



000

SUMMARY

DETECTION

DETAILS

BEHAVIOR

COMMUNITY





Tencent HABO ✓ 3

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\shell32.dll

 $C: WINDOWS \\ WinsxS \\ x86_Microsoft. Windows. Common-Controls_6595b64144ccf1df_6.0.2600.5512_x-ww_35d4ce83 \\ \\ comctl32.dll. \\ comctl32.dll. \\ comctl32.dll. \\ \\ comctl32.dll. \\ comctl32.dlll. \\ comctl32.dll. \\ comctl32.dlll. \\ comctl32.dlll. \\ comctl32.dlll. \\ comctl32.$

C:\WINDOWS\WindowsShell.Manifest

~

Files Written

C:\WINDOWS\MSKern32.exe

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

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

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

Files Deleted

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

 $\hbox{C:$\backslash Documents and Settings$\backslash Administrator$\backslash Local Settings$\backslash Temp$$\backslash Tem$

Files Copied

- + C:\Documents and Settings\Administrator\Local Settings\Temp\EB93A6\996E.exe
- + C:\DOCUME~1\ADMINI~1\LOCALS~1\Temp\MPS2.tmp

Registry Actions

Registry Keys Opened

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

\Registry\MACHINE\System\CurrentControlSet\Control\SafeBoot\Option

\Registry\Machine\Software\Policies\Microsoft\Windows\Safer\Codeldentifiers

\REGISTRY\MACHINE\SOFTWARE\Policies\Microsoft\Windows\Safer\Codeldentifiers\TransparentEnabled

\REG|STRY\USER\S-1-5-21-1482476501-1645522239-1417001333-500\Software\Policies\Microsoft\Windows\Safer\Code|dentifiers

\Registry\Machine\Software\Microsoft\Windows NT\CurrentVersion\Image File Execution Options\SHELL32.DLL

\Reaistrv\Machine\Software\Microsoft\Windows NT\Current\Version\Image File Execution Options\comctl32 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 KERNEL32.dll

Design All Applies Coft, warph Airport Misson of Walindows NTV Current Version Unage File Evenution Option of CD122 ellipses

Ok