



Confidence in a connected world.

Symantec Internet Security Threat Report

April 2010

Regional Data Sheet—Asia-Pacific/Japan

An important note about these statistics

The statistics discussed in this document are based on attacks against an extensive sample of Symantec customers. The attack activity was detected by the Symantec™ Global Intelligence Network, which includes Symantec Managed Security Services and Symantec DeepSight™ Threat Management System, both of which use automated systems to map the IP address of the attacking system to identify where it is located. However, because attackers frequently use compromised systems situated around the world to launch attacks remotely, the location of the attacking system may differ from the location of the attacker.

Introduction

Symantec has established some of the most comprehensive sources of Internet threat data in the world through the Symantec Global Intelligence Network. More than 240,000 sensors in over 200 countries and territories monitor attack activity through a combination of Symantec products and services such as Symantec DeepSight Threat Management System, Symantec Managed Security Services and Norton™ consumer products, as well as additional third-party data sources.

Symantec also gathers malicious code intelligence from more than 133 million client, server, and gateway systems that have deployed its antivirus products. Additionally, Symantec's distributed honeypot network collects data from around the globe, capturing previously unseen threats and attacks and providing valuable insight into attacker methods.

Spam and phishing data is captured through a variety of sources including: the Symantec Probe Network, a system of more than 5 million decoy accounts; MessageLabs Intelligence, a respected source of data and analysis for messaging security issues, trends and statistics; and other Symantec technologies. Data is collected in more than 86 countries. Over 8 billion email messages, as well as over 1 billion Web requests, are processed per day across 16 data centers. Symantec also gathers phishing information through an extensive antifraud community of enterprises, security vendors and more than 50 million consumers.

These resources give Symantec's analysts unparalleled sources of data with which to identify, analyze, and provide informed commentary on emerging trends in attacks, malicious code activity, phishing, and spam. The result is the Symantec *Internet Security Threat Report*, which gives enterprises and consumers the essential information to effectively secure their systems now and into the future.

In addition to gathering Internet-wide attack data for the Symantec *Global Internet Security Threat Report*, Symantec also gathers and analyzes attack data that is detected by sensors deployed in specific regions. This regional data sheet will discuss notable aspects of malicious activity Symantec has observed in the Asia-Pacific/Japan (APJ) region for 2009. This is designed to provide a balanced view of the trends in the threat activity landscape that Symantec has observed in the APJ region in comparison to global activity.

Highlights

Threat Activity Trends Highlights

- Globally in 2009, United States ranked first for overall malicious activity as measured by Symantec, with 19 percent of the total, while China ranked second worldwide, with 8 percent. In APJ, China ranked first for malicious activity in 2009, with 32 percent of the regional total, which is down from 41 percent in 2008. The United States and China are always likely to rank highly due to population size, number of computer users, and high broadband penetration. China has the most broadband subscribers in the world (significantly more than anywhere else in the APJ region) and malicious activity tends to increase in relation to growth in broadband infrastructure.
- The United States ranked first for originating attacks detected by APJ-based sensors in 2009, accounting for 26 percent of all detected attacks, down from 28 percent in 2008. Globally, the United States also ranked first in 2009 for originating attacks against global targets in 2009, with 23 percent of the worldwide total.
- The most common Web-based attack against users in APJ in 2009 was associated with the MSIE ADODB.Stream Object File Installation Weakness vulnerability, which accounted for 23 percent of the regional total. In 2008, the most common Web-based attack against users in APJ in 2008 was associated with the Adobe® SWF Remote Code Executable Vulnerability, which accounted for 32 percent of the regional total at that time.
- The United States again ranked first for Web-based attacks globally in 2009, accounting for 34 percent of the worldwide total. China ranked second globally in 2009, with 7 percent, which is a decrease from 13 percent in 2008. In the APJ region, although China ranked first for Web-based attacks in 2009, its 37 percent total for this reporting period is a significant decrease from 2008, when it accounted for 79 percent of the total for the APJ region.
- In 2009, Symantec observed an average of 10,440 active bots per day in the APJ region. This is an 11 percent decrease from 2008, when Symantec observed an average of 11,683 active bot-infected computers per day in the region.
- Globally in 2009, China ranked second for bot-infected computers, with 11 percent of the worldwide total. In APJ during this period, China ranked first for bot-infected computers, with 41 percent of the regional total, which represents a double-digit decrease from its 58 percent total in 2008.
- Taipei was the top city in the APJ region for bot-infected computers in 2009, with 19 percent of the total. This is more than double its 9 percent total in 2008, when it also ranked first in the region for bot-infected computers. Taipei also ranked first globally in 2009, accounting for 5 percent of all bot-infected computers observed.
- In 2009, Symantec identified 7,402 distinct bot command-and-control servers in the APJ region, of which 36 percent were controlled through IRC channels and 64 percent through HTTP. In 2008, Symantec identified 3,567 distinct bot command-and-control servers in APJ, of which 30 percent were operated through IRC channels and 70 percent through HTTP.
- Globally in 2009, the United States had the most bot command-and-control servers, with 34 percent of the worldwide total observed by Symantec. In the APJ region in 2009, China ranked first for bot command-and-control servers, with 27 percent of the regional total—a slight increase from 24 percent in 2008. As with malicious activity in general, this percentage is most likely due to China being the world's most populous country and that it continues to enjoy high broadband penetration growth rates.

Malicious Code Trends Highlights

- Worms were the most common type of malicious code in the APJ region in 2009, accounting for 51 percent of the volume of the top 50 potential infections. This is an increase from 43 percent in 2008, when worms ranked second to Trojans.
- The rankings for malicious code types in the APJ region remained unchanged in 2009 from the previous reporting period; China ranked first for back doors and Trojans, and India ranked first for viruses and worms.
- The Sality.AE virus was the top malicious code sample by potential infection in the APJ region in 2008, replacing the Gampass Trojan from the year previous. Sality.AE was the top malicious code sample causing potential infection globally in 2009.
- The Induc virus was the top new malicious code family reported in the APJ region in 2009, as it was globally.
- In the APJ region in 2009, 90 percent of confidential information threats allowed remote access. This is substantially higher than 2008, when 69 percent of confidential information threats allowed remote access.
- The most common propagation method for malicious code in the APJ region in 2009 was again through file-sharing executables, which accounted for 67 percent of potential infections—an increase from 65 percent in 2008.

Phishing and Spam Trends Highlights

- In 2009, South Korea hosted the highest percentage of phishing URLs, with 43 percent of the total. This is a substantial increase from 29 percent in 2008, when South Korea ranked second behind China, which decreased to 12 percent in 2009 from 35 percent previously. Of the phishing URLs identified in South Korea in 2009, 91 percent targeted the financial services sector.
- In 2009, 21 percent of all spam detected worldwide originated in the APJ region. Within the region in 2009, India ranked first for originating spam, with 21 percent of the regional total. In 2008, China ranked first, with 22 percent of the regional total. Globally in 2009, India accounted for 4 percent of spam detected and ranked third.

Threat Activity Trends

This section will discuss the following metrics:

- Malicious activity
- Originating attacks
- Web-based attacks by type
- Web-based attacks by region
- Bot-infected computers
- Bot-infected computers by region

Malicious activity

This metric will assess where the highest amount of malicious activity took place or originated in the APJ region in 2009. To determine this, Symantec has compiled geographical data on numerous malicious activities, including malicious code reports, spam zombies, phishing website hosts, bot-infected computers, and originating attacks. The rankings are determined by calculating the average of the proportion of these malicious activities that originated in each location.

Globally in 2009, United States had the most overall malicious activity as measured by Symantec, with 19 percent of the worldwide total; China ranked second globally, with 8 percent. In APJ, China ranked first for malicious activity in 2009, accounting for 32 percent of the total, down from 41 percent in 2008 (table 1). On a per-category basis within the APJ region, China ranked first in bot-infected computers and originating attacks, while ranking second in malicious code, spam zombies, and phishing hosts.

China is likely to continue to rank first in malicious activity simply because malicious activity tends to increase in relation to growth in broadband infrastructure and China has the most broadband subscribers in the world (and, it should be noted, significantly more than anywhere else in the APJ region).¹ Malicious activity usually affects computers that are connected to high-speed broadband Internet because these connections make attractive targets for attackers. This is because broadband connections typically provide larger bandwidth capacities than other connection types, faster speeds, the potential of constantly connected systems, and more stable connections. Moreover, new or inexperienced users may be unaccustomed to, or unaware of, the increased risk of exposure to malicious attacks from such robust connections and unknowingly allowing inroads for attack.

The decrease in China's percentage share of malicious activity in 2009 can be explained by the increase in malicious code activity and spam zombies in India during this reporting period. This is because activity in these categories increased in India during this reporting period, as it rose to first rank in both, up from second in 2008. There was also a decrease in spam zombies in China in 2009. Spam zombies in China are expected to decline further in 2010 because of an enhanced domain registration procedure introduced by the China Internet Network Information Center (CNNIC) in December 2009.² Early observations indicate that the daily volume of spam originating from .cn domains fluctuated around 20 percent after the changes were implemented, down from an average of around 40 percent prior to the changes. This could also affect the number of phishing URLs being hosted in China in the future.

¹ <http://www.point-topic.com>

² <http://www.symantec.com/connect/blogs/drop-cn-spam>

APJ Rank		Global Rank 2009	Region	Percentage		2009 Activity Rank				
2009	2008			2009	2008	Malicious Code	Spam Zombies	Phishing Hosts	Bots	Attack Origin
1	1	2	China	32%	41%	2	2	2	1	1
2	3	5	India	15%	10%	1	1	6	5	6
3	2	14	South Korea	11%	11%	8	4	1	4	3
4	4	11	Taiwan	11%	8%	7	6	3	2	4
5	5	15	Japan	8%	7%	3	8	4	3	2
6	7	21	Thailand	5%	4%	11	5	5	6	8
7	8	20	Vietnam	5%	3%	9	3	12	11	7
8	6	22	Australia	4%	5%	4	11	7	8	5
9	12	32	Indonesia	3%	2%	6	7	8	12	9
10	10	33	Philippines	2%	2%	5	10	9	10	11

Table 1. Malicious activity, APJ

Source: Symantec Corporation

India ranked second for malicious activity in the APJ region in 2009, accounting for 15 percent of the total, an increase from 10 percent in 2008. India ranked sixth globally in 2009, with 4 percent of that total. For specific categories of measurement in the region, India increased one rank in malicious code, spam zombies and phishing hosts from 2008, while it dropped one rank in bot activity. As noted above, malicious activity tends to increase in areas experiencing rapid growth in broadband infrastructure and connectivity, and India has experienced significant growth in these areas over the past few years.³

South Korea ranked third for malicious activity in the APJ region in 2009, with 11 percent of the total. This is the same percentage as in 2008, when South Korea ranked second. For specific categories of measurement, South Korea ranked first for phishing hosts, up from second 2008. It ranked slightly less for other categories than in the previous year, although the percentage differences represent typical variances in activity from one reporting period to the next.

Originating attacks

This metric discusses the location of originating attacks that are targeting the APJ region. An attack is generally considered to be any malicious activity carried out over a network that has been detected by an intrusion detection system (IDS), intrusion prevention system (IPS) or firewall.

In 2009, the United States ranked first for attacks detected by APJ-based sensors, accounting for 26 percent of all detected attacks in the region—a decrease from 28 percent in 2008 (table 2). Globally in 2009, the United States ranked first for originating attacks against worldwide targets, with 23 percent of that total. As has been the case in previous reporting periods, the proportion of attacks originating in the United States that were detected by APJ-based sensors were similar to Internet-wide attacks originating there, which indicates that attacks from the United States are not targeting the APJ region in particular.

³ See <http://point-topic.com/dslanalysis.php> and <http://www.indiabroadband.net/india-broadband-telecom-news/11682-india-register-500-growth-broadband-services-within-5-years.html>

APJ Rank		Region	Percentage		
2009	2008		2009 APJ	2008 APJ	2009 Global
1	1	United States	26%	28%	23%
2	4	Japan	15%	5%	3%
3	2	China	11%	15%	12%
4	3	South Korea	11%	11%	2%
5	5	Australia	6%	4%	2%
6	14	Singapore	4%	2%	<1%
7	11	Taiwan	3%	2%	2%
8	16	India	2%	1%	1%
9	12	France	2%	2%	4%
10	6	United Kingdom	2%	3%	6%

Table 2. Originating attacks targeting APJ

Source: Symantec

Japan ranked second for attack origination in the APJ region in 2009, with 15 percent of the total; this is an increase from 2008, when it ranked fourth with 5 percent of the total. Globally in 2009, Japan accounted for 3 percent of originating attacks. This indicates that attacks originating in Japan are being specifically directed at targets in the APJ region. Previous editions of the Symantec *Global Internet Security Threat Report* have noted that attacks originating in a location often target the region in which they originate due to proximity, shared language, or similar social and cultural interests.⁴ It is also likely that targets within the region are of more interest to attackers based there than are external targets. Japan's increased percentage in attack origin in the region in 2009 is also partly due to the drop in percentage of attacks targeting the region that originated from China during this reporting period.

APJ-targeted attacks originating in China dropped from 15 percent and second rank in 2008 to 11 percent and third rank in 2009. In previous reporting periods, China accounted for a substantially larger proportion of APJ-targeted attacks than attacks directed globally. However, the proportion of APJ-directed attacks originating in China in 2009 was very similar to its percentage for worldwide attacks, indicating that attacks originating in China were not focusing on APJ targets in particular. This would explain its drop in regional percentage and rank in 2009 in this measurement.

Web-based attacks by type

This metric will assess the top distinct Web-based attacks that targeted Web users in the APJ region that originated from compromised legitimate sites, as well as websites that were intentionally developed for malicious purposes. The increasing pervasiveness of Web browser applications along with increasingly common, easily exploited Web browser application security vulnerabilities has resulted in the widespread growth of Web-based threats.

⁴ http://eval.symantec.com/mktginfo/enterprise/white_papers/ent-whitepaper_symantec_internet_security_threat_report_v.pdf : p. 11

Asia-Pacific/Japan Data Sheet

In 2009, the most common Web-based attack targeting the APJ region was related to the Microsoft® Internet Explorer® ADODB.Stream Object File Installation Weakness vulnerability, which accounted for 23 percent of the total (table 3).⁵ This attack was ranked second for Web-based attacks observed globally in 2009, accounting for 18 percent of the worldwide total. It did not rank in the top 10 in the APJ region in 2008. This weakness allows attackers to install malicious files on a vulnerable computer when a user visits a website hosting an exploit. This issue was published on August 23, 2003 and fixes have been available since July 2, 2004.

Rank	Attack	Percentage
1	MSIE ADODB.Stream Object File Installation Weakness	23%
2	HTTP MSIE7 Uninitialized Memory Code Execution	22%
3	PDF Suspicious File Download	16%
4	HTTP MS MPEG2TuneRequestControl ActiveX Buffer Overload	10%
5	HTTP Adobe SWF Remote Code Execution	7%
6	HTTP MSIE Malformed XML Buffer Overload	4%
7	HTTP MSIE WPAD Spoofing	3%
8	HTTP MS MPEG2TuneRequestControl ActiveX Instantiation	2%
9	MSIE BaoFeng MPS ActiveX Buffer Overload	2%
10	MSIE Baidu Soba Search Bar ActiveX Buffer Overload	1%

Table 3. Top Web-based attacks, APJ

Source: Symantec

The second most common Web-based attack in the APJ region in 2009 was related to the Microsoft Internet Explorer 7 Uninitialized Memory Code Execution vulnerability, which accounted for 22 percent of the regional total.⁶ It was the third most common Web-based attack globally in 2009, accounting for 6 percent of the worldwide total. This vulnerability was not ranked in the top Web-based attacks observed in the region in 2008. It was published on February 10, 2009 and fixes have been available since that time. One week later, the issue was being actively exploited in the wild and exploit code was publicly available on February 18, 2009.

The third most common Web-based attack in the APJ region in 2009 was related to malicious PDF download activity,⁷ which accounted for 16 percent of the regional total—up from fourth rank and 2 percent in 2008. This attack ranked first globally in 2009, with 49 percent of the worldwide total. This attack consists of attempts by attackers to distribute malicious PDF content to victims through the Web. The attack is not directly related to any specific vulnerability, although the contents of the malicious PDF file would be designed to exploit arbitrary vulnerabilities in applications that are able to process PDFs. Successful attacks could ultimately result in the compromise of the integrity and security of the affected computers. This attack is assumed to be popular to due the common use and distribution of PDF documents on the Web, especially because most browsers can be set-up to automatically render a PDF document by default.

⁵ See http://www.symantec.com/business/security_response/attacksignatures/detail.jsp?asid=50031 or <http://www.securityfocus.com/bid/10514>

⁶ See http://www.symantec.com/business/security_response/attacksignatures/detail.jsp?asid=23291 or <http://www.securityfocus.com/bid/33627>

⁷ http://www.symantec.com/business/security_response/attacksignatures/detail.jsp?asid=23153

Web-based attacks by region

This metric will assess where the most Web-based attacks against users in the APJ region are originating by determining the location of computers from which the attack occurred. Note that the server used for the attack may not necessarily be the same server that the user has visited due to redirection. A user could visit a website that redirects his or her browser to a malicious server in another location.

Globally in 2009, China ranked second for Web-based attacks with 7 percent of the worldwide total. In 2009, China ranked first for Web-based attacks against users in APJ, accounting for 37 percent of the regional total (table 4). This is a significant decrease from the 79 percent recorded in 2008. The main reason for the higher percentage in 2008 was likely due to compromised websites relating to the 2008 Beijing Olympic Games. It is reasonable to assume that the number of attacks from these websites has tapered off since the conclusion of the games and may be a significant factor in the decrease of Web attacks originating from computers in China in 2009.

Overall Rank		Region	Percentage	
APJ	Global		APJ	Global
1	2	China	37%	7%
2	7	India	16%	3%
3	12	Japan	10%	2%
4	15	South Korea	9%	2%
5	16	Taiwan	8%	2%
6	20	Philippines	6%	1%
7	25	Australia	4%	1%
8	26	Indonesia	3%	1%
9	32	Thailand	2%	0%
10	36	Singapore	2%	0%

Table 4. Top Web-based attacks by region, APJ

Source: Symantec

In 2009, India ranked second for Web-based attacks in APJ, with 16 percent of the regional total. This is a significant increase from the previous reporting period, when India accounted for less than 1 percent of Web-based attacks in the region. Globally in 2009, India ranked seventh with 3 percent of the worldwide total. In previous reports, Symantec discussed indications that malicious activity in India was likely to increase substantially as broadband Internet infrastructure and usage grew. This was true in 2009, with India increasing its percentage share in malicious activity across a number of different categories that Symantec measures, including overall malicious activity, spam zombies, phishing URLs, and originating attacks.

Japan ranked third for Web-based attacks in the APJ region in 2009, with 10 percent of the total. This percentage is similar to 2008, when Japan accounted for 9 percent of Web-based attacks in APJ and ranked second in this metric. The small variance in percentage and large increase of activity in India indicate that Web-based attack activity in Japan remained consistent with 2008, despite the drop in rank.

Bot-infected computers

A bot-infected computer is considered active on a given day if it carries out at least one attack on that day. This does not have to be continuous; rather, a single such computer can be active on a number of different days.

In 2009, 26 percent of bot-infected computers observed globally were located in the APJ region (figure 1). Symantec observed an average of 10,440 active bots per day in the APJ region. This is an 11 percent decrease from 2008, when Symantec observed an average of 11,683 active bot-infected computers per day in the region.

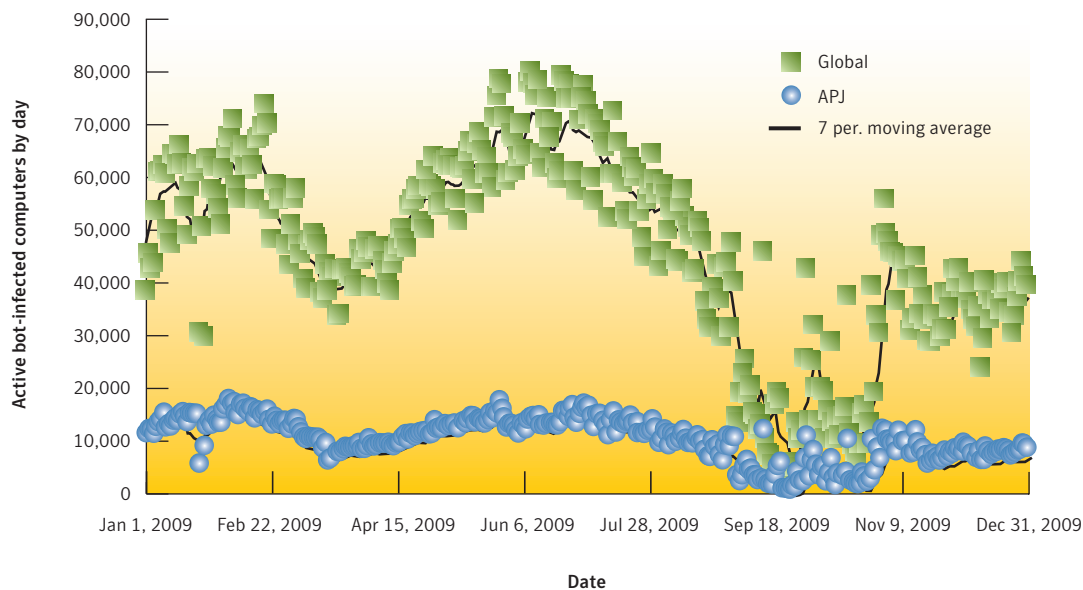


Figure 1. Active bot-infected computers, APJ and global

Source: Symantec

Symantec also measures distinct bot-infected computers, which are computers that were active at least once during the reporting period. There were 1,756,793 distinct bot-infected computers recorded in the APJ region in 2009. This is 15 percent less than the 2,075,968 observed in the region in 2008.

It is worth noting that while the global pattern in active bot-infected computers showed considerable variability in 2009, the rate of activity in the APJ region was relatively steady. The global variance was strongly influenced by the activity of the Peacomm Trojan (a.k.a., the Storm botnet),⁸ as well as by the shutdown of two U.S.-based Web hosting companies late in 2008 that were responsible for hosting command-and-control (C&C) servers for a number of major botnets.⁹ The latter event likely contributed to the decrease in active bot-infected computers globally in September and November 2009, and would explain the drop in APJ numbers at that time.

⁸ http://www.symantec.com/security_response/writeup.jsp?docid=2007-041314-1900-99

⁹ See http://eval.symantec.com/mktginfo/enterprise/other_resources/b-state_of_spam_report_12-2008.en-us.pdf and http://eval.symantec.com/mktginfo/enterprise/white_papers/b-whitepaper_internet_security_threat_report_xiv_04-2009.en-us.pdf

Bot-infected computers by region

Globally, China ranked second for bot-infected computers, with 11 percent of the worldwide total. In 2009, China ranked first for bot-infected computers in the APJ region, accounting for 41 percent of the total, which is a double-digit decrease from 58 percent in 2008 (table 5). The decrease in percentage in bot-infected computers in China is partly due to increases elsewhere in the APJ region, specifically in Taiwan and Japan, both of which significantly increased their percentages for bot-infected computers in the region in 2009.

APJ Rank		Global Rank 2009	Region	Percentage		
2009	2008			2009 APJ	2008 APJ	2009 Global
1	1	2	China	41%	58%	11%
2	2	4	Taiwan	28%	12%	7%
3	5	11	Japan	11%	4%	3%
4	3	16	South Korea	6%	8%	2%
5	4	20	India	4%	5%	1%
6	8	27	Thailand	2%	2%	1%
7	6	28	Singapore	2%	3%	1%
8	7	30	Australia	2%	3%	<1%
9	9	33	Malaysia	1%	2%	<1%
10	10	38	Philippines	1%	1%	<1%

Table 5. Bot-infected computers by region, APJ

Source: Symantec

Taiwan had the second-highest percentage of bot-infected computers in the APJ region in 2009, with 28 percent of the total. This is a significant increase from 2008, when 12 percent of the region's bot-infected computers were in Taiwan. Globally in 2009, Taiwan accounted for 7 percent of the worldwide total. Taipei, Taiwan was again the top city for bot-infected computers in APJ and worldwide in 2009, with 19 percent and 5 percent, respectively.

Taiwan has ranked second in this category for a number of reports. The high bot activity in Taiwan may be due to the high broadband penetration there. Previously, the Symantec *Global Internet Security Threat Report* attributed this to the increasing levels of fiber-to-the-home/building (FTTH/B) deployment in Taiwan.¹⁰ As noted, malicious activity tends to grow with increased broadband capacity and FTTH/B connections currently provide the highest bandwidth capacities over traditional DSL or cable lines.

Japan had the third-highest percentage of bot-infected computers in the APJ region in 2009, with 11 percent of the total. This is an increase from 4 percent in 2008, when Japan ranked fifth in the region. Globally in 2009, Japan had three percent of the total for bot-infected computers. Japan's high rank may also be explained by its advanced Internet infrastructure as well as by the significant deployment of FTTH/B there.

¹⁰ <http://www.ftthcouncil.org/en/newsroom/2010/02/26/g-20-need-to-speed-up-on-fiber-to-the-home>

Malicious Code Trends

This section will discuss the following metrics:

- Malicious code types
- Geolocation by type of malicious code
- Malicious code samples
- New malicious code families
- Threats to confidential information
- Propagation mechanisms

Malicious code types

Worms were the most common type of malicious code observed in the APJ region in 2009, accounting for 51 percent of the volume of the top 50 potential infections (figure 2); this is an increase from 43 percent in 2008, when worms ranked second to Trojans in the region. This is also a higher percentage than the global total for worms of 43 percent in 2009.

One of the primary contributors to this increase may be the rapid spread of the Downadup (a.k.a., Conficker) worm,¹¹ which is designed with certain geolocation features that enable it to target specific regions, one of which is China.¹² Moreover, eight of the top 10 malicious threats in the region in 2009 were worms, or had a worm component, up from seven in 2008. In addition, the volume of worm activity in the region increased by approximately 10 percent in 2009. The increased worm activity also explains a degree of the percentage decreases in the other threat types in the region in 2009.

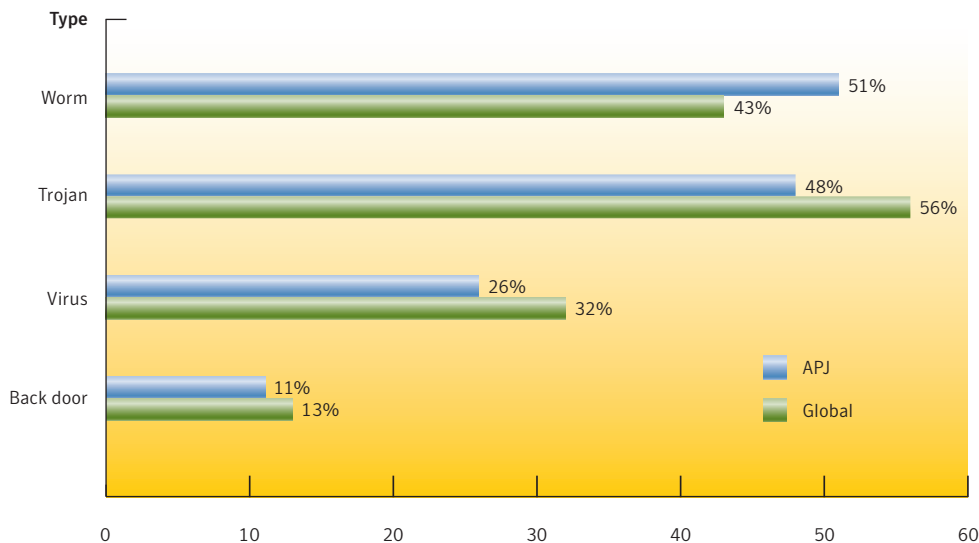


Figure 2. Potential infections by type, APJ
Source: Symantec

¹¹ http://www.symantec.com/security_response/writeup.jsp?docid=2008-112203-2408-99
¹² http://www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/the_downadup_codex_ed2.pdf

Trojans were the second most common type of malicious code in the APJ region in 2009, accounting for 48 percent of the volume of the top 50 potential infections, which is a decrease from 55 percent in 2008. The global percentage for Trojans in 2009 was 56 percent. As noted above, the decrease in the percentage for Trojan activity is mostly due to increased worm activity in the APJ region in 2009.

Viruses were the third-ranked potential infection by type in 2009, with 26 percent of the total, which is an increase from 19 percent in 2008. Globally in 2009, viruses accounted for 32 percent of the volume of the top 50 potential infections. These percentages are in keeping with the number of the top samples being classified as viruses: four samples were classified as a virus in the top 10 malicious code samples observed in the APJ region in 2009, compared to five viruses in the top 10 samples globally.

Geolocation by type of malicious code

This metric examines the top locations for potential malicious code infections in the APJ region by malicious code type. Table 6 shows the top reporting locations in the APJ region in 2009 for each of the main malicious code categories.

Rank	Location by Type			
	Back doors	Trojans	Viruses	Worms
1	China	China	India	India
2	India	India	Indonesia	China
3	Japan	Japan	China	Japan

Table 6. Geolocation by type of malicious code, APJ

Source: Symantec

Worms

India had the highest number of potential worm infections in the APJ region in 2009, which is unchanged from 2008. China and Japan were ranked second and third for potential worm infections in 2009, respectively. India's prominence in this measurement is likely due to its increase in malicious code activity, as it rose in that measurement to first rank in 2009, from second in 2008 (as is discussed in "Malicious activity" previously).

Trojans

For Trojans in the APJ region in both 2009 and 2008, China, India, and Japan were the top three locations, in that order. By volume in 2009, as with 2008, Trojan counts for China were almost three times that of India and Japan, with the latter two again having comparable counts from year to year. As was discussed in the previous volume of the Symantec *Global Internet Security Threat Report*, the close interrelation between Trojans and back doors likely contributes to the similarity of proportions for attack counts between these two attack types.¹³

Viruses

The top three ranked locations for the number of potential virus infections in the APJ region in 2009 were India, Indonesia, and China, in that order. Over the past few reporting periods, Indonesia moved from eighth rank in 2007, to third in 2008, and now second in 2009, overtaking China. China's potential virus infection numbers have decreased from 2008, which may explain the rise in rank of Indonesia. Meanwhile, India's potential infection counts for viruses have again risen and it now has a significantly higher detection count than anywhere else in the APJ region, indicating that India may remain in top rank in this measurement for the near future.

Back doors

For back doors in the APJ region in 2009, the top three ranked locations were China, India, and Japan, in that order. These rankings are unchanged from 2008. By volume, China had almost twice the count as both India and Japan in 2009, with both of the latter two having similar numbers. These are similar proportions to 2008. One reason for the preponderance of China for back doors may be due to the spread of the Downadup worm and its ability to target China, as noted in the "Malicious code types" discussion. Although classified as a worm, Downadup also includes a back door component, so it affects both back door and worm numbers.

Malicious code samples

In 2009, Symantec created 2,895,802 new malicious code signatures. This is a 71 percent increase over 2008, when 1,691,323 new malicious code signatures were added. Although the percentage increase in signatures added is less than the 139 percent increase from 2007 to 2008, the overall number of malicious code signatures by the end of 2009 grew to 5,724,106. This means that of all the malicious code signatures created by Symantec, 51 percent of that total was created in 2009.

The most common malicious code sample by potential infection in the APJ region in 2009 was the Sality.AE virus (table 7), moving up from ninth rank in 2008.¹⁴ It was also the top malicious code sample causing potential infection globally in 2009. Sality.AE is designed to download and install additional malicious software on a victim's computer, as well as to prevent access to various security-related domains, stop security-related services, and delete security-related files in the process. The virus infects .exe and .scr files on a compromised local (C) drive as well as on any writable networked resource. Sality.AE also copies itself to attached removable drives.

¹⁴ http://www.symantec.com/security_response/writeup.jsp?docid=2008-042106-1847-99

Asia-Pacific/Japan Data Sheet

Rank	Sample	Type	Infection Vectors	Top Ranked Region	Second Ranked Region	Impact
1	Sality.AE	Virus, worm	Executables	India	Indonesia	Removes security applications and services
2	SillyFDC	Worm	Mapped and removable drives	India	China	Downloads and installs additional threats
3	Downadup	Worm, back door	P2P, CIFS, remote vulnerabilities	India	Indonesia	Downloads and installs additional threats
4	Gampass	Trojan	N/A	China	India	Steals online game account credentials
5	Almanahe	Worm, virus	CIFS	India	Indonesia	Downloads and installs additional threats
6	Fujacks	Worm, virus	CIFS, executables	China	India	Lowers security settings, downloads and installs further security threats
7	Gammima	Worm, virus	Removable drives	India	Taiwan	Steals online game account credentials
8	Imaut	Worm	Instant messages, remote vulnerabilities	India	Philippines	Ends security-related processes, shows ads, and generates ad clicks
9	SillyDC	Worm	Removable drives	China	India	Downloads and installs additional threats
10	Brisv	Trojan	N/A	India	China	Modifies multimedia files, causing multimedia players to open malicious URLs

Table 7. Top malicious code samples, APJ

Source: Symantec

The second-ranked malicious code sample causing potential infection in APJ during 2009 was the SillyFDC worm.¹⁵ SillyFDC was the third-ranked sample globally in 2009. It did not rank in the top 10 for malicious code samples by potential infection in the region in 2008. SillyFDC propagates by copying itself to any removable media storage devices attached to a compromised computer. Once the worm is installed on a computer, it also attempts to download and install additional threats. Malicious code threats such as SillyFDC have likely been developed to capitalize on the resurgent use of (and the ability to exploit) removable media such as portable USB hard drives and flash drives.

The third most frequently reported malicious code sample causing potential infection in the APJ region in 2009 was the Downadup worm. It propagates by exploiting a remote vulnerability in Microsoft Windows, as well as through peer-to-peer (P2P), Common Internet File Sharing (CIFS) and through a back door component.¹⁶ Downadup spread late in 2008 and into early 2009, with China being one of the most affected areas in the region.¹⁷ A patch for the vulnerability that Downadup exploits was made available on October 23, 2008.¹⁸

¹⁵ http://www.symantec.com/security_response/writeup.jsp?docid=2006-071111-0646-99

¹⁶ CIFS is a file-sharing protocol that allows files and other resources on a computer to be shared with other computers across the Internet. One or more directories on a computer can be shared to allow other computers to access the files within.

¹⁷ http://www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/the_downadup_codex_ed2.pdf : p. 12

¹⁸ <http://technet.microsoft.com/en-us/security/dd452420.aspx>

New malicious code families

In 2009, the Induc¹⁹ virus was the most common new malicious code sample by potential infection observed in the APJ region (table 8). This virus also ranked first globally during this reporting period. Induc infects the Delphi compilation process so that all files compiled with Delphi will also be infected. The virus propagates as the infected applications are distributed. South Korea was responsible for the most potential infections of Induc in the region in 2009, followed by China.

Rank	Sample	Type	Infection Vectors	Top Ranked Region	Second Ranked Region	Impact
1	Induc	Virus	Delphi compiled applications	South Korea	China	Infects the Delphi compilation process
2	Zbot	Trojan	N/A	Japan	Australia	Steals confidential information and downloads additional files
3	Ergrun	Trojan	N/A	Japan	India	Downloads additional files
4	Bredolab	Trojan	N/A	Japan	Australia	Downloads additional files
5	Pilleuz	Worm, back door	P2P, IM, removable drives	India	Malaysia	Opens a back door, copies itself to shared folders and sends IM messages with links to itself
6	Kuaiput	Trojan	N/A	Taiwan	China	Downloads additional files
7	Changeup	Worm	Mapped and removable drives	India	Singapore	Contacts external URLs
8	Fostrem	Trojan	N/A	China	India	Exploits an ActiveX vulnerability and downloads additional files
9	Swifi	Trojan	N/A	China	Australia	Exploits a vulnerability in Adobe Flash® Player
10	Palevo	Worm	Exploits vulnerabilities	India	Australia	Lowers security settings and checks for further commands

Table 8. Top new malicious code families, APJ

Source: Symantec

The second most common new malicious code family in the APJ region in 2009 was the Zbot Trojan.²⁰ Zbot is designed to steal sensitive information relating to online banking, social networking sites, Web-based email, and saved passwords. It also downloads further threats based on a configuration file that allows malicious software authors to easily modify its behavior. Zbot is also sold as the Zeus toolkit on underground forums, where it is advertised as allowing novices to create customized Trojans and C&C servers.²¹ Zeus has become a prevalent threat that is responsible for widespread bot networks and is typically spread through spam and drive-by downloads.²²

The Ergrun Trojan was the third most common new malicious code family observed in the APJ region in 2009. Once on a compromised computer, Ergrun downloads and installs additional threats. Malicious software such as Ergrun is typically included as a component in staged-downloader threat and is intended to be spread through spam or installed through malicious websites.

¹⁹ http://www.symantec.com/security_response/writeup.jsp?docid=2009-081816-3934-99

²⁰ http://www.symantec.com/security_response/writeup.jsp?docid=2010-011016-3514-99

²¹ http://www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/zeus_king_of_bots.pdf

²² A drive-by download is any download that occurs without a user's prior knowledge or authorization and does not require user interaction. Typically, this is an executable file.

Threats to confidential information

Some malicious code programs are designed specifically to expose confidential information on a compromised computer. These threats may expose sensitive data such as system information, confidential files and documents, or various logon credentials. Some malicious code threats, such as back doors, can give a remote attacker complete control over a compromised computer. Threats to confidential information are a particular concern because of their potential for use in criminal activities. With the widespread use of online shopping and Internet banking, compromises of this nature can result in significant financial loss, particularly if credit card information or banking details are exposed.

In the APJ region in 2009, 90 percent of confidential information threats allowed remote access (figure 3). This is substantially higher than 2008, when 69 percent of confidential information threats allowed remote access. A likely explanation for the large increase is because the addition of remote access features and other confidential information threats to malicious software has become widespread, and that they are now included in the majority of new threats. Their increased prevalence would coincide with the increased availability of malicious software creation toolkits on underground economy forums.

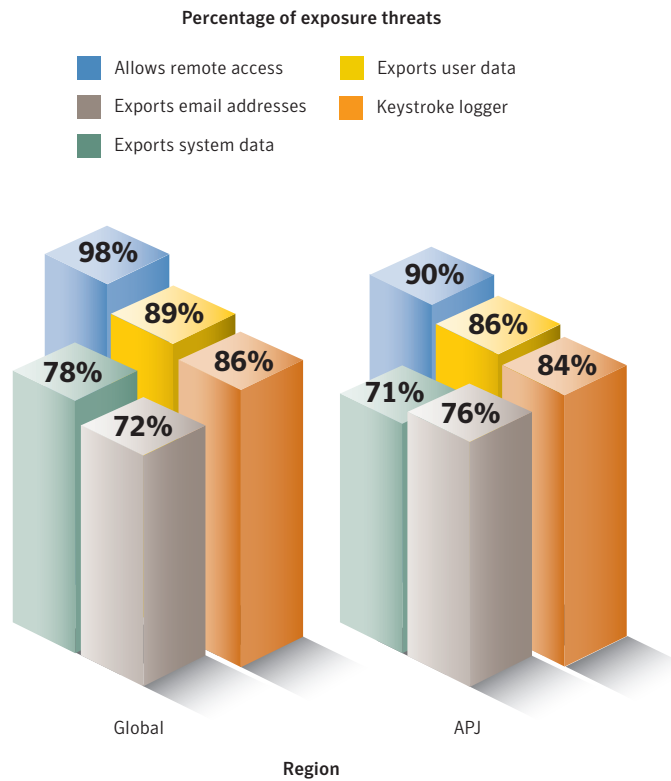


Figure 3. Threats to confidential information, APJ and global

Source: Symantec

The second-highest total observed in the APJ region in 2009 for threats to confidential information was for threats that export user data, of which 86 percent had that capability. This regional percentage is slightly lower than the 89 percent recorded globally in 2009 and slightly higher than the 82 percent recorded regionally in 2008. Threats that are capable of this type of information exposure are favored by attackers because they are effective tools for identity theft and for mounting additional attacks. Increases in this type of exposure are not surprising considering the potential value of harvested information. For example, the sale of bank account credentials observed by Symantec in the underground economy in 2009 ranged between \$15 and \$850, while credit card information was being sold for as high as \$30 per sample.²³

The third most prevalent threat to confidential information of the volume of the top 50 malicious code samples in the APJ region in 2009 was keystroke loggers, with 84 percent of threats having this capability. This is slightly lower than the global total of 86 percent observed in 2009 and slightly higher than the 80 percent observed in 2008. Successfully installed keystroke loggers record keystrokes on compromised computers and then return the data to the attacker, who can then process the results to extract any worthwhile, saleable information, such as account credentials for online banking, stock-trading websites, or online game accounts.

Propagation mechanisms

Worms and viruses use various means to transfer themselves, or propagate, from one computer to another. These means are collectively referred to as propagation mechanisms.²⁴

The most common propagation method for malicious code in the APJ region in 2009 was again through file-sharing executables, with 67 percent of the volume of potential infections capable of propagating by this manner (table 9). This is a slight increase from 65 percent in 2008. Globally, 72 percent of malicious code was capable of propagating through file-sharing executables. Shared executable files are the propagation mechanisms employed by viruses and some worms to copy themselves onto removable media. The continuing resurgence in this vector over the past few years coincides with the increased use of removable drives and other portable devices.

Rank	Propagation Mechanism	Percentage	
		APJ	Global
1	File-sharing executables	67%	72%
2	File transfer, CIFS	33%	42%
3	Remotely exploitable vulnerability	20%	24%
4	File transfer, email attachment	14%	25%
5	File transfer, embedded HTTP URI, instant messenger	6%	4%
6	File sharing, P2P	5%	5%
7	SQL	1%	2%
8	Back door, Kuang2	1%	2%
9	Back door, SubSeven	1%	2%
10	File transfer, data files	1%	1%

Table 9. Top propagation vectors, APJ

Source: Symantec

²³ http://eval.symantec.com/mktginfo/enterprise/white_papers/b-whitepaper_internet_security_threat_report_xv_04-2010.en-us.pdf : p. 73; all currency in U.S. dollars.

²⁴ Many malicious code samples employ multiple propagation mechanisms in an effort to increase the probability of successful propagation; as a result, cumulative percentages included in this discussion may exceed 100 percent.

Asia-Pacific/Japan Data Sheet

In the APJ region in 2009, 33 percent of the volume of the top 50 malicious code samples was able to propagate using CIFS. This is lower than the 42 percent observed for CIFS globally in 2009, but higher than the 25 percent recorded in the region in 2008. CIFS continues to be a popular propagation mechanism in the region likely due to several pervasive threats that employ it. This includes Almanah²⁵ and Fujacks,²⁶ which have ranked in the top 50 malicious threats in the APJ region for several reporting periods. Noteworthy as well is that Downadup is also capable of propagating via CIFS.

The third-ranked propagation method in the APJ region in 2009 was for malicious code that spreads via remotely exploitable vulnerabilities, of which 20 percent of threats had this capability. Globally in 2009, the total for remotely exploitable vulnerabilities was 24 percent, while the total for 2008 was just 7 percent. The increase in exploiting remote vulnerabilities can be almost exclusively tied to Downadup, as it alone of the top 10 malicious code threats in the region in 2009 exploits a remote vulnerability to propagate.

²⁵ http://www.symantec.com/security_response/writeup.jsp?docid=2007-041317-4330-99

²⁶ http://www.symantec.com/security_response/writeup.jsp?docid=2006-111415-0546-99

Phishing and Spam Trends

This section will discuss the following metrics:

- Phishing URLs by region and top targeted sectors
- Originating spam

Phishing URLs by region and top targeted sectors

This metric assesses where the most phishing URLs are hosted during the reporting period, as well as the sector most frequently targeted in each location. This data is a snapshot in time and does not offer insight into changes in the locations of certain phishing URLs over the course of the reporting period. It should also be noted that the fact that a phishing URL is hosted in a certain area does not necessarily mean that the attacker is located there.

In 2009, South Korea hosted the highest percentage of phishing URLs in the APJ region, with 43 percent of the total (table 10). This is an increase from 29 percent in 2008, when South Korea ranked second behind China in this measurement. Globally, South Korea ranked second in 2009, with 5 percent of the phishing URLs identified, although this was significantly less than the 36 percent total of the top-ranked United States. Of the phishing URLs identified in South Korea in 2009, 91 percent targeted the financial services sector.

APJ Rank		Global Rank	Region	Percentage		2009 Top Sector Targeted	Percentage of URLs Targeting Sector
2009	2008	2009		2009	2008		
1	2	2	South Korea	43%	29%	Financial services	91%
2	4	17	Japan	12%	9%	Financial services	88%
3	1	18	China	12%	35%	Financial services	37%
4	3	22	Taiwan	8%	10%	Financial services	90%
5	6	24	Thailand	6%	4%	Financial services	88%
6	7	27	India	5%	2%	Financial services	91%
7	5	28	Australia	4%	5%	Financial services	78%
8	11	34	Philippines	3%	1%	Financial services	92%
9	8	36	Indonesia	2%	2%	Financial services	91%
10	9	40	Malaysia	2%	1%	Financial services	86%

Table 10. Top phishing URLs by region and top-targeted sectors

Source: Symantec

South Korea's high ranking here is due to it having the highest number of phishing website hosts in the APJ region during this reporting period. South Korea's high ranking may also be due to its extensive broadband infrastructure, which makes an appealing target for attackers looking to host phishing and spam sites. Not only is South Korea one of the most broadband-connected areas globally,²⁷ it also has the highest penetration of FTTH/B in the world.²⁸ South Korea's rise is also partly due to the drop in percentage and rank of China in this measurement in 2009.

²⁷ http://www.google.com/publicdata?ds=wb-wdi&met=it_net_user_p2&tdim=true&dl=en&hl=en&q=global+internet+usage#met=it_net_user_p2&idim=country:USA:KOR:FRA:DEU:ESP:ITA:CAN:GBR&tdim=true

²⁸ <http://www.ftthcouncil.org/en/newsroom/2010/02/26/g-20-need-to-speed-up-on-fiber-to-the-home>

Asia-Pacific/Japan Data Sheet

Japan ranked second for phishing URLs identified in the APJ region in 2009, with 12 percent of the total. This is an increase from 9 percent in 2008, when Japan ranked fourth in the region. Along with being partly due to the decrease in percentage and rank of China in this measurement in 2009, Japan's increased percentage may be because it had the fourth highest percentage of phishing website hosts in the APJ region in 2009.

China ranked third for phishing websites in APJ in 2009, with 12 percent of the regional total. This is a significant decrease from 2008, when China ranked first regionally with 35 percent of the total. One reason for this drop may be that Chinese companies and government organizations last year formed an antiphishing group that may have helped reduce phishing incidents.²⁹

The top sector targeted by phishing URLs in each of the top 10 locations in the APJ region in 2009 was the financial sector. Globally, financial service organizations were spoofed by 79 percent of all detected phishing URLs in 2009. The motive behind the predominant percentage of phishing is likely financial gain. Phishers typically exploit brands associated with the financial sector because data garnered from phished financial websites is most likely to yield online banking account and login details.

Interestingly, the financial services sector was only targeted by 37 percent of phishing activity in China, significantly less than in any of the other top-ranked countries in the region. In 2008, the most frequently targeted sector in China was ISPs, with 46 percent of the total at that time. ISP accounts can be valuable targets for phishers because people frequently use the same authentication credentials (such as usernames and passwords) for multiple accounts, including email accounts. This information may provide access to other accounts, such as online banking accounts. Phishers actively targeting users in China likely shifted their focus to financial services because it is a more effective tactic to gain financially rewarding information.

Originating spam

In 2009, 21 percent of all spam detected worldwide originated in the APJ region. Regionally, India ranked first with 21 percent of all spam detected in 2009 (table 11). India's regional share increased substantially from 2008, when it accounted for 12 percent of spam and ranked third. Globally, India accounted for 4 percent of spam detected in 2009 and ranked third.

Overall Rank		Region	Percentage	
APJ	Global		APJ	Global
1	3	India	21%	4%
2	4	South Korea	21%	4%
3	6	China	15%	3%
4	9	Vietnam	13%	3%
5	18	Taiwan	8%	2%
6	20	Thailand	6%	1%
7	24	Japan	5%	1%
8	36	Indonesia	2%	0%
9	40	Australia	2%	0%
10	41	Philippines	2%	0%

Table 11. Originating spam, APJ

Source: Symantec

²⁹ <http://news.techworld.com/security/3208909/chinese-virus-makers-end-up-in-jail/>

One reason for India's high percentage of originating spam is that it has recently experienced significant growth in IT infrastructure and broadband penetration.³⁰ Moreover, India's broadband penetration is still expanding to meet its burgeoning economy and large population and it is estimated that India will continue to rise in the rankings for broadband connectivity in the coming future.³¹

South Korea ranked second for originating spam in the APJ region in 2009, with 21 percent of the total. This is an increase over 2008, when South Korea had 13 percent of originating spam in the region, and also ranked second at that time.

China ranked third for originating spam the APJ region in 2009, accounting for 15 percent of the total. In 2008, China had the highest percentage of originating spam detected in the region, with 22 percent of the total during that period.

The drop in China's percentage of malicious activity in 2009 was mainly due to a decrease in spam zombies there. China ranked second for spam zombies this reporting period, down from first in 2008. This may decline further in 2010 because of the enhanced domain registration procedure introduced by the China Internet Network Information Center (CNNIC), discussed previously in "Malicious activity." In addition, China's regional percentage share for bots dropped to 41 percent in 2009 from 58 percent in 2008. This likely had an impact on the decrease in spam originating from China over the past year because bots are the primary means for sending spam.

³⁰ <http://point-topic.com/dslanalysis.php>

³¹ <http://www.indiabroadband.net/india-broadband-telecom-news/11682-india-register-500-growth-broadband-services-within-5-years.html>

Appendix A—Symantec Best Practices

Symantec encourages all users and administrators to adhere to the following basic security best practices:

Enterprise best practices

- Employ defense-in-depth strategies, which emphasize multiple, overlapping, and mutually supportive defensive systems to guard against single-point failures in any specific technology or protection method. This should include the deployment of regularly updated antivirus, firewalls, intrusion detection, and intrusion protection systems on client systems. Using a firewall can also prevent threats that send information back to the attacker from opening a communication channel.
- Administrators should limit privileges on systems for users that do not require such access and they should restrict unauthorized devices, such as external portable hard-drives and other removable media.
- Turn off and remove services that are not needed for normal company network operations.
- Test security regularly to ensure that adequate controls are in place.
- Educate management on security budgeting needs.
- If malicious code or some other threat exploits one or more network services, disable or block access to those services until a patch is applied.
- Administrators should update antivirus definitions regularly to protect against the high quantity of new malicious code threats and ensure that all desktop, laptop, and server computers are updated with all necessary security patches from their operating system vendor. IDS, IPS, and other behavior-blocking technologies should also be employed to prevent compromise by new threats.
- Always keep patch levels up to date, especially on computers that host public services and applications—such as HTTP, FTP, SMTP, and DNS servers—and that are accessible through a firewall or placed in a DMZ.
- As compromised computers can be a threat to other systems, Symantec recommends that affected enterprises notify their ISPs of any potentially malicious activity.
- Consider implementing network compliance solutions that will help keep infected mobile users out of the network (and disinfect them before rejoining the network).
- Enforce an effective password policy. Ensure that passwords are a mix of letters and numbers, and change them often. Passwords should not consist of words from the dictionary.
- Perform both ingress and egress filtering on all network traffic to ensure that malicious activity and unauthorized communications are not taking place.
- Mail servers should be configured to block email that appears to come from within the company, but that actually originates from external sources.
- Consider using domain-level or email authentication in order to verify the actual origin of an email message to protect against phishers who are spoofing email domains.
- Configure mail servers to block or remove email that contains file attachments that are commonly used to spread viruses, such as .vbs, .bat, .exe, .pif, and .scr files.

Asia-Pacific/Japan Data Sheet

- Clicking on links and/or attachments in email messages (or IM messages) may also expose computers to unnecessary risks. Ensure that only applications approved by the organization are deployed on desktop computers.
- Isolate infected computers quickly to prevent the risk of further infection within the organization.
- Train employees to not open attachments unless they are expected and come from a known and trusted source, and to not execute software that is downloaded from the Internet unless it has been scanned for viruses.
- Perform a forensic analysis and restore the computers using trusted media.
- Ensure that emergency response procedures are in place. This includes having a backup-and-restore solution in place in order to restore lost or compromised data in the event of successful attack or catastrophic data loss.
- Be aware that security risks may be automatically installed on computers with the installation of file-sharing programs, free downloads, and freeware and shareware versions of software.
- Employ Web-server log monitoring to track if and when complete downloads of company websites, logos, and images are occurring, as this may indicate that someone is attempting to use the legitimate website to create an illegitimate website for phishing.
- Network administrators should review Web proxy logs to determine if any users have visited known blacklisted sites.

Consumer best practices

- Use an Internet security solution that combines antivirus, firewall, intrusion detection, and vulnerability management for maximum protection against malicious code and other threats.
- Ensure that security patches are up to date and that they are applied to all vulnerable applications in a timely manner.
- Ensure that passwords are a mix of letters and numbers, and change them often. Passwords should not consist of words from the dictionary.
- Never view, open, or execute any email attachment unless the attachment is expected and the purpose of the attachment is known.
- Keep virus definitions updated regularly. By deploying the latest virus definitions, you can protect your computer against the latest viruses known to be spreading in the wild.
- Routinely check to see if your operating system is vulnerable to threats. A free security scan is available through the Symantec Security Check at www.symantec.com/securitycheck.
- Get involved by tracking and reporting attack attempts. With Symantec Security Check's tracing service, users can quickly identify the location of potential hackers and forward the information to the attacker's ISP or local police.
- Deploy an antiphishing solution, such as an antiphishing toolbar for Web browsers. Also, never disclose any confidential personal or financial information unless and until you can confirm that any request for such information is legitimate.

Asia-Pacific/Japan Data Sheet

- When conducting higher-risk Internet activities, such as online banking or purchases, consumers should do so only on their own computers and not public ones. Further, they should not store passwords or bankcard numbers.
- Review bank, credit card, and credit information frequently to monitor any irregular activities. For further information, the Internet Crime Complaint Center (IC3) has also released a set of guidelines on how to avoid Internet-related scams. See <http://www.ic3.gov/default.aspx> for more information.
- Be aware that security risks may be automatically installed on computers with the installation of file-sharing programs, free downloads, and freeware and shareware versions of software.
- Avoid clicking on links and/or attachments in email or IM messages, as these may also expose computers to unnecessary risks.
- Read end-user license agreements (EULAs) carefully and understand all terms before agreeing to them as some security risks can be installed after an end user has accepted the EULA or because of that acceptance.
- Be aware of programs that flash ads in the user interface. Many spyware programs track how users respond to these ads, and their presence is a red flag. These ads may be spyware.

Asia-Pacific/Japan Data Sheet

About Symantec

Symantec is a global leader in providing security, storage, and systems management solutions to help consumers and organizations secure and manage their information-driven world. Our software and services protect against more risks at more points, more completely and efficiently, enabling confidence wherever information is used or stored.

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

Symantec Corporation
World Headquarters
350 Ellis Street
Mountain View, CA 94043 USA
+1 (650) 527 8000
1 (800) 721 3934
www.symantec.com

Copyright © 2010 Symantec Corporation. All rights reserved. Symantec and the Symantec Logo are trademarks or registered trademarks of Symantec Corporation or its affiliates in the U.S. and other countries. Other names may be trademarks of their respective owners.
04/10 20959305