



## **Symantec™ Security Update - June 2005**

### **Worldwide and Americas**

Monthly report examining recent high severity vulnerabilities, cyber attacks, malicious code and spam activity.

# **Symantec Security Update - June 2005**

## **Worldwide and Americas**

### **AN IMPORTANT NOTE ABOUT THE FOLLOWING DISCUSSION**

The attack data discussed in this document is based on attacks targeting an extensive sample of Symantec customers. The attack activity was detected by Symantec between May 24 and June 23, 2005.

Symantec uses automated systems to map the IP address of the attacking system to identify the country in which it is located. However, because attackers frequently use compromised systems located around the world to launch attacks remotely, the location of the attacking system may differ from the location of the attacker. Despite the uncertainty that this creates, Symantec feels that this type of data is useful in creating a high-level profile of global attack patterns.

The number of contributing sensors in each region varies. Combined with different standard security practices, these variations may result in different attack data being recorded in each region. This may preclude valid comparisons between regions.

## **Executive Summary**

This *Symantec Security Update* offers a brief summary of Internet security activity for the month of June 2005. The update covers developments in vulnerabilities, attacks, malicious code, and spam. This report will discuss security developments in the Americas region, which includes both North America and South America, over the past month.

Symantec maintains one of the world's most comprehensive databases of security vulnerabilities, currently consisting of over 11,000 vulnerabilities (spanning more than a decade), affecting more than 20,000 technologies from over 2,000 vendors. This report will discuss three vulnerabilities disclosed during the month of June that Symantec analysts have identified as being particularly noteworthy, either because of their severity or because they represent an interesting development. The vulnerabilities discussed include two in the Microsoft Windows operating system, and one in the Macintosh OS X operating system. All three vulnerabilities have the potential to compromise system integrity. All three may be mitigated by the application of patches recently released by the vendors.

Symantec comprehensively tracks attack activity across the Internet. Over 20,000 sensors deployed in over 180 countries by Symantec DeepSight™ Threat Management System and Symantec™ Managed Security Services gather this data. The attack statistics discussed in this document are based on attacks detected by these sensors between May 24 and June 23, 2005.

During the month of June 2005, the top attack, both worldwide and in the Americas region, was related to the SQL Slammer worm. While this worm was first detected in January 2003, it continues to propagate. Bot-network computers, computers compromised by remote control programs and used in concert for attacks, remain a problem for networks. Recognizing the ongoing threat posed by bot networks, Symantec tracks the distribution of bot-infected computers around the world. The city that had the highest percentage of bot-infected computers in the Americas region this month was Toronto.

Symantec gathers data from over 120 million desktops that have deployed Symantec's antivirus products in consumer and corporate environments. The Symantec Digital Immune System™ and Scan and Deliver technologies allow customers to automate this submission process. This discussion is based on malicious code samples submitted to Symantec for analysis from May 24 to June 23, 2005. During this period, the top reported malicious code sample in the Americas region was the B variant of the Tooso Trojan, which was first discovered on February 28, 2005. This variant joins two other Tooso variants in the top malicious code reports for the month. Tooso is a family of Trojans that was used by mass-mailing viruses and attempts to hide itself on the compromised computer by disabling antivirus systems and taking other protective measures.

## Top Vulnerabilities

Symantec has analyzed the vulnerabilities disclosed between May 24 and June 23, 2005 and identified three of the most noteworthy severe vulnerabilities (table 1). Severe vulnerabilities are those that result in a compromise of the entire system if successfully exploited. In almost all cases, successful exploitation can result in a complete loss of confidentiality, integrity, and availability of data stored on or transmitted across the system. The threat of severe vulnerabilities is increased if and when an associated exploit is released publicly or if the vulnerability can be exploited trivially.

BID Number	Vulnerability
13941	Microsoft Internet Explorer PNG Image Rendering Buffer Overflow Vulnerability
13951	Microsoft Outlook Express NNTP Response Parsing Buffer Overflow Vulnerability
13899	Apple Mac OS Apple Filing Server Remote Buffer Overflow Vulnerability

Table 1. Top vulnerabilities, June 2005

Source: Symantec Corporation

The Microsoft Internet Explorer PNG Image Rendering Buffer Overflow Vulnerability<sup>1</sup> was first disclosed on June 14, 2005. The PNG image file format is a popular format similar to the GIF format that is widely used for Web sites. This buffer overflow vulnerability<sup>2</sup> allows remote attackers to compromise a browser to gain the privileges of the user running the vulnerable Internet Explorer. For instance, if an administrator were running Internet Explorer, the attacker would gain administrator privileges.

Exploitation occurs when Internet Explorer loads a Web page containing a malicious PNG image file. When the browser attempts to display the malicious PNG image, the malicious data within the PNG file triggers the vulnerability and exploitation occurs. Remotely exploitable buffer overflow vulnerabilities are particularly dangerous, as skilled attackers can carry out exploitation without alerting a target user to the attack.

As outlined in the previous two volumes (September 2004 and March 2005) of the Symantec *Internet Security Threat Report*,<sup>3</sup> vulnerabilities that affect Web browsers have become much more common targets of attacks. This can be attributed to the widespread implementation and use of browser on both home and corporate computers. The success of Web browser attacks is helped by the fact that Web traffic is not typically filtered by firewalls, so that such attacks are able to bypass traditional perimeter security. As a result, attackers can gain access to an entire network by exploiting one vulnerable desktop browser.

Symantec advises users and administrators to apply the appropriate patches to all affected Microsoft Internet Explorer packages. It may be possible to prevent exploitation of these issues by implementing intrusion detection systems to monitor HTTP traffic for potential attacks, and to filter them out before they become successful. It may also be

<sup>1</sup> <http://www.securityfocus.com/bid/13941>

<sup>2</sup> A buffer overflow vulnerability exists when a process fails to limit the user data that it will store. This allows an attacker to force the vulnerable process to store more data than it was intended to, causing the excess data to overwrite critical values stored in memory. The attacker can then manipulate the vulnerable process and insert malicious instructions that will be executed.

<sup>3</sup> <http://enterprisesecurity.symantec.com/content.cfm?articleid=1539>

possible to reduce exposure to these attacks by educating users to be extremely cautious about visiting potentially malicious Web sites or following links in unsolicited emails.

The Microsoft Outlook Express Network News Transport Protocol (NNTP) Response Parsing Buffer Overflow Vulnerability<sup>4</sup> was originally disclosed on June 14, 2005. The Network News Transport Protocol (NNTP) facilitates the transfer of newsgroup messages over a network. Microsoft Outlook Express is the default news client on Microsoft Windows operating systems.

This vulnerability allows an attacker to compromise a browser to gain the privileges of the user running the vulnerable application. For instance, if an administrator were running the application, the attacker would gain administrator privileges. Due to its common use NNTP is not typically considered a vector for attack; as a result, it is likely that its associated ports will not be blocked at the network perimeter. Successful exploitation of this vulnerability could allow an attacker to find their way past the corporate perimeter security and gain a platform within the corporate network to carry out further attacks.

Exploitation of this vulnerability may be carried out through a number of remote methods. The most likely method of attack is through an HTML NNTP link (`news://`) embedded on a Web page. The link will invoke the news protocol and contain data designed to trigger and exploit the buffer overflow vulnerability. When a user follows the malicious link, Outlook Express will be started in order to handle the news protocol data. The user will be required to approve the download of a newsgroup list from a server. When the user approves the download, the buffer overflow is triggered.

Symantec advises users and administrators to apply the appropriate patches to all affected Microsoft Windows products. It may also be possible to reduce exposure to these attacks by educating users to be extremely cautious about visiting potentially malicious Web sites or following links in unsolicited emails. Finally, it may be possible to reduce the threat of this issue by implementing rule sets at the router or firewall to block traffic to the NNTP port (119) at the network perimeter.

The Apple Mac OS Apple Filing Server Remote Buffer Overflow Vulnerability<sup>5</sup> was disclosed on June 8, 2005. The Apple Filing Server implements Apple's Apple Filing Protocol, which is the foundation of AppleShare file sharing technology. AppleShare allows Mac OS users to share their files with other AppleShare enabled computers at the click of a button. All Apple Mac OS X and earlier operating systems implement AppleShare technology.

The Apple Mac OS Apple Filing Server Remote Buffer Overflow Vulnerability allows attackers to compromise a vulnerable computer to gain administrator access. This vulnerability is remotely exploitable, allowing network-based attacks. Attackers can exploit this vulnerability by sending malicious data to the affected computer over a network or the Internet. Once exploitation occurs, the attacker gains complete control over the target computer.

Although AppleShare is not enabled by default it remains a popular method for Mac users to share files and is a viable vector for attacks from malicious code and attackers. Furthermore, when a user activates file sharing, the default firewall is automatically reconfigured to allow Apple Filing Protocol (AFP) traffic to access the affected computer,

---

<sup>4</sup> <http://www.securityfocus.com/bid/13951>

<sup>5</sup> <http://www.securityfocus.com/bid/13899>

potentially opening users up to attack without their knowledge. Due to the widespread deployment of the vulnerable software, there is a possibility that malicious code that exploits this issue will be developed.

Symantec advises users and administrators to apply the appropriate Apple security update to all affected Mac OS X products. Administrators should also disable file sharing if it is not required and ensure that traffic over the Apple Filing Protocol Ports (548 and 427) is allowed only between trusted networks by implementing firewall rule sets.

## Top Attacks

Between May 24 and June 23, 2005, the most common attack, both worldwide (table 2) and in the Americas region (table 3), was the SQL Slammer attack. Performed by 14% of the attacking IP addresses located in the Americas region, this attack is commonly associated with three high-profile malicious code samples: Slammer,<sup>6</sup> Gaobot,<sup>7</sup> and Spybot.<sup>8</sup> The attack affects both the Microsoft SQL Server and the MSDE (Microsoft Desktop Engine) that is included with some third-party software, which makes it difficult to patch all vulnerable systems.

World Rank	Top Attacks - Worldwide	Percentage of Total Attackers	Affected Service
1	SQLExp Incoming Worm Attack	17%	Microsoft SQL Server
2	Generic HTTP CONNECT TCP Tunnel Attack	9%	Generic Web (HTTP) Service
3	Generic X86 Buffer Overflow (TCP NOPS) Attack	7%	Generic Attack

Table 2. Top attacks worldwide, June 2005

Source: Symantec Corporation

Region Rank	Top Attacks - Americas	Percentage of Total Region Attackers	Affected Service	World Rank	Percentage of Total World Attackers
1	SQLExp Incoming Worm Attack	14%	Microsoft SQL Server	1	17%
2	SGL IRIX cgi-bin Wrap Attack	11%	SGL Web Application	7	6%
3	Generic X86 Buffer Overflow (TCP NOPS) Attack	8%	Generic Attack	3	7%

Table 3. Top attacks originating in Americas region, June 2005

Source: Symantec Corporation

The high ranking of this attack is likely due to two factors related to the use of UDP as the transport mechanism. First, the use of UDP allows a complete attack<sup>9</sup> to be sent to every potential victim computer, regardless of whether SQL Server is installed or running. Most intrusion detection systems will therefore interpret each attempt as a full attack, even if

<sup>6</sup> <http://securityresponse.symantec.com/avcenter/venc/data/w32.sqlexp.worm.html>

<sup>7</sup> <http://securityresponse.symantec.com/avcenter/venc/data/w32.hllw.gaobot.aa.html>

<sup>8</sup> <http://securityresponse.symantec.com/avcenter/venc/data/w32.spybot.worm.html>

<sup>9</sup> UDP does not require that any form of synchronization be done before data is sent and accepted by the target service. By contrast, an attack that uses TCP must go through the three-way handshake to synchronize the systems prior to data being sent; therefore, a TCP-based attack will only be seen if the service being targeted is accepting connections. In the case of UDP, the attacking system can simply send the complete attack without regard for whether the service is listening.

the destination computer is not turned on. Secondly, the use of UDP also allows this attack to come from a spoofed source address, which may inflate the number of observed source IP addresses. Slammer did not spoof its source; however, as the attack is now used by other malicious code this ability could be added.

This attack is particularly risky for mobile computers. If they become infected outside the traditional perimeter they could transfer the malicious code inside the perimeter through a VPN connection or by plugging directly into the network. Perimeter filtering of Microsoft SQL ports and strong policy compliance can significantly reduce the risk of compromise by this attack.

The second most common attack originating in the Americas region between May 24 and June 23, 2005 was the SGI IRIX cgi-bin Wrap Attack. Used by 11% of all attacking IP addresses located in the Americas, this attack is a Web-related attack that often depends on a specific string to be present in the URL request for the signature. SGI IRIX systems that are vulnerable can allow any world-readable file to be accessed if an attacker makes a request to the wrap CGI Web application with a “../..../” directory traversal string as a parameter.

As with all Web application vulnerabilities, administrators should ensure that up-to-date patches are applied. Web application target systems often provide a public service; therefore, systems providing public access should be segmented from private networks by a firewall or demilitarized zone (DMZ). This will limit network exposure should a compromise occur. All public IP addresses should be scanned and audited to ensure that only legitimate services are running.

The third most common attack detected originating in the Americas region between May 24 and June 23, 2005 was the Generic X86 Buffer Overflow (TCP NOPS) Attack. This attack, which was used by 7% of attackers situated in the Americas region, is a generic attack that indicates suspicious activity identified on the network. This attack indicates that a series of X86 No-Op instructions (no operation) were identified. No-Ops are often seen when an attacker is attempting a buffer overflow attempt.

Organizations should ensure that all publicly deployed Web servers are configured using a standard template that has been audited to protect against this kind of attack. Firewalls should also be placed between publicly accessible computers and internal networks, creating a demilitarized zone to limit the scope of a compromise.

## Top Cities by Bot-Infected Computers

Bot-infected computers operate in a coordinated fashion under the direction of an attacker and can number in the hundreds or thousands. These networks of computers can scan for and compromise additional computers and may be used to perform denial of service attacks.

Recognizing the ongoing threat posed by bot networks, Symantec tracks the distribution of bot-infected computers both worldwide (table 4) and across the Americas region (table 5). In order to do this, Symantec calculates the number of computers worldwide that are known to be infected with bots and assesses which cities are home to the highest percentages of these computers. The identification of bot-infected computers is important, as a high percentage of infected machines could mean a greater potential for bot-related attacks. It may also indicate the level of patching and/or security awareness.

World Rank	City	Country	Percentage of World's Bots
1	Winsford	United Kingdom	5%
2	Seoul	South Korea	4%
3	Beijing	China	3%

Table 4. Top three bot-infected cities, Worldwide, June 2005

Source:  
Symantec Corporation

Region Rank	City	Country	Percentage of Region's Bots	World Rank	Percentage of World's Bots
1	Toronto	Canada	9%	6	2%
2	Montreal	Canada	5%	14	1%
3	New York	United States	3%	24	1%

Table 5. Top bot-infected cities, Americas region, June 2005

Source: Symantec Corporation

In the March 2005 edition of the *Internet Security Threat Report*, Symantec speculated that a city's rate of bot infection is related to two factors: the size of the city and the rate of broadband growth in that city. Two Canadian cities, Toronto and Montreal, account for 9% and 5% of the bot-infected computers in the Americas region respectively (table 5). As both Toronto and Montreal are significantly smaller than other cities in the Americas region, the high ranking of these cities may be due to a significant number of new high-speed Internet customers. New York, one of the largest cities in the region, is home to the 3% of the Americas region's bot-controlled computers.

Bot-infected computers can be used to perform secondary attacks, such as denial of service attacks, on other targets. To protect against compromise by a bot network, Symantec recommends that administrators ensure that ingress and egress filtering is in place to block known bot-network traffic and that antivirus definitions are updated regularly. As compromised computers can be a threat to other systems, Symantec also recommends that notification of ISPs regarding all malicious activity be included as part of a incident response plan.

## Malicious Code

The top malicious code samples reported to Symantec in June 2005 from the Americas region bears many similarities to the top samples reported worldwide for the same period. The top reported sample, both worldwide and for the Americas (table 6), was the B variant of the Tooso Trojan, which was initially discovered on February 28, 2005. Notably, there are three variants of Tooso present in both the top ten worldwide and in the Americas.

Worldwide		Americas	
Rank	Sample	Rank	Sample
1	Tooso.B	1	Tooso. B
2	Netsky.P	2	Tooso.F
3	Spybot	3	Netsky.P
4	Tooso.F	4	Mytob.CU
5	Mytob.CU	5	Sober.O
6	Gaobot	6	Tooso.I
7	Lineage	7	Phel
8	Lemir	8	Mytob.ED
9	Tooso.I	9	Spybot
10	Redlof	10	Mydoom.BU

Table 6. Top ten malicious code, June 2005

Source: Symantec Corporation

Tooso.B<sup>10</sup> is a Trojan that was mass-mailed by two variants of the Beagle mass-mailing worm, Beagle.BG<sup>11</sup> and Beagle.BH.<sup>12</sup> Once installed on a computer, Tooso.B disables antivirus and security applications by terminating their processes and deleting associated registry keys and files. It also hinders access to antivirus and security application vendor Web sites by creating entries in the HOSTS file that redirect access to these sites. Tooso.B also attempts to download a file from a number of Web sites; however, this file has never been available.

The Tooso.F Trojan was mass mailed by the BN<sup>13</sup> variant of the Beagle worm. This Trojan, discovered on April 15, 2005, bears many similarities to the Beagle family of mass-mailing worms but does not contain any code to perform its own mass mailing. Instead, Tooso disables antivirus and security software on the compromised computer by terminating processes, stopping services, removing registry keys, and deleting files related to these applications. Tooso also overwrites the HOSTS file on the computer in order to prevent access to Web sites of antivirus and security companies. Finally, the Trojan also attempts to download and execute a file from remote locations at six-hour intervals. The downloaded file is an updated version of the Tooso Trojan.

Netsky.P<sup>14</sup> remains one of the malicious code samples most widely reported by Symantec customers. While Tooso.B and Tooso.F were each discovered in early 2005, Netsky.P was discovered in March 2004. Netsky.P is a mass-mailing worm that may send itself in a ZIP archive that can bypass some email gateway antivirus scanners. The worm also copies

<sup>10</sup> <http://securityresponse.symantec.com/avcenter/venc/data/trojan.tooso.b.html>

<sup>11</sup> <http://securityresponse.symantec.com/avcenter/venc/data/w32.beagle.bg@mm.html>

<sup>12</sup> <http://securityresponse.symantec.com/avcenter/venc/data/w32.beagle.bh@mm.html>

<sup>13</sup> <http://securityresponse.symantec.com/avcenter/venc/data/w32.beagle.bn@mm.html>

<sup>14</sup> <http://securityresponse.symantec.com/avcenter/venc/data/w32.netsky.p@mm.html>

itself to shared folders used by various peer-to-peer file-sharing applications in order to make itself available for download on those networks.

Two variants of the Mytob<sup>15</sup> worm were also prevalent in the Americas during the month of June. These are mass-mailing worms that install an IRC bot on compromised computers. Symantec suspects that members of the same group likely created these two variants since both variants connect to the same IRC server.

To protect against and mitigate all malicious code infection, Symantec recommends that end users practice defense in-depth, including the deployment of antivirus, firewall and intrusion detection solutions. Users should update antivirus definitions regularly. They should also ensure that all desktop, laptop, and server computers are updated with all necessary security patches from their operating system vendor. They should never view, open, or execute any email attachment unless the attachment is expected and comes from a known, trusted source and the purpose of the attachment is known.

---

<sup>15</sup> <http://securityresponse.symantec.com/avcenter/venc/data/w32.mytob.aw@mm.html>

## Spam

The Symantec Probe Network consists of millions of decoy email addresses that are configured to attract a large stream of spam attacks that are representative of spam activity across the Internet as a whole. An attack can consist of one or more spam messages, and is defined as a group of similar messages. The data used in this analysis is based on the spam messages detected by Symantec Probe Network sensors based in the Americas region between May 24 and June 23, 2005. It will assess spam activity according to two criteria: the type of product or service with which it is associated and the region from which the spam originated.

### Spam by Type

Symantec assesses spam messages and analyzes them according to the type of product or service with which they are associated. Symantec has assessed both worldwide spam and spam detected by probes based in the Americas region. During the month of June, the most common worldwide spam (figure 1) was related to products, accounting for 21.4%. Spam related to financial products or services was the second most common type, making up 20.1% of all worldwide spam messages. Finally, spam related to health products or services was the third most common type of spam, constituting 13.0% of all spam across the Internet as a whole.

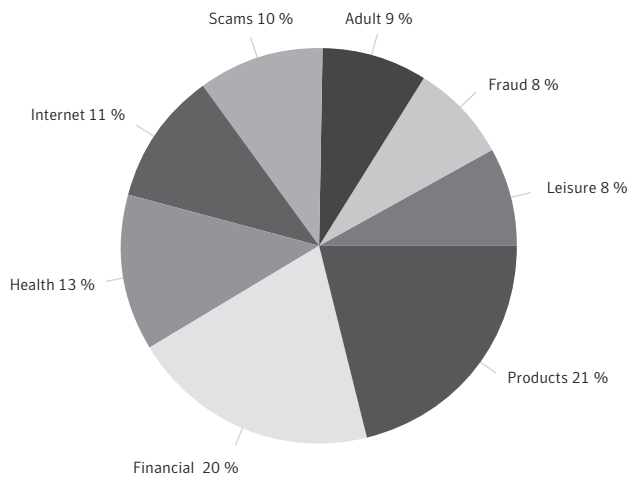


Figure 1. Worldwide spam by type, June 2005

Source: Symantec Corporation

A very similar pattern was detected in the Americas region. During the month of June, the most common type of spam messages detected by probes in the Americas (figure 2) was related to products, which accounted for 21.7% of detected message. Financial services made up the second most common type, 20.5%. The third most common type of spam messages during this period was related to health products or services (12.7%).

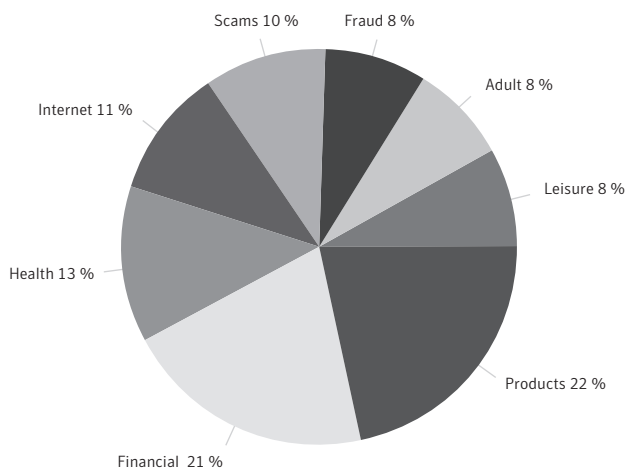


Figure 2: Americas spam by type, June 2005

Source: Symantec Corporation

### Spam - Region of Origin

North America continues to be the highest region of origin for spam detected by the Symantec Probe Network. Symantec believes that this is likely due to the widespread accessibility to cheaper broadband connectivity in this region, although Europe and Asia also have high rates of broadband connectivity. As more spam is likely to be sent from hijacked desktop computers, Symantec expects to continue to see large amounts of spam coming from those regions with high bandwidth capabilities.

As many spammers attempt to redirect attention away from their place of operation, this could also lead to less spam “originating” from the regions within which spammers are actually located. Spammers can build networks of compromised computers globally and utilize only those networks that are geographically disparate from their place of operation. In doing so, they will likely focus on compromised computers in those regions with the largest bandwidth capabilities. Following this logic, the region from which the spam originates may not correspond with the region in which the spammers are located.

Under this scenario, a spammer based in Europe could be more likely to send spam to European recipients from non-European IP spaces. When the same spammer sends spam to the Americas, the spam can be sent from an American-based IP to an American recipient with less risk of prosecution for the European spammer (versus sending spam locally to European recipients from European IP's).

## 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](http://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 800 745 6054.

Symantec Corporation  
World Headquarters  
20330 Stevens Creek Boulevard  
Cupertino, CA 95014 USA  
408 517 8000  
800 721 3934  
[www.symantec.com](http://www.symantec.com)

Symantec and the Symantec logo are U.S. registered trademarks of Symantec Corporation. Other brands and products are trademarks of their respective holder/s. Any technical information that is made available by Symantec Corporation is the copyrighted work of Symantec Corporation and is owned by Symantec Corporation. NO WARRANTY. The technical information is being delivered to you as-is and Symantec Corporation makes no warranty as to its accuracy or use. Any use of the technical documentation or the information contained herein is at the risk of the user. Copyright © 2005 Symantec Corporation. All rights reserved. 07/05 10431085