SYMANTEC ENTERPRISE SECURITY

Confidence in a connected world.

Symantec APJ Internet Security Threat Report

Trends for January–June 07

Volume XII, Published September 2007

Dean Turner
Executive Editor
Symantec Security Response

Stephen Entwisle
Senior Editor
Symantec Security Response

Eric Johnson
Editor
Symantec Security Response

Marc Fossi
Analyst
Symantec Security Response

Joseph Blackbird
Analyst
Symantec Security Response

David McKinney
Analyst
Symantec Security Response

Ronald Bowes
Analyst
Symantec Security Response

Nicholas Sullivan
Analyst
Symantec Security Response

Candid Wueest
Analyst
Symantec Security Response

Ollie Whitehouse
Security Architect—Advanced Threat Research
Symantec Security Response

Zulfikar Ramzan
Analyst—Advanced Threat Research
Symantec Security Response

Jim Hoagland
Principal Software Engineer
Symantec Security Response

Chris Wee
Manager, Development
Symantec Security Response

Contributors

David Cowings
Sr. Manager of Operations
Symantec Business Intelligence

Dylan Morss
Manager
Symantec Business Intelligence

Shravan Shashikant
Principal Business Intelligence Analyst
Symantec Business Intelligence

Volume XII, Published September 2007

Symantec APJ Internet Security Threat Report

Contents

APJ Internet Security Threat Report 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 in the six-month period from January 1 to June 30, 2007. 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.

Symantec has established some of the most comprehensive sources of Internet threat data in the world. The Symantec™ Global Intelligence Network tracks attack activity across the entire Internet. It consists of over 40,000 sensors monitoring network activity in over 180 countries. As well, Symantec gathers malicious code reports from over 120 million client, server, and gateway systems that have deployed Symantec's antivirus products.

Symantec operates one of the most popular forums for the disclosure and discussion of vulnerabilities on the Internet, the BugTraq™ mailing list, which has approximately 50,000 direct subscribers who contribute, receive, and discuss vulnerability research on a daily basis.[1] Symantec also maintains one of the world's most comprehensive vulnerability databases, currently consisting of over 22,000 vulnerabilities (spanning more than a decade) affecting more than 50,000 technologies from over 8,000 vendors.

Finally, the Symantec Probe Network, a system of over two million decoy accounts, attracts email messages from 20 different countries around the world, allowing Symantec to gauge global spam and phishing activity. These resources give Symantec analysts unparalleled sources of data with which to identify emerging trends in attacks and malicious code activity. Symantec also gathers phishing information through the Symantec Phish Report Network, an extensive antifraud community of enterprises and consumers. Members of the network contribute and receive fraudulent Web site addresses for alerting and filtering across a broad range of solutions.

The Symantec *APJ Internet Security Threat Report* is grounded principally on the expert analysis of data provided by all of these sources. By publishing the analysis of Internet security activity in this report, Symantec hopes to provide enterprises and consumers in the APJ region with the information they need to help effectively secure their systems now and in the future.

Executive Summary

The following section will offer a brief summary of the security trends that Symantec observed during the first half of 2007 based on data provided by the sources listed above. This summary includes all of the metrics that are included in the *APJ Internet Security Threat Report*.

[1] The BugTraq mailing list is hosted by SecurityFocus (http://www.securityfocus.com). Archives are available at http://www.securityfocus.com/archive/1

Attack Trends Highlights

- The United States was the country of origin of the most attacks against APJ-based computers, accounting for 29 percent of attacks detected there.
- China was targeted by 74 percent of DoS attacks in the APJ region during this period, an increase over the 63 percent seen during the previous period.
- Symantec observed an average of 15,447 active bot-infected computers per day in the APJ region, 29 percent of the worldwide daily average of 52,771.
- China had the most bot-infected computers in APJ, accounting for 78 percent of the total, up from 71 percent during the second half of 2006.
- Beijing, China was the APJ city with the most bot-infected computers during the first six months of 2007, as it was in the previous reporting period.
- China accounted for 42 percent of malicious activity in the APJ region, the most of any country, up from 39 percent in the previous reporting period.
- Sri Lanka was the most highly ranked country for malicious activity per Internet user, followed by Bangladesh and Taiwan.

Malicious Code Trends Highlights

- Trojans accounted for 51 percent of potential malicious code infections in the APJ region. They made up 73 percent of potential infections worldwide.
- China was the top APJ country for all malicious code types with the exception of worms, for which Japan was the top reporting country.
- The top reported malicious code sample for the APJ region was the Gampass Trojan.
- The most prevalent new malicious code family reported in the APJ region during this period was the Fubalca worm.
- Threats to confidential information made up 57 percent of potential infections by the top 50 malicious code samples in the APJ region, less than the worldwide percentage of 65 percent.
- Of all threats to confidential information in APJ, 79 percent could be used to export user data and 78 percent had a keystroke-logging component.
- SMTP was most common propagation mechanism in the APJ region; it was used by 37 percent of propagating malicious code during this period.

Phishing Trends Highlights

- Japan was home to the highest percentage of phishing Web sites in the APJ region, but only the eighth highest in the world.
- Taipei, Taiwan was the city with the most phishing Web sites in the APJ region in the first six months of 2007, as it was in the previous reporting period.

Spam Trends Highlights

- Twenty-five percent of all spam detected from the APJ region during this period originated in China, more than any other country in the region.
- China was home to more spam zombies than any other APJ country, with 40 percent of the regional total.
- Bangkok, Thailand had highest number of spam zombies of any APJ city during this period.
- Spam made up 70 percent of all monitored email traffic in the APJ region during this reporting period.
- Of the top 20 email-producing countries in the APJ region, Uzbekistan produced the highest percentage of spam, with 88 percent.

Attack Trends

This section of the *APJ Internet Security Threat Report* will provide an analysis of attack activity that Symantec observed in the APJ region between January 1 and June 30, 2007. Attacks are defined as any malicious activity carried out over a network that has been detected by an intrusion detection system (IDS) or firewall.

The Symantec™ Global Intelligence Network, which includes Symantec DeepSight™ Threat Management System and Symantec™ Managed Security Services, tracks attack activity across the entire Internet. It consists of over 40,000 sensors monitoring network activity in over 180 countries. Symantec uses proprietary technologies to monitor bot command-and-control servers across the Internet. These resources give Symantec an unparalleled ability to identify, investigate, and respond to emerging threats. This discussion will be based on data provided by all of these sources.

This section of the *APJ Internet Security Threat Report* will discuss:

- Top countries of attack origin
- Top countries targeted by denial of service attacks
- Active bot-infected computers
- Bot-infected computers by country
- Bot-infected computers by city
- Malicious activity by country
- Malicious activity by country per Internet user

Top countries of attack origin

Over the first six months of 2007, the United States was the country of origin of the most attacks against APJ-based computers, accounting for 29 percent of attacks detected by sensors in the region (table 1). This is slightly higher than the 25 percent of Internet-wide attacks that originated in the United States. This indicates that attacks originating in the United States were likely not targeting the APJ region in particular.

Regional Rank	Previous Regional Rank	Country	Percentage of Regional Attacks	Previous Percentage of Regional Attacks	Percentage of Worldwide Attacks
1	1	United States	29%	39%	25%
2	2	China	18%	19%	13%
3	3	Japan	9%	5%	2%
4	4	Australia	7%	5%	2%
5	8	Argentina	3%	3%	1%
6	12	Spain	3%	2%	5%
7	10	Canada	3%	2%	4%
8	7	United Kingdom	2%	3%	5%
9	11	Germany	2%	2%	8%
10	9	France	2%	2%	6%

Table 1. Top countries of origin of attacks targeting the APJ region
Source: Symantec Corporation

This high rate of attacks is partially due to the United States having the highest number of broadband connections in the world, with 20 percent of all connections.[2] The United States also hosts 18 percent of all worldwide Internet connections.[3] As a result, computers there are more likely to become infected with worm or bot software and, once infected, can launch more attacks that can be detected by sensors.

Users in the United States may be attacking countries in the APJ region in an attempt to establish bot networks. It is possible that attackers in the United States target APJ-based countries more frequently than other countries because they believe that computers in the APJ region, particularly in China, are easier targets than computers in the rest of the world.[4] This belief may be caused by the fact that China has 29 percent of bot-infected computers in the world, higher than any other country.[5] Attackers attempting to exploit computers to install bot software likely know that China is prone to bot infections, so it is possible that they target Chinese IP ranges. These attackers may see this high proportion of bots as an indication that the region is more susceptible and, therefore, a better target. The reasons for the high numbers of bot infections in China will be discussed in greater depth in the "Bot-infected computers by country" section below.

China was the country of origin of the second highest percentage of attacks detected by sensors in the APJ region during this period, accounting for 18 percent of the total. China accounted for 13 percent of attacks detected by sensors worldwide.

China's high position is likely due the number of broadband connections in the country. China has the second highest number of broadband connections in the world, with 20 percent of broadband connections, which is just behind the United States.[6] China also hosts 13 percent of all Internet connections in the world.[7] With more connected computers, worms and bots in China have more opportunity to attack.

In previous versions of the *Internet Security Threat Report*, Symantec has noted that attackers typically target their own region.[8] This is likely because local organizations tend to have higher profiles and, therefore, make more attractive targets for local attackers. It is also likely due to factors such as sharing a common language and living in a nearby time zone. The trend is reinforced by the fact that several APJ countries—China, Japan, and Australia—all attack the APJ region more frequently than they attack the rest of the world. China's higher ranking for attacks against the APJ region is likely a result of this tendency.

The high percentage of attacks originating in China may also be linked to the fact that China hosts 78 percent of bots in APJ and 29 percent of bots worldwide. Since attacking vulnerable computer systems is necessary when building and expanding bot networks, bots are often instructed to attack random IP addresses much like worms do when propagating. Since the number of bot-infected computers is higher in China than any other country,[9] the high number of attacks coming from China may be caused by bot-infected computers in China. That said, bot-related attack activity may not be initiated by attackers in China. Bots in that country are likely being controlled by command-and-control servers that are situated outside the country, as is discussed in greater depth in the "Active bot-infected computers" section below.

[2] http://www.point-topic.com
[3] http://www.internetworldstats.com
[4] http://www.usatoday.com/tech/news/computersecurity/infotheft/2005-03-29-chinese-phishers_x.htm
[5] For more information on bot-infected computer rankings, please see the main *Internet Security Threat Report*: http://www.symantec.com/enterprise/theme.jsp?themeid=threatreport
[6] http://www.point-topic.com
[7] http://www.internetworldstats.com
[8] Symantec *Internet Security Threat Report*, Volume IX (March 2006): http://eval.symantec.com/mktginfo/enterprise/white_papers/ent-whitepaper_symantec_internet_security_threat_report_ix.pdf : p. 13
[9] For more information on bot-infected computer rankings, please see the main *Internet Security Threat Report*: http://www.symantec.com/enterprise/theme.jsp?themeid=threatreport

Japan was the originating country of the third highest number of attacks detected by sensors deployed in the APJ region, accounting for nine percent of the regional total. This is significantly higher than the two percent of Internet-wide attacks originating in Japan during this period, which would indicate that attacks originating there were targeting the APJ region specifically. This is likely related to geographical considerations. As noted above, countries have a tendency to attack targets in their own region. As such, it is not surprising that Japan had a higher proportion of attacks against the APJ region than worldwide.

Like the United States and China, Japan's ranking is likely attributable to the high number of broadband connections there. Japan has the third highest number of broadband connections in the world behind the United States and China, with nine percent of all connections.[10] Japan also has the third highest number of Internet users, with eight percent of the worldwide total.[11]

Top countries targeted by denial of service attacks

This metric will assess the geographic location of targets of denial of service (DoS) attacks. Insight into the locations targeted by these attacks is valuable in determining global trends in DoS attack patterns. It may also help administrators and organizations in affected countries to take the necessary steps to protect against or minimize the effects of DoS attacks.

DoS 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. This could result in the disruption of organizational communications, a significant loss of revenue, and/or damage to the organization's reputation. Furthermore, as Symantec discussed in a previous *Internet Security Threat Report*, criminals have been known to use DoS attacks in extortion schemes.[12]

Over the first six months of 2007, China was the APJ country most frequently targeted by DoS attacks, accounting for 74 percent of attacks in the region during this period (table 2). This is a large increase over the 63 percent seen during the previous period.

Regional Rank	Previous Regional Rank	Country	Percentage of Regional Attacks	Previous Percentage of Regional Attacks	Percentage of Worldwide Attacks
1	1	China	74%	63%	8%
2	4	Australia	11%	4%	1%
3	2	South Korea	5%	13%	1%
4	5	Japan	4%	4%	0%
5	3	Taiwan	2%	8%	0%
6	7	Singapore	1%	2%	0%
7	9	New Zealand	1%	1%	0%
8	6	Thailand	1%	2%	0%
9	8	Malaysia	0%	1%	0%
10	10	Indonesia	0%	1%	0%

Table 2. Top countries targeted by DoS attacks, APJ region
Source: Symantec Corporation

[10] http://www.point-topic.com
[11] http://www.internetworldstats.com/top20.htm
[12] Symantec *Internet Security Threat Report*, Volume VIII (September 2005): http://eval.symantec.com/mktginfo/enterprise/white_papers/ent-whitepaper_symantec_internet_security_threat_report_viii.pdf : p. 11 and 30

DoS attacks against Web sites are likely more common than DoS attacks against computers belonging to individual users. Attackers typically launch DoS attacks to protest an unpopular decision by a government or company, or, in some cases, as part of an extortion attempt.

Attackers that make use of DoS attacks likely want their DoS attacks to be noticed by as many people as possible. An organization's Web site is its primary online public presence, so it is logical for an attacker to attempt to block access to it as a form of protest.[13] This can be even more damaging to online stores, since it blocks users' ability to purchase goods, which could disrupt the organization's revenue stream. Therefore, attackers are likely to target Web sites, as opposed to individual users or other organizational resources. As China hosts the most Web sites in the APJ region, it is logical that it should also be the target of the most DoS attacks.[14]

Australia was targeted by the second highest number of DoS attacks in the APJ region in the first half of 2007. It was targeted by 11 percent of attacks during this period, up from four percent in the second half of 2006, when it was ranked fourth. As this metric is a proportional measure, Australia's increase was likely caused by a decrease in DoS attacks detected in South Korea, which fell from 13 percent to five percent, and Taiwan, which fell from eight percent to two percent in the past six months.

Australia has the second highest number of Web sites in the APJ region, behind China,[15] which likely influences the country's rank in this metric. Australia had the highest increase in the total number of Web sites in APJ in the first six months of 2007, along with the second highest increase worldwide (behind the United States).[16] This increase, combined with South Korea and Taiwan's decrease, were likely the primary contributors to Australia's heightened position in this period.

South Korea was targeted by the third highest number of DoS attacks in the APJ region,[17] accounting for five percent of attacks during this period. This is a decrease from 13 percent in the second half of 2006, when South Korea was the second most targeted country. South Korea's ranking may be related to the number of Web sites located there; South Korea has the fourth highest number of Web sites in the APJ region, behind China, Australia, and Japan. It may also be the result of the popularity of online games there.

In Volume XI of the Symantec *Internet Security Threat Report* for APJ,[18] Symantec speculated that the high proportion of DoS attacks against South Korea may be a result of a high interest in online games.[19] A large amount of money is involved with online games and virtual assets, enough that the Korean government has started taxing some virtual transactions.[20] Attackers may have seen an opportunity in attacking online games for purposes such as extortion. DoS attacks against game servers may also provide attackers with an opportunity to phish for account information.[21] Since game servers are typically located in the same country as the majority of the players,[22] many servers for popular games are likely located in South Korea.

Organizations should ensure that a documented procedure exists for responding to DoS events. One of the best ways to mitigate a DoS attack is to filter upstream of the target. For most organizations, this filtering will involve working in conjunction with their Internet service provider (ISP). Symantec also recommends that organizations perform egress filtering on all outbound traffic. DoS victims frequently need to engage their upstream ISP to help filter the traffic to mitigate the effects of attacks.

[13] One example of a defacement attack can be seen here: http://www.symantec.com/security_response/vulnerability.jsp?bid=symantec.enterprise.security.products.protect.against.potential.chinese-based.attacks#
[14] Based on the number of unique domain names registered: http://www.webhosting.info/domains/country_stats/
[15] Based on the number of unique domain names registered: http://www.webhosting.info/domains/country_stats/
[16] Based on the number of unique domains registered, sorted by net gain: http://www.webhosting.info/domains/country_stats/?ob=NET&oo=DESC
[17] Based on the number of unique domain names registered: http://www.webhosting.info/domains/country_stats/
[18] *Internet Security Threat Report* for APJ, Page 10
[19] http://news.com.com/Consumers+Gaming+their+way+to+growth+-+Part+3+of+South+Koreas+Digital+Dynasty/2009-1040_3-5239555.html
[20] http://kotaku.com/gaming/one-of-the-only-certainties-in-life/south-korea-to-tax-virtual-assets-273957.php
[21] For example, attackers may deny service to a game server before emailing users a supposed "support" message asking for account information. Although this type of attack is not widespread, it is possible that some attackers have attempted it.
[22] Large geographical separation between players and servers can cause delays in gameplay while data is in transit. See http://www-03.ibm.com/industries/media/doc/content/bin/Games_LOB_G565_1461_00_hi-rez.pdf page 21.

Active 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). These channels allow the remote attacker to control a large number of compromised computers over a single, reliable channel in a bot network, 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 an organization's Web site. Furthermore, bots within an organization's network can be used to attack other organizations' Web sites, which can have serious business and legal consequences.

Bots can be used by attackers to harvest confidential information from compromised computers, which can lead to identity theft. They can also be used to distribute spam and phishing attacks, as well as spyware, adware, and misleading applications.

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. Between January 1 and June 30, 2007, Symantec observed an average of 15,447 active distinct bot-infected computers per day in the APJ region (figure 1). This was a 19 percent decrease from the 19,095 active bot-infected computers per day in the APJ region during the previous reporting period. The APJ region accounted for about 29 percent of the 52,771 worldwide active bot-infected computers in an average day.

The number of active bot-infected computers per day in APJ has been steady over the past 12 months (figure 1). This likely indicates that no recent bot infection has propagated specifically in the APJ region over the past 12 months.

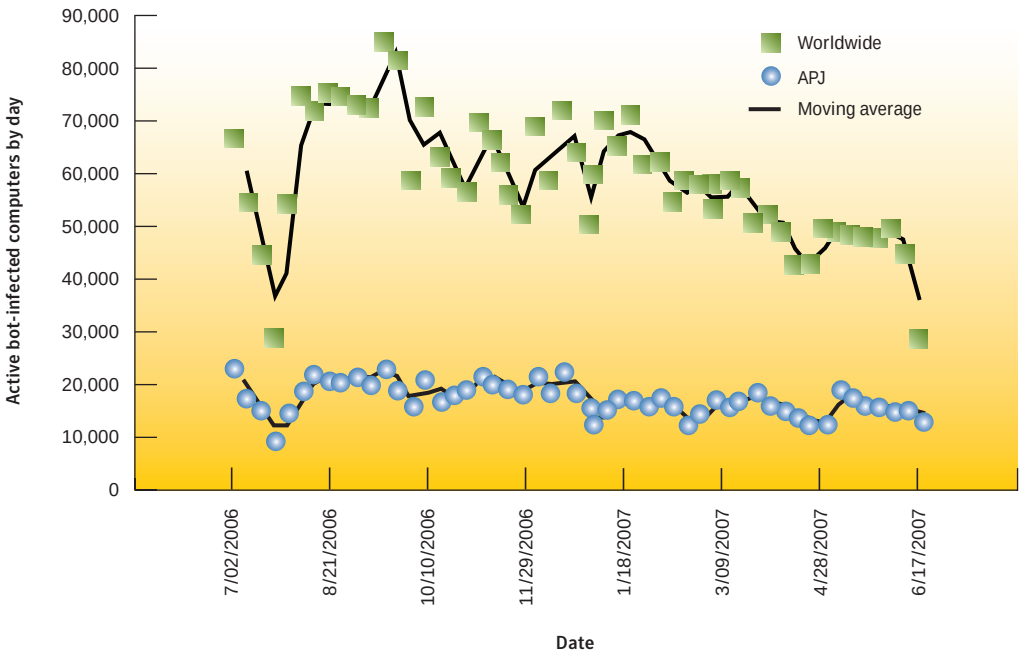

Figure 1. Active bot-infected computers per day, APJ region
Source: Symantec Corporation

A distinct bot-infected computer is a distinct computer that was active at least once during the period. In the first half of 2007, Symantec identified 1,782,416 distinct bot-infected computers that were considered active in APJ at any one point in time (or more) during the period. This is 35 percent of the 5,029,309 active distinct bot-infected computers detected worldwide during this period. It is also 21 percent less than the 2,268,219 active bot-infected computers that Symantec identified in the APJ region during the second half of 2006. Likewise, the number of bot-infected computers worldwide fell by 17 percent.

The primary reason for the decrease in bots observed over the past six months is likely a change in bot attack methods. As has been discussed in previous volumes of the Symantec *Internet Security Threat Report*, the exploitation of network-based vulnerabilities to distribute bots is being abandoned for methods that are more likely to succeed, such as bots that send a mass mailing of themselves.[23] The introduction of default firewalls in popular operating systems such as Microsoft Windows XP, as well as a generally increasing awareness of computer security issues among organizations and computer users has made these forms of attack less likely to succeed. As a result, their use has declined.

Bot-infected computers may be attacking more quietly in an attempt to remain undetected. Bots making quiet and slow attacks may be increasingly indistinguishable from Internet background noise caused by worms, misconfigured systems, or ordinary traffic that is detected as being malicious.[24]

Symantec also tracks the number of bot command-and-control servers in each region. Command-and-control servers are computers that bot network owners use to relay commands to bot-infected computers on their networks. During the first six months of 2007, 16 percent of worldwide command-and-control servers were located in the APJ region, compared to the 35 percent of active bot-infected computers that are located in the region. In the previous period, APJ hosted 23 percent of command-and-control servers and 34 percent of active bot-infected computers.

The discrepancy between command-and-control servers and bot-infected computers is important, as it indicates that bots in APJ are likely being controlled by command-and-control servers that are situated outside the region. This means that attack activity originating in the region is not necessarily being initiated by computers located in the APJ region. This supports the speculation in the “Top attacking countries” section of this report that the prevalence of attack activity originating in China may be partly due to attack activity controlled by attackers in countries outside the APJ region.

To reduce exposure to bot-related attacks, end users should employ defense-in-depth strategies, including the deployment of antivirus software and a firewall.[25] 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.

[23] For instance, please see the Symantec *Internet Security Threat Report*, Volume IX (March 2006): http://eval.symantec.com/mktginfo/enterprise/white_papers/ent-whitepaper_symantec_internet_security_threat_report_ix.pdf : p. 30
[24] For more information on Internet background noise, see http://www.switch.ch/security/services/IBN/
[25] Defense-in-depth strategies emphasize multiple, overlapping, and mutually supportive defensive systems to guard against single-point failures in any specific technology or protection methodology. They should include the deployment of antivirus, firewalls, and intrusion detection systems, among other security measures.

Bot-infected computers by country

Recognizing the ongoing threat posed by bot networks, Symantec tracks the distribution of bot-infected computers both worldwide and across the APJ region. In order to do this, Symantec calculates the number of computers worldwide that are known to be infected with bots, and assesses which countries within the APJ 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.

Between January 1 and June 30, 2007, China had the highest number of bot-infected computers in the APJ region, accounting for 78 percent of the total (table 3). This is an increase from the 71 percent during the second half of 2006 when China also had the most bot-infected computers in the APJ region.

In Volume XI of the Symantec *Internet Security Threat Report*, Symantec speculated that the number of new users adopting high-speed Internet in a country may be a significant factor in the rate of bot infections.[26] Frequently, rapidly expanding ISPs will focus their resources on meeting growing broadband demand at the expense of implementing adequate security measures, such as port blocking and ingress and egress filtering. As a result, they may have security infrastructures and practices that are insufficient for their needs. Furthermore, it is also likely that home users and system administrators in rapidly expanding countries are also struggling to adapt their security practices and policies to deal with broadband Internet.

Between May 2006 and May 2007, China had a greater increase in broadband connections than any other country in the world. China has the highest number of broadband connections in APJ, with 52 percent, and the second highest number of broadband connections in the world, below the United States.[27] China's high percentage of bot infections is likely related to China's broadband penetration and growth.

This high percentage of bot infections may be related to a high rate of software piracy in China. Pirated software is often unable to receive updates.[28] As a result, it may be more vulnerable to successful exploitation. Because many bots use these types of vulnerabilities to propagate, countries with higher piracy rates will likely have a higher percentage of bot infections than they otherwise would.

In 2006, China's software piracy rate was 82 percent, which is significantly higher than the regional average of 55 percent and the worldwide average of 35 percent.[29] With the highest number of broadband connections in the APJ region and a relatively high percentage of pirated software, China likely has more computers on the Internet that are vulnerable to attack than other APJ countries.

Of the top ten bot-infected countries, five have higher piracy rates than the APJ average: China, Malaysia, the Philippines, Thailand, and Vietnam.[30] Because these countries, with the exception of China, have relatively low numbers of broadband connections,[31] their position in the top ten bot-infected countries are likely due to higher-than-average piracy rates.

[26] http://eval.symantec.com/mktginfo/enterprise/white_papers/ent-whitepaper_internet_security_threat_report_xi_03_2007.en-us.pdf page 36
[27] http://www.point-topic.com
[28] http://www.msnbc.msn.com/id/6868504/
[29] http://w3.bsa.org/globalstudy//upload/2007-Losses-Global.pdf
[30] http://w3.bsa.org/globalstudy//upload/2007-Losses-Global.pdf
[31] Malaysia, the Philippines, Thailand, and Vietnam collectively host two percent of all broadband connections in the APJ region. http://www.point-topic.com.

Regional Rank	Previous Regional Rank	Country	Percentage of Regional Bots	Previous Percentage of Regional Bots	Percentage of Worldwide Bots	Average Lifespan (days)	Percentage of Command-and-Control Servers
1	1	China	78%	71%	29%	3	22%
2	2	Taiwan	7%	11%	3%	2	18%
3	3	South Korea	5%	6%	2%	3	37%
4	4	Japan	2%	3%	1%	6	9%
5	5	Australia	2%	3%	1%	4	4%
6	6	Malaysia	1%	1%	<1%	3	3%
7	7	Singapore	1%	1%	<1%	4	2%
8	8	Philippines	1%	1%	<1%	4	<1%
9	9	Thailand	1%	1%	<1%	5	2%
10	10	Vietnam	0%	0%	<1%	4	<1%

Table 3. Bot-infected computers by country, APJ region
Source: Symantec Corporation

Taiwan accounted for seven percent of bot-infected computers in the APJ region in the first half of 2007, the second highest total in the region. This is a decrease from the previous reporting period where Taiwan accounted for 11 percent of bot-infected computers in APJ, when it was also the second ranked country in the region. Taiwan has the fourth highest number of broadband connections in APJ, accounting for four percent of connections in the region.

Taiwan had the lowest rate of broadband growth in APJ between May 2006 and May 2007, increasing its number of broadband connections by only seven percent.[32] This may explain why the proportion of bot-infected computers decreased over the past six months. Because Taiwan's broadband is not expanding particularly quickly, ISPs may be catching up to security requirements. Taiwanese ISPs may thus be taking a more active approach to bot infections.

As broadband use becomes established in Taiwan, users there may also be more aware of security issues, such as bots, and may be more capable of adequately securing their computers against such threats. This is supported by the shorter lifespan of bots in Taiwan, where an average bot is only active for two days, compared to the regional average of three days and the worldwide average of four days.

The country's decrease in bot-infected computers may also be attributed to Taiwanese officials working with the US Federal Bureau of Investigation (FBI) on their recent program,[33] Bot Roast, which is an attempt by the FBI to find and eliminate bot infections. This relationship between the FBI and Taiwan might mean that Taiwan, like the FBI, is beginning to take a more active approach towards eliminating bot infections.[34]

South Korea had the third highest number of bot-infected computers in the APJ region, with five percent of the total. This is a small decrease from six percent during the previous reporting period, when South Korea also had the third highest number of bot-infected computers. Because this is a proportional measure, this decrease was likely a result of the increase in China's percentage, not an actual decrease in bots in South Korea.

[32] http://www.point-topic.com
[33] http://www.taiwanheadlines.gov.tw/fp.asp?xItem=51397&CtNode=47
[34] http://www.fbi.gov/page2/june07/botnet061307.htm

The high percentage of bots in South Korea may be related to the amount of time spent online in South Korea. A recent study showed that users in South Korea spend more time online than any other country in APJ and the third most time online worldwide (behind Canada and Israel).[35] Users that spend more time online have more of an opportunity to become infected by Trojans or other malicious programs.

In addition to bots, South Korea also has the most command-and-control servers in the region, with 37 percent. This is likely a result of South Korea being a highly connected country. South Korea has the third highest number of broadband connections in the APJ region, and one of the lowest rates of broadband growth.[36] This likely implies that Internet users in South Korea are familiar with the Internet and have higher-than-average technical experience. Since setting up and maintaining a command-and-control server requires some level of expertise, sometimes including programming knowledge for modifying standard IRC servers, countries with users who have more technical experience are more likely to have high numbers of command-and-control servers.

Bot-infected computers by city

Beijing, China was the APJ city with the highest number of bot-infected computers during the first six months of 2007 (table 4), which is unchanged from the previous reporting period. Chinese cities now account for nine of the top ten bot-infected cities in APJ, up from seven during the previous reporting period. Since China accounts for 78 percent of all bots in APJ, it is not surprising that the most bot-infected cities would be in China. In addition to having the vast majority of bots in the region, China also has a very large population spread out in a number of large cities,[37] so bot-infected computers are distributed widely throughout the country. As a result, many cities in China have significant numbers of bot-infected computers.

Regional Rank	Previous Regional Rank	City	Country
1	1	Beijing	China
2	2	Guangzhou	China
3	3	Hangzhou	China
4	4	Shanghai	China
5	5	Ningbo	China
6	7	Fuzhou	China
7	6	Kuala Lumpur	Malaysia
8	10	Liuzhou	China
9	14	Changsha	China
10	13	Wuhan	China

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

[35] http://www.websiteoptimization.com/bw/0703/
[36] South Korea has the third highest number of broadband connections in the APJ region and, like Japan, has a relatively low growth: 13.19 percent. For more information, see http://point-topic.com/contentDownload/dslanalysis/world%20broadband%20statistics%20q1%202007.pdf (requires free registration).
[37] http://www.paulnoll.com/China/Population/population-distribution.html

Guangzhou, China had the second highest number of bot-infected computers in the APJ region. This is unchanged from the previous reporting period. Hangzhou, China was ranked third in the region. This is also unchanged from the previous reporting period. All three top cities in APJ were also ranked in the top ten worldwide cities for bot-infected computers.

Because China has more broadband connections than any other country in the APJ region, with 52 percent of all APJ broadband connections, it has more potential bot targets than other countries in the region. For this reason alone, attackers who randomly scan for new computers to infect will scan China more frequently than other APJ countries. In some cases, attackers may target countries that they perceive to have weaker defenses in an attempt to collect as many bots as possible with the lowest risk to themselves and to their bot networks.[38] This type of attacker may infect a disproportionately high number of computers in China.

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

Malicious activity by country

This metric will assess the countries in which the highest amount of malicious activity takes place or originates. To determine this, Symantec has compiled geographical data on numerous malicious activities that are based in APJ countries, namely: bot-infected computers, bot command-and-control servers, phishing Web sites, malicious code reports, spam zombies, and Internet attacks.

To determine the amount of Internet-wide malicious activity that originated in each country, Symantec calculated the mean average of the proportions of all of the aforementioned activities that originated in each country. This average was taken to represent the proportion of overall malicious activity that originated in the country in question and was used to rank each country within the APJ region. This section will discuss those findings.

In the first six months of 2007, China accounted for 42 percent of malicious activity in the APJ region, the most of any country (table 5). This is a small increase from 39 percent in the previous reporting period, when it was also the top ranked country in the region. China accounts for the majority of broadband connections in the APJ region, with 52 percent of broadband connections in the region.[39]

China continues to be the top-ranked country for most metrics, with the exception of command-and-control servers and phishing Web sites, for both of which China ranked second. These high rankings are likely a result of China having a higher number of broadband connections and a higher rate of broadband adoption than any other country in APJ.[40] More broadband connections mean that more computers are online that can potentially become infected with malicious code, and a high broadband gain means that more inexperienced users have Internet connections.

[38] http://www.usatoday.com/tech/news/computersecurity/infotheft/2005-03-29-chinese-phishers_x.htm
[39] http://www.point-topic.com
[40] http://www.point-topic.com

Malicious activity by country per Internet user

Having evaluated the top countries in APJ by malicious activity, Symantec also evaluated the top 15 of these countries according to the number of Internet users located there. This measure is intended to remove the bias of countries with a large population of Internet users from the consideration of the "Malicious activity by country" metric.

In order to determine this, Symantec divided the amount of malicious activity originating in each of the top 15 countries in the APJ region by the number of Internet users who are located in that country. The proportion assigned to each country in this discussion thus equates to the proportion of malicious activity that could be attributed to a single (average) Internet user in that country. The proportion of malicious activity that would be carried out by each person is the proportion assigned to each country in the discussion below.

Sri Lanka was the most highly ranked country for malicious activity per Internet user in the APJ during the first six months of 2007. If one person from each of the top 15 countries were assessed as a representation of their country's Internet users, the average user in Sri Lanka would carry out 21 percent of the group's malicious activity (table 6). Sri Lanka was previously ranked in fifth place. This increase is mostly due to some new command-and-control servers that were detected there, combined with the relatively small Internet population.

Regional Rank	Previous Regional Rank	Country	Proportion of Regional Activity
1	5	Sri Lanka	21%
2	3	Bangladesh	17%
3	1	Taiwan	14%
4	2	Singapore	13%
5	4	South Korea	9%
6	7	China	6%
7	6	Australia	5%
8	9	Thailand	5%
9	12	Malaysia	3%
10	8	New Zealand	3%

Table 6. Malicious activity by country per Internet user
Source: Symantec Corporation

Bangladesh accounted for 17 percent of malicious activity per Internet user, the second highest percentage in the region, a small increase from their previous ranking of third place. Bangladesh's position is largely influenced by some new phishing Web sites that were detected, as well as several new command-and-control servers.

Taiwan ranked third, accounting for 14 percent of malicious activity per Internet user, a fall from the previous reporting period, when it was first place. The drop was largely influenced by the drop in bot-infected computers in Taiwan, which is discussed in the "Bot-infected computer by country" discussion of this report.

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 January 1 and June 30, 2007.

In previous editions of the Symantec *Internet Security Threat Report*, the number and volume of threats analyzed were based upon the number of malicious code reports received from enterprise and home users. However, this report will examine malicious code according to potential infections. This will allow Symantec to determine which malicious code sample was attempting to infect computers and the number of potential infections worldwide.

Symantec categorizes malicious code in two ways: families and variants. A family is a new, distinct sample of malicious code. For instance, W32.Sober@mm (also known as Sober) was the founding sample, or the primary source code, of the Sober family. In some cases, a malicious code family may have variants. A variant is a new iteration of the same family, one that has minor differences but that is still based on the original. A new variant is created when the source code of a successful virus or worm is modified slightly to bypass antivirus detection definitions developed for the original sample. For instance, Sober.X is a variant of Sober.

The "Malicious Code Trends" section will discuss:

- Malicious code types
- Geolocation by type
- Top ten malicious code samples
- Top three new malicious code families
- Threats to confidential information
- Propagation mechanisms
- Malicious code—prevention and mitigation

Malicious code types

In the first half of 2007, worms made up 42 percent of potential malicious code infections in the APJ region (figure 2) and 22 percent of worldwide.[43] Six of the top ten malicious code samples reported in APJ during this reporting period were worms, which demonstrates their continued ability to propagate in significant numbers within the region.

This is likely due to a lack of port blocking and email attachment scanning by ISPs and enterprises in the region. Typically, when a country experiences significant Internet user growth, as is currently occurring in China,[44] ISPs struggle to keep up with the demands placed on expanding their infrastructure. As a result, they are often not able to place significant emphasis upon securing their networks. At the same time, a large influx of new users on their networks may bring an abundance of computers that do not have security patches installed yet. If these users do not have sufficient security applications installed such as antivirus and firewalls, they may be susceptible to older worms that are no longer as common in other regions and countries.

[43] Some malicious code samples are categorized as being more than one threat type. As a result, cumulative percentages in this discussion may exceed 100 percent.
[44] http://www.networkworld.com/news/2007/071907-china-hits-162-million-internet.html

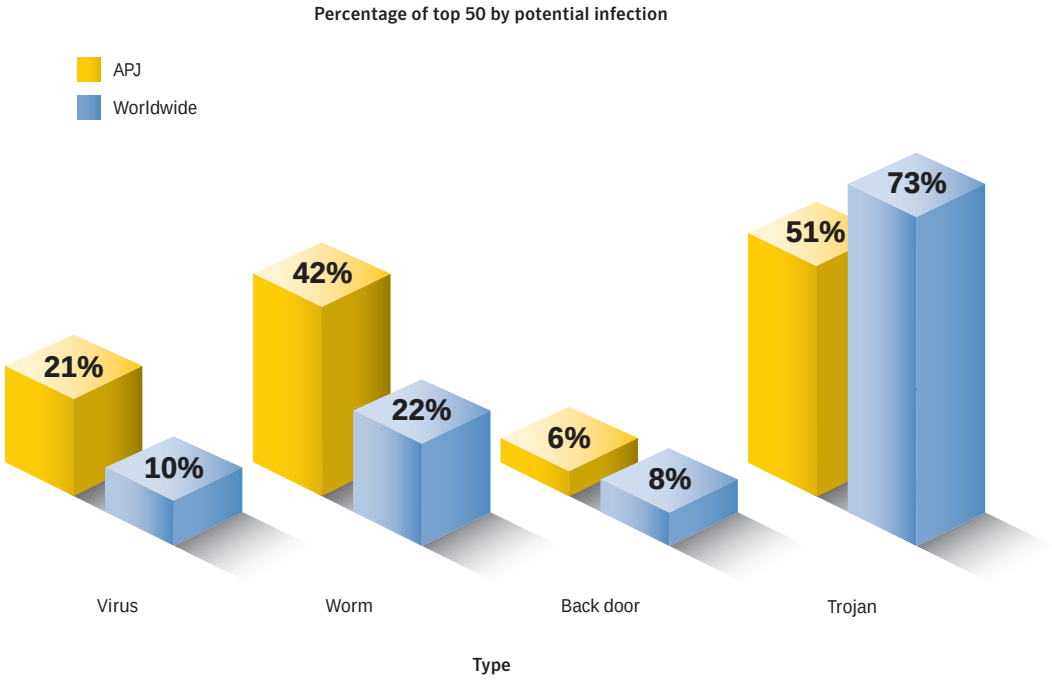

Figure 2. Malicious code types by potential infection
Source: Symantec Corporation

While the general effectiveness of worms has declined in other regions, particularly over the last two six-month reporting periods, this does not yet appear to be the case in the APJ region.[45] This likely indicates that worms are still experiencing a high enough degree of success in the region for attackers to continue creating them in large numbers.

Many of the worms that are prominent in the APJ region are tailored specifically towards users in the region. For example, the Antinny worm was propagates over Winny, a Japanese peer-to-peer (P2P) file-sharing program, and was one of the top ten malicious code samples observed in the region.[46] Other worms, such as Looked.BK,[47] also caused significant numbers of potential infections in the region. Looked.BK specifically disables Chinese language security applications.

To protect against worms, administrators should configure their email server to block or remove email that contains file attachments that are commonly used to spread viruses, such as .vbs, .bat, .exe, .com, .pif, and .scr files. Users should update antivirus definitions regularly. 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.

In general, as the effectiveness of worms has declined, attackers have shifted their efforts towards Trojans instead. During the first six months of 2007, Trojans accounted for 51 percent of potential malicious code infections in the APJ region. During the same period, they made up 73 percent of potential infections worldwide.[48]

[45] The Symantec *Internet Security Threat Report*, Volume XI (March 2006): http://eval.symantec.com/mktginfo/enterprise/white_papers/ent-whitepaper_internet_security_threat_report_xi_03_2007.en-us.pdf : p. 55, 57
[46] http://www.symantec.com/security_response/writeup.jsp?docid=2003-080817-4045-99
[47] http://www.symantec.com/security_response/writeup.jsp?docid=2006-112813-0222-99
[48] It should be noted that several malicious code samples reported in this period are categorized under more than one type, as a result, cumulative percentages included in this discussion may exceed 100 percent.

The lower percentage of Trojans in APJ than worldwide is not entirely due to lower volumes, but also to a higher proportion of viruses and worms in the region. Although worms and viruses make up a significant proportion of the malicious code samples in the region, Trojans still have a significant presence. In fact, the most frequently reported malicious code sample in the APJ region this period was the Gampass Trojan, as is discussed in the "Top ten malicious code samples" section of this report. In the first half of 2007, three of the top ten samples in the region were Trojans, which indicates that an increase in Trojans may be observed in upcoming periods.

Trojans can expose confidential information, and can be used to install other malicious programs. Attackers are currently moving towards staged downloaders. These are small, specialized Trojans that download and install other malicious programs, such as back doors or worms. Many of these Trojans are installed using Web browser vulnerabilities and zero-day vulnerabilities in other applications.

To protect against Trojans, users should avoid executing software that is downloaded from the Internet unless it has been scanned for viruses. They should also ensure that all desktop, laptop, and server computers are updated with all necessary security patches from their operating system vendor. Simply visiting a compromised Web site can cause infection if certain browser vulnerabilities are not patched.

Viruses made up 21 percent of the volume of the top 50 malicious code reports in the APJ region during this reporting period, compared to 10 percent worldwide. Two of the top ten malicious code samples in the APJ region this period were worms, and all three of the top new malicious code families in the region were viruses or employed a viral component.

Potential infections for most of these viruses were reported in high numbers in China and employed features that were specific towards Chinese language programs like the Whybo virus,[49] which attempts to close the application windows of Chinese security programs. This is discussed in further detail in the "Top three new malicious code families" section of this report.

Geolocation by type

As has been stated previously, in this edition of the *Internet Security Threat Report*, Symantec is examining the top countries reporting potential malicious code infections. It is also assessing the types of malicious code causing those potential infections. 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.

In the first six months of 2007, China was the top APJ country for all malicious code types with the exception of worms. This is likely due in part to the rapid growth in Internet connectivity China, where the Internet population growth is outpacing that of the United States.[50] With so many new users coming online at such a high rate, it is likely that many of them are unaware of the threats they may encounter and how to protect themselves against those threats. For three of the top five malicious code samples this period, potential infections were reported most frequently from China including the top two threats, Gampass and Looked.BK.

[49] http://www.symantec.com/security_response/writeup.jsp?docid=2007-040316-2416-99
[50] http://www.pewinternet.org/PPF/r/218/report_display.asp

Rank	Top Country
1	China
2	Japan
3	Australia

Table 7. Top three countries for Trojans, APJ
Source: Symantec Corporation

Japan was the second ranked APJ country of origin for Trojans, viruses, and back doors, while it was the highest ranked for worms. Five of the top ten malicious code samples this period caused the most potential infections in Japan. Of these five, four were worms and the fifth was a virus. Mass-mailing worms such as Netsky.P were more frequently reported from Japan than any other country in the region during this period.

Rank	Top Country
1	Japan
2	China
3	Australia

Table 8. Top three countries for worms, APJ
Source: Symantec Corporation

One of the worms, Antinny,[51] propagates through the Winny P2P file-sharing network. This P2P network was created in Japan and has a large number of users there. It was originally developed to offer users anonymity to download copyrighted works. Since this network operates in an illegal fashion, it is likely that files shared are not controlled in any way. Frequently, users search for programs called “cracks” and “key generators” that are used to break copy protection on legitimate applications. Many worms that propagate through P2P networks use names that make them appear to be these cracks and key-generators.

Rank	Top Country
1	China
2	Japan
3	Taiwan

Table 9. Top three countries for viruses, APJ
Source: Symantec Corporation

Rank	Top Country
1	China
2	Japan
3	Australia

Table 10. Top three countries for back doors, APJ
Source: Symantec Corporation

[51] http://www.symantec.com/security_response/writeup.jsp?docid=2003-080817-4045-99

In the first six months of 2007, Australia reported the third highest number of potential infections of Trojans, worms, and back doors. Australia experienced a large growth in registered domains this period, second only to the United States.[52] This indicates that more local Web sites are being created to service the needs of a growing online population.

As a result of this growth, attackers appear to be targeting Australian users, as was evidenced by the Nuklus Trojan attack in February of this year.[53] In this attack, an email message was spammed to Australian users that claimed that the Australian Prime Minister had suffered a heart attack. The message contained URLs that appeared to link to news articles about the incident; instead, the links led to malicious Web sites that attempted to download and install malicious code on the user's computer. As users become more reliant upon the Internet for daily activities such as news, shopping, and banking, attackers are more likely to tailor their attacks specifically for those activities.

Taiwan experienced the third most potential virus infections in the first six months of 2007. While Taiwan has a smaller population than China, with 23 million people,[54] it is home to a significant number of broadband users, with 4.5 million broadband Internet connections.[55] Furthermore, because the primary language spoken there is Mandarin Chinese, Taiwan is affected by many of the same malicious code threats as China, including viruses like Whybo, which is tailored towards Chinese-speaking users.

Top ten malicious code samples

The top reported malicious code sample for the APJ region was the Gampass Trojan (table 11).[56] Eighty-four percent of worldwide potential infections of Gampass were reported in this region. This Trojan is notable because the attacker can use it to target users of online games such as Lineage, Ragnarok Online, Rohan, and Rexue Jianghue. These games are more popular in the APJ region than in the rest of the world.[57]

China and Taiwan were the top countries reporting potential infections of Gampass this period. In 2007, the online game market in China alone is expected to grow by 35 percent,[58] where there were 30 million Internet gamers by the end of 2006.[59] Online games often feature goods, such as prizes, that are exchanged by players, often for money. The total annual wealth created within virtual worlds has been placed at approximately 10 billion USD.[60] As such, it is not surprising that attackers appear to be turning their attention to these games.

[52] http://www.webhosting.info/domains/country_stats/?ob=NET&oo=DESC
[53] http://www.symantec.com/security_response/writeup.jsp?docid=2007-031616-1256-99
[54] https://www.cia.gov/library/publications/the-world-factbook/geos/tw.html#People
[55] http://www.point-topic.com
[56] http://www.symantec.com/security_response/writeup.jsp?docid=2006-111201-3853-99
[57] http://news.com.com/Consumers+Gaming+their+way+to+growth+-+Part+3+of+South+Koreas+Digital+Dynasty/2009-1040_3-5239555.html
[58] http://uk.reuters.com/article/internetNews/idUKSHA27160820070628
[59] http://abcnews.go.com/Technology/wireStory?id=3386396
[60] http://www.pcworld.com/article/id,128270-page,2-c,onlineentertainment/article.html

Regional Rank	Sample	Type	Top Reporting Country	Second Reporting Country	Propagation Vectors	Impact/Features
1	Gampass	Trojan	China	Taiwan	N/A	Steals online gaming account information
2	Looked.BK	Worm, Virus	China	Taiwan	CIFS	Disables security applications
3	Netsky.P	Worm	Japan	Australia	SMTP, P2P	Keystroke logger targets www.e-gold.com
4	Antinny	Worm	Japan	China	P2P	Copies itself to Winny shared folders
5	Anicmoo	Trojan	China	Taiwan	Remote Vulnerability	Downloads and installs other threats
6	Pinfi	Virus	Japan	China	File sharing	Infects portable executable files
7	Netsky.D	Worm	Japan	Australia	SMTP	Creates a mass mailing of itself
8	Vundo	Trojan	Australia	Japan	N/A	Displays advertisements, downloads and installs additional threats
9	Rahack.W	Worm	Japan	Malaysia	CIFS	Modifies HTML files
10	Netsky.Q	Worm	Japan	Taiwan	SMTP	Performs denial of service attacks

Table 11. Top ten malicious code samples
Source: Symantec Corporation

The second most frequently reported malicious code sample in the APJ region during this period was the Looked.BK worm.[61] The worm disables the processes of several security applications, which is a tactic that is commonly employed by malicious code writers. However, Looked.BK specifically attempts to bypass security warning messages that are composed in simplified and traditional Chinese. This indicates that it may have been written to specifically target users in those countries.

The third most frequently reported malicious code sample was the Netsky.P mass-mailing worm.[62] It was mainly reported to cause potential infections in Japan in the first half of 2007. Two other Netsky variants—Netsky.D[63] and Netsky.Q[64]—were also among the top ten malicious code samples in the APJ region and reported most frequently from Japan.

Netsky.P propagates both by sending email messages with an executable attachment and through P2P file-sharing networks. Since variants of Netsky are quite old, it is likely that users still experiencing potential infections of these worms are opening email attachments and files downloaded from P2P networks without first scanning them with antivirus applications using current signatures.

Top three new malicious code families

The most prevalent new malicious code family reported in the APJ region during this period was the Fubalca worm (table 12).[65] This worm propagates by infecting files on all drives except for those on the drive on which Windows is installed. If it locates any HTML files on the drives, it adds exploit code to the page that

[61] http://www.symantec.com/security_response/writeup.jsp?docid=2006-112813-0222-99
[62] http://www.symantec.com/security_response/writeup.jsp?docid=2004-032110-4938-99
[63] http://www.symantec.com/security_response/writeup.jsp?docid=2004-030110-0232-99
[64] http://www.symantec.com/security_response/writeup.jsp?docid=2004-032913-5722-99
[65] http://www.symantec.com/security_response/writeup.jsp?docid=2007-040106-1154-99

attempts to take advantage of a vulnerability in the way Microsoft Windows handles cursor and icon ANI format files.[66] If a user views one of these HTML files with a vulnerable version of Internet Explorer, the exploit will cause the Anicmoo Trojan to be downloaded and installed on the computer.[67] If Fubalca compromises a computer hosting a Web site, users that trust this site could then be compromised by Anicmoo.

Fubalca also downloads and installs either the Gampass or Perfwo Trojans onto the compromised computer.[68] These multistaged threats appear to have been tailored to target Chinese users in order to profit from the rapid growth of these online games in China. Gampass was the top malicious code threat in the APJ region this period and steals account information for various online games (as is discussed in the "Top ten malicious code samples" section of this report). Perfwo steals account information for an online game called Perfect World, which was created by a company in Beijing.

Regional Rank	Sample	Type	Propagation Vectors	Impact/Features	Top Reporting Country
1	Fubalca	Worm, Virus	File sharing, Web pages	Downloads and installs other threats	China
2	Whybo	Virus	File sharing	Disables security applications, downloads and installs other threats	China
3	Anivip	Virus	Web pages	Downloads and installs other threats	Japan

Table 12. Top three new malicious code families
Source: Symantec Corporation

In the first half of 2007, the Whybo virus was the second most common new malicious code family in the APJ region.[69] This virus propagates by infecting portable executable files on all local and shared drives on the compromised computer. Interestingly, it avoids infecting files in certain directories, mainly those associated with Windows and some commonly used applications like Internet Explorer, likely in an attempt to remain unnoticed for as long as possible. The longer a threat remains unnoticed and active on a computer, the greater an opportunity it will have to cause more damage.

Once the computer is infected, Whybo also closes windows with certain strings in their names. These strings are primarily related to security applications, and many of them are in Chinese, indicating that the virus was likely authored in China or is intended to target Chinese users.

Between January 1 and June 30, 2007, the Anivip virus was the third most common new malicious code family in the APJ region.[70] Anivip is similar to Fubalca in some respects. When it infects a computer, it adds code to ASP, PHP, and HTML files that redirect browsers to a Web site that attempts to exploit a vulnerability in the way Microsoft Windows handles cursor and icon ANI format files. If a user views one of these HTML files with a vulnerable version of Internet Explorer, the exploit will cause a downloader Trojan to be downloaded and installed on the computer. The Web site that hosts the exploit and the downloader Trojan is registered using a Chinese domain; however, potential infections of this virus during this period were primarily reported from Japan.

[66] http://www.securityfocus.com/bid/23194
[67] http://www.symantec.com/security_response/writeup.jsp?docid=2005-021610-3724-99
[68] http://www.symantec.com/security_response/writeup.jsp?docid=2006-103015-0937-99
[69] http://www.symantec.com/security_response/writeup.jsp?docid=2007-040316-2416-99
[70] http://www.symantec.com/security_response/writeup.jsp?docid=2007-042016-1706-99

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, and/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—this can also severely undermine customer confidence as well as violate local laws.[71] Sensitive corporate information could also be leaked from compromised computers including financial details, business plans, and proprietary technologies.

Threats to confidential information made up 57 percent of potential infections by the top 50 malicious code samples in the APJ region. This is less than the worldwide percentage of 65 percent. This is due to the relatively low proportion of threats that export system data, export email addresses, and allow remote access. This may indicate that there is a lack of market for this type of information in the APJ region. Instead, as is discussed below, the most common threats to confidential information found in the APJ region, such as the Gampass Trojan,[72] target users of online games. This likely indicates that online game accounts are more sought after than other forms of confidential information, which is probably due to the number of players of online games.

In the APJ region, threats that allow remote access, such as back doors, made up 60 percent of potential infections by confidential information threats, less than the 88 percent that was reported worldwide during this period (figure 3).[73] Remote access threats are popular with attackers because they are able to perform almost any action on the compromised computer. The main contributors to the higher worldwide percentage were the Vundo Trojan[74] and Spybot worm,[75] which ranked second and seventeenth worldwide, but only ranked eleventh and forty-second in the APJ region, respectively.

[71] Many countries have implemented their own laws in this regard, such as the UK Data Protection Act, which can be found at http://www.opsi.gov.uk/ACTS/acts1998/19980029.htm
[72] http://www.symantec.com/security_response/writeup.jsp?docid=2006-111201-3853-99
[73] It should be noted that many threats to confidential information have numerous capabilities. As a result, cumulative percentages included in this discussion may exceed 100 percent.
[74] http://www.symantec.com/security_response/writeup.jsp?docid=2004-112111-3912-99
[75] http://www.symantec.com/security_response/writeup.jsp?docid=2003-053013-5943-99

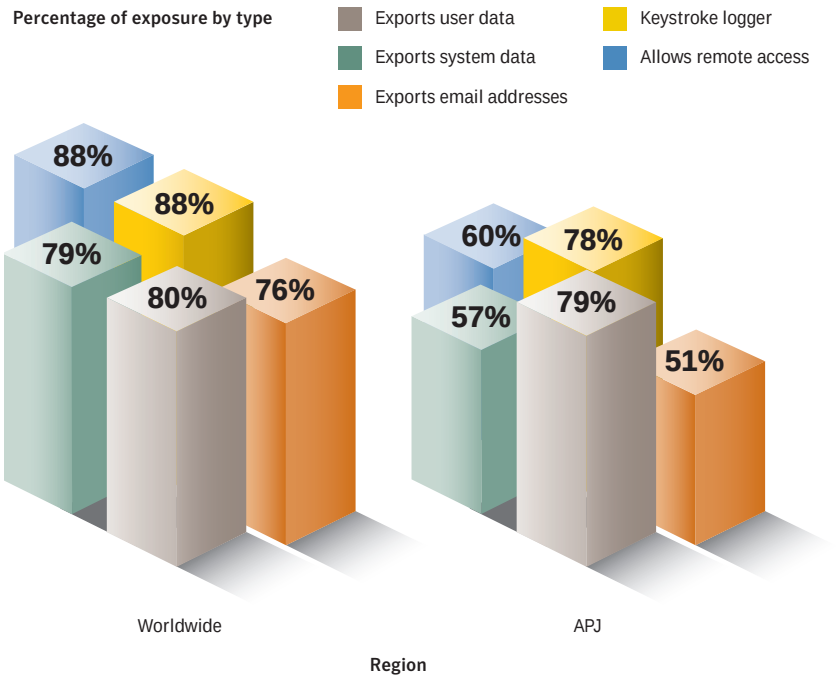

Figure 3. Threats to confidential information by type
Source: Symantec Corporation

The Vundo Trojan can be placed on Web sites, where it exploits a vulnerability in Internet Explorer.[76] Attackers can target specific groups of users by putting the exploit on Web sites that appeal to those groups. Since the number of potential Vundo infections reported in APJ is relatively low, it appears that attackers using this Trojan aren't targeting users in APJ as frequently as those in other regions.

Threats that could be used to export user data accounted for 79 percent of potential infections of confidential-information threats in the APJ region during this reporting period. Across the Internet as a whole, these threats made up 80 percent of infections by threats to confidential information during this period. Keystroke logging threats made up 78 percent of the volume of potential infection by confidential-information threats in the APJ region, compared to 88 percent worldwide.

[76] http://www.microsoft.com/technet/security/bulletin/ms04-040.mspx

Threats that export user data and log keystrokes are the two most common threats in APJ, by a large margin. This can largely be attributed to the several Trojans that target online games. The Gampass Trojan,[77] for example, ranked second in the APJ region, eighth worldwide, and 45th in the Europe, Middle East, and Africa (EMEA) region during the first six months of 2007. As was stated previously, this Trojan is notable because it can be used to target one of several online games that are more popular in the APJ region than the rest of the world.[78] As a result, 84 percent of worldwide potential infections of Gampass originated from that region.

The ability of attackers to configure this threat to target multiple games likely contributes to its popularity. When it is installed, the Trojan will log keystrokes when the user connects to the specified online gaming site and send the log to a Web site or email address. Gampass may also attempt to disable the processes of antivirus and other security products, leaving compromised users open to additional threats.

Fifty-seven percent of confidential-information threats reported in the APJ region during the first six months of 2007 could be used to export system data, compared to 79 percent of Internet-wide threats. These forms of data leakage can enable an attacker to steal a user's identity or launch further attacks. If the attacker has access to the user's personal and system data, he or she can use it to craft a targeted social engineering attack that is highly tailored to that particular user.

This report has already noted that the sale of APJ-based identities and other personal data appears to be much less common than the sale of identities and data belonging to North American and European users.[79] As a result, it is likely that APJ users are not targeted by authors of this type of malicious software. The Lineage infostealer, which targets the online game Lineage, was one malicious code sample that was used to export system information in APJ during this reporting period. The Lineage infostealer ranked fifteenth in APJ, thirty-third worldwide, and higher than fiftieth in EMEA during the first six months of 2007.

Threats that could be used to export email addresses accounted for 51 percent of potential infections by confidential information threats, compared to 76 percent worldwide. This form of information harvesting is often used to compile lists of valid email addresses, which are subsequently sold to spammers. In the first half of 2007, 60 percent of spam emails detected by Symantec were written in English,[80] which would indicate that English-speaking mailing lists would be more valuable than lists in other languages. This likely explains the relatively low number of these threats in the APJ region during this period.

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),[81] 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.

[77] http://www.symantec.com/security_response/writeup.jsp?docid=2006-111201-3853-99
[78] http://news.com.com/Consumers+Gaming+their+way+to+growth+-+Part+3+of+South+Koreas+Digital+Dynasty/2009-1040_3-5239555.html
[79] Please see the "Underground economy servers" of the main *Internet Security Threat Report* for more information.
[80] *Internet Security Threat Report* XII, "Spam and Phishing" section.
[81] Common Internet File Sharing (CIFS) is a protocol that defines a standard for remote file access. CIFS allows applications to open and share files across the Internet.

This metric will discuss some of the propagation mechanisms used by malicious code samples reported to Symantec during the first six months 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.

SMTP was used by 37 percent of the volume of propagating samples in the APJ region during this period, making it the most common propagation mechanism in the region (table 13). It accounted for 46 percent of the volume of the propagating samples worldwide. SMTP emails are usually written in English and, as a result, propagate less successfully in non-English speaking countries.

Regional Rank	Propagation Mechanism	Regional Percentage of Threats	Worldwide Percentage of Threats
1	File Transfer/Email Attachment	37%	46%
2	File Transfer/CIFS	34%	24%
3	File Sharing/Executables	33%	22%
4	File Sharing/Peer to Peer	18%	22%
5	Remotely Exploitable Vulnerability	17%	18%
6	File Sharing/Peer to Peer/Winny	17%	5%
7	File Sharing/Peer to Peer /Kazaa	16%	18%
8	File Sharing/Peer to Peer /eDonkey	15%	15%
9	File Sharing/Peer to Peer/Morpheus	15%	15%
10	Web	1%	1%

Table 13. Propagation mechanisms
Source: Symantec Corporation

That said, not all malicious code uses English to propagate. Some mass-mailing worms use different languages, such as Sober.AA,[82] which uses English and German. Rontokbro[83] was a notable mass mailer that targeted APJ-based users, using the Indonesian language in its emails.

In the first half of 2007 in the APJ region, malicious code that propagates by CIFS made up 34 percent of malicious code that propagates, compared to 24 percent worldwide. The difference between regional and worldwide data can largely be attributed to the higher number of reports in the APJ region for the Looked.BK[84] and Looked.P worms,[85] both of which use CIFS to propagate. These worms search for network shares with weak password protection, to which they can copy themselves. They also contain a viral component to infect executable files on a compromised computer. Looked.BK ranked third in APJ during this period, compared to ninth worldwide, while Looked.P ranked twentieth in APJ and thirty-seventh worldwide.

[82] http://www.symantec.com/enterprise/security_response/writeup.jsp?docid=2007-043010-5416-99
[83] http://www.symantec.com/security_response/writeup.jsp?docid=2005-092311-2608-99
[84] http://www.symantec.com/security_response/writeup.jsp?docid=2006-112813-0222-99
[85] http://www.symantec.com/security_response/writeup.jsp?docid=2006-071212-0124-99

Malicious code that propagates using CIFS is similar to malicious code that propagates by using file sharing/executables, which ranked third place, making up 33 percent of malicious code that propagates. Both mechanisms make use of a viral component to infect potentially innocent files.

In the first six months of 2007, 18 percent of propagating malicious code reported in the APJ region used P2P to propagate, compared to 22 percent globally. One of the most prevalent families of worms in the APJ region was the Antinny family, with five variants in the top 50 malicious code samples from the APJ region, all of which propagate through the Winny file-sharing program. By comparison, only two variants were in the top 50 samples worldwide.

Malicious code—prevention 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 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.[86]

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 address space layout randomization (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.

[86] 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.

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. This section of the Symantec *APJ Internet Security Threat Report* will discuss phishing activity that Symantec detected in the APJ region between January 1 and June 30, 2007.

The data provided in this section is based on statistics derived from the Symantec Probe Network, which consists of over two million decoy email accounts that attract email messages from 20 different countries around the world. The main purpose of the network is to attract spam, phishing, viruses, and other email-borne threats. It encompasses more than 600 participating enterprises around the world, 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 *APJ Internet Security Threat Report* will discuss:

- Top countries hosting phishing Web sites
- Top cities hosting phishing Web sites
- Phishing—prevention and mitigation

Top countries hosting phishing Web sites

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

This section of the Symantec *APJ Internet Security Threat Report* will discuss the top countries and cities in which phishing Web sites are hosted. This data is a snapshot in time and, therefore, does not have insight into changes in the locations of certain phishing sites throughout the period. It should also be noted that because a phishing Web site is hosted in a certain country, this does not mean that the attacker is located in the same country. However, it is likely that a phishing Web site will be located in the same country as the intended victims of the attack.

During the first six months of 2007, Japan was home to the highest percentage of phishing Web sites in the APJ region (table 14). It had the eighth highest number of phishing Web sites in the world during this period. Japan is one of the richest and most technologically advanced countries in the region. Furthermore, according to a recent report by Nielsen,[87] Japan is among the most modern countries in the world in terms of their banking practices, which means that online banking is likely a well established practice. The popularity of online banking as well as the high average standard of living makes Japan a preferred target for phishers.

[87] http://au.acnielsen.com/site/documents/GlobalBankingServicesReportApril07.pdf

Japanese computers are excellent platforms for hosting Japanese phishing sites, particularly because of language concerns. Almost every computer in Japan already has the Japanese language pack installed. To host a Japanese phishing Web site on a computer without this character set, the attacker would have to download and install it on the compromised computer, which would reduce the likelihood of a successful attack.

In the current *Internet Security Threat Report*, Symantec noted that some phishing Web sites were pointed to by multiple URLs. This is an indication that phishing toolkits were used in those attacks. A phishing toolkit is a set of scripts that allows an attacker to automatically set up phishing Web sites that spoof the legitimate Web sites of different brands, including the images and logos associated with those brands. The scripts also help to generate corresponding phishing email messages.

However, in Japan very few phishing Web sites were pointed to by multiple URLs. This indicates that, despite the number of phishing Web sites in Japan during this period, few of them were the result of known phishing kits. This indicates that most phishing activity in Japan during this period was conducted by numerous smaller phishing operations, which were likely using phishing Web sites hosted on the networks of smaller Web-hosting companies.

Regional Rank	Previous Rank	Country	Regional Percentage	Previous Regional Percentage	Worldwide Percentage	Previous Worldwide Percentage
1	1	Japan	18%	21%	2%	3%
2	3	China	16%	17%	1%	2%
3	2	Taiwan	16%	20%	1%	3%
4	4	South Korea	13%	15%	1%	2%
5	6	Thailand	8%	6%	1%	1%
6	5	Australia	8%	8%	1%	1%
7	11	Indonesia	7%	2%	1%	<1%
8	7	Malaysia	2%	3%	<1%	<1%
9	8	Singapore	2%	2%	<1%	<1%
10	9	Bangladesh	2%	2%	<1%	<1%

Table 14. Top countries hosting phishing Web sites
Source: Symantec Corporation

China had the second highest number of phishing Web sites in the APJ region in this reporting period. Bot-infected computers are frequently used to host phishing sites by downloading other threats. China was host to the most bots in the world, but it is likely that the majority of these bots were used for other purposes, such as DoS attacks (for which China was by far the highest country in APJ as described in the "Attack Trends" section of this report) and spam zombies, of which China had 40 percent in APJ during this period. Despite these considerations, China still ranks high in terms of phishing Web sites on this list, likely because it is a large country with a large Internet population.[88]

[88] http://www.networkworld.com/news/2007/012307-china-internet-market-grows-to.html

Between January 1 and June 30, 2007, Taiwan had the third highest number of phishing Web sites in the APJ region with 16 percent of the total. There are relatively few Web-hosting companies in Taiwan,[89] so phishers likely host many of their sites on compromised computers. Taiwan ranked second in the APJ region for bots during this period, so there are many computers available to host phishing sites in this manner. Furthermore, many of the Taiwanese phishing Web sites are hosted on users' personal Web pages.

Top cities hosting phishing Web sites

Taipei was the city with the most phishing Web sites in the APJ region in the first six months of 2007 (table 15). This is unchanged from the previous six-month reporting period. Taipei's prominence in this metric is likely due to the fact that the city is the main commercial, political, and economic hub of Taiwan, the country that had 16 percent of the phishing Web sites in the APJ region. It is also home to the major ISPs and Internet companies of the country.

Regional Rank	Previous Regional Rank	City	Country
1	1	Taipei	Taiwan
2	4	Hong Kong	China
3	5	Bangkok	Thailand
4	3	Tokyo	Japan
5	2	Seoul	South Korea
6	14	Sakura	Japan
7	12	Jakarta	Indonesia
8	8	Singapore	Singapore
9	9	Beijing	China
10	7	Kuala Lumpur	Malaysia

Table 15. Top cities by phishing Web sites
Source: Symantec Corporation

Hong Kong hosted the second most phishing Web sites in the APJ region during this reporting period. It ranked fourth in the last six months of 2006. The average income and purchasing power is higher in Hong Kong than in most other parts of China,[90] making the residents of Hong Kong the target of attacks from phishers. Another possible reason for Hong Kong's prominence is that the special administrative region's unique .hk domains are easier to register than elsewhere in China and provide convincing platforms for conducting phishing attacks against residents of the city.

Bangkok was host to the third most phishing Web sites in the APJ region. It was the fifth-ranked country for this category in the second half of 2006. The Thai government has substantially increased its control over the Internet since the last reporting period, including blocking access to YouTube entirely,[91] although that ban has recently been partially lifted.[92] This may be leading phishers who are targeting Thai citizens to bypass control mechanisms by hosting more phishing Web sites within the country. Since Bangkok is the capital city, the primary populous center, and the economic and political hub of the country, most of the Thai phishing sites are likely located in there.

[89] http://www.webhosting.info/webhosts/tophosts/global/
[90] http://www.economist.com/countries/HongKong/profile.cfm?folder=Profile-FactSheet
[91] http://news.bbc.co.uk/1/hi/world/asia-pacific/6528303.stm
[92] http://www.nytimes.com/2007/08/31/world/asia/31cnd-Thai.html?ex=1346212800&en=281abf3154d40f6b&ei=5088&partner=rssnyt&emc=rss

Phishing—prevention 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.[93]

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.[94]

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.[95] 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.[96] Additionally, network administrators can review Web proxy logs to determine if any users have visited known phishing sites.

[93] 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.
[94] A good resource for information on the latest phishing threats can be found at http://www.antiphishing.org
[95] Cousin domains is a term that 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.
[96] 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 January 1 and June 30, 2007.

The data used in this analysis is based on data returned from the Symantec Probe Network as well as data gathered from a statistical sampling of the Symantec Brightmail AntiSpam customer base. Specifically, statistics are gathered from enterprise customers' Symantec Brightmail AntiSpam servers that receive more than 1,000 email messages per day. This removes the smaller data samples (that is, smaller customers and test servers), thereby allowing for a more accurate representation of data.

The Symantec Probe Network consists of millions of decoy email addresses that are configured to attract a large stream of spam attacks. An attack can consist of one or more messages. The goal of the Probe Network is to simulate a wide variety of Internet email users, thereby attracting a stream of traffic that is representative of spam activity across the Internet as a whole. For this reason, it is continuously optimized in order to attract new varieties of spam attacks. This is accomplished through internal production changes that are made to the network, which thus affect the number of new spam attacks it receives as a whole.

This section of the Symantec *APJ Internet Security Threat Report* will explore the following:

- Top ten countries of spam origin
- Top spam zombie countries and cities
- Spam as a percentage of all email by country

Top ten countries of spam origin

This section will discuss the top ten originating countries of spam sent from the APJ region. 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 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-five percent of all spam detected from the APJ region during this period originated in China, the most of any country in the region (table 16). Although China maintained the top spot in this ranking, it has fallen in terms of percentage from last period, when it had 37 percent of the regional total.

The percentage of email from China that is spam has remained constant at 68 percent; however, the percentage of the region's spam detected from China has decreased. This indicates that the total amount of mail detected from China has decreased. The rapid growth in email usage that took place in China over the previous few periods appears to have slowed down. This may be because email is being replaced by other forms of online communication, such as instant messaging.

Regional Rank	Previous Rank	Country	Regional Percentage	Previous Regional Percentage	Worldwide Percentage	Previous Worldwide Percentage	Percent of Email That is Spam	Previous Percent of Email That is Spam
1	1	China	25%	37%	4%	6%	68%	68%
2	3	Japan	24%	20%	4%	3%	64%	61%
3	2	South Korea	19%	21%	3%	3%	85%	84%
4	4	Taiwan	19%	8%	3%	1%	83%	84%
5	6	Malaysia	3%	3%	<1%	<1%	77%	84%
6	7	Australia	2%	2%	<1%	<1%	37%	41%
7	5	New Zealand	2%	4%	<1%	1%	33%	50%
8	8	Vietnam	2%	2%	<1%	<1%	84%	86%
9	9	Philippines	1%	1%	<1%	<1%	88%	88%
10	11	Thailand	1%	1%	<1%	<1%	82%	76%

Table 16. Top ten countries of spam origin, APJ region
Source: Symantec Corporation

The second highest volume of spam detected from the APJ region during this period originated in Japan, which accounted for 24 percent of the total. This is an increase from 20 percent in the previous period, and is notable because it was not accompanied by an increase in spam zombies in the region, the regional percentage of which dropped by three percentage points during this period (see the "Spam zombies" discussion below for a more in-depth discussion). This indicates that most of the spam in Japan is sent through legitimate mailing mechanisms rather than compromised computers.

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 illicitly. Japan has high levels of free wireless Internet connectivity and usage.[97] This likely allows spammers to connect to these legitimate mail servers and send large amounts of spam through them from almost any location.

South Korea had the third highest volume of spam in the APJ region in the first six months of 2007, accounting for 19 percent of the region's total. This percentage is a slight decrease over the 21 percent in the previous reporting period. The high volume of spam being sent from South Korea is made possible by the high rate of connectivity there and the availability of legitimate mail servers. South Korea also had the second highest number of spam zombies in the APJ region during the first half of 2007. It is very likely that a large amount of the spam from South Korea is sent through both compromised computers and legitimate mail servers.

[97] http://www.ipsos-na.com/news/pressrelease.cfm?id=3049

Taiwan had the largest increase in spam over the past six months, jumping from eight percent of spam in the APJ region in the second half of 2006 to 19 percent this period. The number of spam zombies in Taiwan has decreased this period, indicating that spam from Taiwan in this period was likely sent through legitimate servers at a higher rate than in the previous period. Sometimes the total volume of spam from one region can be affected by a small number of high-volume spam campaigns during a given period; it is possible that such a campaign is the cause of the increase in spam coming from Taiwan in this period.

Top spam zombie countries and cities

A spam zombie is a computer infected with a bot or some other malicious code that allows email messages to be relayed. Between January 1 and June 30, 2007, China was home to more spam zombies than any other APJ country, with 40 percent of the regional total (table 17). Just as in the second half of 2006, China was home to the largest number of bot-infected computers in the region during this period. This connection is not coincidental; many bots are designed to be used mainly to send spam and are detected as spam zombies.

Regional Rank	Previous Rank	Country	Regional Percentage	Previous Regional Percentage	Worldwide Percentage	Previous Worldwide Percentage
1	1	China	40%	43%	9%	9%
2	2	South Korea	17%	15%	4%	3%
3	3	Taiwan	10%	13%	2%	3%
4	5	Thailand	9%	5%	2%	1%
5	4	Japan	6%	9%	1%	2%
6	6	Vietnam	5%	3%	1%	1%
7	8	Philippines	4%	3%	1%	1%
8	7	Malaysia	4%	3%	1%	1%
9	9	Singapore	2%	2%	<1%	<1%
10	10	Australia	2%	2%	<1%	<1%

Table 17. Top spam zombie countries
Source: Symantec Corporation

South Korea accounted for the second most spam zombies in the APJ region with 17 percent. South Korea likely ranks high because it has the highest broadband penetration per household in the world.[98] Broadband-connected computers make ideal spam zombies because, in many cases, they are always connected to the Internet and have enough bandwidth to send many spam messages at once. Further, in countries in which rapid expansion of connectivity is taking place, many users who connected to the Internet are not well informed about computer security practices. These users' computers are more likely to be infected by a bot or other malicious code and thus used as spam zombies. Further, once infected, these machines are likely to remain undetected for extended periods of time.

[98] http://point-topic.com/contentDownload/dslanalysis/world%20broadband%20statistics%20q1%202007.pdf

Taiwan had the third highest number of spam zombies in the APJ region during the first half of 2007, with 10 percent of the region's total. This is likely due to the fact that Taiwan is home to the second largest number of bot-infected computers in the region, many of which could be used to send spam. This number has decreased somewhat from 13 percent, reflecting a trend in Taiwan away from Trojans that send spam and towards Trojans focused on stealing information from online games.

Bangkok had the highest number of spam zombies of any APJ city during this period (table 18). This is a jump from third place in the second half of 2006. The increase is mainly due to the fact that Thailand had the fourth highest number of spam zombies in the region during this period, and that Bangkok is the largest city in the country. Spam zombies in Thailand increased from five percent to nine percent during this period, and most of this growth was focused in Bangkok.

Regional Rank	Previous Regional Rank	City	Country
1	3	Bangkok	Thailand
2	1	Seoul	South Korea
3	12	Manila	Philippines
4	7	Hanoi	Vietnam
5	15	Shanghai	China
6	11	Tokyo	Japan
7	2	Taipei	Taiwan
8	6	Kuala Lumpur	Malaysia
9	18	Hangzhou	China
10	10	Singapore	Singapore

Table 18. Top spam zombie cities
Source: Symantec Corporation

Seoul had the second highest number of spam zombies in the APJ region in the first half of 2007. It had the most spam zombies in the previous reporting period. There is no apparent reason for a drop in spam zombies in Seoul during this time, so it may be that the drop in rank, from first to second, is due more to the rise in spam zombies in Bangkok than a decrease in Seoul.

Manila had the third highest number of spam zombies in the APJ region during this period. The Philippines experienced 23 percent growth in broadband use in the first quarter of 2007.[99] Much of this growth is focused in urban Manila. Countries with rapid increases in broadband usership tend to also see increases in Internet threats such as malicious code infection and spam zombies.

Additionally, the high percentage of spam zombies in Manila may be related to software piracy. The Philippines has a 71 percent piracy rate, which is higher than the 55 percent piracy rate across the APJ region and 35 percent worldwide.[100] Pirated software is often unable to receive updates, which includes security patches.[101] As such, computers in countries with a high rate of piracy are likely to be more susceptible to attacks. These attacks can install malicious programs, which can include spam zombie software. As a result, users in the Philippines, particularly those using pirated software, are more susceptible to spam zombies.

[99] http://point-topic.com/contentDownload/dslanalysis/world%20broadband%20statistics%20q1%202007.pdf
[100] http://w3.bsa.org/globalstudy//upload/2007-Losses-Global.pdf
[101] http://w3.bsa.org/globalstudy//upload/2007-Losses-Global.pdf

Spam as a percentage of all email by country

Symantec calculates the percentage of email that is spam by dividing the total number of emails that are identified as spam by Symantec Brightmail AntiSpam filters by the total of the inbound email messages received by the sample customer base.[102] Between January 1 and June 30, 2007, spam made up 61 percent of all monitored email traffic across the Internet as a whole. In the APJ region alone, spam made up 70 percent of all monitored email traffic during this reporting period.

The higher percentage of spam originating from this region is likely caused by two factors. Four APJ countries—China, South Korea, Thailand, and Japan—are all amongst the top 20 countries worldwide hosting spam zombies. Further, bots can be utilized to relay spam among other activities; the APJ region is the second highest in the world for bot activity and China was the highest country for bot infections.

Of the top 15 email-producing countries in the APJ region, the top five countries according to the volume of spam by volume are listed in table 19. It is important to note that these percentages are not related to the total volume of spam produced by these countries, but are instead a representation of the percentage of all email originating from each country that Symantec has identified as spam.

Country	Percent	Previous Percent
Uzbekistan	88%	88%
Philippines	87%	88%
Vietnam	84%	86%
South Korea	83%	84%
Mongolia	82%	82%

Table 19. Top five APJ countries by percentage of spam
Source: Symantec Corporation

Of the top 20 email-producing countries in the APJ region, Uzbekistan produced the highest percentage of spam, with 88 percent. The Philippines had the second highest percentage of spam, with 87 percent. Vietnam had a spam percentage of 84 percent, making it the third highest spam-producing country in the APJ region.

[102] Symantec Brightmail AntiSpam only gathers data at the SMTP layer and not at 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.

Appendix A—Symantec Best Practices

Enterprise Best Practices

1. 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.
2. Turn off and remove services that are not needed.
3. 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.
4. 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.
5. Consider implementing network compliance solutions that will help keep infected mobile users out of the network (and disinfect them before rejoining the network).
6. Enforce an effective password policy.
7. 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.
8. 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.
9. 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.
10. 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.
11. Educate management on security budgeting needs.
12. Test security to ensure that adequate controls are in place.
13. 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

1. 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.
2. Consumers should ensure that security patches are up-to-date and that they are applied to all vulnerable applications in a timely manner.
3. 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.
4. Consumers should never view, open, or execute any email attachment unless the attachment is expected and the purpose of the attachment is known.
5. 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.
6. Consumers should routinely check to see if their operating system is vulnerable to threats by using Symantec Security Check at www.symantec.com/securitycheck.
7. 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.
8. 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.
9. 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.
10. 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.
11. Consumers should beware 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.

Attack definitions

In order to avoid ambiguity with the findings presented in this discussion, Symantec's methodology for identifying various forms of attack activity is outlined clearly below. This methodology is applied consistently throughout our monitoring and analysis. The first step in analyzing attack activity is to define precisely what an attack is. Attacks are individual instances of malicious network activity. Attacks consist of one IDS or firewall alert that is indicative of a single attack action.

Explanation of research inquiries

This section will provide more detail on specific methodologies used to gather and analyze the data and statistics in this report. While most methodologies are adequately explained in the analysis section of the report, the following investigations warranted additional detail.

Denial of service attacks

Although there are numerous methods for carrying out denial of service (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 bots based on coordinated scanning and attack behavior observed in network traffic. For an attacking computer to be considered to be participating in this 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 network computer, and may identify other malicious code or individual attackers behaving in a similarly coordinated way as a bot network. This behavioral matching will, however, identify many of the most coordinated and aggressive bot-infected computers and will give insight into the population trends of bot network 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.

This metric explores the number of active bot-infected computers that the Symantec™ Global Intelligence Network has detected and identified during the first six months of 2007. Identification is carried out on an individual basis by analyzing attack and scanning patterns. Computers generating attack patterns that show a high degree of coordination are considered to be bot-infected computers.

As a consequence of this, Symantec does not identify all bot-infected computers, but only those that are actively working in a well coordinated and aggressive fashion. Given Symantec's extensive and globally distributed sensor base, it is reasonable to assume that the bot activities discussed here are representative of worldwide bot trends, and can thus provide an understanding of current bot activity across the Internet as a whole.

Bot-infected computers by countries and cities

This metric is based on the same data as the "Bot-infected computers" discussion of the "Attacks Trends" section of the report. 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.

Lifespan of bot-infected computers

Using previously identified bot-infected computers, Symantec determined the life span of these infections by measuring the time between their first and last detected activity. However, to ensure that the lifespan reflects a continuous bot infection, if the identified computer was inactive for 30 days or longer it was considered to be disinfected. As such, any further bot-like activity would be considered a new infection.

Top originating countries

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.

Appendix C—Malicious Code Trends Methodology

The trends in the "Malicious Code Trends" section 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 the "Malicious Code Trends" section are based on empirical data and expert analysis of this data. The data and analysis draw primarily from 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.

Phishing attempt definition

The Symantec Probe Network is a system of over two million decoy accounts that attract email messages from 20 different countries 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 covers countries in the Americas, Europe, Asia, Africa, and Australia/Oceania.

The Symantec Probe Network data is used to track the growth in new phishing activity. A phishing attempt is a group of email messages with similar properties, such as headers and content, that are sent to unique users. The messages attempt to gain confidential and personal information from online users.

Symantec Brightmail AntiSpam software reports statistics to Symantec Security Response that indicate 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 is used to identify general trends in phishing email messages.

Top countries and cities 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. 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.

Appendix E—Spam Trends Methodology

The Symantec Probe Network is a system of over two million decoy accounts that attract email messages from 20 different countries 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 at 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 having more than 1,000 total messages per day. This normalization yields a more accurate summary of Internet spam trends by ruling out problematic and laboratory test servers that produce smaller sample sets.

Explanation of research inquiries

This section will provide more detail on specific methodologies used to produce the data and statistics in this report. While most methodologies are adequately explained in the analysis section of the report, the following investigations warranted additional detail.

Top countries and cities 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.

Top countries and cities by spam zombies

The data in this section is determined by examining the logical connecting IP addresses in spam messages received by the Symantec Probe Network. IP addresses that meet a certain volume requirement are processed through a set of heuristics to determine if they are behaving like zombie servers. If an IP address meets some or all of the heuristic requirements, it will be listed as a zombie IP address. Symantec then cross-references the addresses with several third-party subscription-based databases that link the geographic locations of systems to IP addresses. 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 spam zombies.

Spam as a percentage of email scanned

The data for this section is determined by dividing the number of email messages that trigger antispam filters in the field by the total number of email messages scanned. These filters are distributed across the Symantec Brightmail AntiSpam customer base. The data for this section is based on monthly totals.

About Symantec

Symantec is a global leader in infrastructure software, enabling businesses and consumers to have confidence in a connected world. The company helps customers protect their infrastructure, information, and interactions by delivering software and services that address risks to security, availability, compliance, and performance. Headquartered in Cupertino, Calif., Symantec has operations in 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

09/07 12755153