Confidence in a connected world.

Informe de Symantec sobre las Amenazas a la Seguridad en Internet

Abril del 2010

Hoja de datos regionales — América Latina

Nota importante sobre estas estadísticas

Las estadísticas que se describen en este documento se basan en los ataques contra una amplia muestra de clientes de Symantec. La actividad de los ataques fue detectada por Symantec™ Global Intelligence Network, que incluye los Servicios de Seguridad Administrados de Symantec y el Sistema de Control de Amenazas DeepSight™ de Symantec, ambos utilizan sistemas automatizados para asignar la dirección IP del sistema atacante para identificar el país en el que se encuentra. Sin embargo, debido a que los atacantes utilizan con frecuencia sistemas comprometidos, situados alrededor del mundo para lanzar ataques de forma remota, la ubicación del sistema atacante puede diferir de la ubicación del atacante.

Introducción

Symantec ha establecido algunas de las fuentes más completas de datos de amenazas en Internet en el mundo a través de la red de inteligencia global de Symantec. Más de 240.000 sensores en más de 200 países y territorios supervisan la actividad de los ataques a través de una combinación de productos y servicios de Symantec, tales como el Sistema de Control de Amenazas DeepSight de Symantec, los Servicios de Seguridad Administrados de Symantec y productos de consumo Norton™, así como fuentes de datos adicionales de otros proveedores.

Symantec también recopila inteligencia de códigos maliciosos de más de 133 millones de sistemas cliente, servidores y Gateway, que han implementado sus productos antivirus. Además, la red distribuida honeypot de Symantec recopila datos alrededor del mundo, después de capturar previamente amenazas y ataques inadvertidos y proporcionar información valiosa sobre los métodos de los atacantes.

Los datos de spam y phishing son capturados a través de una variedad de fuentes, como: Symantec Probe Network, un sistema de más de 5 millones de cuentas señuelo; MessageLabs Intelligence, una respetada fuente de datos y análisis de problemas, tendencias y estadísticas de seguridad de los mensajes; y otras tecnologías de Symantec. Los datos son recopilados en más de 86 países. Más de 8 millones de mensajes de correo electrónico, así como solicitudes Web superiores a 1.000 millones, se procesan diariamente en 16 centros de datos. Symantec también recopila información de phishing a través de una amplia comunidad antifraude de empresas, proveedores de seguridad y más de 50 millones de consumidores.

Estos recursos brindan a los analistas de Symantec fuentes sin precedentes de datos con que identificar, analizar y proporcionar comentarios informados sobre las nuevas tendencias de los ataques, la actividad de códigos maliciosos, phishing y spam. El resultado es el Informe Global sobre las Amenazas a Seguridad de Symantec, que brinda a las empresas y consumidores información esencial para proteger eficazmente sus sistemas en el presente y futuro.

Además de la recopilación de datos de ataques en Internet para el *Informe de Amenazas a la Seguridad*, Symantec también analiza los datos de ataques detectados por sensores desplegados en regiones específicas. Esta hoja de datos regionales abordará aspectos destacados de la actividad maliciosa, que Symantec ha observado en la región de América Latina en 2009.

Aspectos destacados

- Brasil fue el país con mayor actividad maliciosa en la región de América Latina en 2009, con el 43 por ciento del total. En el ámbito mundial, Brasil fue tercero, con un 6 por ciento del total de actividad maliciosa por país.
- Estados Unidos fue el país que más ataques originó, detectados por los sensores en América Latina en 2009, con 40 por ciento de todos los ataques detectados, lo que significó una disminución con respecto al 58 por ciento que representó en 2008. Estados Unidos también fue el país que más ataques originó contra objetivos mundiales en 2009, con un 23 por ciento de la actividad mundial.
- Brasil fue el país con más equipos infectados por bots en la región de América Latina en 2009, un 54 por ciento del total. A nivel mundial, en 2009, Brasil ocupó el tercer lugar en equipos infectados por bots, con un 7 por ciento del total.
- En 2009, el gusano Downadup.B fue la muestra de códigos malicioso más frecuentemente observada por infección potencial en la región de América Latina; este gusano se ubicó en la sexta posición a nivel mundial en 2009.
- En 2009, Brasil fue el país que originó el mayor volumen de spam en América Latina con 54 por ciento del total. A nivel mundial en 2009, Brasil ocupó el segundo lugar en cuanto al origen del spam con un 11 por ciento del total mundial.

Actividad maliciosa por país

Esta métrica evalúa los países de América Latina con mayor volumen de actividades maliciosas en 2009. Para determinarlo, Symantec ha compilado datos geográficos en numerosas actividades maliciosas, incluyendo informes de códigos maliciosos, zombis de spam, hosts de phishing, equipos infectados por bots y origen de los ataques. La clasificación se determina mediante el cálculo del promedio de la proporción de estas actividades maliciosas que se originaron en cada país.

La actividad maliciosa generalmente afecta a los equipos que están conectados a Internet de banda ancha de alta velocidad, debido a que estas conexiones son destinos atractivos para los atacantes. Las conexiones de banda ancha ofrecen más capacidades que otros tipos de conexión, velocidades más rápidas, el potencial de sistemas constantemente conectados y normalmente mayor estabilidad en la conexión. Symantec ha observado en el pasado que la actividad maliciosa en un país tiende a aumentar en relación con el crecimiento de la infraestructura de banda ancha. Esto indica que los nuevos usuarios pueden no estar habituados o desconocen el mayor riesgo de exposición a ataques maliciosos de estas conexiones sólidas.

Brasil fue de nuevo el país con mayor actividad maliciosa en la región de América Latina en 2009, con el 43 por ciento del total regional, lo que significó un incremento con relación al 34 por ciento en 2008 (Tabla 1). A nivel mundial en 2009, Brasil representó un 6 por ciento del total y clasificó en tercer lugar en esta medición, un aumento del 4 por ciento y quinto lugar en 2008. Esta es la primera vez que un país distinto a Estados Unidos, China o Alemania está en los tres primeros lugares a nivel mundial en esta categoría, desde que Symantec la integró al reporte en 2006.

LAM Ranking 2009	LAM Ranking 2008	País	Porcentaje 2009	Porcentaje 2008	Ranking 2009 por Actividad: Código Malicioso	Spam Zombies	Phishing	Bots
1	1	Brasil	43%	34%	1	1	1	1
2	2	México	13%	17%	2	4	4	5
3	3	Argentina	13%	15%	6	2	2	2
4	4	Chile	7%	8%	5	5	3	3
5	5	Colombia	7%	7%	4	3	5	6
6	7	Venezuela	3%	3%	3	9	6	10
7	6	Perú	3%	4%	7	6	8	4
8	9	República Dominicana	1%	1%	11	7	19	7
9	8	Puerto Rico	1%	2%	9	12	10	8
10	12	Uruguay	1%	1%	24	8	9	12

Tabla 1. Actividad maliciosa por país, América Latina
Fuente: Symantec

Brasil ocupó el primer lugar en todas las actividades consideradas maliciosas en la región generadas en 2009 y también ocupó el primer lugar en todas las categorías en 2008, excepto en códigos maliciosos, en el que ocupó el segundo lugar después de México. En 2009, Brasil aumentó su participación en la región en todas las mediciones de categorías específicas. Se considera que los aumentos obedecen al rápido crecimiento continuo de su infraestructura de Internet y el uso de banda ancha, así como el hecho de que Brasil fue uno de los países más afectados por las variantes del gusano Downadup[i] (también conocido como Conficker) en 2009.

El aumento del porcentaje de Brasil en la actividad general maliciosa en 2009 se atribuye principalmente a un aumento significativo en su clasificación de códigos maliciosos. No sólo superó a México al ocupar el primer lugar en la región, sino que también ocupó el quinto lugar a nivel mundial en códigos maliciosos en 2009, después de ocupar el puesto número 16 en 2008. Esto probablemente se debe a la propagación de las infecciones Downadup ocurridas en 2009 y en las que Brasil ocupó el cuarto lugar a nivel mundial. Una explicación del éxito de Downadup en Brasil es que, como parte de su funcionalidad, el gusano puede centrarse específicamente en regiones con base en su capacidad para identificar la configuración del idioma de una computadora atacada, de los cuales uno es el "portugués (brasilero)[ii]".

Además, Brasil ocupó el tercer puesto a nivel mundial en posibles infecciones por virus y cuarto por posibles infecciones por gusanos en 2009. Esta clasificación representa grandes aumentos con respecto a los periodos anteriores, lo que indica que una cantidad significativa de actividad de códigos maliciosos persiste en Brasil. En el pasado, Brasil fue también una fuente importante de códigos maliciosos que roban la información bancaria y algunas de las más notorias muestras que procedían de Brasil permanecen activas[iii]. Por ejemplo, el troyano Bancos, descubierto por primera vez allí en 2003, aún es una de las 50 muestras de códigos más maliciosos y causantes de posibles infecciones en 2009[iv].

Una consecuencia del creciente nivel de actividad de códigos maliciosos que afecta a este país ha sido la propuesta de un nuevo proyecto de ley de delitos informáticos[v]. La iniciativa también puede ser el resultado de ciertos ataques cibernéticos de alto perfil perpetrados allí en los últimos años[vi]. Uno de los ataques provocó un apagón masivo de la red eléctrica, mientras que otro resultó en el robo de datos valiosos y una solicitud de rescate por US$350.000, después de que un sitio Web del gobierno fuera atacado, lo que también produjo más de 3.000 empleados que no pudieron acceder a este sitio durante 24 horas[vii].

México ocupó el segundo lugar en actividad maliciosa en América Latina en 2009, con un 13 por ciento del total regional. También ocupó el segundo lugar en 2008, con 17 por ciento del total. Argentina fue tercero en actividad maliciosa en la región, con 13 por ciento de la actividad maliciosa total. El año pasado, Argentina también ocupó el tercer lugar a nivel regional, con 15 por ciento de la actividad maliciosa total en 2008.

Una de las razones para la alta clasificación de estos países también se debe a la propagación de Downadup en la región. Los cinco primeros países en esta métrica también se ubicaron entre los 10 países más afectados por la difusión inicial de la Downadup y en conjunto representaron el 27 por ciento del total mundial inicial[viii].

Países que originan los ataques

En este informe se evalúa los países que son fuentes generadoras de ataques dirigidos a los países de una región específica. Un ataque generalmente es toda actividad maliciosa perpetrada en una red que ha sido detectada por un sistema de detección de intrusos (IDS), sistema de prevención de intrusos (IPS) o firewall.

En 2009, Estados Unidos fue de nuevo el país que más ataques originó, detectados por los sensores de Symantec, ubicados en la región de América Latina, con 40 por ciento del total (Tabla 2). Se trata de una disminución con respecto a 2008, cuando un 58 por ciento de los ataques dirigidos a la región se originaron en ese país. El primer lugar que ha ocupado continuamente Estados Unidos probablemente se explica por al alto nivel de actividad de los ataques globales que se originaron generalmente allí, puesto que Estados Unidos también fue el país que más ataques originó contra objetivos mundiales, con 23 por ciento de ese total en 2009. La mayor proporción de ataques dirigidos a la región con respecto a los objetivos mundiales en conjunto indica que los ataques que se originaron en Estados Unidos pueden estar específicamente destinados a los países de la región de América Latina.

Ranking LAM 2009	Ranking LAM 2008	País	Porcentaje 2009 LAM	Porcentaje 2008 LAM	Porcentaje 2009 Global
1	1	Estados Unidos	40%	58%	23%
2	5	Brasil	13%	3%	4%
3	16	México	5%	<1%	1%
4	4	Argentina	5%	3%	1%
5	2	China	4%	8%	12%
6	18	Costa Rica	3%	<1%	<1%
7	3	Chile	3%	3%	1%
8	7	Canadá	2%	2%	2%
9	6	España	2%	2%	3%
10	10	Colombia	2%	1%	1%

Tabla 2. Países que más generan ataques hacia América Latina
Fuente: Symantec

La disminución de 2008 a 2009 en la actividad maliciosa destinada a la región de América Latina, que se originó en Estados Unidos (de 58 por ciento a 40 por ciento) es probablemente debido a la disminución de la actividad maliciosa, que se originó en Estados Unidos en general, puesto que su participación global en esta métrica disminuyó de un 23 por ciento en 2008 a un 19 por ciento en 2009.

Brasil ocupó el segundo lugar en 2009 en actividad de ataques dirigidos a los países de la región LAM, con 13 por ciento del total. Se trata de un aumento significativo con respecto a 2008, cuando el total de Brasil en esta medición fue tan solo de un 3 por ciento. Parte de este aumento se explica por

la disminución en el porcentaje de actividad originada en Estados Unidos. Sin embargo, también es probable debido al aumento general en la actividad maliciosa, originada en Brasil el año pasado, de 34 a 43 por ciento del total regional (Tabla 1). Esto, a su vez, fue debido en gran parte al gusano Downadup, como se explicó anteriormente. Además cabe señalar que Downadup descarga códigos maliciosos en computadoras infectadas, que posiblemente incluyen bots, lo que probablemente produciría una cantidad elevada de ataques.

México fue el tercero que más actividad de ataques dirigidos a los países de la región LAM originó en 2009, con 5 por ciento del total, lo que representó un incremento con respecto al puesto 16 que ocupó y menos del 1 por ciento del total en 2008. México fue el segundo país de la región en actividades maliciosas en 2009 y en 2008, por lo que parece que la actividad general no ha aumentado considerablemente, sin embargo, puede ser que esa actividad de ataques procedente de México y que previamente había atacado áreas fuera de la región, con Estados Unidos como el destino más probable, haya cambiado en 2009 a objetivos dentro de la región de Latinoamérica.

De los 10 países que más ataques originaron en la región en 2009, seis se encuentran en la misma región. Esto representa un aumento con respecto a 2008, cuando sólo cuatro de los 10 países que más originaban ataques se encontraban en la región. Los porcentajes regionales de cada uno de los ataques fueron significativamente más altos que los porcentajes globales, lo que indica que estos países pueden estar atacando específicamente a la región de Latinoamérica. Symantec ha observado que los ataques a menudo atacan la región en donde se originan, debido a la proximidad, el idioma compartido o intereses similares, sociales y culturales[ix].

Computadoras por país infectadas con bots

Los bots son programas que se instalan silenciosamente en el equipo del usuario, a fin de permitir a un atacante controlar de forma remota el sistema de destino a través de un canal de comunicación, como sistemas IRC (Internet Relay Chat), redes punto a punto (p2p) o HTTP. Estos canales permiten al atacante remoto controlar un gran número de equipos atacados por un canal único y confiable en un botnet, que luego puede ser utilizado para lanzar ataques coordinados. Reconociendo la amenaza constante de los botnets, Symantec rastrea la distribución de equipos infectados con bots a nivel mundial y regional. Symantec también evalúa qué países de la región tienen los mayores porcentajes de equipos infectados por bots.

En 2009, la región latinoamericana representó 14 por ciento del total de equipos infectados por bots que se han detectado mundialmente, lo que correspondió a un incremento con respecto al 13 por ciento en 2008. En la región, Brasil tuvo el mayor porcentaje de computadoras infectadas por bots, con 54 por ciento del total regional (tabla 3); esto representó un aumento en relación al 42 por ciento en 2008, cuando Brasil también fue el país con más computadoras infectadas de la región. A nivel mundial en 2009, Brasil tenía un 7 por ciento del total y ocupaba el tercer lugar: un aumento con respecto al 6 por ciento y quinto lugar en 2008.

El margen abrumador por el cual Brasil fue el país que más equipos infectados por bots tuvo en la región, fue probablemente debido a la prevalencia del gusano Downadup. Este fue la muestra más común de códigos maliciosos por infección potencial en la región durante el año pasado y, como se ha señalado, Brasil fue el país más afectado de la región. Un importante vector de ataque de Downadup descarga códigos maliciosos adicionales en los equipos infectados con bots, donde los bots son una de sus posibles cargas destructivas.

Ranking LAM	Ranking Global	País	Porcentaje LAM	Porcentaje Global
1	3	Brasil	54%	7%
2	12	Argentina	18%	3%
3	21	Chile	7%	1%
4	22	Perú	6%	1%
5	25	México	5%	1%
6	29	Colombia	4%	<1%
7	37	República Dominicana	2%	<1%
8	50	Puerto Rico	1%	<1%
9	62	Bolivia	<1%	<1%
10	63	Venezuela	<1%	<1%

Tabla 3. Computadoras infectadas con bots por país, LAM
Fuente: Symantec

Argentina ocupó el segundo lugar en equipos infectados por bots en la región LAM en 2009, con un 18 por ciento del total; se trata de un ligero incremento con respecto al 17 por ciento en 2008, cuando también se ubicó segundo en la región. Argentina tuvo el 3 por ciento del total mundial de equipos infectados por bots en 2009 y ocupó el puesto número doce. Chile fue tercero en la región en 2009, con un 7 por ciento del total, reemplazando a Perú, que descendió al cuarto lugar. A nivel mundial, Chile tuvo el 1 por ciento del total de equipos infectados por bots en 2009 y ocupó el puesto 21. Los cambios en los porcentajes y totales no varían enormemente con relación a las cifras de 2008 y pueden ser atribuidos a ligeras variaciones de un período al otro.

Muestras de códigos maliciosos

El año pasado, el ejemplo más común de muestras de códigos maliciosos detectados en América Latina que podría causar infecciones potenciales (hablamos de potencial porque fueron detenidas por Symantec) fue el gusano Downadup.B (Tabla 4). Este gusano se clasificó sexto a nivel mundial en 2009. Descubierto por primera vez en noviembre de 2008, Downadup fue capaz de propagarse rápidamente debido a su habilidad para aprovechar una vulnerabilidad de día cero que permitía la ejecución de códigos remotos, lo que le permitió propagarse a través de dispositivos extraíbles. Una vez que el código está en un equipo comprometido, Downadup utiliza un mecanismo de actualización Web o P2P para descargar versiones actualizadas de sí mismo o para instalar otros programas maliciosos, como el código para convertir el equipo atacado en un bot.

Posición	Muestra	Tipo	Vectores de Infección	País con más Muestras	Segundo País con Más Muestras	Impacto
1	Downadup.B	Gusano	Explota vulnerabilidades, redes compartidas	Brasil	México	Descarga e instala amenazas adicionales
2	SillyFDC	Gusano	Asignación de una unidad de disco a dispositivos removibles	México	Brasil	Descarga e instala amenazas adicionales
3	Sality.AE	Gusano, virus	Asignación de una unidad de disco a dispositivos removibles	Brasil	México	Descarga e instala amenazas adicionales
4	Gammima.AG	Gusano, virus	Drives removibles	México	Brasil	Roba credenciales de cuentas de juegos en línea
5	Gampass	Caballo de Troya	N/A	México	Brasil	Roba credenciales de cuentas de juegos en línea
6	Almanahe.B	Gusano, virus	Asignación de una unidad de disco a dispositivos removibles	Brasil	México	Manipula registro y descarga e instala amenazas adicionales
7	SillyDC	Gusano	Asignación de una unidad de disco a dispositivos removibles	México	Brasil	Descarga e instala amenazas adicionales
8	IRCBot	Gusano, caballo de Troya	Drives removibles, SMTP	México	Brasil	Descarga e instala amenazas adicionales
9	Brisv.A	Gusano, caballo de Troya	SMTP	Brasil	México	Descarga e instala amenazas adicionales
10	Downadup	Gusano	Asignación de una unidad de disco a dispositivos removibles	Chile	Brasil	Descarga e instala amenazas adicionales

Tabla 4. Muestras más representativas de códigos maliciosos (infecciones potenciales) en América Latina
Fuente: Symantec

El código malicioso que ocupó el segundo lugar y generó infecciones potenciales en la región LAM en 2009 fue el gusano SillyFDc SillyFDc[x]. Este gusano se propaga por copias de sí mismo a cualquier dispositivo de almacenamiento de medios extraíbles conectado al equipo atacado. Una vez instalado, también intenta descargar e instalar amenazas adicionales en el equipo comprometido. Este gusano también fue la muestra de códigos maliciosos que ocupó el segundo lugar en la región en 2008.

La tercera muestra de códigos maliciosos más frecuentemente reportada que causa infecciones potenciales en Latinoamérica en 2009 fue el virus Sality.ae[xi]. Este virus fue la muestra de código malicioso que causó más infecciones potenciales a nivel mundial en 2009. Sality está diseñado para descargar e instalar software malicioso adicional en el equipo de la víctima, para impedir acceso a los diversos dominios relacionados con seguridad, detener los servicios relacionados con protección y eliminar los archivos relacionados con la seguridad en el proceso. El virus también infecta los archivos .exe y .scr en una unidad de disco (C) local atacada y en cualquier recurso de red escribible. Sality también se copia a sí mismo en unidades extraíbles conectadas.

Es de notar que cinco de las diez muestras de códigos maliciosos en la región registradas en 2008 siguen ocupando la misma posición en esta categoría en 2009 y además varios de estos códigos también se ubicaron en los primeros 10 lugares en 2007. La prevalencia continua de estas muestras puede indicar que los usuarios y administradores no actualizan sus programas antivirus contra las amenazas más comunes.

Países Generadores de Spam

En esta sección se mencionarán los diez países que más generan spam en América Latina. Cabe señalar que, debido a que los spammers intentan redirigir la atención lejos de sus ubicaciones, la región en la que se identificó el origen del spam puede no corresponder a la región en la que se encuentran localizados físicamente los spammers.

En 2009, el 20 por ciento de todo el spam detectado alrededor del mundo por Symantec se originó en América Latina, lo que representó un aumento frente al 12 por ciento en 2008. En la región, Brasil ocupó el primer lugar con 54 por ciento, como el país que más spam origina. A nivel mundial en 2009, Brasil ocupó el segundo lugar con 11 por ciento como originador de spam en todo el mundo. La alta tasa de spam originado en Brasil probablemente se correlaciona con el alto porcentaje de zombis de spam situados allí, puesto que Brasil ocupó el primer lugar en zombis de spam en la región y, más significativamente, a nivel mundial en 2009.

Ranking			Porcentaje	
LAM	Global	País	LAM	Global
1	2	Brasil	54%	11%
2	10	Colombia	12%	2%
3	11	Argentina	12%	2%
4	19	Chile	7%	1%
5	26	México	4%	1%
6	32	Perú	3%	1%
7	42	República Dominicana	2%	<1%
8	46	Venezuela	1%	<1%
9	54	Uruguay	1%	<1%
10	60	Guatemala	1%	<1%

Tabla 5. Países que más spam generan hacia América Latina
Fuente: Symantec

Colombia ocupó el segundo lugar como generador de spam en América Latina, con 12 por ciento del total y se colocó como el décimo lugar a nivel mundial en 2009, lo que correspondió a un 2 por ciento del total mundial. En 2008, Colombia fue tercero en la región, también con 12 por ciento del total. A pesar de que Colombia tenía sólo el quinto porcentaje de actividad maliciosa más alto en la región de América Latina en 2008, tuvo el tercer porcentaje más alto de zombis de spam, lo que explica el alto volumen de actividad de spam originado en dicho país.

Argentina fue el tercer mayor generador de spam en Latinoamérica en 2009, también con un 12 por ciento del total (la diferencia en la clasificación se debe a la aproximación de las cifras) y ocupó el onceavo lugar a nivel global, con 2 por ciento del total mundial. En 2008, Argentina ocupó el segundo lugar como originador de spam en América Latina, con 15 por ciento del total. Al igual que Brasil y Colombia, Argentina tenía un alto volumen de zombis de spam, con el segundo volumen más alto en la región en 2009.

Anexo A: Mejores Prácticas de Symantec

Symantec comparte con los usuarios y administradores las siguientes recomendaciones básicas de seguridad, que les ayudarán a mantener su información a salvo.

Mejores Prácticas para las Empresas

- Emplear estrategias de defensa en profundidad, que enfaticen sistemas de protección múltiples, superpuestos y mutuamente complementarios para protegerse de fallas específicas en cualquier método específico de tecnología o protección. Esto debe incluir el uso de antivirus, firewalls, detección de intrusos y sistemas de protección de intrusos actualizados periódicamente en los sistemas cliente. El uso de un firewall también puede evitar que las amenazas que envían información al atacante abran un canal de comunicación.

- Los administradores deben limitar los privilegios en los sistemas para los usuarios que no requieren dicho acceso y deben restringir dispositivos no autorizados, como unidades de discos duros externos portátiles y otros medios extraíbles.

- Desconectar y eliminar los servicios que no son necesarios para el normal funcionamiento de la red de la empresa.

- Evaluar la seguridad regularmente para garantizar que se implementen y se cuenten con los controles adecuados.

- Educar a la administración en cuanto a las necesidades presupuestales de la seguridad.

- Si los códigos maliciosos u otra amenaza atacan uno o más servicios de red, deshabilitan o bloquean el acceso a estos servicios, se debe aplicar un parche.

- Los administradores deben actualizar las definiciones antivirus regularmente para protegerse de la gran cantidad de nuevas amenazas de códigos maliciosos y garantizar que todos los equipos de escritorio, portátiles y servidores se actualicen con todos los parches de seguridad necesarios de su proveedor de sistema operativo. IDS, IPS y otras tecnologías de bloqueo de comportamiento deberían también ser empleadas para evitar el ataque de nuevas amenazas.

- Siempre mantener los niveles de parches actualizados, especialmente en los equipos que alojan las aplicaciones y servicios públicos — como HTTP, FTP, SMTP, y servidores DNS — a los que se accede a través de un firewall o que son colocados en un DMZ

- Puesto que los equipos atacados pueden ser una amenaza para otros sistemas, Symantec recomienda a las empresas afectadas notificar a los ISPs sobre cualquier actividad potencialmente maliciosa.

- Considerar la implementación de soluciones de cumplimiento de normas para la red que ayuden a mantener a los usuarios móviles infectados fuera de la red (y desinfectarlos antes de reincorporarse a la red).

- Aplicar una política eficaz de contraseñas. Asegurarse de que las contraseñas sean una mezcla de letras y números y cambiarlas con frecuencia. Sugerimos que en ellas, no se incluyan palabras que se encuentren en un diccionario.

- Realizar filtrado de entrada y salida de todo el tráfico de la red para reducir la actividad maliciosa y evitar comunicaciones no autorizadas.

- Deben configurarse los servidores de correo para bloquear el correo electrónico que parece provenir del interior de la empresa, pero que en realidad se origina de fuentes externas.

- Considerar el uso de autenticación de dominio o de correo electrónico a fin de comprobar el origen real de un mensaje de correo electrónico para protegerse de los estafadores que falsifican los dominios de correo electrónico.

- Configurar los servidores de correo para bloquear o eliminar el correo electrónico que contiene archivos adjuntos que se utilizan comúnmente para la propagación de virus, tales como .vbs, .bat, .exe, .pif y archivos.scr.

- Es recomendable no dar clic en los enlaces o archivos adjuntos de los mensajes de correo electrónico (o mensajeros instantáneos) ya que puede exponer los equipos a riesgos innecesarios. Se debe garantizar que se implementen en los equipos de escritorio solamente las aplicaciones aprobadas por la organización.

- Aislar los equipos infectados rápidamente para evitar más riesgos de infección en la organización.

- Capacitar a los empleados para que no abran archivos adjuntos a menos que los estén esperando y provengan de una fuente conocida y confiable y no ejecuten el software que se descarga de Internet, a menos que se haya escaneado en busca de virus.

- Realizar un análisis forense y restaurar los equipos usando medios confiables.

- Garantizar que se implementen procedimientos de respuesta de emergencia. Esto incluye tener una solución de copias de respaldo y recuperación con el fin de restaurar datos perdidos o infectados en caso de un ataque exitoso o pérdida de datos catastrófica.

- Tener en cuenta que los riesgos de seguridad pueden instalarse automáticamente en las computadoras con la instalación de programas de uso de archivos compartidos, descargas gratuitas y versiones freeware y shareware de software.

- Emplear la supervisión de los registros de servidores Web para realizar un seguimiento cuando se produzcan descargas completas de sitios Web, logotipos e imágenes de la compañía, puesto que esto puede indicar que alguien está intentando usar el sitio Web legítimo para crear un sitio Web ilegítimo de phishing.

- Los administradores de red deben revisar los registros de los proxis Web para determinar si los usuarios han visitado sitios de listas negras.

Mejores Prácticas para los Consumidores

- 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.

- Garantizar que los parches de seguridad estén actualizados y que se apliquen a todas las aplicaciones vulnerables de manera oportuna.

- Asegurarse de que las contraseñas sean una mezcla de letras y números (símbolos de ser posible) 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. Mediante la implementación de las últimas definiciones de virus, se puede proteger los equipos de las amenazas más nuevas que se propagan rápidamente.

- Verificar periódicamente si su sistema operativo es vulnerable a las amenazas. Un análisis de seguridad gratuito está disponible a través de Symantec Security Check en www.symantec.com/securitycheck.

- Participar en el seguimiento y reportes de intentos de ataques. Con el servicio de seguimiento de Symantec Security Check, los usuarios pueden identificar rápidamente la ubicación de posibles atacantes informáticos y reenviar la información al ISP del atacante o a la policía local.

- Implementar una solución antiphishing, como la barra de herramientas antiphishing para navegadores Web. Además, nunca revelar información personal o financiera confidencial a menos que y hasta que se pueda confirmar que la solicitud de dicha información es legítima.

- Cuando los clientes realizan actividades de Internet de alto riesgo, como transacciones bancarias o compras en línea, deben hacerlo desde sus computadoras y no desde computadoras públicas. Además, es recomendable no almacenar contraseñas o números de tarjetas de crédito/débito.

- Revisar la información bancaria con frecuencia para identificar las actividades irregulares.

- Tener en cuenta que los riesgos de seguridad pueden instalarse automáticamente en las computadoras mediante programas de uso compartido de archivos, descargas gratuitas y versiones freeware y shareware de software.

- Evitar hacer clic en enlaces o archivos adjuntos en mensajes de correo electrónico o textos de Mensajería Instantánea, puesto que estos también pueden exponer los equipos a riesgos innecesarios.

- Leer cuidadosamente los acuerdos de licencia de usuario final (EULAs) y comprender todos los términos antes de aceptarlos ya que se pueden instalar algunos riesgos de seguridad después de que un usuario final haya aceptado los EULA o como consecuencia de esta aceptación.

- Tener cuidado con los programas que presentan anuncios en la interfaz de usuario. Muchos programas de spyware realizan un seguimiento sobre la forma cómo los usuarios responden a estos anuncios y su presencia es una advertencia. Estos anuncios pueden ser spyware.

Acerca de Security Technology and Response

La organización Security Technology and Response (STAR) de Symantec, que incluye Security Response, es un equipo mundial de ingenieros de seguridad, analistas de amenazas e investigadores que ofrecen funcionalidades, contenido y soporte para todas las soluciones de seguridad de consumo y empresariales de Symantec. Con centros de respuesta globales ubicados alrededor del mundo, STAR monitorea informes de códigos maliciosos de más de 130 millones de sistemas en Internet, recibe datos de 240,000 sensores de redes en más de 200 países y rastrea más de 32,000 vulnerabilidades que afectan más de 72,000 tecnologías de más de 11,000 fabricantes. El equipo utiliza toda esta inteligencia para desarrollar y ofrecer la protección de seguridad más completa del mundo contra las amenazas actuales y emergentes.

Acerca de Symantec Global Intelligence Network

Symantec ha establecido algunas de las más completas fuentes de datos en el mundo sobre las amenazas a Internet a través de Symantec Global Intelligence Network (Red Global de Inteligencia de Symantec). Esta red captura información de inteligencia de seguridad que le brinda a los analistas de Symantec fuentes de data incomparables para identificar, analizar, brindar protección y comentarios sobre tendencias emergentes en ataques, actividad de códigos maliciosos, phishing y spam. Más de 240,000 sensores en más de 200 países monitorean los ataques a través de una combinación de productos y servicios de Symantec, así como datos adicionales provenientes de terceros.

Acerca de Symantec

Symantec es líder mundial en soluciones de seguridad, almacenamiento y administración de sistemas que ayudan a las empresas y consumidores a proteger y administrar su mundo activado por la información. Nuestro software y servicios protegen contra más riesgos en más puntos, en forma más completa y eficiente, lo que permite que sea confiable el lugar donde se usa o almacena la información. Visite www.symantec.com/la para más información.

Más información sobre este reporte: www.symantec.com/la/gin

[i] *http://www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/the_downadup_codex_ed2.pdf and http://www.symantec.com/security_response/writeup.jsp?docid=2008-112203-2408-99*
[ii] *http://www.symantec.com/connect/sites/default/files/the_downadup_codex_ed1_0.pdf : p. 16*
[iii] *http://www.symantec.com/connect/blogs/brazilian-msn-worm-looks-familiar*
[iv] *http://www.symantec.com/security_response/writeup.jsp?docid=2003-071710-2826-99*
[v] *http://www.eff.org/deeplinks/2009/07/lula-and-cybercrime*
[vi] *http://www.foreignpolicyjournal.com/2009/11/15/brazils-next-battlefield-cyberspace/*
[vii] *Todos los costos están en dólares americanos*
[viii] *https://forums2.symantec.com/t5/malicious-code/Downadup-Geo-location-Fingerprinting-and-piracy/ba-p/380993*
[ix] *http://eval.symantec.com/mktginfo/enterprise/white_papers/ent-whitepaper_symantec_internet_security_threat_report_v.pdf : p. 11*
[x] *http://www.symantec.com/security_response/writeup.jsp?docid=2006-071111-0646-99*
[xi] *http://www.symantec.com/security_response/writeup.jsp?docid=2008-042106-1847-99*