





# Anubis - Analysis Report



## Analysis Report for WoWEmuHacker5.exe

MD5: 9b0c00b2306ffee35a0e413aeac9a7a8

### Summary:

Description	Risk
<b>Performs File Modification and Destruction:</b> The executable modifies and destructs files which are not temporary.	 high
<b>Performs Registry Activities:</b> The executable reads and modifies register values. It also creates and monitors register keys.	 low

## Dependency overview:



**WoWEmuHack.exe** C:\WoWEmuHack.exe

Analysis reason: Primary Analysis Subject

## **Table of Contents:**

1. General Information.....	4
2. WoWEmuHack.exe.....	4
a) Registry Activities.....	5
b) File Activities.....	10
c) Other Activities.....	11



## 1. General Information

### Information about Anubis' invocation

Time needed:	241 s
Report created:	09/26/10, 21:26:37 UTC
Termination reason:	Timeout
Program version:	1.74.3195

## 2. WoWEmuHack.exe

### General information about this executable

Analysis Reason:	Primary Analysis Subject
Filename:	WoWEmuHack.exe
MD5:	9b0c00b2306ffee35a0e413aeac9a7a8
SHA-1:	f4e163fa7492fe04f875e7f3b5f8a7c2cda718ed
File Size:	198656
Command Line:	"C:\WoWEmuHack.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\WINSPOOL.DRV	0x73000000	0x00026000
C:\WINDOWS\system32\oledlg.dll	0x7DF70000	0x00022000
C:\WINDOWS\system32\ole32.dll	0x774E0000	0x0013D000
C:\WINDOWS\system32\OLEAUT32.dll	0x77120000	0x0008B000
C:\WINDOWS\system32\WINMM.dll	0x76B40000	0x0002D000
C:\WINDOWS\WinSxS\x86_Microsoft.Windows.Common-Controls_6595b64144ccf1df_6.0.2600.5512_x-ww_35d4ce83\comctl32.dll	0x773D0000	0x00103000

### Run-time Dlls

Module Name	Base Address	Size
C:\WINDOWS\system32\UxTheme.dll	0x5AD70000	0x00038000
C:\WINDOWS\system32\NETAPI32.dll	0x5B860000	0x00055000
C:\WINDOWS\system32\MSCTF.dll	0x74720000	0x0004C000
C:\WINDOWS\system32\RichEd20.dll	0x74E30000	0x0006D000
C:\WINDOWS\system32\CRYPTUI.dll	0x754D0000	0x00080000
C:\WINDOWS\system32\browseui.dll	0x75F80000	0x000FD000
C:\WINDOWS\System32\CSCDLL.dll	0x76600000	0x0001D000
C:\WINDOWS\system32\ntshrui.dll	0x76990000	0x00025000
C:\WINDOWS\system32\USERENV.dll	0x769C0000	0x000B4000
C:\WINDOWS\system32\ATL.DLL	0x76B20000	0x00011000
C:\WINDOWS\system32\WINTRUST.dll	0x76C30000	0x0002E000
C:\WINDOWS\system32\IMAGEHLP.dll	0x76C90000	0x00028000
C:\WINDOWS\system32\WLDAP32.dll	0x76F60000	0x0002C000



## Run-time DLLs

Module Name	Base Address	Size
C:\WINDOWS\system32\CLBCATQ.DLL	0x76FD0000	0x0007F000
C:\WINDOWS\system32\COMRes.dll	0x77050000	0x000C5000
C:\WINDOWS\system32\WININET.dll	0x771B0000	0x000AA000
C:\WINDOWS\system32\SETUPAPI.dll	0x77920000	0x000F3000
C:\WINDOWS\System32\cscui.dll	0x77A20000	0x00054000
C:\WINDOWS\system32\CRYPT32.dll	0x77A80000	0x00095000
C:\WINDOWS\system32\MSASN1.dll	0x77B20000	0x00012000
C:\WINDOWS\system32\appHelp.dll	0x77B40000	0x00022000
C:\WINDOWS\system32\VERSION.dll	0x77C00000	0x00008000
C:\WINDOWS\system32\shdocvw.dll	0x7E290000	0x00171000

## SigBuster Output

FSG V1.0-1.2 SN: 1717

## Ikarus Virus Scanner

possible-Threat.Hacktool.WoW (Sig-Id:42707943)

**2.a) WoWEmuHack.exe - Registry Activities**

## Registry Keys Created:

HKLM\SOFTWARE\DeathSoft  
 HKLM\SOFTWARE\DeathSoft\WoWEmuHacker5  
 HKU\S-1-5-21-842925246-1425521274-308236825-500\\\  
 HKU\S-1-5-21-842925246-1425521274-308236825-500\\\

## Registry Values Modified:

Key	Name	New Value
HKU\S-1-5-21-842925246-1425521274-308236825-500\Software\Microsoft\Windows\CurrentVersion\Explorer\MountPoints2\{a1094da8-30a0-11dd-817b-806d6172696f}	BaseClass	Drive
HKU\S-1-5-21-842925246-1425521274-308236825-500\Software\Microsoft\Windows\CurrentVersion\Explorer\MountPoints2\{a1094daa-30a0-11dd-817b-806d6172696f}	BaseClass	Drive
HKU\S-1-5-21-842925246-1425521274-308236825-500\Software\Microsoft\Windows\CurrentVersion\Explorer\Shell Folders	Desktop	C:\Documents and Settings\Administrator\Desktop
HKU\S-1-5-21-842925246-1425521274-308236825-500\Software\Microsoft\Windows\CurrentVersion\Explorer\Shell Folders	Favorites	C:\Documents and Settings\Administrator\Favorites
HKU\S-1-5-21-842925246-1425521274-308236825-500\Software\Microsoft\Windows\CurrentVersion\Explorer\Shell Folders	Personal	C:\Documents and Settings\Administrator\My Documents
HKU\S-1-5-21-842925246-1425521274-308236825-500\Software\Microsoft\Windows\CurrentVersion\Explorer\Shell Folders	Recent	C:\Documents and Settings\Administrator\Recent
HKU\S-1-5-21-842925246-1425521274-308236825-500\Software\Microsoft\Windows\ShellNoRoam\MUICache\	@shell32.dll,-12691	My Recent Documents
HKU\S-1-5-21-842925246-1425521274-308236825-500\Software\Microsoft\Windows\ShellNoRoam\BagMRU	MRUListEx	0x000000001000000fffff
HKU\S-1-5-21-842925246-1425521274-308236825-500\Software\Microsoft\Windows\ShellNoRoam\BagMRU	NodeSlots	0x02020202
HKU\S-1-5-21-842925246-1425521274-308236825-500\Software\Microsoft\Windows\ShellNoRoam\Bags\1\Shell	FolderType	MyDocuments

## Registry Values Read:

Key	Name	Value	Times
HKLM\SOFTWARE\CLASSES\INI		inifile	1
HKLM\SOFTWARE\CLASSES\CLSID\{00BB2763-6A77-11D0-A535-00C04FD7D062}\INPROCERVER32		%SystemRoot%\system32\browseui.dll	2



## Registry Values Read:

Key	Name	Value	Times
HKLM\SOFTWARE\CLASSES\CLSID\{00BB2763-6A77-11D0-A535-00C04FD7D062}\INPROCSERVER32	ThreadingModel	Apartment	1
HKLM\SOFTWARE\CLASSES\CLSID\{03C036F1-A186-11D0-824A-00AA005B4383}\INPROCSERVER32		%SystemRoot%\system32\browseui.dll	3
HKLM\SOFTWARE\CLASSES\CLSID\{03C036F1-A186-11D0-824A-00AA005B4383}\INPROCSERVER32	ThreadingModel	Apartment	1
HKLM\SOFTWARE\CLASSES\CLSID\{208D2C60-3AEA-1069-A2D7-08002B30309D}	LocalizedString	@%SystemRoot%\system32\SHELL32.dll,-9217	1
HKLM\SOFTWARE\CLASSES\CLSID\{208D2C60-3AEA-1069-A2D7-08002B30309D}\DEFAULTICON		%SystemRoot%\system32\SHELL32.dll,17	1
HKLM\SOFTWARE\CLASSES\CLSID\{20D04FE0-3AEA-1069-A2D8-08002B30309D}	LocalizedString	@%SystemRoot%\system32\SHELL32.dll,-9216	1
HKLM\SOFTWARE\CLASSES\CLSID\{20D04FE0-3AEA-1069-A2D8-08002B30309D}\DEFAULTICON		%SystemRoot%\Explorer.exe,0	1
HKLM\SOFTWARE\CLASSES\CLSID\{20D04FE0-3AEA-1069-A2D8-08002B30309D}\INPROCSERVER32		%SystemRoot%\system32\SHELL32.dll	2
HKLM\SOFTWARE\CLASSES\CLSID\{42AEDC87-2188-41FD-B9A3-0C966FEABEC1}\INPROCSERVER32		%SystemRoot%\system32\shdocvw.dll	4
HKLM\SOFTWARE\CLASSES\CLSID\{42AEDC87-2188-41FD-B9A3-0C966FEABEC1}\INPROCSERVER32	ThreadingModel	Apartment	1
HKLM\SOFTWARE\CLASSES\CLSID\{450D8FBA-AD25-11D0-98A8-0800361B1103}	LocalizedString	@%SystemRoot%\system32\SHELL32.dll,-9227	2
HKLM\SOFTWARE\CLASSES\CLSID\{450D8FBA-AD25-11D0-98A8-0800361B1103}\SHELLFOLDER	Attributes	4034920765	5
HKLM\SOFTWARE\CLASSES\CLSID\{450D8FBA-AD25-11D0-98A8-0800361B1103}\SHELLFOLDER	CallForAttributes	131136	3
HKLM\SOFTWARE\CLASSES\CLSID\{450D8FBA-AD25-11D0-98A8-0800361B1103}\SHELLFOLDER	WantsFORPARSING		4
HKLM\SOFTWARE\CLASSES\CLSID\{603D3800-BD81-11D0-A3A5-00C04FD706EC}\INPROCSERVER32		%SystemRoot%\system32\browseui.dll	2
HKLM\SOFTWARE\CLASSES\CLSID\{603D3800-BD81-11D0-A3A5-00C04FD706EC}\INPROCSERVER32	ThreadingModel	Apartment	1
HKLM\SOFTWARE\CLASSES\CLSID\{750FDF0E-2A26-11D1-A3EA-080036587F03}\INPROCSERVER32		%SystemRoot%\System32\csui.dll	2
HKLM\SOFTWARE\CLASSES\CLSID\{750FDF0E-2A26-11D1-A3EA-080036587F03}\INPROCSERVER32	ThreadingModel	Apartment	1
HKLM\SOFTWARE\CLASSES\DIRECTORY	AlwaysShowExt		1
HKLM\SOFTWARE\CLASSES\DRIVE\SHELLEX\FOLDEREXTENSIONS\{FBEB8A05-BEEE-4442-804E-409D6C4515E9}	DriveMask	32	1
HKLM\SOFTWARE\CLASSES\INTERFACE\{000214E6-0000-0000-C000-000000000046}\PROXYSTUBCLSID32		{bf50b68e-29b8-4386-ae9c-9734d5117cd5}	1
HKLM\SOFTWARE\CLASSES\INTERFACE\{79EAC9C4-BAF9-11CE-8C82-00AA004BA90B}\PROXYSTUBCLSID32		{B8DA6310-E19B-11D0-933C-00A0C90DCAA9}	1
HKLM\SOFTWARE\CLASSES\INTERFACE\{93F2F68C-1D1B-11D3-A30E-00C04F79ABD1}\PROXYSTUBCLSID32		{bf50b68e-29b8-4386-ae9c-9734d5117cd5}	1
HKLM\SOFTWARE\CLASSES\INTERFACE\{B722BCCB-4E68-101B-A2BC-00AA00404770}\PROXYSTUBCLSID32		{B8DA6310-E19B-11D0-933C-00A0C90DCAA9}	1
HKLM\SOFTWARE\CLASSES\INTERFACE\{EAB22AC1-30C1-11CF-A7EB-0000C05BAE0B}\TYPELIB		{EAB22AC0-30C1-11CF-A7EB-0000C05BAE0B}	1
HKLM\SOFTWARE\CLASSES\NETWORK\SHARINGHANDLER		ntshui.dll	1



## Registry Values Read:

Key	Name	Value	Times
HKLM\SOFTWARE\Microsoft\CTF\SystemShared\	CUAS	0	1
HKLM\SYSTEM\CurrentControlSet\Control\Session Manager	CriticalSectionTimeout	2592000	1
HKLM\SYSTEM\Setup	OsLoaderPath	\	2
HKLM\SYSTEM\Setup	SystemPartition	\Device\HarddiskVolume1	2
HKLM\SYSTEM\Setup	SystemSetupInProgress	0	1
HKLM\Software\Classes\CLSID\{00bb2763-6a77-11d0-a535-00c04fd7d062}\InProcServer32		%SystemRoot%\system32\browseui.dll	1
HKLM\Software\Classes\CLSID\{03c036f1-a186-11d0-824a-00aa005b4383}\InProcServer32		%SystemRoot%\system32\browseui.dll	1
HKLM\Software\Classes\CLSID\{750fdf0e-2a26-11d1-a3ea-080036587f03}\InProcServer32		%SystemRoot%\System32\cscui.dll	1
HKLM\Software\Microsoft\COM3	Com+Enabled	1	4
HKLM\Software\Microsoft\COM3	REGDBVersion	0x0700000000000000	20
HKLM\Software\Microsoft\Windows NT\CurrentVersion\FontSubstitutes	MS Shell Dlg	Microsoft Sans Serif	1
HKLM\Software\Microsoft\Windows NT\CurrentVersion\ProfileList\S-1-5-21-842925246-1425521274-308236825-500	CentralProfile		1
HKLM\Software\Microsoft\Windows NT\CurrentVersion\ProfileList\S-1-5-21-842925246-1425521274-308236825-500	Flags	0	1
HKLM\Software\Microsoft\Windows NT\CurrentVersion\ProfileList\S-1-5-21-842925246-1425521274-308236825-500	ProfileImagePath	%SystemDrive%\Documents and Settings\Administrator	3
HKLM\Software\Microsoft\Windows NT\CurrentVersion\ProfileList\S-1-5-21-842925246-1425521274-308236825-500	ProfileLoadTimeHigh	30014298	1
HKLM\Software\Microsoft\Windows NT\CurrentVersion\ProfileList\S-1-5-21-842925246-1425521274-308236825-500	ProfileLoadTimeLow	833226792	1
HKLM\Software\Microsoft\Windows NT\CurrentVersion\ProfileList\S-1-5-21-842925246-1425521274-308236825-500	State	256	1
HKLM\Software\Microsoft\Windows\CurrentVersion	DevicePath	%SystemRoot%\inf	1
HKLM\Software\Microsoft\Windows\CurrentVersion\Explorer\ShellIconOverlayIdentifiers\Offline Files		{750fdf0e-2a26-11d1-a3ea-080036587f03}	1
HKLM\Software\Microsoft\Windows\CurrentVersion\Explorer\User Shell Folders	Common Start Menu	%ALLUSERSPROFILE%\Start Menu	3
HKLM\Software\Microsoft\Windows\CurrentVersion\Setup	DriverCachePath	%SystemRoot%\Driver Cache	2
HKLM\Software\Microsoft\Windows\CurrentVersion\Setup	LogLevel	0	2
HKLM\Software\Microsoft\Windows\CurrentVersion\Setup	ServicePackCachePath	c:\windows\ServicePackFiles\ServicePackCache	2
HKLM\Software\Microsoft\Windows\CurrentVersion\Setup	ServicePackSourcePath	D:\	2
HKLM\Software\Microsoft\Windows\CurrentVersion\Setup	SourcePath	D:\	2
HKLM\Software\Policies\Microsoft\Windows\Safer\CodeIdentifiers	TransparentEnabled	1	1
HKLM\System\CurrentControlSet\Control\ComputerName\ActiveComputerName	ComputerName	PC	2
HKLM\System\CurrentControlSet\Control\MediaProperties\PrivateProperties\Joystick\Winmm	wheel	1	1
HKLM\System\CurrentControlSet\Control\ProductOptions	ProductType	WinNT	2
HKLM\System\CurrentControlSet\Services\LDAP	LdapClientIntegrity	1	1
HKLM\System\CurrentControlSet\Services\Tcpip\Parameters	Domain		1
HKLM\System\CurrentControlSet\Services\Tcpip\Parameters	Hostname	pc	1
HKLM\System\Setup	SystemSetupInProgress	0	1
HKLM\System\WPA\PnP	seed	1274198464	1
HKU\S-1-5-21-842925246-1425521274-308236825-500\Control Panel\Desktop\WindowMetrics	Shell Icon Bpp	16	1
HKU\S-1-5-21-842925246-1425521274-308236825-500\Control Panel\Desktop\WindowMetrics	Shell Icon Size	32	1









Device Control Communication:

File	Control Code	Times
MountPointManager	0x006D0034	4

Memory Mapped Files:

File Name
C:\WINDOWS\Explorer.exe
C:\WINDOWS\SYSTEM32\mydocs.dll
C:\WINDOWS\System32\CSCDLL.dll
C:\WINDOWS\System32\cscuri.dll
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\ATL.DLL
C:\WINDOWS\system32\CLBCATQ.DLL
C:\WINDOWS\system32\COMCTL32.dll
C:\WINDOWS\system32\COMRes.dll
C:\WINDOWS\system32\MSCTF.dll
C:\WINDOWS\system32\RichEd20.dll
C:\WINDOWS\system32\SETUPAPI.dll
C:\WINDOWS\system32\SHELL32.dll
C:\WINDOWS\system32\UxTheme.dll
C:\WINDOWS\system32\WININET.dll
C:\WINDOWS\system32\WINMM.dll
C:\WINDOWS\system32\WINSPOOL.DRV
C:\WINDOWS\system32\browserui.dll
C:\WINDOWS\system32\imm32.dll
C:\WINDOWS\system32\ntshrui.dll
C:\WINDOWS\system32\oledlg.dll
C:\WINDOWS\system32\rpcss.dll
C:\WINDOWS\system32\shdocvw.dll
C:\WINDOWS\system32\shell32.dll

2.c) WoWEmuHack.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
Shell.CMruPidList

Keyboard Keys Monitored:

Virtual Key Code	Times
VK_ESCAPE (27)	22
VK_LBUTTON (1)	5