SOPHOS

Informe de amenazas de seguridad: 2013

Nuevas plataformas y evolución de las amenazas

Índice

Ilustraciones

Vídeos

Programas publicitarios
Los programas publicitarios muestran anuncios en los ordenadores

Prólogo

El 2012 ha sido un año de mucho ajetreo para el mundo de la ciberseguridad y, haciendo repaso, me gustaría destacar algunas de las principales observaciones. El aumento de la movilidad de los datos en los entornos corporativos ha sido sin duda uno de los retos más importantes a los que nos hemos enfrentado. Los usuarios están aceptando de forma definitiva la posibilidad de acceder a los datos desde cualquier lugar. La rápida adopción del uso de dispositivos personales en entornos laborales (fenómeno conocido también por las siglas BYOD del inglés) y la nube está acelerando esta tendencia y generando nuevos vectores de ataque.

Otra de las tendencias que estamos observando es el cambio en la naturaleza de las estaciones de trabajo, que está transformando los entornos empresariales tradicionales y homogéneos de sistemas Windows en entornos con diversidad de plataformas. Los programas maliciosos actuales resultan eficaces a la hora de atacar plataformas nuevas y hemos observado un rápido aumento en el número de programas maliciosos dirigidos a dispositivos móviles. Hace unos años, los programas maliciosos para Android eran simples muestras de laboratorio, pero se han convertido en una amenaza seria y cada vez mayor.

El uso de dispositivos personales en entornos laborales también está evolucionando rápidamente, y muchos de nuestros clientes y usuarios ya participan de forma activa en esta tendencia. Los empleados quieren utilizar sus teléfonos inteligentes, tabletas o portátiles de última generación para conectarse a las redes empresariales, por lo que los departamentos informáticos deben proteger datos delicados en dispositivos sobre los que tienen muy poco control. El uso de dispositivos personales en el trabajo puede resultar beneficioso tanto para los usuarios como para los empleados, pero los problemas para la seguridad se acentúan a medida que la línea que separa la vida privada de la laboral se difumina. Es necesario determinar a quién pertenecen los dispositivos y los datos que almacenan, quién los administra y quién se encarga de protegerlos.

Por último, Internet sigue siendo la principal vía de distribución de programas maliciosos, sobre todo, cuando utilizan técnicas de ingeniería social o los exploits están dirigidos al navegador o a las aplicaciones relacionadas. Por ejemplo, los kits de malware como Blackhole contienen mezclas potentes de diez o más exploits diseñados para penetrar por los agujeros de seguridad más diminutos y sacar partido de los sistemas en los que faltan parches.

Los ciberdelincuentes suelen concentrarse en los puntos débiles y utilizan las técnicas hasta que dejan de ser eficaces y encuentran nuevos objetivos. La seguridad es un componente fundamental en el uso de dispositivos personales en el trabajo y la nube. Para proteger los datos en un mundo en el que los sistemas cambian rápidamente y la información fluye con total libertad, es necesario un ecosistema coordinado de tecnologías de seguridad en las estaciones de trabajo, las puertas de enlace, los dispositivos móviles y la nube.

La seguridad informática está dejando de basarse en los dispositivos para centrarse en los usuarios y los requisitos de seguridad abundan. Las estrategias de seguridad actuales deben centrarse en todos los componentes principales: la imposición de políticas de uso, el cifrado de los datos, el acceso seguro a las redes corporativas, el filtrado de la productividad y el contenido, la gestión de las vulnerabilidades y los parches, y por supuesto la protección contra las amenazas y los programas maliciosos.

Un cordial saludo,

Gerhard Eschelbeck Director tecnológico de Sophos

Revisión del año 2012: nuevas plataformas y evolución de las amenazas

Durante el año 2012, vimos cómo los delincuentes ampliaban su radio de acción a más plataformas (desde redes sociales a servicios en la nube o dispositivos móviles Android), reaccionaban más rápidamente a los resultados de las investigaciones de seguridad y aprovechaban de forma más eficaz las vulnerabilidades de día cero.

A lo largo del pasado año, los creadores de los programas maliciosos más sofisticados pusieron el listón más alto con modelos empresariales y paradigmas de software nuevos destinados a generar ataques más peligrosos y continuados. Por ejemplo, los responsables de Blackhole, un kit clandestino de herramientas maliciosas distribuido mediante el alquiler de programas de software como servicio (o paquetes delictivos), anunciaron el lanzamiento de una versión nueva. Tras reconocer los logros de las empresas antivirus a la hora de frustrar sus actividades, prometieron subir el nivel en 2012.

Según parece, a los delincuentes privados se unieron personajes y aliados locales capaces de lanzar ataques avanzados contra objetivos estratégicos. Aparecieron entonces informes sobre ataques de programas maliciosos contra infraestructuras del sector energético en diferentes puntos de Oriente Próximo, importantes ataques distribuidos de denegación de servicio contra bancos internacionales y ataques selectivos de spearphishing contra instalaciones clave.

De forma más tradicional, los delincuentes siguieron atacando miles de sitios web mal configurados y bases de datos para revelar contraseñas y distribuir programas maliciosos, poniendo de relieve una vez más la necesidad de prestar más atención a la instalación de las actualizaciones de seguridad y la reducción de las superficies de ataque. Mientras tanto, una nueva generación de víctimas sufrían ataques de ingeniería social todavía sin mitigar, como antivirus falsos y ransomware, que exigían pagos de forma ilegal.

A pesar del aumento de los riesgos, el año 2012 también trajo buenas noticias. Los departamentos informáticos y demás organismos protectores reconocieron cada vez más la importancia de las defensas por capas. Muchas empresas empezaron a hacer frente a los problemas de seguridad introducidos por los teléfonos inteligentes, las tabletas y el uso de dispositivos personales en entornos laborales, a reducir la exposición de plataformas como Java y Flash a las vulnerabilidades, y a exigir correcciones más rápidas a los proveedores de software y sistemas.

Además, las autoridades consiguieron logros significativos en la lucha contra las redes de programas maliciosos, como el arresto de un ciberdelincuente ruso acusado de infectar 4,5 millones de ordenadores con el objetivo de secuestrar cuentas bancarias, o la sentencia impuesta en Armenia al responsable de la enorme red de bots Bredolab. La participación civil de Microsoft en el desmantelamiento de la red de bots Nitol este año[1] es una buena señal de que también vigilamos a aquellos que facilitan la ciberdelincuencia.

En 2013, a medida que la informática se traslade cada vez más a los servicios virtuales en la nube y las plataformas móviles, los delincuentes, como de costumbre, seguirán el mismo camino. Como consecuencia, los departamentos informáticos y los usuarios deberán plantear nuevas preguntas a sus socios y proveedores de servicios, proteger diferentes dispositivos y las infraestructuras de red de forma más sistemática, y responder a las amenazas nuevas con mayor agilidad. Cuente con nuestra ayuda en todo momento.

Aumento de los ataques relacionados con Facebook y otras plataformas de redes sociales

A lo largo de 2012, las redes sociales atrajeron a cientos de millones de usuarios, pero también a gran cantidad de delincuentes dedicados a crear nuevos ataques de ingeniería social muy ocurrentes basados en las principales inquietudes de los usuarios, como el escepticismo generalizado con respecto a los nuevos perfiles biográficos de Facebook[2] o la preocupación natural por imágenes personales recién publicadas. Los delincuentes también atacaron otras plataformas en desarrollo, como Twitter, y servicios cada vez más populares como la red social de intercambio de contenido Pinterest.

En septiembre de 2012, Sophos advirtió sobre el envío generalizado de mensajes directos de Twitter desde cuentas recién secuestradas. Dichos mensajes (supuestamente enviados por amigos virtuales) fingen avisar a los usuarios sobre vídeos publicados en Facebook en los

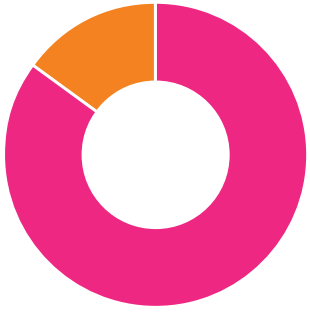
Más información sobre ataques relacionados con las redes sociales

Cuatro amenazas para los datos en la era pos-PC

Beth Jones, de SophosLabs, nos habla sobre la ingeniería social

Encuesta de Naked Security

¿Deberían engañar las empresas a los trabajadores para que abran mensajes de correo electrónico inadecuados con fines educativos?



Sí	**85,21 %**
No	**14,79 %**

Según la votación de 933 encuestados
Fuente: Naked Security

que aparecen. Al hacer clic en el enlace incluido, se abre una página web en la que se indica al usuario que, para ver el vídeo, debe actualizar el reproductor de YouTube. Cualquier acción posterior provoca la infección del sistema con el troyano de puerta trasera Troj/Mdrop-EML.[3]

Durante el mes de septiembre aparecieron también los primeros secuestros generalizados de cuentas de Pinterest. Los ataques publicaban imágenes no deseadas en otras redes sociales como Twitter y Facebook. Los usuarios afectados cuyas cuentas de Pinterest estaban vinculadas a dichas redes se encontraron enviando tweets y publicando mensajes en los muros de sus amigos para animarles a participar en programas de trabajo desde casa de mala reputación.[4]

Con 1000 millones de usuarios, Facebook sigue siendo la principal red social y, por consiguiente, el principal objetivo. En abril, Sophos colaboró con Facebook y otros proveedores de seguridad para ayudar a mejorar la resistencia de Facebook contra los programas maliciosos. En la actualidad, Facebook hace uso de nuestras amplias listas de enlaces maliciosos y sitios fraudulentos, actualizadas de forma constante, para reducir los riesgos de que los usuarios corran peligro.[5] Evidentemente, esta medida es solo uno de los componentes de la solución. Los investigadores de Sophos y otras instituciones siguen trabajando para encontrar nuevos métodos con los que proteger a los usuarios contra los ataques en redes sociales.

Por ejemplo, según Dark Reading, los informáticos de la Universidad de California, Riverside, han creado una aplicación de prueba para Facebook que, en teoría, puede detectar de forma precisa el 97 % de los programas maliciosos y timos distribuidos a través de los canales de noticias de los usuarios.[6] Innovaciones como la autenticación social, técnica mediante la cual Facebook muestra fotos de los amigos para que el usuario los identifique (algo que los hackers supuestamente no pueden hacer), también pueden resultar útiles.[7]

Riesgos emergentes para los servicios en la nube

En 2012, las ventajas económicas y administrativas de los servicios en la nube atrajeron a muchos departamentos informáticos. Además de utilizar más programas empresariales alojados y servicios informales, como el sitio de almacenamiento Dropbox, las empresas empezaron a invertir con más fuerza en nubes privadas creadas con tecnología virtual. Este paso plantea más dudas sobre lo que los usuarios de la nube pueden y deben hacer para no poner en peligro a las empresas y cumplir las normativas.

La seguridad en la nube despertó cierto interés en 2012 después de que Dropbox reconociera el uso de nombres y contraseñas robados en otros sitios web para iniciar sesión en algunas de sus cuentas. Un empleado de Dropbox había utilizado la misma contraseña para todas sus cuentas, incluidas las de trabajo con acceso a datos delicados. Al robar la contraseña en otro sitio, el delincuente se dio cuenta de que podía utilizarla contra Dropbox. Los casos de este tipo nos recuerdan claramente que los usuarios deben utilizar contraseñas diferentes para todos los servicios y sitios seguros.

Tras eliminar por error la protección de todas las contraseñas de los archivos de los usuarios en 2011 durante cerca de cuatro horas,[8] los problemas de autenticación en la nube no son ninguna novedad para Dropbox.

Más información sobre servicios en la nube

Adopción de servicios en la nube con cifrado permanente

Solución a los problemas de Dropbox

Gerhard Eschelbeck, director tecnológico, nos habla sobre el almacenamiento en la nube y el uso de dispositivos personales en entornos laborales

Por otra parte, VentureBeat señaló que la aplicación de iOS de la empresa almacenaba credenciales de inicio de sesión de los usuarios en archivos de texto sin cifrar, a la vista de cualquiera que tuviera acceso físico a los teléfonos.

Desde entonces, Dropbox ha mejorado la seguridad mediante la introducción de funciones optativas de autenticación de doble factor,[9] pero los problemas suscitan cuestiones de mayor envergadura. En mayo de 2012, el Instituto Fraunhofer para la Seguridad Informática descubrió vulnerabilidades relacionadas con el registro, el inicio de sesión, el cifrado y el acceso a datos compartidos en siete sitios de almacenamiento en la nube.[10]

Cabe mencionar que Dropbox y algunos sitios más ya cifran los datos almacenados y en tránsito, pero estas medidas solo protegen los datos a los que no se ha accedido con un nombre de usuario y una contraseña legítimos. Los datos almacenados en sistemas de nubes públicas están sujetos a las leyes de vigilancia e interceptación de las jurisdicciones en las que están ubicados los servidores.

En general, las dificultades de Dropbox han llamado aún más la atención sobre la seguridad de los servicios en la nube. Si los departamentos informáticos no pueden controlar las infraestructuras y servicios públicos en la nube, ¿qué deben hacer las empresas para garantizar la seguridad y el cumplimiento de las normativas? La autenticación de doble factor (o multifactor) es una medida obligatoria pero, ¿es suficiente? Estas son algunas de las cuestiones a tener en cuenta:

- ¿Cómo gestionará las filtraciones de información? En concreto, ¿cómo sabe si existen usuarios internos con malas intenciones que estén reenviándose información delicada para tenerla a su disposición incluso si les despiden?[11]

- ¿Cómo investiga a los proveedores y administradores que utilizan sus sistemas? ¿Aplica estándares y requisitos contractuales igual de estrictos que los que exige a otros socios vitales para el negocio que ven datos confidenciales o estratégicos?[12]

- ¿Puede evitar que se tomen instantáneas de los servidores virtuales para capturar imágenes actuales de la memoria operativa, incluidas todas las claves de cifrado en funcionamiento? Según algunos expertos, como Mel Beckman o System iNEWS, esta posibilidad lleva a descartar el uso de la nube pública en entornos en los que el cumplimiento de las normativas exige el control físico del hardware (por ejemplo, la normativa HIPAA).[13]

A pesar de las dificultades, si decide utilizar servicios en la nube, estos tres pasos pueden ayudarle a proteger los datos:

1. Aplique políticas web para filtrar el contenido, controlar el acceso a sitios web de almacenamiento en nubes públicas y evitar que los usuarios visiten sitios que haya prohibido.

2. Utilice funciones de restricción para bloquear o permitir diferentes aplicaciones, tanto en toda la empresa como en grupos específicos.

3. Cifre los archivos de forma automática antes de que se carguen en la nube desde cualquier estación de trabajo administrada. Con una solución de cifrado, los usuarios pueden elegir los servicios de almacenamiento en la nube que prefieran porque los archivos se cifran siempre y las claves son siempre propias. Y puesto que el cifrado se lleva a cabo en la estación de trabajo antes de sincronizar los datos, el control sobre la seguridad de los datos es total. No tendrá que preocuparse por las posibles infracciones de la seguridad sufridas por su proveedor de almacenamiento en la nube. Gracias a las claves centrales, los usuarios o grupos autorizados pueden acceder a los archivos que están cifrados para los demás. Si por cualquier motivo se perdiese la clave web (por ejemplo, si el usuario simplemente olvida la contraseña), el responsable de seguridad de la empresa tendría acceso a las claves para asegurarse de que las personas adecuadas tienen permiso para ver dicho archivo.

Blackhole: líder del mercado actual de programas maliciosos

Incluye datos de investigaciones de SophosLabs

Al analizar Blackhole en detalle, resulta fácil darse cuenta de lo sofisticados que se han vuelto los creadores de programas maliciosos. Blackhole, el kit de **exploits** maliciosos más destacado y conocido del mundo hoy en día, es una mezcla de una destreza técnica extraordinaria y un modelo empresarial ejemplar. Y, salvo que las autoridades intervengan, es muy probable que los proveedores de seguridad y los departamentos informáticos sigan luchando contra él durante años.

Los kits de explotación son herramientas de software preconfiguradas que pueden utilizarse en servidores web maliciosos para introducir **malware** en equipos sin que los usuarios se den cuenta. Estos kits identifican y aprovechan las vulnerabilidades (defectos o agujeros en la seguridad) del software presente en los equipos para realizar instalaciones automáticas. El contenido de una página web engaña al software (navegadores, lectores de PDF y otros visualizadores de contenido virtual) para que descargue y ejecute el programa malicioso de forma silenciosa sin generar los avisos o diálogos habituales. Al igual que otros kits de explotación, Blackhole puede utilizarse para distribuir una gran variedad de cargas. Los creadores obtienen beneficios mediante la distribución de cargas para terceros y, hasta la fecha, los han utilizado para difundir desde antivirus falsos a **ransomware**, Zeus o **rootkits** como TDSS y ZeroAccess. Blackhole puede servir para atacar Windows, OS X y Linux: es un kit en favor de la igualdad de oportunidades.

Desde octubre de 2011 a marzo de 2012, cerca del 30 % de las amenazas detectadas por SophosLabs procedían directamente de Blackhole o redirigían a kits de Blackhole desde sitios legítimos secuestrados. Blackhole destaca no solo por su eficacia, sino también por el modelo de alquiler del software como servicio, similar a muchos de los programas actuales basados en la nube. En el archivo Readme incluido en el kit se especifican (en ruso) las tarifas por el alquiler semanal, así como otros recargos por servicios de dominios adicionales. Al igual que los proveedores legales de software de alquiler, los creadores de Blackhole proporcionan actualizaciones gratuitas durante el período de vigencia de la suscripción.

Los clientes que desean ejecutar sus propios servidores de Blackhole pueden adquirir licencias de mayor duración, pero la versión que reciben está muy camuflada. Esta es una de las muchas medidas que los creadores de Blackhole han tomado para conservar el control del producto. Todavía no hemos detectado productos derivados de Blackhole procedentes de fuentes no relacionadas, pero otros creadores están empezando a tomar prestadas las técnicas utilizadas en las amplias y numerosas actualizaciones del kit.

Las cuatro fases del ciclo de vida de Blackhole

1. Envío de los usuarios a un sitio de exploits Blackhole

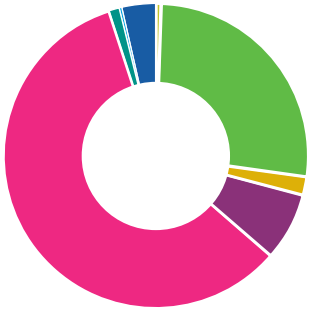
Los delincuentes acceden de forma ilegal a sitios web legítimos e introducen contenido malicioso (normalmente, **snippets** de JavaScript) que genera enlaces a las páginas del sitio de Blackhole. Cuando algún usuario desprevenido visita el sitio legítimo, el navegador descarga de forma automática del servidor de Blackhole el código del kit de explotación.[14]

Los sitios que alojan Blackhole cambian a menudo. Normalmente, utilizan dominios recién registrados y adquiridos mediante el uso ilegal de servicios de DNS dinámicos como ddns., 1dumb.com y dlinkddns.com. Con frecuencia, los **hosts** desaparecen en el plazo de un día. La capacidad de Blackhole para enviar tráfico constantemente a los **hosts** correctos demuestra un nivel de control centralizado impresionante.

Blackhole cuenta con varias estrategias para controlar el tráfico de usuarios. Últimamente, hemos observado que los propietarios utilizan programas de afiliación de forma ilegal. Los **hosts** web introducen de manera voluntaria el código de Blackhole a cambio de un pequeño pago, quizás sin conocer la finalidad del mismo. También hemos visto ejemplos en los que Blackhole utiliza métodos anticuados como el envío de enlaces y adjuntos en mensajes de correo no deseado, por ejemplo, sobre problemas en cuentas bancarias o para solicitar documentos.

Blackhole representa el 27 % de las redirecciones y sitios de explotación

En 2012, más del 80 % de las amenazas detectadas fueron redirecciones, principalmente, de sitios legítimos secuestrados, una advertencia de peso acerca de la necesidad de proteger los sitios web y actualizar tanto las aplicaciones como las secuencias de comandos de los servidores.



Sitio de exploits (Blackhole)	**0,7 %**
Redirección automática (Blackhole)	**26,7 %**
Sitio de exploits (excepto Blackhole)	**1,8 %**
Carga	**7,5 %**
Redirección automática (excepto Blackhole)	**58,5 %**
SEO	**1,1 %**
Antivirus falsos	**0,4 %**
Otros	**3,4 %**

Fuente: SophosLabs

2. Carga del código infectado a partir de la página de destino

El ataque comienza en cuanto el navegador absorbe el contenido del kit de explotación del servidor de Blackhole. En primer lugar, el código (normalmente, JavaScript) averigua cómo ha llegado el navegador al servidor de Blackhole y registra la información para identificar a los socios que han generado el tráfico y pagarles como lo haría una empresa legal. A continuación, obtiene la huella o el perfil del navegador para detectar el sistema operativo utilizado, la versión y si existen complementos de Flash, PDF, Java, etc. instalados.

Aunque hemos observado ataques basados en muchos tipos de vulnerabilidades, los agujeros en la seguridad de Java parecen ser la principal causa de las infecciones con Blackhole. Una vez más, Blackhole utiliza código legítimo siempre que es posible. Por ejemplo, carga el código del **exploit** a través del motor Java Open Business Engine, utilizado para ofrecer compatibilidad con diferentes aplicaciones y sistemas de flujo de trabajo, como el informe diario de amenazas terroristas del presidente de los Estados Unidos.[15]

3. Entrega de la carga

Una vez penetrado el sistema de la víctima, Blackhole puede entregar la carga indicada. Las cargas suelen ser polimórficas y cambian cada vez que infectan un equipo. Los creadores de Blackhole han utilizado de forma exhaustiva técnicas avanzadas de camuflaje del código y polimorfismo del lado del servidor. Al conservar un control central estricto, pueden implementar actualizaciones a gran velocidad. En comparación con otros kits de explotación adquiridos y alojados por los delincuentes, el comportamiento y la eficacia de Blackhole cambian rápidamente. Las cargas de Blackhole también suelen utilizar herramientas personalizadas de cifrado diseñadas para evitar ser detectadas por los antivirus. Los clientes de Blackhole añaden las herramientas y Blackhole contribuye con un servicio optativo que comprueba las funciones antivirus de los sistemas a los que intenta atacar.

4. Seguimiento, aprendizaje y mejoras

Blackhole toma nota de qué **exploits** funcionan con cada combinación de navegadores, sistemas operativos y complementos. De esta forma, los creadores de Blackhole pueden medir qué **exploits** son más eficaces con cada una de ellas. Esta técnica de seguimiento es bastante habitual, pero los creadores de Blackhole se esmeran en actualizar el kit según la información obtenida.

Blackhole es igual de eficaz a la hora de aprovechar vulnerabilidades nuevas de día cero. Por ejemplo, en agosto de 2012, intentó aprovechar una vulnerabilidad muy difundida en la Ayuda y el Centro de soporte de Microsoft para distribuir secuencias de comandos de VBS contaminadas. Blackhole lanzó un ataque nuevo basado en una vulnerabilidad muy peligrosa de Java 7 (CVE-2012-4681) que permite al código infectar el sistema de comprobación de permisos de Java.[16] Sorprendentemente, 12 horas después de hacerse pública la prueba para el ataque, Blackhole ya la incluía.[17] Oracle, por su parte, distribuyó un parche urgente a finales de agosto, pero muchos sistemas siguen sin tenerlo instalado.

Más información sobre Blackhole

Programas maliciosos de la B a la Z: análisis de amenazas, desde Blackhole a ZeroAccess

Mark Harris presenta SophosLabs

Fraser Howard, de SophosLabs, analiza Blackhole

Dada la sofisticación y la agilidad mostradas por los creadores de Blackhole, resulta extraño que hayan dejado prácticamente estancadas algunas partes del kit, como las rutas de las direcciones web, los nombres de los archivos y la estructura de las cadenas de consulta. SophosLabs espera que la situación cambie, aportando nuevas oportunidades a los creadores de Blackhole para mejorar los ataques.

Qué hacemos al respecto y qué puede hacer usted

SophosLabs vigila Blackhole las 24 horas del día para garantizar que la detección genérica y el filtrado por reputación están siempre actualizados conforme a los cambios del kit de explotación. En cuanto Blackhole aprende a combatirlos, implementamos rápidamente las actualizaciones necesarias a través de la nube. Además, aplicamos técnicas de última generación para identificar y analizar ataques polimórficos del lado del servidor como Blackhole.

En el caso de los usuarios, la mejor protección contra Blackhole es una defensa a fondo.

1. Es importante instalar rápidamente los parches de los sistemas operativos y las aplicaciones, y lo más aconsejable es automatizar el proceso.
2. Para reducir la superficie de ataque, desactive los sistemas vulnerables (como Java o Flash) cuando no los necesite.
3. Bloquee los sitios web legítimos secuestrados y de explotación mediante la combinación de tecnologías de filtrado por reputación y detección del contenido (que también puede servir para bloquear cargas). Recuerde que, a menudo, el filtrado por reputación puede bloquear sitios de exploits antes de que se detecte el contenido, pero no es infalible por sí solo.
4. Evite o reduzca los ataques de ingeniería social generados a través del correo no deseado con filtros anti-spam actualizados y mediante la formación de los usuarios.
5. Si el producto de seguridad para estaciones de trabajo que utiliza dispone de funciones HIPS (sistema de prevención de intrusiones en el host), utilícelas para conseguir mayor protección contra exploits nuevos o modificados.

Dónde se alojan los sitios de exploits Blackhole

Países que alojan sitios de exploits Blackhole (2012)

Brasil	**1,49 %**	Italia	**5,75 %**
Gran Bretaña	**2,24 %**	Chile	**10,77 %**
Países Bajos	**2,55 %**	Rusia	**17,88 %**
Alemania	**3,68 %**	Estados Unidos	**30,81 %**
China	**5,22 %**	Otros	**13,88 %**
Turquía	**5,74 %**		

Fuente: SophosLabs

Los ataques de Java alcanzan a un colectivo fundamental

El 2012 fue un año difícil para los complementos de Java de los navegadores, que se vieron afectados reiteradamente por vulnerabilidades nuevas importantes, llevando a muchas empresas a eliminarlos en la medida de lo posible.

En abril, más de 600 000 usuarios de Mac se vieron atrapados en la red internacional de bots Flashplayer (o Flashback) por culpa de una vulnerabilidad de Java presente en OS X que debía haberse corregido hace tiempo. Tras la publicación de una herramienta de eliminación y un parche para Java por parte de Apple, Oracle asumió la responsabilidad directa de publicar Java para OS X en el futuro, y prometió proporcionar parches de Java para OS X y Windows, así como publicar los de Java al mismo tiempo que los de Windows.[18]

Los desarrolladores de Java de Oracle no tardaron en tener que crear parches rápidamente. A pocos días de descubrirse una vulnerabilidad nueva de día cero que afectaba a Java 7 en todos los sistemas operativos y plataformas, el defecto ya se aprovechaba para ataques selectivos, estaba incluido en el ampliamente utilizado kit de explotación Blackhole[19] e incluso había aparecido en un contrato falso de servicios de Microsoft enviado por correo electrónico para suplantar identidades.[20] Según un análisis detallado, gracias al exploit, era posible acceder con código malicioso a clases que deberían estar reservadas e incluso desactivar el gestor de seguridad de Java.[21]

Cumpliendo su promesa, Oracle publicó una corrección no programada más rápido de lo que algunos críticos esperaban. Sin embargo, al cabo de unas semanas, aparecieron otros defectos importantes. Security Explorations, los mismos investigadores que descubrieron el primer problema, encontraron otra forma de burlar el espacio seguro de aplicaciones de Java, esta vez no solo en Java 7, sino también en Java 5 y 6,[22] y en todos los principales navegadores. El nuevo exploit puso en peligro 1000 millones de dispositivos.

Hoy en día, pocos usuarios necesitan programas de Java basados en navegadores (conocidos como applets). En la mayoría de los navegadores, los applets se han sustituido por JavaScript y otras tecnologías. A menos que realmente necesite Java en el navegador, Sophos recomienda desactivarlo.

En nuestro sitio web encontrará instrucciones sobre cómo hacerlo en Internet Explorer, Firefox, Google Chrome, Safari y Opera. [23]

Si utiliza sitios web que exijan Java, puede activarlo en un navegador secundario para abrirlos, y seguir utilizando el navegador principal con Java desactivado para todo lo demás.

Java no es la única plataforma de complementos que ha provocado complicaciones para la seguridad. En años anteriores, Flash de Adobe también fue objetivo de exploits destacados. Por suerte, la necesidad de complementos como Flash para los navegadores está disminuyendo. Los navegadores compatibles con HTML5 cuentan con funciones integradas para reproducir audio y vídeo, eliminando la necesidad de utilizar complementos.

Las contraseñas de los usuarios siguen sin protegerse correctamente en empresas importantes

Las vulnerabilidades de las contraseñas deberían ser algo excepcional. Existen técnicas muy conocidas y fáciles de poner en práctica para generar, utilizar y almacenar contraseñas de forma que ni las empresas ni los usuarios corran peligro. Aun así, en 2012, se produjeron grandes y repetidas filtraciones de contraseñas en un elevado número de empresas importantes.

- Ciertos ciberdelincuentes rusos publicaron cerca de 6,5 millones de contraseñas de LinkedIn en Internet. Los grupos de hackers se pusieron manos a la obra rápidamente y consiguieron descifrar más del 60 % en cuestión de días. La tarea resultó aún más fácil porque LinkedIn no había salpicado la base de datos de contraseñas con datos aleatorios antes de cifrarla.[24]

- Tras sufrir el mismo ataque que LinkedIn, el sitio web de contactos eHarmony informó rápidamente sobre la carga de cerca de 1,5 millones de sus contraseñas en Internet.[25]

- Formspring descubrió que las contraseñas de 420 000 usuarios se habían publicado en Internet y estaban en peligro, y tuvo que pedir a los 28 millones de inscritos en el sitio que cambiaran sus contraseñas a modo de precaución.[26]

- Yahoo Voices reconoció el robo de casi 500 000 direcciones de correo electrónico y contraseñas.[27]

- La multinacional de tecnología Philips sufrió el ataque de la banda r00tbeer, que consiguió robar miles de nombres, números de teléfono, direcciones y contraseñas sin cifrar.[28]

- IEEE, la principal asociación profesional mundial para el avance tecnológico, dejó un registro de cerca de 400 millones de solicitudes web en un directorio legible para todos los usuarios. Las solicitudes incluían nombres de usuario y contraseñas en texto sin formato de cerca de 100 000 usuarios.[29]

Más información sobre las amenazas actuales

 Forme a los usuarios para que no corran peligro con nuestro kit de herramientas gratuito.

 Cinco consejos para reducir los riesgos provocados por las amenazas web actuales

Qué se puede aprender de las fugas de datos, además de que es mejor evitarlas

Si es un usuario:

- Utilice contraseñas seguras y diferentes en todos los sitios que almacenen información importante.
- Utilice programas de gestión de contraseñas como 1Password, KeePass o LastPass. Algunas de estas herramientas incluso generan contraseñas difíciles de averiguar.[30]

Si está al mando de bases de contraseñas:

- No las almacene nunca en formato de texto sin cifrar.
- Aplique siempre a todas las contraseñas sal generada de forma aleatoria antes de aplicarles un algoritmo hash y cifrarlas para almacenarlas.
- No aplique simplemente la sal y el algoritmo hash. Aplique algoritmos hash varias veces para que resulte más difícil probar las contraseñas durante un ataque. Es mejor utilizar un algoritmo de procesamiento de contraseñas reconocido como bcrypt, scrypt o PBKDF2.
- Compare las posibles vulnerabilidades de su sitio con los 10 principales riesgos de seguridad del proyecto OWASP, sobre todo, las de las contraseñas asociadas con la gestión de sesiones y fallos de la autenticación.[31]
- Por último, proteja la base de datos de contraseñas, la red y los servidores con defensas por capas.

Android: el principal objetivo en la actualidad

Incluye datos de investigaciones de SophosLabs

Solo durante el segundo trimestre de 2012, se vendieron más de 100 millones de teléfonos Android.[32] Según una encuesta realizada en los Estados Unidos en septiembre de 2012 entre los usuarios de teléfonos inteligentes, Android contaba con un impresionante 52,2 % de la cuota de mercado.[33] Los creadores de programas maliciosos no pueden resistirse a objetivos así de amplios. De hecho, los ataques contra dispositivos Android están aumentando rápidamente. A continuación, le ofrecemos algunos ejemplos y nuestra opinión, por ejemplo, sobre la seriedad de los ataques, las probabilidades de que aumenten o empeoren, y los pasos a seguir tanto por parte de las empresas como de los usuarios para protegerse.

Poco sofisticados pero rentables: programas falsos y mensajes SMS no autorizados

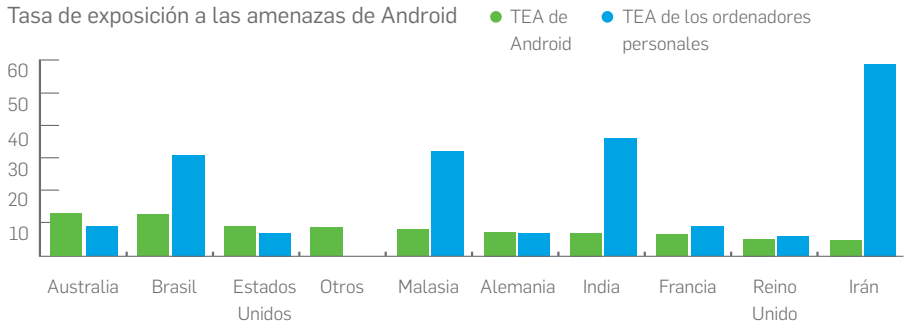
Hoy en día, el modelo empresarial más habitual de los ataques de programas maliciosos contra Android consiste en instalar aplicaciones falsas que envían mensajes de forma secreta a servicios de SMS de tarifas especiales. Entre los ejemplos más recientes se incluyen versiones falsificadas de Angry Birds Space o Instagram, y productos antivirus para Android falsos.[34] En mayo de 2012, el organismo que regula el sector de la telefonía móvil en el Reino Unido descubrió que 1391 usuarios de Android habían sido víctimas de alguno de estos timos e impuso una multa a la empresa encargada del sistema de pagos utilizado, detuvo las transferencias de fondos y exigió devoluciones para aquellos usuarios que habían realizado pagos. Sin embargo, los usuarios británicos resultaron ser tan solo un 10 % de las víctimas de este programa malicioso, detectado después en al menos otros 18 países.

En la actualidad, una familia de programas maliciosos para Android, Andr/Boxer, es responsable de la mayor cantidad de muestras detectadas, aproximadamente un tercio del total. Vinculado a los dominios .ru alojados en Ucrania, Andr/Boxer envía mensajes en ruso y ha atacado de forma desproporcionada a usuarios de Android de Europa del Este que visitan sitios en los que creen que encontrarán fotos de mujeres atractivas.

Al abrirlos, los usuarios ven una página web especialmente diseñada para incitarles a que descarguen e instalen una aplicación maliciosa. Por ejemplo, el usuario puede recibir una notificación (en ruso) para que instale una actualización falsa de productos como Opera o Skype. En otros casos, se ejecuta un escaneado antivirus falso que informa sobre infecciones que no existen y recomienda la instalación de un programa antivirus falso. Una vez instalada, la

Aumentan las amenazas para Android

Según las observaciones de Sophos, la tasa de exposición a las amenazas (TEA) de Android ya supera a la de los ordenadores personales en Australia y los Estados Unidos.



Tasa de exposición a las amenazas (TEA): porcentaje de ordenadores personales y dispositivos Android que sufrieron ataques de programas maliciosos, tanto fructíferos como fallidos, en un plazo de tres meses.

Fuente: SophosLabs

Más información sobre gestión de dispositivos móviles

Herramienta gratuita: Mobile Security para Android

Kit de herramientas de seguridad para dispositivos móviles

Guía para la adquisición de soluciones de gestión de dispositivos móviles

Los programas maliciosos llegan a los dispositivos móviles

Vanja Svajcer, de SophosLabs, analiza los programas maliciosos para Android

aplicación nueva empieza a enviar mensajes SMS caros. Muchos de estos troyanos se instalan con el denominado permiso INSTALL_PACKAGES de Android, que les permite descargar e instalar programas maliciosos adicionales en el futuro.

Ingreso en la red de bots

Hasta hace poco, la mayoría de ataques de programas falsos contra dispositivos Android han sido poco sofisticados. Algunos utilizan, por ejemplo, métodos polimórficos primitivos basados en imágenes aleatorias que cambian las sumas de verificación para evitar ser detectados. Las principales empresas de seguridad aprendieron a derrotar esta táctica hace muchos años.

Pero los delincuentes siguen avanzando. Las ediciones de Angry Birds Space infectadas con programas maliciosos observadas en abril de 2012 (Andr/KongFu-L) son un buen ejemplo. Disponibles solamente, como de costumbre, a través de mercados no oficiales de aplicaciones para Android, los troyanos funcionan como el juego de verdad, pero utilizan un truco de software conocido como el **exploit** GingerBreak para conseguir acceso a la raíz, instalar código malicioso y comunicarse con un sitio web remoto para descargar e instalar programas maliciosos adicionales. De esta forma, evitan ser detectados y eliminados, además de añadir el dispositivo a una red de **bots** internacional.

Captura de mensajes y cuentas bancarias

También hemos empezado a ver programas maliciosos para Android que espían los mensajes SMS entrantes y los reenvían a otro servidor o número de SMS. Este tipo de filtración de datos representa un riesgo significativo tanto para los usuarios como para las empresas.

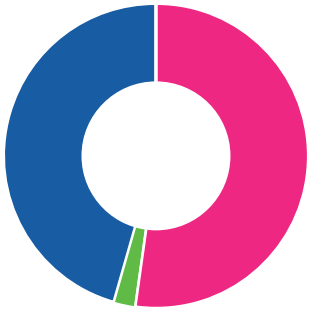
Estos ataques pueden dirigirse a servicios de banca electrónica que envían números de autenticación de transacciones a través de SMS. Muchos bancos envían códigos de autenticación a los teléfonos de los usuarios cada vez que realizan una transacción por Internet. Por eso, los delincuentes ya no pueden hacerse con el control de las cuentas con solo robar las contraseñas de inicio de sesión. Pero los programas maliciosos diseñados para atacar teléfonos (como Andr/Zitmo, basado en Zeus, y versiones similares especiales para dispositivos BlackBerry) son capaces de interceptar dichos mensajes SMS.

Pongámonos en el siguiente supuesto: a través de un ataque tradicional de suplantación de identidades, una víctima proporciona suficiente información a los delincuentes para que inicien sesión en su cuenta bancaria móvil y traspasen el número de teléfono (algo que ya ha ocurrido). A partir de ese momento, tienen acceso a la cuenta y pueden recibir los mensajes SMS que contienen el token de autenticación de doble factor necesario para completar la transacción.

Mediante el uso de aplicaciones de Android maliciosas para recibir mensajes SMS en tiempo real y técnicas de ingeniería social, los delincuentes consiguen una breve oportunidad para robar el token y utilizarlo antes de que el usuario pueda impedírselo.

Encuesta de Naked Security

¿Le suponen un problema los mensajes de texto o SMS no deseados a teléfonos inteligentes?



- Sí **43,78 %**
- Antes sí, pero descargué una aplicación y el problema está solucionado **2,36 %**
- No, apenas recibo mensajes de texto SMS no deseados en mi teléfono **45,29 %**

Según 552 votos
Fuente: Naked Security

Aplicaciones no deseadas (PUA): menos peligrosas que el malware pero aun así arriesgadas

Vale la pena mencionar la presencia generalizada de aplicaciones no deseadas (también conocidas como PUA, por sus siglas en inglés), pequeños programas para Android que no pueden clasificarse exactamente como maliciosos pero pueden provocar igualmente riesgos para la seguridad o de otro tipo.

En primer lugar, muchos usuarios instalan aplicaciones vinculadas a potentes redes publicitarias que pueden hacer un seguimiento de los dispositivos y las aplicaciones e incluso robar datos de contactos. Dichas aplicaciones obtienen beneficios por el simple hecho de mostrar anuncios pornográficos. Dada la información que revelan o con el fin de proteger a los usuarios contra contenido inadecuado o un entorno de trabajo desagradable, muchas empresas pueden preferir eliminarlas.

En segundo lugar, algunos usuarios sofisticados de Android han decidido instalar Andr/DrSheep-A en sus dispositivos. De forma similar a la conocida herramienta Firesheep, Andr/DrSheep-A puede rastrear el tráfico inalámbrico e interceptar cookies sin cifrar en sitios como Facebook o Twitter. La finalidad lícita de la herramienta es probar redes propias. Sin embargo, suele utilizarse para hacerse pasar por usuarios situados en los alrededores sin su conocimiento. Hoy en día, Andr/DrSheep-A está presente en alrededor del 2,6 % de los dispositivos Android protegidos con Sophos Mobile Security. Los departamentos informáticos de las empresas no suelen permitir la instalación ni mucho menos el uso de este tipo de herramientas.

Al liberar el acceso a la raíz de los dispositivos (técnica conocida como rooting, del inglés root o raíz, en referencia a las cuentas de administrador de los sistemas operativos tipo UNIX como Android), los programas de software obtienen derechos de administración totales. El proceso es conocido porque proporciona un mayor control del dispositivo, por ejemplo, para eliminar complementos de software no deseados incluidos por el proveedor de los servicios y sustituirlos por otros alternativos.

Además, traspasa el modelo de seguridad incorporado de Android que limita el acceso de las aplicaciones a los datos de otras. Los programas maliciosos obtienen derechos totales y evitan ser detectados y eliminados más fácilmente en los dispositivos con raíces liberadas. Para los departamentos informáticos que permiten el uso de dispositivos personales en el trabajo, los dispositivos Android con acceso a la raíz aumentan los riesgos.

Reducción de los riesgos mientras sea posible

A estas alturas, los riesgos provocados por los dispositivos Android todavía son moderados en la mayoría de entornos empresariales. Pero dichos riesgos están aumentando. Google sigue mejorando la plataforma para protegerla contra las amenazas más evidentes, pero aparecen otras nuevas. Por ejemplo, algunos expertos en seguridad han expresado recientemente su preocupación acerca de los riesgos provocados por las nuevas funciones NFC (del inglés, near field communications), destinadas a permitir el uso de dispositivos Android avanzados como tarjetas de crédito.

Incluso hoy en día, los programas maliciosos para Android pueden revelar información estratégica o robar contraseñas, y poner en peligro el futuro de cualquier empresa. Teniendo esto en cuenta, los departamentos informáticos deben proteger los dispositivos Android contra programas maliciosos, fugas de datos y otras amenazas. Sophos recomienda seguir los pasos que se describen a continuación para reducir la gravedad de los riesgos. Recuerde que ninguno de estos consejos es infalible ni suficiente de forma aislada, pero en la mayoría de entornos resultan muy efectivos.

- Amplíe la seguridad informática y las políticas de uso aceptable a los dispositivos Android si aún no lo ha hecho.
- Impida el acceso a dispositivos Android con raíces liberadas.
- Plantéese la posibilidad de utilizar funciones de cifrado completo de los dispositivos para protegerlos contra fugas de datos y poder borrar de forma remota los datos

que almacenan en caso de robo o extravío. Si decide cifrarlos, asegúrese de que la solución elegida también cifra las tarjetas SD optativas que puedan contener datos delicados, incluso si dichas tarjetas tienen formatos diferentes.

- Siempre que sea posible, establezca procesos automatizados de actualización de los dispositivos Android para reflejar cualquier corrección. Mantenga los dispositivos Android actualizados con los parches de seguridad proporcionados por el fabricante y los proveedores de cualquier programa adicional instalado.

- Plantéese la posibilidad de limitar las aplicaciones instaladas a aquellas obtenidas en la tienda oficial de Google, Play Store. Aunque han aparecido programas maliciosos en Play Store, son mucho menos frecuentes que en los mercados de aplicaciones no oficiales y sin regular, especialmente, en los ubicados en Europa del Este y Asia.

- Al autorizar las tiendas de aplicaciones, restrinja las aplicaciones que los usuarios pueden descargar a aquellas con un historial positivo y buena clasificación.

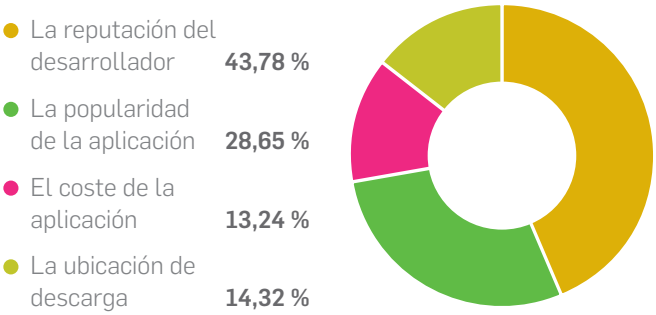
- Evite los ataques de ingeniería social y ayude a sus compañeros a evitarlos, por ejemplo, revisando con cuidado los permisos que solicitan las aplicaciones al instalarlas. Si no se le ocurre ninguna razón concreta por la que una aplicación necesita enviar mensajes SMS, no lo permita. Y párese a pensar si aún desea instalarla.[35]

- Por último, plantéese la posibilidad de utilizar una solución anti-malware y de gestión de dispositivos móviles en los dispositivos Android como Sophos Mobile Control. Pero, elija la solución que elija, asegúrese de que el proveedor dispone de una amplia experiencia tanto en soluciones antivirus como en otros problemas de seguridad de mayor envergadura. ¿Por qué? En primer lugar, porque las técnicas de ataque están empezando a migrar de otras plataformas a Android. El proveedor de la solución elegida debería saber ya cómo hacerles frente. Además, los ataques aparecen y cambian más rápido. El proveedor debería contar con la infraestructura global permanente necesaria para identificar amenazas e infraestructuras en la nube para reaccionar de forma inmediata.

En tercer lugar y sobre todo, porque las complejas infraestructuras actuales exigen una respuesta integrada que vaya más allá de los antivirus aislados para abarcar problemas diversos, desde las redes al cifrado.

Encuesta de Naked Security

¿Qué es lo que más tiene en cuenta a la hora de instalar una aplicación en su dispositivo Android?



Según 370 encuestados
Fuente: Naked Security

La diversidad de plataformas y tecnologías aumenta las oportunidades de ataque

Antes, casi todo el mundo utilizaba Windows. Los delincuentes atacaban Windows y los encargados de la seguridad protegían Windows. Pero esos tiempos ya son historia.

En 2012 aparecieron gran cantidad de agujeros y vulnerabilidades específicas de Windows. Por ejemplo, Windows Sidebar y Gadgets de Windows Vista y Windows 7 resultaron ser tan peligrosos que Microsoft los eliminó inmediatamente y proporcionó herramientas a los clientes para que los deshabilitaran.

Windows Sidebar alojaba miniprogramas (**gadgets**) de noticias, bolsa y meteorología, en respuesta al popular Dashboard de Widgets de Apple. Sin embargo, los investigadores de seguridad Mickey Shkatov y Toby Kohlenberg anunciaron que podían señalar varios vectores de ataque en los **gadgets**, mostrar cómo crear **gadgets** maliciosos e identificar defectos en los **gadgets** publicados.[36] Microsoft ya estaba buscando una alternativa a estas aplicaciones en miniatura para Windows 8, por lo que retiró Sidebar y Gadgets al instante.

Aunque la mayor parte de los usuarios de ordenadores siguen utilizando Windows, en la actualidad, el desarrollo es mucho mayor en Internet y las plataformas móviles. Por eso, tanto las empresas como los usuarios deben prestar atención a los riesgos para la seguridad de entornos nuevos y menos tradicionales como Android.

Estos son algunos ejemplos de filtraciones de seguridad ocurridas en 2012 que sirven para ilustrar las amenazas a las que nos enfrentamos y por qué nuestras defensas deben estar formadas cada vez por más capas y ser más preventivas y completas.

- En febrero de 2012, un **hacker** detectó agujeros de secuencias de comandos entre sitios (XSS) en 25 tiendas electrónicas del Reino Unido que contaban con la certificación de seguridad de VeriSign, Visa o MasterCard.[37] Los delincuentes pueden aprovechar este tipo de defectos para robar credenciales de autenticación o información de facturación de los clientes que pueden dar lugar a robos de identidades. Los agujeros aparecieron por una causa habitual: una secuencia de comandos para filtrar búsquedas de los usuarios mal escrita. Otro ejemplo que recuerda a los usuarios que la seguridad no es cuestión de palabras ni iconos. El hecho de ver https://, un candado o el logotipo de VeriSign Trusted no significa que podamos bajar la guardia. Y un gran aviso para que los profesionales de Internet mantengan las aplicaciones y las secuencias de comandos actualizadas, incluidas aquellas puestas a disposición del público por parte de otros autores.

- Miles de sitios de WordPress autoalojados estaban alojando el peligroso **exploit** Blackhole.[38] En agosto de 2012, Sophos descubrió una campaña de **malware** importante que intenta infectar ordenadores con el conocido kit de explotación Blackhole. Los usuarios reciben mensajes de correo electrónico de verificación de pedidos que contienen enlaces a blogs legítimos de WordPress contaminados para descargar programas maliciosos. Los usuarios del servicio alojado WordPress.com no corren peligro: el proveedor de servicios Automattic se ocupa de la seguridad de los servidores de WordPress.com.

- Los delincuentes han demostrado al menos la posibilidad de atacar desde tarjetas de tránsito público a los nuevos teléfonos inteligentes compatibles con la tecnología NFC (del inglés near field communication).[39]

El retorno del ransomware

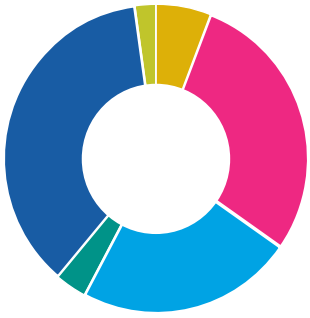
Algunos ataques parecen cíclicos. A pesar de fracasar durante años, resultan demasiado sencillos y tentadores para que los ciberdelincuentes los abandonen por completo. Por ejemplo, en 2012, Sophos observó el resurgimiento de ataques de **ransomware** que impedían que los usuarios accedieran a sus equipos hasta que realizaran el pago correspondiente.

Pero el **ransomware** no es nada nuevo. En 1989, los primeros programas de **ransomware** se distribuían en disquetes enviados por correo ordinario. Los usuarios esperaban recibir programas avanzados de software con información sobre el SIDA pero, en lugar de eso, se encontraban con que los discos duros de sus equipos se cifraban. El programa solicitaba el pago de 189 dólares a una dirección de Panamá mediante transferencia, cheque o giro postal.[40]

En la actualidad, el **ransomware** llega a través de técnicas modernas como mensajes de correo electrónico con trucos de ingeniería social y páginas web contaminadas. Existe un tipo de **ransomware** que simplemente congela el ordenador y pide dinero, sin afectar a los archivos de fondo. Aunque las infecciones

Encuesta de Naked Security

¿Qué navegador web recomienda?



Internet Explorer	**5,95 %**
Chrome	**28,9 %**
Firefox	**23,09 %**
Safari	**3,25 %**
Opera	**36,75 %**
Indiferente	**2,06 %**

Según 370 encuestados
Fuente: Naked Security

son perjudiciales, suelen ser reparables. El otro tipo de ransomware cifra los archivos, por lo que puede provocar la pérdida completa del equipo o fallos totales del disco.

En el momento de la publicación de este informe, el tipo de ransomware más generalizado es el primero. Reveton, por ejemplo, también conocido como Citadel o Troj/Ransom, esconde el escritorio de Windows, impide acceder a todos los programas y muestra una ventana completa con el logotipo del FBI (u otro cuerpo de policía local). El usuario recibe una demanda urgente sobre la detección en el equipo de material con derechos de autor descargado de forma ilegal y una multa (normalmente, de 200 dólares) para recuperar el acceso.

El ataque puede detenerse con una herramienta antivirus que contenga su propio sistema operativo para evitar entrar en Windows (por ejemplo, Sophos Bootable Anti-Virus). Una vez que la herramienta está en funcionamiento, los usuarios pueden escanear el sistema, eliminar la infección y restaurarlo.[41]

Por desgracia, también hemos observado un número cada vez mayor de infecciones que cifran por completo los discos duros de los usuarios con potentes tecnologías de cifrado y envían de forma segura a los delincuentes la única clave. En julio de 2012, detectamos una variedad que amenazaba con proporcionar a la policía una contraseña especial para revelar archivos de pornografía infantil en el equipo de la víctima.[42]

En casi todos los casos, el uso de un programa antivirus actualizado puede impedir la instalación y la ejecución del ransomware. Pero si no ha protegido el equipo y sufre un ataque con cifrado, probablemente sea demasiado tarde. Algunos cifrados de ransomware pueden deshacerse (Sophos dispone de herramientas gratuitas que pueden ser útiles), pero solo si los delincuentes han cometido errores criptográficos. En ciertas ocasiones no tienen remedio, por lo que la prevención es siempre la medida más aconsejable.

Más información sobre ransomware

5 mitos sobre la navegación segura por Internet

James Lyne, director de estrategias tecnológicas, explica qué es el ransomware

OS X y Mac: más usuarios y más riesgos

Incluye datos de investigaciones de SophosLabs

A la mayoría de los creadores de programas maliciosos les ha resultado más rentable atacar Windows que aprender las técnicas necesarias para dirigir los ataques a la comunidad más reducida de usuarios de OS X. Pero cada vez más empresas e instituciones gubernamentales utilizan equipos Mac, y los delincuentes están al tanto de la situación.

Según el analista Frank Gillette, de Forrester Research, "casi la mitad de las empresas de 1000 empleados o más proporcionan equipos Mac a, por lo menos, algunos de ellos y esperan que la cantidad aumente en un 52 % en 2012".[43] Además, el uso de dispositivos personales en el trabajo está haciendo que se introduzcan aún más de forma extraoficial, ya que suelen ser los dispositivos elegidos por los ejecutivos para acceder a Internet o a aplicaciones en la nube. Dado el aumento del uso de Mac, muchos departamentos informáticos deben evaluar de forma objetiva, mitigar y anticipar por primera vez las amenazas de programas maliciosos relacionadas con el sistema. Y los riesgos, sin duda, están aumentando.

Antivirus falsos y Flashback: discípulos cada vez más ágiles de los programas maliciosos para Windows

En 2011 observamos un ataque continuado contra usuarios de Mac, provocado por la familia de programas maliciosos MacDefender. El programa malicioso, un antivirus falso, constituyó el primer ataque significativo contra Mac distribuido a través de páginas de resultados de búsquedas que llevaban a los usuarios a sitios legítimos contaminados con malware.

A estas alturas, vale la pena analizar MacDefender porque demuestra que los programas maliciosos para Mac siguen la misma trayectoria que los antiguos ataques contra Windows. A la hora de predecir el futuro de los programas maliciosos para Mac, resulta prudente observar los peligros a los que se enfrentan en la actualidad los usuarios de Windows. Por ejemplo, cabría esperar nuevos ataques personalizados basados en polimorfismos del lado del servidor.

Con técnicas prestadas de MacDefender e innovaciones propias, los creadores de la red de bots Flashback (también conocida como OSX/Flshplyr) infectaron más de 600 000 equipos Mac durante la primavera de 2012. Flashback apareció por primera vez como un programa de instalación falso de Adobe Flash a finales de 2011. En abril de 2012, Flashback empezó a instalarse mediante descargas automáticas aprovechando una vulnerabilidad de Java sin corregir en OS X, semanas después de que Microsoft proporcionara un parche a los usuarios de Windows. Apple terminó corrigiendo OS X 10.7 y 10.6, pero no otras versiones anteriores. En el punto más álgido de la infección, el antivirus gratuito para Mac de Sophos detectó programas maliciosos relacionados con Flashback en alrededor del 2,1 % de los equipos Mac protegidos.

A pesar de que tanto MacDefender como Flashback ya no son igual de eficaces, ambos demuestran que los creadores de programas maliciosos para Mac están ganando agilidad. Además, hemos observado cambios en los mecanismos de distribución de programas maliciosos conocidos e intentos de aprovechar vulnerabilidades de día cero.

Representación de los programas maliciosos para Mac OS X

Durante una semana normal, SophosLabs detecta 4900 muestras de programas maliciosos para OS X en equipos Mac. El gráfico contiene una representación del malware para Mac detectado en la semana del 1 al 6 de agosto de 2012

OSX/FkCodec-A	**26 %**	OSX/Flshplyer-D	**3,2 %**
OSX/FakeAV-DWN	**13,28 %**	OSX/FakeAV-A	**2,8 %**
OSX/FakeAVZp-C	**13 %**	OSX/DnsCha-E	**2,7 %**
OSX/FakeAVDl-A	**8,6 %**	OSX/RSplug-A	**2,4 %**
OSX/FakeAV-DPU	**7,1 %**	OSX/Flshplyr-E	**2,4 %**
OSX/FakeAVDl-B	**6,2 %**	OSX/FakeAV-FNV	**2,3 %**
OSX/SafExinj-B	**4,1 %**	OSX/Jahlav-C	**2,1 %**
OSX/FakeAV-FFN	**3,3 %**		

Fuente: SophosLabs

Morcut/Crisis: más sofisticado y virtualmente más peligroso

Para aportar ganancias a los ciberdelincuentes, los programas antivirus falsos suelen convencer a los usuarios para que adquieran software que no necesitan y proporcionen información de tarjetas de crédito personales. Para la mayor parte de las empresas, los inconvenientes de los antivirus falsos han sido relativamente moderados, pero los programas maliciosos como OSX/Morcut-A (también conocido como Crisis), descubierto por primera vez a finales de julio de 2012, suponen riesgos mayores.

Morcut es un programa espía y puede vigilar de forma remota prácticamente cualquier tipo de comunicación de los usuarios: coordenadas del ratón, mensajería instantánea, datos de llamadas de Skype, ubicaciones, cámaras y micrófonos de equipos Mac, el contenido del portapapeles, pulsaciones del teclado, aplicaciones en funcionamiento, direcciones web, capturas de pantalla, calendarios y libretas de direcciones, alertas, información de dispositivos e incluso metadatos de los sistemas de archivos.

Morcut se hace pasar por un archivo JAR (Java Archive) supuestamente firmado de forma digital por VeriSign. Si el usuario lo instala, Morcut implementa componentes del controlador del núcleo para ocultarse y ejecutarse sin autenticación del administrador;[44] un componente de puerta trasera que abre el Mac a otros usuarios de la red; funciones de mando y control para aceptar instrucciones remotas y adaptar su comportamiento; y, sobre todo, código para robar datos del usuario.

La propagación de Morcut puede convertirse en una amenaza muy seria para el cumplimiento de las normativas y la seguridad interna de las empresas. Por las posibilidades que ofrece, resulta especialmente útil en ataques selectivos diseñados para obtener información sobre usuarios conocidos de Mac que ocupan puestos empresariales importantes. A diferencia de la mayoría de programas maliciosos para Mac antiguos, también demuestra un gran dominio de las técnicas de programación, las funciones y los posibles puntos débiles de los sistemas Mac. Ya están apareciendo técnicas de puertas traseras similares en otros sitios. Por ejemplo, hace poco, las encontramos incrustadas por primera vez en OSX/NetWrdRC-A, un kit primitivo, lleno de errores y fácil de detener.[45] Pero es una señal de que el futuro nos depara ataques más sofisticados y peligrosos.

Más información sobre los nuevos riesgos para OS X

Herramienta gratuita: Sophos Anti-Virus para Mac

Andrew Ludgate, de SophosLabs, analiza los programas maliciosos para Mac

Programas maliciosos de Windows ocultos en equipos Mac

Gran parte del malware detectado en equipos Mac son programas maliciosos diseñados para Windows. Durante muchos años, los usuarios de Mac no les han prestado atención creyendo que no pueden dañar sus sistemas y sin tener en cuenta los daños que pueden causar a los usuarios de Windows. Pero los administradores informáticos encargados de entornos multiplataforma (o que trabajan con socios y clientes que utilizan Windows) probablemente no opinen igual. Además, las particiones de Windows de los equipos Mac de doble arranque, así como las sesiones virtuales de Windows realizadas en Parallels, VMware, VirtualBox e incluso el programa de código abierto WINE, sí pueden sufrir infecciones.

A veces, los usuarios de Mac que necesitan utilizar programas de Windows de forma esporádica deciden descargarlos de terceros y crean claves de licencias de forma ilegal utilizando generadores que incluyen programas maliciosos como Mal/KeyGen-M (una familia de generadores de claves "troyanizados" que hemos detectado en alrededor de un 7 % de los equipos Mac con Sophos Anti-Virus instalado).

Otra fuente habitual de programas maliciosos de Windows en equipos Mac hoy en día son los archivos de TV o películas de Windows Media falsos que contienen enlaces web de autoreenvío y prometen proporcionar el códec necesario para ver el vídeo pero, en lugar de eso, distribuyen programas maliciosos de día cero. Normalmente, los archivos de Windows Media no pueden ejecutarse en equipos Mac, pero los usuarios de Mac suelen intercambiarlos para mejorar su clasificación en páginas privadas de rastreo sin darse cuenta de que el contenido es malicioso. Después, los usuarios de Windows intentan reproducir los vídeos e infectan sus equipos.

Mejoras recientes de la seguridad de OS X y limitaciones

Mac OS X, desarrollado inicialmente en BSD UNIX, cuenta con un potente modelo de seguridad. En 2009, con el lanzamiento de OS X 10.6 Snow Leopard, Apple añadió funciones limitadas de detección de programas maliciosos a través del sistema Launch Services Quarantine (LSQuarantine) y la tecnología XProtect. A mediados de 2011, XProtect se convirtió en un servicio dinámico de actualizaciones automáticas con más potencia para detectar y limpiar archivos con características maliciosas.

A mediados de 2012, con OS X 10.8 Mountain Lion, Apple introdujo Gatekeeper para administrar los permisos de ejecución del código obtenido a través de programas de software aprobados. De forma predeterminada, Gatekeeper preautoriza todos los programas firmados con claves de desarrollador oficial de Apple que no se hayan bloqueado anteriormente por usos no permitidos.

Gatekeeper representa una mejora considerable y necesaria de la seguridad de Mac, pero es solo una solución parcial. Los programas de software copiados de memorias USB, ya presentes en el equipo, copiados directamente de un equipo a otro o transferidos mediante sistemas no estandarizados como BitTorrent pueden evadirlo. Y los usuarios individuales con credenciales de administrador pueden cambiar la configuración predeterminada para permitir la instalación de aplicaciones sin firmar sin recibir alertas.[46]

Además, tanto los usuarios como los procesos en ejecución pueden eliminar la marca de LSQuarantine de los archivos, los programas sin firmar pueden autorizarse y ejecutarse con solo hacer clic en ellos con el botón derecho del ratón y abrirlos desde el Finder (en lugar de hacer doble clic en los iconos), y las versiones de OS X anteriores a 10.8 ni siquiera incluyen Gatekeeper.

Por último, Apple preautoriza todos los intérpretes en tiempo de ejecución para las secuencias de comandos de shell de Java, Flash y OS X, que pueden ejecutar cualquier código que deseen. Java y Flash han sido dos vectores de ataque importantes en la plataforma Mac, pero es posible que la situación mejore poco a poco tras el refuerzo reciente de la versión de Java para Mac y la sustitución paulatina de Adobe Flash por HTML5.

Implementación de soluciones anti-malware completas en Mac

Gatekeeper, LSQuarantine y XProtect solo ofrecen una solución parcial. Para proteger los entornos de Mac al completo contra programas maliciosos, son necesarios además los componentes siguientes:

- **Formación de los usuarios:** ayude a los usuarios de Mac a comprender que las amenazas son considerables, que aparecerán más a medida que el sistema gane popularidad en las empresas y que los ataques de ingeniería social pueden estar dirigidos tanto a usuarios de Mac como de Windows.

- **Protección por capas:** hoy en día, es fundamental proteger las estaciones de trabajo de Mac y actualizar la protección constantemente, pero no debemos olvidar los servidores, las puertas de enlace a Internet y al correo, y la infraestructura de red.
  Recuerde que ciertos programas maliciosos capaces de atacar clientes de Mac han aprovechado de forma considerable aplicaciones de servidores como WordPress y Drupal. Tenga en cuenta que muchos escáneres de virus ligeros, sobre todo los incluidos en dispositivos integrados de puertas de enlace y cortafuegos, no detectan malware ni exploits para Mac, por lo que no proporcionan dicha capa de protección

- **Dominio específico de la plataforma Mac:** contrate especialistas o forme al personal existente sobre las características exclusivas de la plataforma. Por ejemplo, puede que las políticas heurísticas de routers y cortafuegos deban reflejar las diferencias en el tráfico de Mac asociado con el registro previo en la caché del navegador web Safari o las difusiones de la detección de redes generadas por los servicios Bonjour de Mac. Una configuración acertada del sistema de archivos puede reforzar los sistemas Mac/Windows de doble arranque contra los ataques.

  Cuando los usuarios de Mac utilizan Mail.app u otros clientes de correo tipo UNIX, un almacenamiento adecuado de los mensajes puede reducir las probabilidades de que los usuarios de Windows abran archivos .zip por equivocación. Los cimientos de Mac están basados en BSD UNIX, pero no la interfaz de usuario. Por eso, resulta muy útil tener conocimientos generales de UNIX, aunque no siempre son suficientes.

- **Políticas y procesos informáticos sólidos:** siempre que sea posible, amplíe las políticas de prácticas recomendadas tipo ITIL tanto a los equipos de Mac como de Windows. Instale rápidamente y de forma automática los parches necesarios tanto de los dispositivos de Mac como de Windows, así como de Java, Flash, las aplicaciones y el propio sistema OS X. Si es posible, controle la capacidad de los usuarios para instalar programas de software nuevos. Asegúrese de que los desarrolladores internos firman de forma digital sus propios programas de OS X. Por último, gestione correctamente los registros. Los equipos Mac registran prácticamente todo en tiempo real, lo que permite identificar amenazas nuevas y bloquearlas mediante cambios en las políticas del cortafuegos o aislando partes de la red.

- **Realismo:** los altos cargos y los grupos creativos que necesitan un control máximo de sus ordenadores suelen utilizar Mac, por lo que puede que tenga que aceptar la presencia de algunos equipos que no sean de confianza. Pero eso no quiere decir que no deban estar protegidos. Ofrezca a los usuarios toda la protección que resulte viable. Además, las empresas no pueden olvidar los requisitos legales asociados con las notificaciones sobre filtraciones y seguridad. La imposición de dichos requisitos puede ser especialmente importante cuando se trata con altos cargos ejecutivos. Según muchos expertos en seguridad, cada vez es más difícil proteger los perímetros y todos los sistemas deberían tratarse como si no fueran de confianza, no solo los equipos Mac.

Las autoridades realizan arrestos y desarticulaciones importantes

Más información sobre programas maliciosos

El dinero que esconden los programas maliciosos

A la hora de proteger sus sistemas y recursos, los profesionales de la seguridad dependen principalmente de sí mismos. Pero en 2012 recibimos más ayuda de las autoridades, lo que supone un gran alivio.

En quizás uno de sus logros más destacados y como continuación a los arrestos de los conocidos delincuentes de LulzSec realizados en 2011, las autoridades federales de los Estados Unidos consiguieron la cooperación de uno de los principales integrantes de la banda, Héctor Xavier Monsegur ("Sabu"). Después de mucho tiempo criticando duramente al gobierno norteamericano bajo el apodo de Sabu, al parecer, Monsegur se prestó a colaborar en secreto durante meses para ayudar a preparar la incriminación de los responsables de ataques contra la CIA, el Pentágono, el Senado de los Estados Unidos, el organismo británico contra la delincuencia organizada SOCA y muchas otras instituciones importantes. Monsegur ayudó a capturar a Jake Davis (también conocido como Topiary) en las islas Shetland, donde según se dice escondía 750 000 contraseñas robadas. En agosto de 2012, los fiscales solicitaron un nuevo retraso de seis meses en la sentencia de Monsegur para poder seguir contando con su colaboración.[47]

Es posible que LulzSec haya sido el caso más comentado del año, pero ni mucho menos ha sido el único. El 2012 comenzó con la extradición del supuesto ciberdelincuente ruso Vladimir Zdorovenin a los Estados Unidos. Zdorovenin estaba acusado de instalar registradores de pulsaciones en los equipos de usuarios norteamericanos con el fin de robar números de tarjetas de crédito y utilizar las cuentas para realizar compras aparentemente legítimas en sus propios negocios electrónicos, además de introducirse en las cuentas de los servicios financieros de las víctimas para manipular precios de acciones.[48] Zdorovenin se declaró culpable de conspiración y fraude electrónico.[49]

Durante el mes de mayo, el cerebro de Bredolab, una red de bots que llegó a secuestrar 30 millones de ordenadores en su momento de máximo apogeo, fue condenado a cuatro años de cárcel en Armenia. Según los fiscales, el alquiler del acceso a la red a delincuentes para el envío de correo no deseado y programas maliciosos aportaba a Georg Avanesov unos beneficios de 100 000 euros mensuales. En su punto más álgido, Bredolab llegó a emitir más de 3000 millones de mensajes de correo electrónico infectados al día, mientras Avanesov disfrutaba de vacaciones de lujo en las islas Seychelles.[50]

En junio, la Oficina Federal de Investigaciones de los Estados Unidos culminó una investigación internacional de dos años sobre fraudes de tarjetas de crédito con el arresto de 24 supuestos ciberdelincuentes de los Estados Unidos, Reino Unido, Bosnia, Bulgaria, Noruega y Alemania, entre otros países. Entre los detenidos se encontraban varios expertos en la creación de troyanos de acceso remoto y estafas de garantías de productos de Apple. Según el FBI, la operación evitó transacciones fraudulentas que podrían haber superado los 205 millones de dólares, y permitió identificar 411 000 tarjetas robadas e informar a 47 empresas que corrían peligro.[51]

A finales del mismo mes, la policía de Tokio arrestaba a seis individuos en relación con una aplicación que infectaba teléfonos inteligentes Android, robaba datos personales y solicitaba pagos. Según la policía, 9252 personas habían descargado ya la aplicación maliciosa y 211 de ellas estaban decididas a pagar el importe solicitado (más de 250 000 dólares en total).[52]

Más tarde, en el mes de julio, la unidad de la policía británica contra la ciberdelincuencia PCeU informó sobre las duras sentencias impuestas a tres ciudadanos de los países bálticos acusados de utilizar el troyano SpyEye para realizar robos en cuentas bancarias del Reino Unido, Dinamarca, Países bajos y Nueva Zelanda.[53]

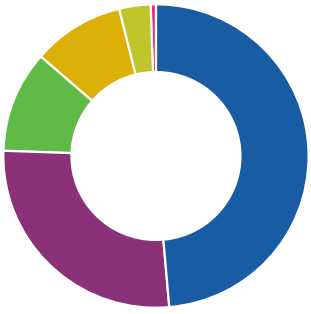
Días más tarde, la policía belga desmantelaba los equipos secundarios de mando y control utilizados por la enorme red de bots Grum, justo una semana después de hacerse pública su existencia.[54] Poco más tarde, otro equipo conseguía deshabilitar los ordenadores principales de mando y control de la red en Panamá y Rusia, acabando con el sistema responsable de alrededor del 17 % del correo no deseado mundial.[55]

Principales 12 países en generación de spam

1. India	**12,19 %**	7. Rusia	**3,34 %**
2. Estados Unidos	**7,06 %**	8. Francia	**3,04 %**
3. Italia	**6,95 %**	9. Pakistán	**2,95 %**
4. Corea	**5,37 %**	10. Polonia	**2,77 %**
5. Brasil	**4,17 %**	11. Indonesia	**2,73 %**
6. Vietnam	**4,16 %**	12. China	**2,73 %**

Porcentaje de todo el spam
Fuente: SophosLabs

Fuentes de spam por continente



Asia	**48,66 %**
Europa	**27,07 %**
Sudamérica	**10,89 %**
Norteamérica	**9,68 %**
África	**3,20 %**
Oceanía	**0,05 %**

Porcentaje de todo el spam
Fuente: SophosLabs

Aumento del número de ataques selectivos peligrosos

Al mismo tiempo que las autoridades empezaban a actuar de forma más eficaz en la lucha contra los ciberdelincuentes, durante 2012, aumentó también la preocupación por los ciberataques patrocinados por gobiernos y organizados en colaboración con estos para conseguir objetivos estratégicos. Si dichos ataques se confirman y proliferan, ciertos objetivos privados y gubernamentales importantes se enfrentarán a nuevos riesgos muy preocupantes y otros menos vitales necesitarán intensificar la vigilancia para evitar daños colaterales, por ejemplo, reforzando la seguridad de las redes e integrándola con otros servicios de protección para detectar y ahuyentar ataques más rápidamente.[56]

El ataque de Flame fue uno de los más destacados de este tipo en 2012, aunque su importancia y eficacia no están muy claras. Más recientemente, el destructivo troyano Shamoon (Troj/Mdrop-ELD) causó daños considerables en todo el sector energético de Oriente Próximo. Según la BBC y The Register,[57] infectó alrededor de 30 000 ordenadores, consiguiendo dejar fuera de juego la red nacional de compañías petroleras de Arabia Saudita.[58] Poco después, la empresa de gas natural de Qatar RasGas sufrió un ataque que dejó las redes y el sitio web sin conexión, y los sistemas administrativos inutilizables.[59]

También observamos atisbos de ciberataques organizados contra los Estados Unidos. A finales de septiembre, el senador norteamericano Joseph Lieberman informó sobre importantes ataques de DDoS dirigidos recientemente a entidades como Bank of America, JPMorgan Chase, Wells Fargo, Citigroup y PNC Bank, alegando sin pruebas públicas que "procedían de Irán... en respuesta al aumento de las fuertes sanciones económicas impuestas por los Estados Unidos y sus aliados a las instituciones financieras iraníes. Puede decirse que es un contraataque".[60]

Según Bloomberg, independientemente de su procedencia, estos nuevos ataques "han puesto en peligro algunas de las defensas informáticas más avanzadas del país y han sacado a la luz la vulnerabilidad de la estructura".[61]

Por su propia naturaleza, los ciberataques patrocinados por los gobiernos (así como los organizados por equipos privados muy sofisticados y con fuertes alianzas estatales) son difíciles de detectar y probar, e igual de susceptibles a exageraciones. No obstante, los responsables parecen estar desarrollando la capacidad de llevarlos a cabo. Y una vez que lo consigan, la tentación de utilizarla será considerable.

Países seguros y peligrosos

Tasa de exposición a las amenazas por país

Los 10 países más seguros

	TEA		TEA
1. Noruega	**1,81 %**	6. Estados Unidos	**3.82 %**
2. Suecia	**2,59 %**	7. Eslovenia	**4.21 %**
3. Japón	**2,63 %**	8. Canadá	**4.26 %**
4. Reino Unido	**3,51 %**	9. Austria	**4.27 %**
5. Suiza	**3,81 %**	10. Países Bajos	**4.28 %**

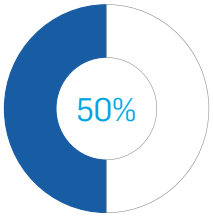
Los 10 países más peligrosos

	TEA		TEA
1. Indonesia	**23,54 %**	6. India	**15,88 %**
2. China	**21,26 %**	7. México	**15,66 %**
3. Tailandia	**20,78 %**	8. EEAAUU	**13,67 %**
4. Filipinas	**19,81 %**	9. Taiwán	**12,66 %**
5. Malasia	**17,44 %**	10. Hong Kong	**11,47 %**

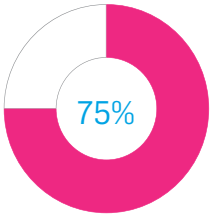
Tasa de exposición a las amenazas (TEA): porcentaje de ordenadores personales que sufrieron ataques de programas maliciosos, tanto fructíferos como fallidos, en un plazo de tres meses.

Fuente: SophosLabs

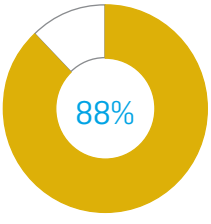
Bienvenido a la era del malware personalizado



El 50 % de nuestras detecciones están basadas en solo 19 identidades de programas maliciosos.



El 75 % de las muestras únicas de programas maliciosos se detectan en solo una empresa.



El 88 % de los programas maliciosos se detecta en menos de 10 empresas.

Fuente: SophosLabs

Ataques polimórficos y selectivos: la larga cola

Más información sobre la larga cola

Richard Wang, de SophosLabs, nos habla de la larga cola

Incluye datos de investigaciones de SophosLabs

El término "larga cola" se ha convertido en una forma habitual de describir los eventos que no pueden clasificarse dentro de la distribución estadística tradicional y tienen lugar de forma aislada o por pares en la parte final de la curva de distribución.
El fenómeno se produce en el comercio minorista, en el que los productos personalizados representan un porcentaje en aumento de las ventas, y cada vez más a menudo entre los programas maliciosos.

El 75 % de los archivos de malware de los que Sophos tiene noticia solo aparecen en una empresa. Este grado de polimorfismo no tiene precedentes. Además, los delincuentes han empezado a desarrollar técnicas más sofisticadas para evitar que los proveedores de seguridad y los departamentos informáticos descubran los ataques. Esta lucha tiene serias implicaciones y, por eso, es importante entender la situación actual, cómo responde Sophos y lo que puede hacer para protegerse.

Polimorfismo: nada nuevo pero más problemático

El polimorfismo no es una idea nueva: los creadores de programas maliciosos llevan 20 años utilizándolo. En pocas palabras, el código polimórfico cambia de aspecto para intentar evitar ser detectado sin cambiar de comportamiento ni objetivos. Los delincuentes esperan que, al tener una apariencia lo suficientemente distinta, los programas antivirus lo pasen por alto o generen tantos falsos positivos que los usuarios los desactiven.

En los ataques polimórficos, el código suele estar cifrado para que parezca que no tiene sentido y va acompañado de un descifrador que lo convierte de nuevo en un formato ejecutable. Cada vez que se descifra, un motor de mutación cambia la sintaxis, la semántica o ambas. Por ejemplo, los creadores de programas maliciosos para Windows han utilizado con frecuencia control de excepciones estructurado para dificultar el flujo y los análisis estáticos de los programas antes de que se ejecuten.[62]

Los virus polimórficos tradicionales son autónomos y deben contener el motor de mutación para reproducirse. Sophos y otras empresas de seguridad se han convertido en expertos a la hora de detectar estas formas de malware. Al tener acceso al motor de mutación, resulta más fácil analizar el comportamiento.

Hoy en día, cada vez más delincuentes utilizan programas maliciosos distribuidos por Internet que dependen del polimorfismo del lado del servidor. Ahora, el motor de mutación y las herramientas relacionadas residen por completo en el servidor. Los delincuentes pueden utilizar estas herramientas para crear archivos con contenido muy diverso sobre la marcha. Los destinatarios del contenido (ya sean archivos .exe de Windows, PDF de Adobe, JavaScript o cualquier otro) solo ven un ejemplo de lo que el motor puede crear. No llegan a ver el propio motor.

Las empresas de seguridad suelen recoger muchos ejemplos diferentes de las creaciones del motor para estudiar su funcionamiento y escribir el código de detección genérico.

Cómo se contrarresta el polimorfismo del lado del servidor

En Sophos hemos utilizado la analogía de la genética para conseguir ser más eficaces en la detección de polimorfismo del lado del servidor y otros ataques. La tecnología de genotipos de comportamientos de Sophos detecta los programas maliciosos nuevos mediante el reconocimiento y la extracción de los "genes" (o componentes del comportamiento). Gracias a un sistema preciso de puntuaciones creado en base a todos los programas maliciosos que hemos recopilado hasta la fecha, podemos identificar combinaciones de genes (genotipos) que diferencian los programas maliciosos del código legítimo. Esta información la comparamos con los genes de archivos benignos para reducir al mínimo el número de falsos positivos.

Se trata de una tecnología flexible y ampliable. Podemos añadir o modificar genes en cualquier momento o generar genes predictivos para detectar los cambios más probables en el futuro. Además, podemos observar cómo reaccionan a las detecciones de otras empresas de seguridad. Los creadores de programas maliciosos suelen hacer cambios que no afectan de forma inmediata a nuestra tecnología de detección. Mediante el ajuste preventivo de los perfiles genéticos para reflejar dichos cambios, es menos probable que los cambios realizados en el futuro nos impidan ver el ataque.

En el caso de ciertos programas maliciosos con polimorfismo del lado del servidor, el tira y afloja entre los proveedores de seguridad y los creadores de programas maliciosos ha aumentado de forma drástica. Por ejemplo, los creadores de programas maliciosos sofisticados intentan determinar constantemente qué partes del código se detectan. Hemos visto cómo algunos delincuentes modifican y sustituyen el código en cuestión de horas. Por supuesto, nosotros también trabajamos sin descanso para adelantarnos y reaccionar.

El polimorfismo del lado del servidor se utilizó por primera vez en sistemas Windows y se ha utilizado principalmente en archivos ejecutables de Windows y contenido web de JavaScript. En 2012, observamos por primera vez su uso en programas maliciosos para Android y creemos que se extenderá a OS X muy pronto. El conocido kit de explotación Blackhole depende en gran medida de esta técnica, aunque esconde muchos otros trucos en la manga.

Ataques selectivos: limitados, concentrados y peligrosos

Como la mayoría de los ataques polimórficos del lado del servidor, Blackhole intenta distribuir su carga de forma generalizada e indiscriminada. Pero otros ataques de la larga cola son mucho más selectivos. Los creadores de programas maliciosos pueden intentar atacar solo a unas cuantas empresas para obtener determinados datos financieros o credenciales bancarias, y preparan los ataques con cuidado mediante investigaciones y reconocimientos previos. Los ataques pueden consistir en mensajes de correo electrónico falsificados que contienen documentos adjuntos infectados y diseñados para tentar a determinados destinatarios.

Por ejemplo, un encargado del departamento financiero puede recibir una hoja de cálculo infectada que, supuestamente, contiene datos de las ventas trimestrales. Si la persona objetivo abre el documento infectado sin que se generen avisos y el programa malicioso se instala, puede permanecer oculto hasta que algún usuario inicie sesión en el sitio de banca electrónica de la empresa. Llegado el momento, el programa malicioso puede robar credenciales mediante el registro de las pulsaciones en el teclado o interceptando el segundo factor de autenticación en un sistema de autenticación de doble factor. El delincuente puede utilizar las credenciales para futuros ataques.

Los ataques selectivos suelen tener como objetivo pequeñas y medianas empresas sin demasiada presencia informática. Y, puesto que los programas maliciosos solo se distribuyen a un número reducido de objetivos, los proveedores de seguridad de las empresas pueden no conocerlos y pasar desapercibidos incluso sin utilizar técnicas de polimorfismo avanzadas. Esta es otra de las ventajas de la técnica basada en genes de Sophos. Nuestro cliente de protección de estaciones de trabajo puede reconocer normalmente programas maliciosos nuevos según su comportamiento y sus características, incluso si no lo hemos detectado anteriormente.

Los delincuentes pueden concentrarse en secuestrar un sitio web determinado que saben que los usuarios de la empresa visitan. Entre los objetivos se incluyen pequeños socios de la cadena de suministro, porque suelen contar con una seguridad informática más débil.[63]

Además de utilizar protección avanzada en las estaciones de trabajo, las pymes pueden reducir los riesgos reservando un mismo equipo para los servicios financieros por Internet, es decir, un equipo que no se utilice para navegar de forma general por Internet ni acceder al correo electrónico o redes sociales.

Protección exhaustiva contra el polimorfismo del lado del servidor

Los profesionales informáticos y de la seguridad deben estar bien preparados para hacer frente a los ataques polimórficos del lado del servidor y selectivos. En primer lugar, es necesaria una protección exhaustiva por capas.

Por ejemplo, el rootkit y la red de bots ZeroAccess pueden detectarse normalmente por la forma en que se conectan a la red de intercambio. Al detectar dichas comunicaciones en el cortafuegos, es posible llegar al equipo infectado.

Las reglas de seguridad deben combinar análisis estáticos y dinámicos para identificar programas maliciosos. Por ejemplo, el contenido sospechoso detectado al analizar por primera vez un archivo (por ejemplo, un cifrado poco habitual) puede vincularse después a actividades sospechosas como conexiones inesperadas a redes.

Los profesionales informáticos deben tener en cuenta el riesgo de las herramientas de administración aparentemente legítimas de los ataques selectivos. Dichas herramientas no se detectan como maliciosas pero pueden tener gran potencia en manos de los delincuentes. La limitación de los tipos de aplicaciones no empresariales que pueden ejecutar los usuarios (función conocida normalmente como restricción de aplicaciones) es una medida eficaz.

Por último, los profesionales de la informática deben contrarrestar de forma agresiva las oportunidades de los delincuentes para encontrar y aprovechar vulnerabilidades, mediante la reducción de las superficies de ataque en las redes, el software y los usuarios. La instalación periódica y automatizada de los parches es siempre una práctica recomendada, pero es incluso más urgente en el panorama de amenazas actual.

Seguridad completa

Para bloquear las amenazas en continua evolución, proteger los datos en todos los puntos, administrar las necesidades de libertad de movimiento de los usuarios y aliviar la presión de los departamentos informáticos, es necesaria una estrategia de protección completa que abarque el ciclo de vida completo de la seguridad. La seguridad completa puede dividirse en cuatro estrategias principales:

- Reducción de la superficie expuesta a ataques: adopte un enfoque activo para vigilar no solo los programas maliciosos, sino también amenazas como las vulnerabilidades, las aplicaciones, los sitios web y el correo no deseado.
- Protección en todos los puntos: asegúrese de que los usuarios están protegidos en cualquier lugar e independientemente del dispositivo que utilicen, y utilice tecnologías para estaciones de trabajo (incluso móviles), puertas de enlace y la nube para intercambiar datos y colaborar que ofrezcan mayor protección sin afectar a los usuarios ni al rendimiento.
- Bloqueo de ataques y filtraciones: es hora de dejar de depender simplemente de las firmas antivirus y buscar capas de detección que bloqueen las amenazas en diferentes fases de su ejecución. Asegúrese de que la protección vigila también los comportamientos peligrosos de los usuarios, no solo del código malicioso.
- Conservación de la productividad: incluida la de los usuarios y el personal informático. Mediante la simplificación de las tareas que quitan demasiado tiempo hoy en día (con sistemas de seguridad que ofrezcan total visibilidad y controles precisos), es posible ver rápidamente si algo falla y corregirlo.

Analice las dos vías de Sophos hacia una seguridad completa

Sophos UTM

Ofrece seguridad completa con un solo dispositivo. Elija solo la protección que necesite en cada momento y la plataforma de hardware, software o virtual más adecuada para su empresa. Todas ellas ofrecen el mismo número de funciones, tanto si necesita proteger 10 como 5000 usuarios. Y gracias a nuestra consola web de administración, podrá gestionar toda la seguridad fácilmente y de forma conjunta.

Suites de seguridad completa de Sophos

Protegen todos los puntos, desde las redes a los servidores, las estaciones de trabajo o los dispositivos móviles. Y, como todos los componentes son productos de Sophos, funcionan mejor en conjunto, resultan más fáciles de usar para que ahorre tiempo y dinero, y cuentan con el respaldo de un proveedor de confianza.

Estaciones de trabajo

Nuestra protección para estaciones evita las salidas fortuitas de datos y la entrada de programas maliciosos sin exceder su presupuesto de seguridad.

Redes

Proteja las infraestructuras de red de forma integral.

Cifrado

Protegemos la información confidencial de su empresa y le ayudamos a cumplir las normativas.

Correo electrónico

Cifrado de mensajes de correo electrónico confidenciales, prevención de fugas de datos y bloqueo de spam.

Dispositivos móviles

Le ayudamos a proteger y administrar sus dispositivos móviles y datos.

Internet

Navegue por Internet de forma más segura y productiva.

UTM

Disfrute de un dispositivo que elimina las complicaciones de gestionar varias soluciones independientes.

Expectativas para el 2013

James Lyne, director de estrategias tecnológicas

En Sophos estamos orgullosos de identificar, gestionar y responder rápidamente a las amenazas.

Aunque los ciberdelincuentes suelen aprovechar cualquier oportunidad, en 2013, la disponibilidad de plataformas de pruebas (algunas de ellas con garantías de devolución de los patrocinadores) puede aumentar las probabilidades de que los programas maliciosos sigan colándose en los sistemas de seguridad tradicionales de un solo nivel. Como consecuencia, creemos que aparecerán ataques más largos y perjudiciales. En respuesta, es probable que la seguridad por capas y las detecciones a lo largo del ciclo de vida completo de las amenazas (no solo en el punto de entrada inicial) vuelvan a convertirse en una tónica importante el próximo año. También creemos que las siguientes cinco tendencias afectarán al panorama de la seguridad informática en 2013.

Errores básicos en servidores web

Durante 2012, observamos un aumento de los ataques de inyección de SQL en servidores web y bases de datos para robar grandes volúmenes de nombres de usuario y contraseñas, tanto en pequeñas como grandes empresas y con fines tanto políticos como económicos. Dado el incremento de este tipo de extracciones, los profesionales de la informática deberán prestar la misma atención a la protección de los equipos que a la protección del entorno de servidores web.

Más programas maliciosos irreversibles

Los programas maliciosos que cifran los datos y los secuestran hasta que el usuario paga un rescate, o ransomware, mejoraron en calidad y volvieron a ganar popularidad en 2012. La disponibilidad de criptografía de clave pública y mecanismos inteligentes de mando y control está haciendo que cada vez sea más difícil (cuando no imposible) reparar los daños. Durante el año que comienza, esperamos ver más ataques que obligarán a los profesionales de la informática a prestar más atención a los mecanismos de protección basados en comportamientos, así como al refuerzo de los sistemas y los procedimientos de copia de seguridad y restauración.

Kits de herramientas de ataque con funciones avanzadas

Durante los últimos 12 meses, los ciberdelincuentes han invertido de forma considerable en kits de herramientas como el kit de explotación Blackhole. Estos kits incluyen funciones incorporadas como servicios web programables, interfaces API, plataformas de control de calidad del malware, anti-análisis, prácticas interfaces para la creación de informes y mecanismos de autoprotección. Durante el próximo año, es probable que seamos testigos de una evolución continuada de la madurez de estos kits y sus funciones, que facilitará aún más el acceso a código malicioso de alta calidad.

Atenuación mejorada de las vulnerabilidades

Aunque el número de vulnerabilidades pareció aumentar en 2012 (incluidos todos los complementos de Java publicados durante los últimos ocho años), la modernización y el refuerzo de los sistemas operativos contribuyeron a que resultara más difícil aprovecharlas, así como la disponibilidad de tecnologías como DEP y ASLR, los espacios seguros, plataformas móviles más restringidas y nuevos mecanismos de arranque de confianza (entre otros). No esperamos que simplemente dejen de aprovecharse, pero su disminución puede verse compensada por un aumento de los ataques de ingeniería social contra una amplia variedad de plataformas.

Problemas de seguridad, integración y privacidad

Durante el pasado año, los dispositivos móviles y aplicaciones como las redes sociales empezaron a estar más integradas y la integración en estos de nuevas tecnologías como NFC, además del uso cada vez más creativo de las funciones de GPS para conectar nuestras vidas digitales y físicas, ofrecerán más oportunidades a los ciberdelincuentes para poner en peligro la seguridad y la privacidad. Esta tendencia puede verse no solo en relación con los dispositivos móviles, sino con la informática en general. En el año que comienza, veremos ejemplos nuevos de ataques basados en estas tecnologías.

Más información sobre protección de dispositivos móviles

Protección de dispositivos móviles: qué nos depara el futuro

Conclusión

La seguridad no debe limitarse a Microsoft.
Los ordenadores personales siguen siendo el principal objetivo del código malicioso hoy en día, pero los ciberdelincuentes también han atacado equipos Mac de forma eficaz con antivirus falsos. Además, a medida que empezamos a utilizar una nueva gama de sistemas operativos con modelos de seguridad y vectores de ataque diferentes, los creadores de programas maliciosos están dirigiendo también sus ataques a los dispositivos móviles. Debemos concentrarnos en proteger y capacitar a los usuarios independientemente de la plataforma, el dispositivo o el sistema operativo que elijan.

Fuentes

1. Microsoft Settles Lawsuit Against 3322 dot org, Reveals Scale of Nitol Botnet in China, http://nakedsecurity.sophos.com/2012/10/05/microsoft-settles-lawsuit-against-3322-dot-org/
2. Beware Remove Your Facebook Timeline Scams, Naked Security, http://nakedsecurity.sophos.com/2012/05/29/beware-remove-your-facebook-timeline-scams/; 'Remove Facebook Timeline' Themed Scam Circulating on Facebook, ZDNet, http://www.zdnet.com/blog/security/remove-facebook-timeline-themed-scam-circulating-on-facebook/9989
3. Twitter DMs From Your Friends Can Lead to Facebook Video Malware Attack, Naked Security, http://nakedsecurity.sophos.com/2012/09/24/twitter-facebook-video-malware/
4. OMG This Is So Cool! Pinterest Hack Feeds Spam to Twitter and Facebook, Naked Security, http://nakedsecurity.sophos.com/2012/09/12/omg-this-is-so-cool-pinterest-hack-feeds-spam-to-twitter-and-facebook/
5. Facebook Teams Up With Sophos and Other Security Vendors, Naked Security, http://nakedsecurity.sophos.com/2012/04/25/facebook-teams-up-sophos-other-vendors/
6. Application Detects Social Network Spam, Malware, Dark Reading, http://www.darkreading.com/security-monitoring/167901086/security/vulnerabilities/240006232/application-detects-social-network-spam-malware.html
7. A Continued Commitment to Security, The Facebook Blog, http://www.facebook.com/blog/blog.php?post=486790652130
8. Latest Black Eye For Dropbox Shines Spotlight On Larger Problem, Dark Reading, http://www.darkreading.com/blog/240004868/latest-black-eye-for-dropbox-shines-spotlight-on-larger-problem.html
9. Another Layer of Security for Your Dropbox Account, Dropbox Blog, 8/27/12, https://blog.dropbox.com/index.php/another-layer-of-security-for-your-dropbox-account
10. Fraunhofer Institute Finds Security Vulnerabilites in Cloud Storage Services, The H Security, http://www.h-online.com/security/news/item/Fraunhofer-Institute-finds-security-vulnerabilites-in-cloud-storage-services-1575935.html
11. 5 Dropbox Security Warnings for Businesses, InformationWeek, http://www.informationweek.com/security/management/5-dropbox-security-warnings-for-business/240005413?pgno=2
12. As you move forward with cloud computing, you may find it valuable to read Security Guidance for Critical Areas of Focus in Cloud Computing V3.0, available from the Cloud Security Alliance at https://cloudsecurityalliance.org/guidance/csaguide.v3.0.pdf
13. Cloud Security: Top 5 Vulnerabilities of the Public Cloud, iPro Developer, http://www.iprodeveloper.com/article/security/public-cloud-security-698785
14. Sophos Technical Paper: Exploring the Blackhole Exploit Kit, http://www.sophos.com/en-us/why-sophos/our-people/technical-papers/exploring-the-blackhole-exploit-kit.aspx
15. The Open Business Engine, http://obe.sourceforge.net/
16. ImmunityProducts.Blogspot.com, http://immunityproducts.blogspot.com/2012/08/java-0day-analysis-cve-2012-4681.html
17. Java Flaws Already Included in Blackhole Exploit Kit Oracle Was Informed of Vulnerabilities in April, Naked Security, http://nakedsecurity.sophos.com/2012/08/30/java-flaws-already-included-in-blackhole-exploit-kit-oracle-was-informed-of-vulnerabilities-in-april/
18. Oracle Updates Java, Supports OS X, Claims Full and Timely Updates for Apple Users, Naked Security, http://nakedsecurity.sophos.com/2012/08/15/oracle-updates-java-claims-full-and-timely-updates-for-apple-users/
19. Unpatched Java Exploit Spreads Like Wildfire, Naked Security, 8/28/12, http://nakedsecurity.sophos.com/2012/08/28/unpatched-java-exploit-spreads-like-wildfire/
20. Attacks on Java Security Hole Hidden in Bogus Microsoft Services Agreement Email, Naked Security, http://nakedsecurity.sophos.com/2012/09/03/java-security-hole-microsoft/
21. CVE-2012-4681 Java 7 0-Day vulnerability analysis, Deep End Research, http://www.deependresearch.org/2012/08/java-7-vulnerability-analysis.html
22. New Security Hole Found in Multiple Java Versions, Naked Security, http://nakedsecurity.sophos.com/2012/09/26/new-security-hole-multiple-java-versions/
23. Visit: http://www.sophos.com/en-us/security-news-trends/security-trends/java-zero-day-exploit-disable-browser.aspx
24. New Security Hole Found in Multiple Java Versions, Naked Security, http://nakedsecurity.sophos.com/2012/09/26/new-security-hole-multiple-java-versions/
25. Philips Hacked as R00tbeer Gang Strikes Again, Naked Security, http://nakedsecurity.sophos.com/2012/08/21/r00tbeer-returns-philips-hacked-poor-passwords/
26. Security Spill at the IEEE, Naked Security, http://nakedsecurity.sophos.com/2012/09/26/ieee-squirms-after-sensational-security-spill/
27. The Worst Passwords You Could Ever Choose Exposed by Yahoo Voices Hack, Naked Security, 7/13/12, http://nakedsecurity.sophos.com/2012/07/13/yahoo-voices-poor-passwords/
28. Philips Hacked as R00tbeer Gang Strikes Again, Naked Security, http://nakedsecurity.sophos.com/2012/08/21/r00tbeer-returns-philips-hacked-poor-passwords/
29. Security Spill at the IEEE, Naked Security, http://nakedsecurity.sophos.com/2012/09/26/ieee-squirms-after-sensational-security-spill/
30. The Worst Passwords You Could Ever Choose Exposed by Yahoo Voices Hack, Naked Security, 7/13/12, http://nakedsecurity.sophos.com/2012/07/13/yahoo-voices-poor-passwords/
31. OWASP Top Ten 2010: The Ten Most Critical Web Application Security Risks, The Open Web Application Security Project (OWASP), http://owasptop10.googlecode.com/files/OWASP%20Top%2010%20-%202010.pdf
32. Source: IDC. http://money.cnn.com/2012/08/08/technology/smartphone-market-share/index.html
33. Source: ComScore. http://www.comscore.com/Press_Events/Press_Releases/2012/9/comScore_Reports_July_2012_U.S._Mobile_Subscriber_Market_Share

34. Angry Birds Malware Firm Fined £50,000 for Profiting From Fake Android Apps, Naked Security, http://nakedsecurity.sophos.com/2012/05/24/angry-birds-malware-fine/
35. Reading this, you might be curious why Sophos Anti-Virus requests permission to send SMS messages. When you do a remote lock or locate, it wants to send you an SMS with latitude/longitude or confirmation that the lock was successful.
36. Disable Windows Sidebar and Gadgets Now on Vista and Windows 7. Microsoft Warns of Security Risk, Naked Security, http://nakedsecurity.sophos.com/2012/07/12/disable-windows-sidebar-gadgets/
37. 25 VeriSign Trusted Shops Found to Have XSS Holes, Naked Security, http://nakedsecurity.sophos.com/2012/02/28/verisign-xss-holes/
38. Insecure WordPress Blogs Unwittingly Host Blackhole Malware Attack, Naked Security, http://nakedsecurity.sophos.com/2012/08/10/blackhole-malware-attack/
39. Android NFC Hack Lets Subway Riders Evade Fares, Naked Security, http://nakedsecurity.sophos.com/2012/09/24/android-nfc-hack-lets-subway-riders-evade-fares/
40. Ransomware: Would You Pay Up? Naked Security, http://nakedsecurity.sophos.com/2012/09/25/ransomware-would-you-pay-up/
41. Reveton/FBI Ransomware: Exposed, Explained and Eliminated, Naked Security, http://nakedsecurity.sophos.com/2012/08/29/reveton-ransomware-exposed-explained-and-eliminated/
42. Ransomware Makes Child Porn Menaces in Broken English, Naked Security, http://nakedsecurity.sophos.com/2012/07/04/ransomware-menaces/
43. Apple Infiltrates the Enterprise: 1/5 of Global Info Workers Use Apple Products for Work, http://blogs.forrester.com/frank_gillett/12-01-26-apple_infiltrates_the_enterprise_15_of_global_info_workers_use_apple_products_for_work_0
44. Mac Malware Spies on Email, Survives Reboots, http://www.informationweek.com/security/attacks/mac-malware-spies-on-email-survives-rebo/240004583
45. Apple Zombie Malware "NetWeird" Rummages for Browser and Email Passwords, http://nakedsecurity.sophos.com/2012/08/24/apple-zombie-malware-netweird-rummages-for-browser-and-email-passwords/
46. Mountain Lion: Hands on With Gatekeeper, http://www.macworld.com/article/1165408/mountain_lion_hands_on_with_gatekeeper.html
47. LulzSec Informant Sabu Rewarded With Six Months Freedom for Helping Feds, Naked Security, http://nakedsecurity.sophos.com/2012/08/23/sabu-lulzsec-freedom/
48. Alleged Russian Cybercriminal Extradited to the US, Naked Security, http://nakedsecurity.sophos.com/2012/01/19/alleged-cybercriminal-extradited-usa/
49. Russian Man Pleads Guilty to Cyber-Fraud Conspiracy in U.S., Bloomberg, http://www.bloomberg.com/news/2012-02-24/russian-national-pleads-guilty-to-cyber-fraud-conspiracy-in-u-s-.html
50. Bredolab: Jail for Man Who Masterminded Botnet of 30 Million Computers, Naked Security, http://nakedsecurity.sophos.com/2012/05/23/bredolab-jail-botnet/
51. FBI Arrests 24 in Internet Credit Card Fraud Ring, Naked Security, http://nakedsecurity.sophos.com/2012/06/27/fbi-arrests-24-in-internet-credit-card-fraud-ring/
52. Android Porn Malware Leads to Arrests in Japan, Naked Security, http://nakedsecurity.sophos.com/2012/06/18/android-porn-malware/
53. Baltic SpyEye Malware Trio Sent to Prison, Naked Security, http://nakedsecurity.sophos.com/2012/07/01/uk-cops-announce-sentencing-of-baltic-malware-trio/
54. Dutch Police Takedown C&Cs Used by Grum Botnet, Security Week, http://www.securityweek.com/dutch-police-takedown-ccs-used-grum-botnet
55. Top Spam Botnet 'Grum' Unplugged, Krebs on Security, http://krebsonsecurity.com/2012/07/top-spam-botnet-grum-unplugged/
56. Midyear Security Predictions: What You Should Know and Look Out For, Dark Reading, http://www.darkreading.com/blog/240002287/midyear-security-predictions-what-you-should-know-and-look-out-for.html
57. 30,000 Machines Infected in Targeted Attack on Saudi Aramco, The Register, http://www.theregister.co.uk/2012/08/30/rasgas_malware_outbreak/
58. Shamoon Virus Targets Energy Sector Infrastructure, BBC, http://www.bbc.com/news/technology-19293797
59. More Dangerous Attacks Against Major Energy Providers: Mystery Virus Attack Blows Qatari Gas Giant RasGas Offline, Cyberseecure, http://cyberseecure.com/2012/08/mystery-virus-attack-blows-qatari-gas-giant-rasgas-offline-the-register/
60. U.S. Senator Blames Iran for Cyber Attacks on Banks, Naked Security, http://nakedsecurity.sophos.com/2012/09/26/us-iran-banks/
61. Cyber Attacks on U.S. Banks Expose Computer Vulnerability, Bloomberg, http://www.bloomberg.com/news/2012-09-28/cyber-attacks-on-u-s-banks-expose-computer-vulnerability.html
62. Taxonomy of Malware Polymorphism, http://www.foocodechu.com/?q=node/54
63. European Aeronautical Supplier's Website Infected With "State-Sponsored" Zero-Day Exploit], http://nakedsecurity.sophos.com/2012/06/20/aeronautical-state-sponsored-exploit/

Ventas en el Reino Unido:
Teléfono: +44 8447 671131
Correo electrónico: sales@sophos.com

Sophos Security Threat Report 2013.es.12.12

SOPHOS