Anubis - Analysis Report

Analysis Report for EsetCrackme2013.exe

MD5: f8134a5f026964d0338591bc73217c3b

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

Dependency overview:

EsetCrackm.exe C:\EsetCrackm.exe

Analysis reason: Primary Analysis Subject

Table of Contents:

1. General Information

Information about Anubis' invocation	
Time needed:	25 s
Report created:	08/12/13, 15:34:32 UTC
Termination reason:	All tracked processes have exited
Program version:	1.76.3886

2. EsetCrackm.exe

General information about this executable	
Analysis Reason:	Primary Analysis Subject
Filename:	EsetCrackm.exe
MD5:	f8134a5f026964d0338591bc73217c3b
SHA-1:	e391761999ad0393b467a050259a2de70d8a14f9
File Size:	30936
Command Line:	"C:\EsetCrackm.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
C:\WINDOWS\system32\advapi32.dll	0x77DD0000	0x0009B000
C:\WINDOWS\system32\RPCRT4.dll	0x77E70000	0x00092000
C:\WINDOWS\system32\Secur32.dll	0x77FE0000	0x00011000
C:\WINDOWS\system32\user32.dll	0x7E410000	0x00091000
C:\WINDOWS\system32\GDI32.dll	0x77F10000	0x00049000

Run-time Dlls

Module Name	Base Address	Size
C:\WINDOWS\system32\Flt.dll	0x10000000	0x00004000
C:\WINDOWS\system32\comctl32.dll	0x5D090000	0x0009A000
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\ole32.dll	0x774E0000	0x0013D000
C:\WINDOWS\system32\CRYPT32.dll	0x77A80000	0x00095000
C:\WINDOWS\system32\MSASN1.dll	0x77B20000	0x00012000
C:\WINDOWS\system32\VERSION.dll	0x77C00000	0x00008000
C:\WINDOWS\system32\msvcrt.dll	0x77C10000	0x00058000
C:\WINDOWS\system32\SHLWAPI.dll	0x77F60000	0x00076000
C:\WINDOWS\system32\shell32.dll	0x7C9C0000	0x00817000
C:\WINDOWS\system32\urlmon.dll	0x7E1E0000	0x000A2000

2.a) EsetCrackm.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\Microsoft\Internet Explorer\Main\FeatureControl\FEATURE_BEHAVIORS	*	1	1

Registry Values Read:

Key	Name	Value	Times
HKLM\Software\Microsoft\Internet Explorer\Main\ FeatureControl\FEATURE_DISABLE_MK_PROTOCOL	*	1	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

2.b) EsetCrackm.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\Wininet.dll
C:\WINDOWS\system32\comctl32.dll
C:\WINDOWS\system32\shell32.dll
C:\WINDOWS\system32\urlmon.dll

2.c) EsetCrackm.exe - Other Activities

Mutexes Created:

DBWinMutex
Eset Crackme 2013
ZonesCacheCounterMutex
ZonesCounterMutex
ZonesLockedCacheCounterMutex

Windows SEH exceptions:

Description	Times
Exception 0x40010006 at 0x7c812aeb	1