Tencent HABO
Analysis System

SHA256:	afe0a54b66aecdbb28311a50ec56a7c808f600986ea59da2dfaf2071a877ec8b
File type:	EXE
Copyright:	
Version:	
Shell or compiler:	PACKER:UPX 0.89.6 - 1.02 / 1.05 - 1.24 -> Markus & Laszlo [Overlay]
Sub-file information:	Detail

Key behaviour

Behaviour:	Modify registry of IE homepage
Detail info:	\REGISTRY\USER\S-*\Software\Microsoft\Internet Explorer\Main\Start Page
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\MsVbdll
Behaviour:	Get TickCount value
Detail info:	TickCount = 403359, SleepMilliseconds = 1000.

Process

Behaviour:	Create process
Detail info:	[0x00000a18]ImagePath = C:\WINDOWS\system32\wscript.exe, CmdLine = wscript C:\passion.vbs
Behaviour:	Create local thread
Detail info:	TargetProcess: %temp%****.exe, InheritedFromPID = 1792, ProcessID = 2520, ThreadID = 2548, StartAddress = 5BA7D7 TargetProcess: %temp%****.exe, InheritedFromPID = 1792, ProcessID = 2520, ThreadID = 2576, StartAddress = 6D163F TargetProcess: %temp%****.exe, InheritedFromPID = 1792, ProcessID = 2520, ThreadID = 2580, StartAddress = 45DC9E TargetProcess: wscript.exe, InheritedFromPID = 2520, ProcessID = 2584, ThreadID = 2592, StartAddress = 01002FD4, Pa TargetProcess: wscript.exe, InheritedFromPID = 2520, ProcessID = 2584, ThreadID = 2604, StartAddress = 765E964D, Pa

File

Behaviour:	Create file

Detail info: C:\WINDOWS\Passion.txt
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~
C:\passion.vbs
C:\WINDOWS\AllMail.txt

Behaviour: 修改脚本文件

Detail info: C:\passion.vbs ---> Offset = 0

Behaviour: Overwrite existing file

Detail info: C:\Documents and Settings\Administrator\Local Settings\Temp\MPS2.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\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
FileName = C:\WINDOWS
FileName = C:\WINDOWS\system32
FileName = C:\WINDOWS\system32\wscript.exe
FileName = C:\passion.vbs

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 SettC:\WINDOWS\system32\MsVbdll32.exe ---> C:\WINDOWS\system32
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\Passion.txt ---> Offset = 0
C:\WINDOWS\Passion.txt ---> Offset = 40
C:\WINDOWS\Passion.txt ---> Offset = 56
C:\WINDOWS\Passion.txt ---> Offset = 102
C:\WINDOWS\Passion.txt ---> Offset = 124
C:\WINDOWS\Passion.txt ---> Offset = 151
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

Registry

Behaviour: Modify registry

Detail info: \REGISTRY\USER\S-*\Software\Microsoft\Internet Explorer\Main\Local Page
\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

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 IE homepage

Detail info: \REGISTRY\USER\S-*\Software\Microsoft\Internet Explorer\Main\Start Page

Behaviour: Modify registry of IE key property

Detail info: \REGISTRY\USER\S-*\Software\Microsoft\Internet Explorer\Main\Default_Page_URL
\REGISTRY\USER\S-*\Software\Microsoft\Internet Explorer\Main\Search Page

Behaviour: Modify registry of startup

Detail info: \REGISTRY\MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run\MsVbdll

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-*
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
MPSWABOlkStoreNotifyMutex

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: Get TickCount value

Detail info: TickCount = 403359, SleepMilliseconds = 1000.

Behaviour: Modify process token privilege

Detail info: SE_LOAD_DRIVER_PRIVILEGE

Behaviour: Open event

Detail info: HookSwitchHookEnabledEvent
Global\crypt32LogoffEvent
\SECURITY\LSA_AUTHENTICATION_INITIALIZED
Global\SvcctrlStartEvent_A3752DX
Global\PS_SERVICE_STARTED
_fCanRegisterWithShellService
MSFT.VSA.COM.DISABLE.2584
MSFT.VSA.IEC.STATUS.6c736db0

Behaviour: Call Sleep function

Detail info: [1]: MilliSeconds = 1000.

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: _!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
ShimCacheMutex