



Anubis - Analysis Report



Analysis Report for winlogon32.exe

MD5: 38d541e8e0ed43c6b08c894e1464a3ec

Summary:

Description	Risk
Autostart capabilities: This executable registers processes to be executed at system start. This could result in unwanted actions to be performed automatically.	 medium
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:



winlogon32.exe C:\winlogon32.exe

Analysis reason: Primary Analysis Subject

Table of Contents:

1. General Information.....	4
2. winlogon32.exe.....	4
a) Registry Activities.....	4
b) File Activities.....	5



1. General Information

Information about Anubis' invocation

Time needed:	239 s
Report created:	01/06/10, 14:46:34 UTC
Termination reason:	Timeout
Program version:	1.73.0

2. winlogon32.exe

General information about this executable

Analysis Reason:	Primary Analysis Subject
Filename:	winlogon32.exe
MD5:	38d541e8e0ed43c6b08c894e1464a3ec
SHA-1:	558869a34cf83de77e60482e456fdd9ebcae91a5
File Size:	25600
Command Line:	"C:\winlogon32.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\ole32.dll	0x774E0000	0x0013D000
C:\WINDOWS\system32\ADVAPI32.dll	0x77DD0000	0x0009B000
C:\WINDOWS\system32\RPCRT4.dll	0x77E70000	0x00092000
C:\WINDOWS\system32\Secur32.dll	0x77FE0000	0x00011000
C:\WINDOWS\system32\msvcrt.dll	0x77C10000	0x00058000

Run-time Dlls

Module Name	Base Address	Size
C:\WINDOWS\system32\comctl32.dll	0x5D090000	0x0009A000
C:\WINDOWS\system32\MSCTF.dll	0x74720000	0x0004C000
C:\WINDOWS\system32\PSAPI.DLL	0x76BF0000	0x0000B000
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\CRYPT32.dll	0x77A80000	0x00095000
C:\WINDOWS\system32\MSASN1.dll	0x77B20000	0x00012000
C:\WINDOWS\system32\SHLWAPI.dll	0x77F60000	0x00076000
C:\WINDOWS\system32\SHELL32.dll	0x7C9C0000	0x00817000

2.a) winlogon32.exe - Registry Activities

Registry Keys Created:

HKUS-1-5-21-842925246-1425521274-308236825-500\Software\Microsoft\Windows\CurrentVersion\Policies\System
HKUS-1-5-21-842925246-1425521274-308236825-500\Software\Microsoft\Windows\CurrentVersion\Policies\ActiveDesktop
HKLM\Software\Microsoft\Windows\CurrentVersion\Policies\Explorer
HKLM\Software\Microsoft\Windows\CurrentVersion\Policies\ActiveDesktop



Registry Values Modified:

Key	Name	New Value
HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon	Userinit	C:\WINDOWS\system32\winlogon32.exe
HKLM\Software\Microsoft\Windows\CurrentVersion\Policies\ActiveDesktop	NoChangingWallpaper	1
HKLM\Software\Microsoft\Windows\CurrentVersion\Policies\Explorer	NoActiveDesktopChange	1
HKLM\Software\Microsoft\Windows\CurrentVersion\Policies\Explorer	NoSetActiveDesktop	1
HKLM\Software\Microsoft\Windows\CurrentVersion\Run	smss32.exe	C:\WINDOWS\system32\smss32.exe
HKU\S-1-5-21-842925246-1425521274-308236825-500\Software\Microsoft\Windows\CurrentVersion\Policies\ActiveDesktop	NoChangingWallpaper	1
HKU\S-1-5-21-842925246-1425521274-308236825-500\Software\Microsoft\Windows\CurrentVersion\Policies\Explorer	NoActiveDesktopChange	1
HKU\S-1-5-21-842925246-1425521274-308236825-500\Software\Microsoft\Windows\CurrentVersion\Policies\Explorer	NoSetActiveDesktop	1
HKU\S-1-5-21-842925246-1425521274-308236825-500\Software\Microsoft\Windows\CurrentVersion\Policies\System	DisableTaskMgr	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	SystemSetupInProgress	0	1
HKLM\Software\Microsoft\Windows NT\CurrentVersion\Windows	AppInit_DLLs		1
HKLM\Software\Policies\Microsoft\Windows\Safer\CodeIdentifiers	TransparentEnabled	1	1
HKLM\System\CurrentControlSet\Control\Terminal Server	TSAppCompat	0	3
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

2.b) winlogon32.exe - File Activities

Files Created:

C:\WINDOWS\system32\smss32.exe
C:\WINDOWS\system32\winlogon32.exe

Files Read:

C:\winlogon32.exe

Files Modified:

C:\WINDOWS\system32\smss32.exe
C:\WINDOWS\system32\winlogon32.exe

File System Control Communication:

File	Control Code	Times
C:\	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\MSCTF.dll
C:\WINDOWS\system32\PSAPI.DLL
C:\WINDOWS\system32\SHELL32.dll
C:\WINDOWS\system32\WININET.dll
C:\WINDOWS\system32\comctl32.dll
C:\WINDOWS\system32\imm32.dll
C:\winlogon32.exe