Why Don't Anti-malware Tools Work Better?

I've been an independent computer repair tech for over 12 years now. The question I get the most (and have the hardest time answering) is this: how come my antivirus program didn't stop me from getting this virus? When you're installing AVG, the program says that only 3% of today's security problems are caused by traditional viruses. Is this true? Is it true for the other antivirus programs as well?

In other words, why don't anti-malware tools work better than we want or even expect them to? ☺

I have to fault AVG for the phrase “traditional viruses”. I think that puts an unrealistic spin on your expectations. Malware is malware, and that includes viruses, spyware, ransomware, rootkits, zombies, and gosh knows what else.

What do they mean by “traditional”? I have no idea. I also have no idea where that 3% figure comes from.

But there's a kernel of truth in AVG's statement. No matter what program you run, there's still a chance your computer will get infected.

A common goal

In the past, we categorized security software by the type of malware being targeted.

Anti-virus programs examined files for data patterns matching those of known viruses. Anti-spyware tools monitored your machine for known spyware behavior. Anti-rootkit programs specifically countered advanced techniques used by rootkits to hide files.

Basically, any “anti-whatever” program sliced the malware universe in a unique way, using specific techniques to look for or protect against specific types of threats.

In recent years, the lines between different types of malware has become significantly blurred. Spyware might include malware-like behaviors, viruses might employ some of the techniques of a rootkit, and so on.

Security software vendors adjusted their approach too. Most packages are just that — *security*packages — ideally addressing all aspects of malware detection, prevention, and recovery, regardless of the style of attack.

These varying classes of malware still require different techniques for detection and prevention, and each anti-malware tool is likely to be stronger in some areas and weaker in others.

Different programs, different techniques

Even within the same category, anti-malware tools from competing vendors often use different techniques to detect malware. This is one of the biggest reasons one tool will not detect the same malware as another.

Malware is crafty. It uses a variety of techniques to avoid detection and get into your system. From making sure that no two copies of itself look alike, to encrypting key parts of its inner workings, the ways malware can hide is only limited by the malware author's skill.

That's why anti-malware tools constant play a game of catch-up. Every time new malware is found, the tools must be updated. Most often, it's a simple matter of updating the database of known malware with new information.

But this can be more involved than you think. Malware can be so good at hiding itself that a simple database update isn't enough; the fundamental technique used simply can't detect the new malware. In such a case, the tool itself needs to be updated.

Different companies, different responses

New malware of all forms is discovered daily. This means anti-malware companies need the resources and dedication to continually update their database and tools. They also need the infrastructure, maturity, and means to rapidly implement, test, and deploy changes to those tools.

That's another source of disparity among security software vendors: some are better at effective, rapid deployment than others.

It may not even be a matter of competence, but prioritization. Specific malware might be considered high priority by one company, requiring an immediate update, while another company might see it as less important and thus take longer to respond.

I don't mean to imply that any of this is easy. We've seen major security vendors push out updates that have failed, or even crashed some customer's machines. It should never happen, but in the rush to get updates tested and out quickly… well, I'm surprised these problems don't happen more often. It's exceptionally difficult to get it right 100% of the time, especially when we expect anti-malware tools to not impact the performance or functionality of our machines while they do their important work.

Dancing bunnies?

I've written about “The Dancing Bunnies Problem” before. In essence, it's simply this: people explicitly ignore, disable, and bypass all security measures to access something they've been led to believe is desirable. If an email you get says “download the attachment to see dancing bunnies”, some percentage of users will do exactly that and more, if necessary, because they've been promised dancing bunnies, *dammit*.

Put in more relevant terms, you can have the best anti-malware and security software that could possibly exist, and it'll do you absolutely no good if you ignore its warnings or bypass its restrictions.

Your security software “allowed” you to get malware because you told it to, explicitly, against its warnings and advice.

It didn't matter what security software you were running, or how good it might be.

What's it all mean?

There is no single best anti-malware tool.

Security tool “A” may catch this newly-released virus today, but tomorrow's new virus might be caught more effectively by program “B”. Most vendors know this, so they're continually working to improve the coverage of their products.

The techniques used by program “C” may work with little to no impact on my system, yet be a major resource hog on yours. The best vendors test across a wide variety of systems and configurations, but by definition, doing so is in direct conflict with getting important updates out as quickly as possible.

And of course there's still a race between malware authors releasing new versions, and anti-malware vendors struggling to make sure each new issue gets caught quickly and safely. There's always a hole in the coverage and something will slip through.

The best anti-malware tool

You are the most important anti-malware tool your computer has.

Your ability to recognize and skip malware is far superior to that of most anti-malware tools. You can recognize spam and bogus attachments. You know you shouldn't have visited that website. You know that too-good-to-be-true offer was, indeed, too good to be true. You know that the dancing bunnies were never real.

That knowledge, and what you do with it, is what keeps your machine safest.

Related Links & Comments: Why Don't Anti-malware Tools Work Better?
https://askleo.com/4728