Five Steps to Ditching Malware

Security scams abound, but here are some practical ways to clean up the mess.

Michael Horowitz, Computerworld

Apr 17, 2009 11:24 am

Malware (malicious software) seems to be getting worse. No surprise, since there's big money in it as a recent article in the Wall Street Journal pointed out. Typical scams aim to scare unsophisticated users with phony warnings that their computer is infected with a virus. Conveniently, the warning is followed by prompts to install software to remove the virus. Victims pay for the phony antivirus software and end up infected to boot. The term for this is scareware. A recent Microsoft report found one particular scareware program installed on 4.4 million computers. Scareware is not something that Vista's UAC can prevent since the user invites it in. Among the scareware programs are Antivirus'09, Personal Antivirus, WinDefender 2008, P Antispyware 09, WinPC Antivirus, RapidAntivirus, WinAntivirus, XP Antivirus and DriveCleaner. So, many people need malware removal. But how?

BACKUP FIRST

I suggest that the first step be to make a disk image backup of the infected machine. A disk image backup insures that all your files are backed up. No matter how well meaning any person or software may be; things can go wrong in the cleanup process. Any worthwhile disk image backup program should be able to run from a bootable CD or USB flash drive and write the backup to an external hard drive or another computer on a LAN. You should then be able to mount the backup on another computer and copy off individual files as needed.

If the important files on the infected computer are few in number, then you might boot the machine using a Linux Live CD or a bootable USB flash drive running Linux. I'm partial to Ubuntu, but there are many Linux distributions that can run from a bootable CD and/or USB flash drive. As with the disk image backup, Linux should be able to copy files to an external hard drive or another machine on a LAN. If the files are small enough, they can be copied to a USB flash drive.

THE WORST OPTION

The worst option is the one most people probably use. Install anti-malware software on the infected machine and let it try to remove the infection. What makes this a poor option is that much of the current crop of malware is sophisticated and defends itself well. The big money to be made peddling malware draws talented programmers. To see this up close and personal, take a look at the SRI International Technical Report An Analysis of Conficker's Logic and Rendezvous Points. It's obvious from the report how much care and effort went into constructing Conficker.

You have to think of the infected copy of Windows as your enemy rather than your friend. That's why my two suggestions so far involved not running the infected OS at all. Any solution that involves running the infected copy of Windows is suspect because the OS itself is suspect.

As Roger Grimes put it "... don't let a well-meaning friend or computer geek talk you into merely scanning and "removing" the malware and hoping for the best."

SAFE MODE

The next best option is to run anti-malware in safe mode. While this is better than booting normally, it's still not optimal. Yes, safe mode prevents many auto-started programs from running, but the malware may have infected the operating system itself. In my previous posting, I discussed rootkits and how they can modify the operating system to hide their files. That's only one way that rootkit software can compromise the system. It might also, for example, hide its process. Once Windows has been compromised, you can't count on safe mode to provide a truly clean environment.

REMOVING THE HARD DISK

For anti-malware software to have the best chance of detecting and removing an infection it has to see all the files and all the processes. In other words, it needs to run on a clean system. Kind of ironic actually. The best way to accomplish this is to remove the infected hard drive from the infected computer and connect it as a data (non-booting) drive on a clean system. I discussed this too in my previous posting.

Is this extra effort worthwhile?

I think so. As you do more and more things with your computer, it becomes more valuable, both to you and to the bad guys. Security maven Steve Gibson recently mentioned that's what he did when cleaning up a computer for a friend.

There are many good anti-malware programs. Previously, on this blog, I've written about Malwarebytes' Anti-Malware, Avira Antivirus and Microsoft's Malicious Software Removal Tool. The most important point is not to try and find the best program but to use more than one. No program is perfect. Back in January, I wrote about Avira Antivirus finding malware to remove after many other anti-malware programs had removed what they found from a terribly infected machine. Likewise, my experience sending suspicious files to virustotal.com confirms that the best approach is to use multiple products. I suggest running at least three anti-malware programs, five is better.

But even that's not really sufficient.

After removing malware and restoring the hard drive back to the original computer, you should probably run a couple anti-rootkit scanners before connecting the machine to any network. I've had very good luck with the free GMER scanner. RootkitRevealer is meant for techies and comes from a trustworthy source (Bryce Cogswell and Mark Russinovich of Microsoft) but hasn't been updated in a few years. Many companies offering antivirus software also offer dedicated anti-rootkit software.

CLEAN RE-INSTALL

Up till now, the choices have been easy; safe mode is better than a normal boot and removing the hard disk is better than safe mode. But is even removing the hard disk sufficient? Should you instead give up and walk away from an infected copy of Windows without even bothering to do any remediation?

Tough call.

Leo Notenboom, the man behind ask-leo.com says, “Once your machine has been infected, it's not your machine any more. Trying to remove an infection is the most common approach, and it often works; problem is there's no way to be absolutely certain. Thinking that you've cleared an infection and being wrong can, in the long run, cost more time, effort and risk of data loss than simply biting the bullet, reinstalling and being sure.”

Roger Grimes over at InfoWorld is also a proponent of a fresh, clean OS installation rather than remediation. He says, “Don't simply dismiss today's computer exploitations as an annoyance like we did just a few years ago. That was play time; this is serious. ... 99 percent of malware is crimeware designed to hurt you financially. If you discover that a malware program is active on your computer, you don't want to take any chances. Even if your antivirus program tells you it is simple adware, don't take any chances ... Today's malware exists to steal your money, whether it is through your identity, passwords, data, or bank account. There is no way to tell how the malware has modified your computer beyond the rogue executables you or your antivirus program has found. There is no antivirus removal program that can be guaranteed to have completely cleaned your machine. Your livelihood is at stake. So don't fight malware -- eradicate it!”

The easy solutions are sub-optimal and the better solutions are, frankly, a huge pain in the neck. Defensive computing, preparing for trouble ahead of time, is the way to go. Leo Notenboom agrees, "Prevention - through appropriate tools, technologies and behaviors - is much easier and cheaper than the cure" he says.

When prevention fails, you want to have an old, clean disk image backup to fall back on. It's a far better option than either a clean OS install or removing the hard drive to scan it from a clean machine.