

Re: Why does XP establish HTTP connection when browsing network shares?

Source: <http://www.derkeiler.com/Mailing-Lists/securityfocus/focus-ms/2002-05/0155.html>

From: Dave Feustel (dfeustel@mindspring.com)

Date: 05/27/02

From: "Dave Feustel" <dfeustel@mindspring.com>
To: "o00o_j" <o00o_j@yahoo.com>, <focus-ms@securityfocus.com>
Date: Mon, 27 May 2002 10:06:21 -0500

I have discovered since installing Zone Alert 3.0 that XP IE/OE *constantly* load components that attempt to connect to the internet whenever I do simple things like print a file, send email, etc. NONE of the things I'm doing that generate these requests have ANY need to access the internet. These components load requests even occur after I have attempted to exit these programs. The most common result of denying internet access to these components is that OE can no longer send email (tcpip error) and IE starts reporting 100% page not found. Both of these errors are cleared by exiting IE and/or OE and restarting the malfunctioning program.

There is one component load request that, when denied, *instantly* and repeatedly crashes XP. This behavior has been confirmed by other XP users.

I assume I have a virus (possibly created by MS :-) on my machine.

Note: I'm running XP Pro with all critical updates and most application updates applied. This behavior appeared about a month ago.

Dave Feustel
<http://www.mindspring.com/~dfeustel>
260-483-1857

----- Original Message -----

From: "o00o_j" <o00o_j@yahoo.com>

To: <focus-ms@securityfocus.com>

Sent: Friday, May 24, 2002 2:13 PM

Subject: Why does XP establish HTTP connection when browsing network shares?

> I've noticed some strange behavior from our IDS. Ever since deploying
> Windows XP to our network, I've been seeing connection attempts to port 80
> on servers not running HTTP daemons. Taking a closer look, I discovered
> darn near every one was from a windows XP machine belonging to techs who
> service those servers. I left it as a curiosity until one day, by chance,
> I noticed my machine triggered the same IDS alarm right after I opened a

SecurityFocus Microsoft: Re: Why does XP establish HTTP connection when browsing network shares?

> network share (C\$) on that machine.
>
> Digging down further, I captured a TCP conversation between my PC (an XP
> machine) and a server. Sure enough, towards the end of all the SMB jargon
> is an HTTP exchange, with my client at one point sending the following:
> ----
> OPTIONS / HTTP/1.1
> translate: f
> User-Agent: Microsoft-WebDAV-MiniRedir/5.1.2600
> Host: [NetBIOS name of host i'm trying to connect to]
> ----
> and receiving back a canned warning from my IDS. I'm sure this is nothing
> to worry about, however I'm concerned about disabling it to limit false
> positives on my IDS. Any ideas? thoughts? Any info. would help here...
> our XP guru in-house had never heard of this before. thanks in advance.
>
> -j
>
>
> _____
> Do You Yahoo!?
> LAUNCH – Your Yahoo! Music Experience
> <http://launch.yahoo.com>

-
- **Previous message:** [Mike Coppins: "Re: About ping request?"](#)
 - **In reply to:** [_o0o_ j: "Why does XP establish HTTP connection when browsing network shares?"](#)
 - **Messages sorted by:** [\[date \]](#) [\[thread \]](#) [\[subject \]](#) [\[author \]](#) [\[attachment \]](#)