

Re: how to stop transmitting ip address and harddrive contents

Source: <http://www.derkeiler.com/Newsgroups/comp.security.firewalls/2002-11/2781.html>

From: Duane Arnold (darnold92@Insightbb.com)

Date: 11/28/02

From: "Duane Arnold" <darnold92@Insightbb.com>

Date: Thu, 28 Nov 2002 02:08:03 GMT

Well, I don't know what to tell you. Because I have gone to a couple of these sites that supposedly show you the content of your <C> and not once has it been shown to me.

- 1) Put IE back into its default state.
- 2) put machine into the DMZ on the router
- 3) connected machine without router to the Internet

I went to these sites with BlackIce and nothing. I even looked at the script and RESPONSE.WRITE that had file://c:/ in it. Everything about the page displayed except for the content of the <C> being shown to me. So, I don't know what else can be stopping it, other then BlackIce.

I did a cut/paste of file://c:/ into the IE Address Box and pressed the GO and it certainly did it. It just will not do it from a Website across the Internet in a script.

I am using Win 2k and have done some O/S hardening, but I have done nothing that's stopping file://c:/ from executing.

And yes, I view that as a security issue. I see it as an issue anytime from across the Internet a machine can be asked to do something like that and it does it. No matter how trivial it may be. The machine was ask to do something and it did.

So, from my view point or in my opinion, the machine is open to attack.

Duane :)

"Eye of the Storm" <noemail@noemail.net> wrote in message news:j9pauusmn71sal8hdmqt4eq2ihog0j0lr@4ax.com...

> On Wed, 27 Nov 2002 22:18:04 GMT, "Duane Arnold"

> <darnold92@Insightbb.com> wrote:

>

> >Yeah, maybe you do and maybe you don't see. I can go to the same website

and

> >the content of my <C> is not shown to me. Like I said before in a long
> >drawn out previous post thread, I view that file://c:/ being executed in
> >script as a potential security issue to the machine. IE on my machines is
in
> >its default unsecured and unprotected state. And yet BlackIce on the
> >machines will not let file://c:/ or anything like it coming in the
network
> >traffic to be executed.
>
> I don't see how it could possibly be a security issue. Besides, I am
> using BlackICE also, on the paranoid setting, and it in no way blocks
> Internet Explorer content.