The effectiveness of anti-malware tools

Bruce Potter, founder, Ponte Technologies, and organiser, Shmoocon
Greg Day, senior security researcher, McAfee

An increasing number of security experts are questioning the utility of anti-malware tools. They cite malware writers' ability to test their products against anti-malware engines, and argue that these tools are ineffective against zero-day attacks. This face-off column pits Bruce Potter, organiser of the Shmoocon conference and an anti-malware sceptic, against Greg Day, senior security researcher at McAfee, who has his own perspectives.

Bruce Potter, Ponte Technologies

There are two types of attacks today on the internet: those you can stop with commodity security products, and those that you can't. Dedicated attackers spend a great deal of time and energy developing new attacks that evade detection by the existing security infrastructure. These attacks are then launched and used for a variety of purposes including theft, corporate espionage, and even simple thrill seeking.

"Using tools and techniques that are already known about will dramatically decrease the operation's likelihood of success"

Eventually these new attacks are discovered by users, analysed by security vendors, and their signatures and habits get integrated into products such as anti-virus and IDS. Once an attack moves from the 'unstoppable' to the 'stoppable' bucket, their utility drops dramatically, and attackers stop using these attacks in favour of new ones.

Cat and mouse

It may seem simplistic, but this is the general cycle of viruses, worms, and malware that has been occurring for decades. Attackers are no different than normal IT users when it comes to getting their job done. An attacker makes a risk/reward trade off when executing an attack. When attempting to commit fraud at a bank, an attacker wants to use malware that has a high probability of success with a low probability of getting caught.

Using tools and techniques that are already known about will dramatically decrease the operation's likelihood of success. If someone is going to go through the hassle of committing fraud or stealing a company's secrets, they're going to make sure they're using a tool that will allow them to succeed.

This cycle puts anti-virus software in an odd situation. We all know anti-virus can't be 100% effective. It turns out that in the face of a dedicated attacker, AV isn't anywhere near 100% effective, and the effectiveness rate of AV in the face of directed attacks is probably even much worse. However, the bread and butter of AV is stopping all the known attacks. The success rate with known viruses and malware is much higher, but how much is the overhead of antivirus worth when you compare it to the class of attacks it is stopping? Further, how many of these known attacks can be stopped by simply using good computing practices?

An unacceptable overhead?

The overhead of AV on individuals and corporations can be very high. Companies spend huge amounts of money each year to keep AV products on end user desktops. Further, each AV instance needs to be supported and fixed if something goes wrong. When you look at the average number of IT security staff in a given organisation, there can be a disparate number of hours spent on dealing with individual user AV issues when compared to dealing with more strategic, enterprise security issues such as maintaining firewalls and attack detection. Desktop AV can pull staff away from projects and programs that have large scale impact and have them dealing with individual user needs.

For users at home and home offices, AV can represent a significant percentage of the purchase price of a PC. Many home PCs can be purchased for around $500 at any major retailer, while the cost of activating AV on the system can be as high as $50. That increases the cost of the PC by 10% just to make the system more 'secure'. Beyond that, these users are often their own help desk for all problems, including security related issues. Troubleshooting AV for non-IT experts can be fantastically complicated and result in unneeded reinstalls of the OS and fear of security threats that don't exist.

Honestly, AV is probably a security product best handled at the enterprise edge. Scanning for viruses and malware at the email gateway (or relying on your ISP to handle it for you if you're a home user) is probably the best way to go. Keeping the desktop secure is probably better handled through user education than through death by security products. Informing users of security best practices such as not opening unwanted attachments, verifying links before you click on them,

and that Javascript-based dialogues and windows can often not be what they seem can go a long way towards keeping the desktop environment secure. Ultimately a slightly educated user and AV at the mail gateway is probably a better economic and security bet than AV on every single desktop.

As a side note, I'm a security professional by day and go to many unsavoury parts of the internet for my job. But through diligence and common sense, I've never had a virus, worm, or malware on any of my PCs - and I haven't run anti-virus software in over 10 years.

Greg Day, security analyst, McAfee

Dr Solomon's anti-virus, now McAfee, started when Alan Solomon wrote a program to remove an early virus. At the time, he was offering a hard disk recovery service and had received several drives with the same virus issue. To save time, he wrote additional code to recognise the infection, so he knew when to run his program.

This is the fundamental premise on which anti-virus software has been based for more than 20 years: the ability to identify a unique malicious attack and then clean the infected system to eliminate it.

Evolving threats

Since the first anti-virus signatures were written, threats have evolved and so too has technology. The challenge in security is in keeping pace with changing threats, as cybercriminals adapt their methodologies to try to stay ahead of defences. Signatures, a key method of defence and response in those early days, have demonstrated their worth, but also their limitations and other approaches have moved anti-virus on significantly.

Anti-virus today is a combination of all the evolutionary steps that it has taken. From the reactive approach of signature-based detection, it has become increasingly more proactive and, ultimately, what we have today is a combination of both approaches. That first step that anti-virus took all those years ago has proven to be of the utmost importance. It enables not only alerting, but also the cleaning of systems, facilitating recovery. However, signatures require time-consuming analysis, development and testing. Heuristics were the first step in staying ahead of the threat, done by looking for actions indicative of an attack and blocking that attack.

The evolution of detection

Next came generic detection and repair, which dealt with the myriad new threats and variants that emerged in the late 1990s, thanks to malware generation tools. This again strengthened what anti-virus could do, and reduced the number of signature updates required to block a threat, making it more efficient.

"Using anti-malware experts' experience to define easy-to-use behavioural controls based on common threat behaviour enables anti-virus tools to block malware proactively"

The turn of the century marked another key development, when behavioural controls mimicked the approach of whitelists and blacklists to permit only trusted behaviour, eliminating behaviours that implied an action was illegitimate. Diversity of IT systems was a challenge here, because most businesses' IT departments often lacked the bandwidth to carry out necessary analysis to get the most out of this approach.

Ultimately, combining both techniques is most effective. Using anti-malware experts' experience to define easy-to-use behavioural controls based on common threat behaviour enables anti-virus tools to block malware proactively. At the same time, signatures provide the ability to define the threat and clean any damage.

For the signature element, time still remained a challenge when coping with creation, testing and customer rollout. Most recently, in-the-cloud security linked customer and vendor. It uses the concept of behavioural heuristics to identify potential threats, allowing an informational fingerprint to be sent to the security vendor and, if recognised, blocking the threat.

Closing the window

This closes the window between discovery and defence from hours to minutes, making real-time protection a reality. Additionally, new threats can be identified and blocked based purely on the collective intelligence that in-the-cloud security provides.

Anti-virus has evolved considerably from early reactionary signature-based detection, retaining its relevance and stopping it from being superseded by another newfangled technology. Blending reactive and proactive controls provides the best of both worlds: proactive behavioural detection that can be easily implemented to defend against the unknown, and signature-based detection to give an understanding of the attack and its implications.

In-the-cloud security has continued the progress along this evolutionary path, virtually closing the time gap between discovery and signature defence. Those most likely to question its value may not fully appreciate the range of approaches it now combines.

Ultimately, anti-virus goes to the important next step – one that cannot be reached by behavioural blocking alone – to removing any infections, enabling confidence and continuity in a world where business just can't wait.