



SUMMARY DETECTION DETAILS **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\wsock32.dll
C:\Documents and Settings\Administrator\Local Settings\Temp\EB93A6\996E.exe
C:\WINDOWS\system32\shell32.dll



Files Written

C:\WINDOWS\RUNW32.EXE
C:\WINDOWS\system32\MSVA.EXE
C:\Documents and Settings\Administrator\「开始」菜单\程序\启动\VARegistered.htm

Files Copied

- + C:\Documents and Settings\Administrator\Local Settings\Temp\EB93A6\996E.exe
- + C:\Documents and Settings\Administrator\Local Settings\Temp\EB93A6\996E.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\WSOCK32.dll
\Registry\Machine\Software\Microsoft\Windows NT\CurrentVersion\Image File Execution Options\ntdll.dll
\Registry\Machine\Software\Microsoft\Windows NT\CurrentVersion\Image File Execution Options\KERNEL32.dll
\Registry\Machine\Software\Microsoft\Windows NT\CurrentVersion\Image File Execution Options\GDI32.dll
\Registry\Machine\Software\Microsoft\Windows NT\CurrentVersion\Image File Execution Options\USER32.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.](#) Ok

