Anubis - Analysis Report

Analysis Report for 46890643

MD5: a5efa6e91c390d29e1cf02cd32e9ac3c

Summary:

Description	Risk
Write to foreign memory areas: This executable tampers with the execution of another process.	high
AV Hit: This executable is detected by an antivirus software.	high

Dependency overview:

46890643.exe C:\46890643.exe

Analysis reason: Primary Analysis Subject

Explorer.EXE C:\WINDOWS\Explorer.EXE

Analysis reason: 46890643.exe wrote to the virtual memory of this process

Table of Contents:

1. General Information.....4
2. 46890643.exe.....4
   a) Registry Activities.....4
   b) File Activities.....5
   c) Process Activities.....5
3. Explorer.EXE.....5

1. General Information

Information about Anubis' invocation	
Time needed:	250 s
Report created:	04/23/11, 05:21:10 UTC
Termination reason:	Timeout
Program version:	1.75.3394

2. 46890643.exe

General information about this executable	
Analysis Reason:	Primary Analysis Subject
Filename:	46890643.exe
MD5:	a5efa6e91c390d29e1cf02cd32e9ac3c
SHA-1:	78027cbe27d67d841dfae0ed3c1971fed113cb7d
File Size:	105984
Command Line:	"C:\46890643.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\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

Worm.Win32.Rimecud (Sig-Id:1281099)

2.a) 46890643.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

2.b) 46890643.exe - File Activities

Files Created:

C:\RECYCLER\S-1-5-21-4244603681-8379039464-692207096-8961
C:\RECYCLER\S-1-5-21-4244603681-8379039464-692207096-8961\Desktop.ini

Files Modified:

C:\RECYCLER\S-1-5-21-4244603681-8379039464-692207096-8961\Desktop.ini

Directories Created:

C:\RECYCLER\S-1-5-21-4244603681-8379039464-692207096-8961

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) 46890643.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:	46890643.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

General information about this executable

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
C:\WINDOWS\system32\webcheck.dll	0x74B30000	0x00046000
C:\WINDOWS\system32\WSOCK32.dll	0x71AD0000	0x00009000
C:\WINDOWS\system32\WS2_32.dll	0x71AB0000	0x00017000

Load-time Dlls

Module Name	Base Address	Size
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