Why Less is More in Antivirus Protection

By Joe Wells, Chief Antivirus Architect

White Paper

July 2003

Abstract

Many of the antivirus products currently on the market claim that "there are nearly 60,000 known computer viruses infecting cyberspace today" and suggest that the sheer number of viruses, worms, Trojans and other threats covered by an antivirus product correlates directly with the level of protection it provides. However, as evidenced by the widely accepted practices of the industry's most respected testing organizations, antivirus products are best evaluated based on their ability to detect a much smaller list comprised of several hundred viruses that are found "in the wild," i.e., those that are actually determined to be spreading and infecting users' systems. The other 59,000-plus "attacks" – labeled as "zoo" viruses by the antivirus industry – are the network security equivalent of dinosaurs: They're interesting from an historical point of view but they're simply not found in practice in today's computer systems. Unfortunately for users, it's easy to conclude that scanning for thousands of additional attacks must somehow provide better protection. But in fact the opposite is true: Scanning for zoo viruses reduces the effectiveness of antivirus products and exposes users to far bigger threats. This paper explains the facts regarding virus threats, traces the history of the WildList, and explains why the term "Less is More" provides the most appropriate benchmark for evaluating the effectiveness of antivirus products.

The Surprising World of Antivirus Testing

In the spring of 2002 I participated in the design of a review of commercial antivirus software products for *PC Magazine*. The review, published in June 2002, was similar in several respects to many such reviews that I've participated in during my more than 15-year career in the antivirus business. Specifically:

- The methodology that we used to evaluate the antivirus products tested their ability to detect a total of 201 viruses, worms, Trojans and other types of content-based threats.
- Several of the products included in the review included statements in their marketing documentation and on their packaging that read essentially as follows:

  "There are nearly 60,000 known computer viruses infecting Cyberspace today."

Clearly, there must be a disconnect somewhere: If there are truly 60,000 known viruses (and related threats like worms, Trojans, etc.) that can infect and spread among computer systems, then why would *PC Magazine* allow a hand-picked team of virus industry experts to evaluate products based on a tiny list with a mere 201 attacks? The answer is simple: The statement regarding the potential threat from "60,000 known computer viruses" is intentionally misleading at best, and is patently false at worst.

While it may be true that tens of thousands of virus threats have been created and identified over the course of the last 20 years, in fact only a tiny fraction of these threats are actually found "in the wild," i.e., the vast majority of known attacks are extinct – or, to use industry jargon, are "zoo viruses."

Like dinosaurs, zoo viruses may be found in a petrified state in museums and laboratories, but you'll never see one in the jungle, or in the case of viruses, you'll never find a zoo virus spreading over data networks and infecting computer systems. This is why virtually all legitimate antivirus product testing today is conducted using a small and widely acknowledged list of so-called "WildList" viruses that are found "in the wild," i.e., they are known to have successfully spread and infected computer systems.

The WildList and the concepts behind it are now more than 10 years old. Yet, still today, considerable confusion grips customers when faced with evaluating antivirus solutions – a fact that is easily exploited by the incumbents in the antivirus industry, for arguably understandable reasons (e.g., the desire to prevent the entry of new potential competitors). However, a careful review of virus history and a consideration of today's rapidly shifting network environment suggest that, rather than providing more protection, antivirus products that scan for thousands of extinct zoo viruses provide no additional benefits and in fact can expose users to significantly greater threats.

The History of the WildList

Approximately 10 years ago, antivirus product vendors were routinely stating that any effective antivirus product should detect "all known viruses." The problem was that no one at that time (myself included) could definitively state what would constitute the list of "all known viruses." To remedy that situation, I consolidated several lists of "common viruses" and posted the combined lists to several of the world's top antivirus experts. I asked them to confirm or refute the listed viruses and to add any that they knew were spreading on users' systems. The list was refined over the course of several months and in mid-1993 I posted the list and called it the WildList (www.wildlist.org).

Before long, the WildList became the industry standard by which products were tested and certified. Today, the WildList is compiled every month using contributions from over 70 of the world's leading virus researchers representing approximately 40 commercial, academic and industry organizations that include Computer Associates, EICAR, F-Secure, ICSA, Kaspersky Labs, McAfee, Microsoft, Panda, Sophos, Symantec, TrendMicro and Virus Bulletin. Many respected testing organizations, including ICSA Labs, Secure Computing and Virus Bulletin, rely on the WildList to establish the benchmark for their antivirus product testing and certification programs. For a few years some testing bodies also tested against additional "zoo" viruses that weren't on the WildList; however, this practice is rarely seen in objective, industry-recognized testing.

Today's WildList has evolved to include several sections that ensure the widest possible representation for reported threats. In all cases, only those attacks for which samples have been obtained and verified are included:

- The "Main List" includes those viruses that have been reported by at least two researchers. The May 2003 WildList registered 210 viruses in the Main List. This number tends to vary by plus or minus 10 viruses each month, representing the addition of 10-20 new attacks and the removal of a similar number that no longer meet the Main List criteria.
- The "Supplemental List" includes viruses that have been reported by only a single researcher. The May 2003 WildList contains 326 entries on the Supplemental List, and tends to range from between 300 to 400 in any given month, for a total of 500 to 600 viruses between the Main and Supplemental lists.
- The WildList also periodically posts a list of "Other" attacks, such as non-PC viruses that attack other operating systems (e.g., Linux, SunOS, etc.) and/or that may not meet the strict definition of a virus but which have been shown to attack user systems. This list typically includes fewer than a dozen viruses.

Over time, a few more viruses are added each month versus the number that are removed, leading to a slow but predictable net increase in the number of combined threats between the Main, Supplemental, and Other Lists published by the Wild List Organization (WLO).

So, despite what one may read in product data sheets and glossy, fear-inducing advertisements, the collective view of the experts representing essentially the entire antivirus industry is that there are far fewer than 60,000 viruses infecting computer systems in Cyberspace. In fact, the number as of May 2003 was precisely 541 threats (including the "Other" list) – less than 1% of the 60,000 claimed!

Reconciling the WildList with Wild Claims

The notion that over 99% of all "known" attacks are harmless is initially difficult to accept. How can the facts regarding the modest size of the WildList (as reported by the world's antivirus researchers from competing vendors) and the marketing claims of traditional antivirus software vendors be reconciled? There are several pieces of evidence to explain the situation:

1. The size of the list of "known viruses" is inflated.

Antivirus software vendors have been exaggerating the number of virus threats for several years. For example, many viruses have dozens of variations that differ in only minor ways from the main virus program. So in the same way that a car manufacturer might try to claim that each combination of interior and exterior colors constitutes a different model car, the antivirus vendors report each variation as a separate virus. In fact, the actual number of virus strains (without counting all of the minor variants) is probably less than 10,000 and may be as few as 5,000.

2. Viruses frequently become extinct when computer hardware and software technologies change.

   - Many older viruses would execute only on specific hardware platforms. An example is the Ping Pong virus, which used to be "in the wild." The Ping Pong virus only executes on Intel 8086 or 8088 processors, and therefore is extinct in today's computing environment, because it cannot run on 286, 386, 486 or Pentium CPUs.
   - Entire classes of viruses tend to become extinct when operating systems change. For example, when Windows 3.1 became common, viruses that infected DOS files went into steep decline. The same occurred when Windows 95 was introduced, and saw the end of many common boot viruses.
   - Changes to popular applications also tend to make the computing environment less friendly to certain viruses. For example, the introduction and rise of Microsoft Office saw the demise of WordBasic viruses like Concept.

3. Many viruses are created in limited or closed environments and never have an opportunity to spread.

   This last category is often the most unsettling type of "non-threat." In theory, is it not possible for some of these zoo viruses to "escape" into the wild? Theoretically this may be so, but the fact is, in over a decade of monitoring and reporting on the virus threat via the WildList, this simply has not happened. We see perhaps 1-2 dozen new viruses each month. Sometimes new viruses are relatively benign, and sometimes they're devastating. But in

virtually all cases on record, new WildList viruses are just that – they're new. And in light of the tendency for viruses to become extinct due to changes in hardware, operating systems and applications, zoo viruses are not likely to retain their potency for very long. As time goes on systems tend to change in ways that reduce or eliminate the vulnerabilities that the zoo viruses exploit. So while it may seem appealing, the idea that having protection against zoo viruses is a good idea "just in case" simply has no basis in actual experience.

When you consider all the factors, i.e., the tendency to inflate the "marketing" (versus the "engineering") number of viruses and the tendency for viruses to become extinct as the environment changes, it isn't hard to see where the 60,000 "known virus" number comes from, and why it has little meaning in the real world.

But How Can It Hurt to be "Protected"?

So this brings us to the final and most critical question: Suppose there really are only about 600 in-the-wild viruses, and that the other 59,000+ really are just variations of perhaps a few thousand base viruses, many of which couldn't possibly attack today's hardware, operating systems and applications. What is the harm in an antivirus product that scans for zoo viruses?

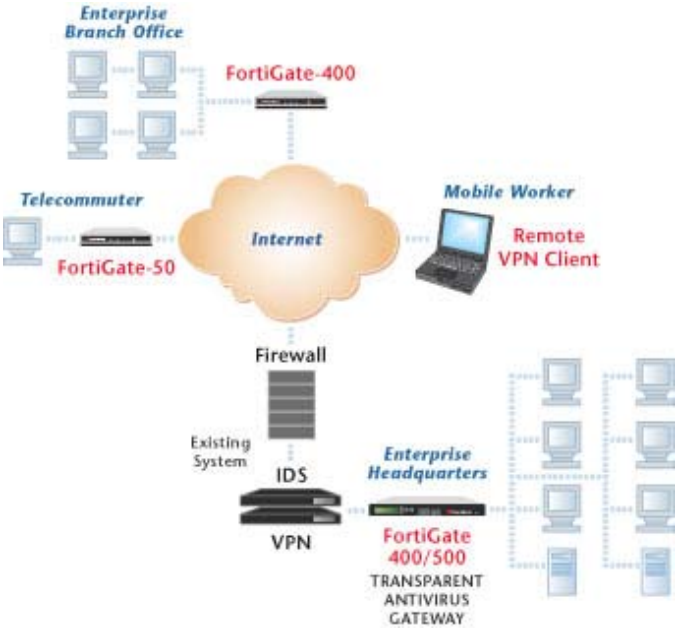
The answer, which may be surprising, is antivirus products that scan for non-threats actually can do much more harm than good compared with those that only scan for real threats, for several reasons:

1. Scanning for zoo viruses increases the size of the virus database by a factor of nearly 100. This means that it takes 100 times as much memory to store the database, and 100 times as much bandwidth to update the database (or else 100 times longer to update the database using the same bandwidth) compared with a WildList virus database. As attacks spread more and more rapidly, the time-to-protection – i.e., the time between when a threat is unleashed and when a new virus signature is loaded on the antivirus system – is increasingly critical. Those products that conserve space and bandwidth by only scanning for real threats can provide faster time-to-protection and better limit the spread of new attacks.

2. Scanning files and other content for zoo viruses requires much more computing power than scanning just for WildList viruses, and contributes to the relatively low performance of virus scanning software when deployed on standard computing platforms. The delays caused by low antivirus scanning performance may lead to dangerous and costly behaviors: Users routinely disable antivirus software if they find that it causes noticeable delays. Low performance is also the primary reason cited by the many organizations that do not scan their real-time Web traffic for viruses and other content-based threats. The slow performance of antivirus software adds too much delay to Web interactions, and so unprotected users are completely vulnerable to the numerous attacks that are carried in JavaScript, ActiveX, Web downloads, Web based mail, and many other applications delivered via the Web (versus traditional email). In fact, many users who fault their email-based antivirus systems for allowing virus attacks are in fact initially infected from Web-based traffic, which completely bypasses email-based antivirus software.
3. The need to maintain backward-compatibility of their scanning engines with the thousands of zoo viruses limits innovation by incumbent antivirus vendors. It also erects unnecessary barriers to new market entrants and impedes significant advances in the antivirus industry.

Before the advent of the Web and the rise of real-time applications, the delays imposed by virus scanning were not always noticeable to the user. For example, if an email message required an extra 30 seconds to be scanned at the mail server before being posted to a user's inbox, the delay was not visible to the user. However, delays in real-time applications, like Web applications, are immediately visible to the user, and thus the relative lack of concern with antivirus screening performance is no longer acceptable. By trading performance for the illusion of added protection that is thought to come by scanning for zoo viruses, organizations put themselves at risk to damage from the real threats, which are today's sophisticated, fast-spreading, in-the-wild attacks.

Toward a New Paradigm in Virus Protection



Fortinet has pioneered a new, network-based virus protection system that takes full advantage of a unique architectural approach to processing application-layer content in the network rather than on host computers. Intended as a complement to host-based antivirus software, Fortinet's ASIC-powered FortiGate™ Antivirus Firewalls can scan traffic at the network edge for viruses, worms and Trojans in real time, without introducing unacceptable network delays as is common with software-based antivirus systems.

By creating the world's first ICSA-certified, ASIC-powered antivirus systems and concentrating on scanning for WildList viruses (including the Main and Supplemental Lists, in addition to all attacks discovered between monthly WildList updates) Fortinet's systems are as much as 10 times faster than conventional systems and deliver up to 25 times the performance per dollar. Fortinet's Global Threat Response Team and FortiProtect™ Network can update every FortiGate system worldwide with updated virus and intrusion attack signature databases in less than five minutes, which is often difficult or impossible to achieve for antivirus software executing on host PCs and servers that sit behind corporate firewalls.

FortiGate systems are hardened network security platforms rather than general computing systems, and are therefore themselves immune from infection and inherently more secure. They are routinely deployed to eliminate content-based threats from Web traffic as well as for email and file transfers, providing a critical layer of edge virus protection with no performance penalty.

Conclusion

The true nature of the worldwide virus threat does not match the current product architectures (or marketing hype) offered by many antivirus software companies. Motivated by a desire to limit competition, incumbent antivirus vendors have exaggerated the nature of the virus threat, claiming the existence of tens of thousands of infectious attacks while their leading researchers routinely report only a few hundred active attacks. Today's real-time networking environment demands real-time antivirus protection, and an essential requirement of a real-time antivirus system is to focus on detecting and eliminating threats that actually exist, rather than trying to build a case for dealing with attacks that may have existed in the past or were never let loose in the wild. Fortinet's FortiGate Antivirus Firewalls provide real-time protection against genuine virus threats, and deliver the highest performance and value by ignoring illegitimate threats, i.e., they deliver more protection with less delay, less waste and less cost.

About Joe Wells

Joe Wells has devoted his career to the advancement of antivirus technology and industry cooperation. He developed his first antivirus technology, a virus/Trojan detector, in 1988. Since then, he has made numerous technical contributions to the industry in development roles with Certus International, Symantec's Peter Norton Group, IBM's Thomas J. Watson Research Center, Cybersoft, and as CEO and chairman of Wells Antivirus Research Laboratory, Inc. (WarLab), a subsidiary of Trend Micro. Mr. Wells has authored over 50 technical articles and scientific papers in the field of virus research. Mr. Wells is best known as the founder of the WildList Organization International (WLO), the single largest cooperative project in the antivirus world.

For More Information

Please visit our web site at www.fortinet.com or email us at info@fortinet.com