IDC
Analyze the Future

I D C V E N D O R S P O T L I G H T

Beyond Signature-Based Antivirus: New Threat Vectors Drive Need for Proactive Antimalware Protection

July 2007

Adapted from *Worldwide Antivirus 2006–2010 Forecast Update and 2005 Vendor Analysis* by Brian E. Burke, IDC #204715

Sponsored by ESET

Trojans, viruses, worms, and other types of malicious code continue to be the most serious threats facing corporations today. Organizations are increasingly asking for more proactive virus-detection techniques because of the rising number and severity of threats entering corporate networks. Forward-looking companies are beginning to realize they cannot rely upon reactive signature-based antivirus (AV) technology alone. Real-time behavior analysis AV technologies, using heuristic algorithms, are needed to complement signature-based AV. This Vendor Spotlight examines the rapidly evolving threat environment and the inadequacy of signature-based-only AV in addressing unknown threats. The paper also looks at advanced AV technology that can protect companies from more than just viruses and discusses the role of ESET in this vitally important segment of the security market.

The New Threat Vector

The volume and sophistication of malicious code (also known as malware), whether viruses, worms, or spyware, are increasing, and organizations are struggling to defend themselves. The threat environment has evolved from a mischievous hobby to a money-making criminal venture that has attracted a new breed of sophisticated hackers and organized crime.

The sophisticated hackers of today are less concerned with destroying systems and knocking out Web servers. They realize that they can gain money from stealing confidential personal information and corporate data and selling it to spammers or those involved in organized crime and fraud. This profit-driven motivation is causing the number of attacks to increase in sophistication, frequency, and severity.

The digital threat environment is rapidly changing not only in the motives of malware writers but also in the vulnerabilities they are targeting. At one time, email-borne viruses were the most attractive weapon of hackers who sought to damage or disrupt business operations. However, there's a larger threat vector of malware attack — the Web.

As many organizations are reasonably protected against traditional email-borne malware, the Web channel has become an alternative target for hackers who exploit multiple vulnerabilities in Web browsers and other applications to launch various types of malware attacks, which in most cases are motivated by financial gain.

Web-based threats can propagate automatically through "drive-by" downloads (an infected Web page can exploit a site visitor's computer without the visitor even having to click on anything located on that page), an email message downloaded from a Web-based mailbox, and other similar techniques. The growing prevalence of Web-based threats that effectively apply these techniques is one of the main reasons for the recent surge in spyware, viruses, worms, keyloggers, and other malware.

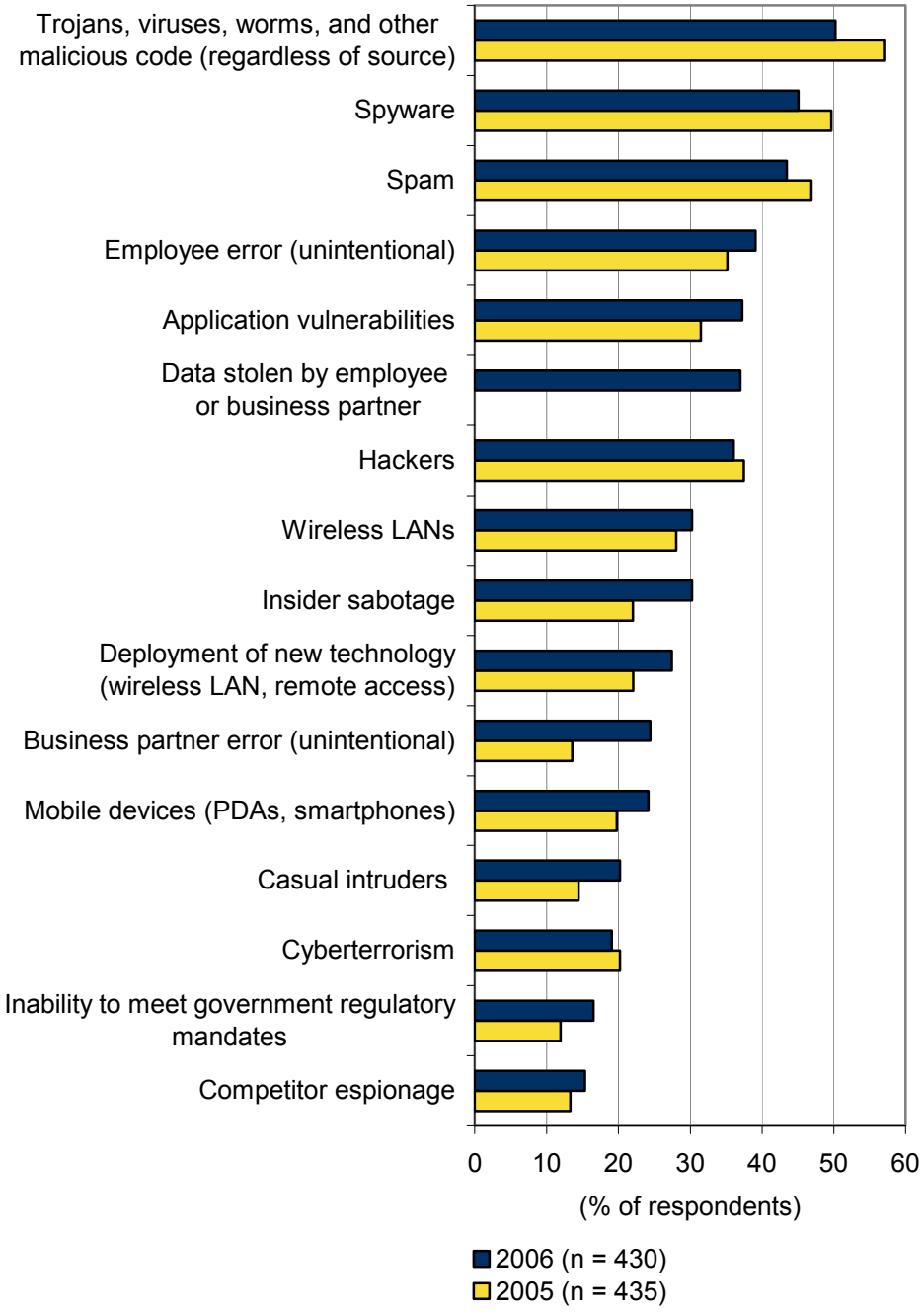
Web-based attacks often employ sophisticated techniques to carry out targeted attacks to steal money, identities, or confidential information. For example, keyloggers, when present on a PC, are able to capture and transmit a user's every keystroke, thereby allowing thieves to get passwords and other identity-related information. Rootkits are installed with malware to hide the presence of the malicious code from users, administrators, and security software.

Web-based attacks are also constantly growing in sophistication. For example, a technique employed with Web-based threats is the use of encryption by hackers to hide malicious code to evade detection by traditional URL filtering and antivirus solutions that are unable to decode it. The use of Web-based attacks is one of the drivers for the recent surge in spyware, which is evidenced by the dramatic increase in the number of Web sites distributing spyware.

According to IDC demand-side research, viruses and other malware continue to dominate the threat scene for enterprises of all sizes (see Figure 1); spyware is the number 2 threat. Zero-day attacks that exploit vulnerabilities for which there is no patch or signature enable both high-profile, worldwide epidemics and covert targeted attacks against businesses. Thus far, it has been very difficult to contain the drain on resources, both staffing and financial, created by fighting viruses, worms, and trojans.

Figure 1

Top Threats to Enterprise Network Security: 2005 and 2006 Survey Results



Notes:

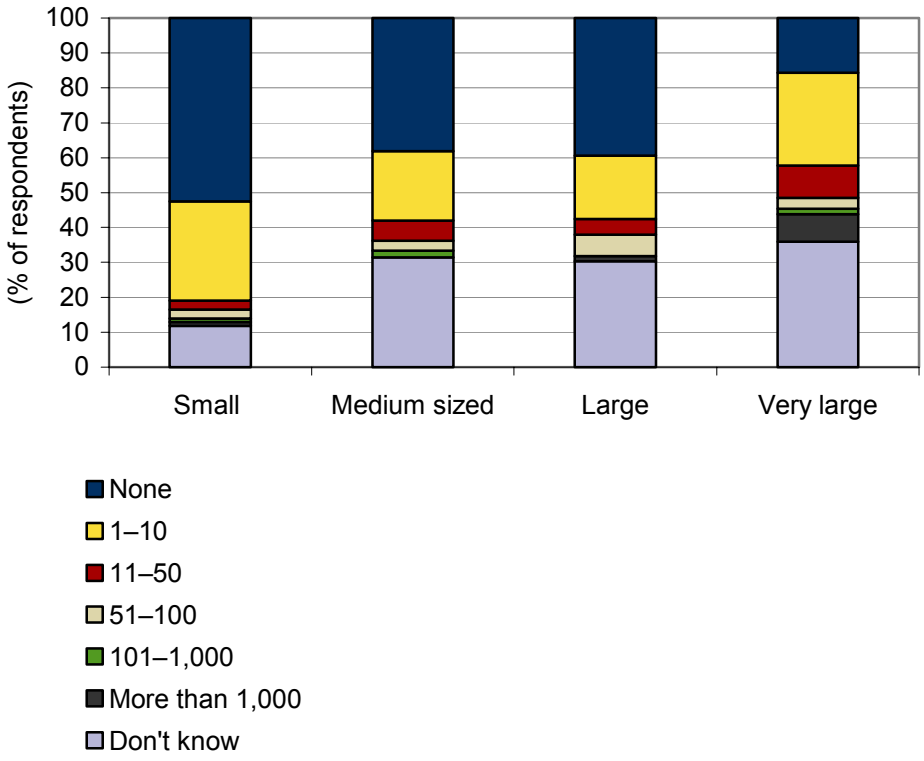
- Values represent those respondents who answered 4 or 5 on a scale of 1–5, where 5 = a significant threat.
- Multiple responses were allowed.
- Casual intruders don't fall under the definitions of competitors, cyberterrorists, employees, or partners.

Source: IDC's *Enterprise Security Survey*, 2005 and 2006

In a corollary survey, 35% of respondents reported successful attacks against their enterprise, while 24% reported 10 or fewer successful attacks (see Figure 2). Additionally, 27% of respondents from very large companies stated that they had 10 or fewer successful attacks on their enterprise.

Figure 2

Number of Successful Attacks in the Past 12 Months by Company Size



n = 430

Note: Small companies are those with 1–99 employees, medium-sized companies are those with 100–999 employees, large companies are those with 1,000–9,999 employees, and very large companies are those with 10,000+ employees.

Source: IDC, 2007

The clear message from Figure 2 is the overwhelming prevalence of at least one successful attack on the enterprise during the past 12 months. Obviously, even 1,000 foiled attempts won't make up for the single breach that costs an enterprise its business.

In light of the growing concerns over Web-based threats, demand is rising for solutions such as Web filtering, Web intrusion prevention, Web antivirus, and Web antispyware. However, the growing sophistication of Web-based threats emphasizes the need for real-time, proactive security to complement traditional security solutions based on developing a signature for each new identified known threat. Many of today's malware attacks are designed to evade these traditional signature-based solutions by applying encryption, polymorphism (each sample looks different) fast-propagation techniques, blended malware, and other approaches to infect a large number of PCs before signatures are ready.

Therefore, to effectively protect against emerging Web-based threats, organizations need antimalware technology that complements existing reactive security solutions — which are still critical in protecting against known threats. Signature-based technology remains important because some of the threats that have had signatures developed in the past are still in the wild and remain dormant until a predetermined or accidental event relaunches an attack.

Signature-Based Versus Heuristic-Based Antimalware

As noted previously, demand for more proactive virus-detection technologies has been heightened due to Web-based threats that have escaped traditional, signature-based virus protection. This problem is primarily due to the fact that the viruses are "unknown" or that enterprises have failed to update signature files.

Unlike traditional viruses, which rely on the user to spread the infected files, these new, "blended" threats are automated. Compromised computers in homes and businesses are always scanning the Internet and local networks for other vulnerable computers to infect — meaning they spread without user interaction. The prolific speed at which malware spreads today is due to its ability to often sneak past traditional antivirus software and entrench itself in desktop and server systems before antivirus vendors can post an appropriate signature.

Since blended threats are designed to get past point-solution security systems, IDC believes there will be a strong push toward a "layered security" approach, which will be better able to combat blended threats. Proactive, behavior-based analysis employing heuristics is increasingly becoming a vital need in layered security architecture.

Similarly, Web sites rely on various embedded programs such as Java and ActiveX controls to create their unique look and feel. These programs can run automatically when the site is viewed by the user, allowing a virus to be embedded on a Web page and infect a user viewing that particular page. Many companies block Java from coming through their firewalls, but, unfortunately, this move can restrict important and legitimate business-related applets.

Real-time behavior analysis using advanced heuristics identifies and analyzes downloaded code as it enters the network. All characteristics of the code are examined for security violations on the fly. Any code that violates the corporate security policies is logged and blocked at the gateway, while end users are notified with an on-screen alert. Examples of security policy violations include attempts to delete files, open network connections, and alter registry settings.

Real-time behavior analysis enables companies to allow trusted Web applications or services into the corporate network and to scan all other Web content for malicious behavior. This approach permits trusted content to flow freely into the network, while all other "unknown" content is checked before it can proceed.

Considering ESET

ESET, a 17-year-old company with U.S. headquarters in San Diego, California, is a global provider of security software for enterprises and consumers. The company's flagship product is NOD32, an antivirus software system that provides real-time protection from known and unknown viruses, spyware, rootkits, and other malware.

NOD32 offers fast, advanced protection with small resource-utilization impact. It has garnered more Virus Bulletin 100 Awards than any other antivirus product. NOD32 is positioned as more than an antivirus product, however — it's designed to be a unified AntiThreat™ system that protects against viruses, spyware, adware, trojans, worms, rootkits, and phishing attacks.

NOD32 offers protection against threats from multiple vectors using the following modules:

- **Antivirus MONitor (AMON)** — an on-access (memory-resident) scanner, which automatically scans files before they're accessed
- **NOD32** — an on-demand scanner, which can be run manually on specific files or disk segments and can also be scheduled to run during off-peak times
- **Internet MONitor (IMON)** — a memory-resident scanner that runs on the Winsock level to prevent infected files from reaching the computer's disks and scans Internet Web browsing traffic (HTTP) and incoming email via the POP3 protocol
- **Email MONitor (EMON)** — an auxiliary module for scanning incoming/outgoing emails via the MAPI interface, such as Microsoft Outlook as well as Microsoft Exchange Extension–compliant mail clients
- **Document MONitor (DMON)** — a module that utilizes the proprietary Microsoft API for scanning Microsoft Office documents (including Internet Explorer)

At the heart of the NOD32 system is ESET's proactive ThreatSense™ technology, which reportedly stops 93% of zero-day threats before they're even released. The optimized engine delivers superior detection and fast scanning with minimal performance impact.

Written mostly in assembly language, NOD32 has won numerous awards for the fastest performance of any antivirus application. NOD32 is up to 34 times faster than rival products, according to the independent Virus Bulletin.

NOD32 is also designed to conserve resources in memory and on disk, leaving more for business-critical applications. The installer is only 11MB, and the application consumes an average 23MB in memory (this fluctuates with changes to the detection technology). ThreatSense updates, which include advanced heuristics logic and signatures, are usually between 20KB and 50KB.

NOD32 is also flexible and configurable, with centralized management and reporting functionality. Businesses and organizations with larger, distributed networks can use the Remote Administrator to centrally deploy, install, monitor, and manage thousands of NOD32 workstations and servers. The broad product platform protects Windows, Linux, Novell, and MS DOS machines.

Challenges and Opportunities

With NOD32 and its real-time behavior analysis capabilities, ESET has made a bold move in tackling the complex challenges inherent in proactive security. The overwhelming majority of organizations IDC speaks with agree that more proactive security solutions are needed to combat the speed at which new threats can spread. These companies simply cannot afford to wait for signatures to be generated.

IDC believes that the biggest challenge facing ESET is that antivirus is the most widely deployed set of security technologies across organizations of all sizes. There are very few "green fields" available for ESET to sell into. The deployment of NOD32 at the desktop level necessitates the displacement of an existing antivirus solution — a task many organizations have historically been reluctant to undertake.

ESET must continue to educate organizations that protecting the enterprise today is much more complex than traditional signature-based antivirus can manage. With the increasing sophistication of today's threat environment, and the rapid-fire "zero-day" infections occurring across the Internet, enterprises are struggling to keep up with the endless assaults on their networks.

It's IDC's opinion that behavioral-analysis tools are an excellent way for enterprises to address certain aspects of proactive security strategy. However, we strongly recommend that behavioral analysis be implemented as part of a holistic security approach. A proactive approach must be considered as a complement to traditional reactive security approaches.

Conclusion

IDC believes that the AV market will continue its evolution from product to suite and will ultimately shift toward more comprehensive security solutions. We further believe that AV will be increasingly sold as a feature of endpoint security, messaging security, Web security, and network security solutions. For example, it's clear that antivirus and antispyware have already converged into a single solution on the endpoint.

IDC demand-side survey results clearly show that organizations want fewer agents on the client. Additionally, organizations want to be able to manage endpoint security with a single console for consolidated administration, policy, and reporting. IDC believes that the integration of real-time behavior analysis technologies, such as advanced heuristics, with traditional signature-based antivirus technologies will allow for a greater degree of accuracy in detecting both known and unknown threats.

IDC forecasts the worldwide antivirus market to grow from $4.3 billion in 2005 to $7.3 billion in 2010, representing an 11% compound annual growth rate. To the extent that ESET can address the challenges described in this paper, the company has a significant opportunity for continued success as it strengthens the antivirus layer with enhanced behavioral protection and adds firewall and antispam protection to create a unified antithreat security suite.
