Tencent HABO Analysis System

SHA256:	49dba7924254a61f7abe42ea0e003dfedbc033d50b49277d73b96d7e06b1736e
File type:	EXE
Copyright:	
Version:	
Shell or compiler:	PACKER:UPX 0.89.6 - 1.02 / 1.05 - 1.24 -> Markus & Laszlo
Sub-file information:	Detail

Key behaviour

Behaviour: Set special directory property

Detail info:
C:\Documents and Settings\Administrator\Local Settings\Temporary Internet Files
C:\Documents and Settings\Administrator\Local Settings\History
C:\Documents and Settings\Administrator\Local Settings\Temporary Internet Files\Content.IE5
C:\Documents and Settings\Administrator\Cookies
C:\Documents and Settings\Administrator\Local Settings\History\History.IE5

Behaviour: Modify registry of startup

Detail info: \REGISTRY\MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run\MS Kernel32

Behaviour: Get TickCount value

Detail info:
TickCount = 431125, SleepMilliseconds = 30000.
TickCount = 431171, SleepMilliseconds = 30000.
TickCount = 431296, SleepMilliseconds = 30000.
TickCount = 431343, SleepMilliseconds = 30000.
TickCount = 431468, SleepMilliseconds = 30000.
TickCount = 431500, SleepMilliseconds = 30000.
TickCount = 431515, SleepMilliseconds = 30000.
TickCount = 431531, SleepMilliseconds = 30000.
TickCount = 431546, SleepMilliseconds = 30000.
TickCount = 431562, SleepMilliseconds = 30000.
TickCount = 431578, SleepMilliseconds = 30000.
TickCount = 431781, SleepMilliseconds = 30000.
TickCount = 431796, SleepMilliseconds = 30000.
TickCount = 431812, SleepMilliseconds = 30000.
TickCount = 431828, SleepMilliseconds = 30000.

Process

Behaviour: Create local thread

Detail info:
TargetProcess: %temp%****.exe, InheritedFromPID = 1792, ProcessID = 2548, ThreadID = 2648, StartAddress = 5BA7D7
TargetProcess: %temp%****.exe, InheritedFromPID = 1792, ProcessID = 2548, ThreadID = 2652, StartAddress = 6D163F
TargetProcess: %temp%****.exe, InheritedFromPID = 1792, ProcessID = 2548, ThreadID = 2656, StartAddress = 45DC9E
TargetProcess: %temp%****.exe, InheritedFromPID = 1792, ProcessID = 2548, ThreadID = 2660, StartAddress = 5BA7D7
TargetProcess: %temp%****.exe, InheritedFromPID = 1792, ProcessID = 2548, ThreadID = 2688, StartAddress = 6D163F
TargetProcess: %temp%****.exe, InheritedFromPID = 1792, ProcessID = 2548, ThreadID = 2692, StartAddress = 45DC9E

Behaviour: Enumerate process

Detail info: N/A

File

Behaviour: Create file

Detail info: C:\WINDOWS\MSKern32.exe
C:\Documents and Settings\Administrator\Local Settings\Application Data\Identities\{CFD7C28A-208C-4447-B3FF-2FDAC
C:\Documents and Settings\Administrator\Local Settings\Application Data\Identities\{CFD7C28A-208C-4447-B3FF-2FDAC
C:\Documents and Settings\Administrator\Application Data\Microsoft\Address Book\Administrator.wab
C:\Documents and Settings\Administrator\Local Settings\Application Data\Identities\{CFD7C28A-208C-4447-B3FF-2FDAC
C:\Documents and Settings\Administrator\Local Settings\Temp\MPS2.tmp
C:\Documents and Settings\Administrator\Application Data\Microsoft\Address Book\Administrator.wab~

Behaviour: Overwrite existing file

Detail info: C:\Documents and Settings\Administrator\Local Settings\Temp\MPS2.tmp

Behaviour: Find file

Detail info: FileName = *.ht*
FileName = *.doc
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\Application Data
FileName = C:\Documents and Settings\Administrator\Local Settings\Application Data\Identities\{CFD7C28A-208C-4447-B
FileName = C:\Documents and Settings\Administrator\Application Data\Microsoft\Address Book\Administrator.wab

Behaviour: File remove

Detail info: C:\Documents and Settings\Administrator\Local Settings\Application Data\Identities\{CFD7C28A-208C-4447-B3FF-2FDAC
C:\Documents and Settings\Administrator\Local Settings\Temp\MPS2.tmp

Behaviour: Copy file

Detail info: C:\Documents and Settings\Administrator\Local Settings\%temp%****.exe ---> C:\WINDOWS\MSKern32.exe
C:\DOCUME~1\ADMINI~1\LOCALS~1\Temp\MPS2.tmp ---> C:\Documents and Settings\Administrator\Application Data\Mi

Behaviour: Set special directory property

Detail info: C:\Documents and Settings\Administrator\Local Settings\Temporary Internet Files
C:\Documents and Settings\Administrator\Local Settings\History
C:\Documents and Settings\Administrator\Local Settings\Temporary Internet Files\Content.IE5
C:\Documents and Settings\Administrator\Cookies
C:\Documents and Settings\Administrator\Local Settings\History\History.IE5

Behaviour: Modify file

Detail info: C:\WINDOWS\MSKern32.exe ---> Offset = 0
C:\Documents and Settings\Administrator\Application Data\Microsoft\Address Book\Administrator.wab ---> Offset = 0
C:\Documents and Settings\Administrator\Application Data\Microsoft\Address Book\Administrator.wab ---> Offset = 164
C:\Documents and Settings\Administrator\Application Data\Microsoft\Address Book\Administrator.wab ---> Offset = 2212
C:\Documents and Settings\Administrator\Application Data\Microsoft\Address Book\Administrator.wab ---> Offset = 6212
C:\Documents and Settings\Administrator\Application Data\Microsoft\Address Book\Administrator.wab ---> Offset = 40212
C:\Documents and Settings\Administrator\Application Data\Microsoft\Address Book\Administrator.wab ---> Offset = 176212
C:\Documents and Settings\Administrator\Application Data\Microsoft\Address Book\Administrator.wab ---> Offset = 176244
C:\Documents and Settings\Administrator\Application Data\Microsoft\Address Book\Administrator.wab ---> Offset = 176280
C:\Documents and Settings\Administrator\Local Settings\Temp\MPS2.tmp ---> Offset = 0
C:\Documents and Settings\Administrator\Local Settings\Temp\MPS2.tmp ---> Offset = 164
C:\Documents and Settings\Administrator\Local Settings\Temp\MPS2.tmp ---> Offset = 2212
C:\Documents and Settings\Administrator\Local Settings\Temp\MPS2.tmp ---> Offset = 6212
C:\Documents and Settings\Administrator\Local Settings\Temp\MPS2.tmp ---> Offset = 40212
C:\Documents and Settings\Administrator\Local Settings\Temp\MPS2.tmp ---> Offset = 176212

Registry

Behaviour: Modify registry

Detail info: \REGISTRY\USER\S-*\Identities\{CFD7C28A-208C-4447-B3FF-2FDAC596C2FD}\Identity Ordinal
\REGISTRY\USER\S-*\Identities\Identity Ordinal
\REGISTRY\USER\S-*\Identities\{CFD7C28A-208C-4447-B3FF-2FDAC596C2FD}\Software\Microsoft\Outlook Express\5.0
\REGISTRY\USER\S-*\Identities\{CFD7C28A-208C-4447-B3FF-2FDAC596C2FD}\Software\Microsoft\Outlook Express\5.0
\REGISTRY\USER\S-*\Identities\{CFD7C28A-208C-4447-B3FF-2FDAC596C2FD}\Software\Microsoft\Outlook Express\5.0
\REGISTRY\USER\S-*\Identities\{CFD7C28A-208C-4447-B3FF-2FDAC596C2FD}\Software\Microsoft\Outlook Express\5.0
\REGISTRY\USER\S-*\Identities\{CFD7C28A-208C-4447-B3FF-2FDAC596C2FD}\Software\Microsoft\Outlook Express\5.0
\REGISTRY\USER\S-*\Identities\{CFD7C28A-208C-4447-B3FF-2FDAC596C2FD}\Software\Microsoft\Outlook Express\5.0
\REGISTRY\USER\S-*\Identities\{CFD7C28A-208C-4447-B3FF-2FDAC596C2FD}\Software\Microsoft\Outlook Express\5.0
\REGISTRY\USER\S-*\Identities\{CFD7C28A-208C-4447-B3FF-2FDAC596C2FD}\Software\Microsoft\Outlook Express\5.0
\REGISTRY\USER\S-*\Identities\{CFD7C28A-208C-4447-B3FF-2FDAC596C2FD}\Software\Microsoft\Outlook Express\5.0
\REGISTRY\USER\S-*\Identities\{CFD7C28A-208C-4447-B3FF-2FDAC596C2FD}\Software\Microsoft\Outlook Express\5.0
\REGISTRY\USER\S-*\Software\Microsoft\Internet Account Manager\Accounts\AssociatedID
\REGISTRY\USER\S-*\Software\Microsoft\Internet Account Manager\Accounts\Active Directory GC\LDAP Server ID

Behaviour: Delete registry item

Detail info: \REGISTRY\USER\S-*\Identities\Changing
\REGISTRY\USER\S-*\Identities\IncomingID
\REGISTRY\USER\S-*\Identities\OutgoingID

Behaviour: Modify registry of startup

Detail info: \REGISTRY\MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run\MS Kernel32

Other

Behaviour: Modify process token privilege

Detail info: SE_LOAD_DRIVER_PRIVILEGE

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
MSIdent Logon
OutlookExpress_InstanceMutex_101897
microsoft_thor_folder_notifyinfo_mutex
c:_documents and settings_administrator_local settings_application data_identities_{cfd7c28a-208c-4447-b3ff-2fdac596c2f
c:_documents and settings_administrator_local settings_application data_identities_{cfd7c28a-208c-4447-b3ff-2fdac596c2f
c:_documents and settings_administrator_local settings_application data_identities_{cfd7c28a-208c-4447-b3ff-2fdac596c2f
c:_documents and settings_administrator_local settings_application data_identities_{cfd7c28a-208c-4447-b3ff-2fdac596c2f
MPSWabDataAccessMutex

Behaviour: Create event

Detail info: EventName = Global\crypt32LogoffEvent
EventName = WAB_Outlook_Event_Refresh_Contacts
EventName = WAB_Outlook_Event_Refresh_Folders

Behaviour: Find specific window

Detail info: NtUserFindWindowEx: [Class,Window] = [Shell_TrayWnd,]

Behaviour: Window information

Detail info: Pid = 2548, Hwnd=0x10318, Text = 确定, ClassName = Button.
Pid = 2548, Hwnd=0x1031c, Text = This file is not a Win32 file valid, ClassName = Static.
Pid = 2548, Hwnd=0x30314, Text = C:\Documents and Settings\Administrator\Local Settings\%temp%****.exe, ClassName

Behaviour: Get TickCount value

Detail info: TickCount = 431125, SleepMilliseconds = 30000.
TickCount = 431171, SleepMilliseconds = 30000.
TickCount = 431296, SleepMilliseconds = 30000.
TickCount = 431343, SleepMilliseconds = 30000.
TickCount = 431468, SleepMilliseconds = 30000.
TickCount = 431500, SleepMilliseconds = 30000.
TickCount = 431515, SleepMilliseconds = 30000.
TickCount = 431531, SleepMilliseconds = 30000.
TickCount = 431546, SleepMilliseconds = 30000.
TickCount = 431562, SleepMilliseconds = 30000.
TickCount = 431578, SleepMilliseconds = 30000.
TickCount = 431781, SleepMilliseconds = 30000.
TickCount = 431796, SleepMilliseconds = 30000.
TickCount = 431812, SleepMilliseconds = 30000.
TickCount = 431828, SleepMilliseconds = 30000.

Behaviour: Get cursor position

Detail info: CursorPos = (72,18467), SleepMilliseconds = 30000.

Behaviour: Open event

Detail info: HookSwitchHookEnabledEvent
CTF.ThreadMIConnectionEvent.00000714.00000000.00000012
CTF.ThreadMarshalInterfaceEvent.00000714.00000000.00000012
MSCTF.SendReceiveConection.Event.EBH.IC
MSCTF.SendReceive.Event.EBH.IC
Global\crypt32LogoffEvent
\SECURITY\LSA_AUTHENTICATION_INITIALIZED
Global\SvcctrlStartEvent_A3752DX
Global\PS_SERVICE_STARTED
_fCanRegisterWithShellService

Behaviour: Call Sleep function

Detail info: [1]: MilliSeconds = 30000.

Behaviour: Hide specific window

Detail info: [Window,Class] = [,ListBox]
[Window,Class] = [,Static]
[Window,Class] = [Animate1,SysAnimate32]
[Window,Class] = [List1,SysListView32]

Behaviour: Open mutex

Detail info: ShimCacheMutex
!MSFTHISTORY!
c:!documents and settings!administrator!local settings!temporary internet files!content.ie5!
c:!documents and settings!administrator!cookies!
c:!documents and settings!administrator!local settings!history!history.ie5!
WininetStartupMutex
WininetConnectionMutex
WininetProxyRegistryMutex