

[NT] Firewall Bypassing With BHO and MSIE

Source: <http://www.derkeiler.com/Mailing-Lists/Securiteam/2003-07/0086.html>

From: SecuriTeam (support_at_securiteam.com)

Date: 07/21/03

To: list@securiteam.com

Date: 21 Jul 2003 18:28:28 +0200

The following security advisory is sent to the securiteam mailing list, and can be found at the SecuriTeam web site: <http://www.securiteam.com>

-- promotion

Beyond Security in Canada

Toronto-based Sunrays Technologies is now Beyond Security's representative in Canada.

We welcome ISPs, system integrators and IT systems resellers

to promote the most advanced vulnerability assessment solutions today.

Contact us at 416-482-0038 or at canadasales@beyondsecurity.com

Firewall Bypassing With BHO and MSIE

SUMMARY

"Internet Explorer is just like any other Win32-based program with its own memory space to preserve. With Browser Helper Objects you can write components specifically, in-process Component Object Model (COM) components that Internet Explorer will load each time it starts up. Such objects run in the same memory context as the browser and can perform any action on the available windows and modules. For example, a BHO could detect the browser's typical events, such as GoBack, GoForward, and DocumentComplete; access the browser's menu and toolbar and make changes; create windows to display additional information on the currently viewed page; and install hooks to monitor messages and actions. In short, a BHO works as a spy sent to infiltrate the browser's land."

Due to the way BHO works, it is possible to use it to send possibly sensitive information via the cooperate Firewall in a covert maner.

DETAILS

BHO is a great way to send information to the Internet under the name of

Securiteam: [NT] Firewall Bypassing With BHO and MSIE

IEXPLORER:

When IEXPLORER is started, our BHO opens a new MSIE window via the script command ("window.open"). That new IE window will also be controlled by our BHO. We then hide this new window. Then the hidden window can be used to send information out by utilizing simple HTML form information posting.

Of course, this trick can also be used to receive commands from a Trojan planter.

Example:

A BHO sample that pops up a window whenever MSIE is started and show all the events (source code included):

<<http://www.euromind.com/iedelphi/ie5tools/bho.htm>>

<http://www.euromind.com/iedelphi/ie5tools/bho.htm>

ADDITIONAL INFORMATION

Information supplied by Liu Die Yu.

All mentioned resources can be found at <<http://umbrella.mx.tc>>

<http://umbrella.mx.tc>

A BHO guide from Microsoft:

<<http://www.microsoft.com/mind/0598/browhelp.asp>> Controlling Internet

Explorer 4.0 with Browser Helper Objects

For more information on BHO:

<<http://msdn.microsoft.com/library/default.asp?url=/library/en-us/dnwebgen/html/bho.asp>> Browser Helper

Objects: The Browser the Way You Want It.

=====

This bulletin is sent to members of the SecuriTeam mailing list.

To unsubscribe from the list, send mail with an empty subject line and body to:

list-unsubscribe@securiteam.com

In order to subscribe to the mailing list, simply forward this email to: list-subscribe@securiteam.com

=====

=====

DISCLAIMER:

The information in this bulletin is provided "AS IS" without warranty of any kind.

In no event shall we be liable for any damages whatsoever including direct, indirect, incidental, consequential, loss of business profits or special damages.