MICHAEL J. TONSING

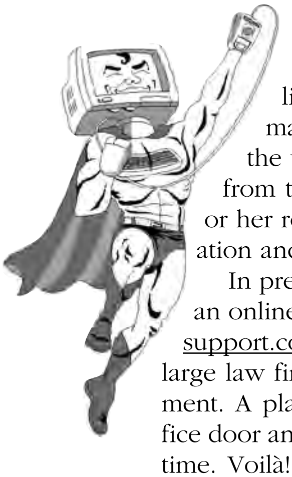
Columnist's Personal Rootkit Horror Leads to Suggestions

My laptop computer was slowing noticeably. Ominously, some programs were refusing to boot up despite repeated clicks on their icons. My suspicions were aroused. I intuitively knew I had a problem that was bigger than my ability to resolve it on my own.

As I later learned, my laptop had been infiltrated by a "rootkit." Sounds bad and it is. It's a stealth program that allows an intruder to masquerade as what Windows™ calls a "system administrator." That means that the phony user can take over, and keep full control of, the "rooted" computer—in this instance, my laptop.

Most rootkits are designed to accomplish such nefarious tasks as hiding files, processes, network connections, blocks of memory, or other essential aspects of an otherwise well-performing computer. (Not every rootkit is malicious. Rootkits may be used for both productive and destructive purposes. However, most rootkits are bad news indeed.)

Most rootkits are surreptitiously installed with the specific intent to abuse a compromised computer's operating system. They often include a so-called backdoor to give the "bad guys" subsequent access at any time they choose to re-enter. A backdoor may also allow the bad guys to look like good guys; processes can be initiated by the nonresident alien operator just as though they were being started by the owner. Yikes!



Adding to their scariness, rootkits are hard to detect with common antivirus programs. In fact, rootkits are often deliberately used in conjunction with other malicious programs as a means of keeping the underlying virus they embed undetectable from the eyes of the computer's owner and his or her routine antivirus scans. I was in a bad situation and I knew it. What to do?

In previous columns, I've extolled the virtues of an online repair service called Support.com (www.support.com). Back in the days when I worked in a large law firm, I'd just call the folks in our IT department. A platoon of geeks would show up at my office door and salute. Problems solved. Back to billable time. Voilà! Now that I am on my own, I am glad I have found the geek platoon's "virtual" replacement—Support.com. It is an online support company that solves hundreds of problems users of personal computers encounter every day.

From removing a virus to optimizing a slow computer, the service has developed "remote technology"—literally taking over your computer's cursor—to diagnose, repair, and even optimize your computer from afar. (Afar is not *too* far. It is not Islamabad. The company is based in Redwood City, Calif.; it is, in other words, in the heart of Silicon Valley. The technician at the other end of my recent call was a college graduate who had majored in computer science and was living in Colorado. Wow! What a concept!) With all due respect to offshore help services, too many have lightweight technicians who operate from a troubleshooting manual; if you listen closely, you can hear them feverishly turning the pages. Given their lack of breadth, it is far too easy for them to avoid confronting the problem and to blame something else. In my experience, it is all too often Microsoft™ that gets the blame, and the technician conveniently wiggles off the hook. Problems unsolved.

The company behind the Support.com concept is SupportSoft Inc., a solid, publicly traded company (SPRT on the NASDAQ exchange) established more than a decade ago. SupportSoft provides outsourced diagnostic, setup, and repair software as well as computer services to larger corporations, including a number of Fortune 100 companies. SupportSoft made the strategic decision to market its same expert computer support, its same tools, and its proprietary technology to individuals and small firms through its online subsidiary, Support.com. The service is my knight in shining armor, ready to slay the rootkit dragon!

After extensive efforts (oh, how glad I am that Support.com quotes a price at the outset and does not charge by the minute or hour), my online engineer in Colorado was beginning to psychologically prepare me for the worst. He began talking about the possibility that we might have to reformat—that is, totally erase—my entire hard drive to cleanse the laptop of the rootkits embedded deeply within it; then, all at once, he lured the varmints out of hiding and was able to totally erase them, leaving everything else intact. Whew!

Just because I dodged the bullet this time doesn't mean *you* will if you are unfortunate enough to download a rootkit of your own. Nor will *I* necessarily have the same happy result the next time. So, here's a lesson on what to do to maximize your protection when you are just starting out with a new computer, or when (Perish the thought!) you have to reformat and start over.

It is tempting to just set up your Vista™ system and start loading your favorite programs, especially if you have no IT department. However, committing to just a few hours at the beginning, taking some simple and prudent precautions, and installing a few mission-critical software applications can keep your system running much more smoothly and safely over the long haul. Here are a few “must do’s” for that first day.

Update Right Out of the Box

In the time your computer sat on a shelf in a warehouse or store—or was in transit to you from an Internet source—important fixes or helpful driver updates could have been released. You will want to verify immediately upon plugging in your new computer that you have the most recent versions and ensure that you’ve been set to get new updates as soon as they’re up and running. This is not only a question of fixing bugs in programs but also an issue of security and data integrity.

But, Wait! First, Get that Firewall Going

In order to get these important fixes or helpful driver updates, you’ll, of course, need to connect to the Internet—potential problem in the making! So, *even before looking for those helpful updates*, be sure your firewall is functioning. If you’ve bought a whole system from a major supplier, chances are good that your computer already has a third-party firewall installed and running; however, you owe it to yourself and your otherwise defenseless little computer to check it out.

If your computer arrives without a firewall, you’ll want at least the basic Windows version working for you. Click your mouse on the Start button in the lower left-hand corner of your screen, then click on Control Panel and after that click on Security. Under the “Windows Firewall” section you will see an option labeled “Turn Windows Firewall on or off.” Click on that option and make sure the radio button next to “On (recommended)” is selected. Then, click OK. On this same screen, just below the Windows Firewall section, you’ll see the Windows Update section. Click on “Turn automatic updating on or off.” If the radio button next to “Install updates automatically (recommended)” is already selected, you’re good to go. If it’s not selected, click that radio button, then use the two drop-down menus beneath that option to specify how often you want Windows to check for updates.

You’ll also need to specify what time you want that check to occur; 3:00 a.m., the default, is generally a good choice (provided that you leave your computer on). Also make sure that “Include recommended updates when downloading, installing, or notifying me about updates” is checked. Then, click OK. Once updates have been found, you can install them by clicking just one button.

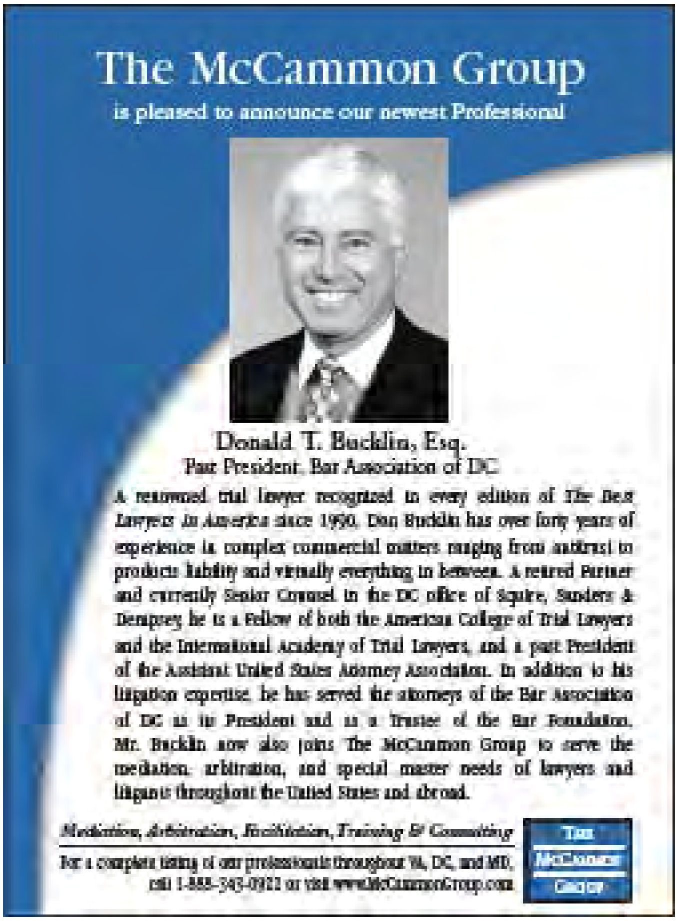
At this point you’ve already set up Windows to download updates automatically, but the first time it does so, you’ll need to run a check manually yourself—unless you’re up past 3 a.m. On that same Security screen, under “Windows Update,” click on “Check for updates.” Depending on the updates that wind up on your list to install, you may need to restart your computer to complete this task.

Back Up Your Pristine Hard Drive

You’ll get only one chance to preserve a backup image of your pristine hard drive. If your Windows installation later gets corrupted (or if you decide at some later date that you just want to start over), having a backup of your system that is “au naturel” could save you grief.

Before installing any software that will alter this sacred moment, make a backup of your entire drive—operating system and all. This is called “ghosting” your hard drive. In fact, there’s a commercial product—Norton Ghost™—that will do just that. It has some added bells and whistles, and you should consider purchasing it, but there is a freeware alternative that you can download very quickly, and, in the right circumstances, that will accomplish the job. DriveImage XML™ (www.runtime.org/driveimage-xml.htm) is a small program that can be easily installed and that will meet all your basic ghosting needs. It is free only

CYBERIA *continued on page 16*



for noncommercial use. An annual license/subscription (which includes all updates) costs $100, and it can cover up to five computers. If you have a second hard drive—or, better yet, an external drive—it would be prudent to ensconce your backup or ghost there.

Configure Windows to automatically back up your files regularly so that your data files are always safe. Even though you've just created a ghost of your operating system, you'll probably be adding new data that you'll also want to protect. So, before doing anything else, set up a system to back up your crucial files. Windows Vista's built-in backup tool is incredibly easy to use. Those using other operating systems (I use Windows XP™) may want to invest in backup software.

We've covered backup systems and programs before in this column. As with your ghost files, you can save your backed-up files anywhere—including your primary hard drive—but if something happens to that drive you could be out of luck. A second internal hard drive is a better choice. An external hard drive that won't be damaged if your computer experiences a massive failure is even better.

In addition, there are online backup services available that will protect even folks whose neighborhoods fall into an abyss when the big earthquake that experts predict for California eventually hits. I use Carbonite™ as a backup service. It encrypts my files before automatically uploading them to the Carbonite server. The service runs $55 per year and is well worth it as a "data insurance policy." Carbonite has been trouble-free and has saved me at least once when my C drive totally deserted me.

Install Security Software

The first software you install should always be security software to keep your data protected whenever you're connected to the Internet. At the absolute minimum, you'll want a virus scanner; other tools (such as antispam or anti-phishing applications) could save you a lot of time wandering around Cyberia in a haze, depending on how you use your computer.

Whether you have to install the security software yourself or it comes pre-installed, activate the software and run a scan immediately. Also be sure to configure the software to scan and update automatically, just like you did when you set up your backup. You never know when a threat can strike, so don't take chances.

Even though Windows comes with its own protection program—Windows Defender—it probably won't be enough. Spybot—Search and Destroy™ is especially useful, because, in addition to scrubbing your hard drive of potentially malicious stealth programs, it also immunizes your computer so you can keep these ugly creatures away in the first place. Put simply, Spybot detects and automatically removes troublesome files from your computer as they enter. Targets for removal can be sent directly to the included file shredder, toasting them completely and thus ensuring their complete elimination from your system. Spybot is freeware. It can be downloaded from a number of sites that feature freeware and shareware, such as one that I have relied on for many years, www.tucows.com, or you can go directly to spybot.s-d2009.com/index.asp?aff=104&camp=gg_sd_us&se=google. (Beware, though, that if you visit www.tucows.com, you are likely to come back with other enthralling and useful programs, too. I find them hard to resist.)

Install Everything Else

Productivity packages, lawyer software, and everything else takes a backseat to safety, so don't even think about installing them until you've protected your computer with the first four steps described above. Then, and only then, are you ready to start using your computer however you want. As you do so, you might consider running DriveImage XML or Norton Ghost again, so that you can preserve a complete image of your system at full bore as well. Just don't lose or delete your baseline backup when you do so! I hope that you'll never need to rely on your backups, but if you do, you'll almost certainly be glad you took the time to set everything up right.

Conclusion

Even though all the steps outlined above will not necessarily inoculate your computer completely from an invasive rootkit like the one I experienced, taking these precautions will dramatically lessen the chances that your computer will get infected. Following these suggestions will certainly improve your odds of keeping your hard drive from needing a hard scrub if your hand-crafted Cyberian protection strategy goes awry. If all else fails, consider a subscription to Support.com. Frankly, the service is a great bargain for those of us who sometimes face compelling deadlines and need highly competent problem-solvers on short notice. **TFL**

Michael J. Tonsing practices law in San Francisco. He is a member of the FBA editorial board and has served on the Executive Committee of Law Practice Management and Tecchnology Section of the State Bar of California. He also mentors less-experienced litigators by serving as a "second chair" to their trials (www.Your-Second-Chair.com). He can be reached at mtonsing@lawyer.com.