SYMANTEC ENTERPRISE SECURITY

Confidence in a connected world.

Symantec APJ Internet Security Threat Report

Trends for July–December 07

Volume XIII, Published April 2008

Dean Turner
Executive Editor
Director, Global Intelligence Network
Symantec Security Response

Marc Fossi
Manager, Development
Symantec Security Response

Eric Johnson
Editor
Symantec Security Response

Trevor Mack
Associate Editor
Symantec Security Response

Joseph Blackbird
Threat Analyst
Symantec Security Response

Stephen Entwisle
Threat Analyst
Symantec Security Response

Mo King Low
Threat Analyst
Symantec Security Response

David McKinney
Threat Analyst
Symantec Security Response

Candid Wueest
Analyst
Symantec Security Response

Volume XIII, Published April 2008

APJ Symantec Internet Security Threat Report

Contents

Overview

The Symantec *APJ Internet Security Threat Report* provides a six-month update of Internet threat activity that Symantec has observed in the Asia-Pacific/Japan (APJ) region. It includes analysis of network-based attacks, a review of known vulnerabilities, and highlights of malicious code. It also discusses numerous issues related to online fraud, including phishing and spam. This volume covers the six-month period from July 1 to December 31, 2007.

Symantec has established some of the most comprehensive sources of Internet threat data in the world. The Symantec™ Global Intelligence Network encompasses worldwide security intelligence data gathered from a wide range of sources, including more than 40,000 sensors monitoring networks in over 180 countries through Symantec products and services such as Symantec DeepSight™ Threat Management System and Symantec™ Managed Security Services, and from other third-party sources.

Symantec gathers malicious code reports from over 120 million client, server, and gateway systems that have deployed its antivirus product, and also maintains one of the world's most comprehensive vulnerability databases, currently consisting of over 25,000 recorded vulnerabilities (spanning more than two decades) affecting more than 55,000 technologies from over 8,000 vendors. Symantec also operates the BugTraq™ mailing list, one of the most popular forums for the disclosure and discussion of vulnerabilities on the Internet, which has approximately 50,000 direct subscribers who contribute, receive, and discuss vulnerability research on a daily basis.

As well, the Symantec Probe Network, a system of over two million decoy accounts in more than 30 countries, attracts email from around the world to gauge global spam and phishing activity. Symantec also gathers phishing information through the Symantec Phish Report Network, an extensive antifraud community of enterprises and consumers whose members contribute and receive fraudulent Web site addresses for alerting and filtering across a broad range of solutions.

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 Symantec *APJ Internet Security Threat Report* gives enterprises and consumers essential information to effectively secure their systems now and into the future.

Highlights

The following section will offer a brief summary of the security trends that Symantec observed during the second half of 2007 based on data provided by the sources listed above. These highlights include all of the metrics that are discussed in the rest of this report.

Attack Trends Highlights

- With 38 percent of the total, China ranked first for malicious activity within APJ in this period, as it did for the previous six-month period.
- Between July 1 and December 31, 2007, China ranked first for originating attacks in APJ, with 32 percent of the total, significantly more than the 18 percent recorded in the previous period.
- China was targeted by the most denial-of-service attacks in the APJ region, with 44 percent of the total, a significant decrease from 74 percent in the previous period.
- Symantec observed an average of 7,640 active bot-infected computers per day in the APJ region, a 52 percent decrease from the 15,447 average recorded in the previous reporting period.
- Symantec identified 901,648 distinct bot-infected computers in the APJ region, which is 18 percent of the 5,060,187 distinct bot-infected computers detected worldwide during this period. It is 49 percent less than the 1,782,416 active bot-infected computers that Symantec identified in the APJ region during the first half of 2007.
- China had the most bot-infected computers in the APJ region during this period, with 43 percent of the total, down from 78 percent of the regional total in the first half of 2007.
- Kuala Lumpur had the most bot infections in the APJ region in the second half of 2007, a significant rise from seventh rank in the first half of the year.

Malicious Code Trends Highlights

- For the second half of 2007, Trojans were the top type of malicious code causing potential infections in APJ, amounting to 47 percent of the volume of the top 50 by potential infections.
- China was the top country for all malicious code types during this period.
- The top malicious code sample causing potential infections for the last six months of 2007 in the APJ region was the Gampass Trojan.
- The most widely reported new malicious code family during this reporting period, both in APJ and worldwide, was the Invadesys worm.
- For the last six months of 2007, confidential information threats made up 51 percent of malicious code threats, a decrease from 57 percent observed in the first six months of the year.
- For the second half of 2007 in APJ, 74 percent of the threats to confidential information had a keystroke logging capability.
- The top propagation vector in APJ during this period was executable file sharing, which was employed by 55 percent of regional threats. In the first half of 2007, this vector ranked third, with 33 percent of regional threats.
- For the last six months of 2007, 18 percent of malicious code samples originating in the APJ region had the ability to modify Web pages, substantially higher than the 5 percent recorded in the first half of 2007.

Spam and Phishing Trends Highlights

- During the last six months of 2007, China was home to the highest percentage of phishing Web sites in APJ, with 69 percent of the regional total.
- The most common top-level domain used by phishing Web sites in the APJ region during this period was .cn, which was used by 37 percent of phishing sites in the region.
- Twenty-four percent of all spam detected from the APJ region during this period originated in China, the most of any country in the region and the same percentage as originated there in the first half of the year.

Attack Trends

The malicious activity discussed in this section includes not only attack activity, but also phishing Web sites hosted, malicious code, spam zombies, bot-infected computers, and command-and-control server activity. Attacks are defined as any malicious activity carried out over a network that has been detected by an intrusion detection system (IDS) or firewall. Definitions for the other types of malicious activity can be found in their respective sections of this report. This section of the *APJ Internet Security Threat Report* will analyze the following attack activities that Symantec observed in the APJ region between July 1 and December 31, 2007:

- Malicious activity by country
- Top countries of attack origin
- Top countries targeted by denial-of-service attacks
- Bot-infected computers
- Bot-infected computers by country
- Bot-infected computers by city
- Attacks—protection and mitigation

Malicious activity by country

This metric will assess the countries in which the largest amount of malicious activity takes place or originates. To determine this, Symantec has compiled geographic data on numerous malicious activities, namely: bot-infected computers, bot command-and-control servers, phishing Web site hosts, malicious code reports, spam zombies, and Internet attack origins. The rankings are determined by calculating the mean average of the proportion of these malicious activities that originated in each country.

China ranked first for malicious activity within APJ in this period, as it did for the previous six-month period. While still ranked first within the region, China's proportion of aggregate malicious activity in APJ dropped slightly to 38 percent, from 42 percent previously (table 1). China's rank is not surprising considering that it has the second highest number of broadband subscribers in the world, with over 63 million, behind only the United States.[1] China ranks first in all malicious activity metrics in APJ for this period, with the exception of bot command-and-control servers, for which it ranks second in the region. This is nearly identical to the first half of 2007, when China ranked first in all categories except for bot command-and-control servers and phishing servers.

[1] http://www.point-topic.com

Current Rank	Previous Rank	Country/ Region	Current Percentage	Previous Percentage	Bot Rank	Command-and-Control Server Rank	Phishing Web Sites Host Rank	Malicious Code Rank	Spam Zombies Rank	Attack Origin Rank
1	1	China	38%	42%	1	2	1	1	1	1
2	2	South Korea	14%	14%	3	1	2	5	2	2
3	4	Taiwan	12%	12%	2	3	5	2	4	3
4	3	Japan	8%	13%	4	4	4	3	6	4
5	5	India	6%	7%	11	11	13	2	9	16
6	6	Australia	5%	5%	5	5	3	4	10	5
7	7	Thailand	4%	4%	9	6	6	11	3	9
8	8	Malaysia	4%	2%	6	7	7	7	7	7
9	9	Singapore	2%	2%	7	8	10	6	9	6
10	10	Philippines	2%	1%	8	10	14	8	8	8

Table 1. Malicious activity by country, APJ
Source: Symantec Corporation

South Korea ranked second for malicious activity, unchanged from the first half of 2007. Its share of total regional malicious activity remained unchanged as well, at 14 percent for both the current and previous reporting periods. South Korea has one of the highest household broadband penetration rates in the world, with 92 percent of households having access to broadband connections.[2] This likely contributes to its high rank for malicious activity within the region.

Taiwan ranked third for malicious activity in APJ, up from fourth in the first half of the year. Taiwan's percentage of activity remained unchanged for both periods, at 12 percent, and its rise in rank is partly due to the drop in percentage of Japan, which decreased from 13 percent in the first six months of 2007 to eight percent for this period.

Only two of the countries or regions in the top 10 increased their percentage of malicious activity within APJ this period. This is likely due to an increase in the aggregate malicious activity of APJ countries with smaller numbers of broadband subscribers outside of the top 10, many of which are experiencing rapid growth in broadband infrastructure and subscribers.

Top countries of attack origin

This version of the *APJ Internet Security Threat Report* will measure the top countries targeting the APJ region for attacks. The analysis is based on aggregate IDS and firewall event data collected through the Symantec Global Intelligence Network.

Between July 1 and December 31, 2007, China ranked first for originating attacks in APJ, with 32 percent of the total (table 2). This is significantly more than the previous period, when attacks on the APJ region originating in China made up 18 percent of the total. With this increase, China has displaced the United States as the top originating country for attacks on the APJ region. Globally, China ranked second, with 10 percent of total originating attacks.

[2] http://www.point-topic.com

In the second half of 2007, there was a noticeable decrease in the number of active bots in China. This is likely due to a significant reduction in the availability of many Web sites and interactive sites, such as Web forums and blogs, for several months in China during this period.[3] The increased share of attacks originating in China may represent attempts by bot controllers to find new hosts to infect while their existing bot networks were unavailable during this period, as one of the main methods for bot propagation is through malicious or compromised Web site forums, using tools such as MPack.[4]

Current Rank	Previous Rank	Country/Region	Current Regional Percentage	Previous Regional Percentage	Current Global Percentage
1	2	China	32%	18%	10%
2	1	United States	19%	29%	24%
3	15	South Korea	10%	1%	2%
4	3	Japan	6%	9%	1%
5	4	Australia	4%	7%	1%
6	8	United Kingdom	3%	2%	4%
7	7	Canada	3%	3%	5%
8	11	Taiwan	3%	2%	1%
9	42	Thailand	2%	<1%	<1%
10	10	France	1%	2%	1%

Table 2. Top countries/regions of attack origin, APJ
Source: Symantec Corporation

The United States ranked second for originating attacks on APJ, with 19 percent, down from 29 percent and the top rank in the first half of 2007. Globally, 24 percent of attacks originated in the United States. The declining proportion of the United States as a source for attacks targeting APJ countries suggests a broader trend of increasing intra-regional attack activity within APJ. Many countries within the region are rapidly expanding their broadband networks, and attackers could be attracted to the opportunities afforded by a localized network where linguistic or cultural similarities may serve to enhance the success of attacks.

One example of a regional attack trend is the reported attacks on virtual-item markets serving game players within the region. At least four such Web sites had suspicious outages that were initially attributed to technical problems, but were later described as targeted DoS attacks, possibly as part of an extortion attempt.[5]

South Korea ranked third for this period, with 10 percent of the total. It did not rank in the top 10 countries for originating attacks on APJ last period, though it did rank fifth in the second half of 2006. Attacks originating in South Korea were responsible for two percent of attacks worldwide. One reason for South Korea's drop in the first half of 2007 from the period before that may have been from increased vigilance from law enforcement in response to at least two high-profile incidents that occurred at the beginning of the year.

In the first, two individuals associated with spam operations were arrested in South Korea in January 2007 for transmitting over 1.6 billion spam messages.[6] They had also reportedly obtained and sold personal information that affected over 12,000 victims. The second incident occurred in February 2007, when there were attacks against a number of DNS servers, a critical component of the Internet's infrastructure.[7] The attacks were reputed to have originated in South Korea as part of an underground economy advertisement

[3] http://www.msnbc.msn.com/id/21268635/
[4] http://www.symantec.com/enterprise/security_response/weblog/2007/05/mpack_packed_full_of_badness.html
[5] http://www.itweek.co.uk/vnunet/news/2201049/hackers-korea-game-traders
[6] http://www.vnunet.com/vnunet/news/2173771/korean-duo-accused-sending
[7] http://www.darkreading.com/document.asp?doc_id=119128&WT.svl=news1_2

to tout the effectiveness of a particular bot network (botnet). The occurrence of these two high-profile incidents may have prompted law enforcement to clamp down on reported attack activity for the following months, resulting in lower attack activity seen originating in South Korea. This vigilance may have eased over the remainder of 2007, and resulted in attacks originating from South Korea increasing in percentage enough to return it to a ranking in line with what was seen in the second half of 2006.

Top countries targeted by denial-of-service attacks

Denial-of-service attacks are a major threat to Internet-dependent organizations. A successful DoS attack can render Web sites or other network services inaccessible to customers and employees, which could result in the disruption of organizational communications, a significant loss of revenue, and/or damage to the organization's reputation. Insight into the locations targeted by DoS attacks is valuable in determining global trends in DoS attack patterns, and may also help administrators and organizations in affected countries to take the necessary steps to protect against or minimize the damages of DoS attacks.

China was the top ranked country for DoS attacks in the region for this period, with 44 percent of the total (table 3). With China's massive Internet presence in the region, it is not surprising that it is the target of the most DoS attacks. However, in spite of its top ranking in the region this period, there was a substantial decrease from the previous period, when 74 percent of all DoS attacks within the region targeted systems in China.

The decline was likely due to a diminished attack capacity because many Web sites and online forums in China went offline during this period, as discussed in "Top countries of attack origin", on previous page.

Current Rank	Previous Rank	Country/Region	Current Regional Percentage	Previous Regional Percentage	Current Global Percentage
1	1	China	44%	74%	11%
2	3	South Korea	24%	5%	6%
3	6	Taiwan	9%	2%	2%
4	2	Australia	7%	11%	2%
5	9	Thailand	4%	1%	1%
6	4	Japan	4%	4%	1%
7	5	India	3%	3%	1%
8	7	Singapore	2%	1%	<1%
9	10	Malaysia	1%	<1%	<1%
10	11	Indonesia	1%	<1%	<1%

Table 3. Top countries/regions targeted by DoS attacks, APJ
Source: Symantec Corporation

South Korea was the second ranked country in the APJ region targeted by DoS attacks, with 24 percent of the total. In the first six months of 2007, South Korea ranked third, with five percent. One reason for the substantial increase may have been due to the presidential elections held in December 2007, during which the Internet emerged as an important campaign tool.[8] There were reports of government controls on Internet discussion sites,[9] forcing many to use other forms of media, such as Internet video to express their opinions and political messages. In this environment, DoS attacks could have been used to block or disrupt access to specific content, such as online videos or blogs. Additionally, the decline in bot activity seen during this period within China may have resulted in a corresponding reduction of DoS attacks targeting that country, which would account for the proportional increase of South Korea during the second half of 2007.

Taiwan ranked third as the target of DoS attacks in APJ this period, with nine percent of the total, up from two percent in the first six months of 2007. DoS attacks targeting Taiwan amounted to two percent of global DoS attacks this period. The increase may stem from increasing activity in the run up to two major elections in Taiwan in 2008—a legislative election in January, and a presidential election in March. With the emergence of the Internet as an effective tool for influencing campaigns, the increased DoS activity may be due to hacktivism[10] by supporters of political parties in Taiwan. There were also reports that targeted attacks around the election were originating in mainland China.[11]

Bot-infected computers

Bots are programs that are covertly installed on a user's machine in order to allow an attacker to remotely control the targeted system through a communication channel such as Internet relay chat (IRC), peer-to-peer (P2P), and HTTP. These channels allow the remote attacker to control a large number of compromised computers over a single, reliable channel in a botnet, which can then be used to launch coordinated attacks.

Bots allow for a wide range of functionality and most can be updated to assume new functionality by downloading new code and features. Bots can be used by external attackers to perform DoS attacks against a Web site. Furthermore, bots within a network can be used to attack external sites, which can have serious business and legal consequences for an organization if its network is thus compromised. Bots can be used by attackers to distribute spam and phishing attacks, as well as spyware, adware, and misleading applications. They can also harvest confidential information from compromised computers, which can lead to identity theft.

Between July 1 and December 31, 2007, Symantec observed an average of 7,640 active bot-infected computers per day in the APJ region (figure 1), a 52 percent decrease from the 15,447 average recorded in the previous reporting period. An active bot-infected computer is one that carries out, on average, at least one attack per day over the reporting period. This does not have to be continuous; rather, a single computer can be active on a number of different days. The APJ region accounted for approximately 12 percent of the 61,940 active bot-infected computers worldwide on an average day.

[8] http://www.iht.com/articles/2007/12/17/business/skvote.php
[9] http://opennet.net/research/profiles/south-korea
[10] Hacktivism = hacking + activism: writing code to promote political ideology
[11] http://www.redorbit.com/news/technology/1204169/chinese_hackers_attacking_computers_of_taiwan_election_body__lawmaker/index.html

At the beginning of this reporting period, the number of bots within APJ was relatively low, with an average of 3073 active bot-infected computers per day recorded for the first 12 days of July. On July 13, the active bot-infected computers recorded jumped to 7361 per day. This increase is likely related to an outbreak of the Mubla worm.[12] These Mubla variants attempt to send themselves to user contacts through the MSN Instant Messenger network, turning the recipient's system into a bot if they are run.

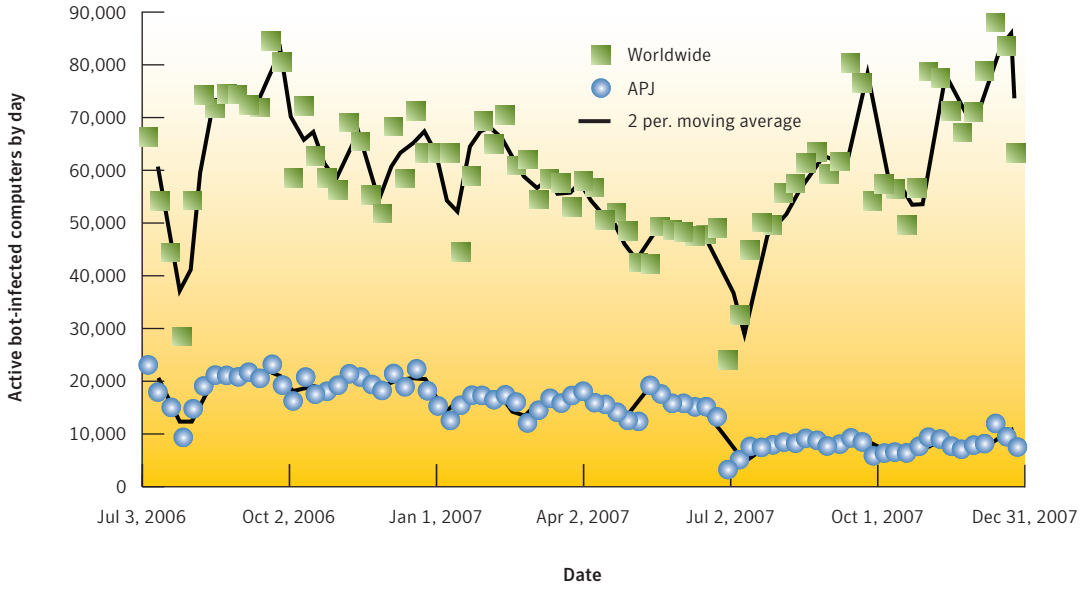

Figure 1. Active bot-infected computers per day, APJ and Global
Source: Symantec Corporation

One reason for the overall decline in bot activity was due to the previously discussed drop in active bots in China during this reporting period. Globally, China dropped to third for bot-infected computers in the second half of 2007, with eight percent, a large decrease from the first half of 2007, when it had 29 percent and ranked first. The decline in active bots in China also correlates to the decrease in spam zombies there. For spam zombies, which are often associated with bot-infected computers, China dropped to fourth in the current period, with six percent of the global total, from third previously and nine percent.

In the second half of 2007, Symantec identified 901,648 distinct bot-infected computers, which amounts to 18 percent of the 5,060,187 distinct bot-infected computers detected worldwide during this period. It is 49 percent less than the 1,782,416 active bot-infected computers that Symantec identified in the APJ region during the first half of 2007. A distinct bot-infected computer is a computer that was active at least once during the period. This large decrease in the total number of regional bots is primarily due to the effect of events in China during this period, as discussed previously.

[12] http://www.cisrt.org/enblog/read.php?133

Bot-infected computers by country

Recognizing the ongoing threat posed by bot networks, Symantec tracks the distribution of bot-infected computers both worldwide and regionally. To do this, Symantec calculates the number of computers worldwide that are known to be infected with bots, and assesses which countries within a region are home to high 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 security awareness in the region.

For the APJ region, the rankings for the second half of 2007 are nearly identical to what was observed in the first half of the year, although the percentages for a number of countries and regions changed substantially. China again ranked first for bot-infected computers in the APJ region for the second half of 2007, but its percentage dropped substantially to 43 percent this period from 78 percent in the previous period (table 4). This is due to the overall decrease in bot activity in China during this period, discussed previously.

Current Rank	Previous Rank	Country/Region	Current Regional Percentage	Previous Regional Percentage	Current Global Percentage	Average Lifespan (days)	Command-and-Control Percentage
1	1	China	43%	78%	8%	2.6	26%
2	2	Taiwan	15%	7%	3%	2	17%
3	3	South Korea	11%	5%	2%	4	29%
4	4	Japan	6%	2%	1%	4	9%
5	6	Australia	5%	2%	1%	4	5%
6	7	Malaysia	4%	1%	1%	3	3%
7	5	India	4%	2%	1%	4	4%
8	8	Singapore	3%	1%	1%	4	2%
9	9	Philippines	2%	1%	<1%	4	0%
10	10	Thailand	2%	1%	<1%	6	3%

Table 4. Bot-infected computers by country, APJ
Source: Symantec Corporation

All of the remaining countries and regions in the top 10 for bot-infected computers increased their share of bot activity this period. This is mainly due to the substantial drop in the number of bot-infected computers in China, which is further borne out by comparing the regional percentages against global proportions. For example, Taiwan's proportion of bots in the region more than doubled to 15 percent from seven percent previously, while its proportion of bot-infections worldwide remained unchanged at three percent for both the current and previous reporting periods. The same is true for South Korea, which more than doubled its share for bot infections regionally this period, to 11 percent from five percent, while its global proportion remained at two percent for both this and the previous reporting period.

Bot-infected computers by city

The top ranked city in the APJ region for bot infections in the second half of 2007 was Kuala Lumpur, Malaysia, which rose to first from seventh in the first half of the year (table 5). One possible explanation for the rise is that Malaysia has a sophisticated telecommunications infrastructure and its broadband penetration is still rapidly growing. Another reason may simply be due to the drop in Chinese cities in this metric for this period because of the substantial drop in bot-infections in China, discussed above.

Current Rank	Previous Rank	City	Country/Region	Current Regional Percentage	Previous Regional Percentage
1	7	Kuala Lumpur	Malaysia	11%	3%
2	1	Beijing	China	9%	17%
3	12	Bangkok	Thailand	7%	2%
4	2	Guangzhou	China	6%	11%
5	15	Hong Kong	China	4%	1%
6	83	Manila	Philippines	4%	<1%
7	13	Taipei	Taiwan	4%	2%
8	19	Singapore	Singapore	4%	1%
9	4	Shanghai	China	3%	4%
10	18	Seoul	South Korea	3%	1%

Table 5. Bot-infected computers by city, APJ
Source: Symantec Corporation

Beijing ranked second for bot infections in the APJ region, from first in the previous reporting period. Again, the change in rank for Beijing—as well as for Guangzhou, Shanghai—can be explained by the drop in bot-infections in China during this period.

The third ranked city for bot infections in the APJ region this period is Bangkok, which is a significant increase from the previous period, when it ranked twelfth. Along with rising in rank due to the proportional drop of Chinese cities this period, the increase may be partly due to cybercrime laws in Thailand that compel ISPs to record the Internet activity of their subscribers.[13] It is possible that their ability to respond to security incidents may have been affected by the increased responsibility of complying with the regulations.

Attacks—protection and mitigation

There are a number of measures that enterprises, administrators, and end users can take to protect against malicious activity. Organizations should monitor all network-connected computers for signs of malicious activity, including bot activity and potential security breaches, ensuring that any infected computers are removed from the network and disinfected as soon as possible. Organizations should employ defense-in-depth strategies, including the deployment of antivirus software and a firewall. Administrators should update antivirus definitions regularly and ensure that all desktop, laptop, and server computers are updated with all necessary security patches from their operating system vendor. As compromised computers can be a threat to other systems, Symantec also recommends that enterprises notify their ISPs of any potentially malicious activity.

[13] http://www.asiasentinel.com/index.php?option=com_content&task=view&id=499&Itemid=31

Symantec recommends that organizations perform both ingress and egress filtering on all network traffic to ensure that malicious activity and unauthorized communications are not taking place.[14] Organizations should also filter out potentially malicious email attachments to reduce exposure to enterprises and end users. In addition, the egress filtering is one of the best ways to mitigate a DoS attack. DoS victims frequently need to engage their upstream ISP to help filter the traffic to mitigate the effects of attacks.

Symantec also advises that users never view, open, or execute any email attachment unless the attachment is expected and comes from a known and trusted source, and unless the purpose of the attachment is known. By creating and enforcing policies that identify and restrict applications that can access the network, organizations can minimize the effect of malicious activity, and hence, minimize the effect on day-to-day operations.

To reduce exposure to bot-related attacks, end users should employ defense-in-depth strategies, including the deployment of antivirus software and a firewall. Creating and enforcing policies that identify and limit applications that can access the network may also help to limit the spread of bot networks. Users should update antivirus definitions regularly and ensure that all desktop, laptop, and server computers are updated with all necessary security patches from their operating system vendor. Symantec also advises that users never view, open, or execute any email attachment unless the attachment is expected and comes from a known and trusted source, and unless the purpose of the attachment is known.

[14] Ingress traffic refers to traffic that is coming into a network from the Internet or another network. Egress traffic refers to traffic that is leaving a network, bound for the Internet or another network.

Malicious Code Trends

Symantec gathers malicious code 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 reporting process. This discussion is based on malicious code samples reported to Symantec for analysis from the APJ region between July 1 and December 31, 2007.

This section will discuss:

- Malicious code types
- Geolocation by type
- Top malicious code samples
- Top new malicious code families
- Threats to confidential information
- Propagation mechanisms
- Malicious code that modifies Web pages
- Malicious code—protection and mitigation

Malicious code types

For the second half of 2007, Trojans were the top type of malicious code causing potential infections in APJ, amounting to 47 percent of the volume of the top 50 by potential infections (figure 2). This is close to what was seen in the previous period, when 51 percent of the volume of the top 50 by potential infections within APJ was classified as Trojans. Worldwide, Trojans were again the top potential infection type, with 71 percent of the volume. The reason for the large percentage of Trojans within APJ is largely due to the Gampass Trojan,[15] which ranked first in the top 10 malicious code samples this period.

[15] http://www.symantec.com/security_response/writeup.jsp?docid=2006-111201-3853-99

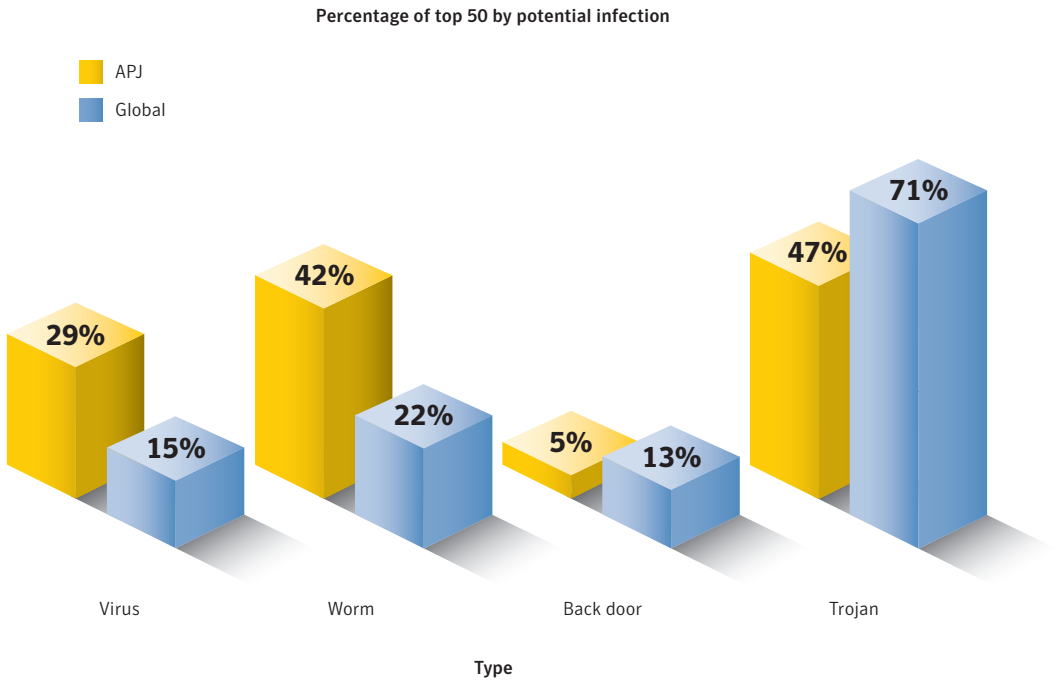

Figure 2. Malicious code types, APJ and Global
Source: Symantec Corporation

Worms made up 42 percent of volume of the top 50 by potential infection within APJ during this period, the same proportion seen in the region during the previous period. Globally, worms accounted for 22 percent of the total volume this period. In the previous volume of the *APJ Internet Security Threat Report*, it was speculated that the differences observed between the APJ region and globally could be due to a lack of port blocking and email attachment scanning in the region. However, seven of the top 10 malicious code types causing potential infections in APJ were classified as worms. Some of these worms target the region specifically, including Looked,[16] which is notable for disabling Chinese-language security applications, and Antinny, a worm that propagated over the Japanese Winny P2P file sharing network.

The proportion of viruses seen in the region during this period increased to 29 percent in the second half of 2007 from 21 percent previously. This is largely due to the appearance of Fujacks[17], classified as both a worm and, because of its file infector capabilities, a virus.

[16] http://www.symantec.com/security_response/writeup.jsp?docid=2006-112813-0222-99
[17] http://www.symantec.com/security_response/writeup.jsp?docid=2007-010509-0134-99

Geolocation by type

Symantec examines the top countries reporting potential malicious code infections by type. Because of the different propagation mechanisms used by different malicious code types, and the different effects that each malicious code type may have, the geographic distribution of malicious code can indicate where network administrators in different regions can increase the focus of their security efforts.

China, with the largest number of broadband subscribers in the region, was the top country for each of the four major malicious code classifications. Japan was third in all categories except back doors, for which it ranked second.

The rankings within the region for Trojans are largely due to the Gampass Trojan, the top ranked sample in APJ, which heavily affected users in China and Taiwan (table 6). The online gaming market in China alone is projected to top $1 billion USD by the end of 2007.[18] With such a large number of online gamers, it is not surprising that Chinese users would be heavily targeted by Gampass and similar Trojans that aim to steal online gaming account credentials.

One high-profile outbreak of worms seen in the region occurred in November 2007, when it was discovered that a number of Maxtor portable hard drives had been delivered from production with a worm that was designed to run when the drive was used through the Windows auto-run feature.[19] The drives were manufactured in Thailand and sold within the region. The incident was blamed on a Chinese subcontractor who may have handled the devices at some point before they reached retail customers. The malicious code attempted to download and install the Gampass Trojan.

Fujacks, the number two worm sample in the region, was mostly seen in China and India, which ranked number one and two for worms, respectively (table 7). As it is classified as both a virus and a worm, Fujacks is also a driver for the virus rankings for China and India (table 8). An additional explanation, however, may be the high rates of piracy in these two countries, estimated at 82 percent for China, and 71 percent for India.[20] Viruses typically spread through the copying and use of executable files, especially those that are from disreputable or unknown sources, as is the case when pirated software is bought or shared.

As noted above, China was the top country in the region for virus potential infections. As a result, variants of the Virut family caused a high number of potential infections there.[21] This virus also contains back door capabilities, which may explain why China also had the highest number of back door potential infections in the region this period (table 9).

[18] http://www.thestreet.com/p/pf/rmoney/gamesandgadgets/10379996.html
[19] http://www.symantec.com/security_response/writeup.jsp?docid=2007-052305-2411-99&tabid=2
[20] http://w3.bsa.org/globalstudy//upload/2007-Global-Piracy-Study-EN.pdf
[21] http://www.symantec.com/security_response/writeup.jsp?docid=2006-051402-1930-99

Rank	Top Country/Region
1	China
2	Taiwan
3	Japan

Table 6. Top countries/regions for Trojans, APJ
Source: Symantec Corporation

Rank	Top Country/Region
1	China
2	India
3	Japan

Table 7. Top countries/regions for worms, APJ
Source: Symantec Corporation

Rank	Top Country/Region
1	China
2	India
3	Japan

Table 8. Top countries/regions for viruses, APJ
Source: Symantec Corporation

Rank	Top Country/Region
1	China
2	Japan
3	Taiwan

Table 9. Top countries/regions for back doors, APJ
Source: Symantec Corporation

Top malicious code samples

The top malicious code sample causing potential infections for the last six months of 2007 within the APJ region was the Gampass Trojan (table 10).[22] It was also the most commonly reported sample within APJ in the previous period. It is not surprising that this is the top sample in APJ, as online gaming is very popular in the region and these games are the favorite target of Gampass. Popular targets include Lineage, based in South Korea with millions of players,[23] Rexue Jianghu, and Rohan. Further boosting the overall infection rate of Gampass is that it is loaded onto a compromised computer by the Mumawow worm,[24] the third ranked sample in APJ this reporting period.

[22] http://www.symantec.com/security_response/writeup.jsp?docid=2006-111201-3853-99
[23] http://pc.gamezone.com/news/12_14_07_04_42PM.htm
[24] http://www.symantec.com/security_response/writeup.jsp?docid=2007-061400-4037-99

Rank	Sample	Type	Top Reporting Country/ Region	Second Reporting Country/ Region	Vectors	Impact
1	Gampass	Trojan	China	Taiwan	N/A	Steals online gaming passwords
2	Fujacks	Worm/virus	India	China	CIFS	Modifies HTML files
3	Mumawow	Virus	China	Taiwan	CIFS	Downloads other threats
4	Gammima	Worm	Taiwan	Australia	CIFS	Steals online gaming passwords
5	Looked	Worm/virus	Taiwan	China	CIFS	Disables security applications
6	Rontokbro	Worm	India	China	SMTP	Performs DoS attacks
7	Netsky	Worm	Japan	Singapore	SMTP	Logs keystrokes
8	Fubalca	Worm/virus	China	Japan	CIFS	Downloads other threats and modifies HTML files
9	Looked.P	Worm/virus	Taiwan	China	CIFS	Disables security applications
10	Adclicker	Trojan	China	Australia	N/A	Clicks advertisements to generate revenue

Table 10. Top 10 regional malicious code samples, APJ
Source: Symantec Corporation

Fujacks was the second most common sample causing potential infections in the region. This instance of malicious code is interesting for two reasons. First, it attempts to modify HTML files on a local file system by seeking out common Web format files (.html, .aspx, etc), and any such files it locates will be appended with an invisible iframe. Second, if and when a browser views that HTML content, either locally or remotely, the browser will be redirected to a malicious Web site where a code download is attempted.

The most substantial change in the malicious code landscape within APJ has been the arrival of the Fujacks worm. This instance of malicious code appears to have had great success in propagation, with nearly as many potential infections this period as top-ranked Gampass. This may have contributed to its high rate of potential infections during this period, and may result in other malicious code authors attempting to adopt and improve on this type of file infector for future attacks. The characteristics that Fujacks exhibits are part of a rising trend in malicious code targeting removable media that Symantec has observed recently, as discussed in the current volume of the *Internet Security Threat Report Executive Summary*.

The third ranked malicious code sample causing potential infections in APJ was the Mumawow worm. This is a file-infector virus that spreads over CIFS file shares and, as mentioned above, attempts to load a variant of Gampass onto a user's computer.

Top new malicious code families

The top new malicious code families observed in APJ for the last six months of 2007 closely correlate with the top families observed globally. The top ranked new malicious code family during this reporting period, both in APJ and worldwide, was the Invadesys[25] worm (table 11). This worm propagates by copying itself to all fixed, removable, and mapped network drives. It also lowers security settings on the compromised computer by terminating certain processes. The worm may also delete files with certain extensions such as .avi and .mpg; however, the most notable impact of this worm is that it prepends its code to any Web pages on the compromised computer.

Users frequently store the pages for personal Web sites on their local drive and upload any modified pages. Web pages that are infected by Invadesys would potentially be uploaded to the user's hosting provider the next time modifications were uploaded. This could result in visitors to the user's site being compromised when they view an infected page.

Rank	Sample	Type	Top Reporting Country/ Region	Second Reporting Country/ Region	Propagation Vectors	Impact
1	Invadesys	Worm	China	Taiwan	CIFS	Lowers security settings and modifies Web pages
2	Niuniu	Worm/virus	China	Malaysia	CIFS	Modifies Web pages
3	Farfli	Trojan	China	Taiwan	N/A	Downloads other threats and modifies Internet Explorer® Start Page
4	Blastclan	Worm	India	Nepal	CIFS	Disables security applications
5	Pidief	Trojan	Japan	Australia	N/A	Exploits Adobe Acrobat vulnerability to lower security settings and download other threats
6	Pagipef	Worm/virus	China	Taiwan	CIFS	Modifies Web pages
7	Mondezimia	Virus	Singapore	Malaysia	CIFS	Modifies Web pages
8	Reapall	Trojan	China	Taiwan	N/A	Downloads other threats
9	Kaxela	Worm	China	Taiwan	Worm	Downloads other threats
10	Mimbot	Worm	Singapore	Australia	MSN Messenger	Allows remote access

Table 11. Top 10 new malicious code families, APJ
Source: Symantec Corporation

The Niuniu[26] worm was the second ranked new malicious code family in the APJ region this period. This worm is similar to the Invadesys worm in that it propagates by copying itself to all fixed, removable, and mapped network drives on the compromised computer. The worm also modifies the user's Internet Explorer start page to a Web site that the attacker likely controls.

[25] http://www.symantec.com/security_response/writeup.jsp?docid=2007-111215-5430-99
[26] http://www.symantec.com/security_response/writeup.jsp?docid=2007-101018-5756-99

Also, like Invadesys, Niuniu adds code to any Web pages it finds on the compromised computer. However, rather than adding code to infect users who view the pages, Niuniu adds an invisible iframe HTML tag to the pages. This tag will redirect the user's browser without his or her knowledge to a Web page that is likely under the attacker's control. This technique is similar to that employed in the MPack attack seen in the first half of 2007.

The Farfli Trojan[27] was the third most common new malicious code family in the second half of 2007 in the APJ region. This Trojan is capable of downloading and installing other threats onto the compromised computer. This is a continuation of the trend of increasing multistage attacks that was noted in the previous version of the Symantec *Internet Security Threat Report*.[28] In a multistage attack, an initial compromise takes place that is intended to facilitate the launch of subsequent attack activity.

In addition to installing other threats on the compromised computer, Farfli also changes the user's Internet Explorer homepage to one the attacker likely controls. This is presumably done to generate revenue for the attacker through affiliate advertising clicks. For each compromised computer that opens the page, the attacker would receive payment from banner advertising.

It is also notable that this Trojan changes the search settings for the Maxthon and TheWorld Web browsers.[29] The settings are changed to use the same revenue-generating pages as previously described. These two Web browsers do not have the same market share as other browsers that are more commonly targeted. This may indicate that Farfli was written to target a certain group of users. Both of these browsers are developed and maintained by Chinese companies, which may indicate that the author of the Trojan is specifically targeting Chinese users. Another indication that Chinese users are specifically targeted is that Farfli changes the search settings to use a popular Chinese search engine. This exemplifies the continuing trend of regionalization of malicious code that was noted in the previous version of the Symantec *Internet Security Threat Report*.[30]

Threats to confidential information

Some malicious code programs are designed specifically to expose confidential information that is stored on an infected computer. These threats may expose sensitive data such as system information, confidential files and documents, or 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.

Within the enterprise, exposure of confidential information can lead to significant data leakage. If it involves customer-related data—such as credit card information—customer confidence in the enterprise can be severely undermined. Moreover, it can also violate local laws. Sensitive corporate information, including financial details, business plans, and proprietary technologies, could also be leaked from compromised computers.

[27] http://www.symantec.com/security_response/writeup.jsp?docid=2007-072901-5957-99
[28] Symantec *Internet Security Threat Report*, Volume XII (September 2007): http://eval.symantec.com/mktginfo/enterprise/white_papers/ent-whitepaper_internet_security_threat_report_xii_09_2007.en-us.pdf : p. 75
[29] Maxthon and TheWorld are Web browsers that make use of the Internet Explorer and Firefox rendering engines. As a result, they behave in a similar manner to these browsers and are also susceptible to the same vulnerabilities.
[30] Symantec *Internet Security Threat Report*, Volume XII (September 2007): http://eval.symantec.com/mktginfo/enterprise/white_papers/ent-whitepaper_internet_security_threat_report_xii_09_2007.en-us.pdf : p. 81

It should be noted that threats that expose confidential information may employ more than one method to do so. As a result, cumulative percentages discussed in this metric may exceed 100 percent.

For the last six months of 2007 in the APJ region, 51 percent of the malicious code threats observed in the APJ region constituted a threat to confidential information (figure 3). This is a slight decrease from 57 percent observed in the first six months of the year. Worldwide, 68 percent of threats were classified as a potential threat to confidential information.

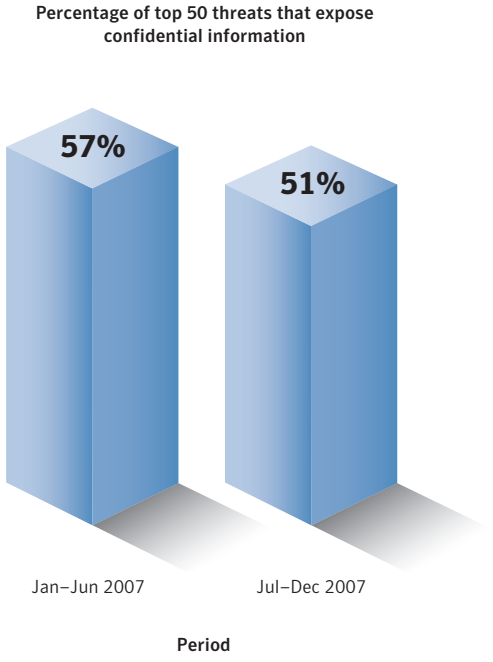

Figure 3. Threats to confidential information by volume, APJ
Source: Symantec Corporation

Confidential information threats with keystroke logging capability were the most common method employed by malicious code targeting the APJ region for this period, with 74 percent of the threats having this capability (figure 4). This is a slight decrease from the previous period, when 78 percent of regional threats had keystroke logging functionality.

A keystroke logger records keystrokes on a compromised computer and either emails the log to the attacker or uploads it to a Web site under the attacker's control. The attacker can use these logs to extract the user's credentials for different types of accounts, such as online banking, trading sites, or ISP account access. The information can then be used as a stepping stone to launch further attacks.

Keystroke logging may rank especially high in relation to other information retrieval methods in APJ because of the popularity of online games and attempts by attackers to steal gaming credentials from users. To steal game credentials, it would be easier to use a keystroke logger than to write specialized code that interfaces with the game, especially if several different online games are targeted.

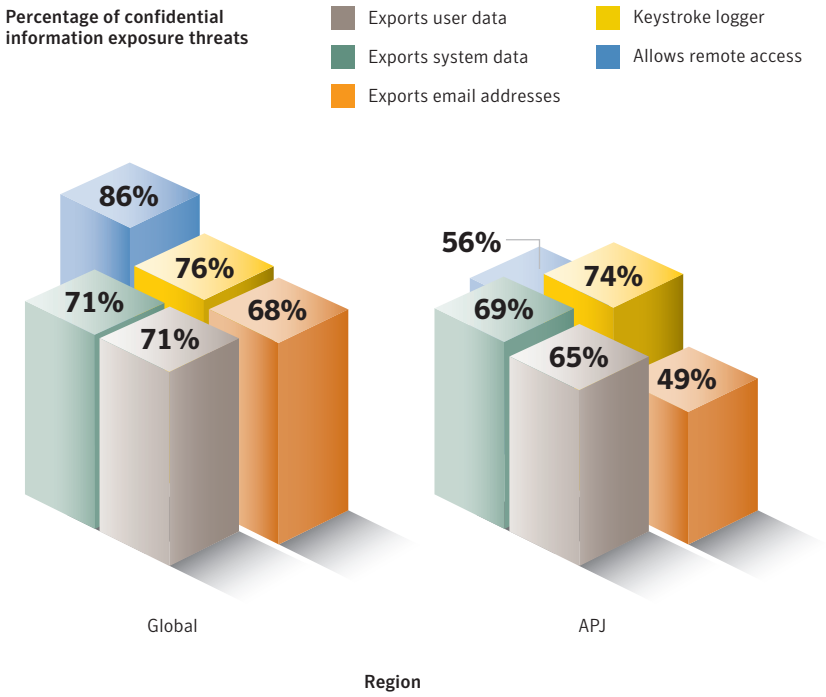

Figure 4. Threats to confidential information by type, APJ
Source: Symantec Corporation

Threats that export user data reported amounted to 65 percent of regional threat volume in APJ for this period, a decrease from the 79 percent observed in the first half of the year. Of the top 50 threats in the region, twelve have functionality that allow for the export of user data. The number one threat in the region, Gampass, attempts to obtain credentials for various online games popular in APJ countries. The overall proportional decrease may mean that malicious code authors targeting the region are focusing their efforts on obtaining information related to online game activities, rather than personal information. The market at this point for virtual items may be better than for personal information.[31]

The proportion of threats in APJ for the second half of the year that attempt to extract email addresses is much lower than what was seen globally, 49 percent compared to 68 percent, respectively. The regional proportion in the first half of the year was 51 percent. In the previous *APJ Internet Security Threat Report*, the disparity between the percentages for attempts to export email addresses in APJ and worldwide was thought to be due to the higher proportion of spam that is composed in English. Symantec believes that this is still true, and anticipates that spam will continue grow in the APJ region. Malicious code will likely reflect this trend by including email harvesting features in the future.

[31] http://www.koreatimes.co.kr/www/news/biz/biz_view.asp?newsIdx=2660&categoryCode=123

Propagation mechanisms

Worms and viruses use various means to transfer themselves, or propagate, from one computer to another. These are collectively referred to as propagation mechanisms. Propagation mechanisms can include a number of different vectors, such as Simple Mail Transfer Protocol (SMTP), Common Internet File System (CIFS), peer-to-peer (P2P), and remotely exploitable vulnerabilities. Some malicious code may even use other malicious code as a propagation vector by locating a computer that has been compromised by a back door server and using it to upload and install itself.

This metric will discuss some of the propagation mechanisms used by malicious code samples in APJ reported to Symantec during the second half of 2007. It should be noted that 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.

The top propagation vector in APJ during this period was file sharing executables, with 55 percent of the total (table 12). This vector has increased in rank and proportion since the last reporting period, when it ranked third with 33 percent of regional threats. Globally, file sharing executables ranked first, with 40 percent of the total.

This propagation vector is usually associated with physical sharing of files, the traditional method employed by the original file infecting computer viruses. Overall, there is a trend indicating the increasing effectiveness of this classic propagation path, which is largely attributable to the increasing capacity and use of removable media, such as USB keys and portable hard drives. These high-capacity and highly portable storage devices allow individuals to easily exchange large amounts of data. The higher proportion within APJ may also be due to the higher levels of software piracy in the region.[32]

Rank	Propagation Mechanism	Regional Percentage	Global Percentage
1	File sharing executables	55%	40%
2	File transfer/CIFS	30%	28%
3	File transfer/email attachment	24%	32%
4	File sharing/P2P	15%	19%
5	Remotely exploitable vulnerability	11%	17%
6	File transfer	40%	2%
7	File transfer/HTTP/embedded URI/Yahoo! Messenger	30%	2%
8	Web	10%	1%
9	Email	10%	1%
10	File transfer/Yahoo! Messenger	10%	2%

Table 12. Propagation vectors, APJ
Source: Symantec Corporation

[32] http://www.zdnetasia.com/news/software/0,39044164,62013101,00.htm

Transfers using the Windows® file sharing protocol (CIFS) was the second ranked propagation vector in APJ for the last six months of 2007, with 30 percent of the total.[33] This is slightly more than the 28 percent reported globally, but less than the 34 percent reported for the region in the first half of 2007. The large proportions and the fact that five of the top 10 submissions in this period propagate via CIFS shares indicate that this vector is still effective.

The third most commonly seen propagation vector is transmission via email attachment. This method declined substantially in APJ this period from last, dropping to 24 percent for the last six months of the year from 37 percent in the first half. File transfers using email attachments also declined worldwide, although the global proportion remains higher, at 32 percent, than the 24 percent reported in APJ.

Malicious code that modifies Web pages

In May 2007, the attack kit MPack[34] was observed in the wild. This kit compromised Web pages, typically through the insertion of iframes, to redirect users to an MPack server that attempted to exploit Web browser and plug-in vulnerabilities and install malicious code on computers.[35] This kit experienced great success because it took advantage of users visiting legitimate, trusted Web pages that had been compromised. Since the Web browser is a user's primary gateway to the Internet, frequently visited, trusted sites—such as online forums and other Internet communities—are a valuable attack vector.

For the first time, in this volume of the *APJ Internet Security Threat Report*, Symantec is examining malicious code that modifies Web pages on a compromised computer in the region. Only threats that modify pages in order to propagate or redirect users were examined. Those that simply deface the pages by adding text or simple images are not included in this metric.

For the last six months of 2007, 18 percent of malicious code samples in the APJ region had the ability to modify Web pages (figure 5). This is significantly more than the seven percent observed globally, and a substantial increase from the five percent recorded in the APJ region during the first half of 2007. One explanation for the greater percentage in APJ is because three of the top malicious code samples and three of the top new malicious code families in the region modify HTML code as a means of propagation.

[33] 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.
[34] http://www.symantec.com/business/security_response/writeup.jsp?docid=2007-052712-1531-99
[35] http://www.symantec.com/enterprise/security_response/weblog/2007/05/mpack_packed_full_of_badness.html

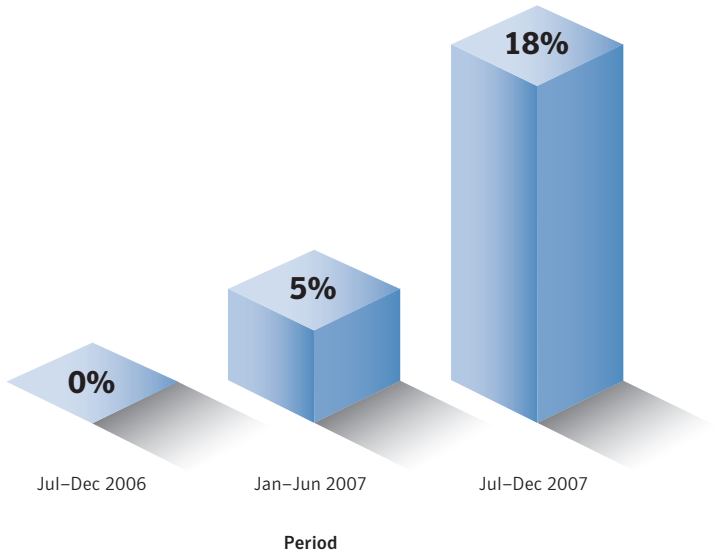

Figure 5. Malicious code modifying Web pages, APJ
Source: Symantec Corporation

The 18 percent observed in APJ indicates the success of this propagation vector for developers of malicious code. For example, the number two ranked malicious code sample, Fujacks, was designed to modify local HTML code. As mentioned previously, the number of potential infections associated with Fujacks was very high in APJ. This may be partly due to its modification of HTML content to propagate. Also contributing to the proportion seen this period is Fubalca,[36] which loads Gampass on infected computers and attempts to spread via removable media and HTML files.

Adoption of this technique has also been seen in three of the top new malicious code families within APJ in this reporting period. This includes: second ranked Niuniu, discussed earlier; Pagipef[37], which attempts to write to HTML files found on a compromised system, as well as attempting to spread over removable media; and Mondezimia,[38] which attempts to add malicious code to both HTML and VBS files, as well as attempting to spread through removable media.

The increasing development of attacks designed to modify Web pages continues a trend being observed by Symantec indicating that the Web has become the primary target as an attack vector. This may be partly due to improvements in security measures in areas such as software and network infrastructures, but it could also be the result of the success attackers are having in targeting end users through the Web.

[36] http://www.symantec.com/security_response/writeup.jsp?docid=2007-040106-1154-99
[37] http://www.symantec.com/security_response/writeup.jsp?docid=2006-111716-1413-99
[38] http://www.symantec.com/security_response/writeup.jsp?docid=2007-102617-2436-99

Malicious code—protection and mitigation

Symantec recommends that certain best security practices always be followed to protect against malicious code infection. Administrators should 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. Email servers should be configured to only allow file attachment types that are required for business needs and to block email that appears to come from within the company, but that actually originates from external sources. Additionally, Symantec recommends that ingress and egress filtering be put in place on perimeter devices to prevent unwanted activity.

To protect against malicious code that installs itself through a Web browser, additional measures should be taken. The use of IPS technologies can prevent exploitation of browser and plug-in vulnerabilities through signatures and behavior-based detection in addition to ASLR.

End users should employ defense-in-depth strategies, including the deployment of antivirus software and a personal firewall. 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 software vendors. They should never view, open, or execute any email attachment unless it is expected and comes from a trusted source, and unless the purpose of the attachment is known.

Phishing Trends

Phishing is an attempt by a third party to solicit confidential information from an individual, group, or organization, often for financial gain. Phishers are groups or individuals who attempt to trick users into disclosing personal data, such as credit card numbers, online banking credentials, and other sensitive information. They may then use the information to commit fraudulent acts.

The data provided in this section is based on statistics derived from the Symantec Probe Network, a system of over two million decoy accounts in more than 30 countries that attracts email from around the world to gauge global spam and phishing activity. It encompasses more than 600 participating enterprises worldwide, attracting email that is representative of traffic that would be received by over 250 million mailboxes. The Probe Network consists of previously used email addresses as well as email accounts that have been generated solely to be used as probes.

This section of the Symantec *APJ Internet Security Threat Report* will discuss the following specific phishing activities that Symantec detected in the APJ region between July 1 and December 31, 2007:

- Top countries hosting phishing Web sites and top targets phished
- Phishing Web site top-level domains
- Phishing—protection and mitigation

Top countries hosting phishing Web sites and top targets phished

A phishing Web site is a site that is designed to mimic the legitimate Web site of the organization whose brand is being spoofed, often an online bank or e-commerce retailer. In many cases, it is set up by the attacker to capture a victim's authentication information or other personal identification information, which can then be used in identity theft or other fraudulent activity.

This section of the Symantec *APJ Internet Security Threat Report* will discuss the top APJ countries in which phishing attacks associated with phishing sites were hosted, and the type of service offered by the organizations whose brands those phishing Web sites most frequently spoofed. Readers should note that phishing Web sites differ from phishing hosts, which are computers that can host one or more phishing Web sites, and which are discussed in "Malicious activity by country" in the "Attack Trends" section of this report.

The data discussed in this section is a snapshot in time and, therefore, does not have insight into changes in the locations of certain phishing Web sites throughout the period. It should also be noted that just because a phishing Web site is hosted in a certain country, it does not necessarily mean that the attacker is located in the same country.

During the last six months of 2007, China was home to the highest percentage of phishing attacks associated with phishing Web sites in APJ, with 69 percent of the region's total (table 13). China had the second highest number of phishing attacks associated with phishing Web sites worldwide during this period, accounting for 14 percent of the total.

China's high ranking in this category is not surprising, as it was the top APJ country for all malicious activities during the last half of the year except for bot command-and-control servers, for which it ranked second. Some of these categories could contribute to phishing activity. For instance, spam zombies are compromised computers that are used to relay spam messages, some of which could include links to phishing Web sites. Additionally, bot-infected computers can be used to host phishing Web sites on a compromised computer, and phishing hosts are used to host one or more phishing Web sites. A high ranking in all of these categories is likely to contribute to a high number of phishing Web sites.

Two other considerations may also influence the number of phishing Web sites located in a country—the number of domains hosted there and the number of Web-hosting companies. The number of domain names registered to a country could correlate to the number of Web sites hosted there. As of January 2008, China had the highest number of domain names in the APJ region and the fifth highest number of domain names in the world. It is not surprising that it also had the highest number of phishing Web sites. The higher number of domain names will not necessarily contribute to a higher number of phishing Web sites; however, it could indicate a higher probability of phishing Web sites, if only as a percentage of the higher number of domain names.

The second consideration is the number of Web-hosting companies located in the country in question. Phishers can use Web-hosting companies to host phishing Web sites in two ways. First, they can employ the hosting company to host a Web site legitimately, but use that site for phishing. Second, they can compromise legitimate Web sites hosted by the company and use them for phishing. At the end of 2007, China had only the fifth most Web-hosting companies in the APJ region, behind India, Australia, Japan, and South Korea. Given this relatively low ranking, it would appear that the high numbers of phishing Web sites hosted in China are hosted on compromised computers, particularly as the number of bot-infected computers and spam zombies located there is very high.

In the current volume of the *Global Internet Security Threat Report*, Symantec observed that many bot networks are now using a fast-flux domain name service scheme, in which control of the botnet is not managed through a centralized command-and-control server, but is instead set up as a decentralized network (somewhat like the Internet itself). This makes botnets more difficult to detect and disable. This is relevant to phishing Web sites because fast-flux allows a single URL to resolve to a number of different IP addresses, or computers, by changing the DNS mapping of the URL rapidly and constantly. In other words, a single URL can be used to point to a number of different computers at different times. This functionality has allowed phishers to host phishing Web sites across a botnet. Because of the decentralized nature of fast-flux, when one phishing Web host is blocked or taken down, the attacker can change the DNS entry so that the URL will point to a different computer that has not been blocked or taken down, but that is hosting the same phishing Web page, allowing the phisher to carry out phishing attacks for longer periods. As a result, a high number of bot-infected computers may lead to a high number of phishing Web sites.

Some observers believe that a substantial number of phishing Web sites located in China may be due to a single group of phishers known as Rock Phish,[39] who are known for employing particularly sophisticated phishing techniques.[40] They may be using phishing sites in China because these sites may be left in place for longer periods, making hosting a site there more desirable and allowing attackers to carry out more attacks. China has the highest amount of malicious activity in the region and the second highest amount worldwide, as discussed in the "Attack Trends" section. Registrars are also reputed to be more permissive in China.[41] These factors make it reasonable to assume that phishers have an easier time hosting and maintaining their phishing sites in China.

The top target of phishing attacks associated with Web sites hosted in China during this period was a social networking site. Social networking pages are easy to obtain and, because these pages are generally trusted by users, phishing attacks spoofing them may have a better chance of success.[42] Once a social networking page is obtained, it could be used to carry out subsequent attacks, which could be successful because the page would already be on the network's domain.

These spoofed pages can include links to false downloads that require users to enter confidential information, such as authentication information or credit card information, that can subsequently be used for fraudulent purposes. Furthermore, phishers may be able to upload content, such as Flash videos, onto a spoofed page that will allow the attacker to hijack the page of anyone who visits that page.[43]

Regional Rank	Global Rank	Country/Region	Regional Percentage	Top Target
1	2	China	69%	Social networking site
2	4	Guam	25%	Social networking site
3	12	South Korea	2%	Banking site
4	15	Japan	1%	Online payment system
5	18	Taiwan	1%	Banking site
6	20	Thailand	1%	Banking site
7	21	Australia	<1%	Online payment system
8	23	Malaysia	<1%	Social networking site
9	38	Indonesia	<1%	Online payment system
10	39	Bangladesh	<1%	Online payment system

Table 13. Top countries/regions hosting phishing Web sites and top targets, APJ
Source: Symantec Corporation

Guam had the second highest number of phishing attacks associated with Web sites in the APJ region in this reporting period, with 25 percent of the total. As was the case with China, the top target of phishing attacks associated with Web sites hosted in Guam during this period was a social networking site.

[39] http://www.rsa.com/solutions/consumer_authentication/intelreport/FRARPT_DS_1007.pdf
[40] http://www.symantec.com/enterprise/security_response/weblog/2007/12/getting_acquainted_with_rock_p.html
[41] http://www.rsa.com/solutions/consumer_authentication/intelreport/FRARPT_DS_1007.pdf
[42] http://www.symantec.com/enterprise/security_response/weblog/2006/09/contextaware_phishing_realized.html
[43] http://www.symantec.com/enterprise/security_response/weblog/2006/07/myspace_shockwave_flash_hack.html

Guam also had the fourth highest number of phishing attacks associated with Web sites worldwide during this period, accounting for five percent of all phishing sites globally, a significant percentage for such a small country. The high rank of Guam for hosting phishing sites, as well as for other malicious activities this period, is surprising. As of January 2008, Guam had only 2,700 broadband Internet subscribers.[44] Furthermore, at that time, it had only 1,687 Web domains registered, which is 132nd in the world.[45] However, it has well-established broadband Internet infrastructure likely because of the importance of Guam as a U.S. military base—the island is home to six U.S. military installations. An Australian ISP is even laying an underwater cable from Guam to Sydney to facilitate additional high-speed Internet for Australian users.[46] Guam also has significant connectivity to Japan and the United States.[47] Thus it appears that broadband connectivity in Guam is expanding rapidly. The security infrastructure may currently be insufficient for this growth.

Phishing Web sites in Guam could be hosted on compromised computers. However, less than one percent of bot-infected computers in the APJ region are located in Guam.[48] On the other hand, Guam was home to four percent of the phishing hosts in the APJ region during this period. This could mean that phishers are using legitimately hosted Web sites for phishing purposes, or it could mean that they have compromised the ISPs' servers and are hosting phishing Web sites on them surreptitiously. As of January 2008, Guam was home to seven Web-hosting companies.[49] It is thus likely that phishing Web sites are hosted as legitimate Web sites on a Guam-based ISP or Web-hosting company. These Web sites may not have been detected. Currently, broadband connectivity in Guam is expanding rapidly. As Symantec has stated in previous *Internet Security Threat Reports*, rapidly expanding ISPs are less likely to have sufficient resources to meet their expanding security needs.

In the second half of 2007, South Korea ranked third for phishing attacks associated with Web sites in the APJ region, with two percent of the total. South Korea had the twelfth highest number of phishing attacks associated with sites worldwide.

The presence of South Korea in this category is not particularly surprising, as it has a reasonably well established history of malicious activity, including phishing.[50] During this reporting period, South Korea had the second most overall malicious activity of any APJ country, including the second highest number of phishing hosts in the region. As phishing hosts can host one or more phishing Web sites, this would obviously contribute to a high number of phishing attacks associated with Web sites located there. Furthermore, South Korea had the third highest number of bot-infected computers, which could be used to host phishing sites.

In addition to these considerations, South Korea had the fourth highest number of domain names in APJ.[51] A high number of domain names will not, in and of itself, contribute to a higher number of phishing Web sites; however, it will indicate a higher probability of phishing Web sites, if only as a percentage of the higher number Web sites indicated by the higher number of domain names.

[44] http://www.point-topic.com
[45] http://www.webhosting.info/domains/country_stats/?pi=2&ob=TOTA%20L&oo=DESC
[46] http://whirlpool.net.au/article.cfm/1772
[47] http://whirlpool.net.au/article.cfm/1772
[48] 0.3 percent of bot-infected computers in the APJ region were located in Guam.
[49] http://webhosting.info/webhosts/globalstats/?pi=14&ob=HC&oo=DESC
[50] For instance, in each of the two previous reporting periods, South Korea had the second most malicious activity in the APJ region.
[51] http://www.webhosting.info/domains

South Korea had only the sixth highest number of Web-hosting companies at that time despite the higher number of domains,[52] suggesting that these Web-hosting companies were relatively large. Large Web-hosting companies may be susceptible to hosting phishing Web sites because the larger number of Web sites managed by those companies may allow phishing sites to exist for a long period in time in relative obscurity, undetected by the hosting provider.

The top target spoofed by phishing attacks associated with Web sites located in South Korea was a bank based in the United States. Phishing attacks are often motivated by financial gain and organizations in the financial sector, such as banks, are particularly attractive targets for phishers. It is likely that phishing Web sites based in South Korea spoofed this bank in order to try to lure customers into entering their banking information into the fraudulent Web page. This information could then be used by phishers to obtain funds from the account or use credit cards associated with the account. It is likely that, as the bank is based in the United States, phishers are targeting users there, as that is where most of the bank's non-commercial operations are located.

Phishing Web site top-level domains

Domain names are the words that are used in URLs to identify particular Web pages, such as www.symantec.com. They resolve to a specific IP address for a particular Web site and are used because names are easier to remember than a long string of numbers. The highest level of domain names is the top-level domain (TLD). Examples include .com (generally used by businesses, but available to anyone), .edu (used by organizations in the education sector), and .org (predominantly used by non-profit organizations). Understanding the TLDs that are most commonly used in phishing Web sites may help end users, security administrators, and organizations to understand which of these domains could be most prone to hosting phishing Web sites, and help alert them to potentially malicious sites. It may also help security analysts further identify which countries or sectors are hosting the most phishing Web sites.

During the last six months of 2007, .cn was the most common TLD used by phishing Web sites in the APJ region, accounting for 37 percent of the total (table 14). During this reporting period, the .cn TLD was used by only 23 percent of phishing Web sites on the Internet as a whole, indicating that phishing Web sites using this TLD were concentrated in the APJ region. This is not surprising as the .cn domain name is the assigned country domain of China, which was home to by far the highest percentage of phishing Web sites in the APJ region during this reporting period, with 69 percent of the region's total.

The .cn TLD is currently used by less than one percent of domain names on the Internet as a whole.[53] However, 23 percent of phishing Web sites worldwide uses this TLD. Thus, the number of phishing Web sites using this TLD is disproportionately very high. This does not necessarily mean that the phishers using these sites are in China; although the .cn TLD was originally restricted to domain names registered in China, it has since been made available internationally.[54] As a result, it is difficult to ascertain whether the phishing Web sites using this TLD are located in China or not. Rather, it likely indicates that phishers in indeterminate locations have compromised Chinese Web sites or ISPs located in China to host their phishing Web sites. This supports the previous discussion, in "Top countries hosting phishing Web sites and top targets phished", that phishers are taking advantage of permissive domain registration rules in China to register Web sites in that country that will be used for phishing activity.

[52] http://webhosting.info/webhosts/globalstats/?pi=2&ob=HC&oo=DESC
[53] http://www.neulevel.cn/
[54] http://www.neulevel.cn/

China was the top APJ country for all malicious activities during the last six months of the year except for bot command-and-control servers, for which it ranked second. For the APJ region during this period, China had the most bot-infected computers, which can be used to host phishing Web sites. It also had the most phishing hosts.

Rank	Top-level Domain	Regional Percentage	Global Percentage
1	.cn	37%	23%
2	.com	31%	44%
3	.net	6%	6%
4	.tw	4%	0%
5	.co.kr	3%	0%
6	.au	2%	0%
7	.org	2%	3%
8	.jp	2%	0%
9	.kr	1%	0%
10	.ac.th	1%	0%

Table 14. Top phishing Web sites by top-level domain, APJ
Source: Symantec Corporation

In the second half of 2007, the second most common TLD used by phishing Web sites located in the APJ region was .com, which was used by 31 percent of the total. This is not surprising, as .com is the most common TLD on the Internet. It is used by roughly 73 percent of all registered general top-level domain names.[55] During this reporting period, it was used by 44 percent of all phishing Web sites detected worldwide.

The percentage of phishing Web sites using the .com TLD is thus somewhat lower than the Internet-wide number, indicating that this TLD is not used by phishing Web sites in the APJ region in particular. Further, the number of phishing Web sites in the APJ region was significantly lower than those using this TLD across the Internet as a whole. This may indicate that phishers in the APJ region are using phishing Web sites that are hosted on local TLDs, such as those indicating specific countries. This may indicate that phishing Web sites located in region are likely targeting clients and customers of local organizations, such as local financial organizations. Using local TLDs may assist them in this process.

The comparatively low number of .com TLDs in APJ phishing Web sites may also illustrate the distribution of TLDs across the Internet. By far the majority of domain names using .com are situated in the United States.[56] Therefore, it is logical that the number of phishing Web sites using .com is lower in APJ than across the Internet as a whole.

The third most common TLD used by phishing Web sites in the APJ region during this period was .net, which was used by six percent of the total. It was used by the same percentage of phishing Web sites across the Internet as a whole, so it does not appear that phishing sites using .net are particularly concentrated in this region. This is likely because, similar to the .com TLD, .net is a generic designation, meaning that it may be used by any number of different organizations or individuals and is not specific to any country or region. It is currently used by approximately 11 percent of all general top-level domains.[57] Therefore, the number of APJ phishing Web sites using .net is in keeping with its distribution on the Internet.

[55] http://www.icannwiki.org/Domain_Statistics
[56] http://www.webhosting.info/registries/country_stats/US
[57] http://www.icannwiki.org/Domain_Statistics

Phishing—protection and mitigation

Symantec recommends that enterprise users protect themselves against phishing threats by filtering email at the server level through the mail transfer agent (MTA). Although this will likely remain the primary point of filtering for phishing, organizations can also use IP-based filtering upstream, as well as HTTP filtering.

DNS block lists also offer protection against potential phishing emails. Organizations could also consider using domain-level or email authentication in order to verify the actual origin of an email message. This can protect against phishers who are spoofing mail domains.[58]

To protect against potential phishing activity, administrators should always follow Symantec best practices as outlined in Appendix A of this report. Symantec also recommends that organizations educate their end users about phishing. They should also keep their employees notified of the latest phishing attacks and how to avoid falling victim to them, and should provide a means to report suspected phishing sites.[59]

Organizations can also employ Web server log monitoring to track if and when complete downloads of their Web sites are occurring. Such activity may indicate that someone is using the legitimate Web site to create an illegitimate Web site that could be used for phishing.

Organizations can detect phishing attacks that use spoofing by monitoring non-deliverable email addresses or bounced email that is returned to non-existent users. They should also monitor the purchasing of cousin domain names by other entities to identify purchases that could be used to spoof their corporate domains.[60] This can be done with the help of companies that specialize in domain monitoring; some registrars even provide this service. End users should follow best security practices, as outlined in "Appendix A" of this report. As some phishing attacks may use spyware and/or keystroke loggers, Symantec advises end users to use antivirus software, antispam software, firewalls, toolbar blockers, and other software detection methods. Symantec also advises end users to never disclose any confidential personal or financial information unless and until they can confirm that any request for such information is legitimate.

Users should review bank, credit card, and credit information frequently. This can provide information on any irregular activities. For further information, the Internet Computer Complaint Center (IC3) has also released a set of guidelines on how to avoid Internet-related scams.[61] Additionally, network administrators can review Web proxy logs to determine if any users have visited known phishing sites.

[58] Spoofing refers to instances where phishers forge the "From:" line of an email message using the domain of the entity they are targeting with the phishing attempt.
[59] A good resource for information on the latest phishing threats can be found at http://www.antiphishing.org
[60] "Cousin domains" refers to domain names that include some of the key words of an organization's domain or brand name; for example, for the corporate domain "bigbank.com" cousin domains could include "bigbank-alerts.com," "big-bank-security.com," and so on.
[61] http://www.ic3.gov/preventiontips.aspx

Spam Trends

Spam is usually defined as junk or unsolicited email sent by a third party. While it is certainly an annoyance to users and administrators, spam is also a serious security concern as it can be used to deliver Trojans, viruses, and phishing attempts, as well as links to malicious Web sites. It could also cause a loss of service or degradation in the performance of network resources and email gateways.

This section of the *APJ Internet Security Threat Report* will discuss developments in spam activity in the APJ region between July 1 and December 31, 2007. The following metric will be discussed:

- Top countries of spam origin

Top countries of spam origin

The nature of spam makes it difficult to identify the location of people who are sending spam. Many spammers try to redirect attention away from their actual geographic location. In an attempt to bypass DNS block lists, they build coordinated networks of bot-infected computers, which allow them to send spam from sites that are distant from their physical location. Following this logic, the region from which the spam originates may not correspond with the region in which the spammers are located. This section will discuss the top 10 originating countries of spam sent from the APJ region during the last six months of 2007.

This discussion is based on data gathered by customer installations of Symantec Brightmail AntiSpam™. This data includes the originating server's IP address, against which frequency statistics are summarized. Each IP address is mapped to a specific country and charted over time.

Twenty-four percent of all spam detected from the APJ region during this period originated in China, the most of any country in the region (table 15). This is the same percentage as originated there in the first half of the year.[62] China accounted for four percent of all worldwide spam in the second half of the year.

Sixty-nine percent of all email detected being sent from China during this period was determined to be spam. This is slightly higher than the previous six-month period.

During this period, China had by far the highest number of spam zombies in the region, accounting for 39 percent of the total. A spam zombie is a computer infected with a bot or some other malicious code that allows email messages to be relayed. The high number of spam zombies in China contributed to the high amount of spam originating there in the second half of 2007. This was also likely influenced by the fact that China had the highest number of bots in the region as well. Many bots are designed to be used mainly to send spam and are detected as spam zombies.

[62] The previous *APJ Internet Security Threat Report* listed this number as 25 percent; however, due to methodological changes over the past six months, figures for the previous reporting period have been revised.

Rank	Country/Region	Current Regional Percentage	Previous Regional Percentage	Current Global Percentage
1	China	24%	24%	4%
2	Taiwan	20%	19%	3%
3	Japan	20%	23%	3%
4	South Korea	17%	19%	3%
5	India	5%	4%	1%
6	Malaysia	4%	2%	1%
7	Thailand	2%	1%	<1%
8	Vietnam	2%	2%	<1%
9	Australia	2%	2%	<1%
10	Singapore	1%	1%	<1%

Table 15. Top 10 countries/regions of spam origin, APJ
Source: Symantec Corporation

The second highest volume of spam detected from the APJ region during this reporting period originated in Taiwan, which accounted for 20 percent of the total, slightly more than the 19 percent recorded in the previous period. The number is likely due to the fact that Taiwan is home to the fourth highest number of spam zombies in the APJ region, with nine percent of the total. It also had the second most bot-infected computers in the region, many of which could be used to send spam.

Taiwan experienced the most dramatic increase in spam in the APJ region in the first half of 2007. At that time, Symantec posited that this may have been due to one or two high-volume, short-term campaigns. However, Taiwan's continued high standing indicates that spammers have become entrenched there. Given the high number of spam zombies and bot-infected computers, it is likely that spammers are using compromised computers, as opposed to legitimate mail servers, as spam relays.

Japan had the third highest volume of spam in the APJ region in the last six months of 2007, accounting for 20 percent of the region's total. This is a decrease from the 23 percent of APJ spam that originated in Japan in the first half of 2007.

Japan had the fourth highest number of bot-infected computers in the region during this period. It also had the sixth highest number of spam zombies in the region. The relatively low numbers for these considerations, combined with the high volume of spam originating in Japan, may indicate that spammers in that country are using compromised mail servers elsewhere to send their bulk messages. Japan has a high number of legitimate email servers that could be used illicitly to relay spam. It is also home to a large number of ISPs. A compromised computer can be used to gain access to the computer's ISP mail server or any other email server that can be accessed by the computer's owner, including free email accounts. Spam can then be sent through the compromised computer to the legitimate mail server and through to its destination. When a country has numerous legitimate mail servers, it is likely that many of them will be used to send spam. This is especially true if any of the servers are wrongly configured and can be used as open relays.[63]

[63] An open mail relay is an SMTP (email) server configured in such a way that it allows anyone on the Internet to relay (i.e. send) email through it.

Appendix A—Symantec 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.
- Turn off and remove services that are not needed.
- 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.
- Always keep patch levels up to date, especially on computers that host public services and are accessible through the firewall, such as HTTP, FTP, mail, and DNS services.
- 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.
- 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.
- Isolate infected computers quickly to prevent the risk of further infection within the organization. Perform a forensic analysis and restore the computers using trusted media.
- 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.
- 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.
- Educate management on security budgeting needs.
- Test security to ensure that adequate controls are in place.
- 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. 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.

Consumer Best Practices

- Consumers should use an Internet security solution that combines antivirus, firewall, intrusion detection, and vulnerability management for maximum protection against malicious code and other threats.
- Consumers should ensure that security patches are up to date and that they are applied to all vulnerable applications in a timely manner.
- Consumers should ensure that passwords are a mix of letters and numbers, and should change them often. Passwords should not consist of words from the dictionary.
- Consumers should never view, open, or execute any email attachment unless the attachment is expected and the purpose of the attachment is known.
- Consumers should keep virus definitions updated regularly. By deploying the latest virus definitions, consumers can protect their computers against the latest viruses known to be spreading in the wild.
- Consumers should routinely check to see if their operating system is vulnerable to threats by using Symantec Security Check at www.symantec.com/securitycheck.
- Consumers should deploy an antiphishing solution. They should never disclose any confidential personal or financial information unless and until they can confirm that any request for such information is legitimate.
- Consumers can get involved in fighting cybercrime by tracking and reporting intruders. 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.
- Consumers should 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. 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.
- Some security risks can be installed after an end user has accepted the end-user license agreement (EULA), or as a consequence of that acceptance. Consumers should read EULAs carefully and understand all terms before agreeing to them.
- Consumers should 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. When users see ads in a program's user interface, they may be looking at a piece of spyware.

Appendix B—Attack Trends Methodology

Attack trends in this report are based on the analysis of data derived from the Symantec Global Intelligence Network, which includes the Symantec DeepSight Threat Management System, Symantec Managed Security Services, and the Symantec Honeypot Network. Symantec combines data derived from these sources for analysis.

Malicious activity by country

To determine the top countries for the "Malicious activity by country" metric, Symantec compiles geographical data on each type of malicious activity to be considered. This includes bot-infected computers, bot command-and-control servers, phishing Web sites, malicious code infections, spam relay hosts, and Internet attacks. The proportion of each activity originating in each country is then determined. The mean of the percentages of each malicious activity that originates in each country is calculated. This average determines the proportion of overall malicious activity that originates from the country in question and is used to rank each country.

Top countries of attack origin

Symantec identifies the national sources of attacks by automatically cross-referencing source IP addresses of every attacking IP with several third-party, subscription-based databases that link the geographic location of systems to source IP addresses. While these databases are generally reliable, there is a small margin of error.

Denial-of-service attacks

Although there are numerous methods for carrying out DoS attacks, Symantec derives this metric by measuring DoS attacks that are carried out by flooding a target with SYN requests. These are often referred to as SYN flood attacks. This type of attack works by overwhelming a target with SYN requests and not completing the initial request, which thus prevents other valid requests from being processed.

In many cases, SYN requests with forged IP addresses are sent to a target, allowing a single attacking computer to initiate multiple connections, resulting in unsolicited traffic, known as backscatter, being sent to other computers on the Internet. This backscatter is used to derive the number of DoS attacks observed throughout the reporting period. Although the values Symantec derives from this metric will not identify all DoS attacks carried out, it will highlight DoS attack trends.

To determine the countries targeted by DoS attacks, Symantec cross-references the target IP addresses of every attack with several third-party, subscription-based databases that link the geographic location of systems to source IP addresses. While these databases are generally reliable, there is a small margin of error.

Sectors targeted by DoS attacks were identified using the same methodology as targeted countries. However, in this case, attackers who were considered were those carrying out a set of DoS attacks that were detected by IDS and IPS software.

Bot-infected computers

Symantec identifies bot-infected computers based on coordinated scanning and attack behavior that is observed in global network traffic. An active bot-infected computer is one that carries out at least one attack per day. This does not have to be continuous; rather, a single computer can be active on a number of different days. Attacks are defined as any malicious activity carried out over a network that has been detected by an IDS or firewall.

For an attacking computer to be considered to be participating in coordinated scanning and attacking, it must fit into that pattern to the exclusion of any other activity. This behavioral matching will not catch every bot-infected computer, and may identify other malicious code or individual attackers behaving in a coordinated way as a botnet. This behavioral matching will, however, identify many of the most coordinated and aggressive bot-infected computers. It will also give insight into the population trends of bot-infected computers, including those that are considered to be actively working in a well coordinated and aggressive fashion at some point in time during the reporting period.

Bot-infected computers by countries and cities

To determine the geolocation of bot-infected computers, Symantec cross-references the IP addresses of every identified bot-infected computer with several third-party subscription-based databases that link the geographic location of systems to IP addresses. While these databases are generally reliable, there is a small margin of error. Only cities that can be determined with a confidence rating of at least four out of five are included for consideration. The data produced is then used to determine the global distribution of bot-infected computers.

Appendix C—Malicious Code Trends Methodology

Malicious code trends are based on statistics from malicious code samples reported to Symantec for analysis. Symantec gathers data from over 120 million client, server, and gateway systems that have deployed Symantec's antivirus products in both consumer and corporate environments. The Symantec Digital Immune System and Scan and Deliver technologies allow customers to automate this reporting process. Observations in this section are based on empirical data and expert analysis of this data. The data and analysis draw primarily from the two databases described below.

Infection database

To help detect and eradicate computer viruses, Symantec developed the Symantec AntiVirus Research Automation (SARA) technology. Symantec uses this technology to analyze, replicate, and define a large subset of the most common computer viruses that are quarantined by Symantec Antivirus customers.

On average, SARA receives hundreds of thousands of suspect files daily from both enterprise and individual consumers located throughout the world. Symantec then analyzes these suspect files, matching them with virus definitions. An analysis of this aggregate data set provides statistics on infection rates for different types of malicious code.

Malicious code database

In addition to infection data, Symantec Security Response analyzes and documents attributes for each new form of malicious code that emerges both in the wild and in a "zoo" (or controlled laboratory) environment. Descriptive records of new forms of malicious code are then entered into a database for future reference. For this report, a historical trend analysis was performed on this database to identify, assess, and discuss any possible trends, such as the use of different infection vectors and the frequency of various types of payloads.

In some cases, Symantec antivirus products may initially detect new malicious code heuristically or by generic signatures. These may later be reclassified and given unique detections. Because of this, there may be slight variance in the presentation of the same data set from one volume of the *Internet Security Threat Report* to the next.

Geographic location of malicious code instances

Several third-party subscription-based databases that link the geographic locations of systems to IP addresses are used along with proprietary Symantec technology to determine the location of computers reporting malicious code instances. While these databases are generally reliable, there is a small margin of error. The data produced is then used to determine the global distribution of malicious code instances.

Appendix D—Phishing Trends Methodology

Phishing attack trends in this report are based on the analysis of data derived from the Symantec Probe Network. Symantec Brightmail AntiSpam data is assessed to gauge the growth in phishing attempts as well as the percentage of Internet mail that is determined to be phishing attempts. Symantec Brightmail AntiSpam field data consists of statistics reported back from customer installations that provide feedback about the detection behaviors of antifraud filters as well as the overall volume of mail being processed.

It should be noted that different monitoring organizations use different methods to track phishing attempts. Some groups may identify and count unique phishing messages based solely on specific content items such as subject headers or URLs. These varied methods can often lead to differences in the number of phishing attempts reported by different organizations.

Top countries hosting phishing Web sites

The data for this section is determined by gathering links in phishing email messages and cross-referencing the addresses with several third-party subscription-based databases that link the geographic locations of systems to IP addresses. In this case, Symantec counts phishing Web sites as the number of unique IP addresses hosting Web pages used for phishing. While these databases are generally reliable, there is a small margin of error. The data produced is then used to determine the global distribution of phishing Web sites.

Phishing Web site top-level domains

The data for this section is determined by deriving the top-level domains of each distinct phishing Web site URL. The resulting top-level domains are tabulated and compared proportionately.

Appendix E—Spam Trends Methodology

The Symantec Probe Network is a system of over two million decoy accounts in over 30 countries that attract email messages from around the world. It encompasses more than 600 participating enterprises and attracts email samples that are representative of traffic that would be received by over 250 million mailboxes. The Probe Network includes accounts in countries in the Americas, Europe, Asia, Africa, and Australia/Oceania.

Spam trends in this report are based on the analysis of data derived from both the Symantec Probe Network as well as Symantec Brightmail AntiSpam field data. Symantec Brightmail AntiSpam software reports statistics to the Brightmail Logistical Operations Center (BLOC) indicating messages processed, messages filtered, and filter-specific data.

Symantec has classified different filters so that spam statistics and phishing statistics can be determined separately. Symantec Brightmail AntiSpam field data includes data reported back from customer installations providing feedback from antispam filters as well as overall mail volume being processed.

Symantec Brightmail AntiSpam only gathers data at the SMTP layer and not the network layer, where DNS block lists typically operate. This is because SMTP-layer spam filtering is more accurate than network-layer filtering and is able to block spam missed at the network layer. Network-layer filtering takes place before email reaches the enterprise mail server. As a result, data from the SMTP layer is a more accurate reflection of the impact of spam on the mail server itself.

Sample set normalization

Due to the numerous variables influencing a company's spam activity, Symantec focuses on identifying spam activity and growth projections with Symantec Brightmail AntiSpam field data from enterprise customer installations. This normalization yields a more accurate summary of Internet spam trends by ruling out problematic and laboratory test servers that produce smaller sample sets.

Top countries of spam origin

The data for this section is determined by calculating the frequency of originating server IP addresses in email messages that trigger antispam filters in the field. The IP addresses are mapped to their host country of origin and the data is summarized by country based on monthly totals. The percentage of spam per country is calculated from the total spam detected in the field.

It should be noted that the location of the computer from which spam is detected being sent is not necessarily the location of the spammer. Spammers can build networks of compromised computers globally and thereby use computers that are geographically separate from their location.

About Symantec

Symantec is a global leader in providing security, storage and systems management solutions to help businesses and consumers secure and manage their information. Headquartered in Cupertino, Calif., Symantec has operations in more than 40 countries. More information is available at www.symantec.com.

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

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

04/08 13585532-1