

Re: Malicious Software Removal Tool

Source:

<http://www.tech-archive.net/Archive/Windows/microsoft.public.windowsupdate/2008-04/msg00091.html>

- *From:* Tim <Tim@xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx>
 - *Date:* Wed, 2 Apr 2008 12:01:01 -0700
-

PA Bear:

I have seen/read your posts in the last week of my largely self-induced PC turmoil . . . My experience would no doubt serve as a good case study on why one should not accept what is written on the web, even when it seems to be a common opinion.

I think the following is more than you wanted to see . . .

This whole thing started with me trying to fix the following problem:

It took ~15 seconds to access "My Computer" or "Save As" items. Though this has been the case for some time, it recently became a particular burden.

My attempts to fix this problem started with web searches. Unfortunately, I followed a path that took me to the point where my computer (T60) would not boot. I did not start logging my actions until a couple of days ago, and I don't have a clear recollection of my late-night/poor choices. I do remember it started with accepting suggestions about Services (the starting point was disabling DCOM) and copying files (replacing files that may have been corrupted). I have a second T60 configured in almost the same way as my primary T60. So, I used some files from that machine. That apparently was not wise. (Though the second T60 was very useful over the past week.)

Another set of actions surrounded my trying to do a chkdsk – the 'well-known' (no to me) issue of XP and SATA drives. My actions trying to get this done also helped lead me to the bottom of the pit.

Unfortunately, one of my actions was to shut off "system restore" . . . which limited my 'downstream' options.

(Note also that the interaction between MS system support software and the vendor supplied Thinkvantage software confused me.)

My primary T60 contains 'my life' wrt communications and documents for the last half a dozen years (rolled forward my files during yearly computer upgrades). I do have backups. I also made a copy (xcopyi) of my drive to a

Re: Malicious Software Removal Tool

usb HD.

After several days on this issue, I ended up learning (at least following along) how to create a BARTPE.

I took a 'snapshot' of the drive. I then installed XP and SP2. After I realized the amount of effort it would take to get back to where I was in terms of software and connectivity, I decided to take big action – I reformatted the HD and reloaded the snapshot.

I then did the slipstream repair install of XP SP2.

Again, I don't have a good log – I started logging at about the time of my snapshot restore – but the above is how I remember things.

(I don't think I left any window open for malicious software to get on the computer. I think one of the issues with the first SP2 install is that I forgot to disable the virus software.)

I am paranoid, and the computer was shutting down at random times, so I ran all of the scans I mentioned in my previous post. (In practice, I scan daily.)

I bookmarked the page you pointed me to, for future reference. Looks like good info. (I am one of those guys who used to have IT support . . .) I was using the other T60 for most interactions with the e-world.

Regards,
Tim

"PA Bear [MS MVP]" wrote:

What "issues" necessitated a Repair Install in the first place? Have you considered a format & reinstall?

After doing the Repair Install (or even a format & reinstall), did you take care of /everything/ on the following web-page before otherwise connecting the machine to the internet (to, e.g., browse; check email; chat; download)?
=> http://www.cert.org/tech_tips/before_you_plug_in.html

—
~PA Bear

Tim wrote:

Jerry, David:

Jerry is correct. After going through the repair install fiasco (mostly through my own issues), I wanted to make sure that nothing had crept into my system. I did a virus scan, a Spybot scan, a Adaware scan, a Defender

Re: Malicious Software Removal Tool

scan,
land a MRT (this is apparently the acronym used) quick scan.

Though those passed, with the usual many minor (cookie and MRU) issues
and

a
couple of firewall issues detected by Spybot, which I attribute to my
attempt to do a SP2 install after my first repair install of XP. So, I ran
full scans using a command line execution once; however, I also used a
'double-click execution' once.

Note that I omitted a perhaps important point the background information I
provided in my opening post: After the second, slipstream-based repair
install, the computer shut down a couple of times. It seemed to stabilize
after doing some work on "Thinkvatage" software – reinstalls.

But these random shutdowns made me concerned that malicious code had
been
introduced during the episode.

BTW: I received an email notification that my opening post had been
replied
to; however, the link provided did not open a page. Is there something I
need to do to get such links to work? No instructions were included in the
email.

This is the first time I have ever done a post in this (or any) community
. . .

Regards,
Tim

"Jerry" wrote:

If he's running it Full Scan he probably downloaded it and is
running it
from his machine directly.

"David H. Lipman" <DLipman~nospam~@Verizon.Net>
wrote in message
news:%238uFt6FIIHA.5396@xxxxxxxxxxxxxxxxxxxxxxxxxxxx

From: "Tim"
<Tim@xxxxxxxxxxxxxxxxxxxxxxxxxxxx>

Please let me know if there
is a more appropriate

Re: Malicious Software Removal Tool

discussion forum for
this question.

Is there a maximum number
of files that MSRT will
check?

I ask this because on two
occasions now, my display
has gone
'unretrievably black' (HD
still being accessed) after
about 2.5 hours of
MSRT execution (Full
Scan). I noticed on the
second scan that there
were
almost a million files
processed. After 'doing
something else for a
bit', I found the situation
described above (for the
second time).

Background:
I have just done a repair
install of XP SP2 on a T60.
Actually, this
was
after doing an XP repair
install, and messing up an
SP2 upgrade. I then
did the XP SP2 repair install
using a slipstream CD. Nice.
Next time,
I
will try to add drivers; e.g.,
for the XP SATA 'issue'.

Regards,
Tim

Tim:

Are you running the MRT from command
line or are you just obtaining it
through Auto Updates
?

--

Re: Malicious Software Removal Tool

Dave

<http://www.claymania.com/removal-trojan-adware.html>

Multi-AV -

<http://www.pctipp.ch/downloads/dl/35905.asp>