

Re: Danger warning! to the public and note to Databaseben

Source:

http://www.tech-archive.net/Archive/WinXP/microsoft.public.windowsxp.help_and_support/2006-10/msg03546.htm

- *From:* MtnLadyinBlackHills1986 <MtnLadyinBlackHills1986@xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx>
 - *Date:* Mon, 23 Oct 2006 21:55:02 -0700
-

Oops! Sorry for the duplicate post. I must be getting tired. Glen, first you didn't get any of the information – now you get two sets....

Sue

"MtnLadyinBlackHills1986" wrote:

Hi again, Glen. Here are the "Add-ons that have been used by Internet Explorer" that you requested and were lost last night when Microsoft picked the worst possible moment to make me log in:

- AUDIO__MID Moniker Class – Microsoft
- AUDIO__WAV Moniker Class – Microsoft
- DHTML Edit Control Safe for Scripting for IE5 – Microsoft
- HHCtrl Object – Microsoft
- HTML Document – Microsoft
- iTunesDetector Class – (Not Verified)
- LSControl Class – Symantec
- LSSupCtl Class – Symantec
- Microsoft Scriptlet Component – Microsoft
- MsnMessengerSetupDownloadControl Class – Microsoft MSN
- MUWebControl Class – Microsoft
- Office Update Installation Engine – (Not Verified) Microsoft
- QuickTime Object – (Not Verified) Apple
- RealPlayer G2 Control – (Not Verified) – RealNetwork
- SearchAssistantOC – Microsoft
- Shell Name Space – Microsoft
- Shockwave Flash Object – Macromedia
- Symantec Script Runner Class – Symantec
- Symantec SmartIssue – Symantec
- SymLTQueries Class – Symantec
- SymSubQueries Class – Symantec
- Tabular Data Control – Microsoft
- Update Class – Microsoft Windows XP Pub.
- Web Browser Applet Control – (Not Verified) Microsoft
- Windows Genuine Advantage Validation Tool – Microsoft

Re: Danger warning! to the public and note to Databaseben

Windows Media Player – Microsoft
Windows Media Player – Microsoft (NOTE: Listed twice – not a typo)
WUWebControl Class – Microsoft
XML Document – Microsoft
YInstStarter Class – Yahoo!
Advanced Searchbar – Advanced Search
Windows Messenger – (No Publisher Given)
Yahoo Messenger – Yahoo!
Adobe PDF Reader Link Helper – Adobe
Advanced Searchbar – Advanced Search (NOTE: Listed twice – not a typo)
CNavExtBho Class – Symantec
eBay Toolbar Helper – eBay
MSN Search Toolbar Helper – Microsoft MSN
PrxcnBHO Class – (Not Verified) Proxyconn
Yahoo! Toolbar Helper – Yahoo!
Advanced Searchbar – Advanced Search (NOTE: Listed 3rd time – not a typo)
eBay Toolbar – eBay
MSN Search Toolbar – Microsoft MSN
Norton AntiVirus – Symantec
Yahoo! Toolbar – Yahoo!

Whew! There they are! All this is certainly improving my typing and proofreading skills! Ha! Good luck in going through them. Maybe you'll find something interesting!

Thanks and good night!

Sue

"MtnLadyinBlackHills1986" wrote:

AAARRRRRHHHHHH! Glen, I wrote you a long answer to your last post, including a very long list of Add-ons used by Internet Explorer and pressed "Post". Pardon my language, but damn Microsoft made me log in again and when I came back, my whole message was gone!!! I've got things to do and I'm just not up to typing that all again. I'll try to give it a shot again tomorrow.

Sue

"glee" wrote:

Replies inline, interspersed below.....

"MtnLadyinBlackHills1986"
<MtnLadyinBlackHills1986@xxxxxxxxxxxxxxxxxxxxxxxxxxxx>
wrote
in message

Re: Danger warning! to the public and note to Databaseben

news:79D6C024-E8C1-469B-8FC7-6D65C1B0206C@xxxxxxxxxxxxxxxxxxxx

Glee, you were correct about the Norton and McAfee virus scans. My local ISP does an email scan using McAfee before it reaches my mailbox. The Norton is on my own system. You say that Norton says its own email scanning is redundant, unnecessary and can cause problems? You'd think they'd remove it from their software line.....

You'd think! By their own admission, it is redundant. As long as you have your resident virus scanner running in the background, the email scanner affords no useful additional protection. yet, most A-V apps include it. Why? Because users *think* it makes them safer, and you give them what helps in their feeling of security. If one supplier adds email scanning, they all must, lest they look like they are not trying to protect you as well as the competition.

I did run another Ad-Aware SE full scan last night, and it did not find any more traces of a Trojan Horse.

That is good, and much as I suspected. From your original description, it was never a trojan horse in the first place, but a trojan downloader, which can download its friends, the trojan horses and other mal-ware. You may have only had it in your browser temporary cache. I can't tell because it is now in quarantine and you cannot give me the exact description from when it was detected. You say it was found in or connected to the Ntregopt file. With this trojan downloader in quarantine, can you still find the original Ntregopt.exe file on your computer in the folder it has been living in all these months?

Re: Danger warning! to the public and note to Databaseben

I will check out the AVG software you gave me the links for. Did you see the post by "Joe"? He mentioned a software called "Free Home" with the option to do a boot scan? Do you know anything about this?

The AVG Anti-Spyware app will find most trojans and spyware, and much that is missed by Ad-Aware and other apps. Do not confuse it with it's sister app, AVG Anti-Virus, which is an A-V program that you don't need, since you already have Norton.

Joe mentioned Avast Free Home A-V....it is another anti-virus program, and you don't need it. Your current A-V can be configured to do a boot scan when you start the computer, if it isn't doing it already. It won't help find a trojan, most likely, as they aren't loading prior to Windows.

I'm sorry to sound so confused, but I am a computer novice. I have several people who are kind enough to want to try to help me, but I'm starting to get "information overload".

Quite understandable, and overload is very easy to hit, even for experienced professionals. I would not have even entered the thread except the info I saw you getting seemed to be too far off the mark. There appears thus far to be no need or reason to wipe anything out, restore anything, or go back months, for this little thing.

But I guess the main point to this post is: in answer to your question, when I did a full rescan on Ad-Aware SE last night, there was NO indication of Trojan Horse traces again. The Trojan trace info in my original post is still quarantined in my Ad-Aware.

Re: Danger warning! to the public and note to Databaseben

Re: Danger warning! to the public and note to Databaseben

OK. Either install and run Ewido/AVG Anti-Spyware as described in my earlier link, or just run their online scanner, which I also linked. Have it quarantine or delete what it finds (quarantine is usually "safer" in terms of avoiding mistakes).

In you reply to DatabaseBen, you mentioned seeing a toolbar/BHO from Proxyconn, Inc which you disabled. That is a legitimate BHO which is the Proxyconn Web Accelerator, used by some ISPs to speed up their dial-up access:
<http://www.proxyconn.com/>

You might check with your ISP as they may have included it. Regardless, you can for now disable it....at worst having it disabled will only slow down your web pages loading.

Go back to where you disabled the BHOs and toolbars, in Internet Explorer> Tools menu> Manage Add-Ons. In the drop-down list, select "Add-ons that have been used by Internet Explorer" rather than just "Add-ons that are currently loaded". If it's not too much work, post back with a list of what is shown there. I don't need all the info listed, just the Names and the first word of the Publishers list.

I can give you some links to reading on how to adjust your settings in IE to help prevent some of these issues, but for now I think you have more than enough to chew on, so I can hold those till later. Or I can simply bow out of the thread if you would rather work with someone else. :-) I'm easy.

—
Glen Ventura, MS MVP Shell/User, A+
<http://dts-1.org/>
<http://dts-1.org/goodpost.htm>

"glee" wrote:

Re: Danger warning! to the public and note to Databaseben

I haven't found Webroot Spysweeper's background monitoring to be very useful, nor the background monitoring of any other anti-spyware utilities. I do prefer AVG Anti-Spyware (formerly Ewido) for on-demand scanning for spyware and trojan downloaders:
<http://www.ewido.net/en/>

They've also got an online scan:
<http://www.ewido.net/en/onlinescan/>

I am not a fan of either Norton or McAfee anti-virus, though either should be effective against viruses, but somewhat less so against trojans and trojan downloaders. I can't imagine having both installed at the same time (in fact, I don't think they will co-habit), so I am guessing the McAfee scan you refer to is just an online email scan that your ISP uses prior to your receiving the email.

Turn off the email scanning in your resident anti-virus (Norton, I presume).....even Symantec support states it is redundant and unnecessary, and can cause problems.

You mentioned that the trojan downloader was quarantined (by Ad-Aware, IIRC), so do you still detect any trojans

Re: Danger warning! to the public and note to Databaseben

or downloader when you
rescan? If so, where are
they
being found...what location
on your hard drive? If they
are being found in
System
Restore or in the Ad-Aware
quarantine folder, then you
only have to clear the
quarantine area through the
Ad-Aware interface, and or
reset System Restore to
delete old restore points.

--
Glen Ventura, MS MVP
Shell/User, A+
<http://dts-1.org/>
<http://dts-1.org/goodpost.htm>

"MtnLadyinBlackHills1986"

<MtnLadyinBlackHills1986@xxxxxxxxxxxxxxxxxxxxxxxxxxxx>

wrote

in message

<news:B24E2E08-5C4A-43E7-A154-2031978DBB1E@xxxxxxxxxxxxxxxxxxxx>

Glee, I
found from
talking to
another
person later
that the
NTREGOPT
program
was not the
cause of the
Trojan
Horse,
although
possibly it
could have
used
it to "sneak"
the Trojan
Horse onto
my
computer.

So now it
appears I

Re: Danger warning! to the public and note to Databaseben

have a
Trojan
Horse on
my system!
I have used
security
software
from 3
major
companies
(LavaSoft,
Symantec/Norton,
and
Webroot),
have
installed all
the security
downloads
from
Microsoft,
have my
firewall
up, have not
added any
toolbars, do
not go to
the
so-called
"dark side"
of
the web,
have 2
email
scanners
(Symantec/Norton
and McAfee
from my
local
ISP), do not
use links for
"free
checkups"
of my
computer
and similar
dangerous
links, do not
use Instant
Messaging,
and I still
got a Trojan

Re: Danger warning! to the public and note to Databaseben

Re: Danger warning! to the public and note to Databaseben

Horse!

I am a
computer
novice and
have done
everything I
know how
to do to
keep my
computer
safe. I have
"crashed" in
the past,
and I'm
beginning
to feel that
I want to
abandon the
Internet. For
me, it has
changed
from a
source of
fun
and
information
to a
dangerous
maze with a
hazard
around
every
corner.

Can you
give me any
information
on how to
find and
remove this
Internet
Devil? I'd
really
appreciate
any help
you can
give me.

"glee"
wrote:

Re: Danger warning! to the public and note to Databaseben

This
program
has
been
used
for
years
on
countless
computers,
and
has
been
downloaded
alone
and
also
in
the
package
with
its
sister
app,
ERUNT.
The
fact
that
you
ran
it
successfully
for
months
and
only
got
a
warning
about
a
trojan
last
week,
indicates
that
you
simply
have

Re: Danger warning! to the public and note to Databaseben

a
trojan
on
your
system,
and
it
may
have
replaced
that
app,
using
its
name.
It
does
not
in
any
way
implicate
the
download
you
got
months
ago
from
majorgeeks.

In
your
paste
of
the
trojan
information,
I
don't
see
any
mention
of
NTREGOPT.
Are
you
saying
the
file
itself,

Re: Danger warning! to the public and note to Databaseben

Hello,
Databaseben!

I
talked
to
you
way
back
in
July
when
you
were
very
helpful
with
all
my
computer
problems.

In
your
last
post
to
me,
you
recommended
some
free
programs
that
could
help
"clean
up"
my
computer.

I've
put
a
copy
of
part
of
what
you
wrote
below:

["http://www.majorgeeks.com/NTREGOPT_d4824.ht](http://www.majorgeeks.com/NTREGOPT_d4824.ht)

Re: Danger warning! to the public and note to Databaseben

The
program
above
will
optimize
your
registry..."

I
installed
this
program,
and
used
it
without
problem
for
several
months.
But
I
had
an
alarming
finding
about
this
program
when
I
ran
Ad-Aware
SE
on
10/18/06.
Unless
I
have
read
it
wrong,
it
appears
that
a
hacker
got
hold
of

Re: Danger warning! to the public and note to Databaseben

it
and
corrupted
it
badly.
I
saved
the
quarantine
area
of
Ad-Aware.
I
will
copy
what
it
said
about
the
above
software
program,
which
showed
the
program's
name
and
logo
in
the
findings
before
I
quarantined
it.
I
immediately
removed
it
from
my
computer:

ArchiveData(auto-quarantine-
2006-10-18
21-17-51.bckp)
Referencefile
:
SE1R128

Re: Danger warning! to the public and note to Databaseben

warn
others
NOT
to
install
this
software...
But
I
wanted
you
in
particular
to
know,
so
you
won't
recommend
it
to
anyone
else.

Quite
a
world
when
you
try
to
be
helpful
and
evil
people
only
want
to
hurt
others!
Kudos
to
Ad-Aware
SE
to
catching
this!
(I'm
sure
my

Re: Danger warning! to the public and note to Databaseben

Spy
Sweeper
would
have
caught
it
too
but
I
hadn't
done
my
scan
with
it
yet.)

Databaseben,
I
did
want
you
to
know
that
your
other
software
suggestions
have
been
very
helpful
and
I
thank
you!