



# Symantec Internet Security Threat Report

March 2007

Regional Data Sheet—Latin America

## An important note about these statistics

The statistics discussed in this document are based on attacks against an extensive sample of Symantec customers. The attack activity was detected by the Symantec™ Global Intelligence Network, which includes Symantec™ Managed Security Services and Symantec DeepSight™ Threat Management System, between July 1 and December 31, 2006.

Symantec Managed Security Services and Symantec DeepSight Threat Management System use automated systems to map the IP address of the attacking system to identify the country in which it is located. However, because attackers frequently use compromised systems situated around the world to launch attacks remotely, the location of the attacking system may differ from the location of the attacker. Despite the uncertainty that this creates, this type of data is useful in creating a high-level profile of global attack patterns.

## Executive Summary

In addition to gathering Internet-wide attack data for the *Internet Security Threat Report*, Symantec also gathers and analyzes attack data that is detected by sensors deployed in specific regions. This regional data sheet will highlight the top attacks, top countries of attack origin, and top malicious code targeting computers in the Latin America region. It will also identify the Latin American countries and cities with the highest percentage of bot-infected computers and the top countries of origin for spam detected in the Latin America region.

The top attack detected by Latin America-based sensors in the last six months was the Generic TCP Segment Overwrite Attack, which accounted for 47 percent of detected attacks. This attack is often carried out to mask other attacks. It could allow an attacker to bypass some perimeter defenses such as network intrusion detection systems, potentially opening up the network to further attacks.

The most frequently reported malicious code sample from the Latin America region and worldwide in the last six months of 2006 was Mytob.AG. This is a mass-mailing worm that propagates by using social engineering to persuade a user to run its email attachment or by exploiting a remote vulnerability. Like other Mytob variants, Mytob.AG sends its email messages in English.

For the second half of 2006, Brazil had the highest percentage of bot-infected computers in the Latin America region, with 41 percent of the region's total. Argentina and Mexico had the second and third most bot-infected computers in the region, respectively. Buenos Aires, Argentina was the Latin America city with the most bot-infected computers.

## Latin America Data Sheet

The United States was the top country of origin for attacks detected by Latin America-based sensors, accounting for 47 percent of all detected attacks. This is likely due to the high level of general attack activity originating there: 33 percent of all Internet-wide attack activity originated in the United States in the second half of 2006. The United States continues to have more Internet users than any other country.

### Top Attacks

Current Rank	Attack	Percentage of Attackers in Region	Percentage of Attackers Worldwide
1	Generic TCP Segment Overwrite Attack	47%	11%
2	Generic SMTP Invalid Domain Name Attack	17%	11%
3	Generic TCP RST Flood Denial of Service Attack	9%	9%
4	Microsoft SQL Server 2000 Resolution Service Stack Overflow Attack	7%	1%
5	Generic TCP RST-ACK Flood Denial of Service Attack	5%	0%
6	Generic TCP Segment With Invalid Checksum Event	2%	4%
7	Generic HTTP CONNECT TCP Tunnel Attack	2%	0%
8	Generic ICMP Flood Attack	2%	1%
9	Generic TCP Hijacking Attack	2%	0%
10	Generic SMB Authentication Failure Event	1%	0%

**Table 1. Top attacks, Latin America region**

Source: Symantec Corporation

For the purposes of this data sheet, top attacks were determined by the percentage of total attackers performing each attack. The most common attack detected by sensors in the Latin America region in the last six months of 2006 was the Generic TCP Segment Overwrite Attack (table 1), which was used by 47 percent of attacking IP addresses.

This attack is often carried out to mask other attacks. The TCP protocol allows messages to be sent in segments over a network, reassembling them when they arrive at the destination. TCP allows for segments to be overwritten by other data during the reassembly process. By using data in one segment to overwrite data in a subsequent segment, it may be possible to hide attacks. This attack may allow an attacker to bypass some perimeter defenses such as network intrusion detection systems, potentially opening up the network to further attacks.

Organizations should ensure that intrusion detection systems that are able to identify and filter network traffic that behaves suspiciously are deployed. Flagging and filtering suspicious and potentially malicious data can greatly reduce the risk associated with this attack.

## Latin America Data Sheet

The second most common attack detected in the Latin America region in the second half of 2006 was the Generic SMTP Invalid Domain Name Attack, which was used by 17 percent of all detected attacking IP addresses. Detection of this attack is triggered when an attacker attempts to connect to an SMTP server with an invalid domain name.<sup>1</sup> This is likely the result of attackers attempting to manipulate email protocols, which is probably driven by spammers who are attempting to locate computers that can be used to deliver unsolicited email. This could result in unauthorized consumption of network bandwidth, which could lead to denial of service conditions. Organizations whose systems are identified as being used to send spam risk being placed on DNS block lists,<sup>2</sup> which may subsequently limit their end users' ability to send email successfully.

The third most prominent attack during the period was the Generic TCP RST Flood Denial of Service Attack. This attack occurs when an attacker sends an overwhelming number of RST or Reset packets to a remote system in an attempt to cause a denial of service condition. These packets are used to end a TCP/IP connection; however, they can be sent in sufficiently large numbers to saturate the bandwidth of a computer, thereby causing denial of service conditions.

A denial of service (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.

Organizations should ensure that a documented procedure exists for responding to DoS attacks. One of the best ways to mitigate the effects of a DoS attack is to filter upstream of the target. For most organizations, this filtering would involve contacting their Internet service provider. Symantec also recommends that organizations perform egress filtering on all outbound traffic.<sup>3</sup> Many firewall and operating systems have configuration parameters that can be changed to help mitigate the effect of a net flood attack. Organizations should ensure that all potential DoS targets are appropriately configured to minimize impact should an attack occur.

### Top Countries of Attack Origin

Current Rank	Country	Percentage of Attacks in Region	Percentage of Attacks Worldwide
1	United States	47%	33%
2	China	16%	11%
3	United Kingdom	14%	5%
4	Brazil	4%	1%
5	Germany	2%	7%
6	Mexico	2%	<1%
7	Spain	2%	4%
8	France	2%	6%
9	Canada	1%	5%
10	Netherlands	1%	1%

**Table 2. Top countries of origin of attacks targeting the Latin America region**

Source: Symantec Corporation

<sup>1</sup> Simple Mail Transfer Protocol. SMTP is designed to facilitate the delivery of email messages across the Internet.

<sup>2</sup> A DNS block list is a list of IP addresses that are known to send unwanted email traffic. The DNSBL is used by email software to either allow or reject email coming from IP addresses on the list.

<sup>3</sup> Egress traffic refers to traffic that is leaving a network, bound for the Internet or another network.

## Latin America Data Sheet

The United States was the top country of origin for attacks detected by Latin America-based sensors, accounting for 47 percent of all detected attacks (table 2). This is likely due to the high level of general attack activity originating there: 54 percent of all Internet-wide attack activity originated in the United States in the second half of 2006. The high degree of malicious activity originating in the United States is likely driven by the expansive Internet infrastructure there. The United States continues to have more Internet users than any other country.<sup>4</sup>

China was the country of origin of the second most attacks detected by sensors in the Latin America region, accounting for 16 percent of all attacking IP addresses. This is somewhat higher than the 11 percent of Internet-wide attacks that originated there during this period. This indicates that attack activity originating in China is targeting Latin America to some degree.

China had the highest number of bot-infected computers during this reporting period, but had only the fourth highest number of command-and-control servers. This indicates that many bot-infected computers in the country are being controlled by servers outside the country. Therefore, much of the attack activity originating in China that is targeting the LAM region may be instigated by attackers located outside the country, possibly within the LAM region itself.

The United Kingdom was the country of origin for the third most attacks targeting the Latin America region during this period, accounting for 14 percent of all attacking IP addresses. This is higher than the United Kingdom's worldwide proportion of five percent. This discrepancy likely means that some attacks originating in the United Kingdom are specifically targeting computers in the Latin America region. This may indicate that a number of attacking computers in the United Kingdom are being controlled by attackers in the Latin America region.

In the current volume of the *Internet Security Threat Report*, the distribution of bot-infected computers and bot command-and control-servers indicates that the majority of bot network computers are controlled by servers outside of the United Kingdom. Symantec has also observed that attackers often attack within their region using bot network computers based in other regions. Therefore, it is possible that computers in the United Kingdom that are targeting computers in Latin America are controlled by attackers in Latin America.

Only two of the top ten originating countries of attacks targeting Latin America, Mexico and Brazil, are located within the region itself. Four percent of attacks originated in Brazil, while two percent came from Mexico. Both of these figures are higher than the Internet-wide attack activity that originated in these countries, which was one percent for Brazil and less than one percent for Mexico. This would indicate that attack activity originating in these countries is specifically targeting the Latin America region. Their combined attack activity targeting the region accounts for only six percent of attacks detected by sensors within the region. This supports Symantec's assertion that attacks commonly originate from computers situated in the same region as the region of detection.

<sup>4</sup> <http://www.internetworldstats.com>

## Bot-Infected Computers by Country

Regional Rank	Country	Percentage of Regional Bots	Percentage of Worldwide Bots
1	Brazil	41%	3%
2	Argentina	14%	1%
3	Mexico	12%	1%
4	Chile	10%	1%
5	Peru	8%	1%
6	Colombia	3%	0%
7	Dominican Republic	2%	0%
8	Uruguay	2%	0%
9	Puerto Rico	2%	0%
10	Venezuela	1%	0%

**Table 3. Bot-infected computers by country, Latin America region**

Source: Symantec Corporation

Bot-infected computers operate in a coordinated fashion under the direction of an attacker and can number in the hundreds or thousands. These coordinated networks of computers can scan for and compromise additional computers and may be used to perform DoS attacks and to relay spam.

Recognizing the ongoing threat posed by bot networks, Symantec tracks the distribution of bot-infected computers both worldwide and across the Latin America 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 what percentage of these computers are located in each country in the Latin America region. The identification of bot-infected computers is important, as a high percentage could mean a greater potential for bot-related attacks. It may also indicate the level of patching and security awareness.

Between July 1 and December 31, 2006, Brazil was the location of the highest percentage of bot-infected computers in the region, 41 percent of the total were situated there. Brazil's prominence is likely due to its broadband penetration; it was a leader in the region in broadband infrastructure during this period.

Argentina had the second most bot-infected computers in the Latin America region with 14 percent of the total. Mexico had the third highest percentage, with 12 percent of the region's bot-infected computers. Other than Brazil, Argentina and Mexico lead the region in the number of broadband users, which likely explains their prominence in this metric.

To reduce exposure to bot-related attacks, end users should employ defense-in-depth strategies, including the deployment of antivirus software and a firewall.<sup>5</sup> 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 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.

<sup>5</sup> Defense-in-depth strategies emphasize multiple, overlapping, and mutually supportive defensive systems to guard against single-point failures in any specific technology or protection methodology. They should include the deployment of antivirus, firewalls, and intrusion detection systems, among other security measures.

### Bot-Infected Computers by City

Rank	City	Country	Percentage of Attacks in Region	Percentage of Attacks Worldwide
1	Buenos Aires	Argentina	17%	83%
2	Santiago	Chile	12%	79%
3	Lima	Peru	8%	93%
4	Sao Paulo	Brazil	7%	32%
5	Mexico City	Mexico	6%	51%
6	Rio de Janeiro	Brazil	5%	26%
7	Bogota	Colombia	5%	78%
8	San Juan	Puerto Rico	3%	90%
9	Santo Domingo	Dominican Republic	2%	100%
10	Valdivia	Chile	2%	14%

**Table 4. Bot-infected computers by city, Latin America region**

Source: Symantec Corporation

In addition to identifying top bot-infected countries, Symantec also tracks the distribution of bot-infected computers by city.<sup>6</sup> As with the previous metric, the identification of bot-infected computers is important, as a high percentage of infected machines likely indicates a greater potential for bot-related attacks. It could also give insight into the level of patching and security awareness amongst computer administrators and users in a given city.

Buenos Aires, Argentina was the city with the most active bot-infected computers detected within the region during the last half of 2006 (table 4), accounting for 17 percent of the total number of bots that are traceable back to specific cities. Santiago, Chile ranked second with 12 percent while Lima, Peru ranked third with eight percent.

All three cities also host the majority of the bots within their respective countries, which likely indicates that either Internet users or the Internet service providers are concentrated in these cities. To further support this distribution theory, while Brazil is the most infected country in Latin America, Sao Paulo, is only the fourth-ranked city, indicating that bot-infections in Brazil are not concentrated within its cities, but dispersed throughout the country. This may be because Brazil, unlike Argentina, Peru, and Chile, has numerous major metropolitan centers, such as Rio de Janeiro and Brasilia.

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.

<sup>6</sup> 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.

## Top Ten Malicious Code Samples

Regional Rank	Sample	Type	Propagation Vectors	Impact	Top Reporting Country
1	Mytob.AG	Worm	Worm, Back door, Remote vulnerability	Bot	Puerto Rico
2	Blackmal.E	Trojan	SMTP, File sharing	Overwrites files	Mexico
3	Netsky.P	Worm	SMTP, P2P	Keystroke logger targets www.e-gold.com	Mexico
4	Mytob.EU	Worm	Worm, Back door	Bot	Puerto Rico
5	Mydoom.L	Worm, Back door	SMTP, P2P	Bot	Colombia
6	Netsky.AD	Worm	SMTP, P2P	Portuguese email message	Brazil
7	Stration.DL	Worm	SMTP	Downloads and installs other threats	Mexico
8	Mytob.C	Worm, Back door	SMTP, Remote vulnerability	Bot	Colombia
9	Mytob.GA	Worm, Back door	SMTP	Bot	Mexico
10	Netsky.W	Worm, Back door	SMTP	Sends itself to email addresses on infected computer	Mexico

**Table 5. Top ten malicious code samples, Latin America region**

Source: Symantec Corporation

The most frequently reported malicious code sample from the Latin America region, and worldwide, in the last six months of 2006 was Mytob.AG (table 5).<sup>7</sup> Mytob.AG is a mass-mailing worm that propagates by using social engineering to persuade a user to run its email attachment or by exploiting a remote vulnerability. Like other Mytob variants, Mytob.AG sends its email messages in English.

Blackmal.E was the second most frequently reported malicious code sample from Latin America in the second half of 2006.<sup>8</sup> Also known as the Kama Sutra worm, this destructive worm attempts to delete all files on a compromised computer with certain extensions—such as .doc, .xls, and .pdf—on the third day of each month. The worm propagates by using a mass-mailing component and by copying itself to network shares on remote computers. The worm also attempts to disable antivirus and security applications on compromised computers.

The third most frequently reported malicious code sample in the Latin America region during this period was Netsky.P.<sup>9</sup> This Netsky variant, like previous versions, is a mass-mailing worm that uses its own SMTP engine to send itself to addresses it gathers from files on the compromised computer. It also attempts to copy itself to any folders on the computer that may be used for peer-to-peer file-sharing applications.

In order to prevent malicious code infection, it is crucial to employ best practices as recommended by Symantec.<sup>10</sup> 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 block or remove all email attachments and only allow file types that are required for business needs. Alternatively, other means can be used to transfer files such as file servers, FTP or SSH.

<sup>7</sup> [http://www.symantec.com/security\\_response/writeup.jsp?docid=2005-041009-4908-99](http://www.symantec.com/security_response/writeup.jsp?docid=2005-041009-4908-99)

<sup>8</sup> [http://www.symantec.com/security\\_response/writeup.jsp?docid=2006-011712-2537-99](http://www.symantec.com/security_response/writeup.jsp?docid=2006-011712-2537-99)

<sup>9</sup> [http://www.symantec.com/security\\_response/writeup.jsp?docid=2004-032110-4938-99](http://www.symantec.com/security_response/writeup.jsp?docid=2004-032110-4938-99)

<sup>10</sup> 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](http://eval.veritas.com/mktginfo/enterprise/white_papers/ent-whitepaper_symantec_internet_security_threat_report_ix.pdf) : p. 102

## Latin America Data Sheet

End users should employ defense-in-depth strategies, including antivirus software and a firewall. Antivirus definitions should be updated regularly. Users should also ensure that their system is updated with all necessary security patches from their operating system vendor. They should never view, open, or execute any email attachment unless the attachment is expected, comes from a known and trusted source and the purpose of the attachment is known. Organizations should also remind employees to never run software that has not been authorized by the organization.

### Spam

During the last six months of 2006, no countries from the Latin America region were present in the top ten spam originating countries worldwide. In this period, 44 percent of all spam detected worldwide originated in the United States. This is likely due to the high number of broadband users in that country and the high bot infection percentage, as is discussed in the "Attack Trends" section of the current edition of the Symantec *Internet Security Threat Report*. Since spammers most often use bots to send their bulk mailings, this correlation is not surprising.

Regional Rank	Country	Regional Percentage
1	Brazil	42%
2	Argentina	14%
3	Chile	11%
4	Mexico	9%
5	Peru	6%
6	Colombia	6%
7	Costa Rica	3%
8	Dominican Republic	3%
9	Venezuela	2%
10	Panama	1%

**Table 6. Top ten countries of spam origin, Latin America region**

Source: Symantec Corporation

During the second half of 2006, 42 percent of all spam detected from this region originated in Brazil (table 6). However, this country only contributed one percent of worldwide spam. Brazil was the highest ranked country in the region for bot-infected computers. Spammers often use bots to send their bulk mailings, so it is reasonable that Brazil would be the top country of spam origin in the region.

The second highest amount of spam detected in the Latin America region during this period originated in Argentina with 14 percent of the total, while Chile contributed the third highest percentage, with 11 percent of the region's spam, and Mexico contributed nine percent. After Brazil, these three countries lead the region in the number of broadband users, which likely explains their prominence in this metric.

## 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](http://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 Boulevard  
Cupertino, CA 95014 USA  
+1 (408) 517 8000  
1 (800) 721 3934  
[www.symantec.com](http://www.symantec.com)

Copyright © 2007 Symantec Corporation. All rights reserved. Symantec, the Symantec Logo, BindView, Enterprise Security Manager, Sygate, Veritas, Enterprise Vault, NetBackup and LiveState are trademarks or registered trademarks of Symantec Corporation or its affiliates in the U.S. and other countries. Other names may be trademarks of their respective owners.  
03/07 12114891