

SecurityFocus BASICS: RE: Just a questionNEWWWS !!!!

RE: Just a questionNEWWWS !!!!

Source: <http://www.derkeiler.com/Mailing-Lists/securityfocus/security-basics/2002-02/0994.html>

From: Douglas Gullett (dougg03@comcast.net)

Date: 02/27/02

Date: Wed, 27 Feb 2002 13:26:22 -0500

From: Douglas Gullett <dougg03@comcast.net>

To: Security-Basics <security-basics@security-focus.com>

Windows 98 machine?

Run "msconfig" and remove the support-http.exe program from start up and remove it from the startup list in the System Registry. Also go to the file and left-click on it and look at it's properties. It might have some more company information that will might jog your memory about it being something you installed or something someone else has tricked you into installing.

Also, see if you can go to your "Control Panel" and "Add/Remove" the program. More than likely, if it is a Trojan, it will try to mutate itself and change its name, and install itself all over the place.

Either way, I wouldn't trust it, because it sounds like it is trying to be covert, and I am a control freak. Hunt it and kill it like the invader it is!

Douglas Gullett, CCNA, CCDA, CCNP

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

From: Bassam ALHUSSEIN [<mailto:bhussein@scs-net.org>]

Sent: Saturday, February 23, 2002 10:32 AM

To: SECURITY-BASICS@securityfocus.com

Subject: Just a questionNEWWWS !!!!

Hi Again thank you all for answering, but I've got some news

I didn't use fport (which was a proposition of someone of you), but I tried to block this address by ZoneAlarm Pro that is installed and running.

Zapro gave me then an alert every 20 seconds, and said that Microsoft outlook express

tried to connect to

www.myhost.com which resolves in the browser directly to weguardyou.com

....!!

the alert is :

" Your computer was prevented from connecting to a restricted site (www.myhost.com).

User: Bassam ALHUSSEIN

RE: Just a questionNEWWWS !!!!

SecurityFocus BASICS: RE: Just a questionNEWWWS !!!!

Program: Microsoft Outlook Express .
Time: 23/02/2002 03:34:20 PM "

the problem is that I never visited that site before or downloaded something from there ...!!!

softwares that I use at startup are : some Norton utilities and AV, ZoneAlarmPro, and getright !!

I have had these alerts even when outlook is not running ...!!! So when I passed on PROGRAMS SETTINGS in ZApr I found TWO outlooks !!!!

1) Outlook Express (which is the file msimn.exe)
2) Microsoft Outlook Express (which is support-http.exe) and it is this one that was trying to connect to myhost.combut why ??????? (it exists even in the registry to run at the startup ..!! wow but with name of http tunnel ??

I remember ..http-tunnel is a program I used once to bypass my the proxy server of my ISP that blocks free email sites ...!!!)

what do you think ??? should I still block the address and have the alerts every 20 sec...

should I delete that key from the registry ??? Do you know if support-http is really a program from microsoft ? (cause it is in the system folder and http-tunnel that I used is just one exe file on another hard drive)
I am losthelp

I sent email to support@weguardyou.com but got no answer

Bisso

-
- **Previous message:** [Hornat, Charles: "RE: The Best Network Scanner?"](#)
 - **In reply to:** [Bassam ALHUSSEIN: "Just a questionNEWWWS !!!!"](#)
 - **Messages sorted by:** [\[date \]](#) [\[thread \]](#) [\[subject \]](#) [\[author \]](#) [\[attachment \]](#)