TECHNICAL BRIEF: SYMANTEC SECURITY RESPONSE

Handling Today's Tough Security Threats

Mimi Hoang, Group Product Manager,
Symantec Security Response

Technical Brief: Symantec Security Response

Handling Today's Tough Security Threats

Contents

Contents *(cont'd)*

Introduction

The current Internet security threat environment continues to be dominated by lower profile, targeted attacks as cybercriminals identify new ways to steal information or provide remote access to user systems. But the motivation for today's attacks has shifted. Criminals no longer want notoriety—they want financial gain. These criminally motivated attacks have more impact on businesses and their customers than the previous generation of digital vandalism and reckless hacking. Attackers now design threats that can infect, expand, and function undetected by security software. The intent is to gain unauthorized access, which threatens a company's intellectual property and a user's identity. Even when they're detected, these threats tenaciously resist removal.

The evolving threat environment has caused a corresponding shift in market reaction. Companies must deal effectively with threats that utilize evasion, stealth, and aggressive behavior. Previously, security vendors' responses to large-scale threats were measured almost solely in terms of speed—and during these tests nearly all vendors would provide protection within hours, if not minutes, of one another. But measuring vendors' effectiveness against this new breed of stealthy, resilient threats is a different game as they strain against the technology and expertise of security solution providers. Instead of measuring responses in hours and minutes (and without a nod to quality or completeness) it can take anywhere from days to weeks (or even years) before some security solutions are able to handle the "tough" threats. Meanwhile, organizations can be left vulnerable to aggressive attacks.

We can define a "tough threat" in the following ways:

- It is actively seen "in the wild" and is affecting users.
- It shows increasing volume and prevalence based on the threat landscape.
- It poses a major risk or impact to organizations and home users.
- It requires ongoing innovative technology, strong operational processes, and skilled professionals to effectively handle the threat category.

This technology brief covers four types of threats and risks that meet the "tough threat" criteria:

- Polymorphics
- Rootkits
- Advanced evasion techniques
- Zero Day attacks

We will take a closer look at what makes these threats so complex, how they affect organizations that do not have appropriate protection, and finally, how Symantec is best positioned to fight not just one category of tough threat, but all of them.

Polymorphics

What are they?

A polymorphic virus can change its byte pattern when it replicates and is able to avoid detection from simple string-scanning antivirus techniques. Polymorphic code was the first to pose a serious challenge to virus scanners, since no part of it stays the same on each infection, making detection difficult.

The first known polymorphic virus, 1260, was written in the United States by Mark Washburn in 1990. Virus scanners were challenged by 1260 because simple search strings could no longer be extracted from the code.[1]

The next important development in the history of polymorphic viruses was MtE, a mutation engine written by the Bulgarian Dark Avenger. The first version of MtE was released during the summer of 1991, with another version in early 1992, making them widely available for use by other virus authors—as if they were do-it-yourself kits[2].

Trends

According to the Internet Security Threat Report (ISTR)[3] X, polymorphic and self-mutating viruses appear to be enjoying renewed popularity. Over the past several years, authors have been developing increasingly sophisticated malicious code that employs these techniques. However, because these techniques are difficult to implement, malicious-code authors have focused their efforts on developing run-time packers as a means of mass propagation,[4] as opposed to sophisticated malicious code that avoids detection.

With the success of large-scale worms such as Nimda and Code Red and viruses like I Love You, it soon became apparent that malicious code did need not to be sophisticated to infect a large number of machines. Today, there is an increased focus on targeted attacks and more subtle infection methods. As a result, attackers are using polymorphic techniques more and more to avoid detection and aid in propagation.

Improved unpacking support has reduced the effectiveness of using run-time packers to obfuscate malicious code. As a result, malicious-code authors have been forced to employ different means to prevent detection of their code while it is infecting host systems. This may be the main factor in the emergence of the polymorphic malicious code activity that has been observed by Symantec.

1 Peter Szor, *The Art of Computer Virus Research and Defense*, Addison-Wesley, 2005
2 Peter Szor, *The Art of Computer Virus Research and Defense*, Addison-Wesley, 2005
3 ISTR X is Symantec's latest version of the *Internet Security Threat Report*, which provides a comprehensive analysis of Internet security activities and trends every 6 months.
4 Run-time packers are compression routines that allow an executable file to run even though they are compressed.

Because it is so difficult to detect and remove polymorphic viruses, Symantec speculates that more malicious-code authors may begin to use polymorphic techniques at all levels of development. For enterprises, this could result in increased volumes of targeted malicious code from which they have limited protection. Should more malicious code be released using these techniques, targeted organizations may be increasingly at risk because obtaining samples to develop detection signatures will likely be difficult.

Impact

Polymorphics stretch the limits of detection capabilities of antivirus engines, and in many instances go beyond the capabilities of some vendors' solutions. This threat category becomes a differentiator among security vendors—it takes a sophisticated level of emulation and processing capabilities for a virus engine to deal effectively with complex polymorphic threats. In many instances, some security vendors are forced to update their engines before they are able to respond at all. In other instances, code emulation (temporarily freezing the system to examine whether a file is indeed a polymorphic virus) can be unacceptably time consuming, especially if the virus is very complex. As a result, security vendors may not be able to handle every polymorphic threat.

More recent polymorphic threats such as W32.Bacalid are taking polymorphics one step further by using a blended technique that couples file infection capabilities with backdoor or downloader capabilities. This blended technique not only tries to evade detection and bury itself in a system, but also it is able to spread from system to system. Once on a system, the polymorphic can download other stand-alone Trojan horses or other malicious code, or gather sensitive information. The longer a polymorphic can evade scanners or detection, the more time it has to harm a system.

Protection requirements

Polymorphic viruses can change themselves each time they infect a file. Since the fingerprint for polymorphic viruses changes each time, standard methods of detection can't be used. Therefore, the "one detection cure for all" solution is not good enough. Security products require a powerful engine that is designed to use more sophisticated methods for detection—and this is where differentiation among the major security vendors becomes evident.

The testing of security products against polymorphic threats is the most rigorous in the antivirus (AV) community—and one of the most closely watched. The best way to measure the detection strength of an antivirus product is to test it against polymorphic threats. Such a test stresses the underlying power of the engine itself rather than the number of signatures in the database. Being the first to detect a variant of a polymorphic is not an accurate metric on its own for determining effective coverage; with polymorphics the metric needs to address which security vendor has complete detection coverage first. Missing even one variant could mean reinfection by the threat.

The Symantec solution

It is also worthwhile to look at how security vendors handle the general masses of polymorphics. The following chart shows results from the February 2006 polymorphic comparative test from www.AV-Comparatives.org. This organization performs regular, standardized detection tests of all major AV vendors. It is the "gold standard" of comparative tests. This particular test includes the ten most complex polymorphic viruses, which are the most difficult to detect. Symantec was the only vendor to receive 100 percent coverage with on-demand detection of polymorphic viruses.

As can be seen from the data in Figure 1, Symantec is the leader among major security vendors when it comes to detecting polymorphic threats. Customers can use Symantec security products with confidence, knowing that they have employed the most powerful detection capabilities in the industry.

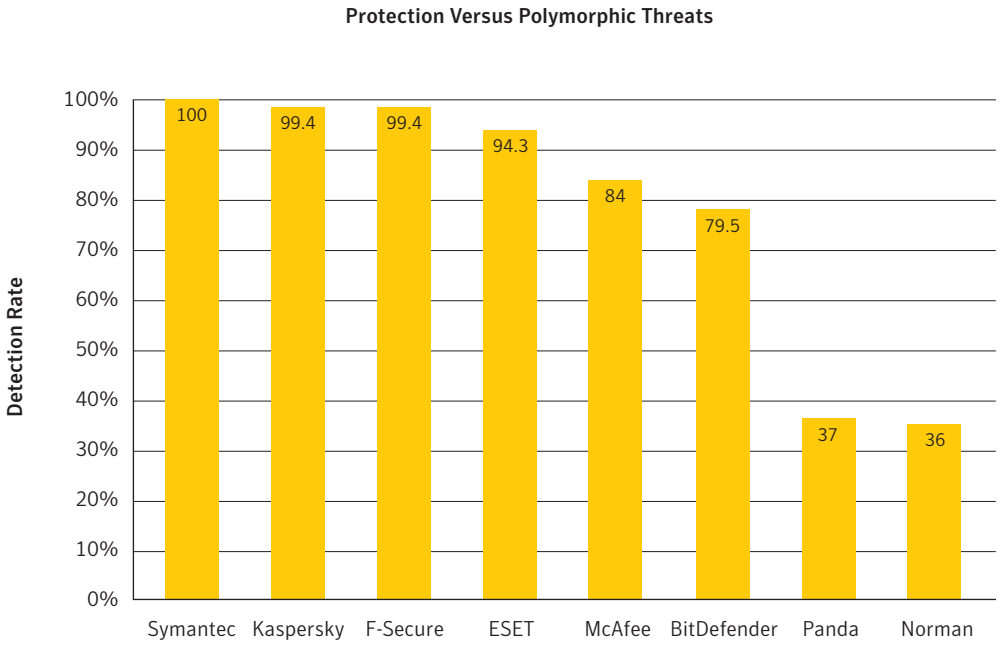

Figure 1. Andreas Clementi's Anti-Virus Comparative No. 9 (February 2006)
Source: AV-Comparatives.org

In the most recent industry test, Anti-Virus Comparative No. 11 (August 2006), thousands of variants were tested for 10 highly complex polymorphic viruses. This test evaluates the quality of the detection routines for polymorphic viruses. These 10 viruses and their variants have been known in the industry for some time; in fact, some of them were also used in the February 2006 test. Even though some of the polymorphic threats have been in existence for years, some security vendors today are still unable to handle them. Symantec's initial detection of a polymorphic named Zmist was released on January 18, 2001, yet more than half of the participating vendors in the August 2006 review were unable to achieve a passing score. While many vendors could not fully detect many of the complex polymorphic viruses, Symantec scored 100 percent across the board.[5]

This high order of achievement comes from longstanding experience and a history of innovative security technology developed to fight polymorphic threats. Of the earlier and critical patents, 5,964,889 and 5,999,723 were granted by the U.S. Patent and Trademark Office to Symantec on January 18, 2000, for technology that detects complex self-mutating or polymorphic viruses.[6] To date, Symantec has accumulated more than 15 issued antivirus patents and has more than 50 patent applications pending.

[5] Find "Anti-VIrus Comparative No. 11" at www.av-comparatives.org/seiten/ergebnisse/report11.pdf.
[6] Symantec news release, www.symantec.com/security_response/writeup.jsp?docid=2005-122917-3955-99

Rootkits

What are they?

The term *rootkit* can take on two very different connotations depending on the intent of the user. Originally, UNIX administrators used *rootkit* to refer to a set of modified administrative tools that hid legitimately running processes and applications from users. But when used maliciously, attackers can leverage a rootkit's functionality to conceal their presence and actions on a system. Stealth techniques may be used in mainstream programs for legitimate purposes, especially in cases with user knowledge and consent. Symantec classifies these programs as a security risk or a potentially unwanted application.

For purposes of this brief, Symantec defines *rootkit* as a component that uses stealth to maintain an undetectable presence on the machine. Actions performed by a rootkit, such as installation and any form of code execution, are done without end user consent or knowledge. Rootkits can be categorized into two general classes based on the modes that they target:

- **User mode** rootkits involve system hooking in the user or application space. Whenever an application makes a system call, the execution of that system call follows a predetermined path and a Microsoft® Windows® based rootkit can hijack the system call at many points along that path. User mode rootkits are more popular because they are easy to create and install.

  For example, EliteBar redirects search requests, modifies internet settings, deletes previously installed toolbars, and displays numerous advertisements. EliteBar uses user-mode rootkit techniques to hide its files, directory, and registry keys. By injecting its code into other processes' memory spaces and hooking various application program interfaces (APIs), EliteBar hides itself from Windows Explorer and the process list in Task Manager.[7]

- **Kernel mode** rootkits involve system hooking or modification in kernel space, which is generally off-limits to standard authorized (or unauthorized) users. A user must have the appropriate rights in order to view or modify kernel memory. A kernel mode rootkit is one of the most advanced because it operates at the lowest level and thus is the most reliable and robust method of system hooking.

  For example, CommonName is an adware application that displays advertisements based on keywords in search engines. CommonName uses the kernel mode driver to prevent its files and registry keys from being deleted and also hides its processes, registry subkeys, and files.[8]

[7] See www.symantec.com/security_response/writeup.jsp?docid=2005-083109-1455-99
[8] See www.symantec.com/security_response/writeup.jsp?docid=2003-080115-0233-99

Trends

Because rootkits are difficult to write, many variants are created from existing rootkits or proofs of concept. Because open source and ready-to-use rootkit applications are widely available on the Internet, malicious-code authors do not need to understand how they work in order to employ them. We can expect to see an increase in the use of rootkits for these reasons.

ISTR X lists Bomka as the second most common new malicious code family reported between January 1 and June 30, 2006. Bomka uses rootkit techniques to obscure its presence.[9] This Trojan horse is downloaded from a link that is included in spam email sent by another Trojan horse program named Spamlia.[10] The email uses social engineering techniques to convince its recipients that the link is the download location for a video clip. Bomka also allows a remote attacker to gain full access to the compromised computer by including a backdoor server component. This could result in the exposure of confidential information. This threat attempts to generate revenue for the attacker by installing a Trojan horse named Adclicker on the infected computer.

Impact

Kernel and user mode rootkits typically hide their files by preventing enumeration of files/directories or by preventing access to files.

Rootkits can provide the attacker with a back door for future attacks, launch and hide other malicious applications, and gather sensitive data. Often, this consists of personal information that can be used for identity theft or fraud. For enterprises, rootkits could be used to gain unauthorized access to privileged, proprietary information, thereby threatening the intellectual property of the organization.

With the widespread adoption of the Microsoft Windows environment, attackers have a large installed base on which to propagate rootkits for malicious use. Rootkit technology has evolved to take advantage of Windows-based functionality, such as hooking and concealment of files, processes, registry keys, and other objects. Once established, rootkit techniques quickly spread beyond malware alone. Modern-day threats (spyware, adware, and other unwanted applications) are now leveraging similar stealth techniques to hide their existence from security solutions in hopes of generating continued income.

[9] See www.symantec.com/security_response/writeup.jsp?docid=2006-012514-0250-99
[10] See www.symantec.com/security_response/writeup.jsp?docid=2005-122917-3955-99

There is ongoing debate about exactly what qualifies as a rootkit. This debate became more visible on October 31, 2005, with Mark Russinovich's findings on Sony BMG's copy protection software, Extended Copy Protection (XCP), for compact discs. XCP's cloaking technique was designed to prevent users from making illegal copies of music files. While Sony can legally use XCP to control how the music CD is used, the manner in which it was installed, the naming of the running process, and how it was implemented were all cause for concern. Perhaps most seriously, the XCP software introduced a vulnerability because it could be leveraged easily to hide any file processes, folders, or registry subkeys that start with "sys". Malicious code appeared on November 10, 2005, making it possible for malware to be installed, invisible to users.[11]

Protection requirements

A security program needs to be able to identify, detect, and remove rootkits without compromising system integrity. Additionally, the security program should also accurately categorize and provide recommendations to the user about the presence of any rootkits or hidden objects. Without this level of detail, an ordinary user would not be able to decide what to do with the files in question. Furthermore, corporate systems can have legitimate uses for hiding files, such as IT hiding backup data directories to avoid accidental deletion. So, a security program should be able to tell the difference between rootkit files and files hidden for legitimate purposes.

The Symantec solution

The latest Symantec Eraser engine release in August 2006 integrates a Veritas™ technology, Veritas Mapping Service (VxMS). This is a user-mode component that directly accesses the raw NTFS[12] volume and bypasses the Windows File System APIs.

Remediation of a stealth or entrenched threat involves direct volume access because the Windows File System is designed to have exclusive access to the volume and direct modification is deemed unsafe while the system is running. To minimize this risk, volume modification is done via a Windows Native application that runs before much of the operating system has been initialized.

Symantec's Native application is designed to remove these stealth threats without harming system integrity. The threat's drivers, services, and other applications are stripped of their protection and exposed, allowing the threat to be cleaned up.

[11] See www.symantec.com/security_response/writeup.jsp?docid=2005-110615-2710-99
[12] New Technology File System is the standard file system for the Microsoft Windows NT® operating system and its descendants.

The impact of this integration is best demonstrated through a third-party analysis of the top security vendors. Thompson Cyber Security Labs was commissioned to run a competitive test (completed on September 13, 2006) evaluating each of the following competitors on their anti-rootkit capabilities:

- Norton AntiVirus™ 2007 from Symantec
- Webroot SpySweeper 5.0.7.1608
- Microsoft Windows Defender Beta 2
- Trend Micro PC-cillin Internet Security 2006 including TMAS
- Sunbelt CounterSpy 1.5.82
- McAfee Internet Security 2006 Version 10.0, build 10.0.27 dat ver 4843
- FSecure Internet Security Suite 2006

Thompson Cyber Security Labs randomly selected 20 rootkits and used their own samples for this test. Each product was allowed all the latest updates as of September 1, 2006. The testing assessed each competitor's ability in the following areas:

- **Detection:** The ability of the product to detect the presence of a rootkit after it is installed on a system. If a particular rootkit is not detected, it could be due to either engine limitations or missing detections for a particular version of the rootkit.
- **Remediation:** The ability of the product to remove the components so that the rootkit is no longer left running on the system, as well as the ability of the product to completely remove the side effects of a rootkit, including registry keys.

Symantec achieved the highest score in both detecting and removing rootkits (Figure 2). The next closest scores were SpySweeper and Fsecure, who tied with 9 out of 20 rootkit removals. Further details on the testing methodology can be found in Appendix A.

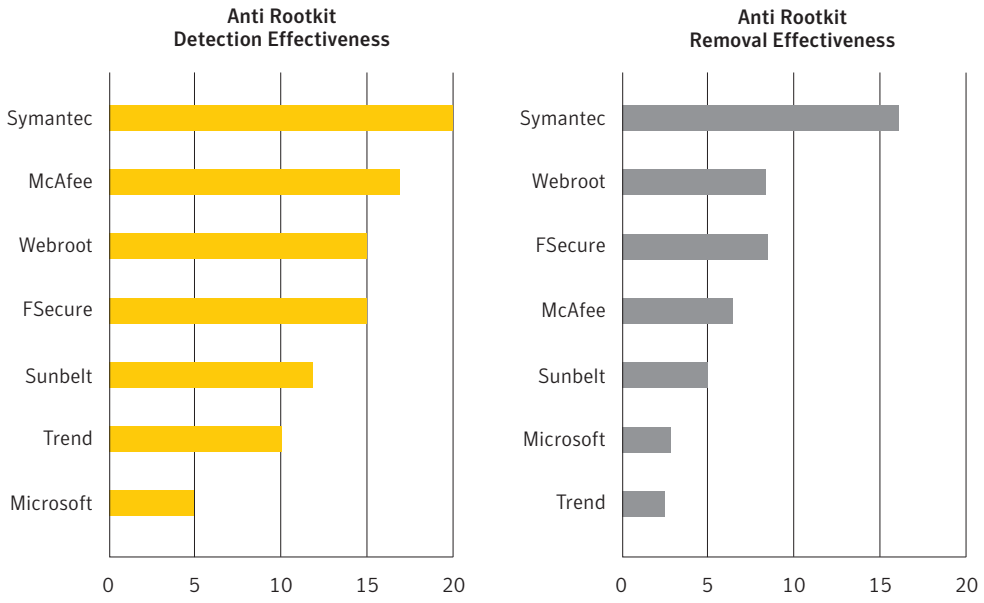

Figure 2. Results of AntiRootkit effectiveness testing
Source: Thompson Cyber Security Labs

Advanced evasion techniques

What are they?

Symantec uses the term *security risks* to refer to a number of programs, such as adware, spyware, misleading applications, and other programs, that users may not want on their systems. Different security risks implement different advanced evasion techniques to resist attempts to detect and/or remove them, which poses a risk to the confidentiality of the user's data. This section will describe some of the advanced evasion techniques that Symantec has observed over the first six months of 2006. It's important to note that, while these behaviors are common in spyware, they are also common in malware as well, where most of them originated long before spyware and adware became popular.

Some security risks inject their own code into processes running on the system to make themselves more difficult to remove. This can cause system instability, degrade performance, and breach system security. It may also allow the security risk program to run with the same permissions as the program into which it has been injected. This can make it very difficult for administrators or users to remove these programs manually, without specialized tools or in-depth knowledge. Of the top ten security risks observed during this period, only the adware program Aurora deployed process injection.

Run-time packers are programs used to evade detection and reduce the size of threats and risks. When packed, the programs are smaller and require less time to download. Run-time packers can also obfuscate the contents of a file, making it difficult for antivirus or antispyware programs to recognize them, unless the program understands the packer format. This technique is commonly used by creators of adware and spyware programs, and is a mainstay of malicious-code authors. For instance, the adware program Lop is dynamically repacked each time it is downloaded, making its detection and removal more difficult.

Watchdog processes are another technique used by security risks or threats to avoid removal. They use twin processes to monitor one another to defend a program against a removal attempt. If one process is stopped, the second process automatically restarts it, and vice versa. Of the top ten security risks reported during this period, the adware program Websearch uses watchdog processes to resist removal.

ISearch uses a slightly different advanced evasion technique. It hooks kernel mode APIs[13] to check whether the user is attempting to delete a file or registry key associated with it, and returns an "access denied" message, thus preventing removal of its components.

Some security risks use stealth techniques to hide from antivirus and antispyware scanners. Of the top ten security risks reported during this period, IEFeats uses a stealth technique whereby it hides part of itself in an alternate data stream. Alternate data streams were created by Microsoft to provide compatibility with Apple's HFS file system so that Macintosh files could be copied to Windows fileshares without being corrupted.[14] Alternate data streams are not typically scanned by many security products. Attackers can use a simple technique to create an alternate data stream to hide content of their choosing within otherwise innocuous files.[15]

[13] Kernel mode APIs are part of the Microsoft Win32 API. A detailed description of the Win32 API and of kernel mode is outside the scope of this report; however, suffice to say that these are low-level system calls associated with commands to delete files, which the security risk intercepts to prevent its deletion from the system.

[14] Alternate data streams were provided as part of the NTFS file system for Windows NT and later versions of Windows to provide compatibility with Apple's old Hierarchical File System (HFS). Files on HFS consist of a data fork, containing the contents of the file, and the resource fork, containing metadata, such as file type and other relevant details. A common problem when copying HFS files to the Windows FAT or FAT32 file system was that the resource fork information would be lost, thereby corrupting the file.

[15] More information on alternate data streams may be found at:
- www.symantec.com/avcenter/reference/ntfs.streams.a.primer.pdf
- www.securityfocus.com/infocus/1822

Trends

Security risks may implement different techniques to resist attempts to remove them from the user's computer. In the first six months of 2006, five of the top ten security risks employed various techniques to avoid removal from systems.

Additionally, the creators of security risks will often alter the characteristics of their program by updating it frequently in hopes of evading antispyware scanners. If a spyware or adware program is updated, some security programs may no longer be able to recognize the security risk and therefore may not be able to remove it. Table 1 lists the top ten most frequently updated security risks in the first half of 2006.

Risk name	Risk type	Updates per day
DialPlatform	Dialer	11.9
ZangoSearch	Adware	10.7
Aurora	Adware	8.3
Sfonditalia	Dialer	7.5
SpySheriff	Adware	6.2
Istbar	Adware	3.6
Lop	Adware	3.6
BetterInternet	Adware	2.9
SurfSideKick	Adware	2.9
DollarRevenue	Adware	2.7

Table 1. Top ten self-updating security risks
Source: Symantec Corporation

Impact

Security risks may pose a huge impact to an enterprise:

- **Privacy: corporate espionage**—Theft of personally identifiable information and company intellectual property, such as customer, employee, or patient files; user names and passwords; or Web browsing behavior. Implementation of new government regulations such as Sarbanes-Oxley, HIPAA, Gramm-Leach-Blilely, Basel II, and others require enterprises to comply in order to protect this kind of confidential information.
- **Performance utilization: network downtime**—Occupying unnecessary and extreme bandwidth that can slow down an enterprise's network, interfering with critical business needs. In addition, dealing with spyware, adware, and malware removal can be a drain on already taxed helpdesk resources.

- **Removal resistance: resource intensive**—Helpdesk and IT resources waste their time making sure that removing spyware and potentially unwanted applications does not prevent legitimate applications from working or does not disrupt system stability.
- **Stealth: hidden problems**—Programs may attempt to install themselves without the user noticing, and then remain hidden in order to prevent detection and removal. Enterprises may not even be aware that there is a problem, and their systems are left exposed.

Protection requirements

Security risks such as spyware, adware, and misleading applications are a complex problem that requires a multipronged approach in order to maximize the effectiveness of the solution. Effective antispyware solutions should have the following characteristics:

- **Breadth of detection.** Provide wide coverage for the prevalent security risks in the wild. This includes staying on top of those security risks that continually update themselves.
- **Thoroughness of removal.** Isolate and clean potentially unwanted programs from the infected machine while leaving the system in stable condition. The antispyware solution should avoid false positives and should not remove components shared between spyware/adware and legitimate, unassociated applications.
- **Proactive prevention capabilities.** Have strong remediation capabilities, especially the initial prevention of an unwanted program being downloaded and installed. This can save IT time and money previously spent on identifying and cleaning infected machines.

The Symantec solution

Symantec commissioned the German based TUEV Saarland (Tekit Consult Bonn) organization to test the effectiveness of antispyware tools from the following vendors:

- Norton Internet Security™ 2006 from Symantec[16]
- Sunbelt CounterSpy 2.0 Beta
- Webroot Spy Sweeper 4.5
- PC Tools Spyware Doctor 3.8
- McAfee Antispyware 2006
- Microsoft Windows Defender

[16] While this product was used for this test, other Symantec products also have these capabilities; Norton AntiVirus 2006 and above, Norton Internet Security 2005 AntiSpyware Edition and above versions, Symantec AntiVirus Corporate Edition 10.x and above versions, Symantec Client Security 3.x and above versions.

This test was conducted by AV-Test (Andreas Marx) under the supervision of TUEV Saarland. Fifty security risk samples were randomly chosen by AV-Test, comprising of the Top 10 lists of various antispyware vendors, including the vendors that were tested. The purpose was to demonstrate how each vendor handled the threats' antiremoval techniques. The latest signature updates for all products were run on June 26, 2006. All of the antispyware vendors included in this review have received the entire sample set used (installers and dropped files) to independently review the test results and improve their detections. For more specifics on which security risks were tested, along with the testing methodology, refer to Appendix B and www.tekit.de.

The results showed Symantec's leadership in the detection and removal of spyware, and adware and other security risk programs (Figure 3). The Symantec solution effectively discovers new security risks and is also able to stay on top of existing programs that continually and aggressively update themselves.

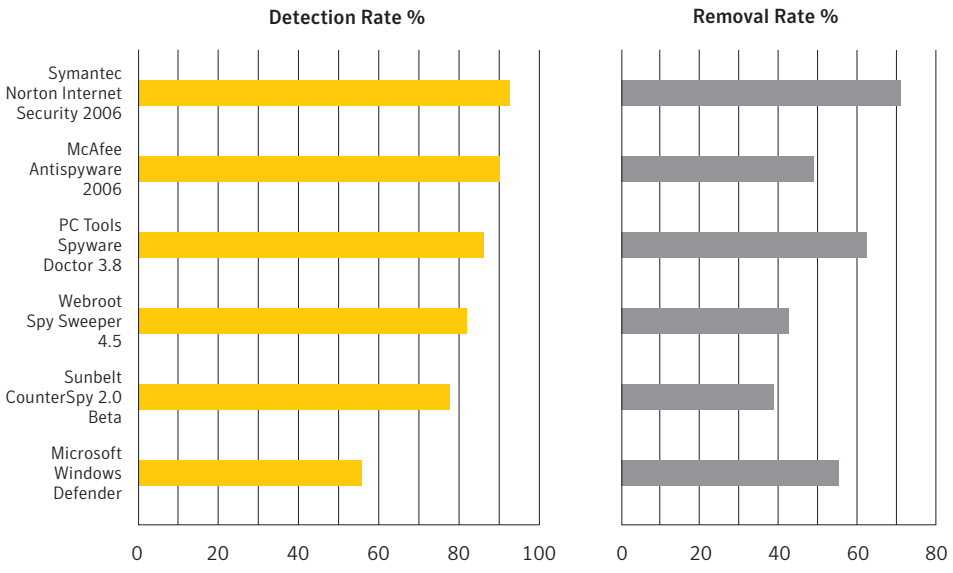

Figure 3. Results of antispyware effectiveness testing
Source: TUEV Saarland, August 2006

In addition, Ziff Davis issued a review of antispyware tools on December 5, 2005. The testing scenario rated how well each product could detect and clean up a range of malware for a large company (more than 150 users) as well as for a smaller company (fewer than 150 users). Symantec was named the winner for the larger company scenario and was the Editor's Choice for the smaller company scenario by "blitzing the field in detection, which is what you really want"[17] (see Figure 4).

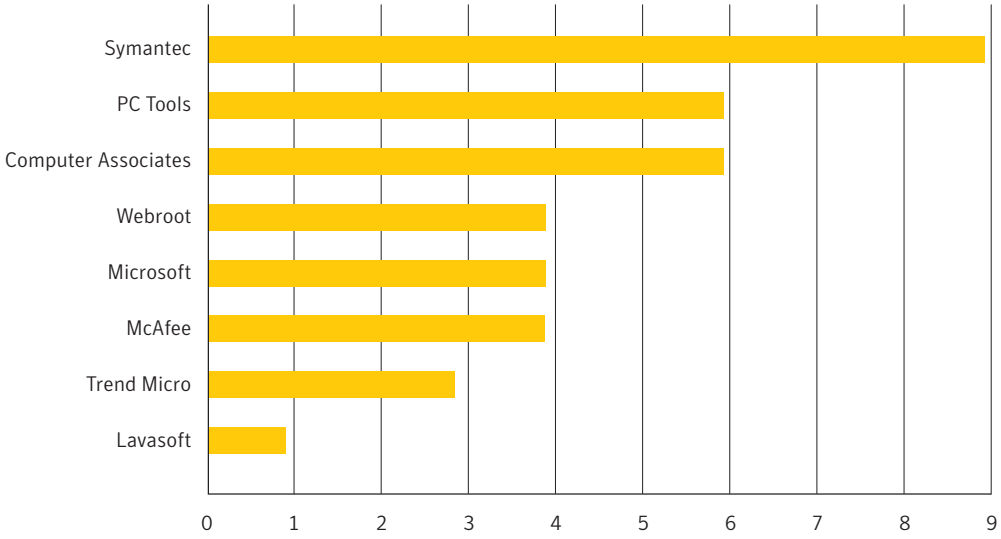

Figure 4. Review of antispyware tools
Source: Ziff Davis

While security risks are not categorized as malicious code, Symantec monitors them with many of the same methods. This involves an ongoing analysis of reports and data delivered from more than 120 million client, server, and gateway email systems deploying Symantec antivirus security solutions, as well as filtration of 25 million email messages per day by Symantec Brightmail AntiSpam™ antifraud filters. Symantec then compiles the most common reports and analyzes them to determine the appropriate categorization.

[17] Read "To catch a spy: Anti-spyware tools reviewed" at www.zdnet.com.au/reviews/software/security/soa/To_catch_a_spy_Eight_anti_spyware_tools_reviewed/0,39023452,39225147,00.htm.

Proactive prevention

To deliver strong protection, vendors must excel at the detection and removal of spyware on an infected machine, and must proactively prevent spyware, adware, and other security risks from being downloaded and executed on the system in the first place.

Security risks such as spyware and adware can be seen as an extension of the malware problem and should be included as part of any antivirus solution. Several Symantec solutions offer additional layers of proactive protection, including auto-protect capabilities, a personal firewall, intrusion prevention, and tamper protection to prevent spyware from getting onto the system.

- While running in the background, Symantec's Auto-Protect solution protects systems by scanning for viruses (including macro), boot sector viruses, memory resident viruses, Trojan horses, and worms. Auto-Protect is activated any time that the files are accessed (e.g., copied, moved, run, or opened) and will scan any files that are received from any sources, such as the Internet, removable disks, or email attachments. On Windows 2000/XP, it also scans for spyware, adware, and other security risks. If Auto-Protect detects suspicious activity, the spyware/adware program will be blocked and installation prevented.
- The firewall monitors all incoming and outgoing Internet traffic, blocking any suspicious activity (programs that are not on Symantec's white list) and alerting users to take action.
- Intrusion prevention signatures block spyware and adware programs from "phoning home" for possible binary updates; attempts to send, post, or upload information to the host server; and other communication transmissions back to the server, such as installation of additional applications or reporting the heartbeat of the installed program.
- Tamper protection provides real-time protection for Symantec applications. It prevents Symantec processes from being attacked and disabled by non-Symantec processes such as worms, Trojans, viruses, and security risks.

A good defense has to be layered; all four layers of Symantec's proactive protection work in collaboration to prevent spyware, adware, and other security risks from being installed on a user's system.

Zero Day attacks

What are they?

The absence of secure programming training in most organizations, as well as an influx of new development technologies and approaches such as AJAX, Ruby on Rails, and others, can lead to vulnerabilities in the resulting applications. Once a vulnerability is known, malicious-code authors can take advantage of this security hole by launching attacks before a patch is available or before administrators have time to test and deploy a patch. Of even greater concern are Zero Day attacks, where a software flaw is only discovered after it is already being exploited in the wild and there is no patch available from the vendor.

Given that new versions of software are typically "layered" on top of the previous version, vulnerabilities in earlier iterations are carried forward and may be buried deeper and deeper in a program. Consequently, there may be vulnerabilities that go unnoticed and lie hidden in programs for some time; for an attacker, this is like buried treasure waiting to be discovered and exploited. Taking Microsoft as an example, there are recent instances of vulnerabilities that affect their products from recent releases to as far back as Windows 98, with new vulnerabilities being reported on a monthly basis.

While vendors are steadily improving the development and release of software fixes to patch vulnerabilities discovered in their products, the reality is that, on average, attackers develop exploits against vulnerabilities faster than vendors can make a patch available for their customers. This leaves affected systems at risk and susceptible to attacks.

Trends

As shown in Figure 5, Symantec documented 2,249 new vulnerabilities in the first half of 2006. This is an increase of 18 percent over the 1,912 vulnerabilities that were documented in the second half of 2005. It is also a 20 percent increase over the 1,874 vulnerabilities reported in the first half of 2005. Symantec documented a higher volume of vulnerabilities in this reporting period than in any other previous six-month period since it began tracking such data in 2002.

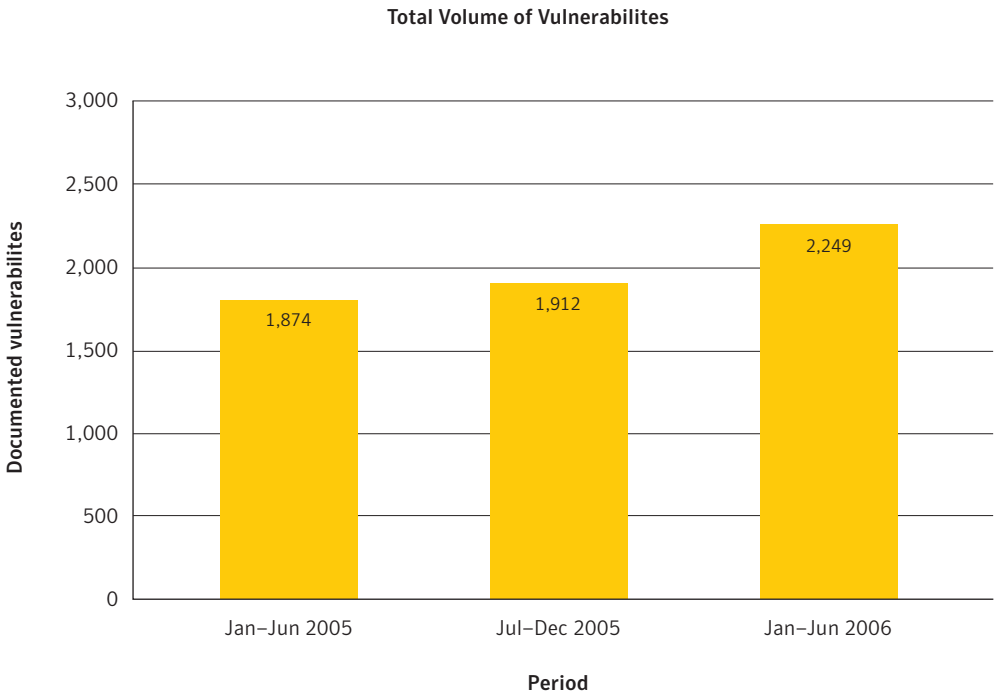

Figure 5. Total volume of vulnerabilities
Source: Symantec Corporation

Of the vulnerabilities documented in the first half of 2006, 80 percent are considered to be easily exploitable, which gives attackers a large pool to leverage for attacks. Moreover, in the same period, approximately 58 percent of exploit codes against the documented vulnerabilities observed were released in six days or less after a vulnerability was announced; of this, 25 percent of the exploits were released in less than one day, while 33 percent fell between one and six days (see Figure 6).

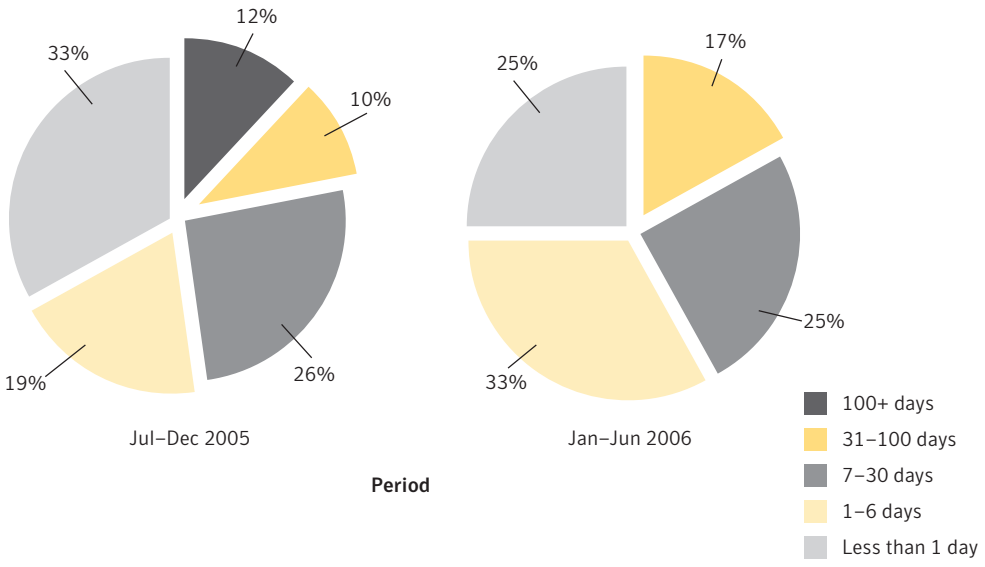

Figure 6. Exploit code release period
Source: Symantec Corporation

Given the rapid development of codes to exploit vulnerabilities, there exists a window of exposure that may put users at risk. The window of exposure is the time between the announcement of a vulnerability and a vendor supplied patch, minus the number of days before the appearance of an exploit (see Figure 7). During this time, the computer or system on which the affected application is deployed may be susceptible to attack, as administrators will likely have no official recourse against a vulnerability and instead will have to resort to best practices and workarounds to reduce the risk of an attack being successful.

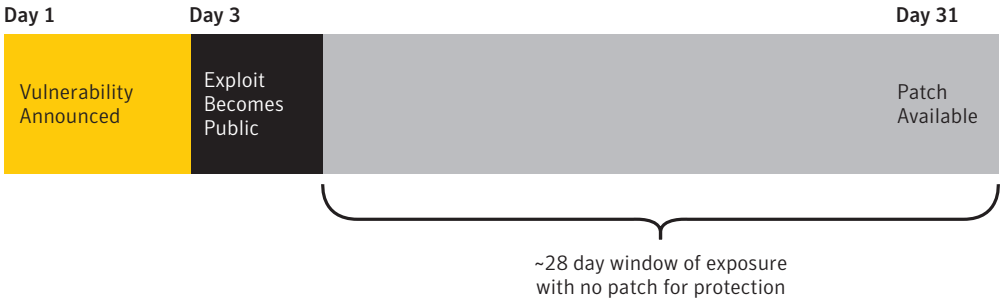

Figure 7. Example of window of exposure
Source: Symantec Corporation

In the first six months of 2006, the average time to develop a patch was 31 days. The average time to develop exploit code during the same period was three days. As a result, the window of exposure for this reporting period was 28 days. As a point of comparison, in the second half of 2005 the window of exposure was 50 days, while in the first half of 2005, it was 60 days.

Although the window of exposure for vulnerabilities in applications developed by enterprise vendors is narrowing due to significant drops in patch development time, the fact remains that a relatively large window of exposure exists. A 28-day window of exposure means that users are exposed to the risk of being attacked successfully for almost a month before a patch is made available.

Impact

Today, attackers are more interested in financial gain than fame. Because of this, they are careful not to draw attention to their activities; the less an attack is noticed, the lower the likelihood it will be stopped, and the greater the chance they can steal information and money. As a result, vulnerabilities are the perfect medium to carry out attacks in stealth, given that they often serve as a silent means of gaining access to a machine. It is not uncommon that successful exploits of vulnerabilities lead to giving an attacker complete control of the compromised machine.

There is a commercial black market for vulnerabilities today that drives some of the most serious Zero Day attacks. WMF is a perfect example: A high-impact Zero Day vulnerability exploit was reportedly sold on the black market to an organization called Iframecash.biz, which was detected using the WMF exploit in the wild during the 2005 holiday season.

Recent types of attacks leveraging these types of vulnerability exploits include espionage, identity theft, and fraud. One example of this was the Microsoft Word 2003 Zero Day vulnerability reported on May 19, 2006, which was leveraged to attack specific organizations. In that attack, a Trojan horse known as Trojan.Mdropper.H was crafted to exploit the vulnerability in order to compromise an affected machine and drop a backdoor on it. The backdoor, known as Backdoor.Ginwui, would then listen on the network for commands from the attacker, such as downloading additional files to carry out further attacks and providing complete control of the victimized machine.

Organizations that are not vigilant against this type of attack risk having confidential information stolen or lost completely, without ever realizing it—or realizing it when it is too late.

Protection requirements

Although firewalls deployed with the appropriate policies help to alleviate some forms of attack, they do not address the bulk of vulnerability exploits. In order to protect against vulnerability exploits, organizations also need adequate Intrusion Prevention Systems (IPS) in place at both the network and host levels. This will provide an effective stopgap against vulnerability exploits and protect the company during the window of exposure before a patch is available. This buys time for vendors to create the necessary patches and for administrators to deploy them.

To be truly effective, IPS solutions must be able to provide broad-based proactive protection for a given vulnerability. Protection from a single instance of a particular exploit is not sufficient. In general, a single vulnerability is often the target of multiple exploits and variants. Solutions that only focus on specific exploit variants are highly reactive and do not effectively protect against the attack. And, in the case where an exploit is unknown, there would be no signatures—and no protection. IPS solutions, however, focus on the vulnerability itself. This results in proactive protection against both known and unknown attempts to exploit that vulnerability. Customers may be able to deploy a single signature to protect against multiple attacks.

The breadth and depth of a vendor's global security intelligence is another key element in providing proactive protection against vulnerability exploits. Both foresight and insight are critical components in designing appropriate, timely protection in today's security environment.

The Symantec solution

Symantec provides proactive protection for vulnerability-based attacks by building a wall against vulnerabilities themselves rather than the exploits. Symantec's IPS technology acts as a shield and attempts to protect a new vulnerability against any future attacks. Additionally, the Symantec Global Intelligence Network (GIN) is the largest security intelligence and probe network in the industry, providing global knowledge and insight into vulnerabilities and security events that allow Symantec to deliver proactive protection to its customers.

During the last eleven months, Symantec has been credited with discovering 11 Zero Day vulnerabilities (see Table 2). These are vulnerabilities where the vendor patch was not available. The Symantec research team has the expertise to identify and differentiate between unknown vulnerabilities and another type of malware. This same expertise is what lies behind the protection it provides its customers—rather than solving symptoms, Symantec solves the root cause. In addition, Symantec notifies vendors of identified vulnerabilities so that they can produce a patch before the vulnerability is publicly known.

Status	MS Bulletin	CVE	Vulnerable applications	Exploiting malware	Disclosure date
Patched	MS05-053	CAN-2005-2124	Windows 2000/XP/2003 (WMF)	N/A	08 November 2005
Not Patched	–	–	Access XP/2003	Trojan.Acdropper, Acdropper.B	01 March 2006
Patched	MS06-012	CVE-2006-0009	Office 2000/XP/2003	Trojan.PPDropper, PPDropper.D	14 March 2006
Patched	MS06-026	CVE-2006-2376	Windows 98/ME (WMF)	N/A	13 June 2006
Patched	MS06-028	CVE-2006-0022	PowerPoint 2000/XP/2003	N/A	13 June 2006
Patched	MS06-031	CVE-2006-2380	Windows 2000 (RPC)	N/A	13 June 2006
Patched	MS06-037	CVE-2006-3059	Excel 2000/XP/2003	Trojan.Mdropper.J	11 July 2006
Patched	MS06-038	CVE-2006-1540	Office 2000/XP/2003 (MSO.DLL)	N/A	11 July 2006
Patched	MS06-047	CVE-2006-3649	Office VBA	Trojan.Mdropper.N	08 August 2006
Patched	MS06-048	CVE-2006-3590	PowerPoint 2000/XP/2003 (MSO.DLL)	Trojan.PPDropper.B	08 August 2006
Not Patched	-	CVE-2006-4534	Word 2000	Trojan.Mdropper.Q	01 September 2006

Table 2. Zero Day vulnerabilities discovered by Symantec
Source: Symantec Corporation

To understand how IPS protects a vulnerability against any future attack, think of a vulnerability as a padlock. Each lock has a set of internal pins that limit the shape of the keys that can open it. If we examine the set of pins in a lock, we can characterize what a key must look like if it is to open the lock, and we can do this without ever seeing the actual key. We can then use the "shape" of the lock to block any attempt to open it, no matter what the key looks like. Similarly, any time a new vulnerability is released, researchers can characterize the "shape" of that vulnerability. In other words, they can describe the specific stream of data that must be sent over the network to the vulnerable computer in order to have any chance of exploiting the vulnerability. Once we have such a characterization, we can produce a signature for this shape that can detect and block any attack (e.g., a worm) that has this telltale "shape."[18]

Vulnerability signatures may initially appear to be similar to traditional antivirus heuristics; however, they are much more robust. Traditional antivirus heuristics work by scanning a file or network stream for a series of suspicious-looking instructions or data sequences—for example, instructions that appear to modify files, format the hard drive, or establish new Internet connections. Ideally, the heuristics are well designed to detect a wide variety of threats; however, there is no guarantee that a particular virus or worm actually employs these instruction sequences. Furthermore, the sequences may be hidden via encryption, compression, or instruction reordering, or the virus author may have decided to tweak the virus until it no longer uses logic detected by existing heuristics.

In contrast, a properly written vulnerability signature cannot be bypassed. In cases where we can accurately characterize the shape of a vulnerability, we can proactively create a signature that detects and blocks all future attacks on that vulnerability. Attempts to modify a worm's exploit packets to make them undetectable by a vulnerability signature result in packets that have the wrong shape. Because of this, the modified exploit is no longer able to attack the targeted vulnerability.[19]

[18] See "Generic Exploit Blocking," www.virusbtn.com/index
[19] See www.computing.co.uk/vnunet/news/2125183/bugwatch-stop-bullet

Symantec has been developing and delivering client-based IPS protection for more than two years in both the consumer and enterprise product lines. In many cases, Symantec has been able to suppress the scale of outbreaks using this technology for many well-known vulnerabilities. An example of this is shown in Figure 8.

Figure 8. Example of IPS protection: W32.Dasher
Source: Symantec Corporation

There have since been more than 40 different worms, bots, and Trojan horses exploiting this vulnerability, as observed by Symantec's Global Intelligence Network. In all instances, Symantec's IPS protection has prevented exploitation prior to the release of antivirus signatures. Table 3 provides examples of the effectiveness of IPS.

Number of variants blocked	Vulnerability/IPS protection signature name	Exploit example
416	MS RPC DCOM BO	Blaster
394	MS LSASS BO	Sasser
65	MS IE MIME Header	W32.HLLW.GOP@mm
55	MS IIS Webdav Exploit	Welchia
51	MS Plug and Play BO	W32.Zotob.A
43	MS Locator Service BO	Trojan.NT.A

Table 3. Examples of IPS effectiveness
Source: Symantec Corporation

Through leveraging the GIN, Symantec continues to make advances in its technology and techniques to ensure that it continues to provide effective and proactive protection against new and emerging vulnerability exploits via its IPS technology.

Conclusion

Cybercriminals motivated by financial gain are constantly identifying new ways to steal information or provide remote access to user systems. Cybercriminals are focusing on new, sophisticated techniques in combination with older but still effective methods to create tough threats that increase the likelihood of successful compromise before security measures can be put in place. Organizations and users need to partner with security vendors that can help them combat not one type of tough threat, but all of them.

While speed is an important measure of how well security vendors respond to a threat, by itself it is not an accurate measure of security effectiveness. The evolving threat landscape dictates that speed must be accompanied by a security vendor's attention to quality and completeness of protection, as well as its ability to deal with the latest threats that rely heavily on evasion, stealth, and aggressive behavior. These tough threats include polymorphics, rootkits, advanced evasion techniques, and Zero Day attacks.

Symantec Security Response is the world's leading Internet security research and support organization. With the evolution of the threat landscape away from large-scale, pandemic threats to quieter, more targeted attacks from multiple vantage points, it is critical to have a clear view of activity taking shape on a global basis and to understand how blended threats can impact customers. If a company looks at threat activity through a single viewpoint, such as spyware or spam, it will miss the real impact. Looking at attacks from every angle is where Symantec Security Response excels—and this translates to comprehensive protection for customers against the latest breed of attacks.

Symantec customers can be confident that they are protected by:

- Continued, innovative security technologies that handle the toughest threats, with more than 250 patents issued to date
- An unrivaled, worldwide security intelligence network
- Timely early warning protection through 24x7 coverage
- The fastest, most comprehensive analysis from a global team of security and operational specialists
- Security intelligence and protection across the breadth of Symantec's products
- A security partner that stays ahead of tomorrow's threats

Symantec is the market leader in tackling tough threats, with the technology, expertise, and history to excel in the new landscape.

Appendix A

Anti-Rootkit Test Methodology

Rootkits tested

The rootkit samples were chosen by the tester and were designed to be representative of the current real-world situation, and were a mix of commercial spyware, adware, and rootkits commonly available from live exploitive and socially engineered Web sites. It's possible that a few of the rootkits were Zoo-level (in other words, from a researcher's collection), but every effort was made to obtain real live samples from the Wild.

- Haxdoor-gp
- CommonName
- QoolAid
- DollarRevenue trojan
- Feebs
- Pcacme standard
- HaxSpy.ab
- Look2Me
- Sony XCP rootkit
- Goldun
- Adlogix
- PcQuick/Hoosmi
- SearchNet
- Spybot
- Haxdoor-ie
- OrderGun.A
- Graybird/Hupigen
- Teros-B
- Frogexer
- Rustok.B

Test methodology

Software platforms:

All tests were conducted on Windows XP SP2, patched to August 2006. All systems were started from a clean image for each test. Each product under test was the most recent publicly available copy, and each product was allowed to update itself prior to each test, if it wanted to. Each product under test was installed with default parameters, except for SpySweeper, which had rootkit detection off by default. This was switched on for the purpose of the test.

The following steps can be used to determine the effectiveness of a product to handle rootkit threats.

1. Install a rootkit by disabling the rootkit blocking features of the product. Credit was given for a rootkit detection regardless of the component in the product that produced the alert (i.e. firewall, shields, etc.).
2. Test to determine whether the product can remove the rootkit. Credit was given for a rootkit removal only if the product was able to both remove the components so that the rootkit is no longer left running on the system and completely remove all side effects of the rootkit, such as registry keys.

Install a rootkit

To install rootkits with different file formats:

1. Run the .exe file if one exists.
2. Use "InstDriver.exe," a tool to install and run a kernel mode driver (.sys) file, if the rootkit has no .exe file.
3. Use "regsvr32 <path_to_dll_file>" to register the .dll file if the rootkit has no .exe file.

The main issue with installing a rootkit is that, once installed, it can be extremely difficult to detect. Tools that should not be used are filemon, regmon, or anything that uses Windows APIs. The generic detector tools in Table 4 were used in this test to determine the presence of rootkits, in no particular order.

Product	Strengths
F-Secure Blacklight	Detects hidden files and processes.
Sysinternals Rootkit revealer	Detects hidden files and registry keys.
IceSword	Detects hidden modules, processes, and services, and for navigating through registries like regedit, including hidden keys.
DarkSpy	Detects hidden modules, processes, services, registry keys, and ports.
GMER	Detects hidden modules, processes, services, registry keys, and ports.
RKDetector	Detects hidden files and registry keys.
Sophos AntiRootkit	Detects hidden alternate data streams (ADS).

Table 4. Rootkit detection capabilities of some freely available anti-rootkit tools

The tools mentioned on the previous page are all freeware and can be downloaded by searching online. There are some instances of rootkits that specifically target well-known anti-rootkit tools to avoid detection. For this reason, the tester should utilize at least two of the tools referenced in Table 4 and a tool that is not widely deployed to test the presence of the rootkit on a system.

Test to detect the presence of a rootkit

Once a rootkit is running on a system as indicated by the tools mentioned in Table 4, the next step is to test the capability of a product to detect it.

1. **Run a scan**

   Run a scan to test whether the product can detect the presence of the rootkit. A scan can be composed of running objects or it can be a full sweep scan of the entire hard disk. If the product detects the presence of some rootkits or hidden objects, they should be properly identified and have an appropriate recommendation.

2. **Test to remove a rootkit using product features**

   If a product detected the rootkit, it was then asked to clean the system. Due to the complex techniques rootkits use, the computer may have to be rebooted before the rootkits are completely removed from the system. The tester followed whatever advice was offered by the product. Once the remediation was complete, the following steps were used to determine if the removal had been successful:

   (a) Examine the system using the generic detectors. If the generic detectors still found hidden files, processes, or registry keys, it was regarded as a fail.

   (b) If no hidden items were found, the next step was to take a snapshot of the system using PC Surgeon, and compare the before and after images to see what remnants, if any, were left behind.

Appendix B

Advanced Evasion Techniques (AntiSpyware) Testing Methodology

Security risks tested:

- Adware.2Search.a
- Adware.2Search.h
- Adware.BHO
- Adware.BookedSpace
- Adware.Casino
- Adware.ClearSearch
- Adware.Coolbar
- Adware.Delf
- Adware.Digitalnames
- Adware.DownloadWare
- Adware.Energyplugin
- Adware.Ezula
- Adware.Gator
- Adware.Hengbang
- Adware.Homeland
- Adware.Hotbar
- Adware.IGetNet
- Adware.KeenValue
- Adware.Look2Me
- Adware.Lop
- Adware.Maxifiles
- Adware.MediaMotor
- Adware.NetNucleus
- Adware.NewWeb
- Adware.Nurvel
- Adware.Psguard
- Adware.PurityScan.ei
- Adware.PurityScan.ej
- Adware.PurityScan.ek
- Adware.RelatedLinks

Detection and repair guidelines

- Start with a clean system.
- Generate a baseline snapshot (#1) with a reputable system snapshot tool such as PCSurgeon.
- Install the spyware threat(s), i.e., run the actual sample.
- Generate another system snapshot (#2) with the system snapshot tool to record changes (additions, deletions, modifications) to the system caused by running the threat(s).
- Run a full system scan with the product under test.
- Run another system snapshot (#3) with the system snapshot tool to see what was removed.
- Save the log from the product under test.
- If a reboot is required, note the name of the file(s) that need a reboot before they can be removed. This can be found in the registry

(HKLM\System\CurrentControlSet\Control\Session Manager\PendingFileRename)

- If a file is mentioned in this location, make sure that when you reboot, the file really has been removed.
- Compare the system snapshots to determine the effectiveness of the threat removal product.

Note: These are high-level steps and may change slightly depending on the product under test.

Notes on detection and repair guidelines

Remediation

Actual remediation of adware, spyware, and other threats is required. Performing the detection process and then making assumptions about a product's remediation capability based on the results is not sufficient.

Product logs

A proper registry monitor is required to find out what is really being removed from the system. This approach needs to be followed when testing any antispyware product. Product logs (from many vendors) are not an accurate gauge of the detection and removal performed on a system. Furthermore, product logs are not an independent source of information.

Independent monitoring tools

There are several suitable independent system monitoring and snapshot tools on the market. One example is PCSurgeon, which gives an accurate depiction of what a threat installs and what a security product removes from a system. It provides a comparison of two system snapshots. This type of independent monitoring tool is recommended for detection and repair testing.

Test types

Two types of tests need to be completed when testing detection and repair capabilities.

1. **Stand-alone test**

   A stand-alone test is performed when an antispyware product is the only such product installed and tested on the system. Ideally, the system will be infected with all samples to be used for testing so the system can be used to test all the products. A manual or on-demand scan is run and then repair is run. See the test guidelines section above for further details. The goal of this test is to see what the antispyware product detected and removed versus what the spyware installed on the system.

   Test 1: Run Product A scan, detection, and removal followed by Product B scan, detection, and removal. Record results.

2. Follow-on test

This test uses the same infected system mentioned above. However, two competing products will be installed on the system (one of which will always be Norton Internet Security). Perform a manual or on-demand scan with one product. Once the scan and repair have been completed with this product, do the same with the second product. Any threats detected and removed by the second product need to be recorded as a metric. Then re-run the test with the sequence reversed. The goal of this test is to determine what an antispyware product will detect and remove after another product has performed detection and repair, and vice versa.

Test 2: Run Product B scan, detect, and removal followed by Product A scan, detect, and removal. Record results. Then compare results.

Scoring

Credit was given for a remediation of a security risk as long as it removed at least 90 percent of the dropped artifacts.

About Symantec

Symantec is the world leader in providing solutions to help individuals and enterprises assure the security, availability, and integrity of their information. Headquartered in Cupertino, Calif., Symantec has operations in more than 40 countries. More information is available at www.symantec.com.

For specific country offices and contact numbers, please visit our Web site. For product information in the U.S., call toll-free 1 (800) 745 6054.

Symantec Corporation
World Headquarters
20330 Stevens Creek Boulevard
Cupertino, CA 95014 USA
+1 (408) 517 8000
1 (800) 721 3934
www.symantec.com

Printed in the U.S.A. 10/06 11310863