

Re: LONG, LONG time to startup 2

Source: <http://www.derkeiler.com/Newsgroups/microsoft.public.security.virus/2005-05/0450.html>

From: Chek (chek_16_at_hootmail.com)

Date: 05/29/05

Date: Sun, 29 May 2005 20:28:07 +0100

Crouchie,

I'll firstly say that while possibly well intentioned, your grasp of modern malware is at best incomplete.

Oh for the days (doesn't Blaster seem a mere innocent now?) when you could simply disable malware in the HKLM Run regkeys.

Things are far more sophisticated these days – imagine guiding a newbie to (say) CLSIDS in the registry then getting them to trash everything they don't recognise?

I have always found David Lipman's advice and recommendations helpful, and in no way self-promoting.

I don't know him apart from his presence on this newsgroup, but Dave is one of the people whose selfless dedication to his area of interest and willingness to share his knowledge, makes the internet worthwhile.

Have you any idea what the big Corporations and some professionals currently charge for personal advice –with no guarantee of a fix at the end of it?

Unless you call re-installing Windows a fix.

And I'm afraid I don't.

To me that's a failure. And Dave's Cleanbat script has worked faultlessly on every Win system I've run them. What's to complain about?

Admittedly a lot of Dave's posts are repetitive, but only because it's a valid procedure to follow for most posters here with their limited knowledge. Sure, more sophisticated tools like Process Explorer, HiJackThis and others may be

needed to actually remove the reported but undeletable files McAfee or Trend find even in Safe Mode (Winlogon being another current fave in the malware start-up routines), but there's always an invitation to report back the findings.

Also, I'd not be without AdAware as part of a malware removal kit.

No software is perfect, and I feel that separate software packages

will be more thorough than one team trying to handle everything, in terms of

inclusions and updates.

I hope that's not come over as discouragement, it's only my opinion.

I did hear Longhorn will warn when any system changes are about to be made – till a way is found round that too.

And so it goes on.

There's a lot to be learned here, by all of us.

Chek

"Crouchie1998" <crouchie1998@spamcop.net> wrote in message news:ejqsbQ9YFHA.2116@TK2MSFTNGP10.phx.gbl...

> *I disagree with downloading Ad Aware from Lavasoft as it is*

> *proven to*

> *produce false negatives. Steer clear of it because you*

> *have the best one*

> *installed already.*

>

> *All you need to do is either download MSCONFIG & disable*

> *some startup items*

> *or the best way, go into the registry editor & delete the*

> *entries manually.*

>

> *All you have to do is create a backup copy of the RUN*

> *registry key & then*

> *delete things like ADOBE, QUICKTIME, Messenger Software,*

> *RealTray, but leave*

> *firewall & antivirus software there.*

>

> *MSConfig can be downloaded here:*

>

> http://www.techadvice.com/specs/files_dl.asp?fnid=3398288

>

- > *All you will have to do is remove the check marks from the*
- > *RUN keys. You can*
- > *also delete the startup Programs from Spybot S & D by*
- > *clicking advanced*
- > *mode/Tools/Startup or that's what its is in version 1.4*
- > *anyway.*
- >
- > *The Registry Editor Way:*
- >
- > *Click START/RUN type 'regedit' & press ENTER*
- > *Click the '+' signs on:*
- > *HKEY_LOCAL_MACHINE*
- > *Software*
- > *Microsoft*
- > *Windows*
- > *CurrentVersion*
- > *& then click the folder (not the plus) of the RUN key. The*
- > *startup programs*
- > *are in the right-hand pane*
- >
- > *Of course Dave wants you to go to the IKS website because*
- > *he has it listed*
- > *as his footer like self promoting his own software.*
- >
- > *Post back if you get into problems*
- >
- > *Crouchie1998*
- > *BA (HONS) MCP MCSE*
- >
- >