

## 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

 $C: WINDOWS \\ WinSxS \\ x86\_Microsoft. \\ Windows. Common-Controls\_6595b64144ccf1df\_6.0.2600.5512\_x-ww\_35d4ce83 \\ \\ comctl32.dll \\ controls\_6595b64144ccf1df\_6.0.2600.5512\_x-ww\_35d4ce83 \\ \\ controls\_6595b641444ccf1df\_6.0.2600.5512\_x-ww\_35d4ce83 \\ \\ controls\_6595b641444500.5512_x-ww\_35d4ce83 \\ \\ controls\_6595b64144400.5512_x-ww\_35d4ce83 \\ \\ controls\_6595b6414400.5512_x-ww\_35d600.5512_x-ww\_35d600.5512_x\\ \\ controls\_6595b6414400.5512_x-ww\_35d600.5512_x-ww\_35d600.5512_x\\ \\ controls\_6595b6414400.5512_x-ww\_35d600.5512_x-ww\_35d600.5512_x\\ \\ controls\_6595b6414400.5512_x-ww\_35d600.5512_x-ww\_35d600.5512_x\\ \\ controls\_6595b6414400.5512_x-ww\_35d600.5512_x\\ \\ controls\_6595b6414400.5512_x-ww\_35d600.5512_x\\ \\ controls\_6595b6414400.5512_x-ww\_35d600.5512_x\\ \\ controls\_6595b6414400.5512_x-ww\_35d600.5512_x\\ \\ controls\_6595b6414000.5512_x-ww\_35d600.5512_x\\ \\ controls\_6595b6414000.5512_x-ww\_35d600.5512_x\\ \\ controls\_6595b6414000.5512_x-ww\_35d600.5512_x\\ \\ controls\_6595b6414000.5512_x-ww\_35d600.5512_x\\ \\ controls\_6595$ 

 $\vee$ 

#### Files Written

C:\WINDOWS\CasperEMail.txt

### Files Copied

+ C:\Documents and Settings\Administrator\Local SettC:\WINDOWS\MsWinsock32.exe

# Registry Actions

# Registry Keys Opened

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

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

\Registry\Machine\Software\Microsoft\Windows NT\CurrentVersion\Image File Execution Options\MSASN1.dll

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

- REGISTRY/USER/S-1-5-21-1482476501-1645522239-1417001333-500/Software/CasperWorm/Author
- + \REGISTRY\USER\S-1-5-21-1482476501-1645522239-1417001333-500\Software\CasperWorm\Version

### **Process And Service Actions**