



SYMANTEC ISTR XI

Informe sobre Amenazas a la Seguridad en Internet América Latina

Marzo 2007

NOTA IMPORTANTE SOBRE ESTAS ESTADÍSTICAS

Las estadísticas presentadas en este documento se basan en los ataques dirigidos a una amplia muestra de clientes de Symantec. La actividad de ataques fue detectada por Symantec™ Global Intelligence Network, que incluye Symantec™ Managed Security Services y Symantec DeepSight™ Threat Management System, entre el 1 de julio y el 31 de diciembre de 2006.

Symantec Managed Security Services y Symantec DeepSight Threat Management System utilizan sistemas automatizados para detectar la dirección IP del sistema atacante e identificar el país en donde está ubicada. Sin embargo, puesto que los atacantes frecuentemente utilizan sistemas infectados situados alrededor del mundo para lanzar los ataques de forma remota, la ubicación del sistema atacante puede diferir de la ubicación del atacante. A pesar de la incertidumbre que esta situación genera, este tipo de datos es útil en la creación de un perfil de alto nivel de los patrones globales de ataque.

Resumen Ejecutivo

Además de recolectar los datos sobre ataques importantes en Internet en el *Informe sobre Amenazas a la Seguridad en Internet*, Symantec también recopila y analiza los datos de los ataques detectados por los sensores que están distribuidos en regiones específicas. Esta hoja de datos regional destacará los principales ataques, los países donde se originan más ataques y los códigos maliciosos más peligrosos que atacan las computadoras en la región de América Latina. También identificará los países con el más alto porcentaje de computadoras infectadas con programas bot y los países - que se ha detectado- originan más spam en la región.

El mayor ataque detectado por los sensores de América Latina en los últimos seis meses fue el Ataque Genérico de Sobre escritura del Segmento TCP, que representó el 47% de los ataques identificados. Este ataque generalmente se realiza para ocultar otros y podría permitir a un atacante burlar defensas en el perímetro como los sistemas de detección de intrusos de red, además de abrir potencialmente la red a más ataques.

La muestra de códigos maliciosos que se reportó con más frecuencia en la región de América Latina y a nivel mundial en los últimos seis meses del 2006 fue Mytob.AG. Este es un gusano mass-mailer que se propaga utilizando la ingeniería social al persuadir al usuario para que ejecute el archivo adjunto de correo electrónico o al explotar una vulnerabilidad remota. Al igual que otras variantes de Mytob, Mytob.AG envía sus mensajes de correo electrónico en inglés.

En el segundo semestre de 2006, Brasil obtuvo el mayor porcentaje de computadoras infectadas con programas bot en América Latina, con un 41% del total regional, mientras que Argentina y México ocuparon el segundo y tercer puesto respectivamente. Buenos Aires en Argentina fue la ciudad con la mayor cantidad de computadoras infectadas por programas bot en América Latina.

Estados Unidos fue el país que originó más ataques detectados por los sensores de América Latina, con un 47% de toda la muestra. Esto probablemente se debe al alto nivel de actividad general de ataques que se origina en dicho país: en el segundo semestre de 2006, 33% de la actividad total de los ataques en Internet se originó en los Estados Unidos, país que tiene el mayor número de usuarios de Internet en el mundo.

Principales Ataques

Posición	Ataque	Porcentaje de atacantes en la región	Porcentaje mundial de atacantes
1	Ataque genérico de sobreescritura del Segmento TCP	47%	11%
2	Ataque genérico SMTP de nombre de dominio inválido	17%	11%
3	Ataque genérico TCP RST de negación de servicio por inundación	9%	9%
4	Ataque de desbordamiento de stack de servicio de resolución de Microsoft SQL Server 2000	7%	1%
5	Ataque TCP RST-ACK genérico de negación de servicio por inundación	5%	0%
6	Segmento genérico TCP con evento inválido de suma de verificación	2%	4%
7	Ataque genérico http por túnel de conexión TCP	2%	0%
8	Ataque genérico por inundación ICMP	2%	1%
9	Ataque TCP genérico de raptó de conexiones	2%	0%
10	Evento genérico de error de autenticación de SMB	1%	0%

Tabla 1. Principales ataques en la región de América Latina Fuente: Symantec Corporation

Para los propósitos de este documento, los principales ataques fueron determinados por el porcentaje total de atacantes que realizan cada ataque. El ataque más frecuente, detectado por los sensores en la región de América Latina durante los últimos seis meses de 2006 fue el Ataque genérico de sobreescritura del segmento TCP (Tabla 1), utilizado por el 47% de las direcciones IP atacantes.

Este ataque frecuentemente se realiza para ocultar otros ataques. El protocolo TCP permite enviar mensajes por una red en segmentos y los reensambla cuando llegan al destino. TCP permite que otros datos sobrescriban los segmentos durante el proceso de reensamble. Al utilizar información en un segmento para sobrescribir los datos en un segmento posterior se pueden ocultar los ataques. Así, este ataque permite a un atacante burlar las defensas en el perímetro como los sistemas de detección de intrusos en la red y abrir ésta a más ataques potenciales.

Por ello, las organizaciones deben garantizar que sistemas de detección de intrusos que identifiquen y filtren el tráfico de la red que se comporta de forma sospechosa sean instalados. Marcar y filtrar los datos sospechosos y potencialmente maliciosos, puede reducir en gran medida el riesgo asociado con este ataque.

El segundo ataque más común detectado en América Latina en el segundo semestre de 2006 fue el Ataque genérico SMTP de nombre de dominio inválido, que fue utilizado por 17% de todas las direcciones IP atacantes detectadas. La detección de este ataque se activa cuando un atacante intenta conectarse a un servidor SMTP con un nombre de dominio inválido.¹ Esto es resultado de la actividad de los atacantes que intentan manipular los protocolos de correo electrónico, lo cual puede ser originado por spammers que intentan localizar computadoras para enviar correo electrónico no solicitado. Esto podría generar el uso no autorizado del ancho de banda de la red y producir condiciones de negación de servicio. Las organizaciones,

¹ SMTP es Simple Mail Transfer Protocol, o bien, Protocolo Sencillo de Transferencia de Correo. SMTP está diseñado para facilitar la entrega de mensajes de correo electrónico en Internet.

cuyos sistemas son utilizados para enviar spam, corren el riesgo de aparecer en listas de bloqueo DNS², lo que posteriormente podría limitar la capacidad de los usuarios para enviar correos de forma exitosa.

El tercer ataque más destacado durante el periodo fue el Ataque genérico TCP RST de negación de servicio por inundación, el cual sucede cuando un atacante envía una cantidad abrumadora de paquetes RST o Reset a un sistema remoto con el fin de producir una condición de negación de servicio. Estos paquetes se utilizan para terminar una conexión TCP/IP; sin embargo, se pueden enviar en cantidades lo suficientemente grandes para saturar el ancho de banda de una computadora y, como consecuencia, causar condiciones de negación de servicio.

Un ataque de Negación de Servicio (DoS, por sus siglas en inglés) puede volver inaccesibles los sitios Web u otros servicios de red para los clientes y empleados. Esto también puede interrumpir las comunicaciones empresariales, e incluso, generar una pérdida importante de ingresos y/o perjuicios a la reputación de la organización.

Las organizaciones deben garantizar la existencia de un procedimiento documentado para responder a los ataques de DoS. Una de las mejores formas de mitigar los efectos de un ataque DoS es filtrar el flujo del ataque. Para la mayoría de organizaciones, este filtrado implica contactar su proveedor de servicio de Internet.

Symantec recomienda a las organizaciones realizar filtrado del tráfico saliente.³ Muchos sistemas operativos y firewalls tienen parámetros de configuración que se pueden cambiar para ayudar a mitigar el efecto de un ataque net flood. Las organizaciones deben asegurarse de que todos los sistemas que puedan ser blancos potenciales de ataques DoS estén debidamente configurados para minimizar el impacto si ocurriera un ataque.

Principales Países Donde se Originan los Ataques

Posición actual	País	Porcentaje de ataques en la región	Porcentaje de ataques mundiales
1	Estados Unidos	47%	33%
2	China	16%	11%
3	Reino Unido	14%	5%
4	Brasil	4%	1%
5	Alemania	2%	7%
6	México	2%	<1%
7	España	2%	4%
8	Francia	2%	6%
9	Canadá	1%	5%
10	Países Bajos	1%	1%

Tabla 2. Países que originan más ataques dirigidos a América Latina

Fuente: Symantec Corporation

² Una lista de bloqueo DNS es una lista de direcciones IP que envía tráfico de correo electrónico no deseado. La lista DNSBL es utilizada por software de correo electrónico para autorizar o rechazar el correo electrónico que proviene de las direcciones IP de la lista.

³ El tráfico de egreso hace referencia al tráfico que sale de la red, con destino a Internet o a otra red.

Estados Unidos fue el país que originó más ataques detectados por los sensores de América Latina, con un 47% del total de ataques detectados (tabla 2).

Probablemente esto se debe al alto nivel de actividad general de la actividad de ataques que ahí se origina: 54% de toda la actividad de ataques en Internet se originó en los Estados Unidos en el segundo semestre de 2006. El alto nivel de actividad maliciosa que se originó en este país es posiblemente es ocasionado por su expansiva infraestructura de Internet. Así, Estados Unidos sigue teniendo el mayor número de usuarios de Internet en el mundo.⁴

China fue el segundo país de origen de ataques detectados por los sensores en América Latina, con 16% de todas las direcciones IP atacantes detectadas. Esto es un poco más que el 11% de los ataques de Internet que se originaron ahí en este periodo. Esto indica que la actividad de ataques que se origina en China en cierto grado está dirigida a América Latina.

China tuvo el número más alto de computadoras infectadas por bots durante este periodo, pero tuvo solo la cuarta posición en lo que se refiere al manejo y control de servidores. Esto indica que muchas computadoras en dicho país están siendo controladas por servidores fuera de éste. Por lo tanto, mucha de la actividad que se origina en China y que está dirigida a LAM puede ser instigada por atacantes localizados fuera del país y posiblemente en la misma región de LAM.

Reino Unido fue el tercer país que originó más ataques dirigidos a América Latina durante este periodo, con 14 % de todas las direcciones IP atacantes. Este es un porcentaje mundial superior a la proporción mundial del Reino Unido de 5%. La discrepancia parece indicar que algunos ataques que se originan en el Reino Unido están dirigidos específicamente a computadoras de América Latina. Esto también podría indicar que una cantidad de computadoras atacantes en el Reino Unido son controladas por atacantes en América Latina.

En este volumen del *Informe sobre Amenazas a la Seguridad en Internet*, la distribución de computadoras infectadas con programas bot y servidores de mando y control de redes bot indica que la mayoría de equipos en red son controlados por servidores que están fuera del Reino Unido. Symantec también ha observado que los atacantes generalmente atacan a su región, usando computadoras basadas en otras regiones. Por lo tanto, es posible que las computadoras en el Reino Unido que están atacando computadoras de América Latina sean controladas por atacantes de América Latina.

Sólo dos de los diez países que originan más ataques dirigidos a América Latina, México, y Brasil, están ubicados en la región. El 4% de los ataques se originó en Brasil mientras que 2% vino de México. Estas dos cifras son superiores a la actividad de ataques en Internet que se originó en estos países y que correspondió a 1% en Brasil y menos del 1% en México. Esto podría indicar que la actividad de ataques que se originó en estos países está dirigida específicamente a la región de América Latina. La actividad de ataques combinados dirigida a la región representa únicamente 6% de los ataques detectados por los sensores de la región. Lo anterior sustenta la

⁴ <http://www.internetworldstats.com>

teoría de Symantec de que los ataques se originan generalmente en equipos ubicados en la misma región de la zona de detección.

Computadoras por País Infechadas con Bots

Posición Regional	País	Porcentaje regional de programas bot	Porcentaje mundial de programas bot
1	Brasil	41%	3%
2	Argentina	14%	1%
3	México	12%	1%
4	Chile	10%	1%
5	Perú	8%	1%
6	Colombia	3%	0%
7	República Dominicana	2%	0%
8	Uruguay	2%	0%
9	Puerto Rico	2%	0%
10	Venezuela	1%	0%

Tabla 3. Equipos infectados con programas bot por país, América Latina

Fuente: Symantec Corporation

Las computadoras infectadas con programas bot funcionan de forma coordinada bajo la dirección de un atacante y pueden ser cientos o miles. Estas redes coordinadas de computadoras pueden explorar y atacar otros equipos que pueden ser utilizados para lanzar ataques de negación de servicio y transmitir spam.

Al reconocer la continua amenaza que representan las redes bot, Symantec rastrea la distribución de computadoras infectadas con programas bot tanto a nivel mundial como en América Latina (Tabla 3). Para ello, calcula la cantidad de computadoras en el mundo que -se sabe- están infectadas con programas bot y evalúa qué porcentaje de estas computadoras están ubicadas en cada país de América Latina. La identificación de computadoras infectas por bots es importante puesto que un alto porcentaje de máquinas infectadas podría significar una mayor posibilidad de lanzar ataques relacionados con bots y también podría indicar el nivel de conocimiento sobre el uso de parches y seguridad.

Entre el 1 de julio y el 31 de diciembre de 2006, Brasil fue el país que tuvo el porcentaje más alto de computadoras infectadas con programas bot en la región, con 41% del total. El predominio de Brasil se debe probablemente a la penetración de banda ancha; fue el líder en la región en infraestructura de banda ancha durante este periodo.

Por su parte, Argentina representó el segundo país de la región con más computadoras infectadas con bots, con 14% del total, mientras que México obtuvo el tercer porcentaje más alto de la región con 12%. A diferencia de Brasil, Argentina y México tienen la mayor cantidad de usuarios de banda ancha en la región, lo que explica su relevancia en este aspecto.

Para reducir la exposición a los ataques relacionados con bots, los usuarios finales deben emplear estrategias de defensa profunda, incluyendo la instalación de software antivirus y firewall⁵ Los usuarios también deben actualizar las definiciones

⁵ La protección profunda enfatiza múltiples sistemas de protección que se superponen y apoyan mutuamente para protegerse de las fallas puntuales de una tecnología o metodología de protección

de antivirus regularmente y asegurarse que las computadoras de escritorio, los equipos portátiles y los servidores estén actualizados con los parches de seguridad necesarios de su proveedor de sistema operativo. Symantec aconseja a los usuarios que nunca vean, abran o ejecuten los archivos adjuntos de correo electrónico a menos que estén esperando un archivo, que provenga de una fuente confiable y que conozcan el propósito del mismo.

Computadoras por Ciudad Infectadas con Bots

Posición	Ciudad	País	Porcentaje de ataques en la región	Porcentaje mundial de ataques
1	Buenos Aires	Argentina	17%	83%
2	Santiago	Chile	12%	79%
3	Lima	Perú	8%	93%
4	Sao Paulo	Brasil	7%	32%
5	Ciudad de México	México	6%	51%
6	Río de Janeiro	Brasil	5%	26%
7	Bogotá	Colombia	5%	78%
8	San Juan	Puerto Rico	3%	90%
9	Santo Domingo	República Dominicana	2%	100%
10	Valdivia	Chile	2%	14%

Tabla 4. Equipos infectados con bots por ciudad, América Latina

Fuente: Symantec Corporation

Además de identificar los países más infectados con programas bot, Symantec también rastrea la distribución de las computadoras infectadas con programas bot por ciudad⁶. Así como la anterior métrica, la identificación de computadoras infectadas con programas bot es importante puesto que un alto porcentaje de máquinas infectadas parece indicar un mayor potencial de ataques relacionados con bots. También podría brindar una perspectiva sobre el conocimiento que tienen los administradores y usuarios informáticos de una ciudad determinada en relación a la importancia de protegerse con parches.

Buenos Aires, Argentina, fue la ciudad donde se detectaron más computadoras activas infectadas con bots en la región durante el segundo semestre de 2006 (Tabla 4), con un 17% del total de bots que se rastrearon en ciudades específicas. Santiago, Chile, ocupó el segundo lugar con 12% mientras que Lima, Perú, fue el tercer lugar con 8%.

Las tres ciudades también alojan la mayoría de bots en sus respectivos países, lo que probablemente indica que los usuarios de Internet o los proveedores de servicio de Internet están concentrados en estas ciudades. Lo que sustenta más esta teoría de distribución, es el hecho de que aunque Brasil es el país más infectado de América Latina, Sao Paulo es la cuarta ciudad, lo que indica que las infecciones de programas

específica. La protección en profundidad también debe incluir la instalación de un antivirus, firewalls y sistemas de detección de intrusos, entre otras medidas de seguridad.

⁶ Cabe decir que este análisis se limita a los bots que pueden ubicarse en una ciudad particular con un nivel de confianza de cuatro de cinco puntos. Si no se obtiene dicha calificación, los datos no se incorporarán en el análisis.

bot en Brasil no están concentradas en sus ciudades, sino dispersas por el país. Esto puede ser porque, a diferencia de Argentina, Perú y Chile, Brasil tiene grandes centros metropolitanos, como Río de Janeiro y Brasilia.

Para evitar la infección por bots, Symantec recomienda a los usuarios finales practicar estrategias de protección a profundidad, como la instalación de antivirus, firewall y soluciones de detección de intrusos. Los administradores de seguridad también deben garantizar que se implemente el filtrado de ingresos y egresos para bloquear el tráfico conocido de redes bot y actualizar las definiciones de antivirus con regularidad.

Las Diez Muestras Más Importantes de Códigos Maliciosos

Posición Regional	Muestra	Tipo	Vectores de propagación	Impacto	País que envía más muestras
1	Mytob.AG	Gusano	Gusano, back door, vulnerabilidad remota	Bot	Puerto Rico
2	Blackmal.E	Troyano	Uso compartido de archivos, SMTP	Sobreescribe archivos	México
3	Netsky.P	Gusano	SMTP, P2P	Keylogger ataca www.e-gold.com	México
4	Mytob.EU	Gusano	Gusano, puerta trasera	Bot	Puerto Rico
5	Mydoom.L	Gusano, puerta trasera	SMTP, P2P	Bot	Colombia
6	Netsky.AD	Gusano	SMTP, P2P	Mensaje de correo electrónico portugués	Brasil
7	Stration.DL	Gusano	SMTP	Descarga e instala otras amenazas	México
8	Mytob.C	Gusano, back door	Vulnerabilidad remota, SMTP	Bot	Colombia
9	Mytob.GA	Gusano, back door	SMTP	Bot	México
10	Netsky.W	Gusano, back door	SMTP	Se reenvía a direcciones de correo en la computadora infectada	México

Tabla 5. Muestras de códigos más importantes en América Latina

Fuente: Symantec Corporation

La muestra de códigos maliciosos de América Latina y a nivel mundial que se reportó con más frecuencia en los últimos seis meses de 2006 fue Mytob.AG. (Tabla 5)⁷.

Mytob.AG es un gusano *mass-mailing* que se propaga mediante ingeniería social al persuadir al usuario para que ejecute el archivo adjunto al correo electrónico o aprovecha una vulnerabilidad remota. Al igual que otras variantes de Mytob, Mytob.AG envía sus mensajes de correo electrónico en inglés.

⁷ http://www.symantec.com/security_response/writeup.jsp?docid=2005-041009-4908-99

Blackmal.E⁸ fue la segunda muestra de código malicioso reportada más frecuentemente en América Latina durante el segundo semestre de 2006. También conocido como el gusano Kama Sutra, este gusano destructivo intenta borrar todos los archivos de la computadora atacada con ciertas extensiones, como .doc, .xls y .pdf el tercer día de cada mes. El gusano se propaga usando un componente *mass-mailing* y copiándose en recursos compartidos de red en equipos remotos. El gusano también intenta deshabilitar las aplicaciones antivirus y de seguridad en los equipos atacados.

La tercera muestra de código malicioso más frecuentemente reportada en la región durante este periodo fue Netsky.P⁹. Esta variante de Netsky, al igual que las versiones anteriores, es un gusano *mass-mailing* que utiliza su propio motor SMTP para autoenviarse a las direcciones que recolecta de los archivos del equipo atacado. También intenta autocopiarse a las carpetas de la computadora que pueden ser utilizadas para aplicaciones de archivos compartidos peer-to-peer.

Para evitar la infección de códigos maliciosos, es crucial emplear mejores prácticas como lo recomienda Symantec¹⁰. Los administradores deben actualizar los parches, especialmente en las computadoras que alojan servicios públicos - como los servidores HTTP, FTP, SMTP y DNS - y a las que se tiene acceso a través de un firewall o que están ubicadas en una zona DMZ. Se deben configurar los servidores de correo electrónico para bloquear o eliminar todos los archivos adjuntos del correo electrónico y permitir únicamente los archivos que se requieren para las necesidades de la organización. También se pueden usar otros medios para la transferencia de archivos como los servidores de archivos, FTP o SSH.

Los usuarios finales deben emplear estrategias de protección profunda incluyendo software antivirus y firewall. Asimismo, las definiciones antivirus se deben actualizar periódicamente. Los usuarios también deben garantizar que su sistema esté actualizado con todos los parches de seguridad necesarios de su proveedor de sistema operativo. Nunca deben ver, abrir o ejecutar los archivos adjuntos del correo electrónico a menos que estén esperando el archivo adjunto, que este provenga de una fuente confiable y que conozcan el propósito del mismo. Por su parte, las organizaciones deben recordar a sus empleados que nunca deben ejecutar software que no esté autorizado por la organización.

Spam

En los últimos seis meses de 2006, ningún país de América Latina encabezó la lista a nivel mundial de los diez países que originaron más correo basura. En este periodo, 44% de todo el spam detectado en el mundo se originó en Estados Unidos. Probablemente esto se debe a la gran cantidad de usuarios de banda ancha en ese país y el alto porcentaje de infección con bots. Dado que los spammers con

⁸ http://www.symantec.com/security_response/writeup.jsp?docid=2006-011712-2537-99

⁹ http://www.symantec.com/security_response/writeup.jsp?docid=2004-032110-4938-99

¹⁰ *Informe sobre Amenazas a la Seguridad en Internet de Symantec, Volumen IX (marzo de 2006)*
http://eval.veritas.com/mktginfo/enterprise/white_papers/ent-whitepaper_symantec_internet_security_threat_report_ix.pdf : p. 102

frecuencia utilizan redes bot para enviar sus correos masivos, esta correlación no es sorprendente.

Posición Regional	País	Porcentaje regional
1	Brasil	42%
2	Argentina	14%
3	Chile	11%
4	México	9%
5	Perú	6%
6	Colombia	6%
7	Costa Rica	3%
8	República Dominicana	3%
9	Venezuela	2%
10	Panamá	1%

Tabla 6. Los diez países que más producen spam en América Latina

Fuente: Symantec Corporation

En el segundo semestre de 2006, el 42% del spam detectado en esta región se originó en Brasil (Tabla 6). Sin embargo, este país contribuyó únicamente con el 1% o del spam mundial. Por otro lado, Brasil fue el país que tuvo el mayor porcentaje de computadoras infectadas por bots en la región. Los spammers con frecuencia utilizan programas bot para enviar sus correos masivos, por lo tanto es razonable que Brasil sea el país que más origina spam en la región.

La segunda mayor cantidad de spam detectada en América Latina durante este periodo se originó en Argentina con un 14% del total, mientras que Chile contribuyó con el tercer porcentaje más alto: 11% del spam de la región y México contribuyó con un 9%. Después de Brasil, estos tres países tienen la mayor cantidad de usuarios de banda ancha en América Latina, lo que explicaría su relevancia en esta métrica.