



000

SUMMARY

DETECTION

DETAILS

BEHAVIOR

COMMUNITY





Tencent HABO v 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\mapi32.dll

C:\WINDOWS\system32\wininet.dll

 $C: WINDOWS \\ WinSxS \\ x86_Microsoft. \\ Windows. Common-Controls_6595b64144ccf1df_6.0.2600.5512_x-ww_35d4ce83 \\ \\ comctl32.dll \\ controls_6595b64144ccf1df_6.0.2600.5512_x-ww_35d4ce83 \\ \\ controls_6595b641444ccf1df_6.0.2600.5512_x-ww_35d4ce83 \\ \\ controls_6595b641444ccf1df_6.0.2600.5512_x-ww_35d4ce83 \\ \\ controls_6595b641444ccf1df_6.0.2600.5512_x-ww_35d4ce83 \\ \\ controls_6595b641444ccf1df_6.0.2600.5512_x-ww_35d4ce83 \\ \\ controls_6595b641444500.5512_x-ww_35d4ce83 \\ \\ controls_6595b64144400.5512_x-ww_35d4ce83 \\ \\ controls_6595b6414400.5512_x-ww_35d4ce83 \\ \\ controls_6595b6414400.5512_x-ww_35d4ce83 \\ \\ controls_6595b6414400.5512_x-ww_35d4ce83 \\ \\ controls_6595b6414400.5512_x-ww_35d4ce83 \\ \\ controls_6595b641400.5512_x-ww_35d6400.5512_x\\ \\ controls_6595b641400.5512_x\\ \\ controls_6595b641400.5512_x\\$

~

Files Written

C:\WINDOWS\Passion.txt

C:\Documents and Settings\Administrator\Application Data\Microsoft\Address Book\Administrator.wab

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

 $C: \label{locuments} \begin{tabular}{l} C: \$

C:\W|NDOWS\AllMai|.txt

Files Deleted

C:\Documents and Settings\Administrator\Local Settings\Application Data\Identities\{CFD7C28A-208C-4447-B3FF-2FDAC596C2FD}\Microsoft\Outlook Express\收件箱.dbx

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

Files Copied

- + C:\Documents and Settings\Administrator\Local SettC:\WINDOWS\system32\MsVbdll32.exe
- + C:\DOCUME~1\ADMINI~1\LOCALS~1\Temp\MPS2.tmp

Registry Actions

Registry Keys Opened

\Registry\Machine\Software\Microsoft\Windows NT\CurrentVersion\Image File Execution Options\996E.exe

\REGISTRY\USER\S-1-5-21-1482476501-1645522239-1417001333-500\Software\Policies\Microsoft\Windows\Safer\Codeldentifiers

\Reaistrv\Machine\Software\Microsoft\Windows NT\CurrentVersion\Image File Execution Options\MAPI32 DLL

We use cookies and related technologies to remember user preferences, for security, to analyse our traffic, and to enable website functionality. Learn more about cookies in our Privacy Policy. Options CRYPT32.dll

Ok