Tencent HABO
Analysis System

SHA256:	a68272db4b475e720ede626c81d750b75ad585f18e0da766301372bbc48a3801
File type:	EXE
Copyright:	The Public
Version:	2.6.0.6---2.6.0
Shell or compiler:	COMPILER:NSIS
Sub-file information:	Detail

Key behaviour

Behaviour: Disable close message of window

Detail info: hWnd = 0x0002031c, Text = AviSynth 2.6.0 , ClassName = #32770.

Process

Behaviour: Create local thread

Detail info: TargetProcess: %temp%****.exe, InheritedFromPID = 1792, ProcessID = 3164, ThreadID = 3352, StartAddress = 7C947E
TargetProcess: %temp%****.exe, InheritedFromPID = 1792, ProcessID = 3164, ThreadID = 3356, StartAddress = 7C9302
TargetProcess: %temp%****.exe, InheritedFromPID = 1792, ProcessID = 3164, ThreadID = 3436, StartAddress = 00404E

File

Behaviour: Create file

Detail info: C:\Documents and Settings\Administrator\Local Settings\Temp\nst2.tmp
C:\Documents and Settings\Administrator\Local Settings\Temp\nsd3.tmp
C:\Documents and Settings\Administrator\Local Settings\Temp\nsy4.tmp
C:\Documents and Settings\Administrator\Local Settings\Temp\nsy4.tmp\LangDLL.dll
C:\Documents and Settings\Administrator\Local Settings\Temp\nsy4.tmp\ioSpecial.ini
C:\Documents and Settings\Administrator\Local Settings\Temp\nsy4.tmp\modern-wizard.bmp
C:\WINDOWS\system32\avisynth.dll
C:\WINDOWS\system32\devil.dll
C:\Program Files\AviSynth\gpl.txt
C:\Program Files\AviSynth\lgpl_for_used_libs.txt
C:\Program Files\AviSynth\License Translations\gpl-cs.txt
C:\Program Files\AviSynth\License Translations\gpl-de.txt
C:\Program Files\AviSynth\License Translations\gpl-el.txt
C:\Program Files\AviSynth\License Translations\gpl-fr.txt
C:\Program Files\AviSynth\License Translations\gpl-it.txt

Behaviour: Add shortcut to sensitive location

Detail info: C:\Documents and Settings\All Users\「开始」菜单\程序\AviSynth\License.lnk
C:\Documents and Settings\All Users\「开始」菜单\程序\AviSynth\Plugin Directory.lnk
C:\Documents and Settings\All Users\「开始」菜单\程序\AviSynth\AviSynth Online.url
C:\Documents and Settings\All Users\「开始」菜单\程序\AviSynth\Download Plugins.url
C:\Documents and Settings\All Users\「开始」菜单\程序\AviSynth\Example Scripts.lnk
C:\Documents and Settings\Administrator\「开始」菜单\程序\AviSynth\Uninstall AviSynth.lnk

Behaviour: Create executable file

Detail info: C:\Documents and Settings\Administrator\Local Settings\Temp\nsy4.tmp\LangDLL.dll
C:\WINDOWS\system32\avisynth.dll
C:\WINDOWS\system32\devil.dll
C:\Program Files\AviSynth\plugins\DirectShowSource.dll
C:\Program Files\AviSynth\plugins\TCPDeliver.dll
C:\Program Files\AviSynth\Uninstall.exe

Behaviour: Overwrite existing file

Detail info: C:\Documents and Settings\Administrator\Local Settings\Temp\nsd3.tmp

Behaviour: Find file

Detail info: FileName = C:\Documents and Settings
FileName = C:\Documents and Settings\Administrator
FileName = C:\Documents and Settings\Administrator\Local Settings
FileName = C:\Documents and Settings\Administrator\Local Settings\Temp
FileName = C:\Documents and Settings\Administrator\Local Settings\%temp%
FileName = C:\DOCUME~1\ADMINI~1\LOCALS~1\Temp\nsy4.tmp
FileName = C:\Program Files\AviSynth
FileName = C:\Program Files
FileName = C:\WINDOWS\system32\msvcp60.dll
FileName = C:\Documents and Settings\All Users\「开始」菜单\程序\AviSynth 2.5
FileName = C:\Documents and Settings\All Users\「开始」菜单\程序\AviSynth\Uninstall AviSynth.lnk
FileName = C:\Documents and Settings\All Users\「开始」菜单\程序\AviSynth
FileName = C:\Documents and Settings\All Users\「开始」菜单\程序
FileName = C:\Documents and Settings\All Users\「开始」菜单
FileName = C:\Documents and Settings\All Users

Behaviour: File remove

Detail info: C:\Documents and Settings\Administrator\Local Settings\Temp\nst2.tmp
C:\Documents and Settings\Administrator\Local Settings\Temp\nsd3.tmp
C:\Documents and Settings\Administrator\Local Settings\Temp\nsy4.tmp

Behaviour: Modify file

Detail info: C:\Documents and Settings\Administrator\Local Settings\Temp\nsd3.tmp ---> Offset = 0
C:\Documents and Settings\Administrator\Local Settings\Temp\nsd3.tmp ---> Offset = 32768
C:\Documents and Settings\Administrator\Local Settings\Temp\nsd3.tmp ---> Offset = 65536
C:\Documents and Settings\Administrator\Local Settings\Temp\nsd3.tmp ---> Offset = 98304
C:\Documents and Settings\Administrator\Local Settings\Temp\nsd3.tmp ---> Offset = 111977
C:\Documents and Settings\Administrator\Local Settings\Temp\nsy4.tmp\LangDLL.dll ---> Offset = 0
C:\Documents and Settings\Administrator\Local Settings\Temp\nsy4.tmp\ioSpecial.ini ---> Offset = 0
C:\Documents and Settings\Administrator\Local Settings\Temp\nsy4.tmp\ioSpecial.ini ---> Offset = 36
C:\Documents and Settings\Administrator\Local Settings\Temp\nsy4.tmp\modern-wizard.bmp ---> Offset = 0
C:\Documents and Settings\Administrator\Local Settings\Temp\nsy4.tmp\modern-wizard.bmp ---> Offset = 16384
C:\Documents and Settings\Administrator\Local Settings\Temp\nsy4.tmp\ioSpecial.ini ---> Offset = 124
C:\WINDOWS\system32\avisynth.dll ---> Offset = 0
C:\WINDOWS\system32\avisynth.dll ---> Offset = 16384
C:\WINDOWS\system32\avisynth.dll ---> Offset = 32768
C:\WINDOWS\system32\avisynth.dll ---> Offset = 49152

Registry

Behaviour: Modify registry

Detail info: \REGISTRY\MACHINE\SOFTWARE\AviSynth\
\REGISTRY\MACHINE\SOFTWARE\AviSynth\plugindir2_5
\REGISTRY\MACHINE\SOFTWARE\AviSynth\initialplugindir
\REGISTRY\MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\AviSynth\DisplayName
\REGISTRY\MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\AviSynth\UninstallString
\REGISTRY\MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\AviSynth\Publisher
\REGISTRY\MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\AviSynth\DisplayIcon
\REGISTRY\MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\AviSynth\DisplayVersion
\REGISTRY\MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\AviSynth\URLInfoAbout
\REGISTRY\MACHINE\SOFTWARE\Classes\.avs\
\REGISTRY\MACHINE\SOFTWARE\Classes\CLSID\{E6D6B700-124D-11D4-86F3-DB80AFD98778}\
\REGISTRY\MACHINE\SOFTWARE\Classes\CLSID\{E6D6B700-124D-11D4-86F3-DB80AFD98778}\InProcServer32\
\REGISTRY\MACHINE\SOFTWARE\Classes\CLSID\{E6D6B700-124D-11D4-86F3-DB80AFD98778}\InProcServer32\Thre
\REGISTRY\MACHINE\SOFTWARE\Classes\Media Type\Extensions\.avs\
\REGISTRY\MACHINE\SOFTWARE\Classes\Media Type\Extensions\.avs\Source Filter

Other

Behaviour: Create mutex

Detail info: CTF.LBES.MutexDefaultS-*
CTF.Compart.MutexDefaultS-*
CTF.Asm.MutexDefaultS-*
CTF.Layouts.MutexDefaultS-*
CTF.TMD.MutexDefaultS-*
CTF.TimListCache.FMPDefaultS-*MUTEX.DefaultS-*
MSCTF.Shared.MUTEX.EBH
MSCTF.Shared.MUTEX.AGM
MSCTF.Shared.MUTEX.MGN

Behaviour: Hide specific window

Detail info: [Window,Class] = [,ComboLBox]
[Window,Class] = [,Button]
[Window,Class] = [,Auto-Suggest Dropdown]
[Window,Class] = [Show &details,Button]

Behaviour: Find specific window

Detail info: NtUserFindWindowEx: [Class,Window] = [Shell_TrayWnd,]
NtUserFindWindowEx: [Class,Window] = [#32770,]
NtUserFindWindowEx: [Class,Window] = [CicLoaderWndClass,]
NtUserFindWindowEx: [Class,Window] = [OleMainThreadWndClass,]

Behaviour: Window information

Detail info: Pid = 3164, Hwnd=0x10320, Text = English, ClassName = ComboBox.
Pid = 3164, Hwnd=0x10324, Text = OK, ClassName = Button.
Pid = 3164, Hwnd=0x10326, Text = Cancel, ClassName = Button.
Pid = 3164, Hwnd=0x10328, Text = Please select a language., ClassName = Static.
Pid = 3164, Hwnd=0x1031c, Text = Installer Language, ClassName = #32770.
Pid = 3164, Hwnd=0x20326, Text = I &Agree, ClassName = Button.
Pid = 3164, Hwnd=0x20324, Text = Cancel, ClassName = Button.
Pid = 3164, Hwnd=0x30318, Text = AviSynth 2.6.0 -- [150419] , ClassName = Static.
Pid = 3164, Hwnd=0x10330, Text = AviSynth 2.6.0 -- [150419], ClassName = Static.
Pid = 3164, Hwnd=0x10334, Text = License Agreement, ClassName = Static.
Pid = 3164, Hwnd=0x10336, Text = Please review the license terms before installing AviSynth., ClassName = Static.
Pid = 3164, Hwnd=0x10340, Text = Press Page Down to see the rest of the agreement., ClassName = Static.
Pid = 3164, Hwnd=0x10342, Text = GNU GENERAL PUBLIC LICENSE Version 2, June 1991 Copyright (C) 1989, 1991 Fre
Pid = 3164, Hwnd=0x10344, Text = If you accept the terms of the agreement, click I Agree to continue. You must accept the
Pid = 3164, Hwnd=0x2031c, Text = AviSynth 2.6.0 , ClassName = #32770.

Behaviour: Modify process token privilege

Detail info: SE_LOAD_DRIVER_PRIVILEGE

Behaviour: Disable close message of window

Detail info: hWnd = 0x0002031c, Text = AviSynth 2.6.0 , ClassName = #32770.

Behaviour: Open event

Detail info: HookSwitchHookEnabledEvent
_fCanRegisterWithShellService
CTF.ThreadMIConnectionEvent.00000714.00000000.00000013
CTF.ThreadMarshalInterfaceEvent.00000714.00000000.00000013
MSCTF.SendReceiveConection.Event.EBH.IC
MSCTF.SendReceive.Event.EBH.IC
CTF.ThreadMIConnectionEvent.00000714.00000000.00000014
CTF.ThreadMarshalInterfaceEvent.00000714.00000000.00000014

Behaviour: Signature of executable file

Detail info: C:\Documents and Settings\Administrator\Local Settings\Temp\nsy4.tmp\LangDLL.dll(签名验证: 未通过)
C:\WINDOWS\system32\avisynth.dll(签名验证: 未通过)
C:\WINDOWS\system32\devil.dll(签名验证: 未通过)
C:\Program Files\AviSynth\plugins\DirectShowSource.dll(签名验证: 未通过)
C:\Program Files\AviSynth\plugins\TCPDeliver.dll(签名验证: 未通过)
C:\Program Files\AviSynth\Uninstall.exe(签名验证: 未通过)

Behaviour: Create event

Detail info: EventName = MSCTF.SendReceive.Event.AGM.IC
EventName = MSCTF.SendReceiveConection.Event.AGM.IC
EventName = Global\userenv: User Profile setup event
EventName = MSCTF.SendReceive.Event.MGN.IC
EventName = MSCTF.SendReceiveConection.Event.MGN.IC

Behaviour: MD5 of executable file

Detail info: C:\Documents and Settings\Administrator\Local Settings\Temp\nsy4.tmp\LangDLL.dll ---> 8c909780802ac2097ea4132e63
C:\WINDOWS\system32\avisynth.dll ---> ae68a7f8f21c51f39174f9d2dd3cf6be
C:\WINDOWS\system32\devil.dll ---> d27959321703b70120025a9356e89a7d
C:\Program Files\AviSynth\plugins\DirectShowSource.dll ---> 329ac5de00b2dbd479ba5c0d44e9e3fd
C:\Program Files\AviSynth\plugins\TCPDeliver.dll ---> 089598caf1180644c34a9e77af0d28af
C:\Program Files\AviSynth\Uninstall.exe ---> 6058de0c6190194ef16fed8201149060

Behaviour: Open mutex

Detail info: ShimCacheMutex

Behaviour: Load addtional file

Detail info: Image: C:\DOCUME~1\ADMINI~1\LOCALS~1\Temp\nsy4.tmp\LangDLL.dll.