VIRUSTOTAL

SUMMARY DETECTION DETAILS RELATIONS BEHAVIOR COMMUNITY

Tencent HABO 2

File System Actions

Files Opened

C:\WINDOWS\system32\winime32.dll
C:\WINDOWS\system32\ws2_32.dll
C:\WINDOWS\system32\ws2help.dll
C:\WINDOWS\system32\psapi.dll
C:\WINDOWS\system32\imm32.dll
C:\WINDOWS\system32\lpk.dll
C:\WINDOWS\system32\usp10.dll
C:\WINDOWS\system32\wininet.dll
C:\WINDOWS\WinSxS\x86_Microsoft.Windows.Common-Controls_6595b64144ccf1df_6.0.2600.5512_x-ww_35d4ce83\comctl32.dll
C:\WINDOWS\WindowsShell.Manifest

Files Copied

+ C:\Documents and Settings\Administrator\Local SettC:\WINDOWS\system32\MsSys32.exe

Registry Actions

Registry Keys Opened

\Registry\Machine\Software\Microsoft\Windows NT\CurrentVersion\Image File Execution Options\996E.exe
\Registry\MACHINE\System\CurrentControlSet\Control\SafeBoot\Option
\Registry\Machine\Software\Policies\Microsoft\Windows\Safer\CodeIdentifiers
\REGISTRY\MACHINE\SOFTWARE\Policies\Microsoft\Windows\Safer\CodeIdentifiers\TransparentEnabled
\REGISTRY\USER\S-1-5-21-1482476501-1645522239-1417001333-500\Software\Policies\Microsoft\Windows\Safer\CodeIdentifiers
\Registry\Machine\Software\Microsoft\Windows NT\CurrentVersion\Image File Execution Options\MSASN1.dll
\Registry\Machine\Software\Microsoft\Windows NT\CurrentVersion\Image File Execution Options\CRYPT32.dll
\Registry\Machine\Software\Microsoft\Windows NT\CurrentVersion\Image File Execution Options\ole32.dll
\Registry\Machine\Software\Microsoft\Windows NT\CurrentVersion\Image File Execution Options\OLEAUT32.dll
\Registry\Machine\Software\Microsoft\Windows NT\CurrentVersion\Image File Execution Options\WININET.dll

Registry Keys Deleted

\REGISTRY\MACHINE\SOFTWARE\Microsoft\PCHealth\ErrorReporting\DW\
\REGISTRY\MACHINE\SOFTWARE\Microsoft\PCHealth\ErrorReporting\DW\DWFileTreeRoot

Modules Loaded

kernel32.dll