Anubis - Analysis Report

Analysis Report for 0020399952

MD5: 49de40ae8f4adb4e86011d2c11879238

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

International Secure Systems Lab
Vienna University of Technology , Eurecom France , UC Santa Barbara
Contact: anubis@iseclab.org

Dependency overview:

0020399952.exe C:\0020399952.exe

Analysis reason: Primary Analysis Subject

Table of Contents:

1. General Information

Information about Anubis' invocation	
Time needed:	73 s
Report created:	12/27/10, 19:21:09 UTC
Termination reason:	All tracked processes have exited
Program version:	1.74.3362

2. 0020399952.exe

General information about this executable	
Analysis Reason:	Primary Analysis Subject
Filename:	0020399952.exe
MD5:	49de40ae8f4adb4e86011d2c11879238
SHA-1:	8c269427049f495ad2912d5812efe8f205d386c8
File Size:	2336249
Command Line:	"C:\0020399952.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\UxTheme.dll	0x5AD70000	0x00038000
C:\WINDOWS\system32\riched32.dll	0x732E0000	0x00005000
C:\WINDOWS\system32\MSCTF.dll	0x74720000	0x0004C000
C:\WINDOWS\system32\RICHED20.dll	0x74E30000	0x0006D000
C:\WINDOWS\system32\browseui.dll	0x75F80000	0x000FD000
C:\WINDOWS\system32\COMDLG32.DLL	0x763B0000	0x00049000
C:\WINDOWS\system32\CLBCATQ.DLL	0x76FD0000	0x0007F000
C:\WINDOWS\system32\COMRes.dll	0x77050000	0x000C5000
C:\WINDOWS\system32\OLEAUT32.dll	0x77120000	0x0008B000
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\VERSION.dll	0x77C00000	0x00008000
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

SigBuster Output

PE_Compact v2.X SN:660 PE_Compact V2.X SN:1620

2.a) 0020399952.exe - Registry Activities

Registry Keys Created:

HKU\S-1-5-21-842925246-1425521274-308236825-500\Software\WinRAR SFX

Registry Values Modified:

Key	Name	New Value
HKU\S-1-5-21-842925246-1425521274-308236825-500\Software\WinRAR SFX	C%%WINDOWS%System32	C:\WINDOWS\System32

Registry Values Read:

Key	Name	Value	Times
HKLM\SOFTWARE\CLASSES\CLSID\{00BB2763-6A77-11D0-A535-00C04FD7D062}\INPROCSERVER32		%SystemRoot%\system32\browseui.dll	2
HKLM\SOFTWARE\CLASSES\CLSID\{00BB2763-6A77-11D0-A535-00C04FD7D062}\INPROCSERVER32	ThreadingModel	Apartment	1
HKLM\SOFTWARE\CLASSES\CLSID\{00BB2765-6A77-11D0-A535-00C04FD7D062}\INPROCSERVER32		%SystemRoot%\system32\browseui.dll	1
HKLM\SOFTWARE\CLASSES\CLSID\{00BB2765-6A77-11D0-A535-00C04FD7D062}\INPROCSERVER32	ThreadingModel	Apartment	1
HKLM\SOFTWARE\CLASSES\CLSID\{03C036F1-A186-11D0-824A-00AA005B4383}\INPROCSERVER32		%SystemRoot%\system32\browseui.dll	2
HKLM\SOFTWARE\CLASSES\CLSID\{03C036F1-A186-11D0-824A-00AA005B4383}\INPROCSERVER32	ThreadingModel	Apartment	1
HKLM\SOFTWARE\Microsoft\CTF\SystemShared\	CUAS	0	1
HKLM\SYSTEM\CurrentControlSet\Control\Session Manager	CriticalSectionTimeout	2592000	1
HKLM\SYSTEM\Setup	SystemSetupInProgres	0	1
HKLM\Software\Microsoft\COM3	Com+Enabled	1	2
HKLM\Software\Microsoft\COM3	REGDBVersion	0x0700000000000000	6
HKLM\Software\Policies\Microsoft\Windows\Safer\CodeIdentifiers	TransparentEnabled	1	1
HKLM\System\CurrentControlSet\Control\Terminal Server	TSUserEnabled	0	1
HKU\S-1-5-21-842925246-1425521274-308236825-500\Keyboard Layout\Toggle	Language Hotkey	1	2
HKU\S-1-5-21-842925246-1425521274-308236825-500\Keyboard Layout\Toggle	Layout Hotkey	2	2
HKU\S-1-5-21-842925246-1425521274-308236825-500\software\Microsoft\Windows\CurrentVersion\Explorer\Advanced	ListviewAlphaSelect	0	1
HKU\S-1-5-21-842925246-1425521274-308236825-500\software\Microsoft\Windows\CurrentVersion\Explorer\Advanced	ListviewShadow	0	1
HKU\S-1-5-21-842925246-1425521274-308236825-500\software\Microsoft\Windows\CurrentVersion\Explorer\Advanced	ListviewWatermark	1	1

Monitored Registry Keys:

Key Name	Watch subtree	Notify Filter	Count
HKLM\Software\Classes	1	Key Change,Value Change	3
HKLM\Software\Classes\CLSID	1	Key Change,Value Change	2
HKLM\Software\Microsoft\COM3	1	Key Change,Value Change	6
HKU	1	Key Change,Value Change	3

2.b) 0020399952.exe - File Activities

Files Deleted:

C:\WINDOWS\System32__tmp_rar_sfx_access_check_506578

Files Created:

C:\WINDOWS\System32\AVCDX.ax

C:\WINDOWS\System32\CoreAAC.ax

Files Created:

C:\WINDOWS\System32\DiracSplitter.ax
C:\WINDOWS\System32\FLACDX.ax
C:\WINDOWS\System32\MPCDx.ax
C:\WINDOWS\System32\MatroskaDX.ax
C:\WINDOWS\System32\RLAPEDec.ax
C:\WINDOWS\System32\RLMPCDec.ax
C:\WINDOWS\System32\RLOgg.ax
C:\WINDOWS\System32\RLSpeexDec.ax
C:\WINDOWS\System32\RLTheoraDec.ax
C:\WINDOWS\System32\RLVorbisDec.ax
C:\WINDOWS\System32\RealMediaDX.ax
C:\WINDOWS\System32\TTADSDecoder.ax
C:\WINDOWS\System32\TTADSSplitter.ax
C:\WINDOWS\System32__tmp_rar_sfx_access_check_506578
C:\WINDOWS\System32\aac_parser.ax
C:\WINDOWS\System32\ac3DX.ax
C:\WINDOWS\System32\flvDX.dll
C:\WINDOWS\System32\msfDX.dll
C:\WINDOWS\System32\nbDX.dll

Files Read:

C:\0020399952.exe
C:\WINDOWS\Registration\R000000000007.clb
C:\WINDOWS\win.ini

Files Modified:

C:\WINDOWS\System32\AVCDX.ax
C:\WINDOWS\System32\CoreAAC.ax
C:\WINDOWS\System32\DiracSplitter.ax
C:\WINDOWS\System32\FLACDX.ax
C:\WINDOWS\System32\MPCDx.ax
C:\WINDOWS\System32\MatroskaDX.ax
C:\WINDOWS\System32\RLAPEDec.ax
C:\WINDOWS\System32\RLMPCDec.ax
C:\WINDOWS\System32\RLOgg.ax
C:\WINDOWS\System32\RLSpeexDec.ax
C:\WINDOWS\System32\RLTheoraDec.ax
C:\WINDOWS\System32\RLVorbisDec.ax
C:\WINDOWS\System32\RealMediaDX.ax
C:\WINDOWS\System32\TTADSDecoder.ax
C:\WINDOWS\System32\TTADSSplitter.ax
C:\WINDOWS\System32\aac_parser.ax
C:\WINDOWS\System32\ac3DX.ax
C:\WINDOWS\System32\flvDX.dll
C:\WINDOWS\System32\msfDX.dll
C:\WINDOWS\System32\nbDX.dll

Device Control Communication:

File	Control Code	Times
\Device\KsecDD	0x00390008	8

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

Memory Mapped Files:

File Name
C:\WINDOWS\system32\CLBCATQ.DLL
C:\WINDOWS\system32\COMRes.dll
C:\WINDOWS\system32\MSCTF.dll
C:\WINDOWS\system32\RICHED20.dll
C:\WINDOWS\system32\SHELL32.dll
C:\WINDOWS\system32\UxTheme.dll
C:\WINDOWS\system32\browseui.dll
C:\WINDOWS\system32\imm32.dll
C:\WINDOWS\system32\riched32.dll
C:\WINDOWS\system32\rpcss.dll

2.c) 0020399952.exe - Other Activities

Mutexes Created:

CTF.Asm.MutexDefaultS-1-5-21-842925246-1425521274-308236825-500
CTF.Compart.MutexDefaultS-1-5-21-842925246-1425521274-308236825-500
CTF.LBES.MutexDefaultS-1-5-21-842925246-1425521274-308236825-500
CTF.Layouts.MutexDefaultS-1-5-21-842925246-1425521274-308236825-500
CTF.TMD.MutexDefaultS-1-5-21-842925246-1425521274-308236825-500
CTF.TimListCache.FMPDefaultS-1-5-21-842925246-1425521274-308236825-500MUTEX.DefaultS-1-5-21-842925246-1425521274-308236825-500

Keyboard Keys Monitored:

Virtual Key Code	Times
VK_ESCAPE (27)	23
VK_SHIFT (16)	1

Windows SEH exceptions:

Description	Times
Exception 0xc0000005 (STATUS_ACCESS_VIOLATION) at 0x401016	1