

Re: man in the middle

Source: <http://www.derkeiler.com/Newsgroups/microsoft.public.security/2008-03/msg00119.html>

- *From:* "BoaterDave" <BoaterDave@xxxxxxxxxxxxxxxx>
 - *Date:* Wed, 19 Mar 2008 16:17:15 -0000
-

Hello Kerry Brown :)

I feel there is much merit in what you say. FYI I did raise this topic here <http://aumha.net/viewtopic.php?t=26677&start=0&postdays=0&postorder=asc&highlight=> before I became persona non grata at AumHa.

Are you aware of any way to check whether or not a router has been compromised – *before* one follows the procedure you have outlined. I should be interested to learn more about this subject. Do you (or anyone else reading here) have any pointers as to where to begin?

I found this item which I found interesting – others may too:–
<http://www.pcadvisor.co.uk/news/index.cfm?newsid=12026>

A fairly recent news item here, too:
<http://www.pcpro.co.uk/news/173883/chinese-backdoors-hidden-in-router-firmware.html>

—
Dave

"Kerry Brown" <kerry@xxxxxxxxxxxxxxxxxxxx*a*m> wrote in message <news:3DC4DC0A-9FCB-43ED-94AD-97E1F2975E0E@xxxxxxxxxxxxxxxx>

I forgot to add – Turn off uPNP on the router after you flash it, reset it, and add an admin password.

—
Kerry Brown
MS-MVP – Windows Desktop Experience: Systems Administration
<http://www.vistahelp.ca/phpBB2/>

"Kerry Brown" <kerry@xxxxxxxxxxxxxxxxxxxx*a*m> wrote in message <news:362DBFF1-1199-47A0-81E0-1E4446F91F81@xxxxxxxxxxxxxxxx>

It sounds like your router may have been compromised.

Re: man in the middle

Unplug one of your computers from the router. Do a clean install of Windows on this computer making sure you delete all partitions then recreate them during the install. Leave this computer unplugged from the router. Don't worry about updating it just yet. On a different computer download the latest firmware for your router. Burn this file to a CD or copy it to a flash drive. Make sure there are no other files on the CD or flash drive. Unplug all of the computers from the router. Unplug the router from the Internet. Reset the router to the factory defaults. Plug in the computer with the fresh Windows install. Use it to flash the router with the downloaded firmware. Reset the router again. Set a password for the admin account. Plug the router back in to the Internet and update this computer. Do not plug in any of the other computers until they have been wiped clean and a fresh install of Windows done.

The key is to flash the router with a clean computer then set a password on the router before reconnecting to the Internet.

--

Kerry Brown

MS-MVP – Windows Desktop Experience: Systems Administration

<http://www.vistahelp.ca/phpBB2/>

"sweathog" <sweathog@xxxxxxxxxxxxxxxxxxxxxxxxxxxx> wrote in message <news:046E1C80-CFEB-48C4-A37B-F10C639BA204@xxxxxxxxxxxxxxxxxxxx>

I'm sorry I'm way beyond frustrated. I have no difficulty in admitting the opposition is much better than I in witts and skill. This isn't my trade. Okay to continue... the only way I could get all the 92 windows update patches was with a fixed ip address at work and behind their firewall. After that...Use of any dynamic ip address,with mac address changed, just wouldn't remain secure. And further formattes and reinstals I'd just get failures to install certain patches,that is with Norton 360 cd loaded as well as Kasperskys 2008 loaded and installed at different times. Trend micro, and pctools I had downloaded. (and yes I also have a dlink 604 router)

Re: man in the middle

i don't download any crap. period we're talking one authentic windows xp and its updates and one firewall/antivirus and its updates NO FURTHER SURFING AT ALL

Shenan Stanley" wrote:

sweathog wrote:

4 firwalls/antivirus products in one month. I've come the the conclusion that there is no security on the internet beyond unplugging your machines permanently. I reformated 3 computers 5 times, reinstalled the windows xp sp2 and updated, and even went so far as to change the mac addresses on the network cards. Within days windows system security settings, and product firewalls would change and it would be downhill from there, not counting the money spent.

In conclusion I've had to cancel my personal isp and email account, what was happening was that I would get these trial versions of security software both downloaded and cds, like them, buy them using https and then they would send me email confirmation

Re: man in the middle

and a link to download the full versions.

Someone had cracked my email and was sending me to spoofed websites. It didn't matter how often I would reformat and reinstall the os after I found this out and NOT use the email.

My question is how is this possible that this hacker could still track me?

PA Bear [MS MVP] wrote:

So How Did I Get Infected Anyway?

<http://www.wilderssecurity.com/showthread.php?t=27971>

sweathog wrote:

It is really as I said, there is no security. If this is all microsoft has as an answer. Watch your active x when downloading free programs.... big deal ! How about wuacle.exe which is the windows update program being modified right from a clean format and install, after your done with the installation cd. You need the active x to run that and you certainly need the updates.

You can be hacked in any number of ways – however – given your first post – either you are being targeted by someone specifically for some vindictive

Re: man in the middle

reason and your skill-set is not enough to
match wits with their tools
or
just the latter. ;-P

How about including the 92
security patches in new os
instalation
cds so you don't have to go
on-line to get them as a
solution
instead.

Can be done by you, someone with the
ability to follow directions and a
CD
burner or in some cases – many more
patches are already included in
some
versions of the CD you can buy.

I'd buy a mac if I was
certain that it couldn't also
be dns cache
poisoning.

Go ahead – You'll probably run Windows on
it as well – most current mac
users do. ;-)

To hell with it don't bother
replying.

Why not?

You are – as I said – either being targetted
and/or don't have the
skills
necessary to prevent being hacked. You
either are missing something
more
obvious each time you supposedly 'start
fresh' or whom ever is
targeting you
has inside information that allows them to

Re: man in the middle

take over.

With a decent and properly configured NAT
router, the Windows Firewall,

a

good and properly obtained and updated
AntiVirus and no 'questionable'
applications installed (trusted apps only,
original installation media,

etc.) – what you say is happening to you
would not happen without a

slip up

on your part or someone who has inside
access already.

--

Shenan Stanley

MS-MVP

--

How To Ask Questions The Smart Way

<http://www.catb.org/~esr/faqs/smart-questions.html>