



Symantec™ Security Update - July 2005

Worldwide and Japan

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

Symantec Security Update - July 2005

Worldwide and Japan

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 June 24 and July 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 July 2005. The update covers developments in vulnerabilities, attacks, malicious code and spam. This report will discuss security developments in the Japan region over the past month.

Symantec maintains one of the world's most comprehensive databases of security vulnerabilities, covering over 13,000 vulnerabilities affecting more than 30,000 technologies from over 4,000 vendors. This report will discuss three vulnerabilities disclosed during the month of July 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 that applies to the cross-platform Web browser Mozilla Firefox. 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 entire 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 June 24 and July 23, 2005.

During the month of July 2005, the top, both worldwide and in the Japan region, was the SQLExp Incoming Worm Attack, also known as the Slammer Attack. While this worm was first detected in January 2003, it continues to propagate. Bot-infected 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 Japan region this month was Tokyo.

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 reported to Symantec. The top reported malicious code worldwide and in the Japanese region from June 24 to July 23, 2005 was the P variant of the Netsky Virus. Netsky.P is a mass-mailing worm that may send itself in a ZIP archive that can bypass some email gateway antivirus scanners.

The Symantec Probe Network consists of millions of decoy email addresses that are configured to attract a large stream of spam attack; representative of spam activity across the Internet as a whole. During July, the most common type of spam, both in the Japan region and worldwide, was related to commercial products. In addition, a majority of the spam detected worldwide originated from computers located inside North America.

Top Vulnerabilities

Symantec maintains one of the world's most comprehensive databases of security vulnerabilities, covering over 13,000 vulnerabilities affecting more than 30,000 technologies from over 4,000 vendors.

Symantec has analyzed vulnerabilities reported between June 24 and July 23, 2005 and identified three of the most noteworthy high-severity vulnerabilities. High-severity vulnerabilities are those that result in a compromise of the entire system if 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.

BID Number	Vulnerability
14214	Microsoft Windows Color Management Module ICC Profile Buffer Overflow Vulnerability
14087	Microsoft Internet Explorer Javaprx.dll COM Object Instantiation Heap Overflow Vulnerability
14242	Mozilla Firefox Set As Wallpaper Arbitrary Code Execution Vulnerability

Table 1. Top vulnerabilities, July 2005

Source: Symantec Corporation

The Microsoft Windows Color Management Module International Color Consortium (ICC) Profile Buffer Overflow¹ Vulnerability² was originally disclosed on July 12, 2005. The ICC standard is a universal standard designed to ensure that colors are represented in the same way on all operating systems and platforms.

This vulnerability can be exploited when the Microsoft Color management System library (mscms.dll) processes an image containing malicious ICC data. Many applications that display images on Microsoft Windows platforms will be affected by this vulnerability, including Microsoft Internet Explorer and Microsoft Office software. This vulnerability allows an attacker to compromise an application to gain privileges of the user running it. For example, if an administrator were running the vulnerable application, the attacker would gain administrator privileges.

This vulnerability can be exploited by causing an application that uses the vulnerable Microsoft Windows component to display a malicious image. An attacker can deliver the malicious image through an email attachment, inside a Microsoft Word document, or on a Web page. When a vulnerable application, such as Internet Explorer, attempts to display the malicious image, the malicious ICC data within the image 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.

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 attacks by educating users to be extremely cautious about visiting potentially malicious Web sites, following untrusted links or viewing image attachments in unsolicited emails.

¹ 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.

² <http://www.securityfocus.com/bid/14214>

The Microsoft Internet Explorer JView Profiler Javaprx.dll Component Object Model (COM) Object Installation Heap Overflow³ Vulnerability⁴ was made public on June 29, 2005. The JView Profiler is a COM object application included with the Microsoft Java Virtual Machine, which allows Java applications to be used on the Microsoft Windows operating system and through the Microsoft Internet Explorer Web browser. This vulnerability allows an attacker to compromise a browser to gain 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 the vulnerable Internet Explorer Web browser loads a malicious site designed to invoke the vulnerable JView COM object. By passing malicious data an attacker can trigger the vulnerability. Remotely exploitable heap and buffer overflow vulnerabilities are particularly dangerous, as skilled attackers can carry out exploitation without alerting a target user to the attack.

Symantec advises users and administrators to apply the appropriate patches to all affected Microsoft Internet Explorer packages. Administrators should also implement intrusion detection systems to monitor HTTP traffic for potential attacks, and to filter them out before they become successful. 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.

The Mozilla Firefox Set As Wallpaper Arbitrary Code Execution Vulnerability⁵ was first disclosed on July 13, 2005. Mozilla Firefox is a popular, freely available Web browser and although it runs on multiple operating system (OS) platforms including Microsoft Windows, Linux, and Apple Mac OS X, some functionality, including the 'Set As Wallpaper' feature, is not available on all platforms limiting the risk to certain OS platforms. Mozilla Firefox allows users to easily save images presented on Web pages directly as their desktop image or wallpaper. This vulnerability allows an attacker to compromise a browser to gain privileges of the user running the vulnerable Mozilla Firefox. For example, if an administrator was running Mozilla Firefox, the attacker would gain administrator privileges.

Exploitation is carried out through a malicious Web page that includes a malformed image with a JavaScript source URI. Exploitation is triggered when a user sets the malicious image as their desktop image using the 'Set as Wallpaper' feature. When the user right clicks on the malicious images and selects the 'Set as Wallpaper' option, the JavaScript URI is executed with their privileges.

The latter two vulnerabilities discussed in this section affect Web browsers. As outlined in the previous two volumes (September 2004 and March 2005) of the Symantec *Internet Security Threat Report*, Web browser vulnerabilities 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

³ A heap overflow vulnerability is similar to a buffer overflow vulnerability, the only difference is that a different region of memory (heap memory) is affected.

⁴ <http://www.securityfocus.com/bid/14087>

⁵ <http://www.securityfocus.com/bid/14242>

an entire network by exploiting one vulnerable desktop browser; as a result, an unpatched Web browser can be a significant risk primarily due to the widespread deployment inside an organization

Symantec advises users and administrators to upgrade all affected Mozilla Browsers to the latest, patched versions. It may also be possible to prevent attacks that exploit this vulnerability by implementing intrusion detection systems to monitor HTTP for signs of attack, and filter them out before they can become successful. To reduce exposure to attacks, Symantec recommends educating users to be extremely cautious about visiting untrusted Web sites or following links embedded in unsolicited emails.

Top Attacks

Between June 24 and July 23, 2005 the most common attack, both worldwide (table 2) and in the Japan region (table 3), was the SQLExp Incoming Worm Attack, also known as the Slammer Attack. Performed by 30% of the attacking IP addresses located in the Japan region, this attack is commonly associated with three high-profile malicious code samples: Slammer,⁶ Gaobot,⁷ and Spybot.⁸ 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	19%	Microsoft SQL Server
2	Generic HTTP CONNECT TCP Tunnel Attack	11%	Generic Web (HTTP) Service
3	Debian Linux httpd Attack	7%	Generic Web Attack

Table 2. Top attacks worldwide, July 2005

Source: Symantec Corporation

Rank	Top Attacks - Japan	Percentage of Total Region Attackers	Affected Service	World Rank	Percentage of Total World Attackers
1	SQLExp Incoming Worm Attack	30%	Microsoft SQL Server	1	7%
2	Microsoft Windows DCOM RPC Interface Buffer Overrun Attack	6%	Microsoft Remote Procedure Call	6	3%
3	Generic ICMP Flood Attack	5%	Generic TCP Service	10	2%

Table 3. Top attacks originating in Japan, July 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 attack⁹ to be sent to every

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

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

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

⁹ 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.

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 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. A single infected host within a network, such as an infected laptop that is connected to the network, either directly or by VPN, can allow the malicious code to propagate internally. 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 Japan region between June 24 and July 23, 2005 was the Microsoft Windows DCOM RPC Interface Buffer Overrun Attack. Used by 6% of all attacking IP addresses located in the Japan, this attack is strongly correlated with highly successful malicious code, including the Blaster and Welchia worms and many Bot network applications and Trojans. The vulnerability is located in default installations of Windows 2000 and Windows XP and can lead to complete system compromise, including control of an affected computer and disclosure of confidential information if a successful attack occurs.

Administrators should ensure that all computers are appropriately patched with vendor-supplied patches, and strong policy compliance, including desktop firewalls, can reduce the chance of successful attack.

The third most common attack detected originating in the Japan region between June 24 and July 23, 2005 was the Generic ICMP Flood Attack. Detection of this attack is indicative of a denial of service (DoS) attack that results when too much ICMP traffic is directed at a target host. Organizations should ensure that all systems are appropriately configured and tuned to minimize the effectiveness of resource exhaustion from high network load and must engage an upstream network provider to filter the malicious traffic should they find themselves the victim of a DoS attack.

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.

Bot network computers are a concern for a variety of reasons, some directly attributable to infection, and some as an indirect consequence of bot network behavior. A single infected host within a network, such as an infected laptop that is connected to the network, either directly or by VPN, can allow the malicious code to propagate internally. Additionally, bot computers can act in concert to perform DoS attacks utilizing bandwidth of both the target and source computers in the attack.

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

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

Source: Symantec Corporation

Region Rank	City	Percentage of Region's Bots	World Rank	Percentage of World's Bots
1	Tokyo	48%	6	2%
2	Osaka	5%	59	<1%
3	Shibuya	3%	105	<1%

Table 5. Top bot-infected cities, Japan region, July 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. Tokyo is host to by far the most bot-infected computers in Japan. This is not surprising given the fact that Tokyo is by far the largest city in the country.

To prevent against bot infection, Symantec recommends that end users practice defense in-depth,¹⁰ including the deployment of antivirus, firewall and intrusion detection solutions. Security administrators should also ensure that ingress and egress filtering is in place to block known bot-network traffic and that antivirus definitions are updated regularly.

Malicious Code

Worldwide		Japan	
Rank	Sample	Rank	Sample
1	Netsky.P	1	Netsky.P
2	Tooso.J	2	Mytob
3	Lineage	3	Rants.A
4	DesktoPhijack	4	Mytob.AW
5	Spybot	5	Redlof.A
6	Mytob.EE	6	Gaobot
7	Tooso.B	7	Webus.G
8	Gaobot	8	Sacrep
9	Fugif	9	Ahker.D
10	Bancos	10	Mytob.EE

Table 6. Top ten malicious code, July 2005

Source: Symantec Corporation

Netsky.P¹¹ remains one of the most widely reported malicious code samples by Symantec customers. 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 itself to shared folders used by various peer-to-peer file-sharing applications in order to make itself available for download on those networks.

Three variants of the Mytob mass-mailing worm were present in the top ten malicious code reports from Japan for July. This worm also includes an IRC bot to allow a remote

¹¹ <http://securityresponse.symantec.com/avcenter/venc/data/w32.netsky.p@mm.html>

attacker to control the compromised computer. Additionally, Mytob¹² and Mytob.AW¹³ also propagate by exploiting the Microsoft Windows Local Security Authority Service Buffer Overflow Vulnerability¹⁴ while Mytob.EE¹⁵ only sent itself in a mass mailing.

The third most prevalent malicious code sample reported to Symantec from Japan was Rants.A¹⁶. This mass-mailing worm propagates by purporting to be an email message from Microsoft claiming that the attachment is Microsoft SP2. If the compromised computer has America Online software installed, the worm will also send a link to other AOL users through the AOL interface. If a user clicks the link, a variant of Spybot¹⁷ is downloaded. Rants.A also disables the features of the Windows Security Center on Windows XP computers with Service Pack 2 installed as well as other security and antivirus applications.

The Webus.G¹⁸ Trojan was discovered on June 10, 2005. It was sent as an attachment to a spam email claiming falsely that Michael Jackson tried to commit suicide. The Trojan deletes services from the computer related to antivirus and security applications, then connects to an IRC server from which it can receive remote commands. The bot can allow a remote attacker to download and execute remote files on the computer or relay spam email.

The Sacrep¹⁹ Trojan was only reported to Symantec from Japan; no reports of this Trojan originated from any other region. This Trojan likely originated in Japan and uses Japanese characters in the names of files it creates during installation. The Trojan logs keystrokes entered on the compromised computer and stores them in a log file. This log file is then emailed to an address in the itpmail.itp.ne.jp domain.

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

¹³ <http://securityresponse.symantec.com/avcenter/venc/data/w32.mytob.aw@mm.html>

¹⁴ <http://www.securityfocus.com/bid/10108>

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

¹⁶ <http://securityresponse.symantec.com/avcenter/venc/data/w32.rants.a@mm.html>

¹⁷ <http://securityresponse.symantec.com/avcenter/venc/data/w32.spybot.worm.html?Open>

¹⁸ <http://securityresponse.symantec.com/avcenter/venc/data/trojan.webus.g.html>

¹⁹ <http://securityresponse.symantec.com/avcenter/venc/data/trojan.sacrep.html>

Spam

The Symantec Probe Network consists of millions of decoy email addresses that are configured to attract a large stream of spam attack; 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 between June 24 and July 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 Japan region. During the month of July, the most common spam worldwide (figure 1) was related to commercial products (merchandise not included in other categories, such as fake Rolex watches, printer supplies, jewelry and other consumer goods), accounting for 24% of the spam worldwide. Spam related to financial products or services was the second most common type, making up 22% of all worldwide spam messages, this category includes mortgages, stock tips and credit card offers. Finally, spam related to scams, including the common 419, or Nigerian scam, made up 11% of global spam messages. The scam category includes home-based businesses, offers to run a online casino from your PC, and other get-rich schemes.

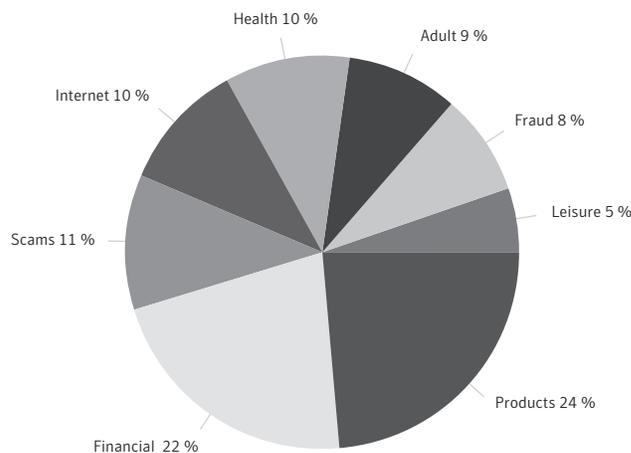


Figure 1. Worldwide spam by type, July 2005

Source: Symantec Corporation

A very similar pattern was detected in the Japan region. During the month of July, the most common type of spam messages detected by probes in Japan (figure 2) was related to commercial products, which accounted for 22% of detected message. Financial services made up the second most common type, 21%. The third most common type of spam messages during this period was related to Internet-delivered products and services, such as software, ringtone downloads, and online greeting cards, which accounted for 12% of spam detected in the Japan region.

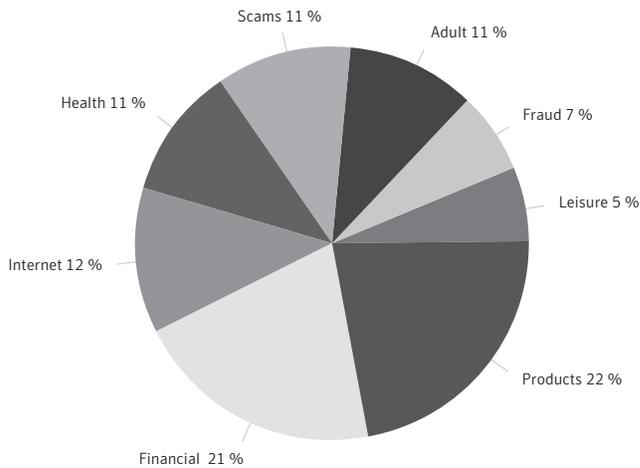


Figure 2. Japan spam by type, July 2005

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 (figure 3). 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.

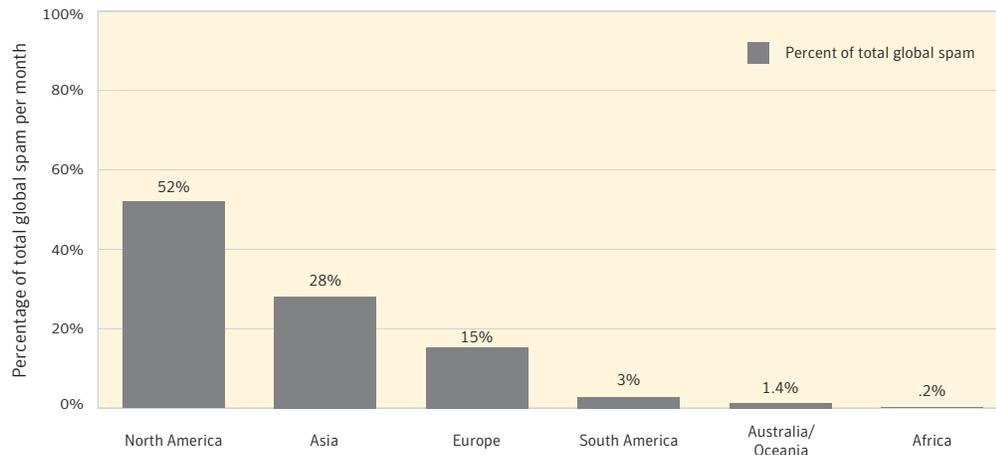


Figure 3. Region of spam origin, July 2005

Source: Symantec Corporation

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 IPs).

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 800 745 6054.

Symantec Corporation
World Headquarters
20330 Stevens Creek Boulevard
Cupertino, CA 95014 USA
408 517 8000
800 721 3934
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. 08/05 10433489