

## Questions Regarding Workable SOHO Windows Installation / Configuration, Diagnostics, & Security Options ver. 3.00 ~ several Kb

*Source:* <http://www.derkeiler.com/Newsgroups/comp.security.misc/2002-04/0322.html>

---

*From:* wlhaught ([wlhaught2002tooth@ameritech.net](mailto:wlhaught2002tooth@ameritech.net))

*Date:* 04/19/02

From: "wlhaught" <[wlhaught2002tooth@ameritech.net](mailto:wlhaught2002tooth@ameritech.net)>

Date: Fri, 19 Apr 2002 00:39:24 GMT

Questions Regarding Workable SOHO Windows Installation / Configuration, Diagnostics, & Security Options ver. 3.00 ~ several Kb

WORKABLE I am wondering about workable options concerning installation, configuration, diagnostics, and security in a Windows environment that are practical for the typical home networking environment. An AS/400 or other real hardware and software isn't an option, and then I wonder if there is a Windows emulator that can handle the ActiveX controls (and how much would even be gained securitywise if that can be done).

I am wondering if there is a program or combination of programs that works in a way I have faith in at a reasonable cost. I'd prefer a solution that doesn't call for four programs and four time consuming 16-bit DOS scans for each of the following: 1) antivirus, 2) anti-trojan, 3) integrity checking, and 4) system change tracking. Or even an additional 5 to 8: additional antivirus and scanning software. Lets see F-Secure for Windows is \$125 per machine. For two machines that's \$250 already, plus if someone wants to use my machines for industrial espionage (and they are competent) they'll write ring 0 code that gets up earlier than than the antivirus program, right?

BARELY WORKS It seems to me that Windows just barely works (if you are lucky enough to get it up and running) before/even without worrying about security. From my experience is that the "98" in Windows 98 stands for the time period between system crashes. I use two computers. Both have 128 Mb RAM. The oldest one has a 500 MHz K-6, and two hard drives 6.4 & 17.2 Gb drives.

ENOUGH TROUBLE WITHOUT As far as memory resident, real time installation tracking and antivirus scanning goes, it seems to me that I am asking for more trouble than I've already got. Sure, my system may become quite secure, assuming for example that it gets so jacked up I cannot reach the net (or anything other than a blue screen, for

Questions Regarding Workable SOHO Windows Installation / Configuration, Diagnostics, & Security Options

example).

There are inherent limitations such as user, system, and GDI resources in Win9X/Me.

PACKED EXES Let's see if I understand this: You are supposed to run antivirus software to keep from getting a virus, yet according to most installation programs you are supposed to turn the antivirus software off when you need it most to prevent conflicts with self-installing executables that (as far as I know) cannot be checked for viruses \*packed in the archive.\*

VIRUS ALREADY LOADED Furthermore, virus scanning (at least solely) from Windows is especially an issue to me, since by the time the operating system loads (let alone the anti-virus software) a competently written virus would be in stealth mode anyway. Perhaps if the antivirus companies use VxDs, they can make it difficult, but this carries with it risks of conflicts. I guess so far we've been lucky the only people who would be both willing and able to write such viruses fall into one or more of three extremes: 1) too busy doing real work, 2) can't afford the time or money to pull it off for one reason or another, 3) smoked or shot-up too much of something.

BORROWED TIME I think time is running out the way 1) attacks are on the rise, 2) it is difficult to tell if all patches are installed & working correctly, 3) the time lag from discovery to recognition to patch, etc. I no longer view the following as sufficient:

- 1) downloading from "trustworthy" sources and CDs
- 2) constantly patching Windows and Internet Explorer
- 3) running Outlook Express in Restricted Sites zone
- 4) avoiding dangerous extensions or using viewers (ex. Word Viewer)
- 5) Note: loading a \*.jpg or \*.txt into a program that cares about format, not extension such as Word thinking it is safe is a good way to get bit.

Besides to error is human.

INTEGRITY AND OVERLAP It seems to me that since integrity checking and keeping track of changes are needed both from various points of views: anti-virus / trojan security and installation / configuration diagnostics, the best program would do both. In fact the program should create databases from write-protected floppies (preferably using a real OS such as Linux and bus mastering 32-bit IDE, SCSI, or USB 2 access if possible for decent scanning speed, although DOS programs built with a 32 bit extender will probably do if it gives fast hard disk access too) and compare results with copies made by a companion Windows program. Of course, the databases need to be stored on the hard drive(s).

DOES GOOD PICTURE TAKING EXIST? I have more faith at taking snapshots at system startup (less likelihood of conflicts), yet the only three programs I know of don't meet my needs. ZDNet's INCTRL5 and ArkoSoft's System Snapshot are too simplistic, while Lanovation's PictureTaker is steeply priced and probably doesn't have the relevant features I'm looking for. I'd want to be able to get reports between any two of periodic snapshots, get lists of frequently changed items to mark ignore or generally ignore, etc.

It seems to me that in combining the most of the various tools mentioned above would make adding anti-trojan capabilities somewhat redundant.

What do you think? Comments appreciated, besides "you don't ask for much." Thanks in advance.

--  
Extract tooth to reply

Additional Keywords and Phrases: boot startup checker CRC checksum checksums diagnostic installations registry setting settings configurations scanner scanners floppy home office home computer small business small businesses change small office home office, trojans, integrity checker

---

- ***Next message:*** those who know me have no need of my name: "Re: Test URL for SSL Client Authentication"
- ***Previous message:*** wlhaught: "Is there a program for converting downloads (ex: ROT13) to protect them from viruses & a DOS or Linux companion prog for reversing the process? ver. 1.10 Plural keyword header copy ignore"
- ***Messages sorted by:*** [ date ] [ thread ] [ subject ] [ author ] [ attachment ]