

Re: IE 6 uses 100% resources

Source:

<http://www.tech-archive.net/Archive/Windows/microsoft.public.windows.inetexplorer.ie6.browser/2006-02/msg0019>

- *From:* "Jan II" <abuseSPAM@xxxxxxxxxxxxxxxxxxxxx>
 - *Date:* Thu, 2 Feb 2006 21:52:45 -0500
-

Jan – not 'may likely be infected' – he IS still infected, unless he has carried out the removals suggested, and confirmed the success of that procedure.

It's the confirmation that is the point of a two-way dialogue – and which provides some security for the future.

In that last log that was posted in the forum I can see a number of active infection vectors – and unless action is taken the OP WILL have worse problems in the near future!! (as I see Nirvana has already commented!)

Well...I was giving the OP the benefit of the doubt that perhaps they had already performed the last step suggested by Nirvana, as they had stated in an earlier reply to you in this thread that they were 'going to do what had been suggested'. However, there was no confirmation that they had, only the post of their HJT log here. I asked that they post the HJT log to the Forum in order to confirm that the log was clean or not, but, they did not. I subsequently posted it there on behalf of the OP for the benefit of those who were helping there to see whether or not the OP had followed through with the suggested task as he had indicated. Thus, I used the term 'may', not having any confirmation that they were in fact still infected.

We can only hope the OP will return to either venue to communicate if they did or did not follow through.

Jan :)
MS MVP – IE [DTS/AumHa]

--
Noel Paton (MS-MVP 2002-2006, Windows)

Nil Carborundum Illegitemi
<http://www.crashfixpc.com/millsrpch.htm>

Re: IE 6 uses 100% resources

<http://tinyurl.com/6oztj>

Please read <http://dts-1.org/goodpost.htm> on how to post messages to NG's "Jan II" <abuseSPAM@xxxxxxxxxxxxxxxxxxxx> wrote in message <news:eAzcsMAKGHA.668@xxxxxxxxxxxxxxxxxxxxxxxxxxxx>

Hi 92griffin :-)

I think I'm OK. Have been web browsing with IE6 for a few days and no problem. I'm hoping it's all fixed. If not, at least I have this thread (and I've saved it to my HD) to look back on.

Thanks a million for all your help. I'll be sure to tell my friends and clients about the helpfulness of the community.

You're very welcome. However, as Noel stated, you really need to complete all the steps as outlined for you in the Forum to be sure your system is fully clean, or you may likely still be infected.

Additionally, if you are still infected, it very well may attract other scumware to your system, and you will soon have equally as bad, if not worse problems than you have just been through.

As you have not done as I requested earlier in this thread, I have posted your the HJT log from this thread to the forum thread for further evaluation by the experts who have been helping you there. Please return to the forum to finish up the good job you have been doing thus far and get and an all clear from them. <g>

Jan :)
MS MVP – IE [DTS/AumHa]
Smiles are meant to be shared,
that's why they're so contagious.

Replies are posted only to the newsgroup for the benefit of other readers.

How to make a good newsgroup post:
<http://www.dts-1.org/goodpost.htm>

"Jan II" wrote:

Re: IE 6 uses 100% resources

Hi 92griffin :-)

Now...remember about keeping replies in one thread, so you should post this log back to the thread on the forum where you have been working so that the experts who have been helping you there can see this information and let you know for sure if you are in the clear. :-)

I'll follow up there as well.

Jan :)
MS MVP – IE [DTS/AumHa]
Smiles are meant to be shared,
that's why they're so contagious.

```
Here's my most recent log...
[01/30/2006, 20:03:00] –
VirtumundoBeGone v1.5 (
"C:\Documents and
Settings\xppro.XP_PRO\Desktop\VirtumundoBeGone.exe"
)
[01/30/2006, 20:03:03] –
Detected System
Information:
[01/30/2006, 20:03:03] –
Windows Version: 5.1.2600,
Service Pack 2
[01/30/2006, 20:03:03] –
Current Username: mc
(Admin)
[01/30/2006, 20:03:03] –
Windows is in NORMAL
mode.
[01/30/2006, 20:03:03] –
Searching for Browser
Helper Objects:
[01/30/2006, 20:03:04] –
BHO 1:
{02478D38–C3F9–4EFB–9B51–7695ECA05670}
(Yahoo! Toolbar Helper)
[01/30/2006, 20:03:04] –
BHO 2:
```

Re: IE 6 uses 100% resources

{06849E9F-C8D7-4D59-B87D-784B7D6BE0B3}
(AcroIEHlprObj Class)
[01/30/2006, 20:03:04] -
BHO 3:
{53707962-6F74-2D53-2644-206D7942484F}
(
[01/30/2006, 20:03:04] -
WARNING: BHO has no
default name. Checking
for
Winlogon reference.
[01/30/2006, 20:03:04] -
Checking for
HKLM\...\Winlogon\Notify\SDHelper
[01/30/2006, 20:03:04] -
Key not found:
HKLM\...\Winlogon\Notify\SDHelper,
continuing.
[01/30/2006, 20:03:04] -
BHO 4:
{5C8B2A36-3DB1-42A4-A3CB-D426709BBFEB}
(PCTools Site Guard)
[01/30/2006, 20:03:04] -
BHO 5:
{83A5F7B7-DC75-44CE-9195-264F41709FA9}
(ATLDistrib Object)
[01/30/2006, 20:03:04] -
ALERT: Found ATLDistrib
Object!
[01/30/2006, 20:03:04] -
BHO 6:
{AE7CD045-E861-484f-8273-0445EE161910}
(AcroIEToolbarHelper
Class)
[01/30/2006, 20:03:04] -
BHO 7:
{B56A7D7D-6927-48C8-A975-17DF180C71AC}
(PCTools Browser Monitor)
[01/30/2006, 20:03:04] -
Finished Searching Browser
Helper Objects
[01/30/2006, 20:03:04] -
*** Detected ATLDistrib
Object
[01/30/2006, 20:03:04] -
Trying to remove
ATLDistrib Object...
[01/30/2006, 20:03:05] -
Terminating Process:
IEXPLORE.EXE
[01/30/2006, 20:03:05] -

Re: IE 6 uses 100% resources

Re: IE 6 uses 100% resources

Terminating Process:
RUNDLL32.EXE
[01/30/2006, 20:03:05] –
Disabling Automatic Shell
Restart
[01/30/2006, 20:03:05] –
Terminating Process:
EXPLORER.EXE
[01/30/2006, 20:03:05] –
Suspending the NT Session
Manager System
Service
[01/30/2006, 20:03:06] –
Terminating Windows NT
Logon/Logoff
Manager
[01/30/2006, 20:03:07] –
Re-enabling Automatic
Shell Restart
[01/30/2006, 20:03:07] –
File to disable:
C:\WINDOWS\system32\jkkjh.dll
[01/30/2006, 20:03:07] –
Renaming
C:\WINDOWS\system32\jkkjh.dll
->
C:\WINDOWS\system32\jkkjh.dll.vir
[01/30/2006, 20:03:07] –
File successfully renamed!
[01/30/2006, 20:03:07] –
Removing
HKLM\...\Browser Helper
Objects\{83A5F7B7-DC75-44CE-9195-264F41709FA9}
[01/30/2006, 20:03:07] –
Removing
HKCR\CLSID\{83A5F7B7-DC75-44CE-9195-264F41709FA9}
[01/30/2006, 20:03:07] –
Adding Kill Bit for ActiveX
for GUID:
{83A5F7B7-DC75-44CE-9195-264F41709FA9}
[01/30/2006, 20:03:07] –
Deleting
ATLEvents/MSEvents
Registry
entries
[01/30/2006, 20:03:07] –
Removing
HKLM\...\Winlogon\Notify\jkkjh
[01/30/2006, 20:03:07] –
Searching for Browser
Helper Objects:

Re: IE 6 uses 100% resources

[01/30/2006, 20:03:07] –

BHO 1:

{02478D38–C3F9–4EFB–9B51–7695ECA05670}

(Yahoo! Toolbar Helper)

[01/30/2006, 20:03:07] –

BHO 2:

{06849E9F–C8D7–4D59–B87D–784B7D6BE0B3}

(AcroIEHlprObj Class)

[01/30/2006, 20:03:07] –

BHO 3:

{53707962–6F74–2D53–2644–206D7942484F}

()

[01/30/2006, 20:03:07] –

WARNING: BHO has no

default name. Checking

for

Winlogon reference.

[01/30/2006, 20:03:07] –

Checking for

HKLM\...\Winlogon\Notify\SDHelper

[01/30/2006, 20:03:07] –

Key not found:

HKLM\...\Winlogon\Notify\SDHelper,

continuing.

[01/30/2006, 20:03:07] –

BHO 4:

{5C8B2A36–3DB1–42A4–A3CB–D426709BBFEB}

(PCTools Site Guard)

[01/30/2006, 20:03:07] –

BHO 5:

{AE7CD045–E861–484f–8273–0445EE161910}

(AcroIEToolbarHelper

Class)

[01/30/2006, 20:03:07] –

BHO 6:

{B56A7D7D–6927–48C8–A975–17DF180C71AC}

(PCTools Browser Monitor)

[01/30/2006, 20:03:07] –

Finished Searching Browser

Helper Objects

[01/30/2006, 20:03:07] –

Finishing up...

[01/30/2006, 20:03:07] – A

restart is needed.

[01/30/2006, 20:03:13] –

Attempting to Restart via

STOP error (Blue

Screen!)

Hope I'm out of the woods.

Thanks to your help and

Re: IE 6 uses 100% resources

suggestions.

"Jan II" wrote:

Hi :-)

Have you fully removed the winfixer malware? If not....your problems are not fully resolved, and can return at any time.

If you have already run the HiJackThis program and posted your log on one of the forums, then please post a link to the forum where you posted it so that I can take a look at what was found. Inquiring minds and all....
<g>

If you have not done so yet, follow these instructions.

Re: IE 6 uses 100% resources

This step
is one
of
the most
important.
Follow all
instructions
carefully.
This
program
should
be run in
Normal
mode.

How to
download
and install
HiJackThis:
Win 98-XP
http://www.download.com/HijackThis/3000-8022_4-10227353.html

Please.. DO
NOT post
your log
HiJackThis
log to this
newsgroup.

It
is
important
that you go
to one of
the
HiJackThis
Support
Forums
below
and
allow the
experts
there to
analyze it
for you.:
AumHa
HiJackThis
Forum
<http://forum.aumha.org/viewforum.php?f=30>
to allow the
experts
there to

Re: IE 6 uses 100% resources

evaluate
your log
and advise
you of
any
necessary
steps to
clean your
system.
(Note: You
will have to
Register
before
posting on
these
Forums.
Please
follow all
posting
instructions
carefully to
avoid
having your
log
deleted
or ignored.

Please post
back a link
to the forum
where you
post your
HJT log and
I
will
monitor the
progress
there.

Hope this
helps.

Jan :)
MS MVP –
IE
[DTS/AumHa]
Smiles are
meant to be
shared,
that's why
they're so

Re: IE 6 uses 100% resources

contagious.

Replies are
posted only
to the
newsgroup
for the
benefit or
other
readers.

How to
make a
good
newsgroup
post:

<http://www.dts-l.org/goodpost.htm>

"92griffin"

<92griffin@xxxxxxxxxxxxxxxxxxxxxxxxxxxx>

wrote in

message

<news:EA017F02-54F5-4C52-B9E8-D16E1DD61507@xxxxxxxxxx>

Thanks
for
your
understanding
and
hanging
in
there
with
me
on
this
thread.

I
seem
to
have
some
success.

Won't
stand
on
it
until
I
have
a

Re: IE 6 uses 100% resources

couple
problem-free
days
with
IE.
Seems
what
I
did
was,
to
go
to
<http://www.bleepingcomputer.com/forums/topic18610.html>,
and
used
VundoFix.exe
to
identify
the
problem.
This
application
doesn't
help
or
solve
the
situation,
but
I
noticed
that
there
were
files
(jkkjh.dll
and
hkkj.*)
in
C:\windows\system32
which
I
carefully
deleted
within
File
Explorer
after
closing
IE.

Re: IE 6 uses 100% resources

Re: IE 6 uses 100% resources

Then
I
restarted
IE
and
browsing
seem
to
be
as
fast
as
before.

Except,
till
now,
every
time
I'd
open
a
new
IE
window,
all
others
will
close,
leaving
only
the
new
one
open.
Right
now,
I
have
four
windows
open,
all
in
this
discussion
group.
I
hope
this
is

Re: IE 6 uses 100% resources

a
fix.

Try
it,
everyone
who
has
the
same
problem!
Mahalo
to
Sandi
and
Zee
on
their
help!

"Jan
II"
wrote:

Hi
92griffin
:-)

And
yes,
I
did
try
the
solutions
offered
on
Sandi's
website,
along
with
detailed
instructions
for
the
same
from

Re: IE 6 uses 100% resources

TrendMicro
PC-cillin.
I've
been
working
on
this
problem
for
a
few
days
now.

Ok...just
let
us
know
which
one
of
the
many
posts
you
will
be
staying
with,
so
that
we
can
go
there
to
give
you
further
assistance.
I
realize
that
these
types
of
problem
can
be
very

Re: IE 6 uses 100% resources

consuming,
especially,
when
they
go
on
for
some
time,
thus,
your
feeling
of
frustration
is
understandable.

I
have
had
a
good
many
of
my
own
that
have
taken
days
to
get
sorted
out.

Now...
your
participation
is
key
to
our
being
able
to
give
you
the
right
information
to
help

Re: IE 6 uses 100% resources

resolve
this
problem
as
soon
as
possible.
Your
feedback
is
our
only
eyes
as
to
what
you
are
seeing
and
what
is
happening
on
your
end.
The
more
information
and
details
of
what
is
happening
will
be
a
lot
of
help
to
us
in
determining
what
we
might
need
to
help

Re: IE 6 uses 100% resources

you
with
from
there.
If
something
didn't
work
then
tell
us
why
it
didn't
work,
not
that
it
'didn't
work',
which
leaves
us
with
nothing
to
work
with.
'k?

Stick
with
us.....we'll
get
you
there.
:-)

Jan
:)
MS
MVP
-
IE
[DTS/AumHa]
Smiles
are
meant
to
be
shared,

Re: IE 6 uses 100% resources

link
to
spyware
info.
I
already
use

TrendMicro's
PC-cillin
Internet
Security
Suite,
and
Spybot
1.4,
plus
a
couple
of
recommendations
from
Sandi
Hardmeier's
website.

I
need
real
concrete
solutions.

You
are
getting
'real
concrete
solutions',
but,
you
are
starting
new
posts
all
over
the
place.
You
need

Re: IE 6 uses 100% resources

Re: IE 6 uses 100% resources

to
stay
in
one
thread
so
that
you
can
tell
what
help
you
are
getting,
and
so
can
other
responders
so
everyone
knows
what
is
going
on.
If
you
want
help,
then
stay
with
a
thread
and
work
the
help
you
are
getting.

The
Winfixer
malware
you
have
is
vicious,

Re: IE 6 uses 100% resources

Re: IE 6 uses 100% resources

and
very
hard
to
get
rid
of.
If
you
bother
to
read
the
responses
all
your
various
posts
you
would
know
that.
There
is
no
one-step
"Voila!"
type
solution
to
what
you
have,
and
you
are
going
to
have
to
do
your
share
of
the
work
to
get
rid
of
it.

Re: IE 6 uses 100% resources

Re: IE 6 uses 100% resources

Did
you
even
try
any
of
the
suggestions
on
Sandi's
site,
or
any
of
the
other
suggestions
that
people
have
given
you
in
your
other
posts?

We
are
not
going
to
chase
you
all
over
the
group
to
give
you
answers
to
try
and
help,
only
to
find
someone
else

Re: IE 6 uses 100% resources

has
already
done
so
or
you
are
not
going
to
even
try
them.
Now
go
back
and
take
a
look,
then
chose
one
and
stay
in
that
thread
if
you
want
further
help,
be
willing
to
do
your
part
to
help
resolve
your
problem,
and
stop
insulting
the
people
who
are

Re: IE 6 uses 100% resources

Re: IE 6 uses 100% resources

trying
to
help
you.

Jan
:)
MS
MVP
–
IE
[DTS/AumHa]
Smiles
are
meant
to
be
shared,
that's
why
they're
so
contagious.

Replies
are
posted
only
to
the
newsgroup
for
the
benefit
or
other
readers.
How
to
make
a
good
newsgroup
post:
<http://www.dts-l.org/goodpost.htm>

"Donny
Broome"

Re: IE 6 uses 100% resources

wrote:

Your
PC
is
infected
with
spyware.
The
page
below
lists
several
fine
products
that
can
help
you
remove
these
pests.
<http://www.broomen>