

Re: Recurring Spyware

Source:

http://www.derkeiler.com/Newsgroups/microsoft.public.windowsxp.security_admin/2006-05/msg00284.html

- *From:* "Dave B" <mail@xxxxxxx>
 - *Date:* Mon, 8 May 2006 14:48:29 -0400
-

What he said every good PC tech knows.

A PC is only as good as it's maintenance. I have a few customers that just will not listen to me and prefer rather to endure a regular bill from me. I clean their PC of spy/malware and trojans, install software, educate them how to use it, said PC is back a month later jam packed with more goodies. I look at the logs of mentioned software, last time it was updated or run was when I ran it when it was in my shop the last time.

Hell, I even get them to purchase Spysweeper, just cause it's mostly automatic and they don't have to pay much attention to it, and they turn it off because it was popping up alerts too often. Gee, wonder why it was doing that?

"Karl in Scottsdale" <KarlInScottsdale@xxxxxxxxxxxxxxxxxxxxxxxxxxxx> wrote in message news:D48FD79C-3853-4189-B732-C53EA914B634@xxxxxxxxxxxxxxxxxxxx

cquirke,

I can't say that I fully comprehend everything you said, but damn I wish you lived close by and I could afford to have you inspect my system...

Thank you,

"cquirke (MVP Windows shell/user)" wrote:

On Sun, 7 May 2006 13:35:21 -0500, "Shenan Stanley"

Karl in Scottsdale wrote:

Furthermore, you are suggesting that the Tech Support folks at MS, having spent much time helping me clean my system in detail using probably most of the steps outlined in Stanley Shenan's reply to my

Re: Recurring Spyware

post, are incompetent – and they left some Spy Ware somewhere on my system that magically 'woke-up' 3-days later to attempt to re-infect my system?

Not incompetent; just not competent enough, in this case. After all, without a maintenance OS that can boot without running ?infected code off the HD, there's a limit to how good things can expected to be.

Did they have you install at least five (5) of the antispysware applications from the list I posted?

I'd love to see that list :-)

I assure you, Panda, after the second Spy Ware event, there is no way in h*** that I knowingly or unknowingly installed Spy Ware on my computer. My Zone Alarm is now set to the highest protection possible, Ad-Aware and Ad-Watch are running full time, SpyBot S&D resident is NOW (since yesterday) running full time, and I have the most up to date version and definitions for Norton Anti Virus, as well as a fully current version of IE.

Sounds good. Any old versions of Sun Java JRE, Winamp, Acrobat Reader or Firefox lying around? Most of these will overwrite vulnerable old versions, but not Sun; they keep the old JREs in place for "backward compatibility" (i.e. so malware can still exploit them)

...while typing and possibly not looking directly at the screen) happen to press ENTER

If typing human language, every 5th character will be Space – and guess what Space does, when a pop-up dialog snatches the focus?

whatever it is has an open-door on your computer.

Re: Recurring Spyware

That can be so anyway, e.g. if F&PS is possible and you have hidden admin shares leaving the entire HD open to drop-ins.

Spybot Search and Destroy 1.4's immunization is passive

So is Spyware Blaster, which I'd recommend. Passive is good, in many ways; no overhead, doesn't crash into other resident defenses, etc.

I should NOT have to rely on the software
that is trying or
succeeding at installing itself to STOP the
Install – WINDOWS
should have its OWN app that will LOCK
the registry and LOCK
whatever loopholes these folks use

The problem is there by design – NT/2000/XP is designed to be a network client, so it waves all sorts of opportunities around. After all, the Internet's just a big network, right?

Well, that's like saying a tree is a chair because it's made out of wood. A network has a bounded and trusted set of entities on it, whereas the Internet is unbounded and wild, so "network client" rapidly devolves to "Internet chew-toy".

Plus, NT is something of a reversal of the whole "PC" thing...

First, we begged mainframe jocks to compute for us
Then the PC arrived and we could do our own thing
Then faster PCs tempted MS to tackle minis and *NIX
So PCs became the "client" end of client-server...
and Big Brother admin was leaved over user control.
So now we beg the sysadmin to allow us to use our PCs

Having deeply-pervasive automated control over things that have no end-user UI makes it really easy for anything that gets a toe in the door to escalate to full control and run away with the PC.

Yes – in a perfect world ...

....a stand-alone OS would put the keyboard into full control, not allow any "remote admin" whatsoever, and would display (and be bound by) risk information about everything you see and can do. Starting with data vs. code file types; no more meaningless "open", you'd trust

Re: Recurring Spyware

data to be capable of doing nothing and you would avoid running code.

Tip Of The Day:
To disable the 'Tip of the Day' feature...
