HTML.Bother.3180

Discovered on: May 23, 2001
Last Updated on: May 23, 2001 at 03:48:57 PM PDT

HTML.Bother.3180 is script that uses ActiveX controls to perform malicious actions on your computer. The script modifies the default home page in Internet Explorer. It also appends itself to all .htm and .html files that it finds in the \My Documents and \Windows\Web folders. Finally, if the day of the month matches a random number, the default icon for .html files is changed.

Also Known As: HTML.Bother.3180.dr

Category: Virus

Infection Length: 3,180 bytes

Virus Definitions: May 23, 2001

Threat Assessment:

Wild:	Damage:	Distribution:
Low	Low	Low

Wild:

- Number of infections: 0 - 49
- Number of sites: 0 - 2
- Geographical distribution: Low
- Threat containment: Easy
- Removal: Easy

Damage:

- Payload: If a randomly generated number matches the current day of the month, the default icon for html files will be changed.
    - Modifies files: Appends itself to .htm and .html files in the WEB folder of the Windows directory and in the My Documents folder.

Technical description:

This is a viral script and not a worm. When the .html file is opened in Internet Explorer, the following message appears, and you are asked to allow the ActiveX control to run:

```
You need ActiveX enabled if you want to see this page.
Please open this page again and click accept ActiveX.
Internet Explorer
```

If you click No, the script does not run and does not infect the system. The script does not infect systems that use Netscape Navigator as the default browser.

If you allow the ActiveX control to run, or if you are using very low security settings for Internet Explorer, the script performs its malicious actions:

1. First it creates the Hello.txt file on the Windows desktop. This is a two-line text file that contains information about the origin of the script. There is no viral code present in this file, and the file should be deleted.
2. Next, the script creates the PetiK.htm file in the \Windows\System folder. This file is set as the default home page for Internet Explorer. It contains your actual home page in a small scrollable frame, and beneath it the script displays the following message:

```
Hi, you have my Worm.
It's not dangerous.
Contact Symantec Corporation (www.symantec.com/avcenter) to disinfect
your computer.
```

3. The script also searches for .htm and .html files in both the \My Documents and the \Windows\Web folders. If .htm and .html files are found in these folders, the script checks for its infection marker. If the files have not been infected, the script appends its code to the end of the file, and leaves a marker at the beginning of the file for future scanning purposes.
4. Finally the script generates a random number, and if that number matches the current day of the month, the script changes the default icon for .html files.

Removal instructions:

NAV will properly repair .htm and .html files that have been infected by HTML.Bother.3180. Files detected as HTML.Bother.3180.dr are the original dropper file, and should be deleted.

To remove the virus:

1. Run LiveUpdate to make sure that you have the most recent virus definitions.
2. Start Norton AntiVirus (NAV), and run a full system scan, making sure that NAV is set to scan all files.
3. If any files are detected as HTML.Bother.3180, click Repair. Any files detected as HTML.Bother.3180.dr should be deleted.
4. Delete the Hello.txt file from the Windows desktop.
5. Using Windows Explorer, locate and delete the \Windows\System\PetiK.htm file.

To restore the Internet Explorer Start Page:

1. Start Internet Explorer, and go the Web page that you want to set as your home page.
2. Click Tools, and then click Internet Options.
3. In the Home page section of the General tab, click "Use Current."