

Stealth & Vulnerability

For many years, anti-malware industry developers and researchers have been waging a bitter war against malware writers. Even if the objectives of the malware writers have radically changed from fun to profit, the arms race has always continued. Malware writers are constantly trying to create programs that will evade antivirus detection. On the other side of no-man's land, antivirus software developers have constantly worked to create innovative and efficient solutions with the best possible malware detection rate.

Various techniques can be used to bypass antivirus software. Some types of malware continuously modify themselves to look different every time they infect or execute, thus fooling some solutions. In fact, in the 1990s the rise of the polymorphic virus changed the face of the industry when some antivirus vendors who were unable to keep up with this trend simply abandoned ship. Another "classic" approach is to hide the evidence of compromise or infection from security software using stealth techniques: we used to call this advanced or level 3 stealth. While present-day rootkits often use stealth techniques to conceal their presence.

http://www.eset.com/download/whitepapers/Whitepaper-Rootkit_Root_Of_All_Evil.pdf). On occasion, malware may attempt to exploit some feature of a specific security program, especially a programming error leading to a vulnerability such as a buffer overflow. While you might get the impression from the media and some sectors of the security industry that this is an enormous problem, in real life such vulnerabilities are dealt with as quickly as possible, and we don't see much evidence that malware authors spend a lot of time on exploiting such vulnerabilities.

More aggressive malware may also try to disable security software, including personal firewalls and antivirus. There's nothing novel about this: we've been seeing it for decades. Malware intentionally interfering with antimalware software goes back to 1990, at least. Antivirus software and malicious software, however sophisticated, are simply programs that execute within an operating system. The fact that one program can sometimes affect the running of another (and even disable it) is not a bug that needs to be fixed, but a normal function within most operating systems. (There are operating systems that enforce much stricter control, but it's unlikely that you have one on your desktop.) For example, it is mandatory for a program that manages the power on a laptop to be able to suspend all processes when the system is going into hibernation.

Some malware families have been trying to disable ESET Antivirus (and other top-rated anti-malware products) for years and, in some scenarios, will succeed: this is something we take seriously and we have implemented various defensive mechanisms to reduce the likelihood of their succeeding. It isn't surprising when the bad guys go out of their way to target a solution that's particularly noted for its ability

to detect many new threats proactively. After all, a program that can evade detection by ESET Antivirus is likely to be missed by many other vendors, too.

While we do our best to mitigate the risks from our side, there are also a number of simple measures that any antivirus user can take to reduce the risk that their scanner will be disabled by a malicious program:

- Make sure your security software is kept up-to-date
- Log onto the system as a normal user without administrative privileges instead of an administrator (in Windows) or root (in Unix-derived systems):. If the antivirus program executes with higher privileges than the user logged in (as happens with Windows service or a Unix daemon), a malicious program with lower privileges (those of a normal user) will normally be unable to terminate the antivirus (assuming the absence of some form of privilege escalation exploit).
- Keep operating systems and applications fully patched and up-to-date with all hot fixes
- Avoid risky web sites (we know, easier said than done: the trick is to be cautious and if in doubt, don't)
- Enable all security features in your web browser
- Above all, don't run software from untrusted and untrustworthy sources.

It doesn't matter how sophisticated malicious code is if it never gets the chance to run. Don't fall into the trap of thinking that security software (even ours!) offers such perfect protection that you don't have to think about whether it's wise to run a program from an unreliable source. Anti-virus can't catch everything, even with advanced heuristics like ours.

The ESET Research Team