

## Re: Downloading updates in advance

---

*Source:*

[http://www.derkeiler.com/Newsgroups/microsoft.public.windowsxp.security\\_admin/2006-02/msg00133.html](http://www.derkeiler.com/Newsgroups/microsoft.public.windowsxp.security_admin/2006-02/msg00133.html)

---

- *From:* "Steven L Umbach" <n9rou@xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx>
  - *Date:* Fri, 3 Feb 2006 15:34:17 -0600
- 

Thanks for the detailed explanation. Did you enable the firewall in XP before you connected to the internet? It is enabled by default in SP2 but not in earlier versions and you should verify that it is in the properties/advanced for your network adapter. I would recommend that you download SP2, burn it to a cdrom and install it before connecting to the internet after a fresh install and then go to Windows Updates. The messenger service messages you receive indicate that you do not have a firewall protecting your computer and those messages are adware messages which are trying to trick you into buying or downloading their product that probably has more spyware. Those messages do NOT mean that there is necessarily anything wrong with your computer or indicate a hack or malware infection. If you make sure that you have the XP firewall enabled and disable the messenger service [done by default in SP2] I would be extremely surprised if you still get those messages. You can use services.msc to open your services and find the messenger service and set it to disabled and make sure it is not started. You can simply select stop to stop the service after you set the startup type to disabled for it. I bet it is frustrating reactivating all the time. You can go to the link at <http://scan.sygatetech.com/> to check your firewall configuration. --- Steve

"omi" <omi@xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx> wrote in message <news:A18FA7C8-F456-4F00-863E-A5AF06C35539@xxxxxxxxxxxxxxxxxxxx>

ok, to prove my point i did another install

i changed my ip a few times and then released it  
i disconnected the internet cable  
i formatted my drive twice (normal & fast)  
installed winxp-home (original cd-rom)  
installed msi-mainboard (original cd-rom)  
(rebooted when nessecairy)

when i inserted the internet cable to activate winxp:  
- immediatly i have a constant up-& downstream  
- after a minute or so i get following pop-up messages:

Messenger-Service

Re: Downloading updates in advance

Message from MICROSOFT to USER

Critical Error

The Microsoft Windows system contains invalid registry entries and your computer will crash. Please download the Windows registry application from:

[www.fixed-pc.com](http://www.fixed-pc.com)

To fix your system immediatly

<<a few seconds later>>

Messenger-Service

Message from Microsoft to inform you about a virus detection.

Critical System Error ! The Windows registry appears to be infected.

Please go to the Universal Registry Infection Cleaner at

[www.cleanmyharddrive.com](http://www.cleanmyharddrive.com) to scan and repair the system registry.

<< every now and then i get diverse popups like this>>

i did not install the 35,3Mb NIS, so that's not it

i only installed the original winxp & msi mainboard

no other hd's are connected

i did not load any files except the 2 i mentioned above (winxp & msi)

those 2 are on original cd-roms so they can't be infected

now there's no point updating winxp or msi

installing NIS & updating also makes no difference

At this time my winxp-key is blocked by MS because i have reinstalled so much, i have to phone them every time to get a new key which contains numbers

only.

The dude on the other side advised me to phone the technical staff instead of reinstalling all the time... because i live from my invalid-payment i do

not have the money to do so, although i found that such assistance should be

free of charge.

Luckely there a free forums like this.

I hope you guys can help me out with this problem.

thnx in advance

omi

"Steven L Umbach" wrote:

All that can certainly happen but you indicated that your computer is being

hacked right after a pristine install of the operating system and just the

operating system with the Windows Firewall enabled by just going to Windows

## Re: Downloading updates in advance

Updates. Again what makes you think it has been hacked just doing that and what evidence such as malicious processes running? Maybe there is an explanation for what you think is being hacked or malicious activity. Even so from your description just because your NIS firewall gives you pop up alerts and says that cookies are being created does not mean a computer has been hacked or infected with malware as that can all be normal.

Firewall alerts do not necessarily mean hack attempts and most often don't but are just asking you questions about what network activity you want to allow or not and in general software firewalls do a poor job in scaring users because of all the alerts for normal network activity such as dns name resolution requests, file and print sharing, computer browser service, or when an application goes to the publishers website to check for updates which is why I usually recommend that users use the Windows Firewall or an internet router or firewall device and forget a firewall like NIS. CPU useage and memory useage can be tracked via Task Manager and you can see what processes are hogging memory or CPU cycles. Maybe you have a program with a memory leak or incomaptibility between applications though of course spyware will make the computer seem to run slow. I have also seen power supply problems cause poor performance of a computer that normally should work well. If booting into Safe Mode makes the computer perform a lot better then you have a problem with a startup application/service/driver that could be related to malware/spyware and you can troubleshoot with msconfig by doing selective startup. --- Steve

"omi" <omi@xxxxxxxxxxxxxxxxxxxxxxxxxxxx> wrote in message  
[news:052B9215-C42B-4248-ABF0-BD7A1D3210CE@xxxxxxxxxxxxxxxxxxxx](mailto:news:052B9215-C42B-4248-ABF0-BD7A1D3210CE@xxxxxxxxxxxxxxxxxxxx)

i have also done what you describe scores of times in the past without problems i am 110% sure that what i am experiencing is abnormal, i might be a semi-noob on the technical side of computers, but i'm no idiot. If you would see the way my cpu is working, the way NIS gives popups, the way i have internet traffic without me doing anything, the way NIS allows

Re: Downloading updates in advance

cookies...  
and all of these things are happening the second i got  
infected. None  
of  
those things were happening in the past.

"Steven L Umbach" wrote:

How do you know you are being hacked and  
what evidence? An attacker  
can  
not  
get past the Windows Firewall as it does not  
allow inbound connections  
by  
default that are not in response to traffic that  
was initiated by your  
computer and a correctly installed pristine  
operating system from  
authentic  
Windows XP install disk would have no  
malware on it. I have done what  
I  
suggested scores of times without any  
problem what so ever. You are  
right  
about changing IP address though as that has  
nothing to do with  
increasing  
security in your situation. ---- Steve

"omi"

<omi@xxxxxxxxxxxxxxxxxxxxxxxxxxxx>

wrote in message

[news:02551193-BB8B-40F5-BC31-E6C6876B267B@xxxxxxxxxxxxxxxxxxxx](mailto:news:02551193-BB8B-40F5-BC31-E6C6876B267B@xxxxxxxxxxxxxxxxxxxx)

i've tried your discription  
about 20 times last month  
formatting the drive,  
installing winxp & msi  
mainboard from original  
cd-roms  
(offline)  
connecting to the internet &  
updating winxp... 1st or 2nd  
time i  
connect  
to  
update i get hacked...

Re: Downloading updates in advance

changing ip doesn't help  
this is a serious issue that  
developpers should look  
into  
there's no way i load  
infected files when  
installing/updating  
i've tried it again today  
same problem  
:((((((((((((((((((((((((((((((((

"Steven L Umbach" wrote:

If you did a  
pristine  
install of  
the  
operating  
system from  
a  
genuine  
Windows  
install disk  
and either  
enable  
Windows  
Firewall or  
are behind  
an  
internet  
router/firewall  
device that  
does not  
allow any  
unsolicited  
inbound  
traffic  
you should  
not have a  
problem  
with getting  
Windows  
Updates  
without  
becoming  
infected or  
hacked.  
However I  
suggest that  
you go to

## Re: Downloading updates in advance

Windows  
Updates  
first  
thing before  
installing  
any  
software on  
your  
computer  
after the  
fresh  
install. I do  
this a lot  
with never a  
problem  
and the next  
thing I  
do  
is  
to  
install  
antivirus  
software  
and update  
it  
immediately.  
Then when  
you  
are  
done  
if you are  
not  
protected by  
an internet  
router or  
firewall  
device  
then  
disconnect  
from the  
network and  
disable the  
Windows  
Firewall  
before  
you  
install  
another  
software  
firewall and  
make sure it

## Re: Downloading updates in advance

is enabled  
before  
connecting  
to the  
internet  
again.  
Personally I  
like using  
the  
Windows  
Firewall  
and do not  
like all the  
noise that  
other  
software  
firewalls  
generate  
with all the  
pop  
messages  
though they  
have there  
place  
especially  
on a shared  
computer  
where you  
want to  
restrict what  
applications  
a  
user  
can  
use to  
access the  
internet. If  
you  
continue to  
have  
problems I  
might  
suspect  
that you  
have  
infected  
files in the  
applications  
or data files  
that  
you

Re: Downloading updates in advance

are  
restring to  
your  
computer  
which you  
should be  
scanning for  
malware  
before  
you  
restore/install  
on your  
computer.  
--- Steve

<http://www.microsoft.com/athome/security/protect/windowsxpsp2/De>

--- Protect

Your PC

tips

<http://scan.sygatetech.com/>

--- Check

your  
firewall  
configuration  
here  
for  
inbound  
threats

"omi"

<omi@xxxxxxxxxxxxxxxxxxxxxxxxxxxx>

wrote in

message

<news:263BB0C6-F1C3-4360-B90E-AB77652317A2@xxxxxxxxxxx>

1)  
that's  
where  
the  
problem  
is,  
when  
i  
go  
online  
for  
updating  
i  
get  
hacked,  
changed

Re: Downloading updates in advance

my  
IP  
zillion  
times,  
no  
luck

3)  
i  
have  
no  
scanner  
or  
printer  
installed  
or  
even  
connected  
i  
get  
5-10  
popups  
from  
NIS  
about  
this  
very  
rapidly...  
i  
don't  
think  
that's  
normal  
also  
when  
i  
open  
a  
webpage,  
NIS  
allows  
+/-  
50  
cookies  
for  
each  
webpage  
also  
i  
got  
a

Re: Downloading updates in advance

NIS  
popup  
request  
for  
Ikernel.exe  
to  
connect  
to  
a  
DNS-server  
(blocked  
it)  
i  
wunder  
if  
there's  
some  
permanent  
RAM  
in  
my  
pc,  
not  
the  
ram-sticks  
but  
something  
like  
the  
BIOS...

4)  
thnx  
for  
the  
tip..  
i  
changed  
the  
registry  
to  
prevent  
messenger  
from  
running

5)  
i  
was  
able  
to

Re: Downloading updates in advance

install  
most  
winxp  
updates  
offline  
except:  
-  
com\_microsoft.886906\_NET10\_SP3\_nld\_5556  
-  
com\_microsoft.888316\_ehome\_guide\_fix  
-  
com\_microsoft.KB867461\_DOT\_NET\_EN\_1\_0\_SP3  
-  
com\_microsoft.KB867461\_DOT\_NET\_Tier3  
-  
com\_microsoft.KB873369\_XP\_SP3\_eHome\_INTL  
-  
com\_microsoft.Q816093\_VM3810\_Ver1  
-  
com\_microsoft.Q900036\_VS\_NET\_ES\_5520

oh  
i  
wish  
i  
could  
get  
my  
hands  
on  
one  
of  
those  
hackers,  
he/she  
would  
suffer  
a  
very  
slow  
death,  
minimum  
a  
month  
after  
messing  
with  
this  
problem  
for  
about

Re: Downloading updates in advance

a  
month  
i'm  
almost  
ready  
for  
a  
mental  
institution

omi

any  
hackers  
that  
wish  
to  
vulontier  
or  
test  
me,  
let's  
set  
up  
a  
meeting  
!!

"Juan"  
wrote:

1)  
You  
may  
need  
to  
go  
to  
the  
Windows  
Update  
Site  
first  
and  
install  
the  
most  
recent  
version  
of

Re: Downloading updates in advance

Windows  
Update  
Software\*  
(accept  
the  
download  
before  
a  
regular  
update  
search)  
and  
after  
that  
you  
can  
install  
updates  
by  
any  
means.

\*Check  
in  
C:\WINDOWS\Downloaded  
Program  
Files  
and  
check  
update  
software;  
Validation  
tool  
and  
Update  
Class,  
activex  
controls  
are  
necessary  
to  
update  
your  
system.

2)  
svchost  
is  
a  
normal  
system

Re: Downloading updates in advance

process

3)  
and  
Generetic  
Host  
Process  
may  
be  
a  
problem  
with  
a  
scanner  
or  
printer  
driver.  
updated  
drivers  
will  
solve  
it.

4)  
How  
to  
disable  
or  
remove  
Messenger  
(msmsgs.exe)  
[http://www.kellys-korner-xp.com/xp\\_messenger.htm](http://www.kellys-korner-xp.com/xp_messenger.htm)  
[http://www.dougknox.com/xp/utills/xp\\_mess\\_disable](http://www.dougknox.com/xp/utills/xp_mess_disable)  
<http://www.updatexp.com/disable-messenger-msn.h>

---

"omi"  
<omi@xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx>  
escribió  
en  
el  
mensaje  
<news:F76B64A1-1643-4EAF-9FE5-D36D77A1DE>

Well  
that  
didn't  
work,

i  
downloaded

Re: Downloading updates in advance

all  
90  
files  
(582Mb)  
i  
formatted  
my  
drive  
and  
reinstalled  
windows  
when  
i  
tried  
to  
perform  
the  
updates  
one  
by  
one  
there  
were  
some  
that  
would  
not  
install  
because  
the  
installation  
program

was

missing  
like  
:  
com\_microsoft.886903\_NET11\_SP1\_XP\_55  
result:  
i  
had  
to  
go  
online  
to  
search  
for  
updates  
i  
needed

Re: Downloading updates in advance

an  
installer  
program  
first,  
then  
28  
downloads  
were  
needed  
Now  
it's  
up  
to  
date  
but  
again  
i'm  
leaking  
Mb's  
:((  
In  
my  
taskmanager  
i  
see  
there  
are  
5  
"svchost.exe"  
that  
are  
active  
is  
this  
normal  
?  
svchost.exe  
-  
local  
service  
svchost.exe  
-  
networkservice  
svchost.exe  
-  
SYSTEM  
svchost.exe  
-  
networkservice  
svchost.exe  
-

Re: Downloading updates in advance

SYSTEM

mmsgs.exe

keeps

activating

itself

My

cpu

keeps

"performing"

without

me

doing

anything

(variable

0–10%)

and

NIS

gives

popups

"Rules

automaticly

created

for

MS

genetic

Host

Process

for

WIN32

server"

-->

c:\Windows\System32\svchost.exe

So

i'm

back

to

where

i

was

Looks

like

performing

updates

offline

is

not

that

easy



Re: Downloading updates in advance

Hello,

i'm  
looking  
for  
a  
way  
to  
dl'd  
winxp-home  
updates  
in  
advance

i  
want  
to  
burn  
them  
all  
on  
cd  
so  
i  
can  
install  
&  
update  
winxp  
completely  
updated  
OFFline

Can  
someone  
give  
me  
the  
URL  
to  
do  
that  
?

A  
friend  
gave  
me  
this  
link  
but  
i  
don't  
know

Re: Downloading updates in advance

19

Re: Downloading updates in advance

if  
it's  
reliable  
<http://www.s>  
I  
think  
i  
prefer  
an  
original  
MSwinxp  
website

thnx  
in  
advance  
omi

Go  
to  
the  
following  
web  
site:

Welcome  
to  
Windows  
Update  
Catalog  
<http://v4.windowssup>

Click  
on  
"Find  
updates  
for  
Microsoft  
Windows  
operating  
systems".  
In  
the  
Operating  
system  
box,  
scroll  
down  
to  
the

Re: Downloading updates in advance

next  
to  
last  
entry,  
Windows  
XP  
SP2.  
Click  
on  
it  
to  
highlight  
it  
and  
hit  
the  
Search  
button.  
Click  
on  
"Critical  
Updates  
and  
Service  
Packs".  
Scroll  
through  
the  
list  
and  
add  
all  
the  
updates  
you  
need  
to  
your  
download  
basket.  
Do  
the  
same  
for  
"Recommended  
Updates".  
Once  
you've  
completed  
the  
selection

Re: Downloading updates in advance

process  
click  
on  
"Go  
to  
Download  
Basket".  
Use  
the  
Browse  
button  
to  
select  
a  
handy  
location  
on  
your  
hard  
drive  
to  
store  
the  
updates.  
Hit  
the  
Download  
button.

Here's  
another  
Microsoft  
source  
for  
updates:

Microsoft  
Security  
Bulletin  
Search  
<http://www.microsoft.com>

Here  
are  
a  
couple  
of  
sites  
you  
may  
find

Re: Downloading updates in advance

useful:

How  
to  
download  
updates  
and  
drivers  
from  
the  
Windows  
Update  
Catalog  
<http://support.microsoft.com>

How  
to  
install  
multiple  
Windows  
updates  
or  
hotfixes  
with