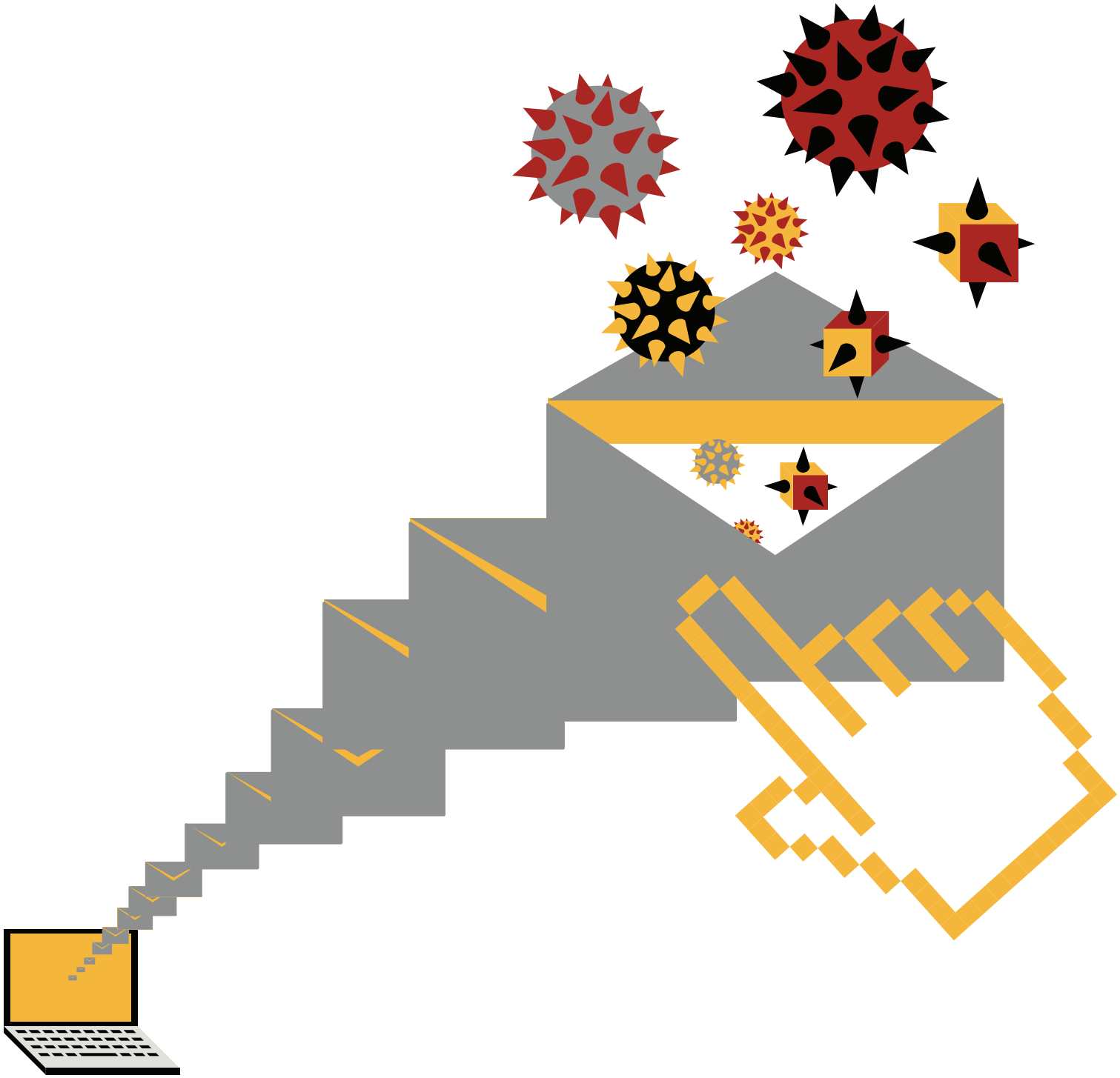
INFORME SOBRE AMENAZAS A LA SEGURIDAD EN INTERNET

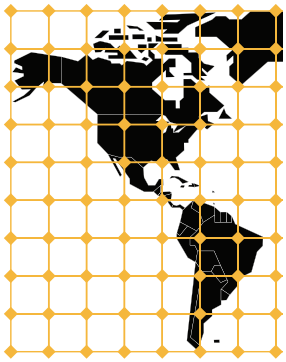
Hallazgos Principales – América

Abril 2012

Symantec™



Contenido



Introducción

Symantec ha establecido una de las fuentes de datos sobre amenazas en Internet más completas del mundo a través de su Red Global de Inteligencia™, la cual está compuesta por más de 64.6 millones de sensores de ataque y monitorea miles de eventos por segundo. Esta red monitorea la actividad de los ataques en más de 200 países y territorios mediante una combinación de productos y servicios de Symantec tales como las soluciones Symantec DeepSight™ Threat Management System, Symantec™ Managed Security Services y los productos de consumo Norton™, así como fuentes de datos adicionales de terceros.

Así, Symantec posee una de las bases de datos sobre vulnerabilidades más completas del mundo, que consiste actualmente en más de 47,662 vulnerabilidades registradas (en un período de más de dos décadas) de más de 15,967 fabricantes que representan más de 40,006 productos.

Datos sobre spam, phishing y código malicioso se capturan a través de una variedad de fuentes que incluyen: Symantec Probe Network, un sistema de más de 5 millones de cuentas señuelo; Symantec.cloud, así como otras tecnologías de seguridad de Symantec. Skeptic™, la tecnología heurística propiedad de Symantec.cloud permite detectar nuevos y sofisticados ataques dirigidos antes de que lleguen a las redes de los clientes.

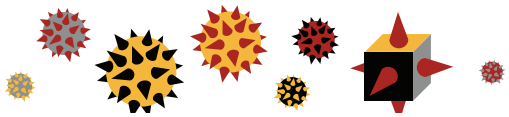
Nuestra tecnología permite monitorear más de 8,000 millones de mensajes de correo electrónico y más de 1,400 millones de solicitudes web al día desde 15 centros de datos. Symantec también recopila información de phishing a través de una amplia comunidad antifraude compuesta por empresas, proveedores de seguridad y más de 50 millones de consumidores.

Estos recursos les brindan a los analistas de Symantec fuentes incomparables de datos para identificar, analizar y realizar informes sobre tendencias emergentes en materia de ataques, actividades de código malicioso, phishing y spam. El resultado de esto es el Informe de Symantec sobre Amenazas a la Seguridad en Internet, que ofrece a empresas y consumidores información esencial para proteger sus sistemas en forma efectiva, hoy y en el futuro.

Además de reunir datos sobre ataques en Internet a nivel mundial, Symantec analiza los datos sobre ataques detectados por sensores implementados en regiones específicas. Este informe aborda los aspectos destacados de la actividad maliciosa que Symantec ha observado en la región de América (que comprende Canadá, Estados Unidos, América Latina y el Caribe) durante el año 2011.

Tendencias de Actividad Maliciosa: América

La sección sobre América del Informe sobre Amenazas a la Seguridad en Internet de Symantec (que incluye Norteamérica y Latinoamérica) ofrece un análisis de la actividad de amenazas, actividad maliciosa y fugas de datos que Symantec observó en esta región durante 2011. La actividad maliciosa analizada en esta sección no sólo incluye actividades de amenazas sino también phishing, código malicioso, zombies de spam, computadoras infectadas por bots y orígenes de ataques a redes. Un ataque se define como toda actividad maliciosa llevada a cabo en una red que ha sido detectada por un sistema de detección de intrusos (IDS, por sus términos en inglés) o firewall. Las definiciones para los demás tipos de actividades maliciosas pueden encontrarse en las respectivas secciones dentro de este informe.
Este análisis se basa en la actividad de amenazas maliciosas detectadas por Symantec en América durante 2011.



Antecedentes

Este indicador evalúa los países en la región de América siendo ésta donde se lleva a cabo o se origina la mayor cantidad de actividad maliciosa a nivel mundial. La actividad maliciosa suele afectar a computadoras que se conectan a Internet mediante banda ancha de alta velocidad dado que estas conexiones son objetivos atractivos para los atacantes. Estas conexiones ofrecen mayor capacidad de ancho de banda que otros tipos de conexión, mejor velocidad, la posibilidad de contar con sistemas continuamente conectados y generalmente una conexión más estable. Symantec clasifica las actividades maliciosas de la siguiente manera:

- **Código malicioso** - Incluye virus, gusanos y Troyanos que se introducen en forma oculta dentro de los programas. Entre los objetivos del código malicioso se encuentran la destrucción de datos, la ejecución de programas destructivos o intrusivos, el robo de información confidencial o sensible, además de poner en peligro la seguridad o integridad de los datos informáticos de la víctima.
- **Zombies de Spam** - Se trata de sistemas afectados que se controlan de manera remota y se utilizan para enviar grandes volúmenes de correo electrónico basura o no deseado (spam). Estos mensajes de correo electrónico pueden utilizarse para transmitir código malicioso y/o realizar intentos de phishing.
- **Hosts de phishing** - Un host de phishing es una computadora que ofrece servicios como aquellos de los sitios web para intentar obtener en forma ilegal información confidencial, personal y financiera simulando que la solicitud proviene de una organización confiable y reconocida. Estos sitios web están diseñados para simular los sitios de empresas legítimas.
- **Computadoras infectadas por bots** - Se trata de computadoras que han sido comprometidas y cuyos atacantes las controlan de manera remota. Habitualmente, el atacante remoto controla una gran cantidad de equipos afectados por medio de un canal único y confiable en una red de bots (botnet) que luego se utiliza para lanzar ataques coordinados.
- **Orígenes de los ataques a redes** - Se trata de las fuentes que dan origen a los ataques por Internet. Por ejemplo, los ataques pueden dirigirse a vulnerabilidades de protocolos SQL o desbordamiento de búfer.
- **Orígenes de ataques basados en web** - Mide las fuentes de ataques que llegan a través de la Web o por HTTP. Por lo general, esto afecta a sitios web legítimos que se utilizan para atacar a visitantes desprevenidos.

Metodología

Para determinar la actividad maliciosa por país, Symantec ha reunido datos geográficos sobre diversas actividades maliciosas que incluyen informes de código malicioso, zombies de spam, hosts de phishing, ordenadores infectados por bots y orígenes de ataques de red. Después, se determina la proporción de cada una de estas actividades que se origina en cada país según la región y se calcula el promedio de los porcentajes de cada actividad maliciosa que se origina en cada país. Este promedio determina la proporción de actividad maliciosa general que se origina en el país en cuestión. Posteriormente se determina el ranking calculando el promedio de la proporción de estas actividades maliciosas que se originaron en cada país.

DATOS

Figura G.1

Actividad Maliciosa por Fuente: Clasificación General – América, 2011

País	Ranking regional 2011	Ranking mundial 2011	Ranking regional 2011 - Código Malicioso	Ranking regional 2011 - Zombies de Spam	Ranking regional 2011 - Hosts de phishing	Ranking regional 2011 – Bots	Ranking regional 2011 – Ataques de Red	Ranking regional 2011 – Ataques Web por País
Brasil	1	4	1	1	1	1	1	1
Estados Unidos	1	1	1	1	1	1	1	1
Argentina	2	22	5	2	3	2	2	4
Canadá	2	16	2	2	2	2	2	2
Colombia	3	28	3	5	2	7	5	5
México	4	29	2	7	5	6	3	2
Chile	5	34	4	4	4	4	4	3
Perú	6	41	7	3	10	3	7	11
Venezuela	7	11	6	9	9	9	6	6
República Dominicana	8	54	9	6	25	5	9	15
Uruguay	9	61	20	8	15	13	8	9
Puerto Rico	10	73	11	17	20	8	10	13

Fuente: Symantec *Países de Norteamérica

Figura G.2

Actividad Maliciosa por Fuente: Código Malicioso - América, 2011

País de origen	Ranking Regional - Código Malicioso 2011	% Regional de Código Malicioso en 2011	Ranking Regional 2011	Ranking Mundial 2011
Estados Unidos	1	91.5%	1	1
Brasil	1	39.9%	1	4
Canadá	2	8.5%	2	16
México	2	21.0%	4	29
Colombia	3	5.5%	3	28
Chile	4	5.4%	5	34
Argentina	5	4.7%	2	22
Venezuela	6	4.3%	7	52
Perú	7	2.7%	6	41
Jamaica	8	2.0%	16	96
República Dominicana	9	1.8%	8	54
Ecuador	10	1.5%	12	76

Fuente: Symantec *Países de Norteamérica

Figura G.3

Actividad Maliciosa por Fuente: Zombies de Spam - América, 2011

País de origen	Ranking Regional – Zombies de Spam	% Regional de Zombies de Spam 2011	Ranking Regional 2011	Ranking Mundial 2011
Estados Unidos	1	93.9%	1	1
Brasil	1	40.4%	1	4
Canadá	2	6.1%	2	16
Argentina	2	14.9%	2	22
Perú	3	9.7%	6	41
Chile	4	8.8%	5	34
Colombia	5	6.7%	3	28
República Dominicana	6	4.6%	8	54
México	7	4.6%	4	29
Uruguay	8	3.5%	9	61
Venezuela	9	2.1%	7	52
Bolivia	10	1.2%	11	75

Fuente: Symantec *Países de Norteamérica

Figura G.4

Actividad Maliciosa por Fuente: Hosts de Phishing -América, 2011

País de origen	Ranking Regional – Host de Phishing 2011	% Regional de Host de Phishing 2011	Ranking Regional 2011	Ranking Mundial 2011
Estados Unidos	1	93.7%	1	1
Brasil	1	39.5%	1	4
Colombia	2	32.7%	3	28
Canadá	2	6.3%	2	16
Argentina	3	8.2%	2	22
Chile	4	5.5%	5	34
México	5	4.8%	4	29
Panamá	6	2.1%	13	79
Islas Vírgenes (Británicas)	7	1.1%	18	110
Ecuador	8	1.0%	12	76
Venezuela	9	0.9%	7	52
Perú	10	0.9%	6	41

Fuente: Symantec *Países de Norteamérica

Figura G.5

Actividad Maliciosa por Fuente: Bots -América, 2011

País de origen	Ranking Regional – Bots 2011	% Regional de Bots 2011	Ranking Regional 2011	Ranking Mundial 2011
Brasil	1	66.3%	1	4
Estados Unidos	1	88.6%	1	1
Canadá	2	11.4%	2	16
Argentina	2	16.6%	2	22
Perú	3	4.0%	6	41
Chile	4	3.5%	5	34
República Dominicana	5	2.2%	8	54
México	6	2.2%	4	29
Colombia	7	1.4%	3	28
Puerto Rico	8	1.0%	10	73
Venezuela	9	0.6%	7	52
Bolivia	10	0.5%	11	75

Fuente: Symantec *Países de Norteamérica

Figura G.6

Actividad Maliciosa por Fuente: Orígenes de Ataques Web -América, 2011

País de origen	Ranking Regional – Ataques Web por Geografía 2011	% Regional de Ataques Web por Geografía 2011	Ranking Regional 2011	Ranking Mundial 2011
Estados Unidos	1	96.6%	1	1
Brasil	1	42.6%	1	4
Canadá	2	3.4	2	16
México	2	12.9%	4	29
Chile	3	10.0%	5	34
Argentina	4	7.7%	2	22
Colombia	5	6.7%	3	28
Venezuela	6	4.7%	7	52
Islas Vírgenes (Británicas)	7	2.6%	18	110
Panamá	8	2.2%	13	79
Uruguay	9	1.6%	9	61
Ecuador	10	1.3%	12	76

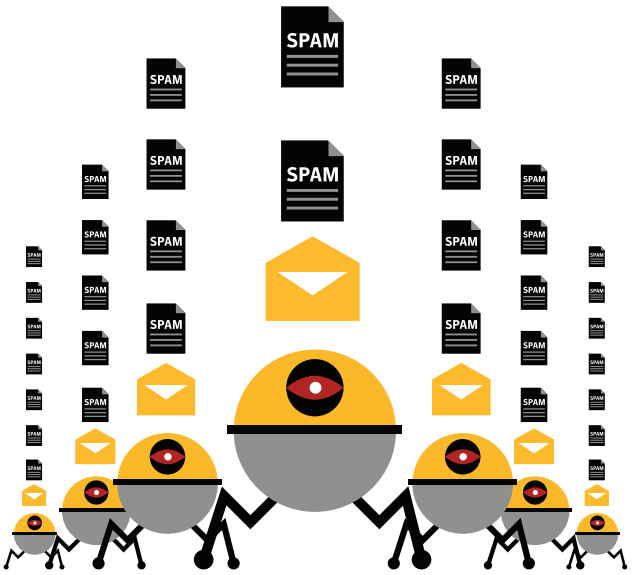
Fuente: Symantec *Países de Norteamérica

Figura G.7

Origen de Ataques de Red - América, 2011

País de origen	Ranking Regional – Ataques de Red por Geografía 2011	% Regional de Ataques de Red por Geografía 2011	Ranking Regional 2011	Ranking Mundial 2011
Brasil	1	42.3%	1	4
Estados Unidos	1	88.5%	1	1
Canadá	2	11.5%	2	16
Argentina	2	14.1%	2	22
México	3	13.0%	4	29
Chile	4	7.0%	5	34
Colombia	5	6.1%	3	28
Venezuela	6	4.9%	7	52
Perú	7	2.4%	6	41
Uruguay	8	2.0%	9	61
República Dominicana	9	1.6%	8	54
Puerto Rico	10	1.2%	10	73

Fuente: Symantec *Países de Norteamérica



Comentario

- La actividad maliciosa originada a partir de computadoras infectadas en Brasil ha llevado al país a ocupar el primer lugar de la tabla como fuente de actividad maliciosa en América Latina durante 2011, y el cuarto lugar a nivel mundial.
- Estados Unidos es el primer lugar en Norteamérica y primero a nivel mundial. Brasil y los Estados Unidos fueron la principal fuente de actividad maliciosa en todas las categorías para cada una de sus respectivas regiones.
- Argentina se clasificó en segundo lugar en el ranking general de América Latina, y también ocupó el segundo sitio para zombies de spam, bots y como fuente de ataques de red en dicha región.

Origen de los Ataques: América

Antecedentes

Esta métrica evalúa los principales países en el mundo desde los cuales se originaron ataques dirigidos a la región de América durante 2011. Debe tenerse en cuenta que, dado que la computadora que lleva a cabo el ataque podría ser controlada en forma remota, el atacante puede estar ubicado en un lugar diferente que donde se encuentra el equipo utilizado para realizar el ataque. Por ejemplo, un atacante ubicado físicamente en Brasil podría lanzar un ataque desde un sistema afectado en Australia contra una red en Japón.

Metodología

Esta sección analiza los principales países desde los cuales se originaron los ataques dirigidos a computadoras situadas en América durante 2011. En general, se considera un ataque de red a cualquier actividad maliciosa que se realiza a través de una red detectada por un sistema de detección de intrusos (IDS), sistema de prevención de intrusos (IPS) o firewall.

DATOS

Figura G.8

Principales Ataques por Fuente - América, 2011

País de origen	Posición	% de Ataques contra la Región en 2011	% de Ataques contra la Región en 2010	Variación (%)
Estados Unidos	1	62.3%	n/a	-
China	2	10.1%	n/a	-
Tailandia	3	2.1%	n/a	-
Canadá	4	1.9%	n/a	-
Corea del Sur	5	1.6%	n/a	-
Rusia	6	1.5%	n/a	-
Reino Unido	7	1.4%	n/a	-
Brasil	8	1.3%	n/a	-
Alemania	9	1.2%	n/a	-
Taiwan	10	1.1%	n/a	-

Fuente: Symantec *Países de Norteamérica

Figura G.8

Principales Ataques por Fuente - Norteamérica, 2011

País de origen	Posición	% de Ataques contra la Región en 2011	% de Ataques contra la Región en 2010	Variación (%)
Estados Unidos	1	62.0%	n/a	-
China	2	10.3%	n/a	-
Tailandia	3	2.2%	n/a	-
Canadá	4	1.9%	n/a	-
Corea del Sur	5	1.7%	n/a	-
Rusia	6	1.5%	n/a	-
Reino Unido	7	1.4%	n/a	-
Brasil	8	1.3%	n/a	-
Alemania	9	1.2%	n/a	-
Taiwan	10	1.1%	n/a	-

Fuente: Symantec *Países de Norteamérica

Figura G.8

Principales Ataques por Fuente - América Latina, 2011

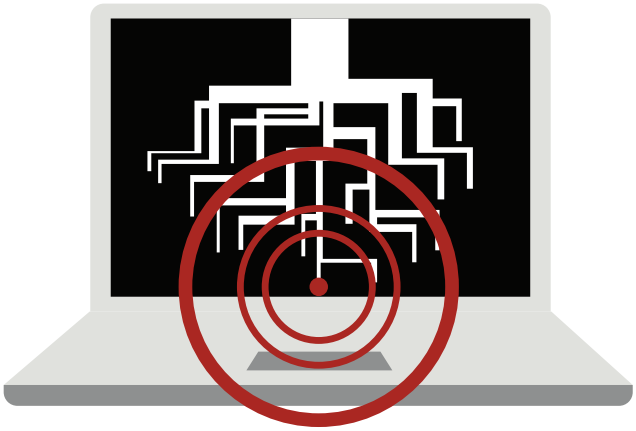
País de origen	Posición	% de Ataques contra la Región en 2011	% de Ataques contra la Región en 2010	Variación (%)
Estados Unidos	1	88.1%	50%	31.8%
Brasil	2	2.3%	7%	-4.7%
México	3	2.1%	14%	-11.9%
China	4	2.0%	2%	0.0%
Reino Unido	5	0.8%	2%	-1.2%
Alemania	6	0.8%	n/a	-
Sudáfrica	7	0.8%	n/a	-
Suecia	8	0.6%	n/a	-
Canadá	9	0.6%	1%	-0.4%
Rusia	10	0.6%	1%	-0.4%

Fuente: Symantec *Países de Norteamérica

Comentario

- Estados Unidos continúa dominando los ataques en la región de América. En 2011, Estados Unidos fue el principal país de origen de ataques contra objetivos en esta zona, representando la mitad del total de ataques detectados por los sensores de Symantec en América.
- Este resultado se debe probablemente al alto nivel de actividad de ataques originados en los Estados Unidos en general, dado que también fue el principal país a nivel mundial donde se originaron ataques Web, con 16.9% del total. También ocupó el segundo lugar a nivel mundial como fuente de ataques de red, ya que 33.5% de los ataques de red fueron originados en dicho país.
- Además, Estados Unidos se ubicó en primer lugar en lo que se refiere a la actividad maliciosa mundial en general, con un 21.1% del total general. Estados Unidos también ocupó el primer lugar a nivel mundial con respecto a computadoras infectadas por bots (12.6%) y en segundo lugar para código malicioso (13.3%); muchas de las actividades de ataques dirigidos a países en la región de América se habrían llevado a cabo a través de estas redes de bots maliciosas.

Tendencias de Código Malicioso: América



Symantec obtiene información de código malicioso de su gran base global de clientes a través de una serie de programas de telemetría anónimos de aceptación voluntaria que incluyen Norton Community Watch, Symantec Digital Immune System y las tecnologías Symantec Scan and Deliver. Más de 133 millones de clientes, servidores y gateways contribuyen activamente con estos programas. Symantec recibe informes sobre nuevas muestras de código malicioso así como de incidentes de detección de tipos de código malicioso conocidos. Los incidentes informados son considerados como posibles infecciones en caso de que se produjera una infección a raíz de la falta de software de seguridad para detectar y eliminar la amenaza.

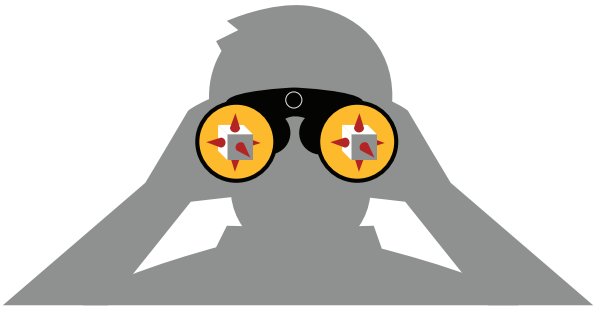
Las amenazas de código malicioso se clasifican en cuatro tipos principales — puertas traseras (backdoors), virus, gusanos y Troyanos:

- **Puertas traseras (backdoors)** - Permiten que un atacante acceda en forma remota a computadoras afectadas.
- **Troyanos** - Son código malicioso que los usuarios instalan en sus computadoras sin darse cuenta, por lo general abriendo adjuntos de correo electrónico o realizando descargas desde Internet. Habitualmente, es otro código malicioso el que descarga e instala el troyano. Los programas troyanos difieren de los gusanos y los virus porque no se propagan por sí mismos.
- **Virus** - Se propagan mediante la infección de archivos existentes en computadoras afectadas con código malicioso.
- **Gusanos** - Son amenazas de código malicioso que pueden replicarse en computadoras infectadas o de algún modo que facilite su copia a otro equipo (por ejemplo, a través de dispositivos de almacenamiento USB).

Muchas amenazas de código malicioso tienen múltiples características. Por ejemplo, una puerta trasera siempre se encuentra junto con otra característica de código malicioso. Normalmente, los backdoor también son Troyanos; no obstante, muchos gusanos y virus también incorporan la funcionalidad de puerta trasera. Además, muchas muestras de código malicioso pueden clasificarse como gusano y como virus debido al modo en que se propagan. Una de las razones de esto es que los desarrolladores de amenazas intentan activar el código malicioso con múltiples vectores de propagación para aumentar las probabilidades de afectar con éxito a las computadoras durante los ataques.

Este análisis se basa en muestras de código malicioso detectadas por Symantec en la región de América durante 2011.

Principales Muestras de Código Malicioso: América



Antecedentes

Este indicador evalúa las principales muestras de código malicioso en la región de América durante 2011. Symantec analiza las muestras de código malicioso nuevas y existentes para determinar qué tipos de amenazas y vectores de ataque se están empleando en las amenazas más frecuentes. Esta información también les permite a los administradores y usuarios familiarizarse con las amenazas preferidas por los atacantes. Los detalles sobre tendencias emergentes en materia de desarrollo de amenazas pueden ayudar a reforzar las medidas de seguridad y mitigar futuros ataques.

Metodología

Para determinar las principales muestras de código malicioso, Symantec clasifica cada una de dichas muestras por el volumen de fuentes únicas de posibles infecciones observadas durante el periodo objeto del informe.

DATOS

Figura G.9

Principales Muestras de Código Malicioso en América, 2011

Posición	Código Malicioso	% de Código Malicioso en la Región
1	W32.Downadup.B	11.8%
2	W32.Sality.AE	11.1%
3	W32.SillyFDC	4.8%
4	W32.Almanahe.B!Inf	4.4%
5	W32.Almanahe.B!Ink	4.1%
6	Trojan.Maljava	3.8%
7	W32.Changeup	2.7%
8	W32.SillyFDC.BDP	2.3%
9	Trojan.FakeAV	2.3%
10	Trojan.ByteVerify	2.0%

Fuente: Symantec

Figura G.9

Principales Muestras de Código Malicioso en Norteamérica, 2011

Posición	Código Malicioso	% de Código Malicioso en la Región
1	W32.Downadup.B	4.5%
2	Trojan.Maljava	3.5%
3	W32.SillyFDC.BDP!lnk	3.4%
4	Trojan.FakeAV	2.1%
5	W32.SillyFDC.BDP	2.0%
6	Trojan.ByteVerify	2.0%
7	Trojan.Malscript!html	1.3%
8	Trojan.Zefarch	1.2%
9	W32.Qakbot	1.0%
10	W32.Ramnit!html	0.9%

Fuente: Symantec

Figura G.9

Principales Muestras de Código Malicioso en América Latina, 2011

Posición	Código Malicioso	% de Código Malicioso en la Región
1	W32.Sality.AE	10.3%
2	W32.Downadup.B	7.3%
3	W32.SillyFDC	4.2%
4	W32.Almanahe.B!inf	3.6%
5	W32.changeup	2.3%
6	W32.Chir.B@mm(html)	1.5%
7	W32.Slugin.A!inf	1.5%
8	W32.Harakit	1.4%
9	W32.Virut.CF	1.4%
10	W32.Downadup!autorun	1.3%

Fuente: Symantec

Comentario

- **W32.Downadup (aka Conficker) domina la región de América**
  W32.Downadup.B se ubicó en el primer lugar en la región en 2011, representando el 7.3% de las posibles infecciones en América Latina y el 4.5% en Norteamérica.
- La familia de malware Downadup ocupó el cuarto lugar a nivel mundial en 2011, aún cuando en 2010 se ubicó como la segunda familia de código más malicioso por volumen de posibles infecciones a nivel mundial.
- Downadup se propaga mediante la explotación de vulnerabilidades con el objeto de copiarse a recursos compartidos por red. Para fin de 2011, se estimó que Downadup aún se encontraba en más de 3 millones de PCd en todo el mundo , en comparación con aproximadamente 5 millones a fin de 2010.
- Es interesante destacar que las variantes de *Ramnit*, que fue la familia número uno de malware a nivel mundial durante 2011, no se ubicó entre los principales 10 malware identificados en la región de América, representando menos del 1% de las posibles infecciones en Norteamérica.
- *W32.Sality.AE* ocupó el primer lugar en América Latina pero no se ubicó entre los primeros diez en Norteamérica. La actividad de este virus, de acuerdo con lo informado, fue el principal factor que contribuyó a que la familia Sality ocupara el segundo lugar como familia de código malicioso a nivel mundial en 2011.
- Desde su descubrimiento en 2008, Sality.AE ha sido una parte importante del panorama de amenazas, incluyendo su lugar como principal familia de código malicioso a nivel mundial identificada por Symantec en 2010 y 2009.
- Sality puede resultarle particularmente atractivo a los atacantes porque utiliza código polimórfico que puede dificultar la detección y también es capaz de desactivar los servicios de seguridad en las computadoras afectadas. Estos dos factores pueden llevar a un mayor índice de instalaciones exitosas para los atacantes.

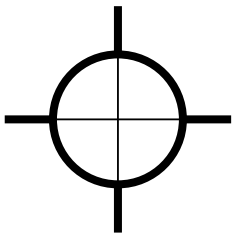
Mejores Prácticas y Recomendaciones

EMPRESAS

- Emplear estrategias de defensa a profundidad.
- Apagar y eliminar servicios que no son necesarios.
- Si algún código malicioso o alguna otra amenaza explota uno o más servicios de red, deshabilite o bloquee el acceso a esos servicios hasta que se aplique un parche. Aisle las computadoras infectadas.
- Mantener los parches actualizados.
- Implementar soluciones de acceso y cumplimiento de políticas de red.
- Crear y establecer políticas efectivas de contraseñas y control de dispositivos.
- Configurar los servidores de correo para bloquear o remover los correos con archivos adjuntos que son usados con frecuencia para diseminar virus.
- Asegurarse que los procedimientos de emergencia estén vigentes y eduque a sus empleados para no abrir archivos de remitentes desconocidos ni descargar software que no ha sido escaneado previamente.

CONSUMIDORES

- Tener contraseñas con una mezcla de letras y números y cambiarlas con frecuencia. Las contraseñas no deben tener palabras del diccionario
- Nunca ver, abrir o ejecutar archivos adjuntos de correo electrónico a menos que se estén esperando y que se conozca el propósito de los mismos.
- Mantener las definiciones de virus actualizadas regularmente.
- Verificar periódicamente para ver si su sistema operativo es vulnerable a las amenazas.
- Nunca revelar información personal o financiera confidencial a menos que y hasta que se pueda confirmar que la solicitud de dicha información es legítima.
- No realizar actividades de Internet de alto riesgo, como transacciones bancarias o compras en línea, desde computadoras públicas.
- Evitar pulsar clic en enlaces o archivos adjuntos en mensajes de correo electrónico o mensajes de Mensajería Instantánea, puesto que estos también pueden exponer los equipos a riesgos innecesarios.
- Utilizar una solución de seguridad de Internet que combine antivirus, firewall, detección de intrusos y gestión de vulnerabilidades para brindar máxima protección contra códigos maliciosos y otras amenazas.
- Tener parches de seguridad actualizados y que se apliquen oportunamente.



RECURSOS ADICIONALES

Informe sobre Amenazas a la Seguridad en Internet: www.symantec.com/la/gin
Otros reportes de Symantec: www.symantec.com/la/reportes
Soluciones de Symantec: www.symantec.com/la/empresas

Acerca de Symantec

Symantec es líder mundial en soluciones de seguridad, almacenamiento y administración de sistemas que ayudan a empresas y consumidores a proteger y administrar su información. Nuestro software y servicios protegen contra más riesgos, en más puntos y de manera más completa y eficaz, generando confianza dondequiera que la información se utilice o guarde.
Más información en www.symantec.com/la