Anubis - Analysis Report

Analysis Report for 58253565

MD5: be217be1ec03c7591d4c982b1175cd47

Summary:

No threats could be detected by Anubis. This does **not** imply that execution of this executable is safe.

Dependency overview:

58253565.exe C:\58253565.exe

Analysis reason: Primary Analysis Subject

Table of Contents:

1. General Information..... 4
2. 58253565.exe.....4
   a) Registry Activities..... 4
   b) File Activities..... 4
   c) Other Activities..... 5

1. General Information

Information about Anubis' invocation	
Time needed:	253 s
Report created:	01/23/12, 00:47:35 UTC
Termination reason:	Timeout
Program version:	1.75.3394

2. 58253565.exe

General information about this executable	
Analysis Reason:	Primary Analysis Subject
Filename:	58253565.exe
MD5:	be217be1ec03c7591d4c982b1175cd47
SHA-1:	b89e3c31759e9a1b68524675c77ca14b7fdc7690
File Size:	81920
Command Line:	"C:\58253565.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\USER32.dll	0x7E410000	0x00091000
C:\WINDOWS\system32\GDI32.dll	0x77F10000	0x00049000
C:\WINDOWS\system32\comdlg32.dll	0x763B0000	0x00049000
C:\WINDOWS\system32\ADVAPI32.dll	0x77DD0000	0x0009B000
C:\WINDOWS\system32\RPCRT4.dll	0x77E70000	0x00092000
C:\WINDOWS\system32\Secur32.dll	0x77FE0000	0x00011000
C:\WINDOWS\system32\COMCTL32.dll	0x5D090000	0x0009A000
C:\WINDOWS\system32\SHELL32.dll	0x7C9C0000	0x00817000
C:\WINDOWS\system32\msvcrt.dll	0x77C10000	0x00058000
C:\WINDOWS\system32\SHLWAPI.dll	0x77F60000	0x00076000
C:\WINDOWS\system32\ole32.dll	0x774E0000	0x0013D000
C:\WINDOWS\WinSxS\x86_Microsoft.Windows.Common-Controls_6595b64144ccf1df_6.0.2600.5512_x-ww_35d4ce83\comctl32.dll	0x773D0000	0x00103000

2.a) 58253565.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
HKLM\Software\Policies\Microsoft\Windows\Safer\CodeIdentifiers	TransparentEnabled	1	1
HKLM\System\CurrentControlSet\Control\Terminal Server	TSUserEnabled	0	1

2.b) 58253565.exe - File Activities

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\COMCTL32.dll
C:\WINDOWS\system32\SHELL32.dll

2.c) 58253565.exe - Other Activities

Mutexes Created:

DBWinMutex

Windows SEH exceptions:

Description	Times
Exception 0x40010006 at 0x7c812aeb	1