

Re: network routing without my permission

Source:

http://www.derkeiler.com/Newsgroups/microsoft.public.windowsxp.security_admin/2005-08/1284.html

From: Cindy (*Cindy_at_discussions.microsoft.com*)

Date: 08/24/05

Date: Wed, 24 Aug 2005 10:27:03 -0700

Kerry,

I did do most of the things you have suggested except flash router bios...didn't know about that. Matter of fact I gave up and am only working with one computer at a time...one is horriably taken over and not being used for ANYTHING important.

The one computer I am working with is not and has not been connected to the router for quite a while. The router firewall log is how I found the problem in June that caused me to disconnect and start again.

The software I install BEFORE connecting to internet is WinXP sp2 and McAfee Security Suite 7. I then have to use the motherboard software CD to update the network card. I have the Microsoft book: Windows SP Inside Out and use it to disable services not needed. Then I turn off automatic updates and connect to the internet and update McAfee. Then I update WinXP.

I have a list of some of the IPs needed to be blocked and block them before going online. Still I notice activity happening shortly after going online. This is why I am wondering if somehow MY internet IP has somehow connected somewhere "out there" that automatically connects the computer and writes something to the registry. I don't have much registry knowledge. I have been reading through the registry and searching for help on the internet as I go along.

I do believe something actually installs itself and rewrites .dll's because the dll's used are WinXP.

Thank you for your help...keep sending suggestions...I will update!

"Kerry Brown" wrote:

- > "Cindy" <*Cindy@discussions.microsoft.com*> wrote in message
- > *news:A34678C8-FFA5-46D2-B765-ADBE8853566B@microsoft.com...*
- > > *About 6 months ago I found out my 2 WinXP computers had been hijacked.*
- > > *After*
- > > *working with wonderful help of Microsoft tech support I thought I was able*

> > to
> > *correct the problems...but I was wrong!*
> >
>
> *I think the key to your problems is in this statement "my 2 WinXP computers"*
> *Did you have both computers disconnected from the Internet while they were*
> *being cleaned? The procedure is to disconnect everything from the Internet*
> *including the router. Disconnect both computers from the router. Delete all*
> *partitions on all hard drives on both computers then reinstall Windows.*
> *Better yet use a utility to overwrite track zero on all hard drives. Make*
> *sure the router is not connected to the Internet. Reset the router to the*
> *factory settings as per the manual. Hook up one of the computers to the*
> *router and make sure the router is not set for remote management and change*
> *the password for it. You may even want to flash the BIOS of the router. This*
> *is to ensure it is not the router being hacked. Hook up the router to the*
> *Internet and hook up the remaining computer to the router. Download and*
> *install the latest drivers and Microsoft Updates for both computers. Install*
> *a good antivirus package on both computers. If you still get hacked then it*
> *must be some program you are installing that does it.*
>
> *Kerry*
>
>
>