

Re: Downloading updates in advance

Source:

http://www.derkeiler.com/Newsgroups/microsoft.public.windowsxp.security_admin/2006-02/msg00098.html

- *From:* omi <omi@xxxxxxxxxxxxxxxxxxxxxxxxxxxx>
 - *Date:* Thu, 2 Feb 2006 15:18:42 -0800
-

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 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>

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... 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:

Re: Downloading updates in advance

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 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 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 are restricting 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/Default.msp>

Re: Downloading updates in advance

---- Protect Your PC tips
<http://scan.syngatetech.com/> ---- Check your firewall
configuration here
for
inbound threats

"omi" <omi@xxxxxxxxxxxxxxxxxxxxxxxxxxxx> wrote in
message
news:263BB0C6-F1C3-4360-B90E-AB77652317A2@xxxxxxxxxxxxxxxxxxxx

1) that's where the problem is, when i go
online for updating i get
hacked,
changed 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 NIS popup request for
Ikernel.exe to connect to a
DNS-server
(blocked it)
i wonder 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 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

Re: Downloading updates in advance

those hackers,
he/she would suffer a very slow death,
minimum a month
after messing with this problem for about a
month i'm almost ready for
a
mental institution

omi

any hackers that wish to volunteer 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 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 process

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

Re: Downloading updates in advance

4) How to disable or remove

Messenger (msmsgs.exe)

http://www.kellys-korner-xp.com/xp_messenger.htm

http://www.dougknox.com/xp/utills/xp_mess_disable.htm

<http://www.updatexp.com/disable-messenger-msn.html>

"omi"

<omi@xxxxxxxxxxxxxxxxxxxxxxxxxxxx>

escribió en el mensaje

news:F76B64A1-1643-4EAF-9FE5-D36D77A1DB56@xxxxxxxxxxxxxxxxxxxx

Well that
didn't work,

i
downloaded
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_5556
result: i had
to go online
to search for
updates
i needed an
installer
program
first,
then 28
downloads

Re: Downloading updates in advance

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
– 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
generetic
Host

Re: Downloading updates in advance

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 as i
thought

Any help's
appreciated
omi

"Nepatsfan"
wrote:

You're
welcome.

Nepatsfan

3F675DAE-549C-497E-98E6-D41D736988AA@xxxxxxxxx
omi
<omi@xxxxxxxxxxxxxxxxxxxxxxxxxxxx>
wrote:

thnx
a
million

hopefully
this
will
end
my
virus-nightmare
that
lasted
a
month

Re: Downloading updates in advance

thnx
again
omi

"Nepatsfan"
wrote:

3D5B70BB-0FAC-4851-BCE6-7BFD5F28
omi
<omi@xxxxxxxxxxxxxxxxxxxxxxxxxxxx>
wrote:

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

Re: Downloading updates in advance

to
do
that
?
A
friend
gave
me
this
link
but
i
don't
know
if
it's
reliable
<http://www.softwarepatch.com/windows>
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.windowsupdate.microsoft.com/catalog>

Click
on
"Find
updates

Re: Downloading updates in advance

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

Re: Downloading updates in advance

your
download
basket.
Do
the
same
for
"Recommended
Updates".
Once
you've
completed
the
selection
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

Re: Downloading updates in advance

Security
Bulletin
Search

<http://www.microsoft.com/technet/security/c>

Here
are
a
couple
of
sites
you
may
find
useful:

How
to
download
updates
and
drivers
from
the
Windows
Update
Catalog

<http://support.microsoft.com/default.aspx?sci>

How
to
install
multiple
Windows
updates
or
hotfixes
with
only
one
reboot

<http://support.microsoft.com/kb/296861/>

Good
luck

Nepatsfan

Re: Downloading updates in advance