KaZaA Worm

Benjamin a ploy for profit

What do you get when you cross a file sharing network with a person desperate for advertising dollars? A worm that drives hits to a website, of course. Dubbed by various antivirus vendors as Worm.Kazaa.Benja or W32/Benjamin, the Benjamin worm disguises itself as an array of popular music and video selections. Unsuspecting KaZaA users who search on one of these topics will be presented with a file list of appropriate titles that aren't legitimate files but rather the Benjamin worm. When the file is downloaded and run, users will be presented with a fake error message:

```
Access error #03A:94574: Invalid pointer operation
File possibly corrupted.
```

Behind the scenes, the worm is busy creating a new file share folder and adding hundreds of copies of itself - all with fake titles of popular search requests. Antivirus vendor F-Secure reports that over 2000 titles are used. Examples include:

> "Deepest Purple-The Very Best of Deep Purple - Smoke on the Water"
> "Metallica - Until it sleeps"
> "Johann Sebastian Bach - Brandenburg Concerto No 4"
> "South Park Vol.3-divx-full-downloader"
> "Star wars Episode 1-divx-full-downloader"
> "F1 Racing Championship-Games-full-downloader"
> "Chessmaster 8000-Games-full-downloader"

"Apparently the worm was written to make money for the virus writer", comments Mikko Hypponen, Manager of Anti-Virus Research at F-Secure Corporation. The worm opens a webpage named benjamin.xww.de which contained advertisments. "Now the page has been taken down, but if the virus author got money based on ad views, he might have created some cashflow here".

After displaying the false error message, Benjamin creates a copy of itself named EXPLORER.SCR in the Windows\System direction and modifies the registry to load on startup.

According to F-Secure, the Benjamin worm spreads only to and from computers that have the KaZaa network clients software installed.

Manual Removal

If infected with the Benjamin worm, the following registry keys will have been modified to include the value shown:

```
[HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Run]
"System-Service"="C:\\WINDOWS\\SYSTEM\\EXPLORER.SCR"

[HKEY_LOCAL_MACHINE\Software\Microsoft]
"syscod"="0065D7DB20008306B6A1"
```

Locate and delete the values shown.
Locate and delete the file EXPLORER.SCR.
Locate and delete the Sys32 subfolder located in the Windows Temp folder.