

Re: Problems with an Outside Threat who is accessing my computer I

Source: <http://www.derkeiler.com/Newsgroups/microsoft.public.security/2005-02/0942.html>

From: Roger Abell (*mvpNOSpam_at_asu.edu*)

Date: 02/20/05

Date: Sun, 20 Feb 2005 11:26:38 -0700

What you failed to do is follow the suggestions given to you in this thread, twice by myself, and also by others, namely

1. clean install with hard disk format while network is not connected

(you are using long, difficult passwords, right?)

2. turn on the built-in firewall, then connect the network and visit Windows Update until there are no more critical and security updates recommended.

Only then consider installing third-party software, like the McAfee that you seem to have installed first, and you say required you to first turn on the internet connection. That is a critical error – enabling network before the system is secured.

Failing to be secured before connecting to the internet can make you system subjected to any number of automated worm based invasions. There may be no one in particular going after you and your system – just a network of other infected machines looking to add to their number – perhaps with some one or group ultimately able to pull strings.

However, if this is some one person directly targetting your machine, then they are rather dumb as being so predictable makes they vulnerable to you if you were to have sufficient evidence to interest local law enforcement. All you would need to do is repeat your process and bang, there they are, at it again. No, it is not someone. It is just network worms trying to enslave another machine in some bot net, perhaps one that does still have a master back behind it, perhaps one that is just spreading without control.

I repeat –

The only way to install is with a fresh format without the network connected. The preferred way to connect the network is only after all critical and security service has

microsoft.public.security: Re: Problems with an Outside Threat who is accessing my computer I

been installed, starting with the latest service pack. If that cannot be done offline, then after making sure that passwords are complex, long, difficult, etc. turn on the built-in firewall then connect the network and visit Windows Update as soon as the network connectivity is available, and revisit it until no more critical or security patches are found needed.

--

Roger Abell

Microsoft MVP (Windows Security)

MCSE (W2k3,W2k,Nt4) MCDBA

"Sidney" <Sidney@discussions.microsoft.com> wrote in message news:80353DCD-18A9-44E6-AF0F-0F0A474BAF89@microsoft.com...

> Hello,

>

> When I came the desktop after formatting the hard drive, I installed entire

> mcafee security center, this mcafee security center was factory installed on

> this dell computer system(and also this mcafee security center is on a

> resource cd from dell) and I enabled the mcafee personal firewall plus

> services first, then the mcafee virus scan and then the mcafee privacy

> services.

>

> There is no wireless in the house.

>

> When I start the computer system up in the mornings, the mcafee personal

> firewall plus services is disabled, the mcafee virus scan program is

> disabled

> and when I restart the mcafee personal firewall plus services, in the

> services, I receive this error message:

> Firewall Background Services Stopped/ A user or other application has

> stopped the mcafee personal firewall plus services.

>

> I have uninstalled and reinstalled and have performed a clean install of the

> entire mcafee security center and I am still faced with the same problems

> with the entire mcafee security center and the mcafee personal firewall

> plus

> services being disabled.

>

> I have uninstalled and reinstalled the mcafee virus scan program, numerous

> times and still the mcafee virus scan program is not listed in the

> services.

>

>

>

> "Matt Gibson" wrote:

>

> > So, when you finally connected the computer to the internet, did you have a

> > firewall running?

> >

> > When you're installing software, is it all from retail media? There are no

> > burned copies?

> >

> > Do you have wireless anywhere in the house?

> >

> > If this is indeed true, and not an elaborate troll, this is interesting.

> >

Re: Problems with an Outside Threat who is accessing my computer I

microsoft.public.security: Re: Problems with an Outside Threat who is accessing my computer I

> > Matt Gibson - GSEC
> >
> > "Sidney" <Sidney@discussions.microsoft.com> wrote in message
> > news:6B11F39D-166E-4351-9E1F-8602619DA4E8@microsoft.com...
> > > Hello,
> > >
> > > I know that I sound like a broken record, singing the same old songs:
> > >
> > > I followed the advice and technical information that was given and a
new
> > > hard drive was installed on 02/15/05 and I had to enable internet
access
> > > in
> > > order to install the mcafee security center programs.
> > >
> > > Because of the many computer problems that I am facing, I formatted
the
> > > hard
> > > drive and I am still faced with the same computer problems:
> > >
> > > I installed a KL-Detector and this program reports that I have a
KEYLOGGER
> > > on my computer system:
> > >
> > > C:\Windows\system32\wbem\logs\webmess.log was modified
> > >
> > > C:\Windows\system32\wbem\logs was modified
> > >
> > > C:\PROGRA~1\SPYWAR~3\common.ini was modified
> > >
> > > C:\Windows\Prefetch was modified
> > >
> > > Formatting the hard drive, Reinstalling the Operating System, Clean
> > > Installs, System Restores, Changing my Passwords Frequently, Clearing
the
> > > Start up Lists, Config StartUp Programs and various others
troubleshooting
> > > steps are not removing and preventing this Outside Threat from
Accessing
> > > this
> > > computer system.
> > >
> > > Thank You,
> > >
> > >
> > >
> > >
> > >
> > >
> > > "Phillip Windell" wrote:
> > >
> > >> "Sidney" <Sidney@discussions.microsoft.com> wrote in message
> > >> news:87EAA5BB-0A73-4E9B-A0F5-CAE6A328354E@microsoft.com...
> > >> > Do you know of a good tracking software to find the IP address of
this
> > >> > outside threat?
> > >>
> > >> There is no such thing because it can not be done.
> > >>
> > >> > Because the firewall is not providing an accurate reading of
> > >> > his IP address,
> > >>

microsoft.public.security: Re: Problems with an Outside Threat who is accessing my computer I

> > >> Firewall don't provide IP addresses, they just report what they are
told.
> > >>
> > >> > because he is using a different zip code for his IP address,
> > >> > so that he can remain uncatchable.
> > >>
> > >> IP address have nothing to do with Zip Codes.
> > >>
> > >> Perhaps if the Post Office used IP address I could stop my junk
postal
> > >> mail
> > >> with a firewall. But would the Mailman be "statefull"? Hmmm.....
> > >>
> > >> --
> > >>
> > >> Phillip Windell [MCP, MVP, CCNA]
> > >> www.wandtv.com
> > >>
> > >>
> > >>
> >
> >
> >