Tencent HABO Analysis System

SHA256:	36ee4e185c6b791ae8d38118bd0e00ae3c2135c1bfcd7f3452165a18c96283dc
File type:	EXE
Copyright:	
Version:	
Shell or compiler:	COMPILER:UPX 0.89.6 - 1.02 / 1.05 - 1.24 -> Markus & Laszlo [Overlay]
Sub-file information:	Detail

File

Behaviour: Copy file

Detail info: C:\Documents and Settings\Administrator\Local SettC:\WINDOWS\system32\MsSys32.exe ---> C:\WINDOWS\system32\M

Registry

Behaviour: Delete registry key

Detail info: \REGISTRY\MACHINE\SOFTWARE\Microsoft\PCHealth\ErrorReporting\DW\

Behaviour: Delete registry item

Detail info: \REGISTRY\MACHINE\SOFTWARE\Microsoft\PCHealth\ErrorReporting\DW\DWFileTreeRoot

Other

Behaviour: Open event

Detail info: Global\crypt32LogoffEvent
HookSwitchHookEnabledEvent

Behaviour: Create event

Detail info: EventName = Global\crypt32LogoffEvent
EventName = Global\userenv: User Profile setup event