Informe

McAfee

Informe de McAfee sobre amenazas: Primer trimestre de 2009

Elaborado por McAfee® Avert® Labs

Índice

El *Informe de McAfee sobre amenazas* le trae las últimas novedades en estadísticas y análisis relacionados con las amenazas que llegan por el correo electrónico y por la Web. Este informe trimestral ha sido elaborado por los investigadores de los laboratorios McAfee Avert Labs, cuyo personal, repartido por todo el mundo, ofrece una perspectiva única del panorama de las amenazas, desde consumidores a empresas y desde los Estados Unidos a países de todo el mundo. Acompáñenos mientras examinamos las principales cuestiones de seguridad de los tres últimos meses. Una vez que haya terminado con el presente informe, podrá encontrar más información en el Centro de amenazas de McAfee: http://www.mcafee.com/us/threat_center/default.asp, o www.trustedsource.org.

En el primer trimestre de 2009, hemos asistido a muchos cambios significativos en el panorama de las amenazas, si lo comparamos con lo que veíamos hace un año o incluso hace pocos meses. Doce meses atrás, nadie habría previsto que los volúmenes del spam descenderían, pero, con el cierre de McColo en noviembre de 2008, eso es exactamente lo que ha sucedido. Los niveles de spam siguen estando un 30% por debajo de sus valores máximos y no se ha producido el incremento habitual en el mes de marzo. La cuestión no es *si* el spam volverá a alcanzar sus niveles anteriores, sino *cuándo*. Existen datos sobre la creación de nuevos zombis y botnets que sugieren que no falta mucho.

La creación de sitios Web maliciosos va en aumento, al igual que la de sitios que albergan malware, de los que a diario aparecen miles. Cada día se crean nuevas formas de malware, y el presente informe detalla las que han alcanzado los mayores niveles de frecuencia.

El gusano Conficker, cuyo nombre oficial es "W32/Conficker.worm", ha recibido tanta atención como cualquier amenaza de seguridad de la historia reciente. Este informe ofrecerá cierta perspectiva respecto a si dicha atención es exagerada o está justificada. También nos centraremos en las amenazas que no reciben el mismo nivel de atención por parte de los medios de comunicación, pero que, de hecho, podrían ser más peligrosas que sus equivalentes más conocidas.

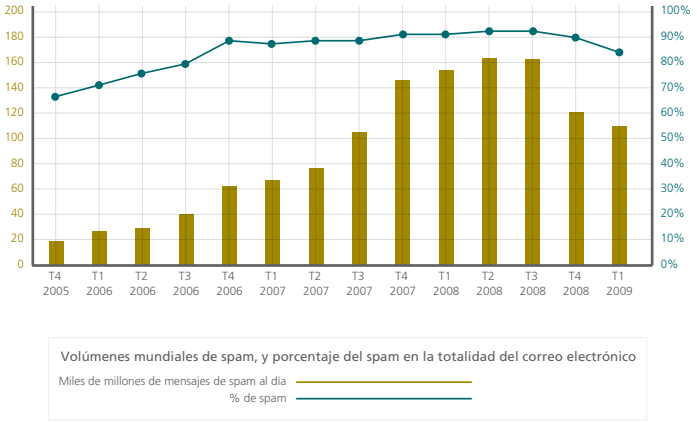
La geografía del panorama de las amenazas continúa evolucionando. Este informe ofrece un análisis de las aportaciones a las amenazas por procedencia geográfica, con indicación del origen del spam, la creación de zombis y las ubicaciones de los sitios de malware, además de identificar los agentes emergentes en el negocio de la creación de amenazas. El informe también facilita algunos detalles interesantes que sugieren que los países que crean las amenazas no vacilan en usarlas contra entidades ubicadas dentro de sus fronteras.

Por último, dirigiremos la cámara hacia nosotros mismos y echaremos un vistazo a algunos de los vaticinios que hicimos en nuestro *Informe de predicciones de amenazas 2009*, publicado en enero, para ver si se están materializando, y cómo. Los aspectos destacados incluyen el uso de los sitios de noticias y de redes sociales para propagar las amenazas a los usuarios desprevenidos.

El spam: sigue siendo un motivo de preocupación global

¿Qué recesión?

Los volúmenes globales de correo electrónico y spam para el primer trimestre de 2009 se hallan a unos niveles que no se veían desde hace casi dos años. ¿Será que los remitentes de spam han seguido los pasos del resto de la economía y han entrado en recesión? En realidad no es ésta la cuestión. Lo que de verdad está pasando es que los niveles de spam aún no se han recuperado del todo del cierre de McColo, que tuvo lugar en noviembre de 2008. Comparados con el mismo trimestre del año anterior, los volúmenes son un 20% más bajos en 2009, y un 30% más bajos que en el tercer trimestre de 2008, que registró los más altos hasta la fecha. Los volúmenes de spam se han recuperado aproximadamente en un 70% desde que se desconectó el host de spam, pero todavía no han alcanzado sus niveles anteriores.



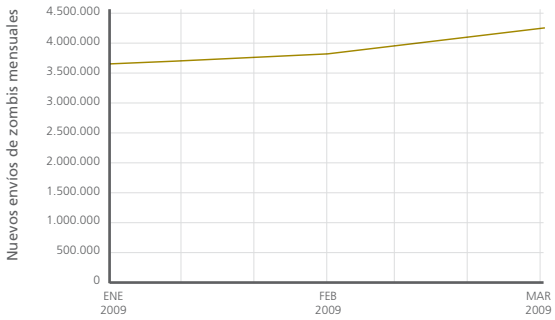
En años recientes, el mes de marzo ha batido récords en los volúmenes de correo electrónico, pero este marzo está lejos de comportarse de esta forma. El año pasado vimos una media de 153.000 millones de mensajes diarios, mientras que en este marzo la media ha sido sólo de unos 100.000 millones.

El porcentaje de spam respecto al correo electrónico total ha caído por debajo de la marca del 90%, un nivel que no veíamos desde 2006. Durante todo el año 2008, el spam supuso un 90% del volumen total de correo electrónico, mientras que en el último trimestre la media ha sido del 86%. Aunque las cuentas de correo y su actividad varían considerablemente, estimamos que los usuarios están recibiendo entre seis y doce veces menos mensajes de correo electrónico diarios que el año pasado.

Estamos convencidos de que los volúmenes de spam recuperarán sus niveles de 2008, pero la reorganización de los centros de mando y de las botnets tras el cierre ha tardado más de lo que muchos vaticinaron en el momento de producirse el cierre. En última instancia, para los remitentes de spam es una cuestión de rentabilidad, como en cualquier negocio.

Los nuevos zombis ponen en marcha la línea de producción

En el trimestre pasado detectamos cerca de doce millones de nuevas direcciones IP que funcionan como "zombis", ordenadores que están bajo el control de los remitentes de spam y otras personas. Esto supone un incremento significativo, casi un 50%, respecto a los niveles del último trimestre de 2008. El tercer trimestre de 2008 también arrojó una cifra récord de nuevos zombis, pero en este trimestre ha sido superado en un millón. Y, aunque los niveles de spam aún no se hayan recuperado del cierre de McColo, el nivel de actividad de los nuevos zombis indica que los remitentes de spam se están esforzando por recuperar la infraestructura perdida y que los volúmenes no tardarán en volver a los niveles anteriores.



Podemos desglosar los sistemas infectados por países. Durante el último trimestre, el 63% de los nuevos zombis ha pertenecido a los diez principales países. Esta cifra supone un ligero descenso respecto a los dos trimestres anteriores. Parece ser que los remitentes de spam están recurriendo a equipos de un mayor número de países para contribuir a sus esfuerzos.

1er. trim. 2009		4º trim. 2008		3er. trim. 2008	
País	**Porcentaje de IPs**	**País**	**Porcentaje de IPs**	**País**	**Porcentaje de IPs**
Estados Unidos	18,0	China	15,8	China	20,4
China	13,4	Estados Unidos	15,4	Estados Unidos	16,5
Australia	6,3	Alemania	6,5	Alemania	6,8
Alemania	5,3	Reino Unido	6,0	Reino Unido	6,0
Reino Unido	4,7	Brasil	4,9	Brasil	4,8
Brasil	4,0	España	4,3	España	3,7
India	3,1	Australia	4,1	India	2,5
España	3,0	Italia	3,5	Rusia	2,4
Corea del Sur	2,8	Rusia	3,1	Corea del Sur	2,4
Rusia	2,5	Corea del Sur	2,4	Italia	2,2
Total	**63,3**	**Total**	**66,0**	**Total**	**67,5**

China y los Estados Unidos se han estado disputando el primer puesto durante los tres últimos trimestres y ocupan una posición dominante en cuanto al número de equipos zombi que se encuentran bajo el control de los remitentes de spam. Un candidato notorio es Australia, que en el tercer trimestre de 2008 no estuvo entre los diez primeros. En dos trimestres, ha dado un salto vertiginoso hasta ocupar la tercera posición, con un 6% de todos los nuevos zombis. Las antípodas están demostrando ser un suelo fértil para el reclutamiento de zombis.

1er. trim. 2009		4º trim. 2008	
País	**% del total**	**País**	**% del total**
Estados Unidos	35,0	Estados Unidos	34,3
Brasil	7,3	Brasil	6,5
India	6,9	China	4,8
Corea del Sur	4,7	India	4,2
China	3,6	Rusia	4,2
Rusia	3,4	Turquía	3,8
Turquía	3,2	Corea del Sur	3,7
Tailandia	2,1	España	2,4
Rumanía	2,0	Reino Unido	2,3
Polonia	1,8	Colombia	2,0
	70,0		**68,3**

El spam por países: Estados Unidos, de nuevo líder mundial

Es posible que los fabricantes de automóviles estadounidenses tengan problemas de producción y ventas, sin embargo, el spam procedente de este país sigue en el primer puesto, con un 35% de la producción mundial. Aunque los centros de operaciones de control del spam constituyen una infraestructura internacional, los remitentes siguen prefiriendo utilizar ordenadores de los Estados Unidos para fabricar el spam. Los diez principales países dominan en cuanto a producción de spam, aportando cerca de un 70% del total, a mucha distancia de los otros más de 200 países del mundo.

Si observamos los dos últimos trimestres, vemos que la India es el país que ha mostrado un mayor incremento porcentual, y aporta ahora casi el 7% del spam global. Su producción de spam ha aumentado a casi el doble respecto al trimestre anterior. Quizá el spam sea el último sector económico en probar suerte con la subcontratación en la India.

También tenemos que dar la bienvenida a los diez primeros puestos a Tailandia, Rumanía y Polonia. Estos datos respaldan la idea de que los remitentes de spam están buscando por todas partes nuevas fuentes para alimentar sus motores de spam.

1er. trim. 2009		4º trim. 2008		3er. trim. 2008	
Medicamento con receta	25,0	Medicamento con receta	37,0	Alargamiento del pene	31,2
Publicidad	21,9	Publicidad	19,3	Publicidad	19,3
Réplica de producto	18,8	Alargamiento del pene	16,8	Medicamento con receta	10,7
Alargamiento del pene	17,5	DSN	9,5	Tormenta	8,0
DSN	7,1	Contactos	3,9	DSN	7,7
Tormenta	1,6	Réplica de producto	2,6	Últimas noticias	6,7
Diploma	1,1	Empleo	1,7	Réplica de producto	6,0
Software	1,1	Software	1,5	Préstamos para deudas	1,6
Préstamos para deudas	1,0	Préstamos para deudas	1,2	Banca	1,1
Otros	4,9	Otros	6,5	Otros	7,7
	100,0		**100,0**		**100,0**

El spam por tipos: sexo, medicamentos y mucho más

El spam sobre temas como alargamientos de pene, medicamentos con receta y publicidad en general continúa ocupando uno de los primeros puestos entre los tipos de spam enviados. Estos tres tipos, por sí solos, representan aproximadamente el 60% del spam enviado durante los tres últimos trimestres. Parece como si el eslogan "sexo, drogas y rock 'n' roll" conservara su vigencia. O casi. Quizá hayamos crecido un poco; hoy la frase es "sexo, medicamentos y economía".

El spam sobre copias de productos (en su mayoría sobre relojes falsos) ha dado un salto notable en este trimestre, aportando casi el 19% del spam total. Este tipo de spam sobre copias ha sido popular durante el pasado año, pero también ha mostrado un crecimiento significativo en este trimestre. Esto sugiere que, en tiempos de crisis, los remitentes de spam nos ayudan a estirar nuestra capacidad de compra descubriendo para nosotros buenas gangas en imitaciones baratas.

El spam de notificación del estado de la entrega sigue representando un uniforme 8% del spam total. Estos mensajes están casi siempre asociados a phishing y adoptan la forma de una aparente notificación de devolución una vez que la dirección de correo de la víctima ha sido manipulada. Está claro que el phishing sigue vivito y coleando. Muchos de estos mensajes son de índole económica e intentan obtener los datos personales del usuario.

Los remitentes de spam no respetan la soberanía de ningún país, incluido el suyo

Dentro de la comunidad de la ciberseguridad, existe el mito de que los delincuentes online —de los que se cree que un porcentaje significativo residen en Europa Oriental— prefieren atacar objetivos de países occidentales y evitan atacar a usuarios o empresas de su jurisdicción local. Empezamos a observar datos que lo desmienten. Internet no conoce fronteras geográficas. Ahora resulta evidente que los ciberdelincuentes atacan cualquier objetivo para el que se presenta la oportunidad. Hemos visto pruebas de que estos delincuentes virtuales han puesto en grave peligro algunos organismos públicos y empresas clave en Rusia y en Europa Oriental, así como a algunos altos funcionarios de dichas entidades.

Recientemente, McAfee TrustedSource™ ha observado correo electrónico y spam con malware que tiene su origen en una serie de organismos públicos e instituciones bancarias rusas. Según nuestro análisis, los bancos rusos comprometidos son:

- Rusfinance Bank
- OGO Bank
- Tusarbank
- Link Capital Investment Bank
- The Maritime Bank
- Vladivostok Alfa Bank
- Bank Eurotreid
- Bank Voronezh
- Bashcreditbank
- Enisey's United Bank
- Inter-Svayz Bank

Nuestros datos indican asimismo que los sistemas informáticos de las oficinas de la Administración rusa están controlados por bandas de ciberdelincuentes:

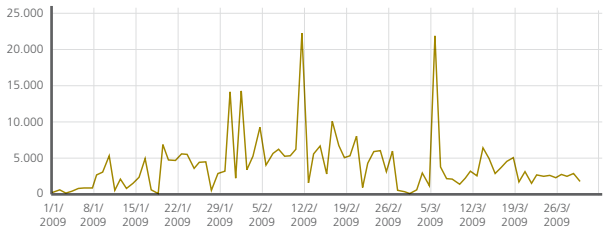
- Ministerio de Fiscalidad de la región de Nazran
- Red de Internet del Estado Ruso
- Instituto Regional de Finanzas y Economía
- Instituto Conjunto para la Investigación Nuclear
- Centro médico del Departamento del Presidente de la Federación Rusa
- Fondo de Pensiones de la Federación Rusa
- Red Personal de los Tribunales de la Federación Rusa
- Comunicaciones móviles chechenas JSC

Estos datos sobre Rusia sugieren que los ciberdelincuentes tienden a no discriminar en cuanto a sus objetivos, y atacan a cualquier organización que tenga para ellos interés económico o de otro tipo. Aunque está claro que Rusia lidera este tipo de actividad (y el tremendo volumen de spam que produce), nuestro análisis muestra el mismo tipo de actividad en otros países de la antigua Unión Soviética, como Ucrania, Belarús, Armenia, Azerbaiyán, Georgia, Kazajstán, Kirguistán, Moldova, Tayikistán, Turkmenistán y Uzbekistán.

Web: todos los días aparecen nuevos sitios Web con reputación de maliciosos

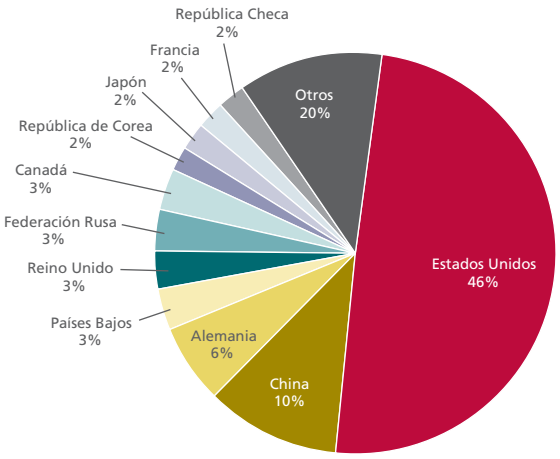
Durante el primer trimestre hemos asistido a una continuación de muchas de las amenazas que se presentaron durante el cuarto trimestre, pero con mayor intensidad. Aunque los medios de comunicación hayan dedicado casi toda su atención a Conficker, esto no significa que haya sido la única amenaza que ha alcanzado difusión durante el primer trimestre. Aun sin tener en cuenta los datos de actividad de Conficker, acabamos con un ligero aumento de la actividad respecto al mismo período del año anterior y con un incremento claro respecto a los trimestres anteriores. El asunto de los antivirus no fiables ha causado bastante preocupación en la Web, junto con los aumentos de la actividad de timos y phishing.

Los gráficos y datos de esta sección no incluyen los dominios maliciosos con los que Conficker debía ponerse en contacto, salvo el gráfico "Distribución de sitios Web con reputación de maliciosos". Aunque constituyen una parte importante del panorama de las amenazas, los datos de Conficker distorsionan la imagen global de la actividad maliciosa. Hay muchas otras amenazas cuya difusión está creciendo. Los autores de malware y los timadores aprovechan los problemas económicos y nuestras inquietudes para impulsar una serie de sitios fraudulentos. Sus estrategias incluyen formas de evitar la ejecución de hipotecas y sitios de phishing sobre cualquier cosa que se nos pueda ocurrir; incluso ofrecen tarjetas de bonificaciones de las tiendas. Los sitios de antivirus no fiables siguen a la caza de usuarios desprevenidos. Y los métodos para atraer usuarios a los sitios Web siguen evolucionando. Aun sin tener en cuenta la actividad de Conficker, las URL que cruzan la línea divisoria de los niveles de reputación "maliciosos" (o "rojos") han aumentado notablemente respecto a los dos últimos trimestres de 2008.



Sitios con reputación de maliciosos que aparecen diariamente

¿Dónde están ubicadas estas URLs con mala reputación en la Web? No donde la mayoría de la gente cree.



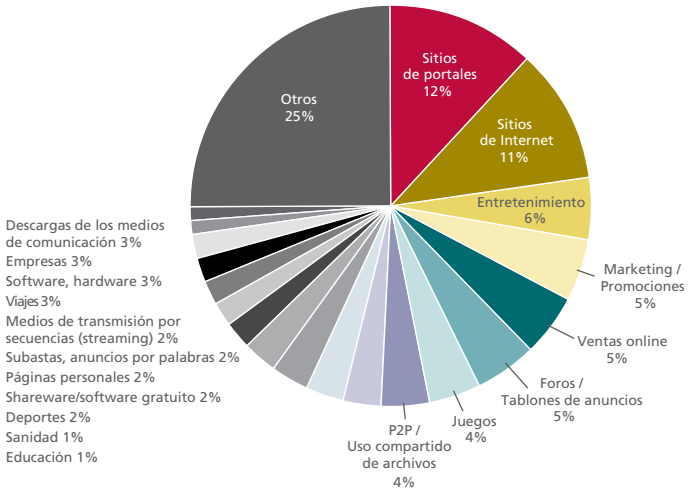
Distribución de sitios Web con reputación de maliciosos

¿Por qué ese cambio repentino en lo que muchos han considerado "la norma" (Estados Unidos, Rusia, China) de la actividad maliciosa en la Web?[1]. Esto no quiere decir que algunos de estos países tengan menos URLs con reputación de maliciosas, sino el mayor crecimiento en otros países. Gran parte de este crecimiento tiene que ver con los lugares en los que Conficker ha alojado algunos de los dominios que piensa contactar o que ha contactado. De hecho, por sí solo, ha colocado a los Países Bajos en situación de empate en el cuarto puesto. Si bien los Países Bajos llevan tiempo siendo una opción popular para el alojamiento de URL de phishing, Cornficker ha sido un salto significativo en cuanto a sitios Web infectados por malware y demás contenidos maliciosos. Pero no todo el cambio puede atribuirse a Conficker. Canadá se ha estado abriendo camino hacia los 10 primeros puestos por alojar servidores Web maliciosos, y esto se centra principalmente en el malware y el spyware distribuidos desde esos sitios.

Una lección importante que podemos extraer, no obstante, es la frecuencia con que estos mismos países aparecen en varios vectores de ataque, como sitios maliciosos, sitios que alojan spyware/adware, phishing y spam. De hecho, los 7 primeros países en alojamiento de sitios Web con reputación de maliciosos se encuentran entre los 10 primeros que alojan sitios de phishing, de spam y de malware/spyware.

1. En el tercer trimestre de 2008, la clasificación era la siguiente: Estados Unidos tenía el 41%; China el 12%; Rusia el 7%; Alemania y los Países Bajos el 5%; Corea del Sur el 4%; Hong Kong el 3%; Taiwán, Canadá y la República Checa el 2%, y otros países el 17%).

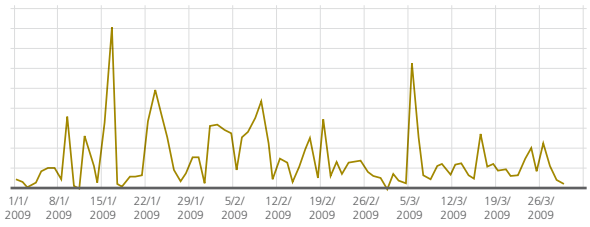
Los sitios con reputación de maliciosos varían considerablemente en sus objetivos, ya sean legítimos, dudosos o fraudulentos. Seguirá corriendo mayor riesgo al visitar un sitio de pornografía o de apuestas que no esté asociado a una empresa reconocida y legítima. No obstante, cualquier sitio es vulnerable, y cualquier tipo de contenido al que un usuario desee acceder es una oportunidad que los distribuidores de malware pueden explotar.



Las 20 principales categorías legítimas a las que TrustedSource concede la reputación de "sito Web malicioso"

Este trimestre, los servidores de contenidos han visto aumentar su popularidad de cara a los distribuidores de malware como herramienta para los contenidos maliciosos e ilegales. Hemos observado esta tendencia tanto en sitios ubicados en (y gestionados por) proveedores acreditados y muy respetados como en otros menos conocidos y más cuestionables. Cuando esta amenaza se combina con el uso extendido de blogs y con la optimización de los motores de búsqueda, es más importante que nunca que todo ordenador cuente con una seguridad Web completa.

Hemos hablado del *dónde*, hablemos ahora de los *tipos* de amenazas de los que hay que preocuparse. Aparte de Conficker, ha sido un trimestre de mucha actividad en cuanto a los nuevos malware y exploits disponibles en la Web.

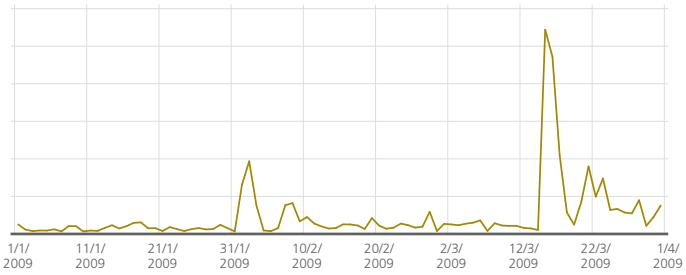


Nuevos sitios Web que envían malware y ventanas emergentes

La tabla anterior ofrece una imagen del número de sitios Web que distribuyen malware y programas potencialmente no deseados (PUP), detectados en este trimestre por la red McAfee TrustedSource. (La tabla muestra los sitios que alojan malware y refleja el tráfico de usuarios a dichos sitios. La tabla no incluye los sitios legítimos que son utilizados para dirigir a los usuarios a los sitios de malware. Además,

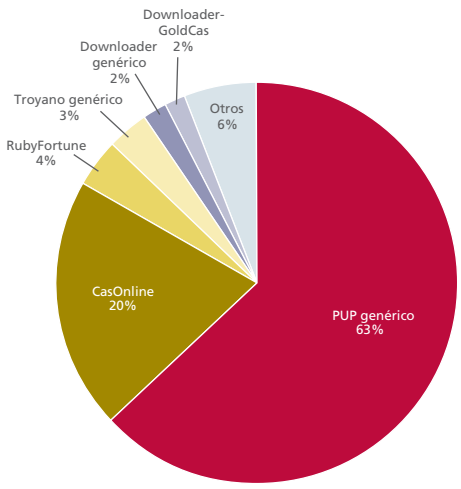
hemos eliminado de esta tabla nuestra investigación proactiva a fin de ofrecer una visión real de las nuevas amenazas exclusivas disponibles en el curso de la navegación normal, ya sea en el colegio, en el trabajo o en casa.)

En contraste, las siguientes tablas ilustran lo que ha encontrado nuestra metodología proactiva respecto a las nuevas descargas de malware únicas distribuidas por los diversos sitios Web. Vemos algunos picos interesantes allí donde se han encontrado "minas" de descargas maliciosas o nuevos PUPs.



Descargas de malware y de ventanas emergentes, identificadas de forma proactiva (por día)

Nuestras observaciones proactivas —exploración regular y verificación de sitios Web, además de métodos exclusivos de prospección de información maliciosa adicional— han mostrado un pico enorme en nuevas descargas de malware relacionadas con casinos hacia finales de enero y principios de febrero, además de un pico en PUPs genéricos hacia el final del trimestre. Esta actividad corresponde a los cuatro tipos principales de descarga de malware durante el trimestre. (Ver tabla siguiente.) Otro malware de interés es la presencia continuada del troyano Vundo, cuya actividad aumentó en los tres últimos meses.

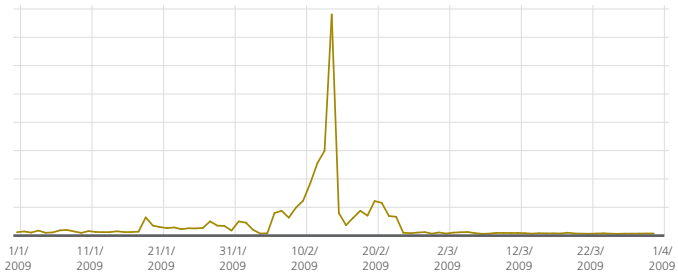


Prevalencia de descargas de malware y de ventanas emergentes, por tipo

Una de las amenazas amorfas de la Web a las que nos enfrentamos es el *exploit*, término que puede significar muchas cosas, a menudo diferentes, para investigadores y para usuarios. Los laboratorios McAfee Avert Labs controlan las nuevas páginas que alojan exploits de navegadores mientras examinamos y supervisamos la Web, e identificamos con regularidad las nuevas vulnerabilidades de seguridad de los navegadores. Cuando los navegadores (y sus complementos) no se mantienen al día,

estas "cajas de arena" pueden convertirse fácilmente en el terreno de juego de un autor de malware. Una vez que este autor se hace con la vulnerabilidad, el equipo del usuario puede recibir código de programación que permite las infecciones por adware, el registro de pulsaciones y otras actividades maliciosas.

Cuando los navegadores (y sus complementos) no se mantienen al día, estas "cajas de arena" pueden convertirse fácilmente en el terreno de juego de un autor de malware.

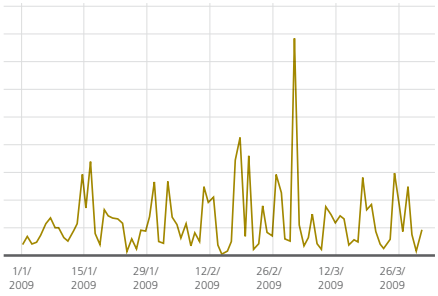


Sitios Web que alojan exploits de navegadores

Actividad de las herramientas de anonimato

Los autores de malware están haciendo un mayor uso de los ataques de URLs redirigidas, ya sea por medio de anonimizadores o de una interfaz Web 2.0 que utilice un servidor de contenidos. Esto puede ser para evitar la detección normal (actuando como URL incrustada y no como URL original) o para aprovechar la reputación del sitio que aparece como distribuidor del malware.

Un anonimizador es una herramienta que oculta la identidad de un usuario mientras éste se encuentra online. La mayoría de ellos no son maliciosos y, por tanto, no se incluyen en nuestras anteriores exposiciones sobre los riesgos de seguridad. Sin embargo, el uso de uno de ellos puede abrir la puerta a un ataque de "intermediario", en el que un anonimizador malicioso o secuestrado inyecta código en los mensajes que viajan, en una u otra dirección, entre el usuario y el servidor. Esto no sólo pone en peligro al usuario, sino también a los hosts y redes que, de otra forma, estarían protegidos. En su conjunto, la actividad de anonimizadores ha aumentado en este trimestre respecto al anterior. También se ha producido un ligero aumento de la actividad de este trimestre respecto al mismo período del año anterior.

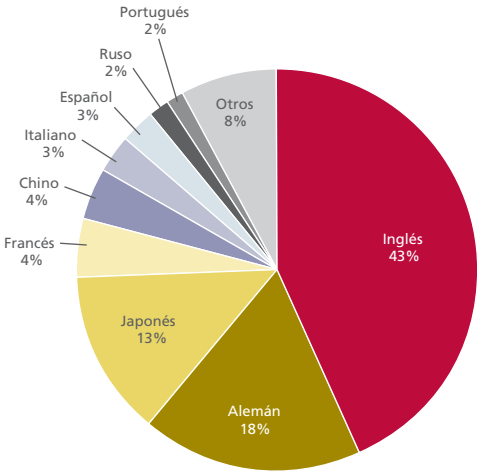


Nuevos anonimizadores por día

Tendencias generales en la Web

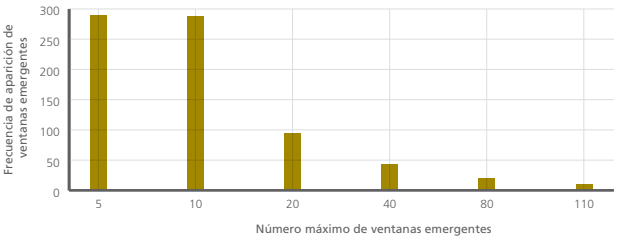
La Web es una comunidad global. Basta ver las conexiones en cualquier sitio de redes profesionales o sociales. El número de páginas Web continúa creciendo constantemente para dar soporte a más idiomas. Los mismos ataques a blogs que aparecen en sitios de alto perfil en los Estados Unidos se difunden también por blogs chinos, brasileños y muchos otros. Y los ataques actuales emplean una red extensa.

Además, dado que los distribuidores de malware se aprovechan del conocimiento de las marcas por parte del público (como en el caso de grandes acontecimientos deportivos y el uso de malware incluido en la programación de torneos y en archivos JPG de los jugadores), hacen uso de las marcas globales para atacar a los usuarios en todos los idiomas.



Distribución de idiomas en Web Content

El factor molestia de las ventanas emergentes sigue en vigor. Es interesante que, a pesar de los bloqueadores de ventanas emergentes y otras herramientas similares, la mayoría de los sitios Web continúan utilizándolas. El número máximo de ventanas emergentes que hemos visto en un sitio Web es de 116.



Distribución de ventanas emergentes en sitios que contienen al menos cinco.

Es necesario someter a las empresas presentes en la Web al mismo escrutinio que a un vendedor ambulante.

Seguimos observando un uso extendido de URL Web 2.0 y comerciales legítimas para la propagación de malware. Hace diez años o más, bastaba con mantenerse alejados de determinados contenidos para estar seguros, pero hoy las amenazas parece que nos encuentran, con independencia de las páginas en las que naveguemos. Cualquier sitio Web que pueda ser explotado (por medio de cualquiera de las numerosas vulnerabilidades existentes) lo será. Habitualmente, los administradores de sitios Web pueden ver análisis que intentan explotar una vulnerabilidad en su servidor. Lo interesante es la elevada frecuencia de dichos análisis procedentes de sitios y servidores asociados a todo tipo de cosas, desde el software ilegal y los sitios maliciosos hasta los anonimizadores. Si un sitio Web de mucho tráfico es vulnerable, la cuestión no es si será explotado, sino cuándo.

Hemos observado un aumento notable de los timos en la Web. Nuestra previsión es que seguirán aumentando a medida que los estafadores aprovechen las inquietudes de la población mundial por medio del spam y la Web. A menudo es muy difícil discernir si una organización es legítima. Es necesario someter a las empresas presentes en la Web al mismo escrutinio que a un vendedor ambulante. Es necesario que los usuarios sepan que, una vez que han facilitado a un timador los datos de su tarjeta de crédito para una donación o un falso servicio online, pueden decir adiós a esos datos.

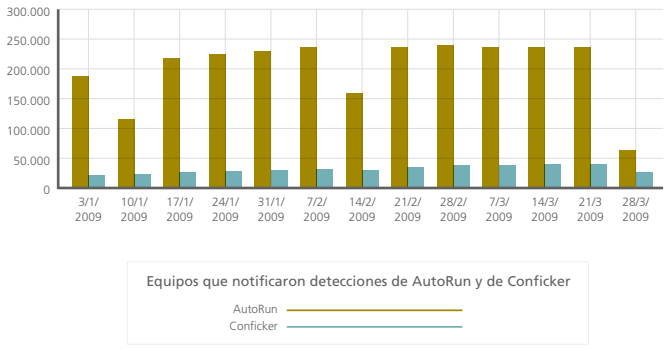
No obstante, nuestra investigación permite albergar alguna esperanza para la economía. Los sitios de inmobiliarias han mostrado un incremento notable en su crecimiento este trimestre, rompiendo la barrera de las 10 principales categorías de contenidos disponibles para los usuarios (y desplazando a los deportes).

Malware: la exageración de Conficker frente a la realidad de AutoRun

En los últimos meses, ha habido muchas historias acerca de Conficker. Podría parecer que se trata de la única amenaza por la que vale la pena preocuparse. Pero cuando analizamos las cifras, vemos que no es así. Conficker no es exactamente el día del juicio final.

Desde luego, Conficker ha sido un ejemplo importante de malware por muchas razones. Ha infectado a muchos hosts. Ha sido desarrollado, mantenido y debatido activamente. Pero las detecciones no son tantas como cabría esperar de un malware que ha recibido tanta atención.

Por otra parte, en este trimestre hemos visto malware preocupante. La historia es diferente para el malware basado en AutoRun, que en su mayoría utiliza unidades USB o memoria flash para reproducirse y que se ha observado en números mucho mayores que Conficker durante este trimestre. Comparémoslos:



En los últimos 30 días, menos del 10% de todas las detecciones notificadas han sido gusanos AutoRun. Conficker empezó en un 1% aproximadamente y esta cifra se ha multiplicado por 12, pero aún así representa menos del 15% del número de detecciones de gusanos AutoRun en el pico de este último.

Actualización de las predicciones

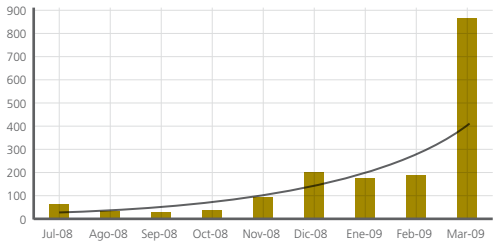
A comienzos de 2009, los laboratorios McAfee Avert Labs publicaron sus *Predicciones de amenazas 2009*[2]. Varias de nuestras estimaciones se han materializado en este trimestre.

El fuego amigo produce bajas

En la última década, uno de los principales vectores de amenazas —la recepción de virus de personas que conocemos— cayó en desuso en gran medida. Sin embargo, la Web 2.0 ha revitalizado este método de ataque de la vieja escuela. Durante este trimestre, muchas variantes de Koobface tomaron por sorpresa a miles de usuarios que recibieron el virus de sus amigos de Facebook. Sin que las víctimas lo supieran, los enlaces asociados a los mensajes enviados por el virus conducían a sitios Web que

2. Centro de amenazas de McAfee Avert Labs. http://www.mcafee.com/us/local_content/reports/2009_threat_predictions_report.pdf

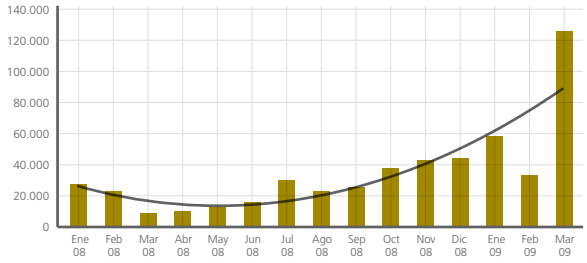
distribuían el gusano. Poco después, sus equipos contraían el virus y enviaban mensajes infectados a su círculo de amistades. Las redes sociales siguen ofreciendo a los atacantes un vector popular para los ataques de ingeniería social.



Binarios Koobface únicos

Red global mundial no fiable

En febrero, la plataforma Facebook fue explotada por atacantes que crearon con ella aplicaciones no fiables. Muchos usuarios picaron e instalaron dichas aplicaciones. Los hechos se divulgaron en los medios de comunicación, lo que llevó a los laboratorios McAfee Avert Labs a descubrir una banda masiva de optimización de motores de búsqueda que tomaba como objetivos los principales términos de búsqueda en Google. Los atacantes no sólo robaron de los sitios populares material protegido por derechos de autor, sino que también hicieron mal uso de otros sitios populares, como Democrats.org, para inflar sus puestos dentro de la clasificación de Google. El objetivo de los atacantes al optimizar los resultados de las búsquedas era instalar software antivirus no fiable. Éste fue un caso de aplicación Facebook no fiable, que condujo a resultados no fiables de las búsquedas, que condujeron a software de seguridad no fiable. Estos incidentes ponen de relieve la necesidad de que los usuarios naveguen de forma segura.

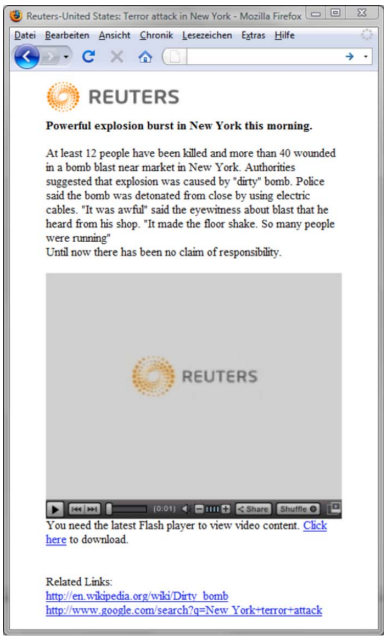


Binarios antivirus únicos no fiables

Las amenazas hablan el mismo idioma que usted

Los atacantes saben que cuanto más relevante y dentro de contexto sea un ataque, mayores son las probabilidades de que una persona reaccione: que haga clic en un enlace, que facilite un nombre de usuario y contraseña, que instale una aplicación. Las historias de sucesos que tienen lugar en nuestro vecindario tienen más probabilidades de llamar nuestra atención que cuando los mismos se producen en una parte remota del mundo. En febrero y en marzo, los ciberdelincuentes autores del virus Waledac explotaron este concepto. Las confiadas víctimas fueron atraídas a sitios Web adaptados a la ubicación geográfica de aquéllas, lo que les prestaba una pátina de autenticidad. Mientras los usuarios leían las "noticias locales", el sitio Web intentaba discretamente instalar el virus mediante código de exploit desapercibido.

Blog de los laboratorios McAfee Avert Labs



Google y el mal uso de los motores de búsqueda

Google. El nombre significa muchas cosas diferentes para muchas personas diferentes. Para quienes buscan trabajo, es una forma de encontrar las ofertas más recientes. Para los empresarios, es una forma de encontrar personal cualificado en Internet. Para los que van de compras, es una herramienta eficaz para localizar los productos que necesitan a precios atractivos. Para los autores de malware y los ciberdelincuentes, es una herramienta cada vez más efectiva para distribuir malware y dedicarse a la ciberdelincuencia. Cuando nos paramos a pensar que los motores de búsqueda representan una proporción muy grande de la actividad en Internet, parece lógico que los autores de malware estudien formas de hacer un mal uso de su potencia como método de distribución de su mercancía. Para ver muestras de este tema, eche un vistazo a estas entradas del blog de McAfee Avert:

- http://www.avertlabs.com/research/blog/index.php/2009/03/15/democratsorg-cans-the-spam/
- http://www.avertlabs.com/research/blog/index.php/2009/03/10/democratsorg-blog-spam-contributes-to-google-search-poisoning/
- http://www.avertlabs.com/research/blog/index.php/2009/02/27/google-bucking-the-trend/
- http://www.avertlabs.com/research/blog/index.php/2009/02/25/google-trends-abused-to-serve-malware/
- http://www.avertlabs.com/research/blog/index.php/2009/01/07/google-code-project-abused-by-spammers/
- http://www.avertlabs.com/research/blog/index.php/2009/01/17/do-not-worry-obama-di-not-refuse-to-be-a-president/

Teniendo en cuenta la potencia combinada de la indexación y las palabras clave más populares con el incentivo del dinero fácil para los ciberdelincuentes, es de suponer que este tipo de mal uso continuará.

La economía y el miedo

Los problemas de la economía global siguen inquietando a mucha gente. Otros se ven aquejados por cuestiones de seguridad y terrorismo. Para los autores de malware y los ciberdelincuentes, resulta fácil convertir estos temores en beneficios. Esta tendencia económica, que estaba incluida entre nuestras Predicciones de amenazas 2009, sin duda ha sido aprovechada durante todo este trimestre de muchas formas inquietantes. El miedo es un poderoso motivador cuando lo usan los ciberdelincuentes como cebo de ingeniería social:

- http://www.avertlabs.com/research/blog/index.php/2009/03/16/breaking-news-waledac-terror-attack-in-a-city-near-you/
- http://www.avertlabs.com/research/blog/index.php/2009/02/23/malware-riding-on-the-tides-of-the-economic-crisis/
- http://www.avertlabs.com/research/blog/index.php/2009/02/06/cybercrime-online-threats-and-the-recession/
- http://www.avertlabs.com/research/blog/index.php/2009/01/05/one-hacker-may-conceal-another/
- http://www.avertlabs.com/research/blog/index.php/2009/01/20/fake-antivirus-and-a-real-threat/
- http://www.avertlabs.com/research/blog/index.php/2009/01/29/hoax-or-not-treat-it-the-same/

Los timos, el spam y el phishing funcionan muy bien en los buenos tiempos; tanto más en los malos. Recuerde siempre que los delincuentes leen las mismas noticias que leemos los demás, y que utilizarán los titulares y los sucesos contra nosotros a menos que nos mantengamos alerta.

Acerca de los laboratorios McAfee Avert Labs

Los laboratorios McAfee Avert Labs son el equipo de investigación mundial de McAfee, Inc. Con unos equipos de investigación dedicados en exclusiva al malware, los programas potencialmente no deseables, las intrusiones en los host y en las redes, el malware en los dispositivos móviles y la divulgación ética de vulnerabilidades, los laboratoriora McAfee Avert Labs disfrutan de una amplia visión sobre la seguridad. Esta amplia visión permite a los investigadores de McAfee mejorar continuamente las tecnologías de seguridad y proteger mejor al público.

Acerca de McAfee, Inc.

McAfee, Inc., con sede en Santa Clara, California, es la empresa más grande del mundo dedicada a la tecnología de la seguridad. McAfee está decididamente comprometida a hacer frente a las peores amenazas de seguridad del mundo. La compañía ofrece soluciones y servicios proactivos y de demostrada eficacia que ayudan a proteger sistemas y redes en todo el mundo y que permiten a los usuarios conectarse a Internet, navegar y hacer compras en la Web sin peligro. Respaldada por un equipo de investigación galardonado, McAfee crea productos innovadores que dotan a usuarios particulares, empresas, sector público y proveedores de servicios de la capacidad de demostrar el cumplimiento de las normativas, proteger los datos, evitar interrupciones, identificar vulnerabilidades y supervisar continuamente la seguridad, además de mejorarla.http://www.mcafee.com/es.

McAfee®

McAfee, Inc.
Avenida de Bruselas nº 22.
Edificio Sauce.
28108 Alcobendas. Madrid.
888 847 8766
www.mcafee.com/es

5395rpt_avert_quarterly-threat_0409