



2010 Informe de amenazas

Documento técnico de Websense®

ÍNDICE

Introducción	3
Aspectos destacados de la investigación de la Red Threatseeker® de Websense®, 2010	4
Descripción general	
Resultados estadísticos clave	
Seguridad Web Seguridad de email Seguridad de datos	
Eventos significativos en 2010	6
Malware: trucos y traición	8
Problemas de la Web	14
Tentaciones del email	15
Peligros para los datos	18
Redes sociales: La gran imagen, los grandes riesgos	20
Websense Security Labs™: Principales descubrimientos 2010	25
Los próximos 12 meses	28
Resumen	29

INTRODUCCIÓN

Websense® Security Labs™ utiliza la Red ThreatSeeker® de Websense para descubrir, clasificar y monitorear las amenazas y tendencias globales de Internet. Este sistema cuenta con la primera red de Internet HoneyGrid™ del mundo y utiliza cientos de tecnologías, que incluyen honeyclients, honeypots, sistemas de reputación, aprendizaje automático, y sistemas avanzados de cómputo en grid, para analizar más de mil millones de piezas de contenido por día en busca de amenazas de seguridad.

La Red Threatseeker escanea más de 40 millones de sitios Web por hora en busca de código malicioso, y casi 10 millones de emails en busca de contenido no deseado y código malicioso. Utiliza más de 50 millones de sistemas de recolección de datos en tiempo real para monitorear y clasificar contenido Web, de email y de datos. Junto con Websense Advanced Classification Engine, un motor de clasificación de contenidos avanzado e incorporado en las soluciones Websense, la Red ThreatSeeker proporciona a Websense una visibilidad inigualable del estado del contenido de Internet y email.

Este informe resume los descubrimientos significativos de los investigadores de Websense mediante el uso de la Red ThreatSeeker durante 2010.

RED THREATSEEKER DE WEBSENSE ASPECTOS DESTACADOS DE LA INVESTIGACIÓN 2010

Descripción general

El panorama de la Web continuó evolucionando durante 2010. Los sitios Web más visitados se separaron del resto por su contenido y funcionalidad y la mayoría tiene ahora una presencia más dinámica desde el punto de vista social. En 2010, los piratas informáticos adaptaron sus estrategias para centrarse en la Web social y dinámica. Los ataques se volvieron más combinados, sofisticados y dirigidos. Muchos de estos ataques utilizaron nuevos trucos y métodos de entrega. Fueron comunes los ataques basados en secuencias de comandos, las campañas de email combinadas y el envenenamiento en la optimización de motores de búsqueda (search engine optimization, SEO). Incluso las amenazas y las botnets detectados con mayor facilidad fueron redireccionados con éxito. La mayoría de los ataques en 2010 tuvo el mismo propósito: el robo de datos.

El nuevo lema podría haber sido: “¡Buscadores de la Web, estén atentos!”, ya que los piratas informáticos dedicaron gran parte de su tiempo a comprometer sitios Web legítimos. Los titulares de último momento y las novedades de entretenimiento continuaron siendo el blanco de los ataques SEO. Los antivirus falsos combinados con el envenenamiento SEO fue una técnica comúnmente utilizada. Los ataques de email se redireccionaron con éxito con archivos HTML y PDF, mientras que resultó un poco más fácil reconocer los ataques tradicionales de phishing.

El año 2010 no sólo presencié la continua sofisticación de los delincuentes informáticos, sino también el ajuste de las estructuras organizacionales en las que operan. Las luchas territoriales entre las organizaciones de delincuencia informática continuará desarrollándose en lo que literalmente se ha transformado en una economía clandestina totalmente operativa.

Resultados estadísticos clave

Seguridad Web

- Websense Security Labs identificó un aumento del 111.4% en el número de sitios Web maliciosos entre 2009 y 2010.
- El 79.9% de los sitios Web con código malicioso eran sitios legítimos que habían sido comprometidos; un aumento del 3% con respecto al período anterior.
- La búsqueda de las últimas novedades y noticias actuales representó un mayor riesgo (22.4%) que la búsqueda de contenido censurable (21.8%).
- Estados Unidos fue el país que más sitios de phishing alojó en 2010.

Seguridad de email

- El 84.3% de los mensajes de email fueron spam; una reducción del 0.7% con respecto al año pasado.
- El 89.9% de todos los emails no deseados en circulación durante este período contenían vínculos a sitios de spam o a sitios Web maliciosos; un aumento del 4% con respecto a 2009.
- La categoría Compras continuó siendo el tema principal de spam (12%), aunque descendió un 13%. Esto se relaciona estrechamente con las tendencias económicas de consumo, ya que la recesión provocó que algunos compradores redujeran el consumo.

El **79.9%** de los sitios Web con código malicioso eran sitios legítimos que habían sido comprometidos.

El **84.3%** de los mensajes de email eran spam.

El **52%** de los ataques de robo de datos ocurrieron en la Web.

- También fueron populares los emails del tipo 'pump and dump' (10%) y los relacionados con educación (9%). El spam 'pump and dump' tiene por objeto hacer que las víctimas compren acciones para subir de manera artificial el precio de las mismas y generar una ganancia para los spammers que compraron las acciones a bajo precio.
- El 9% de los ataques de robo de datos se realizaron en el email.

Seguridad de datos

- Estados Unidos fue el país n.º1 donde el malware se conectó a la Web.
- pc-optimizer.com fue el primer host de código de robo de datos en 2010.
- El 52% de los ataques de robo de datos ocurrieron en la Web.
- Las inquietudes sobre la pérdida accidental de datos se han convertido en un problema prioritario para muchas organizaciones en 2010.
- Estados Unidos y China continuaron siendo los dos países que alojaron la mayor cantidad de crimeware y recibieron la mayor cantidad de datos robados durante 2010. Los Países Bajos se ubicaron dentro de los primeros cinco países de la lista.

EVENTOS SIGNIFICATIVOS EN 2010

Stuxnet: ataque físico 1.0

“Stuxnet tiene las mismas capacidades operatorias que un avión furtivo”.

Ali Mesdaq, Investigador de Seguridad de Websense

La mayoría de las amenazas modernas tienen por objeto obtener una ganancia financiera. En junio de 2010, el mundo presenció lo que se considera el primer ataque importante diseñado específicamente para atacar los sistemas de Control de Supervisión y Adquisición de Datos (Supervisory Control and Data Acquisition, SCADA). Los sistemas SCADA están diseñados para controlar y monitorear diversos procesos dentro de los sistemas industriales. El gusano específico de Windows utilizó diversos ataques del día cero dirigidos al software WinCC/PCS 7 SCADA de Siemens. Se diseminó a través de unidades flash USB infectadas y luego utilizó otras vulnerabilidades para atacar computadoras WinCC basadas en redes. Una vez que ingresó en el sistema, utilizó contraseñas predeterminadas para dominar el software.

Lo que diferenció a Stuxnet de los otros ataques producidos durante 2010 fue el nivel de sofisticación, el hecho de que estaba orientado específicamente a infraestructura esencial, y la ubicación geográficamente específica del evento. Muchos de los ataques estaban orientados a las instalaciones en Irán. Si bien el ataque salió a la superficie en otros países, una gran parte de los ataques se produjo en instalaciones nucleares críticas en Irán. La precisión operativa de los ataques fue estelar y las ubicaciones del ataque han originado especulaciones sobre la identidad de los responsables del ataque.

Arrestos de Zeus: un joven de 20 años usa una computadora portátil para robar 20 millones de dólares y un cuaderno de papel para contar el dinero

Diecinueve personas de Europa del Este fueron arrestadas en septiembre por alzarse con \$3 millones por mes con la ayuda de Zeus, un troyano diseñado para robar información bancaria. El grupo utilizaba a Zeus para infiltrarse silenciosamente en las computadoras que tenían sistemas de seguridad deficientes. Una vez adentro, esperaban que las víctimas se conectaran a diversos bancos específicamente elegidos. Luego, robaban las credenciales de los usuarios y las enviaban al servidor del grupo. Esta organización criminal también utilizó a Zeus para manipular sesiones de navegación en la Web donde Zeus pedía a los usuarios que revelaran información adicional confidencial.

La policía de Londres estimó que más de 600 cuentas fueron afectadas, lo que provocó una pérdida de alrededor de \$20 millones. El líder de la organización era un joven de 20 años que manejó gran parte de la operación desde una computadora portátil en su apartamento de tres dormitorios en el Reino Unido. Usaba un cuaderno de papel y un lápiz para contar el dinero.

Operación Aurora: la amenaza moderna para el email, la Web y los datos

Durante diciembre de 2009 y enero de 2010 circularon noticias de ataques provenientes de China en perjuicio de numerosas compañías. El blanco de los ataques incluía a Adobe, Google, Rackspace, Northrop Grumman, Dow Chemical y a los gobiernos de Alemania y Francia. La suposición inicial era que los ataques se realizaban con archivos PDF maliciosos, hasta que Microsoft publicó información que afirmaba que los ataques se realizaban con una nueva vulnerabilidad de seguridad en Internet Explorer (CVE-2010-0249). Hasta este momento, la mayoría de los ataques había incluido típicamente adjuntos de email (por ej., archivos PDF, Microsoft Word, Excel o PowerPoint) que se enviaban a personas en organizaciones específicas. La vulnerabilidad en Internet Explorer era muy similar a otras vulnerabilidades que hemos visto en el explorador de Microsoft, en el sentido de que permitía que el atacante realizara una descarga oculta de malware ('drive-by'). Esto significa que el sistema de un usuario puede estar

comprometido simplemente por visitar un sitio Web o ver un email HTML especialmente redactado. El ataque Aurora pone de manifiesto que podría ser sólo cuestión de tiempo antes de que veamos más ataques en gran escala que utilizan la nueva vulnerabilidad.

Igualmente alarmante es el hecho de que este ataque reveló que hay muchas organizaciones que continúan utilizando exploradores tan antiguos como Explorer 6.0. Examinamos las estadísticas de visitantes a nuestro sitio Web websense.com y los resultados fueron sorprendentes. Internet Explorer 6.0 resulta ser el segundo explorador más popular, y representa el 19.6% de todas las visitas.

Ataques a WordPress: la mayor plataforma de blogs del mundo sigue recibiendo ataques

Las plataformas de blogs siempre han sido vulnerables a ataques. Y nuestra investigación muestra que el 56% de todos los blogs comprometidos reciben más de un ataque. WordPress, la plataforma de software de blogs más utilizada del mundo (utilizada por más de 13.9 millones de blogs), fue atacada en numerosas oportunidades durante 2010. Si bien WordPress lanza nuevas versiones aproximadamente tres veces al año, nuestra investigación muestra que muchas personas utilizan versiones mucho más antiguas del software. Se sabe que existieron numerosas vulnerabilidades durante el auge de los ataques. GoDaddy (que aloja 43 millones de dominios y otros sitios de alojamiento) vio ataques persistentes en 2010. Otro punto notable es que cuando los blogs de personajes famosos son atacados, muchas personas suponen que esto significa una desfiguración pública o un intento de difamar el estado de la celebridad. Si bien esto sucede en ocasiones, la mayoría de los ataques tienen por objeto una ganancia financiera.

Hospital de Massachusetts pierde 800,000 archivos de datos

En julio, el hospital South Shore de Massachusetts anunció públicamente la pérdida de 800,000 archivos que incluían 15 años de información financiera y de salud de pacientes, socios comerciales, proveedores, personal y voluntarios. La información perdida variaba de una persona a otra, pero incluía lo siguiente: nombre completo, dirección, número de teléfono, fecha de nacimiento, número del Seguro Social, número de licencia de conducir, número de historia clínica, número de paciente, información sobre cuentas bancarias, números de tarjeta de crédito, y diagnóstico médico y registros de tratamientos. Después de investigar el incidente, el hospital eligió no ponerse en contacto con ninguna de las personas potencialmente afectadas por la pérdida. La Oficina del Fiscal General de Massachusetts cuestionó la decisión del hospital y expresó que los consumidores afectados debían recibir una notificación individual en relación con la pérdida de los datos. La Oficina del Fiscal General continúa monitoreando e investigando las acciones del hospital referentes a la pérdida de datos y a la respuesta dada.

Piratas informáticos dejan al descubierto más de 100,000 registros de iPad de clientes de AT&T

En junio, una organización de delincuentes informáticos llamada "Goatse" logró aprovecharse de una falla de seguridad a través de una aplicación Web de AT&T. La falla puso al descubierto las direcciones de email de usuarios de iPad 3G. Muchos medios de alto rango y también miembros del gobierno y del ejército que formaban parte del programa de adopción temprana de Apple figuraban en la lista. También quedó expuesta la información perteneciente a numerosos miembros del equipo de investigación avanzada del Departamento de Defensa de EE. UU. Websense cree que Apple continuará siendo un blanco de ataque, ya que la masificación del consumo de sus productos florece rápidamente en muchos entornos laborales.

MALWARE: TRUCOS Y TRAICIÓN

“La codicia sólo está limitada por la propia imaginación. Los encargados de tomar decisiones de seguridad en la actualidad deben entender lo que esto significa, o perderán”.

Stephan Chenette, Investigador de Seguridad de Websense.

En 2010, el objetivo central de los autores de malware continuó siendo hacer dinero. La creciente sofisticación de sus esquemas ha cambiado en tal medida el panorama de amenazas que la mayoría de las personas no entiende realmente contra qué están intentando defenderse. Las máquinas y las redes ya no son el centro de atención de los autores de malware. Las memorias USB y las redes sociales son mecanismos muy abusados para lograr una ganancia financiera. La naturaleza dinámica de la Web comparada con lo que se está ofreciendo geográficamente cambia a cada hora.

Una de las mayores equivocaciones es creer que la protección antivirus es suficiente. Nuestra investigación reafirma que los atacantes actuales prueban previamente su malware con las principales soluciones antivirus en forma rutinaria. Si bien el antivirus es una herramienta necesaria, las firmas se han convertido en sólo una parte de un problema mucho mayor. La seguridad en tiempo real ha pasado a ser el blanco de ataque del pirata informático moderno.

Nuestras estadísticas muestran que el 22.4% de los resultados de búsquedas en tiempo real relacionadas con entretenimiento conducen a un vínculo malicioso.

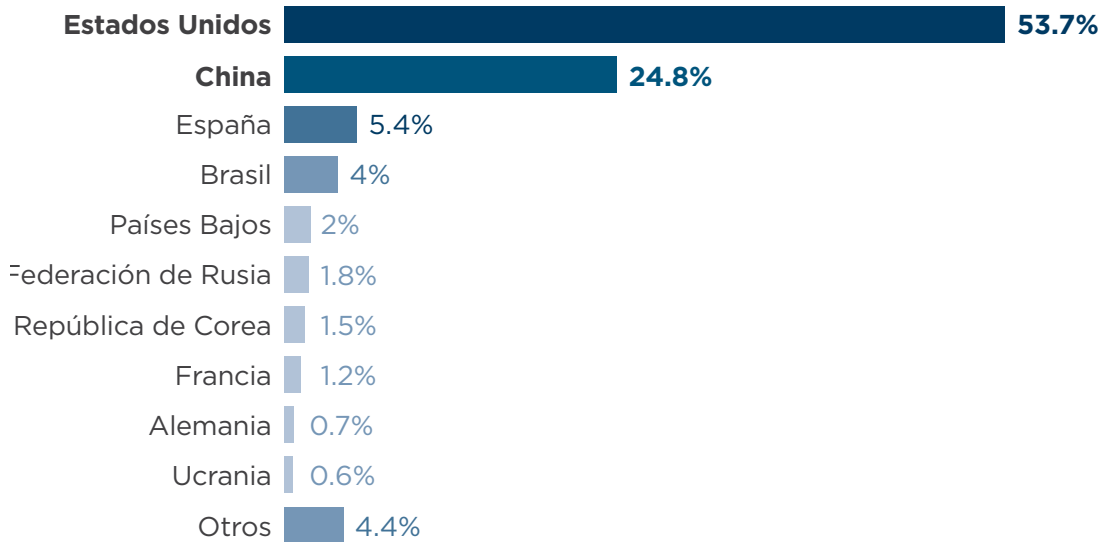
El tiburón nada donde la foca juega. El envenenamiento SEO continuó siendo una de las tendencias más significativas durante 2010, ya que los autores de malware se concentraron en las novedades de entretenimiento y las últimas noticias. Los terremotos en Haití y en Chile, la muerte de Corey Haim y la Copa Mundial de Fútbol fueron algunos ejemplos de resultados de motores de búsqueda manipulados de manera inteligente para conducir a las personas a vínculos falsos con mejores calificaciones que los resultados legítimos. Igual a lo que encontramos en 2009, las botnets detrás de estas campañas son redireccionadas una vez que la campaña ilegítima es eliminada de los resultados de los motores de búsqueda.

Muchos de los ataques SEO de 2010 fueron de naturaleza combinada, con un segundo componente que consistía en un antivirus falso (otra tendencia que vimos el año pasado). Ambos enfoques utilizaban campañas antivirus falsas que ofrecían escaneos gratis que identificaban infecciones falsas. Después de notificar sobre un virus falso, se pedía a los usuarios que descargaran un software antivirus gratis, donde un segundo escaneo les pedía información sobre su tarjeta de crédito para poder eliminar el malware falso.

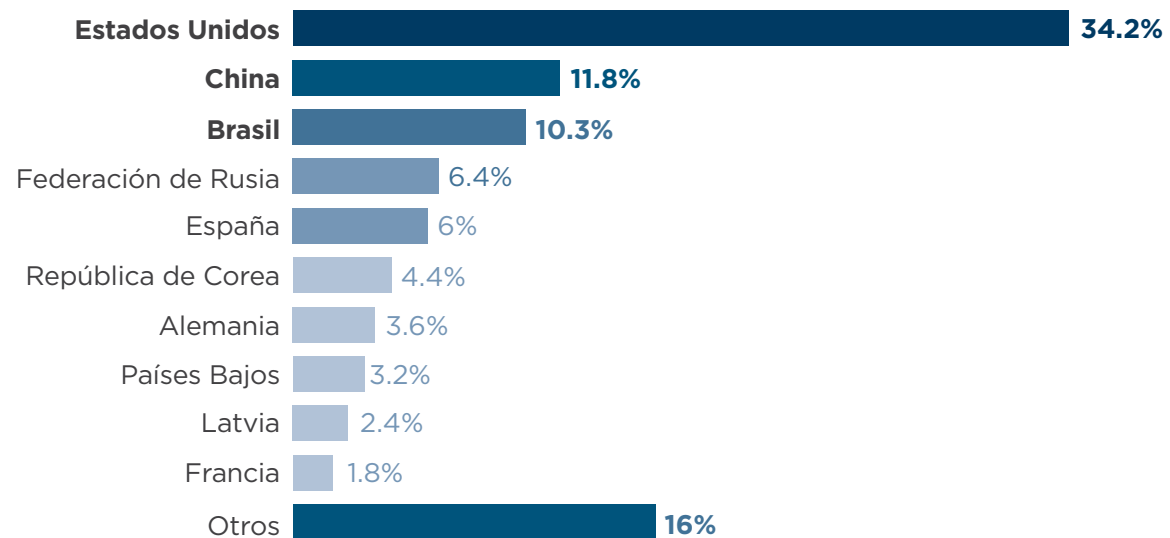
En febrero descubrimos una nueva tendencia en ciertos ataques. Muchos resultados SEO afectados parecían tener archivos PDF en los resultados de los vínculos. Esto resultó exitoso para el ataque, ya que muchas personas lo vieron como una forma de autenticidad.

Nuestras estadísticas muestran que el 22.4% de los resultados de búsquedas en tiempo real relacionadas con entretenimiento conducen a un vínculo malicioso.

Los 10 países principales donde el malware se conectó a la Web en 2010



Los 10 países principales que alojaron crimeware* en la Web en 2010



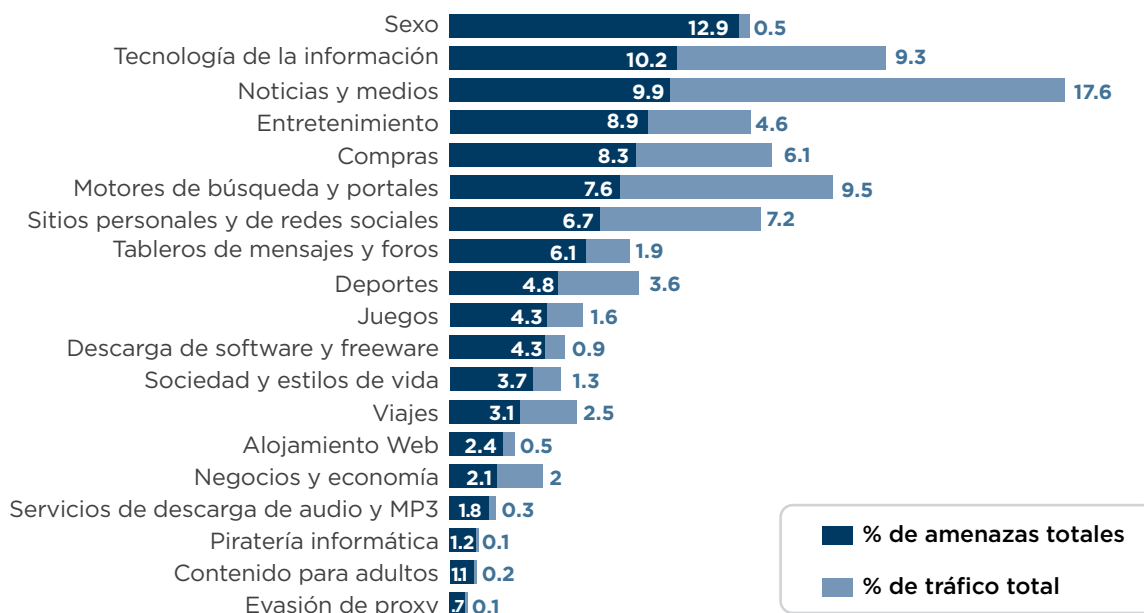
*El crimeware es un tipo de malware que se utiliza específicamente para el crimen informático.

La ruta al malware a través del análisis de los vínculos

Los usuarios de computadoras no visitan sitios Web infectados deliberadamente; por lo tanto, un delincuente informático necesita alguna forma de gancho o incentivo para que el usuario se sienta atraído a visitar un sitio infectado. Esto es lo que con frecuencia se denomina el elemento de “ingeniería social” del delito informático. Basados en nuestro análisis de datos en 2010, describimos qué tipo de patrón de conducta del usuario probablemente lo lleve a quedar expuesto a un software malicioso.

Websense tiene la capacidad de escanear cualquier página en busca de vínculos maliciosos. Se utilizó esta tecnología para analizar el tráfico desde el servicio Web alojado de Websense. Es posible que las páginas Web que contienen vínculos maliciosos no sean una amenaza en sí mismas, pero la existencia de vínculos maliciosos significa que el usuario está a un clic de distancia de un sitio malicioso.

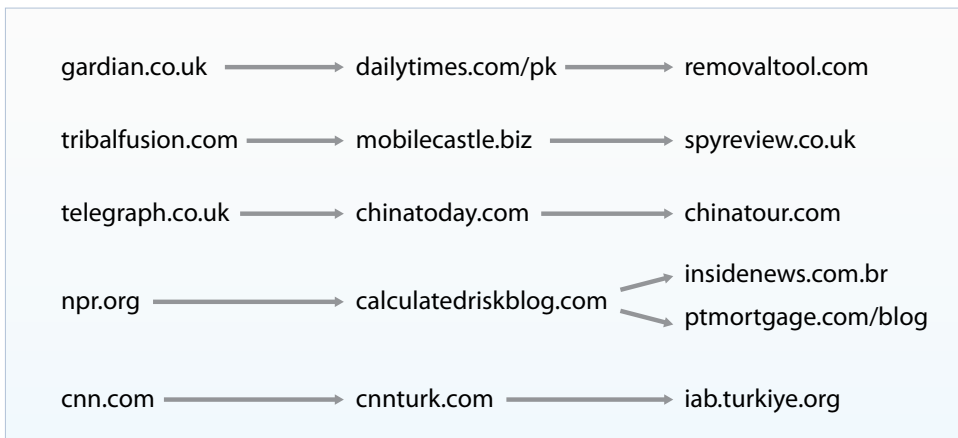
El gráfico siguiente muestra el número de páginas visitadas que contienen vínculos maliciosos para una muestra de tráfico Web alojado obtenida durante 2010.



El contenido explícitamente sexual ha presentado siempre un riesgo para las organizaciones. Para una empresa promedio, la mayor exposición a contenido malicioso proviene del acceso al contenido explícitamente sexual. Esto es así, aun cuando representa un pequeño porcentaje del total del contenido visitado.

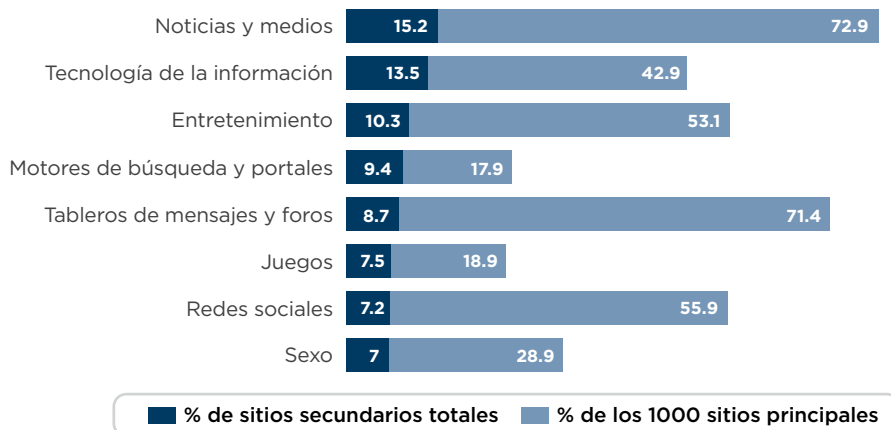
La exposición a sitios que contienen vínculos infectados significa que los usuarios están a un clic de distancia de la infección (sitios principales [parent sites]). Para poder caracterizar los sitios que estaban a dos clics de una infección, examinamos el motor de búsqueda Google para identificar sitios que establecieran un vínculo con estos sitios principales (sitios secundarios [grandparent sites]).

El gráfico siguiente muestra ejemplos de cómo dos clics pueden pasar de la seguridad al peligro.



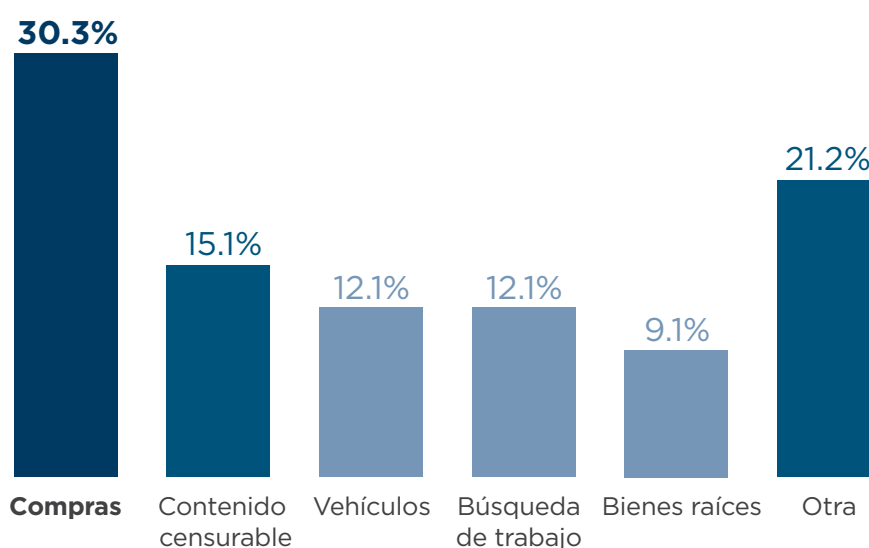
Los sitios que contenían spyware se infectaron en el momento de la investigación. Posiblemente ya no estén infectados.

El gráfico siguiente muestra la distribución de los sitios secundarios por categoría y el porcentaje de los 1000 sitios Alexa principales que fueron identificados a dos clics del malware.



Estos resultados muestran cómo la ruta al malware con frecuencia comienza en la Web recreativa. También muestran que la mayoría de los sitios con alta calificación están muy cerca del peligro.

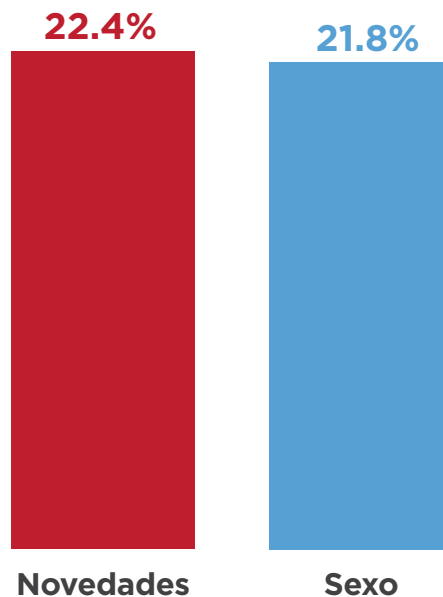
Websense proporciona la Nube ThreatSeeker® de Websense, que extiende la tecnología de seguridad de contenido de Websense y nuestra infraestructura global Security-as-a-Service (SaaS) a terceros, permitiéndoles integrar el análisis de seguridad de URL en sus productos. La Nube ThreatSeeker monitorea el contenido en forma constante en busca de amenazas. El gráfico siguiente muestra cómo analizamos los datos para identificar la categoría principal de sitios en las búsquedas de Google que devolvieron sitios maliciosos.



Como puede ver, las búsquedas no relacionadas con trabajo (por ej., Compras, Vehículos, Búsqueda de trabajo) representan el mayor riesgo de exposición al spyware. Las búsquedas relacionadas con Negocios y Tecnología de la información no representaron un riesgo significativo.

Las búsquedas no relacionadas con el trabajo representan el mayor riesgo de exposición al spyware.

Para continuar con esta investigación, se midieron los índices de infección para conjuntos de términos de búsqueda que incluían términos sexuales conocidos, términos populares de Google y Yahoo, y términos de negocios populares de bnet.com. A continuación se muestra el porcentaje de búsquedas infectadas:



Estos resultados demuestran que las últimas novedades representan un riesgo aun mayor que el contenido censurable. Lo particularmente preocupante es que algunas novedades actuales, como “la Copa Mundial 2014” y “Noticias de ABS-CBN” devolvieron búsquedas donde más del 25% de los sitios alojaba malware.

Ninguna forma de uso de Internet es completamente segura. Aun el acceso legítimo al contenido esencial para la función específica de nuestro puesto de trabajo puede exponer la red a amenazas. Estos datos no están ocultos en los oscuros rincones de la Web, sino que están accesibles a unos pocos clics de los sitios más prominentes.

Los resultados anteriores muestran que negar el acceso al contenido censurable puede reducir en gran medida la exposición a sitios maliciosos. También existe un gran riesgo con el uso no productivo de la Web. La naturaleza peligrosa de los sitios en vanguardia en Internet significa que la protección en las instalaciones que utiliza inspección del contenido ofrece un importante beneficio sobre la protección basada en firmas.

Las últimas novedades representan un riesgo que es aun mayor que el contenido censurable.

PROBLEMAS DE LA WEB

¿“A qué le deben temer más las organizaciones? Ya no es necesario ir hasta oscuros rincones de Internet para encontrar cosas malas”.

Patrik Runalid, Investigador de Seguridad de Websense

En 2010, la Web continuó siendo la principal ruta hacia el malware. Pareciera que nunca dejan de surgir sitios Web malintencionados, creados de manera inteligente y diseñados para dar la peor clase de problemas. Los autores de malware también trabajan del otro lado de la cerca, ya que secretamente alojan sus productos en sitios Web populares legítimos. Las personas ya no tienen que ir a oscuros rincones de Internet para encontrar amenazas. Si bien muchas personas que navegan la Web creen que pueden bajar la guardia cuando visitan sitios más respetables, se encontraron inyecciones de código SQL y publicidades maliciosas (malvertising) en sitios tales como The New York Times, Gizmodo y TechCrunch.

Incluso las búsquedas más comunes estaban repletas de veneno. Muchas organizaciones consideran a Google como uno de los lugares más seguros a los que sus empleados pueden recurrir para obtener información. Sin embargo, los usuarios ahora están recibiendo ataques con mayor frecuencia en los motores de búsqueda.

Los resultados de imágenes de la Web siempre mostraron una estrecha relación entre el material malicioso y el material para adultos. Nuestro análisis 2010 de las consultas sobre imágenes y videos de Bing Adult muestra que el 8.18% derivará en una página de resultados de búsqueda que contiene un vínculo malicioso. Nuestros resultados de la búsqueda de consultas sobre imágenes para adultos en Google fue aun más sorprendente. Encontramos que el 50.38% de las consultas arroja una página de resultados de búsqueda que contiene un vínculo malicioso. Nuestro análisis muestra que una vez que uno entra en el terreno del contenido censurable, el camino lo llevará hacia contenido aun peor.

¿Qué probabilidad hay de que la búsqueda de noticias actuales y palabras de moda conduzca al malware en 2010? **22.4%**

Porcentaje de incremento de sitios maliciosos: **aumento del 111.4% entre 2009 y 2010.**

¿Qué porcentaje de los 100 sitios Web más populares están categorizados como sitios de redes sociales o de búsqueda? **El 65% de los 100 sitios más populares y el 95% de los 20 sitios más populares.**

Porcentaje de sitios Web encontrados con código malicioso que son sitios legítimos comprometidos en comparación con los sitios configurados expresamente. **Total = 79.9% (relativamente estable)**

TENTACIONES DEL EMAIL

“El email lleva el problema a la puerta de su casa y el 75% de las veces el antivirus lo deja entrar a cenar. Es por eso que se requieren análisis de seguridad más avanzados que las firmas”.

Jon Crotty, Gerente de Marketing de Investigación de Websense

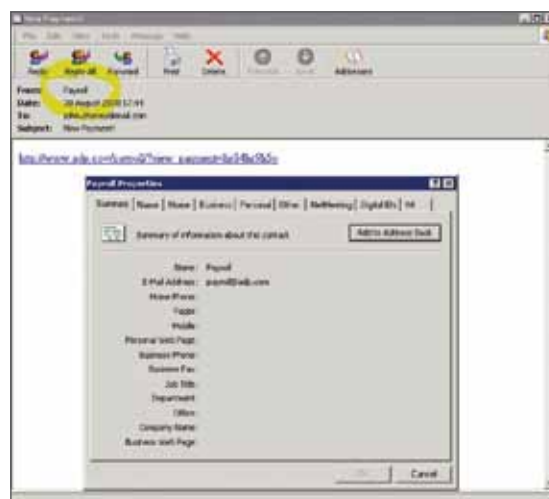
Al igual que otros vectores de amenazas, el objetivo central de los ataques de email ha sido siempre el mismo: entrar de la manera que se pueda y extraer todo lo que se pueda. Encontramos que si bien la creatividad que rodea a las amenazas combinadas y de email disminuyó a principio del año, las nuevas oleadas de ataques combinados están incorporando con éxito el email como punto de entrada. También vimos un flujo constante de nuevos trucos y técnicas. A mediados de 2010, la situación llegó al punto de que algunos de los destinatarios más entendidos no podían distinguir entre emails buenos y malos.

Los servicios de reputación resultan ineficaces, ya que el email desempeña un rol en el gran esquema de los ataques combinados de mayores dimensiones que también poseen componentes de Web y datos. Los piratas informáticos utilizan la naturaleza dinámica de la Web para diseñar estos ataques en tiempo real.

Los indicadores cuantificables no han cambiado demasiado desde una perspectiva histórica. Elementos tales como la cantidad de spam enviado, el volumen de distribución geográfica y los emails con vínculos maliciosos típicamente registran un crecimiento consistente de un solo dígito positivo o negativo, o ambos. En ocasiones, se registra una diferencia considerable en los números, pero en su mayor parte estas tendencias suben y bajan a un ritmo un tanto predecible. El componente más errático de la seguridad de email es la microtendencia dentro de estas categorías. La velocidad con la que los piratas informáticos están redireccionando sus campañas de email es asombrosa.

Los autores de email y malware criminal ponen mucho énfasis en las mismas noticias y tendencias. Se podría decir que operan a velocidades más rápidas que el tiempo real porque tienen la capacidad de planificar ataques operativos basados en el año calendario. No hubo nada que impidiera a las organizaciones criminales planificar campañas de spam combinadas para la Copa Mundial (blog de la Copa Mundial) con meses de anticipación. A menos que el “Patch Tuesday” – el segundo martes de cada mes cuando Microsoft publica sus parches de seguridad – (blog de estafa de Patch Tuesday) cambie a un viernes y que la temporada de impuestos (blog de estafa de la temporada de impuestos) comience en verano, la probabilidad de que el volumen y la potencia de este tipo de amenazas disminuya es muy pequeña.

Durante 2010 fueron frecuentes las estafas de envíos y nóminas de pago diseñadas de manera inteligente que involucraron a empresas tales como ADP, FedEx y UPS. Amazon.com y Buy.com también se utilizaron como fachadas en campañas de spam muy exitosas.



Las amenazas de email utilizadas para el robo de marcas en 2010 probaron que muchas organizaciones que no poseen soluciones de seguridad de contenidos unificada que ofrecen tecnologías de seguridad Web, de email y de datos son blancos fáciles de estos ataques. Hubo numerosos emails masivos que parecían ser de grandes empresas de marcas conocidas, como IKEA, Macy's, Best Buy, Target y Evite. Las campañas usaron un enfoque combinado que ofrecía la misma estrategia de antivirus falso utilizada comúnmente en ataques anteriores. En promedio, sólo uno de cada cuatro compañías de antivirus detectó las amenazas a las grandes marcas.

Después de estar oculto por corto tiempo, Gumblar volvió con todas sus fuerzas para suplantar a Amazon.com. El objetivo de la campaña era engañar a los usuarios desprevenidos para que visitaran una URL de cliente que ofrecía una explotación.

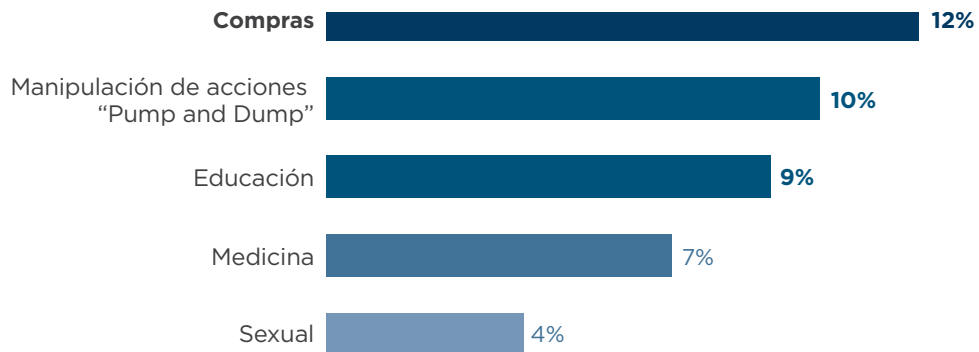
Del mismo modo que algunas de las campañas que presenciábamos en 2009, Zeus pasó por el radar en varias oportunidades. Los atacantes habían usado kits de Zeus para atacar al personal militar y del gobierno en EE. UU. y el Reino Unido. Una campaña pretendía ser del Consejo de Inteligencia Nacional (National Intelligence Council). Los piratas informáticos lo utilizaron para tentar a las víctimas a descargar un documento sobre el "proyecto 2020". Otra campaña estaba destinada al personal de la CIA y los atraían a descargar una "actualización" de Windows contra un ataque. En ambos casos, las víctimas que caían en la trampa encontraban que sus máquinas estaban infectadas con el malware Zeus.

Los troyanos como Zeus se venden como paquetes de explotaciones ("crimepacks") en los mercados clandestinos y son utilizados por una gran variedad de organizaciones criminales. Hay tantas variantes de spam relacionado con Zeus diseminado que es imposible que desaparezca. En el momento en que muchos usuarios comenzaban a comprender los ataques de email más recientes basados en vínculos, los piratas informáticos regresaron con técnicas más furtivas, como el aprovechamiento de archivos PDF y HTML explotados. Los cuerpos de estos emails y los trucos mismos son ahora mucho más atractivos estéticamente y más sofisticados.

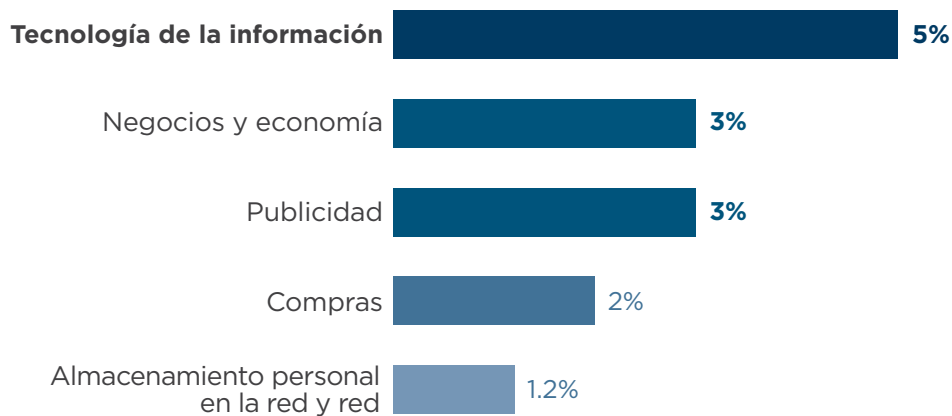


El volumen de spam durante 2010 continuó siendo el 84.3% de todos los emails. Esto permaneció relativamente estable. De hecho, en los dos últimos años sólo hubo una fluctuación del 3%. Durante 2010, el 89.9% de todos los emails no deseados (spam y maliciosos) contenía al menos un vínculo. Esto representó un aumento del 3% con respecto al año pasado.

Porcentaje de temas principales de spam por contenido de email



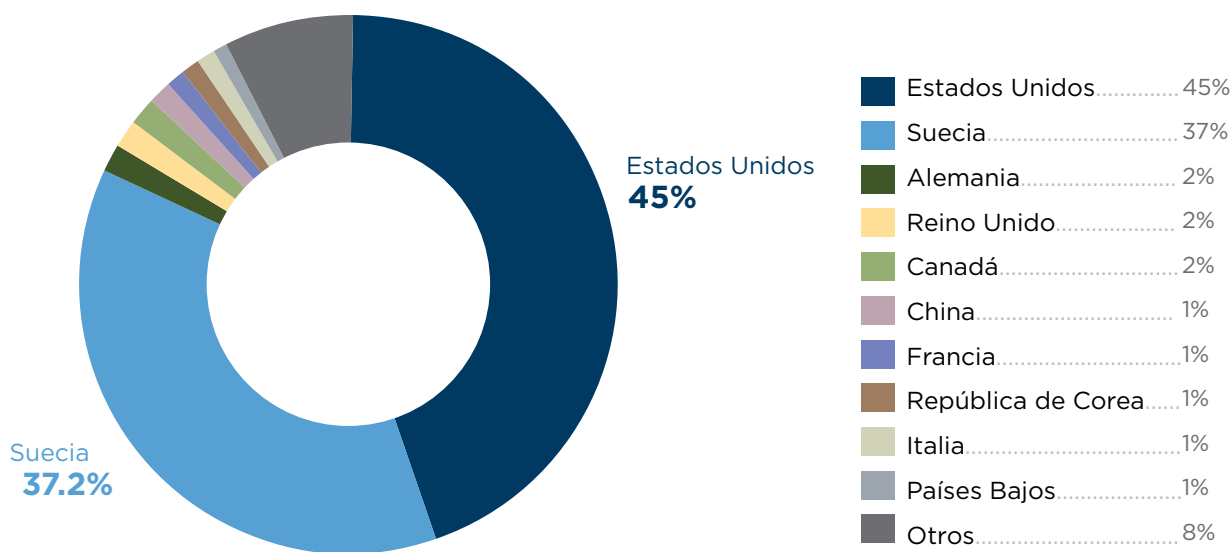
Porcentaje de temas principales de spam por categoría URL



El spam 'Pump and Dump' registró el mayor porcentaje de ganancias, ya que las personas esperaban capitalizarse en el mercado de valores en un clima económico incierto. Este tipo de spam típicamente promete más del 5% de ganancias pero, en realidad, produce pérdidas importantes ya que los spammers se preparan para vender estas acciones una vez enviado el spam. A diferencia de otras técnicas de spam con objetivos financieros (ganancias de loterías falsas y engaños de transferencia de cargos), al destinatario no se le pide que siga en contacto con el remitente.

Los ataques de phishing se acumularon y representaron el 0.6% de los mensajes de spam para contenido de email y el 0.1% para categorías URL. Esta tendencia está ahora en disminución porque muchos usuarios finales pueden reconocer estos tipos de amenazas. En pocas palabras, los ataques básicos no dan más resultado y los autores de malware se están dedicando a ataques mucho másfurtivos. Los tipos de ataques dirigidos que estamos viendo ahora tienen cuerpos y vínculos que parecen legítimos. A los usuarios finales les resulta especialmente difícil diferenciar los emails legítimos de los que no lo son.

Principales países que hospedaron sitios de phishing durante 2010



PELIGRO PARA LOS DATOS

Los delincuentes informáticos y los líderes de negocios se han dado cuenta de que los datos son la nueva forma de divisa global. Ya sea que se trate de tarjetas de crédito, fórmulas químicas, registros de pacientes o números telefónicos, todos los bienes tienen un precio. La pérdida de bienes no sólo daña gravemente el bienestar financiero de una empresa, sino que también cuando la reputación de una empresa se ve amenazada, el problema se transforma en una pesadilla de relaciones públicas

Estos son los 5 principales hosts de código de robo de datos en 2010:

- pc-optimizer.com
- host127-0-0-1.com
- beancountercity.com
- Otexkax7c6hzuidk.com
- googlegroups.com

¿Qué magnitud tiene la pérdida de datos?

En 2008, TJX se convirtió en el caso 'estrella' de fugas de datos cuando once hombres fueron acusados de robar más de 40 millones de números de tarjetas de crédito de la empresa. Esto afectó otras empresas, como OfficeMax, Boston Market y Barnes & Noble. La información confidencial fue vendida a otras organizaciones criminales en Estados Unidos y Europa.

El 20 de enero de 2009, el día de la asunción del Presidente Barack Obama, Heartland Payment Systems anunció que habían descubierto una fuga de datos que se había producido el año anterior. Visa y MasterCard alertaron al procesador de pago sobre actividad sospechosa en algunas de las transacciones con sus tarjetas. Los datos que quedaron expuestos con la fuga incluían números de tarjetas, fechas de vencimiento y, en algunos casos, los nombres de los clientes que utilizaban tarjetas de débito o de crédito en la red de Heartland compuesta por 250,000 empresas.

Hasta la fecha, esta fuga es considerada la mayor fuga de datos de la historia. La empresa destinó un total de \$140 millones a demandas judiciales relacionadas con el caso. Heartland aceptó un arreglo con Visa por \$60 millones, con MasterCard por \$41.1 millones, con Discover por \$5 millones y con American Express por \$3.6 millones. La otra parte de este caso, no tan coincidente, es que la mente maestra detrás de la fuga, Albert "segvec" Gonzales, fue sentenciado a 20 años de prisión en marzo por su participación en la fuga de TJX.

Además de las historias de fugas de datos que tuvieron gran difusión y que presentamos aquí, es importante notar que el volumen de datos que se 'escapan' de una organización es alarmante. Un gran porcentaje de la pérdida de datos se debe a errores de los empleados, no a un robo interno. Existen numerosos casos donde las personas simplemente pierden sus dispositivos. La pérdida accidental puede provocar un daño catastrófico a la base de cualquier corporación.

En muchos casos, la pérdida de datos está relacionada con buenos empleados que cometen malos errores. Esto incluye el envío de datos entre sí en la Web utilizando sitios de Webmail personal (como gmail o hotmail). También, la publicación en aplicaciones en línea, como GoogleDocs, LinkedIn e, incluso, la Web social. En todos estos medios, la información confidencial corre el riesgo de caer en manos equivocadas.

Los datos se han convertido en un bien valioso, ya sea que estén en reposo, en movimiento o en uso. Pero el costo de una fuga de datos puede ser aun más valioso que los datos mismos. Además de las estrictas reglamentaciones y políticas que rodean ahora a los datos, cada vez más gobiernos han comenzado a imponer multas por la pérdida de datos. Estas reglamentaciones, políticas y multas que ahora se aplican a los datos varían en gran manera según las empresas, las industrias y los países involucrados.

En muchos casos, la pérdida de datos está relacionada con buenos empleados que cometen malos errores.

REDES SOCIALES: LA GRAN IMAGEN, LOS GRANDES RIESGOS

Las redes sociales presentan una gran oportunidad para los líderes de negocios con visión de futuro y también para los delincuentes con visión de futuro. Además del hecho de que las redes sociales continúan teniendo un crecimiento explosivo, los beneficios comerciales de aprovechar estos sitios están alcanzando proporciones épicas.

Facebook y Twitter se han convertido en una parte integral de campañas corporativas y actividades promocionales. Los foros han cerrado la brecha entre las empresas y los usuarios, y actúan como centros de información centralizada de soporte técnico y comunicación entre pares. Esto atrae especialmente a los profesionales consumidores que desean mostrar su conocimiento a las personas con las que no han podido comunicarse antes. Todo gerente de departamento de Recursos Humanos o de contrataciones con experiencia comprende los beneficios de usar LinkedIn para buscar candidatos capacitados. Los profesionales de relaciones públicas no sólo usan estos sitios para cobertura, sino también tienen la capacidad de reunir y cuantificar la información que admiradores, usuarios y críticos publican en estos sitios.

En resumen, estos sitios brindan beneficios financieros y sociales a todos los tipos de empresas, tanto grandes como pequeñas. Sin embargo, muchos de los principales sitios de redes sociales no fueron diseñados teniendo en cuenta la seguridad. Piense en una aplicación de 99 centavos; ¿cuánta seguridad piensa que posee una aplicación que cuesta 99 centavos?

La trágica realidad de la situación actual de las redes sociales es que muchas corporaciones no poseen el conocimiento ni la información necesarios para tomar decisiones críticas en relación con el uso de estos sitios. Y más importante, muchos de los encargados de tomar estas decisiones no entienden el panorama de amenazas de las redes sociales que está en constante cambio. El temor y la indecisión a menudo llevan a las empresas a conceder acceso total a estos sitios o bloquear totalmente el acceso a ellos. Ambas decisiones son desacertadas. El desafío es que estos sitios se vuelven cada día más complicados. De hecho, hay una creciente probabilidad de que los sitios de medios sociales tengan los mismos niveles de contenido malicioso que vemos actualmente en el email.

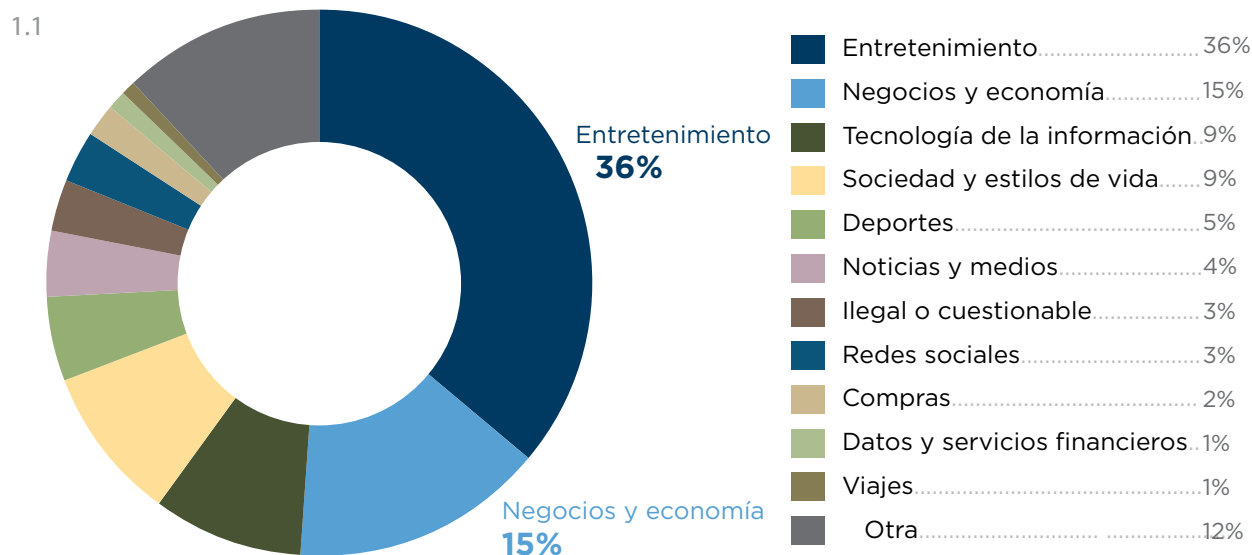
El 40% de todas las actualizaciones de estado de Facebook tienen vínculos y el 10% de estos vínculos son spam o código malicioso.

La categoría Negocios y el contenido censurable codo a codo

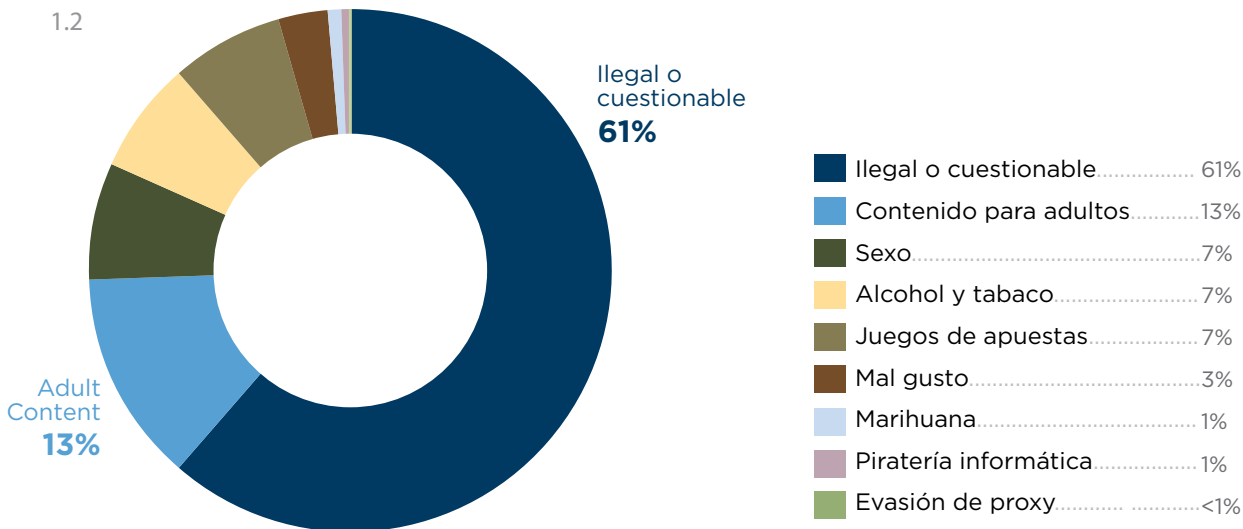
Analizamos una muestra de las 200,000 URL principales en Twitter y Facebook combinadas para ver qué visitaba la gente. Comparamos los dos sitios teniendo en cuenta los temas que están incluidos en una categoría general y los incluidos en categorías que podrían considerarse censurables.

Nuestro análisis del contenido constantemente cambiante de estos dos sitios Web proviene de nuestro motor de clasificación avanzada Websense Advanced Classification Engine (ACE) que utiliza la Red ThreatSeeker.

Twitter

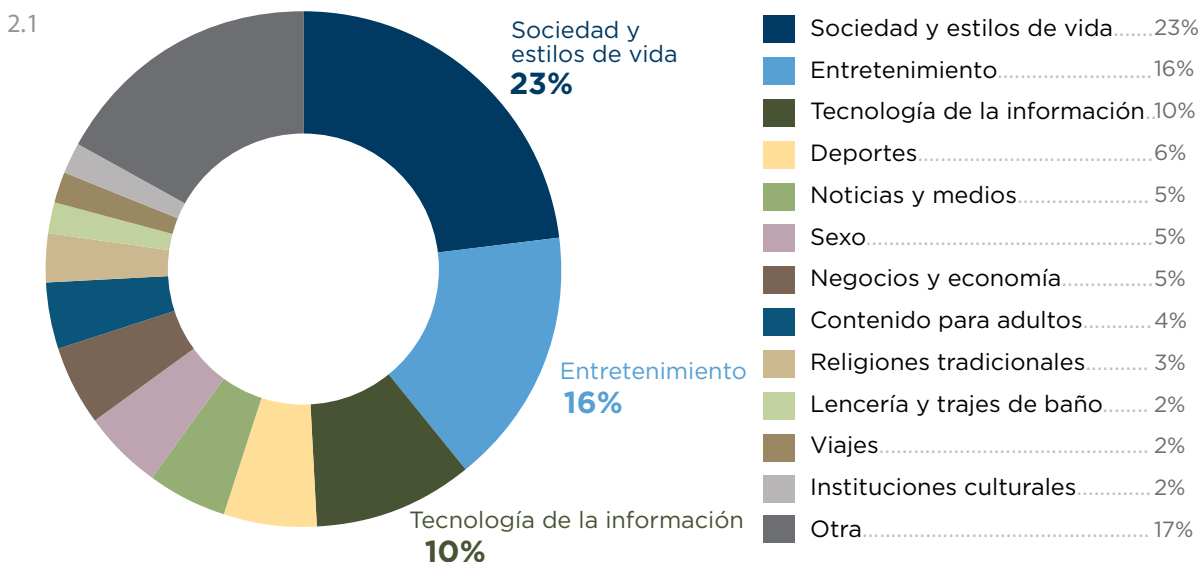


El gráfico 1.1 muestra que entre los 10,000 sitios más populares, la categoría Entretenimiento dominó con una mayoría del 36%, seguido de Negocios y economía, Tecnología de la información, Sociedad y estilos de vida, y Noticias y medios.

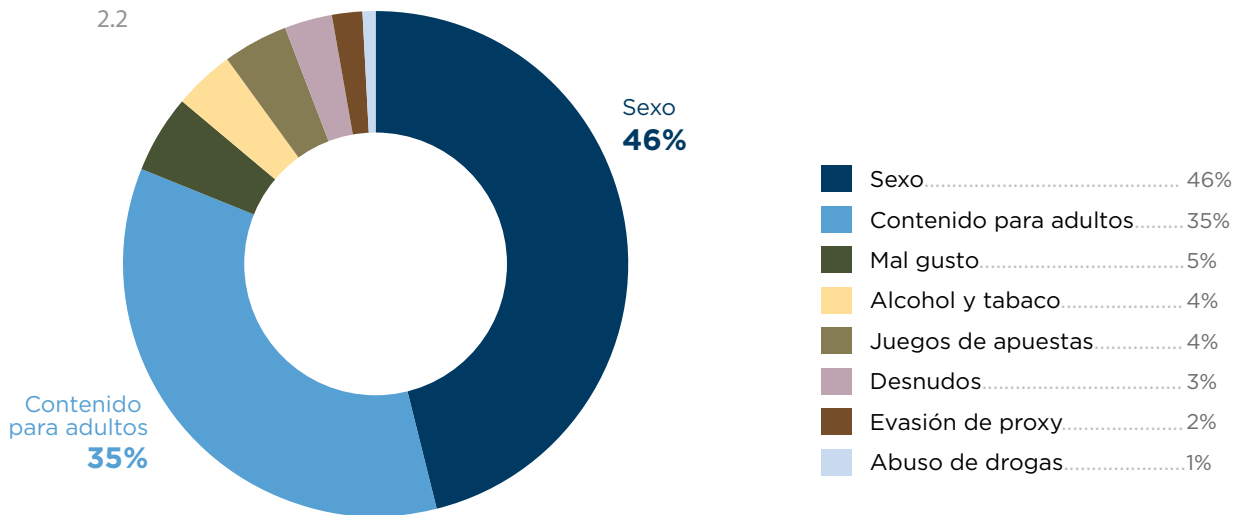


El gráfico 1.2 muestra la distribución del contenido censurable en las 10,000 páginas de Twitter principales. El contenido censurable representó el 4.3% de todos los datos. El 61% del contenido censurable es ilegal o cuestionable, seguido de Contenido para adultos y Sexo.

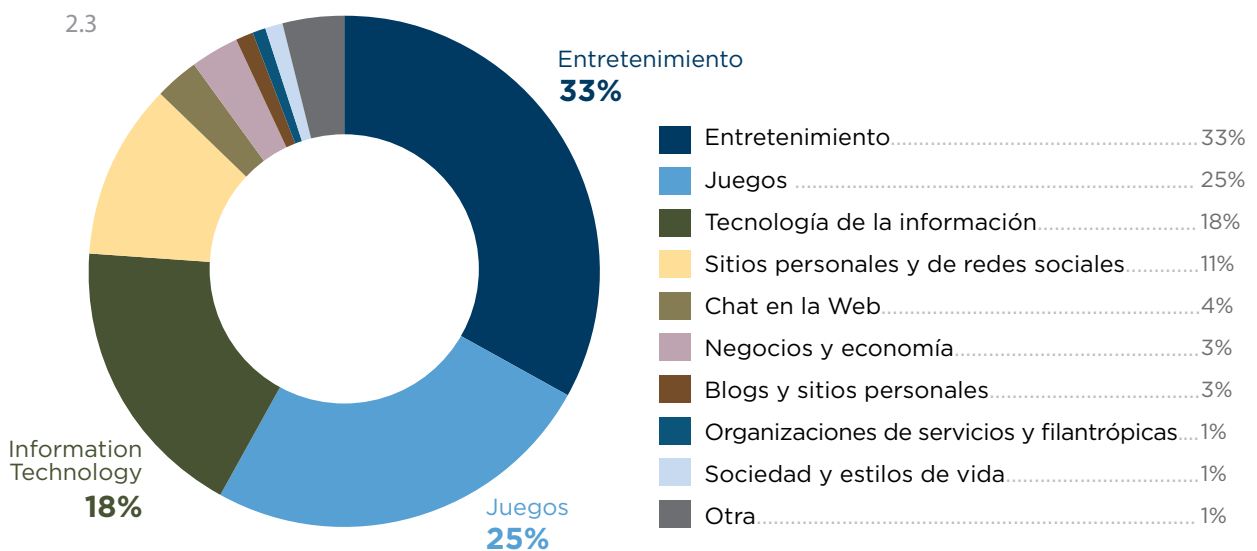
Facebook



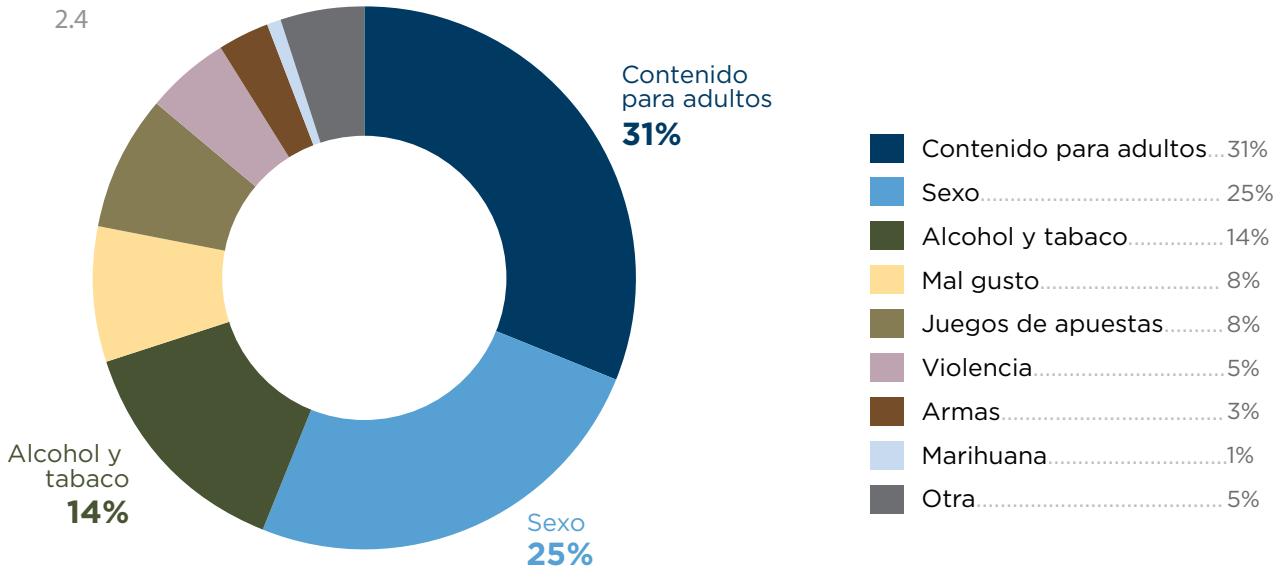
Los gráficos 2.1 y 2.2 representan la distribución de los 800 blogs principales de Facebook ordenados por categoría general y categoría censurable. El gráfico 2.1 muestra que las categorías dominantes de estos blogs son Sociedad y estilos de vida, Entretenimiento y Tecnología de la información. Es interesante notar que Entretenimiento es significativamente inferior que Sociedad y estilos de vida.



El gráfico 2.2 muestra la distribución de las categorías censurables en los 800 blogs principales de Facebook. El contenido censurable constituye el 10.47% de los datos generales. Las tres categorías censurables principales son Sexo, con el 46%, Contenido para adultos, con el 35%, y Mal gusto, con el 5%.



El gráfico 2.3 muestra que las características dominantes de las aplicaciones de Facebook son Entretenimiento, Juegos, Tecnología de la información y Redes sociales y sitios personales.



El gráfico 2.4 muestra la distribución de las categorías censurables encontradas en las aplicaciones de Facebook. El contenido censurable constituye el 79% de los datos generales.

WEBSense SECURITY LABS: PRINCIPALES DESCUBRIMIENTOS 2010

Los resultados de búsquedas en Office.Microsoft.Com puede conducir a un antivirus falso

Fecha del ataque: 01/08/2010

Detalles del ataque: Websense Security Labs y la Red ThreatSeeker de Websense detectaron que los resultados de búsquedas en office.microsoft.com pueden conducir a los usuarios a una página de un antivirus falso. El blanco de este ataque son los usuarios que buscan información relacionada con ayuda para los productos Office en el propio sitio de Microsoft. Posiblemente los usuarios no saben que cuando escriben una pregunta de búsqueda en el sitio, Microsoft busca los resultados en su propio sitio Web pero también obtiene resultados de la Web general. Como la URL de los resultados de búsqueda comienza con http://office.microsoft.com, esto es particularmente alarmante para los usuarios que confían en los sitios simplemente por su reputación. La URL maliciosa funcionaba como una redirección a una página de advertencia y escaneo de virus, que parecía muy real, presentada por un antivirus falso. En el momento del descubrimiento, el ejecutable utilizado en la explotación sólo fue reconocido por uno de los 41 motores antivirus de Virus Total.

Black Hat SEO provocó resultados de búsqueda maliciosos para el terremoto de Haití

Fecha del ataque: 01/13/2010

Detalles del ataque: Websense Security Labs y la Red ThreatSeeker de Websense descubrieron que las búsquedas de términos relacionados con el terremoto de Haití devolvían resultados que conducían a un programa antivirus falso. El terremoto, que se produjo el martes 12 de enero cerca de Puerto Príncipe, tuvo una magnitud de 7.0 y se dice que es el terremoto más fuerte que asoló Haití. Personas de todo el mundo buscaron en Internet las últimas noticias sobre el desastre. Buscaban dónde hacer una donación, intentaban ver la magnitud de la calamidad a través de fotografías o videos, y buscaban la opinión de sus artistas y músicos favoritos sobre el desastre. Desafortunadamente, los chicos malos utilizan los eventos y las crisis como ésta para diseminar su código malicioso. El código malicioso tiene un índice de detección de los principales proveedores de antivirus inferior al 20%, según Virus Total.

Sitio de la Comisión Tributaria de Oklahoma comprometido

Fecha del ataque: 01/29/2010

Detalles del ataque: Websense Security Labs y la Red ThreatSeeker de Websense descubrieron que la página inicial del sitio Web de la Comisión Tributaria de Oklahoma había sido comprometida con código de secuencia de comandos malicioso. Después de que se cargaba la página, el explorador ejecutaba la secuencia de comandos inyectada en segundo plano. El código de la secuencia de comandos inyectada atravesaba una serie de técnicas de deofuscación que, en última instancia, llevaban a la computadora de la víctima a un sitio Web de ataque sin su consentimiento o conocimiento.

Campaña de spam maliciosa falsifica respuesta de solicitud de empleo de Google

Fecha del ataque: 02/1/2010

Detalles del ataque: Websense Security Labs y la Red ThreatSeeker de Websense descubrieron una nueva campaña de spam malicioso que falsificaba las respuestas de solicitudes de empleo de Google. Los mensajes estaban muy bien redactados y eran tan creíbles que probablemente los atacantes habían incluido partes de respuestas de solicitudes de empleo reales de Google. Típicamente, el spam tiene errores ortográficos o gramaticales que hacen que luzca no oficial y actúan como un indicador. Sin embargo, el texto de estos mensajes no tenía errores, lo que los hacía mucho más creíbles, específicamente si el blanco del ataque realmente había solicitado un empleo en Google. La dirección que figuraba en el campo De: había sido falsificada para engañar a las víctimas para que creyeran que el mensaje era enviado por Google. Los mensajes tenían un archivo adjunto llamado CV-20100120-112.zip que contenía una carga maliciosa. Aquí es donde el mensaje era sospechoso, porque el contenido del archivo .zip tenía una extensión doble que terminaba en .exe. Los atacantes intentaron ocultar la extensión .exe anteponiéndole .html o .pdf, seguido de un número de espacios y luego la extensión .exe.

Sitio de evaluación de velocidad Chinaz.com comprometido

Fecha del ataque: 05/25/2010

Detalles del ataque: Websense Security Labs y la Red ThreatSeeker de Websense descubrieron que el sitio de evaluación de velocidad, chinaz.com, había sido comprometido. Chinaz.com es un sitio Web maestro muy famoso que brinda servicio técnico y de descarga de recursos en China. El tráfico diario en este sitio es de más de 50,000 visitas y tiene un puntaje muy alto de Alexa (179). El subdominio inyectado, speed.chinaz.com, es la página que suministra herramientas para evaluar la velocidad de los sitios Web. El sitio primero redirige a un archivo JavaScript en su propia ruta. El código malicioso inyectado por los delincuentes informáticos tenía una carga que contenía dos partes (ap.js y el código de ofuscación en el tag de la secuencia de comandos). Después de analizar esto, notamos que se utilizaba para atacar la vulnerabilidad IE (MS10-018), que descarga un archivo ejecutable llamado dn.exe. Este archivo tenía un buen índice de detección de la mayoría de los proveedores de antivirus; sin embargo, dn.exe se descargaba y ejecutaba archivos remotos y enviaba información local a un servidor remoto. El proceso estaba encubierto como un componente antivirus y, al mismo tiempo, suspendía el software antivirus.

Canal de juegos de MOP BBS comprometido

Fecha del ataque: 05/30/2010

Detalles del ataque: Websense Security Labs y la Red ThreatSeeker de Websense descubrieron que el canal de juegos de MOP BBS había sido comprometido. Mop.com es uno de los foros más grandes y de mayor influencia en China. Fue el lugar de nacimiento de la cultura de redes china y ha pasado a ser un sitio Web con integración de foros, noticias, juegos y entretenimiento, convirtiéndose en una enorme plataforma de información multimedia. Mop.com tiene más de 50 millones de usuarios registrados y más de 200 millones de vistas diarias, lo que lo convierte en el sitio Web n.º275 más popular del mundo según Alexa. El sitio Web es especialmente popular entre los fanáticos del juego World of Warcraft. Este sitio contiene una referencia al archivo JavaScript ajax.js que fue modificado e inyectado con código malicioso

por delincuentes informáticos. La amenaza utilizó una técnica con frecuencia usada por los atacantes de Black Hat SEO en la que sólo los visitantes que abren la página desde los resultados de búsqueda de baidu.com, el popular motor de búsqueda en China, se infectan con el código malicioso. El código luego realiza otro control para determinar si el popular software antivirus chino 360 Safeguard está instalado. Si no lo está, el código continúa explotando la PC (paso 2 de la cadena). Después de esto, redirecciona las dos URL. Ambos sitios tienen la misma carga y ambos utilizan la vulnerabilidad de Microsoft Internet Explorer MS10-018 para infectar al usuario. Luego de un rápido análisis, descubrimos que el shellcode de la explotación descargaba el archivo remoto ejecutable llamado 55.exe. El archivo está cifrado y tiene una detección antivirus muy baja. El shellcode de la explotación se utiliza luego para decodificar el archivo. Una vez descifrado, el archivo es detectado como un ladrón de información de juegos en línea.

Copa Mundial atacada por campaña de spam maliciosa

Fecha del ataque: 06/11/2010

Detalles del ataque: Websense Security Labs y la Red ThreatSeeker de Websense detectaron una nueva oleada de emails maliciosos interesantes. Al comienzo del ansiosamente anticipado torneo de la Copa Mundial, esperábamos estar inundados de spam relacionado con el tema en cuestión. La muestra que encontramos fue bastante diferente de lo habitual, porque la técnica utilizada no levantaba sospechas. En esta nueva campaña vimos más de 80,000 mensajes de email que utilizaban un adjunto de HTML con un JavaScript incorporado. Al ser ejecutada, esta secuencia de comandos conducía a un sitio Web malicioso.

Songlyrics.com comprometido

Fecha del ataque: 09/16/2010

Detalles del ataque: Websense Security Labs y la Red ThreatSeeker de Websense detectaron que el popular sitio Songlyrics.com (con aproximadamente 200,000 páginas visitadas por día y 2,000,000 visitantes únicos) estaba comprometido y se le había inyectado código malicioso ofuscado. Cuando un usuario tenía acceso a la página principal del sitio de letras de canciones, el código inyectado lo redirigía a un sitio de explotación cargado con el kit de explotación Crimepack. Las explotaciones que se intentaron generaron un archivo binario malicioso (VT 39.5%) que se ejecutaba en la computadora de la víctima. Una vez infectada, la máquina se convertía en otra máquina "zombie" de la lista. Es interesante notar que el código malicioso inyectado en Songlyrics.com utilizaba un algoritmo de ofuscación similar al de Crimepack, un software comercial pre-empaquetado utilizado por los atacantes para enviar código malicioso en la Web. Al momento del descubrimiento, la mayoría de las páginas a las que Songlyrics.com brindaba servicio estaban comprometidas.

LOS PRÓXIMOS 12 MESES

A continuación presentamos algunas tendencias emergentes y predicciones que realizaron los investigadores de Websense Security Labs:

Teléfonos inteligentes: Algunas plataformas móviles, incluido el iPhone, ya han sido atacadas. La continua masificación del consumo de estos teléfonos y la creciente cantidad de datos financieros que tocan estos dispositivos los convierten en futuros blancos de ataque. También existe una gran diferencia entre la calidad de las aplicaciones móviles disponibles. Estas aplicaciones abrirán la puerta a vulnerabilidades de seguridad involuntarias. La liberación (jailbreak) de los iPhones es sólo una muestra del oscuro territorio en el que ingresarán estos teléfonos. Las aplicaciones legítimas serán fácilmente redireccionadas para ataques de spam y phishing.

Odio y terrorismo: La evidencia fotográfica de terroristas ocultos en cuevas no es un buen ejemplo del nivel de sofisticación con el que operan estos grupos. Ya hemos visto un aumento de la presencia de estas organizaciones en la Web. Numerosos grupos continuarán concentrándose en la Web para reclutar miembros, hacer dinero y cometer diversos delitos. También esperamos un ajuste de las estructuras organizativas en las que operan estos grupos.

Ataques combinados: La optimización SEO combinada con antivirus falsos y email que contiene componentes de robos de datos no disminuirá en los próximos 12 meses. Recurrir a medidas de seguridad reactivas, como antivirus independientes, no brindará la protección adecuada contra estas técnicas sofisticadas que combinan la Web, la prevención de la pérdida de datos (DLP) y el email.

Spam y email: Las campañas de spam continuarán atacando los muros de Facebook y otros sitios de redes sociales. Los ataques al email continuarán y se volverán más sofisticados, con un énfasis en los vínculos y los adjuntos para ayudar a ocultar las malas intenciones.

Botnets: Igual que en el pasado, la mayoría de los ataques estarán basados en las botnets. Son muy rentables para los delincuentes informáticos y tienen el rango suficiente para llegar muy lejos.

Vulnerabilidades antiguas: Adobe Reader y Microsoft Internet Explorer fueron los blancos preferidos en 2010 y no hay indicios de que los piratas informáticos tengan intenciones de cambiar el rumbo. Las antiguas vulnerabilidades estarán sujetas a una gran cantidad de explotaciones el año próximo.

DLP y la Web dinámica: Los 100 sitios Web más populares tienen contenido que cambia constantemente, y cada sitio recibe miles de millones de visitas. Muchas empresas se encontrarán sin protección y pondrán sus datos en riesgo debido a malas prácticas de negocios relacionadas con la confidencialidad de los datos de estos sitios.

RESUMEN

“La educación es esencial. Las personas necesitan saber contra qué deben defenderse”.

Jay Liew, Investigador de Seguridad de Websense

La evolución del panorama de amenazas durante 2010 ha revelado nuevas amenazas de seguridad y confirmado el peligro constante de las amenazas conocidas.

Nuestra investigación resalta la ineficacia de ejecutar productos antivirus independientes para detener las amenazas actuales centradas en el contenido, y también la ineficacia de utilizar las firmas de amenazas y el filtro de URL. Nuestra investigación también muestra que una solución de prevención de la pérdida de datos ya no es una opción “agradable de tener”, sino que debe considerarse como un requisito esencial. La Web se ha transformado en una plataforma de aplicaciones y negocios. Los sitios de redes sociales en tiempo real continuarán dominando el escenario. Los piratas informáticos continuarán mezclando trucos de ingeniería social con amenazas combinadas, haciendo a la Web más complicada que nunca antes.

La naturaleza combinada de las amenazas actuales significa que todas las medidas de seguridad deben integrar tecnologías de email, Web y datos. Websense anticipa, descubre y mitiga estas amenazas en evolución como parte central de nuestra estrategia tecnológica e integra dicho contenido y el conocimiento de las amenazas en una solución unificada de seguridad Web, seguridad de email y prevención de la pérdida de datos.

Manténgase informado con las alertas de Websense Security Labs

Websense Security Labs descubre e investiga las amenazas avanzadas de Internet actuales y publica los resultados. Las alertas de Websense Security Labs permiten a las organizaciones proteger los entornos informáticos de los empleados de las amenazas de Internet cada vez más sofisticadas y peligrosas. Además de publicarse en websense.com, las alertas de Websense Security Labs están ahora disponible por email.

Regístrese para recibir las últimas advertencias de seguridad sobre eventos maliciosos de Internet, incluido spyware, phishing y sitios Web corruptos, que recibirá directamente en su bandeja de entrada a medida que sean descubiertas por Websense Security Labs: <http://securitylabs.websense.com/content/Subscription.aspx>

Redactado por Jon Crotty.

Acerca de Websense

Websense, Inc. (NASDAQ: WBSN) es el proveedor líder de seguridad de contenidos unificada. Somos el líder global en soluciones de seguridad Web, seguridad de datos y seguridad de email, y proporcionamos la mejor seguridad contra las amenazas modernas al menor costo total de propiedad a cientos de miles de empresas, mercados medios y organizaciones pequeñas en todo el mundo. Distribuidas a través de una red global de socios de canal y suministradas como software, appliances y plataformas Security-as-a-Service (SaaS), las soluciones de seguridad de contenidos de Websense ayudan a las organizaciones a aprovechar las nuevas tecnologías de comunicación y permiten la colaboración y el uso productivo de las herramientas comerciales de la Web 2.0. Al mismo tiempo, protegemos a las organizaciones contra las amenazas persistentes avanzadas, prevenimos la pérdida de la información confidencial e implementamos políticas de seguridad y uso de Internet. Websense tiene sede en San Diego, California, y oficinas en todo el mundo.

Websense Security Labs

Websense Security Labs es la rama de Websense, Inc. dedicada a las investigaciones de seguridad que descubre, investiga e informa sobre las amenazas avanzadas de Internet. A diferencia de otros laboratorios de investigación, Websense cuenta con conocimientos inigualables sobre malware y sus posibles ubicaciones en la Web. De este modo, Websense puede detectar y bloquear nuevas amenazas que los métodos tradicionales de investigación en seguridad pasan por alto, para que las empresas puedan proteger el contenido confidencial del robo, de posibles peligros o de usos inadecuados. Reconocido como líder mundial en investigación de seguridad, Websense Security Labs publica sus resultados para cientos de socios de seguridad, proveedores y otras organizaciones de todas partes del mundo y proporciona criterios de medición de seguridad al Grupo de Trabajo Antiphishing (Anti-Phishing Working Group).

El blog de Websense Security Labs proporciona la información más actualizada y las últimas novedades sobre temas de investigación de seguridad y amenazas avanzadas de Internet. Websense Security Labs investiga y publica información sobre ataques, nuevas amenazas y otros temas relevantes de seguridad Web para proteger a las organizaciones de las crecientes amenazas peligrosas de Internet.

Para obtener más información, visite el blog: <http://www.websense.com/securitylabs/blog>

Websense, Inc.
San Diego, CA USA
tel +1 800 723 1166
fax +1 858 458 2950
www.websense.com

Websense, Latin America
São Paulo, Brasil
tel +55 11 3568 2050
fax +55 11 3568 2200
www.websense.com/latam

websense[®]
ESSENTIAL INFORMATION PROTECTION™