SYMANTEC ENTERPRISE SECURITY

Confidence in a connected world.

Symantec Internet Security Threat Report

April 2009

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, both of which 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.

Introduction

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

Symantec also gathers malicious code intelligence from more than 130 million client, server, and gateway systems that have deployed its antivirus products. Additionally, Symantec's distributed honeypot network collects data from around the globe, capturing previously unseen threats and attacks and providing valuable insight into attacker methods.

Spam data is captured through the Symantec Probe Network, a system of more than 2.5 million decoy email accounts, Symantec MessageLabs Intelligence, and other Symantec technologies in more than 86 countries from around the globe. Over eight billion email messages, as well as over one billion Web requests, are scanned per day across 16 data centers. Symantec also gathers phishing information through an extensive antifraud community of enterprises, security vendors, and more than 50 million consumers.

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

In addition to gathering Internet-wide attack data for the Symantec *Global Internet Security Threat Report*, Symantec also gathers and analyzes attack data that is detected by sensors deployed in specific regions. This regional data sheet will discuss notable aspects of malicious activity Symantec has observed in the Latin America (LAM) region for 2008.

Highlights

- Brazil was the top country for malicious activity in LAM during 2008, accounting for 34 percent of the total. Globally, Brazil ranked fifth, with 4 percent of the total for malicious activity by country.
- The United States was the top country of origin for attacks detected by LAM-based sensors in 2008, accounting for 58 percent of all detected attacks. The United States also maintained its top ranking for originating attacks against global targets in 2008, with 25 percent.
- Brazil was the top country for bot-infected computers in the LAM region for 2008, with 42 percent of the total; Brazil had 6 percent of the total of bot-infected computers globally.
- In 2008, the most frequently observed malicious code sample by potential infection in LAM was the Gammima.AG worm; this worm ranked seventh globally in 2008.
- In 2008, 29 percent of all spam detected in LAM originated in Brazil; globally, Brazil accounted for 4 percent of spam detected worldwide.

Malicious activity by country

This metric will assess the countries in LAM in which the highest amount of malicious activity took place or originated in 2008. To determine this, Symantec has compiled geographical data on numerous malicious activities, including bot-infected computers, phishing website hosts, malicious code reports, spam zombies, and attack origins. The rankings are determined by calculating the average of the proportion of these malicious activities that originated in each country.

Malicious activity usually affects computers that are connected to high-speed broadband Internet because these connections make attractive targets for attackers. Broadband connections provide larger bandwidth capacities than other connection types, faster speeds, the potential of constantly connected systems, and typically more stable connections. Symantec has also noted in the past that malicious activity in a country tends to increase in relation to growth in broadband infrastructure. One particular reason for this is because new users may be unaccustomed to, or unaware of, the increased risk of exposure to malicious attacks from such robust connections.

Each of the top three countries in this metric has a well developed and growing broadband infrastructure: Brazil experienced a growth of 27 percent in broadband subscribers between 2007 and 2008, and both Mexico and Argentina experienced a growth of over 40 percent during the same period.[1] Brazil has the most broadband subscribers in LAM, with 39 percent of the regional total, while Mexico and Argentina currently have 24 percent and 12 percent, respectively.[2]

Brazil was the top ranked country for malicious activity in LAM in 2008, making up 34 percent of the regional total (table 1). Globally, Brazil ranked fifth in this measurement, accounting for 4 percent of the worldwide total—an increase from 3 percent and eighth rank in 2007. Brazil ranked first in all of the considered malicious activities in the LAM region with the exception of malicious code, for which it ranked second.

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

2008 Rank	2007 Rank	Country	2008 Overall Percentage	2007 Overall Percentage	Malicious Code Rank	Spam Zombies Rank	Phishing Websites Host Rank	Bot Rank	Attack Origin Rank
1	1	Brazil	34%	31%	2	1	1	1	1
2	2	Mexico	17%	22%	1	5	4	5	2
3	3	Argentina	15%	13%	6	2	2	2	3
4	4	Chile	8%	8%	5	4	3	4	5
5	5	Colombia	7%	6%	3	3	5	6	4
6	6	Peru	4%	5%	8	6	8	3	7
7	7	Venezuela	3%	3%	4	9	6	10	6
8	8	Puerto Rico	2%	2%	7	10	10	8	8
9	9	Dominican Republic	1%	1%	12	7	18	7	10
10	10	Ecuador	1%	1%	9	18	7	19	14

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

Although it is the most populous country in the LAM region, Brazil's prominence in this metric may also be influenced by certain attacks originating in that country during 2008. In August 2008, it is alleged that attacks on a micro-blogging site originated in Brazil.[3] In this particular attack, a fake user profile was created on the site, which was used to display a link to a video. When followed, the link actually redirected users to download malicious code masquerading as a video player. The malicious code was a banking Trojan designed to steal online banking credentials. Also, a popular social networking site—the majority of whose members are in Brazil—was the target of attack of the Bancorkut worm, which downloads malicious files and then attempts to steal login credentials and email addresses from users' accounts.[4]

Mexico ranked second in LAM for malicious activity in 2008, accounting for 17 percent of the regional total, while Argentina ranked third, accounting for 15 percent. Globally, Mexico ranked seventeenth with 2 percent of the total and Argentina ranked eighteenth accounting for 1 percent. One reason for the high rankings of these countries may be due to the Downadup worm, discovered at the end of 2008.[5] The top five countries in this metric also ranked in the top 10 countries most affected by the Downadup worm during its initial spread. These five countries accounted for 27 percent of the global infection rate of Downadup in 2008.[6]

[3] http://news.bbc.co.uk/1/hi/technology/7543014.stm
[4] http://www.symantec.com/security_response/writeup.jsp?docid=2008-032608-3206-99
[5] http://www.symantec.com/security_response/writeup.jsp?docid=2008-112203-2408-99
[6] https://forums2.symantec.com/t5/Malicious-Code/Downadup-Geo-location-Fingerprinting-and-Piracy/ba-p/380993

Top countries of attack origin

This discussion measures countries as the originating sources of attacks targeting LAM. An attack is generally considered to be any malicious activity carried out over a network that has been detected by an intrusion detection system (IDS) or firewall. In 2008, the United States was the top country of origin for attacks on LAM detected by Symantec sensors based in the region, accounting for 58 percent of all detected attacks (table 2). This result is likely due to the high level of attack activity originating in the United States generally, as it was also the top country of origin for attacks against global targets, with 25 percent of that total in 2008.

Rank	Country	LAM Percentage	Global Percentage
1	United States	58%	25%
2	China	8%	13%
3	Chile	3%	1%
4	Argentina	3%	1%
5	Brazil	3%	3%
6	Spain	2%	3%
7	Canada	2%	3%
8	Netherlands	1%	1%
9	United Kingdom	1%	6%
10	Colombia	1%	1%

Table 2. Top countries of attack origin targeting LAM
Source: Symantec

As mentioned previously, malicious activity is most often associated with computers that are connected to high-speed broadband Internet; the United States ranked second worldwide for broadband subscribers in 2008, behind only China, which ranked second as the country of origin for attacks targeting LAM, accounting for 8 percent of all attacks in 2008.[7]

Of the top 10 originating countries of attacks targeting LAM, only four are located in the region itself. Of these, Chile, Argentina, and Brazil ranked third, fourth, and fifth in this measurement, respectively, with 3 percent of the total each, while Colombia ranked tenth, with 1 percent. The regional percentages for Chile and Argentina were higher than the global percentages, indicating that attacks from these countries may be targeting the LAM region specifically. Symantec has noted that attacks often target the region in which they originate due to proximity, shared language, or often similar social and cultural interests.[8]

[7] http://www.websiteoptimization.com/bw/0812/
[8] http://eval.symantec.com/mktginfo/enterprise/white_papers/ent-whitepaper_symantec_internet_security_threat_report_v.pdf : p. 11

Top bot-infected computers by country

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

Recognizing the ongoing threat posed by botnets, Symantec tracks the distribution of bot-infected computers both worldwide and regionally. For regions, Symantec calculates the number of computers worldwide that are known to be infected with bots, and then assesses which countries within a region are home to high percentages of bot-infected computers. A high percentage of infected machines could mean a greater potential for bot-related attacks, as well as indicating the level of patching and security awareness in the region.

In 2008, the LAM region accounted for 13 percent of the total bot-infected computers detected globally. Within the region, Brazil had the highest percentage of bot-infected computers, with 42 percent of the total (table 3). Globally, Brazil had 6 percent of the total. Argentina ranked second in 2008 for bot-infected computers in LAM, with 17 percent of the total, and Peru ranked third, with 10 percent.

While the high ranking of these countries is most likely due to their proportionally high number of broadband subscribers in the region, Symantec data also shows that the global percentage for spam originating in LAM doubled in 2008, from 2 percent to 4 percent.[9] Bot-infected computers are often associated with spam because they can be programmed to automatically send out a large amount of email. The reason for the percentage increase in these countries may be due to events surrounding the shutdown of a U.S.-based ISP that was alleged to be hosting bot command-and-control servers for several major botnets.[10] Following the takedown of this ISP toward the end of 2008, several botnets were briefly rendered inoperable and global spam levels dropped dramatically. Although global spam levels had returned to previous levels by the end of the year, the drop in spam generation elsewhere may explain the percentage increase in LAM.

LAM Rank	Global Rank	Country	LAM Percentage	Global Percentage
1	5	Brazil	42%	6%
2	12	Argentina	17%	2%
3	18	Peru	10%	1%
4	19	Chile	9%	1%
5	21	Mexico	7%	1%
6	29	Colombia	4%	1%
7	35	Dominican Republic	3%	<1%
8	42	Puerto Rico	2%	<1%
9	55	Uruguay	1%	<1%
10	57	Venezuela	1%	<1%

Table 3. Bot-infected computers by country, LAM
Source: Symantec

[9] http://www.point-topic.com
[10] http://eval.symantec.com/mktginfo/enterprise/other_resources/b-state_of_spam_report_02-2009.en-us.pdf : p. 7

To reduce exposure to bot-related attacks, end users should employ defense-in-depth strategies, including the deployment of antivirus software and a personal firewall.[11] 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.

Top malicious code samples

The most common malicious code sample by potential infections in LAM in 2008 was the Gammima.AG worm (table 4).[12] This worm was ranked seventh globally. Gammima.AG propagates by copying itself to removable media storage devices, such as USB drives and portable audio players. The Gammima.AG worm also steals account credentials for popular online games, and it is one of three top 10 malicious code samples in LAM to do so.

Rank	Sample	Type	Infection Vector(s)	Top Ranked Country	Second Ranked Country	Impact
1	Gammima.AG	Worm, virus	Removable drives	Mexico	Brazil	Steals online game account credentials
2	SillyFDC	Worm	Mapped, removable drives	Mexico	Brazil	Downloads and installs additional threats
3	Rontokbro	Worm	SMTP	Mexico	Chile	Performs DoS attacks
4	Gampass	Trojan	N/A	Mexico	Brazil	Steals online game account credentials
5	SillyDC	Worm	Removable drives	Mexico	Colombia	Downloads and installs additional threats
6	Wimad	Trojan	N/A	Mexico	Brazil	Exploits DRM technology to download additional threats
7	Vundo	Trojan, back door	N/A	Mexico	Brazil	Displays advertisements, and downloads and installs additional threats
8	Gammima	Worm, virus	Removable drives	Mexico	Brazil	Steals online game account credentials
9	Rontokbro.K	Worm	SMTP	Mexico	Colombia	Performs DoS attacks
10	Runauto	Worm	Mapped, removable drives	Mexico	Brazil	Modifies registries to display offensive text in browser windows

Table 4. Top malicious code samples, LAM
Source: Symantec

The second ranked malicious code sample causing potential infections in LAM during 2008 was the SillyFDC worm.[13] As with Gammima.AG, SillyFDC propagates by copying itself to any removable media storage devices attached to the compromised computer. Once the worm is installed on a computer it also attempts to download and install additional threats onto the computer.

[11] Defense-in-depth emphasizes multiple, overlapping, and mutually supportive defensive systems to guard against single-point failures in any specific technology or protection methodology.
[12] http://www.symantec.com/security_response/writeup.jsp?docid=2007-082706-1742-99&tabid=1
[13] http://www.symantec.com/security_response/writeup.jsp?docid=2006-071111-0646-99

The third most frequently reported malicious code sample causing potential infections in LAM during this period was the Rontokbro worm.[14] This worm ranked first in LAM during 2007; it was also one of the top 10 malicious code samples globally in both 2007 and 2008. Rontokbro is mass-mailing worm that gathers email addresses from certain files on compromised computers and then sends copies of itself as an email attachment to those addresses. The worm can also be instructed to launch denial-of-service (DoS) attacks against websites, which can negatively affect network performance on the compromised computer.

Symantec recommends that certain best security practices always be followed to protect against malicious code infection. Administrators should keep patch levels up to date, especially on computers that host public services and applications (such as HTTP, FTP, SMTP, and DNS servers) and which are accessible through a firewall or placed in a DMZ.[15] Email servers should be configured to only allow file attachment types that are required for business needs and to block email that appears to come from within the company, but that actually originates from external sources. Additionally, Symantec recommends that ingress and egress filtering be put in place on perimeter devices to prevent unwanted activity. To protect against malicious code that installs itself through a Web browser, additional measures should be taken. The use of intrusion prevention system (IPS) technologies can prevent the exploitation of browser and plug-in vulnerabilities through signatures and behavior-based detection, in addition to ASLR.[16]

End users should employ defense-in-depth strategies, including the deployment of antivirus software and a personal firewall. Users should update antivirus definitions regularly. They should also ensure that all desktop, laptop, and server computers are updated with all necessary security patches from their software vendors. They should never view, open, or execute any email attachment unless it is expected and comes from a trusted source, and unless the purpose of the attachment is known.

[14] http://www.symantec.com/security_response/writeup.jsp?docid=2005-092311-2608-99
[15] A demilitarized zone (DMZ) is an area within a network that purposely does not have any protection, such as a firewall or port trigger. It also limits access to protected computers on the network.
[16] Address space layout randomization is a security measure used to complicate exploitation of some classes of vulnerabilities by randomizing the layout of process address space to make it less predictable to attackers.

Top countries of spam origin

This section will discuss the top 10 countries of spam origin. The nature of spam and its distribution on the Internet presents challenges in identifying the location of people who are sending it because many spammers try to redirect attention away from their location. As such, the region in which the spam originates may not correspond with the region in which the spammers are located.

In 2008, 12 percent of all spam detected worldwide originated in LAM. On a country basis, Brazil ranked fifth globally and first regionally, which represents 4 percent of the global total and 29 percent of the regional total (table 5). Aside from the fact that Brazil is by far the most populous country in LAM with the most broadband subscribers, the high rate of regional spam from Brazil is likely due to its first-place ranking in both LAM and globally in 2008 for spam zombies. Spam zombies are used to send bulk spam, and Brazil was host to 9 percent of the worldwide total in 2008.

Rank	Country	LAM Percentage	Global Percentage
1	Brazil	29%	4%
2	Argentina	15%	2%
3	Colombia	12%	1%
4	Chile	9%	1%
5	Peru	9%	1%
6	Mexico	6%	1%
7	Bolivia	3%	<1%
8	Dominica	3%	<1%
9	Venezuela	2%	<1%
10	Dominican Republic	2%	<1%

Table 5. Top countries of spam origin, LAM
Source: Symantec

Argentina ranked second for originating spam in the LAM region in 2008, with 15 percent of the total, and Colombia ranked third, with 12 percent. As with Brazil, the prominence of these two countries is likely due to their high ranking for spam zombies in the region, since they ranked second and third in this measurement, respectively.

About Symantec

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

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

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

04/09 20016952