



**Symantec APJ Internet
Security Threat Report**
Trends for July–December 06

Volume XI, Published March 2007

Dean Turner

Executive Editor
Symantec Security Response

Stephen Entwisle

Senior Editor
Symantec Security Response

Marci Denesiuk

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

Peter Coogan

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

Contributors**David Cole**

Director Product Management
Symantec Security Response

Peter Szor

Security Architect
Symantec Security Response

David Cowings

Sr. Business Intelligence Manager
Symantec Business Intelligence

Shravan Shashikant

Pr. Business Intelligence Manager
Symantec Business Intelligence

Igor Moochnick

Sr. Software Engineer
Symantec Instant Messaging Security

Symantec APJ Internet Security Threat Report

Contents

| | |
|---|----|
| <i>APJ Internet Security Threat Report Overview</i> | 4 |
| Executive Summary | 5 |
| Attack Trends | 7 |
| Malicious Code Trends | 19 |
| Phishing | 28 |
| Spam | 32 |
| Appendix A—Symantec Best Practices | 37 |
| Appendix B—Attack Trends Methodology | 39 |
| Appendix C—Malicious Code Trends Methodology | 42 |
| Appendix E—Phishing and Spam Methodology | 43 |

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. It includes analysis of network-based attacks, a review of known vulnerabilities, and highlights of malicious code. It will also discuss numerous issues related to online fraud, including phishing and spam. This summary of the *APJ Internet Security Threat Report* will alert readers to current trends and impending threats. In addition, it will offer recommendations for protection against and mitigation of these concerns. This volume covers the six-month period from July 1 to December 31, 2006.

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. Over 40,000 sensors deployed in more than 180 countries by Symantec DeepSight™ Threat Management System and Symantec™ Managed Security Services gather this data. As well, Symantec gathers malicious code data along with spyware and adware 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 20,000 vulnerabilities (spanning more than a decade) affecting more than 45,000 technologies from over 7,000 vendors. Symantec also tracks and assesses some criminal activities using online fraud monitoring tools.

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 Asia-Pacific/Japan region with the information they need to help effectively secure their systems now and in the future.

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

Executive Summary

The following section will offer a brief summary of the security trends that Symantec observed during the second half of 2006 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*.

Attack Trends Highlights

- The United States was the country of origin of the most attacks against APJ-based computers, accounting for 39 percent of attacks detected by sensors in the region.
- The total number of DoS attacks against targets worldwide during the second half of 2006 was 46,929, a drop of approximately 12 percent from 53,114 in the first half of the year.
- China was the APJ country most frequently targeted by DoS attacks, accounting for 63 percent of attacks in the region during this period.
- Symantec observed an average of 19,095 active distinct bot-infected computers per day in the APJ region.
- Symantec also identified 2,268,219 distinct bot-infected computers that were considered active in APJ at any one point in time (or more) during the second half of 2006.
- China had the highest number of bot-infected computers in the APJ region, accounting for 71 percent of the total.
- Beijing had 16 percent of all bot-infected computers in the APJ region.
- The home user sector was by far the most highly targeted sector in the APJ region, accounting for 98 percent of all targeted attacks.
- China accounted for 39 percent of malicious activity in the APJ region, more than any other country.
- Taiwan had the most malicious activity per Internet user in the APJ region.

Malicious Code Trends Highlights

- Trojans were the most common type of malicious code in the APJ region, accounting for 48 percent of the volume of malicious code reports received from the region.
- The top reported malicious code sample for the APJ region was the file-infecting worm Looked.P.
- The most prevalent new malicious code family reported in the APJ region during this period was the Stration worm.
- Threats to confidential information made up 60 percent of the volume of the top 50 malicious code reports from the APJ region.
- CIFS was the most common propagation vector used by malicious code in the APJ region; it was used by 60 percent of malicious code that propagates.

Phishing and Spam Highlights

- Japan was home to the highest percentage of phishing Web sites in the APJ region during this period.
- Nineteen percent of the phishing sites in the APJ region during this period were located in Taipei, more than any other city in the region.
- Thirty-seven percent of all spam detected from the APJ region during this period originated in China, the most of any country in APJ.
- China had more spam zombies than any other country in the APJ region, with 43 percent of the region's total.
- Seoul was the city with the highest number of spam zombies in the APJ region, with 14 percent of the region's total.
- In the APJ region, spam made up 69 percent of all monitored email traffic.
- Of the top 20 email-producing countries in the APJ region, the Philippines 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 July 1 and December 31, 2006. 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 monitors attack activity across the entire Internet. Over 40,000 sensors deployed in more than 180 countries by Symantec DeepSight™ Threat Management System and Symantec™ Managed Security Services gather this data.

Furthermore, 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
- Top targeted sectors
- Malicious activity by country
- Malicious activity by country per Internet user

Top countries of attack origin

Over the last six months of 2006, the United States was the country of origin of the most attacks against APJ-based computers, accounting for 39 percent of attacks detected by sensors in the region (table 1). This is somewhat higher than the 33 percent of worldwide attacks that originated in the United States. This would indicate that attack activity originating in the United States was targeting computers in the APJ region.

| Regional Rank | Country | Percentage of Regional Attacks | Previous Percentage of Regional Attacks | Percentage of Worldwide Attacks |
|---------------|----------------|--------------------------------|---|---------------------------------|
| 1 | United States | 39% | 39% | 33% |
| 2 | China | 19% | 21% | 11% |
| 3 | Japan | 5% | 2% | 3% |
| 4 | Australia | 5% | 6% | 2% |
| 5 | South Korea | 5% | 8% | 2% |
| 6 | Taiwan | 3% | 3% | 2% |
| 7 | United Kingdom | 3% | 2% | 5% |
| 8 | Argentina | 3% | 1% | 1% |
| 9 | France | 2% | <1% | 6% |
| 10 | Canada | 2% | 2% | 5% |

Table 1. Top countries of origin of attacks targeting the APJ region

Source: Symantec Corporation

Symantec APJ Internet Security Threat Report

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 19 percent of the total. This is higher than the 11 percent of Internet-wide attacks that originated in China during this period. It is thus reasonable to conclude that attacks originating in China were targeting APJ-based computers in particular.

It is possible that while many of these attacks originated from computers located in China, they are not necessarily launched by attackers located in China. During this period, China hosted 26 percent of worldwide bot-infected computers, and only five percent of command-and-control servers.

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 IRC. Command-and-control servers are computers that bot network owners use to relay commands to bot-infected computers on their networks. Since China has relatively few command-and-control servers compared to bots, it is likely that many of the bots located in China are being controlled by attackers in other countries. The number of attacks originating in China that targeted APJ-based computers may be lower than expected because attackers outside China could be using those bots to make attacks against targets in their own country, not against China itself.

Japan was the source country of the third highest number of attacks detected by sensors deployed in the APJ region, accounting for five percent of the total. This is higher than the three percent of worldwide attacks that originated in Japan during this period. Because Japan isn't a significant source of worldwide bots, it is likely that many of these attacks were launched by attackers in Japan, not elsewhere. It is thus reasonable to conclude that attacks originating in Japan were targeting APJ countries, likely Japan itself.

In previous versions of the *Internet Security Threat Report*,² Symantec has noted that attackers typically target their own region. This is 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 shared language and living in the same or a proximate time zone. Five of the top ten source countries of attacks against APJ targets are located within the APJ region, which supports Symantec's speculation that attackers typically attack local targets.

Top countries targeted by denial of service attacks

In this volume of the *APJ Internet Security Threat Report*, Symantec is tracking 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.³

² Symantec *Internet Security Threat Report*, Volume IX (March 2006): <http://enterprisesecurity.symantec.com/content.cfm?articleid=1539> : p. 13

³ Symantec *Internet Security Threat Report*, Volume VIII (September 2005): http://eval.veritas.com/mktginfo/enterprise/white_papers/ent-whitepaper_symantec_internet_security_threat_report_viii.pdf : p. 11 and 30

The total number of DoS attacks against targets worldwide during the second half of 2006 was 46,929, a drop of approximately 12 percent from 53,114 in the first half of the year. The total number of bots worldwide has increased to about six million from about 4.7 million, which is a 29 percent increase over the first half of the year. The combination of increasing bots and decreasing DoS attacks indicates that attackers may be using bots for purposes other than performing DoS attacks. Similarly, DoS attacks against the APJ region have fallen to 9,447 from 9,968, a five percent decrease.

Over the last six months of 2006, China was the APJ country most frequently targeted by DoS attacks, accounting for 63 percent of attacks in the region during this period (table 2). This proportion has changed very little since the previous reporting period, during which 64 percent of DoS attacks in the APJ region targeted China.

| Regional Rank | Country | Percentage of Regional Attacks | Previous Percentage of Regional Attacks | Percentage of Worldwide Attacks |
|---------------|-------------|--------------------------------|---|---------------------------------|
| 1 | China | 63% | 64% | 12% |
| 2 | South Korea | 13% | 10% | 3% |
| 3 | Taiwan | 8% | 10% | 2% |
| 4 | Australia | 4% | 4% | 1% |
| 5 | Japan | 4% | 5% | 1% |
| 6 | Thailand | 2% | 3% | <1% |
| 7 | Singapore | 2% | 2% | <1% |
| 8 | Malaysia | 1% | 1% | <1% |
| 9 | New Zealand | 1% | 1% | <1% |
| 10 | Indonesia | 1% | 1% | <1% |

Table 2. Top countries targeted by DoS attacks, APJ region

Source: Symantec Corporation

One reason for China’s prevalence in this category may be the large number of Web sites hosted there. China has more Web sites than any other country in the APJ region.⁴ Depending on their motivation, some attackers are more likely to target Web sites than individual Internet users because denying service to a Web site is a high profile attack that is evident to many observers. An attack that disrupts the availability of a high-profile Web site will get much wider notice than an attack that takes a single user offline. Additionally, China is an economic, political, and military power in the region. DoS attackers may be targeting organizations in China because they disagree with policies that are developed and implemented by the Chinese government.

South Korea was targeted by the second highest number of DoS attacks in the APJ region in the second half of 2006. It was targeted by 13 percent of attacks in APJ during this period, up from 10 percent in the first half of the year.

⁴ Based on number of unique domain names: http://www.webhosting.info/domains/country_stats

South Korea hosts the third highest number of Web sites in the APJ region,⁵ which means that there are a lot of potential DoS targets in the country. Furthermore, political tensions between North Korea and the rest of the world have been a recurrent issue over the past year. It is possible that attackers are targeting all Korean-based servers in an effort to express their disagreement with policies developed and implemented by the North Korean government. Additionally, the high number of attacks against South Korea may be related to the popularity of online games there.⁶ Users may target an online game's server with DoS attacks in order to disrupt the game for players, to disrupt revenue for game administrators, or simply to create mischief.

Taiwan was the APJ country targeted by the third highest number of DoS attacks, accounting for eight percent of attacks in the region during this period. Like South Korea, online games are popular in Taiwan. Attackers may be launching DoS attacks at online games in an effort to disrupt games. Online games appear to be the focus of increased malicious activity. For example, as is discussed in the "Top three new malicious code families" section of this report, two of the top three new malicious codes in APJ were password stealers for online games, and the top reporting country for both of those was Taiwan. DoS attackers may be targeting online game servers in order to disrupt games for other players or in an attempt at extortion.

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.

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

To reduce exposure to bot-related attacks, end users should employ defense-in-depth strategies, including the deployment of antivirus software and a firewall.⁷ 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.

⁵ Based on number of unique domain names: http://www.webhosting.info/domains/country_stats

⁶ http://news.com.com/Consumers+Gaming+their+way+to+growth++Part+3+of+South+Koreas+Digital+Dynasty/2009-1040_3-5239555.html

⁷ 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.

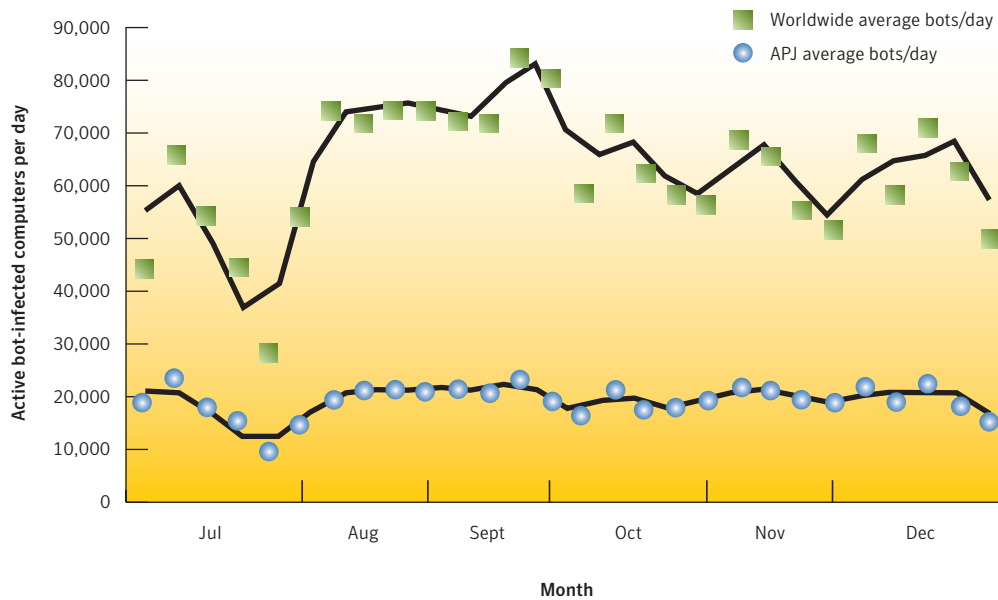


Figure 1. Active bot-infected computers per day, APJ region
 Source: Symantec Corporation

Between July 1, 2006, and December 31, 2006, Symantec observed an average of 19,095 active distinct bot-infected computers per day in the APJ region (figure 1). Worldwide, Symantec detected an average of 63,912 active bot-infected computers per day, so APJ accounted for about 30 percent of active bot-infected computers per day, on average.

Symantec also identified 2,268,219 distinct bot-infected computers that were considered active in APJ at any one point in time (or more) during the second half of 2006. This is 126 percent higher than the 1,002,915 active bot-infected computers that Symantec identified in the APJ region during the previous reporting period. The total number of active distinct bots detected worldwide during the second half of 2006 was 6,049,594, so APJ accounted for about 37 percent of worldwide bots during this period.

The total number of bots in the APJ region has increased significantly over the previous reporting period (both in APJ and worldwide), while the number of DoS attacks in the APJ region has dropped, from 9,968 to 9,447, a five percent decrease. This may be indicative of a fundamental change in the purpose of bots. Traditionally, bots have often been used in DoS attacks and, to a lesser degree, extortion schemes based on DoS attacks. As attackers become more financially motivated, they are likely to switch to methods that are more likely to consistently generate revenue. DoS attacks, and extortion schemes based on them, are resource-intensive and do not always create sufficient returns on the attacker’s investment of time and effort. As a result, attackers may now be using bots to relay spam, an activity that generates revenue for the attacker more consistently and reliably.

Throughout the second half of 2006, the number of active bot-infected computers in the APJ region was roughly constant, even though the worldwide bot activity varied throughout the period, reaching a peak in September. This peak occurred when a number of vulnerabilities that had previously been disclosed were actively exploited by bots. The flat trajectory of activity in the APJ region suggests that bots in the region have likely reached a saturation point. That is, the majority of computers in APJ that are vulnerable to compromise by bots have already been infected, so new vulnerabilities that result in increased bot activity across the Internet don't affect the total number of bots in the APJ region.

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 last six months of 2006, 23 percent of worldwide command-and-control servers were located in the APJ region, compared to the 34 percent of active bots that are located in the region.

This discrepancy is important, as it indicates that bots in APJ are being controlled by command-and-control servers that are situated outside the region. This means that some of the attack activity originating in the region is not necessarily being initiated by computers located in that region, as is discussed in the "Top countries targeted by denial of service" section of this report. As such, it is possible that the prevalence of attack activity originating in China and other APJ countries is partly due to the number of bot-infected computers in those countries being controlled by attackers in countries outside the APJ region.

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 (table 3). 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 July 1 and December 31, 2006, China had by far the highest number of bot-infected computers in the APJ region, accounting for 71 percent of the total. It is not surprising that China has the most bot-infected countries in the region, as it also has the highest number of broadband users.⁸ Broadband use there is currently expanding rapidly. China currently accounts for 11 percent of the world's users and is expected to surpass the United States in users in the next year.⁹

⁸ <http://www.point-topic.com/contentDownload/dslanalysis/world%20broadband%20statistics%20q1%202006.pdf> (access requires registration)
⁹ <http://www.internetworldstats.com>

| Regional Rank | Country | Percentage of Regional Bots | Percentage of Worldwide Bots | Previous Percentage of Worldwide Bots |
|---------------|-------------|-----------------------------|------------------------------|---------------------------------------|
| 1 | China | 71% | 26% | 20% |
| 2 | Taiwan | 11% | 4% | 6% |
| 3 | South Korea | 6% | 2% | <1% |
| 4 | Japan | 3% | 1% | <1% |
| 5 | Australia | 3% | 1% | <1% |
| 6 | Malaysia | 1% | 1% | <1% |
| 7 | Singapore | 1% | <1% | <1% |
| 8 | Philippines | 1% | <1% | <1% |
| 9 | Thailand | 1% | <1% | <1% |
| 10 | Vietnam | <1% | <1% | <1% |

Table 3. Bot-infected computers by country, APJ region

Source: Symantec Corporation

In Volume IX of the *Symantec Internet Security Threat Report*, Symantec speculated that the number of new users adopting high-speed Internet in a country is a significant factor in the rate of bot infections.¹⁰ Symantec believes that new broadband customers may not be aware of the additional security precautions that need to be taken when exposing a computer to an always-on high-speed Internet connection. Furthermore, the addition of many new customers, with the corresponding increase in infrastructure and support costs, may make security less of a priority or slow the response of ISPs to reports of network abuse and infection.

Taiwan accounted for 11 percent of bot-infected computers in the APJ region in the second half of 2006, the second highest total in the region. Taiwan's worldwide proportion of bot-infected computers was four percent, slightly lower than the six percent of the previous reporting period. This indicates that security awareness in Taiwan may be increasing and that Taiwanese users and ISPs are putting adequate security measures, such as antivirus and filtering, in place that block bots and other threats.

South Korea had the third highest number of bot-infected computers in the APJ region, with six percent of the total. Although South Korea had only six percent of bot-infected computers, it had 43 percent of command-and-control servers in the APJ region, more than any other country in the region. This indicates that attackers in South Korea may be controlling bot-infected computers in other countries—either inside or outside the APJ region—and using those bots to launch attacks.

¹⁰ Symantec *Internet Security Threat Report*, Volume IX (March 2006): http://eval.veritas.com/mktginfo/enterprise/white_papers/ent-whitepaper_symantec_internet_security_threat_report_ix.pdf : p. 13

Bot-infected computers by city

| Regional Rank | City | Country | Percentage of Regional Bots | Percentage of Worldwide Bots | Percentage of Bots in Country |
|---------------|--------------|----------|-----------------------------|------------------------------|-------------------------------|
| 1 | Beijing | China | 16% | 5% | 20% |
| 2 | Guangzhou | China | 8% | 2% | 9% |
| 3 | Hangzhou | China | 5% | 2% | 7% |
| 4 | Shanghai | China | 4% | 1% | 5% |
| 5 | Ningbo | China | 3% | 1% | 4% |
| 6 | Kuala Lumpur | Malaysia | 3% | 1% | 96% |
| 7 | Fuzhou | China | 3% | 1% | 3% |
| 8 | Bangkok | Thailand | 3% | 1% | 97% |
| 9 | Taipei | Taiwan | 2% | 1% | 97% |
| 10 | Liuzhou | China | 2% | 1% | 3% |

Table 4. Bot-infected computers by city, APJ region

Source: Symantec Corporation

The top five cities for bot-infected computers in the APJ region during this period were located in China. Beijing had the highest number of bot-infected computers in the region during the last six months of 2006, accounting for 16 percent of the total (table 4). It was also the highest ranked city worldwide during this period. Bot-infections in China are fairly spread out among various cities, with the highest percentage in a single city being only 20 percent of detected bots in China.¹¹

Guangzhou, China had the second highest number of bot-infected computers in the APJ region, accounting for eight percent of the total. Hangzhou, China was ranked third, accounting for five percent of bot-infected computers in the region. All three top cities in the region are ranked in the top ten bot-infected cities worldwide.

Bot-infected computers are often used to relay spam; however, the top ten cities for bot-infected computers do not correspond to the top ten cities for spam zombies, as is discussed in the “Top spam zombie countries and cities” section in this report. Chinese cities have a low proportion of spam zombies and a high proportion of bot-infected computers. This appears to contradict Symantec’s assertion that bot owners are currently shifting away from attack activity (such as DoS attacks) and toward spam relaying. However, it may be because Chinese ISPs filter out content such as spam, which would likely prevent spam zombies from being detected as frequently as bot-infected computers.

Japan had the fourth highest number of bots in APJ, and one of the highest numbers of broadband users in APJ,¹² so it would be reasonable to expect that Japanese cities would have high proportions of region-wide bots. However, the highest ranked Japanese city was Tokyo, which was ranked 52nd. This is due, in part, to the fact that bot infections in Japan are distributed fairly evenly throughout the country rather than being concentrated in one major city.

To prevent against 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.

¹¹ It should be noted that this discussion is limited to bots that can be located in a particular city with a confidence rating of four out of five. If this confidence rating is not achieved, the data will not be incorporated into the discussion.

¹² <http://www.point-topic.com/contentDownload/dslanalysis/world%20broadband%20statistics%20q1%202006.pdf> (access requires registration)

Top targeted sectors

Although many attackers select targets randomly, some attack computers within a specific sector, industry, or organization. For the purposes of this metric, these attacks are referred to as “targeted attacks.” For this discussion, a targeted attack is identified as an IP address that has attacked at least three sensors in a given industry to the exclusion of all other industries during the reporting period.

Between July 1 and December 31, 2006, the home user sector was by far the most highly targeted sector in the APJ region, accounting for 98 percent of all targeted attacks. As computers in the home user sector are less likely to have well established security measures and practices in place, they may be more vulnerable to targeted attacks. Furthermore, home users often store confidential information—such as banking information—on their computers and, as such, represent a fertile resource for identity theft. Therefore, it is likely that many of the targeted attacks against home users are used for fraud or other financially motivated crime.

It should be noted that the number of targeted attacks detected against home users might be inflated due to the way in which they access the Internet. It is likely that the majority of home users share networks that span a single block of IP addresses. As a result, opportunistic attacks targeting a broadband ISP may be noted as targeted attacks, thereby artificially inflating the percentage of targeted attacks against this sector.

Financial services was the second most frequently targeted sector in the second half of 2006, accounting for approximately 1.5 percent of attacks in the APJ region during this period. As has been discussed previously, Symantec believes that attackers are increasingly conducting online criminal activities for financial gain. The financial services industry is typically considered a popular target for attackers hoping to profit from attack activity. Symantec expects that attacks targeting the financial services industry will continue to rise as attackers become more profit driven.

Malicious activity by country

For the first time, in this volume of the *APJ Internet Security Threat Report*, Symantec is evaluating 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 relay hosts, and Internet attacks.

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

Between July 1 and December 31, 2006, China accounted for 39 percent of malicious activity in the APJ region, the most of any country (table 5). For each of the malicious activities taken into account for this measurement, China ranked number one with the exception of command-and-control servers and phishing hosts.

| Regional Rank | Country | Percentage of Malicious Activity | Malicious Code Rank | Spam Host Rank | Command and Control Server Rank | Phishing Host Rank | Bot Rank | Attack Rank |
|---------------|-------------|----------------------------------|---------------------|----------------|---------------------------------|--------------------|----------|-------------|
| 1 | China | 39% | 1 | 1 | 2 | 3 | 1 | 1 |
| 2 | South Korea | 16% | 5 | 2 | 1 | 4 | 3 | 3 |
| 3 | Taiwan | 14% | 3 | 3 | 3 | 2 | 2 | 4 |
| 4 | Japan | 13% | 2 | 4 | 4 | 1 | 4 | 2 |
| 5 | Australia | 6% | 4 | 10 | 5 | 5 | 5 | 5 |
| 6 | Thailand | 3% | 9 | 5 | 6 | 6 | 9 | 10 |
| 7 | Malaysia | 2% | 10 | 7 | 8 | 7 | 6 | 7 |
| 8 | Singapore | 2% | 8 | 9 | 7 | 8 | 7 | 6 |
| 9 | Philippines | 1% | 11 | 8 | 11 | 13 | 8 | 9 |
| 10 | New Zealand | 1% | 7 | 12 | 13 | 10 | 11 | 8 |

Table 5. Malicious activity by country, APJ region

Source: Symantec Corporation

The high number of bot-infected computers in China—71 percent of the region’s total—likely influences the country’s prominence in the other criteria considered for this metric. The relatively small proportion of APJ-based command-and-control servers in China (23 percent of the total) combined with the relatively high number of bots, likely indicates that bot-infected computers are being controlled by command-and-control servers outside the country.

In general, the high rate of malicious activity based in China is likely driven by the high number of Internet users there, as well as the rapid growth in the country’s Internet infrastructure. China has the second highest number of Internet users in the world, accounting for 11 percent of the total. Further, this number is expanding rapidly; the number of Internet users in China is expected to surpass those in the United States in the next year.

South Korea was the second highest country for malicious activity during this six-month reporting period, accounting for 16 percent of all malicious activity based in the APJ region during this period. South Korea ranked first for bot command-and-control servers and second for spam hosts.

South Korea is home to only six percent of the region’s bot-infected computers, but 43 percent of command-and-control servers. It is likely that command-and-control servers in South Korea are controlling bot-infected computers outside the country and using them to launch attacks.

South Korea also has a high proportion of the APJ region’s spam zombies (15 percent) compared to bot-infected computers (six percent). This may indicate that spammers are not using bots to send out their unsolicited email in this region. Because spammers are typically trying to gain profit, this may indicate that sending spam through means other than bots (for example, through open relays or other malicious code infections) is more cost effective than bots.

South Korea’s prominence may be due to its well established Internet population. South Korea has a high penetration of Internet users (66 percent of the population use the Internet, which is among the highest in Asia) and a fairly small Internet growth (78 percent between 2000 and 2007, which is one of the lowest in Asia).¹³ This likely shows that the majority of South Koreans who are using the Internet have been using it for some time, and are likely educated on threats such as bots and other malicious programs. This may also mean that threats like command-and-control servers have become embedded and are difficult to eliminate.

¹³ <http://www.internetworldstats.com>

In the last six months of 2006, Taiwan was the third ranked APJ country for malicious activity, with 14 percent. Taiwan has the seventh highest number of users in APJ, so its third-place rank is surprisingly high. Taiwan's ranking in the criteria activities is fairly constant; it is approximately the third highest country for each considered activity.

Taiwan has strong ties to China, which ranks highest for malicious activity. The relationship between Taiwan and China is complex and often contentious. Some of the malicious activity in Taiwan may be attributed to this. Additionally, Taiwan may have a higher proportion of English-speaking people than many other APJ countries, particularly in Asia, with at least one major institution dedicated to English speakers.¹⁴ Because many Internet-wide malicious code threats—particularly mass-mailer worms—rely on English for the social engineering messages involved in propagation, it is possible that the prevalence of English speakers in Taiwan has contributed to its relatively high ranking in this category.

Japan ranked fourth overall, with 13 percent of malicious activity. Part of the reason for Japan's high ranking is that more phishing Web sites were detected there during this reporting period than any other country. Japan has more Web-hosting companies but significantly fewer Web domains. The large number of companies hosting a small number of domains suggests that there are many small Web-hosting companies in Japan. Many of these small companies could be hosting phishing sites. For more information, see the "Top countries hosting phishing Web sites" section in this report.

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 high 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 percentage assigned to each country in this discussion thus equates to the amount 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.

Taiwan was the most highly ranked country for malicious activity per Internet user. 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 Taiwan would carry out 20 percent of the group's malicious activity (table 6).

¹⁴ <http://www.hess.com.tw/en/about>

| Regional Rank | Country | Proportion |
|---------------|-------------|------------|
| 1 | Taiwan | 20% |
| 2 | Singapore | 14% |
| 3 | Bangladesh | 10% |
| 4 | South Korea | 9% |
| 5 | Sri Lanka | 8% |
| 6 | Australia | 8% |
| 7 | China | 7% |
| 8 | New Zealand | 6% |
| 9 | Thailand | 5% |
| 10 | Philippines | 3% |

Table 6. Malicious activity by country per Internet user

Source: Symantec Corporation

Because Taiwan has less Internet users than many other APJ countries, each malicious activity incident counts for more than it would in a larger country. As a result, when measured by Internet user, malicious activity in Taiwan was fairly high in all regards, especially for bot-infected computers and malicious code. This may be due to the prevalence of English-language speakers, as was discussed in the previous section.

The high level of malicious activity taking place in Taiwan may also be influenced by the popularity of online games there, which is supported by the fact that two of the three new malicious code families in Taiwan are password-stealers for online games. Additionally, as discussed above, Taiwan has a strong relationship to China, which has high levels of malicious activity. The political relationship between Taiwan and China is complex and contentious. Some of the malicious activity in Taiwan may be attributed to this.

Singapore accounted for 14 percent of malicious activity per Internet user, the second highest percentage in the region. Like Taiwan, this is largely due to the small population of Internet users, which means that each incident carries more proportional weight. Additionally, as is the case in Taiwan, English is commonly spoken in Singapore, as it is one of the four official languages there. This would likely increase Singapore's exposure to mass-mailing worms and other English-based malicious code.

Bangladesh ranked third, accounting for 10 percent of malicious activity per Internet user. The high ranking of Bangladesh is mostly due to the large number of phishing sites that are hosted there. The proportion of malicious activity in Bangladesh is low for all of the considered activities except phishing Web sites. However, because Bangladesh has such a low Internet population, with approximately 0.1 percent of Asian Internet connections, the 24 phishing sites hosted there had a significant effect on the overall measure of activity per Internet user.

Japan was the thirteenth ranked country in the APJ region for malicious activity per Internet user. Japan has a relatively high number of Internet users, so a significant number of attacks are required to give Japan a high ranking. Additionally, Japan has a high Internet penetration and low Internet growth.¹⁵ This means that Internet users and ISPs are probably more aware of Internet security issues than their counterparts in countries with less well established Internet usage. As a result, they have likely implemented sufficient security practices and technologies to limit malicious activity in the country.

Malicious Code Trends

Symantec gathers malicious code data from over 120 million desktops that have deployed Symantec's antivirus products in consumer and corporate environments. The Symantec Digital Immune System and Scan and Deliver technologies allow customers to automate this reporting process. This discussion is based on malicious code samples reported to Symantec for analysis from the APJ region between July 1 and December 31, 2006.

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
- Top ten malicious code samples
- Top three new malicious code families
- Threats to confidential information
- Propagation mechanisms

This discussion will include any prevention and mitigation measures that might be relevant to the particular threats being discussed. However, 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—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. Additionally, Symantec recommends that ingress and egress filtering be put in place on perimeter devices to detect anomalous activity.

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 operating system vendor. 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.

Malicious code types

During the last six months of 2006, Trojans were the most common type of malicious code in the APJ region, accounting for 48 percent of the volume of malicious code reports received from the region (figure 2). During this same period, Trojans made up 45 percent of the volume of worldwide malicious code reports.¹⁶

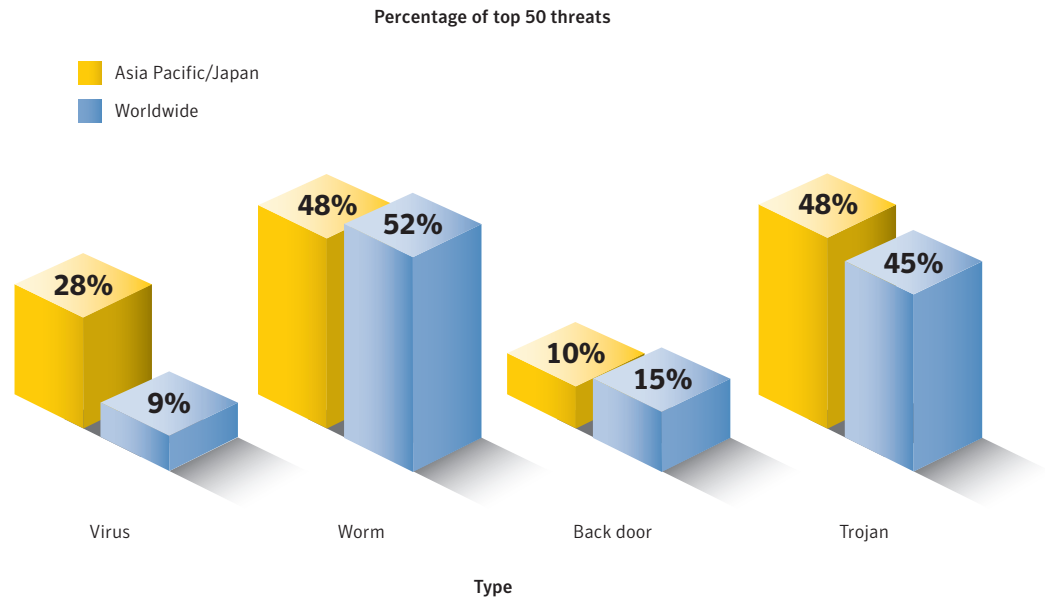


Figure 2. Malicious code types by volume

Source: Symantec Corporation

Trojans can expose confidential information, and can be used to install other malicious programs. Attackers are currently moving towards staged downloaders, which are also referred to as modular malicious code. 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.

In the second half of 2006, worms made up 48 percent of the volume of top 50 malicious code reports in the APJ region and 52 percent of the volume worldwide. Despite the similarity in total volume, there was a difference between the type of worms reported in APJ and worldwide. In the APJ region, there were fewer reports of mass-mailing worms, such as Netsky.P,¹⁷ and more reports of file-infecting worms that propagate through network shares. One example of such a worm was Looked.P.¹⁸ This difference will be examined in greater depth in the “Propagation mechanisms” section of this report.

During the current reporting period, viruses made up 28 percent of the volume of top 50 malicious code reports in the APJ region, compared to nine percent worldwide. This is due to the high number of reports of different variants of the Looked family of worms, most of which are also classified as viruses. Malicious code such as Looked.P that propagate through local networks tend to be more geographically localized. In this case, the majority of the reports were from the APJ region.

¹⁶ 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.

¹⁷ http://www.symantec.com/security_response/writeup.jsp?docid=2004-032110-4938-99

¹⁸ http://www.symantec.com/security_response/writeup.jsp?docid=2006-071212-0124-99

Top ten malicious code samples

The top reported malicious code sample for the APJ region was the file-infecting worm Looked.P (table 7). This worm propagates through insecure shared network drives and has the ability to infect executable files. Reports from China made up 75 reports of Looked.P reports. This will be explored in greater depth later in this section.

| Regional Rank | Worldwide Rank | Sample | Type | Propagation Vectors | Impact | Top Reporting Country |
|---------------|----------------|-----------------|-------------|--|---|-----------------------|
| 1 | 2 | W32.Looked.P | Worm, Virus | File Sharing | Downloads and installs other threats | China |
| 2 | 3 | W32.Stration | Worm | SMTP | Downloads and installs other threats | China |
| 3 | 5 | W32.Stration.DL | Worm | SMTP | Downloads and installs other threats | China |
| 4 | 40 | W32.Looked.O | Worm, Virus | File Sharing | Downloads and installs other threats | China |
| 5 | 1 | W32.Netsky.P | Worm | SMTP, P2P | Keystroke logger targets www.e-gold.com | Taiwan |
| 6 | 11 | W32.Sality.U | Virus | File Sharing | Downloads and installs other threats | New Zealand |
| 7 | >50 | W32.Looked.I | Worm, Virus | File Sharing | Downloads Lineage infostealer | China |
| 8 | 22 | W32.Mytob.U | Worm | SMTP, File Sharing, Remote Vulnerability | Allows remote access | China |
| 9 | 38 | W32.Mytob.AA | Worm | SMTP | Allows remote access | Thailand |
| 10 | 4 | W32.Blackmal.E | Worm | SMTP, File Sharing | Overwrites files | Japan |

Table 7. Top ten malicious code samples, APJ region

Source: Symantec Corporation

Symantec's data suggests that many malicious code samples are found in geographical clusters. The most striking case of this clustering is the Looked family of worms/viruses. Of the Looked variants in the top 25 malicious code samples reported in APJ, 75 percent of Looked.P, 96 percent of Looked.I,¹⁹ 99 percent of Looked.J,²⁰ and 70 percent of Looked.AH reports came from China.²¹ Most variants of this family of worms share the ability to propagate through network file sharing.

Viruses and worms that propagate through file sharing do so by infecting files on a computer connected to mapped network drives. Once a virus infects a file on the mapped drive, the infected file will be accessible to all computers on the network. Computers sharing drives tend to be located on the same corporate network and are often within fairly close geographical proximity to each other. Note that this mostly applies to threats that spread through local networks and share drives, not to malicious code that spreads through P2P networks. P2P networks are geographically diverse in their user base.

¹⁹ http://www.symantec.com/security_response/writeup.jsp?docid=2006-052911-4543-99

²⁰ http://www.symantec.com/security_response/writeup.jsp?docid=2006-061614-3351-99

²¹ http://www.symantec.com/security_response/writeup.jsp?docid=2006-091513-2550-99

Symantec APJ Internet Security Threat Report

If a large network like that of an enterprise is infiltrated by a virus or worm that propagates through file sharing, the number of reports will also be high since many of the computers on the network are likely to become infected or contain infected files. Because of this, the high volume of Looked infections in China could indicate that these viruses infected enterprises or other large organizations in these countries.

Some other geographic clustering is found with certain mass-mailing worms. For instance, all Mytob.AA reports were from Thailand,²² the majority of Mytob.AG²³ and Mytob.EE²⁴ reports were from New Zealand, and the majority of Mytob.U reports were from China.²⁵ The localization of these samples is likely caused by the SMTP propagation mechanisms.

An SMTP worm typically propagates by sending mail to email addresses found on a compromised computer. The addresses found are often those of friends, family, and business associates, many of whom would fall within the same geographical vicinity as the initial infection. As a result, these types of worms tend to take some time to propagate away from the geographic location of the first infection. Furthermore, worms that propagate using email written in a particular language tend to propagate mainly within countries that speak that language.

The second most frequently reported malicious code sample in the APJ region during this period was the mass-mailing worm Stration.²⁶ This worm emails copies of itself with various subject headers, messages, and attachment names to email addresses that are gathered from a compromised computer. Once installed on a computer, the worm also attempts to download and execute remote files from predetermined Web sites.

The third most frequently reported malicious code sample was Stration.DL,²⁷ another member of the Stration family of worms. There were hundreds of variants of Stration reported during this period, all with similar behavior and features. On an Internet-wide basis, this was the most widely reported new malicious code family during this reporting period.

Two Trojans that are designed to steal online game information, Gampass²⁸ and Lineage,²⁹ were the eleventh and thirteenth most frequently reported samples in the APJ region, respectively. Both samples appeared to be more common in Taiwan in this period than in other parts of the APJ region. Taiwan accounted for 81 percent of the Gampass reports and 53 percent of the Lineage reports in APJ in the second half of 2006. This is likely due to the well established online gaming culture in Taiwan and the large number of online game profiles located there.

Bacalid³⁰ and Bacalid.B³¹ are polymorphic viruses that can download other threats. Both viruses have a feature that allows them to cease all malicious activity if the language setting of the computer they are running on is set to simplified Chinese. Simplified Chinese is prevalent in China and Singapore while traditional Chinese is more common in Hong Kong and Taiwan. The only reports of these viruses for this period came from Hong Kong and Taiwan, suggesting that these viruses are being used to target these locations. These viruses are programmed to download and execute other threats from certain specific Web sites that are registered from China with false credentials.

²² http://www.symantec.com/security_response/writeup.jsp?docid=2005-040421-3550-99

²³ http://www.symantec.com/security_response/writeup.jsp?docid=2005-041009-4908-99

²⁴ http://www.symantec.com/security_response/writeup.jsp?docid=2005-061118-3634-99

²⁵ http://www.symantec.com/security_response/writeup.jsp?docid=2005-040116-4532-99

²⁶ http://www.symantec.com/security_response/writeup.jsp?docid=2006-092111-0525-99

²⁷ http://www.symantec.com/security_response/writeup.jsp?docid=2006-103112-2047-99

²⁸ http://www.symantec.com/security_response/writeup.jsp?docid=2006-111201-3853-99

²⁹ <http://securityresponse1.symantec.com/sarc/sarc.nsf/html/Infostealer.lineage.html>

³⁰ http://www.symantec.com/security_response/writeup.jsp?docid=2006-090109-5610-99

³¹ http://www.symantec.com/security_response/writeup.jsp?docid=2006-092010-4342-99

Top three new malicious code families

The most prevalent new malicious code family reported in the APJ region during this period was the Stration worm (table 8). More than 150 variants of this worm were discovered in the last six months of 2006. This worm emails copies of itself to all email addresses gathered from a compromised computer. Once installed on a computer, the worm also attempts to download and execute remote files from predefined Web sites. Unlike the distribution of these worms in the Europe, Middle East, and Africa (EMEA) region, in which Stration was mostly found in the Czech Republic, Stration was distributed fairly evenly in the APJ region. While this family of worms was most frequently reported from China, it was also reported from Japan, Australia, and Taiwan in significant numbers.

| Regional Rank | Worldwide Rank | Sample | Type | Propagation Vectors | Impact | Top Reporting Country |
|---------------|----------------|----------|--------|---------------------|--|-----------------------|
| 1 | 1 | Stration | Worm | SMTP | Downloads and installs other threats | China |
| 2 | 3 | Shufa | Worm | Yahoo! IM, SMTP | Steals passwords for Lineage online game | Taiwan |
| 3 | 2 | Gampass | Trojan | N/A | Steals online gaming passwords | Taiwan |

Table 8. Top three new malicious code families

Source: Symantec Corporation

In the second half of 2006, the Shufa³² worm and the Gampass information-stealing Trojan were the second and third most common new families, respectively. They are indicative of a growing trend towards threats that steal account information for online games. As the popularity of these games continues to grow, so does the potential for profit to be made from them. A secondary market has emerged on various online auction sites in which users buy and sell items gathered within these games. Once an attacker has stolen a user's account information, he or she can sell the user's items and keep the profits.

These online games are popular in the APJ region, particularly in Taiwan and South Korea.³³ As Shufa and Gampass were found primarily in Taiwan, that country appears to be a target of specific information-stealing attacks. Symantec expects to continue to see new threats targeting online gamers.

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.

To protect against Trojans, users should never execute 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.

³² http://www.symantec.com/security_response/writeup.jsp?docid=2006-080815-5056-99

³³ http://news.com.com/Consumers+Gaming+their+way+to+growth+--+Part+3+of+South+Koreas+Digital+Dynasty/2009-1040_3-5239555.html

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.³⁴ Sensitive corporate information could also be leaked from compromised computers including financial details, business plans, and proprietary technologies.

In the last six months of 2006, the volume of threats to confidential information in the top 50 malicious code reported from the APJ region was 60 percent. This is somewhat less than the worldwide proportion of 66 percent. This can partially be attributed to the high volume of Looked.P reports in APJ. This threat was the highest reported sample in the region during this period; however, it does not expose confidential information.

In the APJ region, threats that allow remote access, such as back doors, made up 84 percent of confidential information threats by volume of reports, the same percentage that was reported worldwide during this period (figure 3). Remote access threats tend to be favored by attackers since they are able to perform almost any action on the compromised computer.

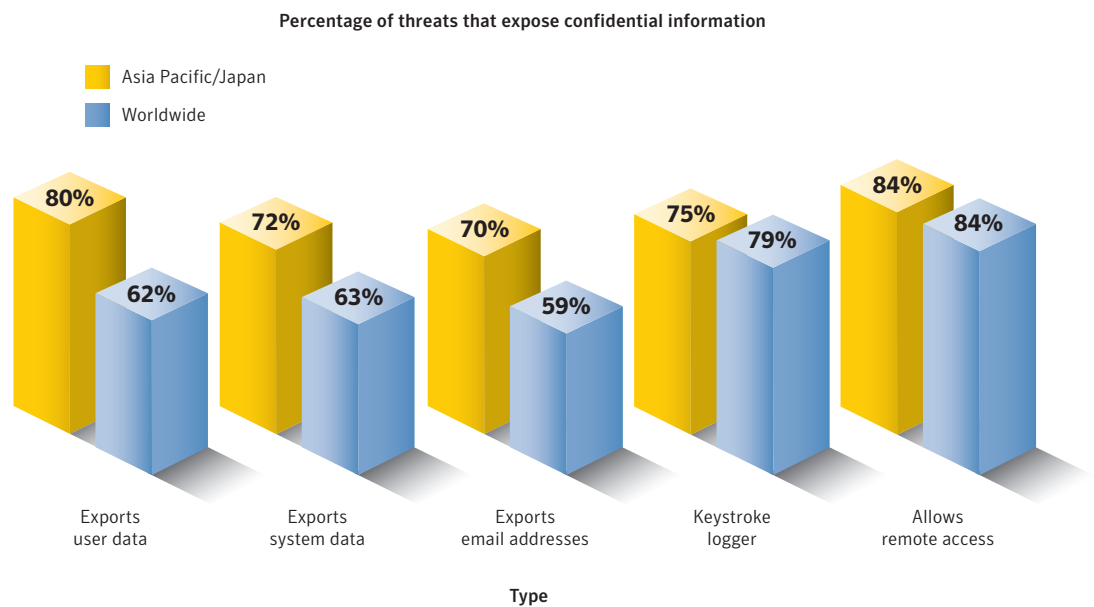


Figure 3. Threats to confidential information by type
 Source: Symantec Corporation

³⁴ 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>

Threats that could be used to export user data accounted for 80 percent of the volume of threats to confidential information in the APJ region during this reporting period. Across the Internet as a whole, threats that export user data made up 62 percent of the volume of threats to confidential information during this period. Since the user data that these threats export could include online account credentials, their popularity in the APJ region is not surprising. As was discussed in the “Top three new malicious code families” section of this report, threats that steal online game account information are becoming increasingly common in the APJ region. Threats that export user data could be used to steal account credentials for online gamers.

The top threat that steals online game information this period was Lineage,³⁵ a Trojan horse that is designed for stealing passwords for the online game Lineage. This Trojan can be downloaded by the Looked.I worm, the seventh highest sample reported in this region. The highest reporting countries for this Trojan in the second half of 2006 were Taiwan, China, South Korea, and Japan. Users who play online games in these countries should be especially aware of information-stealing threats due to their prevalence.

Seventy-two percent of threats to confidential information reported in the APJ region during the last six months of 2006 could be used to export system data, compared to 63 percent of these threats reported worldwide. 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, they can use this to craft a targeted social engineering attack that is highly tailored to that particular user.

The volume of threats that log keystrokes was lower in the APJ region than worldwide for this reporting period. Keystroke logging threats made up 75 percent of confidential information threats by volume of reports, lower than the 79 percent reported globally. A keystroke logger will record keystrokes on the compromised computer and, in most cases, email the log to the attacker or upload it to a Web site that is under the attacker’s control. This makes it easier for an attacker to gather confidential information from a large number of compromised computers with minimal effort.

Threats that could be used to export email addresses accounted for 70 percent of confidential information threats by volume, 11 percent higher than the 59 percent worldwide. This form of information harvesting is often used to compile lists of valid email addresses, which are subsequently sold to spammers.

The volumes and types of threats to confidential information are a reflection of an increasing trend towards more robust malicious code that can be used for financial gain. User data can be used to steal online game profiles and other personal information that can be sold for profit. System information can be used to exploit the compromised computer for other means. Keystroke logging can be used to steal passwords for banking and other online services. Remote access allows an attacker to obtain all of the previously mentioned information by installing other malicious programs.

³⁵ http://www.symantec.com/security_response/writeup.jsp?docid=2005-011211-3355-99

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),³⁶ peer-to-peer services (P2P), and remotely exploitable vulnerabilities. Some malicious code may even use other malicious code as a propagation vector by locating a computer that has been compromised by a back door server and using it to upload and install itself.

This section will discuss some of the propagation mechanisms used by malicious code samples reported to Symantec during the last six months of 2006. Readers should note 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.

Malicious code that propagates by CIFS made up 60 percent of malicious code that propagates in APJ in the second half of 2006 (figure 4). In contrast, the CIFS vector was only used by 32 percent of worldwide reports of malicious code that propagates. The difference between regional and worldwide data can largely be attributed to the higher number of reports in the APJ region for the Looked.P worm,³⁷ which utilizes CIFS to propagate.

This worm searches for network shares with weak password protection to copy itself to and also contains a viral component to infect executable files on a compromised computer. Other variants of this worm also experienced a fair amount of success in the APJ region during this period, particularly Looked.O,³⁸ which shares an almost identical feature set with Looked.P. The seven variants of Looked in the top 50 samples from this region made up 48 percent of propagating malicious code in the APJ region during this period. Worldwide, Looked.P was the only Looked variant that appeared in the top 50, and it accounted for only ten percent of propagating code.

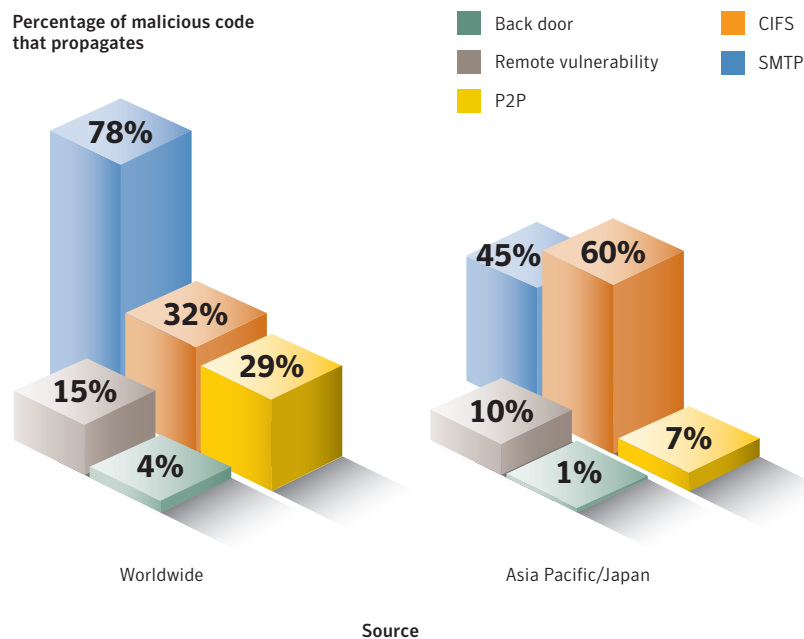


Figure 4. Propagation mechanisms
Source: Symantec Corporation

³⁶ 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.
³⁷ http://www.symantec.com/security_response/writeup.jsp?docid=2006-071212-0124-99
³⁸ http://www.symantec.com/security_response/writeup.jsp?docid=2006-071212-0828-99

SMTP was used by 45 percent of the volume of top 50 samples in the APJ region during this period, making it the second most common propagation mechanism. SMTP accounted 78 percent of the volume of the top 50 malicious code samples worldwide. This percentage of samples in the APJ that propagates over SMTP is limited by the high number of Looked reports.

Another possible reason for the lower number of SMTP reports in the APJ region is that many of the common SMTP propagation worms use social engineering messages that are written in English. As a result, they are likely to be disregarded by the significant portion of the APJ population that consists of non-English speakers.

Only seven percent of propagating malicious code reported in the APJ region during this period used P2P as a means to propagate compared to 29 percent globally. Worms can use P2P as their only means of propagation or use it in conjunction with other propagation mechanisms such as SMTP or remote vulnerabilities. An example of a P2P worm specific to the APJ region is the Antinny family of worms.³⁹ Antinny copies itself into folders that are shared on the popular Japanese P2P program Winny. Antinny gets other users of Winny to download the executable file by using various interesting file names as a lure. Interested downloaders will execute the file and their computers will become infected. Reports of Antinny were high in the first half of 2006, but dropped in the second half of the year.

The lower volume of samples that propagate using P2P that was reported in the APJ region compared to worldwide can be attributed to a lower proportion of mass-mailing worms such as Netsky.P and Mydoom.L⁴⁰ that can use P2P as a propagation vector. A worm of this type propagates by sending out email with a copy of itself as an attachment and by placing copies of itself in folders usually associated with P2P file sharing. Some malicious code is equipped to use more than one propagation mechanism. Many of these worms can use either SMTP or P2P; however, for most, the primary means of propagation is SMTP. As a result, the P2P propagation mechanism is available for use, but does not generally result in as many infections as SMTP.

³⁹ http://www.symantec.com/security_response/writeup.jsp?docid=2003-080817-4045-99

⁴⁰ http://www.symantec.com/security_response/writeup.jsp?docid=2004-071915-0829-99

Phishing

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 July 1 and December 31, 2006.

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

This section of the Symantec *APJ Internet Security Threat Report* will discuss the top countries and cities in which phishing 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 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 site will be located in the same country as the intended victims of the attack.

Japan was home to the highest percentage of phishing Web sites in APJ (table 9). It was the fifth highest country in the world for phishing Web sites after the United States, Germany, the United Kingdom, and France. Japan is home to the second most Web-hosting companies in Asia.⁴¹ A large Web-hosting company is likely to host many domains. Compared to neighboring China, Japan has more Web-hosting companies but significantly fewer Web domains.⁴² The large number of companies hosting a small number of domains suggests that there are many small Web-hosting companies in Japan. Many of these small companies could be hosting phishing sites.

⁴¹ <http://www.webhosting.info/webhosts/globalstats>

⁴² <http://webhosting.info/domains/countrystats>

| Regional Rank | Worldwide Rank | Country | Regional Percentage | Worldwide Percentage |
|---------------|----------------|-------------|---------------------|----------------------|
| 1 | 5 | Japan | 21% | 3% |
| 2 | 6 | Taiwan | 20% | 3% |
| 3 | 8 | China | 17% | 2% |
| 4 | 9 | South Korea | 15% | 2% |
| 5 | 17 | Australia | 8% | 1% |
| 6 | 19 | Thailand | 6% | 1% |
| 7 | 30 | Malaysia | 3% | <1% |
| 8 | 38 | Singapore | 2% | <1% |
| 9 | 39 | Bangladesh | 2% | <1% |
| 10 | 42 | New Zealand | 2% | <1% |

Table 9. Top countries hosting phishing Web sites

Source: Symantec Corporation

Hosting a phishing site with a small Web-hosting company can be advantageous for a phisher. In many cases, these companies do not have the same security and/or support resources as larger Web-hosting companies. As a result, they might not be able to perform constant content monitoring and other security measures may not have been fully implemented. A phisher could thus post a phishing Web site with a small Web-hosting company and have less chance of the site being discovered right away. In such cases, the phishing site is likely to remain active until the owner of the computer discovers it has been compromised. It is likely that many phishing sites in Japan are hosted in this fashion.

Taiwan had the second highest number of phishing Web sites in the APJ region. Web hosting is not as large an industry in Taiwan as it is elsewhere in the region; Taiwan ranks forty-third worldwide in terms of number of Web-hosting companies and forty-fifth in terms of Web domains. However, Taiwan ranks second behind China in the number of bots in the APJ region. These statistics suggest that a greater number of phishing Web sites in Taiwan are hosted on bot-infected computers rather than on Web hosts.

A computer that is compromised by a bot can be used to host phishing sites, but is less reliable than a computer on an actual Web host. A large amount of Web traffic destined to a computer that normally does not receive such traffic—like a home computer—is likely to raise suspicion and result in the site being shut down. However, this method is still used by phishers because even a short-lived phishing site can generate a lot of stolen identities.

China had the third highest number of phishing Web sites in the APJ region with 17 percent of the total. China has by far the highest number of bot-infected computers in the region, but still hosts less phishing Web sites than Taiwan. This is likely because bot-infected computers in China are used for purposes other than hosting phishing sites.

China has the highest number of Web domains in the region by a significant margin, but only ranks fourth in terms of Web-hosting companies. Since there are a small number of companies hosting a large number of sites in China, it is reasonable to conclude that these Web-hosting companies are quite large. Many phishing sites in China are likely located on these large Web-hosting providers. By hosting their sites with large providers, phishers gain the advantage of obscurity. With many sites hosted by a single provider, it may take days for the provider to discover the illegal site and shut it down.

Top cities hosting phishing Web sites

The city hosting the largest number of phishing sites in the region was Taipei (table 10). Nineteen percent of the phishing sites in the APJ region during this period were located there. Worldwide, Taipei ranked third among cities for phishing Web sites after Dallas, U.S.A. and Karlsruhe, Germany. As the largest city and center of commerce for Taiwan, the majority of Internet users in Taiwan likely use an ISP located in Taipei. Since Taiwan hosted the second most phishing sites in this region, Taipei's top ranking is not surprising.

| Regional Rank | Worldwide Rank | City | Country | Regional Percentage | Worldwide Percentage |
|---------------|----------------|--------------|-------------|---------------------|----------------------|
| 1 | 3 | Taipei | Taiwan | 19% | 3% |
| 2 | 6 | Seoul | South Korea | 14% | 2% |
| 3 | 9 | Tokyo | Japan | 11% | 1% |
| 4 | 13 | Hong Kong | China | 9% | 1% |
| 5 | 24 | Bangkok | Thailand | 6% | 1% |
| 6 | 42 | Osaka | Japan | 4% | 1% |
| 7 | 56 | Kuala Lumpur | Malaysia | 3% | <1% |
| 8 | 84 | Singapore | Singapore | 2% | <1% |
| 9 | 91 | Beijing | China | 2% | <1% |
| 10 | 95 | Dhaka | Bangladesh | 1% | <1% |

Table 10. Top cities hosting phishing Web sites

Source: Symantec Corporation

Seoul hosted the second most phishing Web sites in the APJ region. As the capital of South Korea, and the country's most populous center, Seoul has a large number of Internet users. South Korea is also home to the majority of the Web-hosting companies in Asia, most of which are located in Seoul. Many of these providers are likely the unsuspecting hosts of high numbers of phishing Web sites.

Tokyo was host to the third most phishing Web sites in the APJ region. Since Tokyo is highly populated and a center for politics and commerce, it makes sense that there are many Web-hosting companies and a large number of Internet users located there. Furthermore, Japan hosted the most phishing Web sites in the region during this period. Therefore, it follows that the country's largest city should have a high number of phishing Web sites.

Phishing sites are often hosted in the same geographical region as the victims they are intended to defraud. This is more likely to be the case when the brand being phished uses a domain name that uses a country-specific top-level domain such as .jp for Japan or .tw for Taiwan. A phishing victim may be more inclined to believe that the phishing site is legitimate when the top-level domain matches that of the legitimate Web site they expect to be visiting.

It is also to the phisher's advantage to attempt to phish in places where people have significant disposable income. People with more money are more likely to purchase items online, and make use of online banking or trading accounts. It is, therefore, no surprise that the top three cities in this list are also listed as the three most affluent cities in Asia.⁴³

⁴³ http://www.citymayors.com/features/quality_survey.html

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.⁴⁴

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.⁴⁵

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.⁴⁶ 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, antispyware 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.⁴⁷ Several APJ-based organizations including Standard Chartered⁴⁸ and The Australian Institute of Criminology,⁴⁹ also provide advice to help users stay safe online. Additionally, network administrators can review Web proxy logs to determine if any users have visited known phishing sites.

⁴⁴ 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.

⁴⁵ A good resource for information on the latest phishing threats can be found at <http://www.antiphishing.org>

⁴⁶ "Cousin domains" refers to domain names that include some of the key words of an organization's domain or brand name; for example, for the corporate domain "bigbank.com" cousin domains could include "bigbank-alerts.com," "big-bank-security.com," and so on.

⁴⁷ <http://www.ic3.gov/preventiontips.aspx>

⁴⁸ http://www.standardchartered.com/global/home/security_tips/online_threats.htm

⁴⁹ <http://www.aic.gov.au/publications/crm/crm037.html>

Spam

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. It could also cause a loss of service or degradation in the performance of network resources and email gateways. This section of the *APJ Internet Security Threat Report* will discuss developments in spam activity in the APJ region between July 1 and December 31, 2006.

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, the Probe Network 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
- Distribution of spam zombies
- Spam as a percentage of all email by country

Top ten countries of spam origin

This section will discuss the top ten countries of spam origin in the APJ region. The nature of spam and its distribution on the Internet 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.

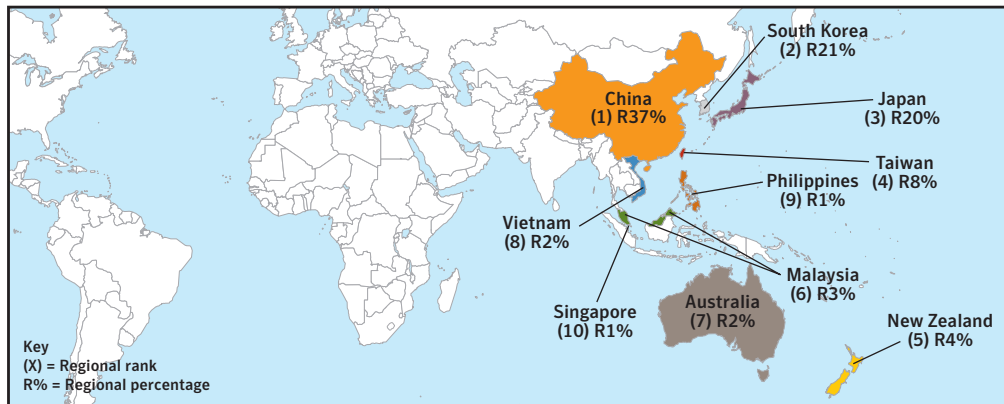


Figure 5. Top ten countries of spam origin, APJ region

Source: Symantec Corporation

Thirty-seven percent of all spam detected from the APJ region during this period originated in China, the most of any country in APJ (figure 5). This is likely due to the high number of broadband users in that country and the high percentage of bot-infected computers located there, as was discussed in the “Bot-infected computers by country” section of this report. Since spammers often use bots to send their bulk mail, this correlation is not surprising. China also had the largest number of spam zombies of any country in the region, with 43 percent of the region’s spam zombies, some of which consist of bots.

The second highest volume of spam detected being sent from the APJ region during this period originated in South Korea, which accounted for 21 percent of the total. This is likely due to the high rate of connectivity in South Korea and the availability of legitimate mail servers. 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. Spam can then be sent through the compromised computer to the legitimate mail server and off to its destination. When a country has numerous legitimate mail servers, it is likely that many of them will be used to send spam. This is especially true if any of the servers are misconfigured and can be used as open relays.⁵⁰ South Korea the second highest number of spam zombies in the APJ region during this period. Therefore, it is likely that a large amount of the spam from Korea is sent through either compromised computers or legitimate mail servers.

Japan had the third highest volume of spam in the APJ region in the last six months of 2006, accounting for 20 percent of the region’s total. Like South Korea, Japan has a high rate of broadband use as well as many legitimate mail servers that could be used illicitly to relay spam. Japan has a large number of ISPs and has the fourth highest number of spam zombies in the region, a number that corresponds closely with its rank in this category.

⁵⁰ An open mail relay is an SMTP (email) server configured in such a way that it allows anyone on the Internet to relay (i.e. send) email through it.

Distribution of spam zombies

A spam zombie is a computer infected with a bot or some other malicious code that allows email messages to be relayed. The countries of spam origin above include spam messages that may also be sent from legitimate email servers.

Between July 1 and December 31, 2006, China was the country with the most spam zombies in the APJ region and the second most in the world after the United States (table 11). Forty-three percent of spam zombies in the region were located there. China is home to the largest number of bot-infected computers in the region. This connection is not coincidental; many bots are designed to be used mainly to send spam and are detected as spam zombies. As previously noted in the “Top ten malicious code samples” section of this report, China was one of the top reporting countries of bots such as Mytob.U, which can be used to send spam.

| Regional Rank | Worldwide Rank | Country | Regional Percentage | Worldwide Percentage |
|---------------|----------------|-------------|---------------------|----------------------|
| 1 | 2 | China | 43% | 9% |
| 2 | 9 | South Korea | 15% | 3% |
| 3 | 11 | Taiwan | 13% | 3% |
| 4 | 16 | Japan | 9% | 2% |
| 5 | 17 | Thailand | 5% | 1% |
| 6 | 24 | Vietnam | 3% | 1% |
| 7 | 26 | Malaysia | 3% | 1% |
| 8 | 27 | Philippines | 3% | 1% |
| 9 | 32 | Singapore | 2% | <1% |
| 10 | 33 | Australia | 2% | <1% |

Table 11. Distribution of spam zombies by country

Source: Symantec Corporation

South Korea accounted for the second most spam zombies in the region with 15 percent. South Korea likely ranks high because it has the highest broadband penetration per household in the world.⁵¹ Broadband-connected computers make ideal spam zombies because they are always connected to the Internet and have enough bandwidth to send many spam messages at once. Also, in countries with high broadband penetration, it is likely that many users who are connected to the Internet are not well informed about computer security practices. These computers could thus more easily be infected by a bot or other malicious code and used as a spam zombie. Further, once infected, these machines are likely to remain undetected for extended periods of time.

Taiwan had the third highest number of spam zombies in the APJ region during the second half of 2006, with 13 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.

Seoul was the city with the highest number of spam zombies in the APJ region, with 14 percent of the region's total (table 12). It also had the second most of any city in the world after Madrid, with three percent of the world's spam zombies. Seoul's high ranking is not surprising, as it is the largest city in South Korea, where 15 percent of the region's spam zombies are located. Furthermore, many of the country's ISPs are situated there. It is reasonable to conclude that a high percentage of South Korea's spam zombies are located in Seoul. Since Seoul was not among the top ten cities for bot-infected computers, many of the spam zombies in the city are likely computers infected with Trojans.

| Regional Rank | Worldwide Rank | City | Country | Regional Percentage | Worldwide Percentage |
|---------------|----------------|--------------|-------------|---------------------|----------------------|
| 1 | 2 | Seoul | South Korea | 14% | 3% |
| 2 | 5 | Taipei | Taiwan | 12% | 3% |
| 3 | 14 | Bangkok | Thailand | 5% | 1% |
| 4 | 15 | Guangzhou | China | 4% | 1% |
| 5 | 18 | Beijing | China | 4% | 1% |
| 6 | 24 | Kuala Lumpur | Malaysia | 3% | 1% |
| 7 | 26 | Hanoi | Vietnam | 3% | 1% |
| 8 | 30 | Fuzhou | China | 3% | 1% |
| 9 | 31 | Jinan | China | 3% | 1% |
| 10 | 37 | Singapore | Singapore | 2% | <1% |

Table 12. Distribution of spam zombies by city

Source: Symantec Corporation

Taipei had the second highest number of spam zombies in the APJ region in the second half of 2006 with 12 percent of the regional total. It was fifth in the world with three percent of worldwide spam zombies. This is not surprising given the fact that Taiwan is home to 13 percent of the region's spam zombies and that Taipei is the political, economic, and demographic hub of the country. Taipei is also home to most of the country's ISPs and there are a large number of broadband-connected computers located there. Finally, Taipei was home to two percent of the APJ region's bot-infected computers during this period, many of which are likely used as spam zombies.

Bangkok was the city with the third highest number of spam zombies in the APJ region during this period, with five percent of the total. This is mainly due to the fact that Thailand had the fifth highest number of spam zombies in the region, and that Bangkok is the largest city in the country. Excluding cities in China, Bangkok was the city with the second highest number of bots in the APJ region during this period, accounting for three percent.

Spam as a percentage of email

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.⁵² Between July 1 and December 31, 2006, spam made up 59 percent of all monitored email traffic across the Internet as a whole. In the APJ region alone, spam made up 69 percent of all monitored email traffic.

For the first time, in this reporting period, Symantec has monitored spam as a percentage of all email on a per-country basis. Of the top 20 email-producing countries in this region, the top five countries according to the volume of spam by volume are listed in Table 13. 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.

| Regional Rank | Country | Spam as a Percentage of Email |
|---------------|-------------|-------------------------------|
| 1 | Philippines | 88% |
| 2 | Vietnam | 86% |
| 3 | Sri Lanka | 86% |
| 4 | Laos | 85% |
| 5 | Malaysia | 84% |

Table 13. Top five APJ countries by percentage of spam

Source: Symantec Corporation

Of the top 20 email-producing countries in the APJ region, the Philippines produced the highest percentage of spam, with 88 percent. Vietnam had the second highest percentage of spam; 86 percent of all mail originating there was classified as spam. Sri Lanka also had a spam percentage of 86 percent, making it the third highest spam-producing country in the APJ region.

The prevalence of pirated software may contribute to the percentage of spam from these countries. Pirated software is generally defined as software that is either not paid for or not legally acquired. A country's computer piracy rate is calculated as the percentage of software put into use over a year that was not paid for or legally acquired.⁵³ Pirated software can contain hidden Trojans or back doors, making the users that install them vulnerable to many different threats, including infection by spam bots. A high piracy rate can contribute to a high percentage of spam from a country. Some of the countries with the highest spam rate also have high computer piracy rates. For example, the piracy rate of the Philippines was 71 percent in 2005. This was significantly higher than the worldwide piracy rate of 35 percent. The piracy rate for Vietnam was the highest in the world in 2005 at 90 percent. These high piracy rates could have contributed to the high percentage of spam in these countries.

Spam made up 61 percent of all email from Japan, which was eight percent lower than the regional average. This may be related to Japan's very low piracy rate of 28 percent. Since Japan was one of the largest producers of spam in this region this also indicates that a high volume of legitimate email is sent from Japan.

⁵² 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 robust 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.

⁵³ <http://www.bsa.org/globalstudy/upload/2005%20Piracy%20Study%20-%20Official%20Version.pdf>

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 PC or Macintosh 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.
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 last six months of 2006. 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.

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.

Top targeted sectors

For the purposes of the *APJ Internet Security Threat Report*, a targeted attacker is defined as one that is detected attacking at least three users or organizations in a specific sector, to the exclusion of all other sectors. The targeted sector attack rate is a measure of the percentage of all attackers that target only organizations or users in a specific sector, and is represented as a proportion of all targeted attacks.

Figure 6 represents the proportional sensor distribution for each sector. Sectors with less than ten sensors have been excluded from the resulting totals.

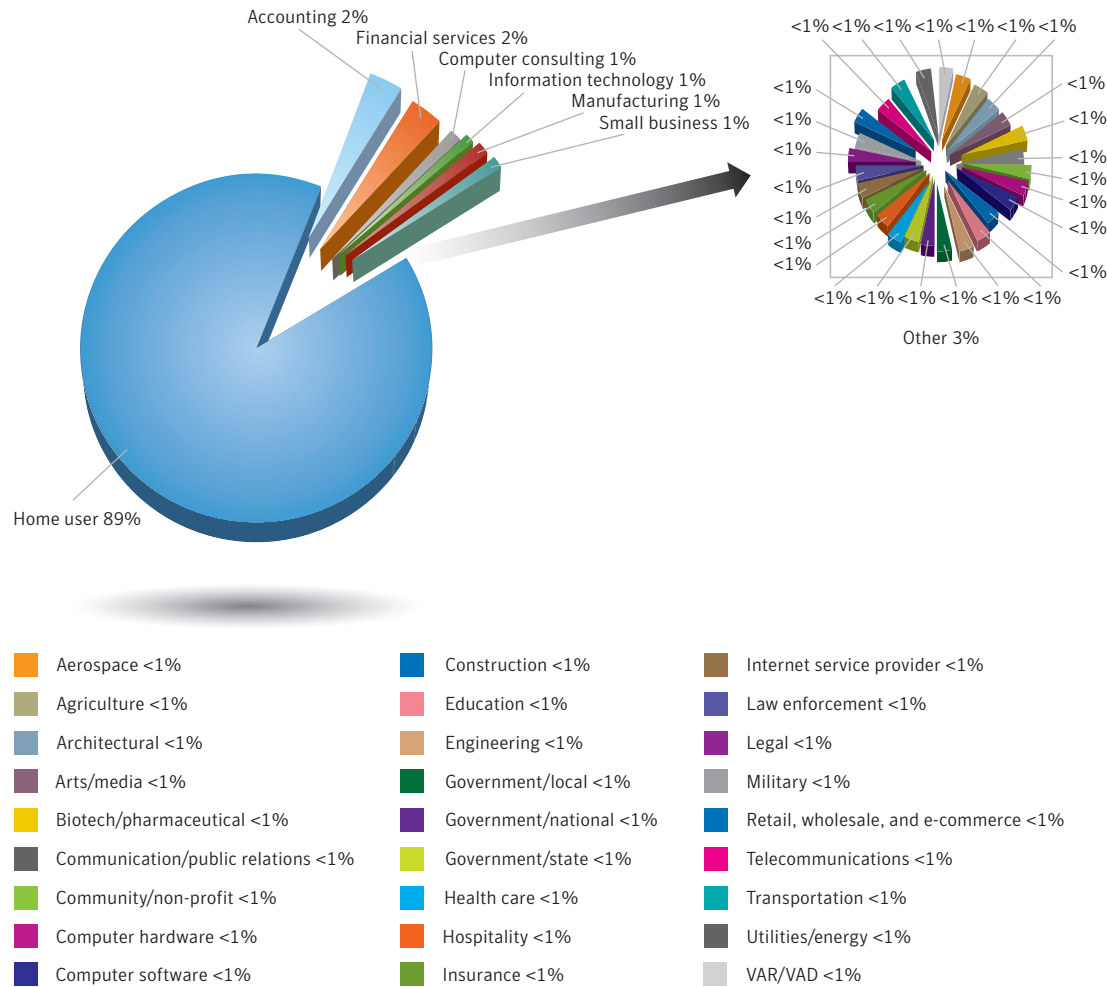


Figure 6. Distribution of sensors by sector
 Source: Symantec Corporation

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.

Appendix D—Phishing and Spam Methodology

Traditionally, the Symantec *APJ Internet Security Threat Report*, has broken security threats down into three general categories: attacks, vulnerabilities, and malicious code. However, as Internet-based services and applications have expanded and diversified, the potential for computer programs to introduce other types of security risks has increased. The emergence of new risks, particularly spam, phishing, spyware, adware, and misleading applications has necessitated an expansion of the traditional security taxonomy.

Symantec has monitored these new concerns as they have developed. In particular, the *APJ Internet Security Threat Report* assesses these risks according to these categories:

- Phishing
- Spam

The methodology for each of these discussions will be discussed in the sections below.

Phishing

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.

Symantec APJ Internet Security Threat Report

Top countries and cities hosting phishing 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.

Spam

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 the network layer, where DNS block lists typically operate. This is because SMTP-layer spam filtering is more robust 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 ten countries of spam origin

The data for this section is determined by calculating the frequency of originating server IP addresses in email messages that trigger antispy 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 by spam zombies

The data for this section is determined by examining the IP addresses in spam messages received by the Symantec Probe Network. Only IP addresses that are dynamically assigned are examined. If the computers at those IP addresses do not appear to be email servers—for example, if they do not respond to requests on TCP port 25—they are classified as spam zombies. 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 antispy 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.

Any technical information that is made available by Symantec Corporation is the copyrighted work of Symantec Corporation and is owned by Symantec Corporation.

NO WARRANTY. The technical information is being delivered to you as is and Symantec Corporation makes no warranty as to its accuracy or use. Any use of the technical documentation or the information contained herein is at the risk of the user. Documentation may include technical or other inaccuracies or typographical errors. Symantec reserves the right to make changes without prior notice.

Copyright © 2007 Symantec Corporation. All rights reserved. Symantec, the Symantec Logo, Brightmail, DeepSight, Digital Immune System, and Symantec AntiVirus are trademarks or registered trademarks of Symantec Corporation or its affiliates in the U.S. and other countries. Apple, Mac OS, and Macintosh are registered trademarks of Apple Inc. Safari is a trademark of Apple Inc. IBM and DB2 are trademarks of International Business Machines Corporation in the United States, other countries, or both. Microsoft, ActiveX, MSN, PowerPoint, Visual Studio, Win32, Windows, and Windows Vista are either registered trademarks or trademarks of Microsoft Corporation in the United States and/or other countries. Sun and Solaris are trademarks or registered trademarks of Sun Microsystems, Inc., in the U.S. or other countries. Other names may be trademarks of their respective owners.

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

Copyright © 2007 Symantec Corporation. All rights reserved.
Any technical information that is made available by Symantec Corporation is the copyrighted work of Symantec Corporation and is owned by Symantec Corporation.
03/07 12078592