Anubis - Analysis Report

Analysis Report for 39792098

MD5: aad02b0475e73730bca416a115c2a16c

Summary:

Description	Risk
Creates files in the Windows system directory: Malware often keeps copies of itself in the Windows directory to stay undetected by users.	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

Dependency overview:

39792098.exe C:\39792098.exe

Analysis reason: Primary Analysis Subject

Table of Contents:

1. General Information..... 4
2. 39792098.exe.....4
   a) Registry Activities.....4
   b) File Activities..... 4
   c) Other Activities..... 5

1. General Information

Information about Anubis' invocation	
Time needed:	28 s
Report created:	01/13/11, 15:48:34 UTC
Termination reason:	All tracked processes have exited
Program version:	1.74.3195

2. 39792098.exe

General information about this executable	
Analysis Reason:	Primary Analysis Subject
Filename:	39792098.exe
MD5:	aad02b0475e73730bca416a115c2a16c
SHA-1:	fab0cfbfbe0efec30f67356c02baf671e4eeb2e2
File Size:	460288
Command Line:	"C:\39792098.exe"
Process-status at analysis end:	dead
Exit Code:	-1073741819

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\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\GDI32.dll	0x77F10000	0x00049000
C:\WINDOWS\system32\USER32.dll	0x7E410000	0x00091000
C:\WINDOWS\system32\msvcrt.dll	0x77C10000	0x00058000

Run-time Dlls

Module Name	Base Address	Size
C:\WINDOWS\system32\Apphelp.dll	0x77B40000	0x00022000

SigBuster Output

PE_Compact v1.68-1.84 SN:709 PE_Compact v1.40-v1.45 SN:1265

Ikarus Virus Scanner

P2P-Worm.Win32.Palevo (Sig-Id:1393623)

2.a) 39792098.exe - Registry Activities

Registry Values Read:

Key	Name	Value	Times
HKLM\SYSTEM\WPA\MediaCenter	Installed	0	1
HKLM\Software\Policies\Microsoft\Windows\Safer\CodeIdentifiers	AuthenticodeEnabled	0	1
HKLM\Software\Policies\Microsoft\Windows\Safer\CodeIdentifiers	TransparentEnabled	1	2
HKLM\System\CurrentControlSet\Control\Terminal Server	TSUserEnabled	0	1

2.b) 39792098.exe - File Activities

Files Created:
C:\39792098 .exe
C:\WINDOWS\System32\geedc.dll

Files Modified:
C:\39792098 .exe
C:\WINDOWS\System32\geedc.dll

Memory Mapped Files:
File Name
C:\39792098 .exe
C:\WINDOWS\System32\geedc.dll
C:\WINDOWS\system32\Apphelp.dll
C:\Windows\AppPatch\sysmain.sdb

2.c) 39792098.exe - Other Activities

Windows SEH exceptions:

Description	Times
Exception 0xc0000096 (STATUS_PRIVILEGED_INSTRUCTION) at 0x100021f3	1
Exception 0xc0000005 (STATUS_ACCESS_VIOLATION) at 0x10001666	1
Exception 0xc0000005 (STATUS_ACCESS_VIOLATION) at 0x10	1