameters\Protocol_Catalog9\Catalog_Entries\000000000007	PackedCatalogItem	%SystemRoot%\system32\mswsock.	1
HKLM\System\CurrentControlSet\Services\WinSock2\Parameters\Protocol_Catalog9\Catalog_Entries\000000000008	PackedCatalogItem	%SystemRoot%\system32\mswsock.	1
HKLM\System\CurrentControlSet\Services\WinSock2\Parameters\Protocol_Catalog9\Catalog_Entries\000000000009	PackedCatalogItem	%SystemRoot%\system32\mswsock.	1
HKLM\System\CurrentControlSet\Services\WinSock2\Parameters\Protocol_Catalog9\Catalog_Entries\000000000010	PackedCatalogItem	%SystemRoot%\system32\mswsock.	1
HKLM\System\CurrentControlSet\Services\WinSock2\Parameters\Protocol_Catalog9\Catalog_Entries\000000000011	PackedCatalogItem	%SystemRoot%\system32\mswsock.	1
HKLM\System\CurrentControlSet\Services\WinSock2\Parameters\Protocol_Catalog9\Catalog_Entries\000000000012	PackedCatalogItem	%SystemRoot%\system32\mswsock.	1
HKLM\System\CurrentControlSet\Services\WinSock2\Parameters\Protocol_Catalog9\Catalog_Entries\000000000013	PackedCatalogItem	%SystemRoot%\system32\mswsock.	1

Registry Values Read:

Key	Name	Value	Times
HKLM\System\Setup	SystemSetupInProgres	0	1

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

3.b) Explorer.EXE - File Activities

Files Created:

C:\RECYCLER\S-1-5-21-8884004121-5077429001-432226802-9869\winlogon.exe
pipe\FhtGvbkgl87F

Files Read:

PIPE\lsarpc

Files Modified:

C:\RECYCLER\S-1-5-21-8884004121-5077429001-432226802-9869\winlogon.exe
PIPE\lsarpc
\Device\Afd\Endpoint
\Device\RasAcd

File System Control Communication:

File	Control Code	Times
PIPE\lsarpc	0x0011C017	3

Device Control Communication:

File	Control Code	Times
\Device\Afd\Endpoint	AFD_GET_INFO (0x0001207B)	2
\Device\Afd\Endpoint	AFD_SET_CONTEXT (0x00012047)	4
\Device\Afd\Endpoint	AFD_SET_INFO (0x0001203B)	2
\Device\RasAcd	0x00F14014	2
\Device\Afd\Endpoint	AFD_BIND (0x00012003)	2
\Device\Afd\Endpoint	AFD_GET_TDI_HAND (0x00012037)	3
\Device\Afd\Endpoint	AFD_GET_SOCK_NAI (0x0001202F)	2
\Device\Afd\Endpoint	AFD_SEND_DATAGR/ (0x00012023)	2

Memory Mapped Files:

File Name
C:\43854473.exe
C:\WINDOWS\System32\winrnr.dll
C:\WINDOWS\System32\wshtcpip.dll
C:\WINDOWS\system32\DNSAPI.dll
C:\WINDOWS\system32\hnetcfg.dll
C:\WINDOWS\system32\mswsock.dll
C:\WINDOWS\system32\rasadhlp.dll

3.c) Explorer.EXE - Network Activity

DNS Queries:

Name	Query Type	Query Result	Successful	Protocol
mail.topgameland.com	DNS_TYPE_A	82.98.86.179	YES	udp
mail.genesisstore.sk	DNS_TYPE_A	69.43.160.174	YES	udp

3.d) Explorer.EXE - Other Activities

Mutexes Created:

x3x_fejh__frg65fx

Keyboard Keys Monitored:

Virtual Key Code	Times
VK_LBUTTON (1)	112

4. ctfmon.exe

General information about this executable

Analysis Reason:	43854473.exe wrote to the virtual memory of this process
Filename:	ctfmon.exe
MD5:	5f1d5f88303d4a4dbc8e5f97ba967cc3
SHA-1:	99cb7370f16773c8e2d0c86fe805ec638ab126e9
File Size:	15360
Command Line:	"C:\WINDOWS\system32\ctfmon.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\msvcrt.dll	0x77C10000	0x00058000
C:\WINDOWS\system32\ADVAPI32.dll	0x77DD0000	0x0009B000
C:\WINDOWS\system32\RPCRT4.dll	0x77E70000	0x00092000
C:\WINDOWS\system32\Secur32.dll	0x77FE0000	0x00011000
C:\WINDOWS\system32\USER32.dll	0x7E410000	0x00091000
C:\WINDOWS\system32\GDI32.dll	0x77F10000	0x00049000
C:\WINDOWS\system32\MSCTF.dll	0x74720000	0x0004C000
C:\WINDOWS\system32\MSUTB.dll	0x5FC10000	0x00033000
C:\WINDOWS\system32\ShimEng.dll	0x5CB70000	0x00026000
C:\WINDOWS\AppPatch\AcGenral.DLL	0x6F880000	0x001CA000
C:\WINDOWS\system32\WINMM.dll	0x76B40000	0x0002D000
C:\WINDOWS\system32\ole32.dll	0x774E0000	0x0013D000
C:\WINDOWS\system32\OLEAUT32.dll	0x77120000	0x0008B000
C:\WINDOWS\system32\MSACM32.dll	0x77BE0000	0x00015000
C:\WINDOWS\system32\VERSION.dll	0x77C00000	0x00008000
C:\WINDOWS\system32\SHELL32.dll	0x7C9C0000	0x00817000
C:\WINDOWS\system32\SHLWAPI.dll	0x77F60000	0x00076000
C:\WINDOWS\system32\USERENV.dll	0x769C0000	0x000B4000
C:\WINDOWS\system32\UxTheme.dll	0x5AD70000	0x00038000
C:\WINDOWS\WinSxS\x86_Microsoft.Windows.Common-Controls_6595b64144ccf1df_6.0.2600.5512_x-ww_35d4ce83\comctl32.dll	0x773D0000	0x00103000

4.a) ctfmon.exe - Registry Activities

Monitored Registry Keys:

Key Name	Watch subtree	Notify Filter	Count
HKU\ S-1-5-21-842925246-1425521274-308236825- Software\Microsoft\Windows\CurrentVersion\ Run	1	Key Change,Value Change	1

4.b) ctfmon.exe - Process Activities

Foreign Memory Regions Read:

Process: C:\WINDOWS\explorer.exe