By Michael Kassner

Cybercriminals are putting forth every effort to make malware difficult to detect. Successfully, I might add. Ever optimistic, I thought I would have a go at providing information on how to make their job a little tougher.

Baselining is an important reference

Knowing exactly what is running on a computer is paramount to learning what shouldn't be. Creating a reference baseline is the best way I've found to accomplish this. Let's look at three applications that do just that.

1 Microsoft Process Explorer (formerly Sysinternals)

Process Explorer provides an excellent way to determine what processes are running on a computer. It also describes the function of each process.

More important, you can use Process Explorer to create a baseline of the running processes used by the computer when it's operating correctly. If for some reason the computer starts behaving poorly, run Process Explorer again and compare the scans. Any differences will be good places to start looking for malware.

2 Trend Micro's HiJackThis

HiJackThis is Process Explorer on steroids, making the application somewhat daunting to those of us not completely familiar with operating systems. Still, running HiJackThis before having malware problems creates a great reference baseline, making it easy to spot changes.

If it's too late to run a baseline scan, do not fear. Several Web sites offer online applications that will automatically analyze the log file from HiJackThis, pointing out possible conflicts. Two that I use are HiJackThis.de Security and NetworkTechs.com. If you would rather have trained experts help, I would recommend WindowSecurity.com's HiJackThis forum.

3 Kaspersky's GetSystemInfo

Kaspersky has an application similar to HiJackThis called GetSystemInfo. I like the fact that Kaspersky has an online parser. Just upload the log file and the parser will point out any disparities. GetSystemInfo, like the other scanners, is a good way to keep track of what's on the computer, and if need be, it can help find any malware that happens to sneak in.

Be careful: As I alluded to earlier, removing processes suggested by the scanners is not for the faint of heart. It requires in-depth knowledge of operating systems or being able to compare before and after scans.

Next, I'd like to discuss two vulnerability scanners.

It's simple: No vulnerabilities, no malware

Anti-malware includes any program that combats malware, whether it's real-time protection or detection and removal of existing malware. Vulnerability scanners proactively detect vulnerabilities so that malware can't gain a foothold. I'd rather update applications than chase malware any day.

4 Microsoft Baseline Security Analyzer

Microsoft Baseline Security Analyzer (MBSA) is a vulnerability scanner that detects insecure configuration settings and checks all installed Microsoft products for missing security updates. I recommend using MBSA when upper management needs convincing. Making a case for needing a vulnerability scanner is sometimes easier if the product is from the OEM.

5 Secunia inspection scanners

Secunia's scanners are similar to MBSA when it comes to Microsoft products. But unlike MBSA, Secunia products also scan hundreds of third-party applications, which gives Secunia a distinct advantage.

All the Secunia scanners, online and client-side, have an intuitive way of determining what is wrong and how to rectify it. They usually offer a link to the application's Web page, where the update can be downloaded.

Not always simple

Remember when I said, "It's simple: No vulnerabilities, no malware"? Well, it's not exactly that easy. It would be, except for those nasty things called zero-day exploits and zero-day viruses. That's where antivirus applications come into play, especially if they use heuristics.

6 Antivirus programs

Lately, antivirus software is getting little respect. Like everyone, I get frustrated when my antivirus program misses malcode that other scanners mange to find. Still, I would not run a computer without antivirus. It's too risky. I subscribe to the layered approach when it comes to security.

Choosing the correct antivirus application is personal. Comments come fast and furious when someone asks TechRepublic members which one is the best. A majority feel that any of the free versions are fine for nonbusiness use. I use Avast or Comodo on Windows machines.

Anti-malware enforcers

The next class of anti-malware is capable of both detecting and removing malware. I'm sure you are wondering why not just use these from the start. I wish it was that simple.

Scanners use signature files and heuristics to detect malware. Malware developers know all about each and can morph their code, which then nullifies signature files and confuses heuristics. That's why malware scanners aren't the cure-all answer. Maybe someday.

More caution: I want to emphasize that you need to be careful when picking malware scanners. The bad guys like to disguise malware (antivirus 2009) as a malware scanner, claiming it will solve all your problems. All four of the scanners I have chosen are recommended by experts.

7 Microsoft's Malicious Software Removal Tool

Malicious Software Removal Tool (MSRT) is a good general malware removal tool, simply because Microsoft should know whether the scanned code is theirs or not. Three things I like about MSRT are:

- The scan and removal process is automated.
- Windows Update keeps the signature file database current automatically.
- It has the advantage of being an OEM product, thus it's less intrusive and more likely to be accepted by management.

8 SUPERAntiSpyware

SUPERAntiSpyware is another general purpose scanner that does a good job of detecting and removing most malware. I have used it on several occasions and found it to be more than adequate.

A number of TechRepublic members have mentioned to me that SUPERAntiSpyware was the only scanner they found capable of completely removing antivirus 2009 (malware).

9 Malwarebyte's Anti-Malware

Malwarebytes Anti-Malware (MBAM) malware scanner was the most successful of the four I tested. I was first introduced to it by world-renowned malware expert Dr. Jose Nazario of Arbor Networks. For a detailed explanation of how MBAM works, refer to my post Malware scanners: MBAM is best of breed.

Still, MBAM does not catch everything. As I pointed out in the MBAM article, it misses some of the more sophisticated malware, especially rootkits. When that happens, I turn to the next malware scanner.

10 GMER

In Rootkits: Is removing them even possible?, I explained why it's hard to find rootkit malware. Fortunately, GMER is one of the best when it comes to detecting and removing rootkits -- enough so that it's recommended by Dr. Nazario.

Final thoughts

Using the above anti-malware techniques will go a long way in making it tough for malware developers, especially if you:

- Make sure all software on your computer is up to date.
- Run a baseline scan and save the log file. (You may need it later.)
- Scan for malware on a regular basis, since sophisticated malware runs quietly.

Additional resources

- TechRepublic's Downloads RSS Feed XML
- Sign up for the Downloads at TechRepublic newsletter
- Sign up for our 10 Things Newsletter
- Check out all of TechRepublic's free newsletters
- The 10 faces of computer malware
- Malware response poster
- 10 things you should do to a new PC before connecting it to the Internet

Version history

Version: 1.0
Published: August 25, 2009

Tell us what you think

TechRepublic downloads are designed to help you get your job done as painlessly and effectively as possible. Because we're continually looking for ways to improve the usefulness of these tools, we need your feedback. Please take a minute to drop us a line and tell us how well this download worked for you and offer your suggestions for improvement.

Thanks!

—The TechRepublic Content Team