

Browser Helper Objects - so what?

A Browser Helper Object (BHO) is a DLL module designed as a plugin for Microsoft's Internet Explorer web browser to provide added functionality.

BHOs were introduced in October 1997 with the release of version 4 of Internet Explorer. Most BHOs are loaded once by each new instance of Internet Explorer.

However, in the case of the Windows File Explorer, a new instance is launched for each window.

Some modules enable the display of different file formats not ordinarily interpretable by the browser. The Adobe Acrobat plugin that allows Internet Explorer users to read PDF files within their browser is a BHO.

The BHO API exposes hooks that allow the BHO to access the Document Object Model (DOM) of the current page and to control navigation. Because BHOs have unrestricted access to the Internet Explorer event model, some forms of malware have also been created as BHOs. For example, the Download.ject exploit installed a BHO that would activate upon detecting a secure HTTP connection to a financial institution, record the user's keystrokes (intending to capture passwords) and transmit the information to a website used by Russian computer criminals. Other BHOs such as the MyWay Searchbar track users' browsing patterns and pass the information they record to third parties.

In response to the problems associated with BHOs and similar extensions to Internet Explorer, Microsoft added an Add-on Manager to Internet Explorer 6 with the release of Service Pack 2 for Windows XP (updating it to IE6 Security Version 1 (a.k.a. SP2). This displays a list of all installed BHOs, browser extensions and ActiveX controls, and allows the user to enable or disable them at will.

Many BHOs install toolbars in Internet Explorer, but others don't produce any visible effect. It is therefore possible that a PC contains BHOs that the owner doesn't know about. The security risk here is that the BHO doesn't need any kind of permission to install malicious components and thus spyware may be spread without the user's knowledge. For instance, the CISpring trojan uses BHOs to install scripts to provide a number of instructions to be performed [such as Adding and deleting registry values, downloading additional file(s) and executing file(s)].

Since it's relatively easy to write BHOs, many poorly written BHOs can harm the computer and compromise its security, and even sometimes destroy valuable data or corrupt system files.