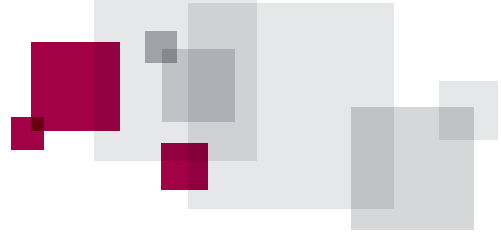




DOCUMENTO TÉCNICO

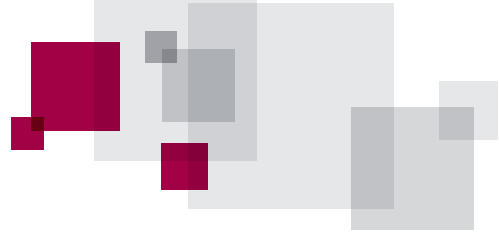
INFORME SOBRE MALWARE: PROTECCIÓN DE EMPRESAS, CONSUMIDORES Y RESULTADOS COMERCIALES



ÍNDICE

- 1 UNA PLAGA QUE ACECHA POR TODA LA RED
- 1 ¿QUÉ ES EL MALWARE?
- 2 ANATOMÍA DE UN ATAQUE DE MALWARE
- 3 MODELO DE NEGOCIO DEL MALWARE
- 4 CONCLUSIÓN
- 4 ACERCA DE VERISIGN





INFORME SOBRE MALWARE: PROTECCIÓN DE EMPRESAS, CONSUMIDORES Y RESULTADOS COMERCIALES

UNA PLAGA QUE ACECHA POR TODA LA RED

Este documento técnico le ayudará a comprender los peligros que entrañan los programas maliciosos, o malware, y los efectos que pueden tener en su negocio por Internet. Conocerá los motivos que impulsan a los delincuentes a propagar estos programas y descubrirá cómo se usan servidores web para esa distribución. Además, aquí se explican las técnicas que tienen a su alcance los administradores para detectar cuándo y cómo se produce un ataque en sus servidores web.

Otros aspectos fundamentales a la hora de estudiar el malware son:

- Métodos de distribución del malware a través de navegadores web en lugar de las técnicas tradicionales, como los mensajes de correo electrónico infectados.
- Motivaciones económicas de los delincuentes actuales para infectar los equipos de los internautas.
- Distribución del malware mediante la infección de sitios web legítimos.
- Herramientas disponibles para infectar la mayor cantidad de páginas posible.
- Técnicas de ataque desarrolladas por los ciberdelincuentes para aprovechar los puntos débiles de los sitios web con el objetivo de infectar miles de ellos a la vez.
- Distribución del código a través de anuncios maliciosos a fin de infectar los sitios web más frecuentados, que suelen estar bien protegidos.

¿QUÉ ES EL MALWARE?

Este término inglés se refiere al software malicioso que circula por Internet y que constituye un problema cada vez más grave. Con estos programas, que los hackers instalan aprovechando las deficiencias de seguridad de los servidores web, los delincuentes obtienen acceso a sitios web ajenos. Dentro del malware se engloban programas desarrollados con distintos fines, como el adware (que muestra publicidad emergente no solicitada) y los troyanos (que recopilan información confidencial, como datos bancarios).

En los últimos años, la cantidad de malware que se propaga a través de los navegadores web ha ido en aumento, ya que los filtros de correo electrónico han conseguido frenar su distribución por medio de mensajes de correo electrónico

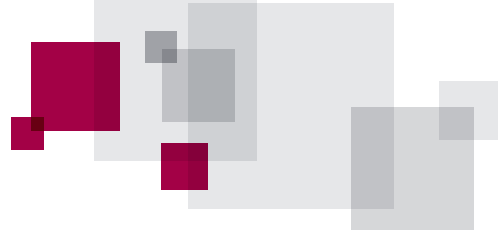
no deseados. Además, el uso extendido de firewalls por parte de empresas y particulares hace que el malware tampoco pueda propagarse fácilmente de un sistema a otro dentro de las redes internas. En cambio, la Red ofrece a los hackers la posibilidad de infiltrarse en un sitio web y, desde ahí, distribuir esos programas maliciosos entre los clientes del sitio.

El código del malware no es fácil de detectar y los ordenadores de sus clientes podrían quedar infectados por el mero hecho de visitar su sitio web. Los usuarios rara vez se dan cuenta de que han sido víctimas de este tipo de ataque, llamado drive-by malware, lo cual supone un peligro añadido, ya que los hackers pueden utilizarlo para propagar virus, tomar el control de los equipos o robar información privada, como números de tarjetas de crédito u otros datos personales.

¿Cómo funciona el drive-by malware? ¿Afecta a los sitios web pequeños?

Este tipo de malware se instala en el equipo del usuario sin su consentimiento. Los ciberdelincuentes aprovechan los fallos de seguridad del navegador o de algún complemento para esconder el malware en una página web como elemento invisible (un marco o un javascript ininteligible) o bien incrustarlo en una imagen (un archivo de Flash o PDF) y que éste se descargue desde el sitio web al equipo del usuario sin previo aviso. Todos los sitios web son susceptibles de ser atacados, pero los más pequeños son más vulnerables porque no suelen contar con los recursos y la experiencia necesarios para detectar y responder rápidamente a estos ataques. Además, cuando un ataque se produce en un sitio web con pocas visitas, pasa inadvertido durante más tiempo y, por lo tanto, puede provocar más daños.





ANATOMÍA DE UN ATAQUE DE MALWARE

Para infectar un equipo a través del navegador web, hay que realizar dos tareas: establecer una conexión con la víctima e instalar el programa en su equipo. En función de la táctica que utilice el hacker, estas dos operaciones pueden suceder muy rápidamente y sin que el usuario se percate de nada. Uno de los métodos utilizados para que el navegador de la víctima ejecute el código malicioso es tan sencillo como pedirle a esa persona que visite un sitio web infectado.

Por supuesto, casi nadie visitaría ese sitio si sabe que está infectado, así que el atacante tiene que enmascarar sus oscuras intenciones. Ahora, los hackers más sofisticados se valen de mecanismos de distribución nuevos y suelen enviar mensajes infectados a las redes sociales, como Facebook, o a través de la mensajería instantánea. Todas estas tácticas han tenido cierto éxito, pero sólo funcionan si el usuario decide visitar el sitio web que se le indica.

Otros delincuentes, en cambio, atacan los sitios web que sus posibles víctimas visitan por voluntad propia. Para ello, el atacante se infiltra en el sitio web objetivo e inserta un pequeño fragmento de código HTML que enlaza con su propio servidor y que se puede ejecutar desde cualquier lugar, incluso desde una página web totalmente diferente. A partir de ese momento, cada vez que un usuario visita la página infectada con este método, el código malicioso puede infectar su equipo.

Mecanismos frecuentes de distribución de malware:

- **Actualizaciones de software:** El malware envía invitaciones a través de las redes sociales para que los usuarios vean un vídeo y, después, se les hace creer que necesitan una actualización de software para verlo. Por supuesto, esa actualización es software malicioso.
- **Publicidad en banners:** Los usuarios hacen clic en un banner que intenta instalar el código malicioso en sus equipos sin que ellos se den cuenta o que les envíe a un sitio web donde se les invita a descargar un PDF con código malicioso oculto. También es posible que se les solicite sus datos bancarios para proceder a la descarga.
- **Documentos descargables:** Se anima al usuario a abrir un programa de confianza, como Microsoft Word o Excel, que en realidad contiene un troyano preinstalado.
- **Ataque de interposición “Man-in-the-Middle”:** El usuario piensa que se está comunicando con un sitio web de confianza, pero la realidad es que un ciberdelincuente está recopilando la información que ese usuario comparte con el sitio, como su nombre de usuario y contraseña. También es posible que el delincuente se infiltre en una sesión y la mantenga abierta después de que el usuario piense que la ha cerrado, de modo que tiene carta blanca para realizar operaciones fraudulentas. Así, el estafador puede transferir dinero si el usuario había iniciado la sesión en su banco, o bien robar el número de tarjeta de crédito durante una transacción de compra por Internet.
- **Keyloggers:** Se engaña al usuario para que descargue un keylogger con cualquiera de las técnicas descritas anteriormente. Ese programa malicioso hace un seguimiento de actividades específicas, como las acciones del ratón o el teclado, y toma capturas de pantalla para registrar datos bancarios o de la tarjeta de crédito.



MODELO DE NEGOCIO DEL MALWARE

¿Cómo obtienen beneficios los delincuentes a partir del malware? Los ordenadores infectados pueden constituir una fuente de ingresos de muchas maneras. Una de las más sencillas es la publicidad: al igual que muchos sitios web obtienen ingresos por mostrar anuncios, el estafador puede cobrar por los anuncios que muestra el malware. Otra alternativa es la extorsión. Cuando cuenta con una amplia red de equipos infectados, o botnet, el atacante puede extorsionar fácilmente los propietarios de sitios web. Gracias a esos recursos ilícitos, el delincuente puede sobrecargar un sitio web, lo que constituye un ataque de denegación de servicio (Denial of Service, DoS), para después contactar al propietario y exigirle un pago a cambio del cese del ataque. Además, los delincuentes suelen valerse de equipos infectados para recopilar información personal de gran valor, como los datos de acceso a bancos por Internet. Ese tipo de malware, conocido como stealer o troyano bancario, es uno de los más sofisticados y difíciles de detectar. Una vez instalado el programa, el estafador podrá utilizar los datos recopilados de forma fraudulenta o venderlos a terceros que estén interesados en sacar provecho de ellos.

¿Qué son las listas negras? ¿Por qué hay que mantenerse fuera de ellas?

Dado el riesgo que supone el malware, los motores de búsqueda como Google, Yahoo y Bing bloquean aquellos sitios web que tienen código malicioso, es decir, los incluyen en una "lista negra". A partir de ese momento, el motor de búsqueda avisa a los posibles visitantes de que el sitio no es seguro, o bien lo excluye por completo de los resultados.

Por mucho que optimice su sitio web para obtener mejores posiciones en las búsquedas, si entra en una lista negra, los efectos en su negocio pueden ser devastadores. Además, la inclusión en listas negras puede producirse sin previo aviso, el propietario no suele enterarse y es un proceso muy difícil de rectificar. Por lo tanto, resulta fundamental tomar las medidas necesarias para evitar que esto ocurra y, así, garantizar el éxito del sitio web a largo plazo.

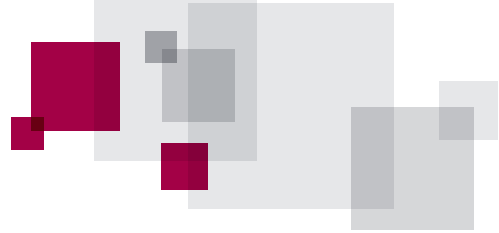
VERISIGN, LÍDER INDISCUTIBLE EN SEGURIDAD EN INTERNET

A mediados de los años 90, VeriSign fue la primera empresa en lanzar una solución SSL al mercado y, a día de hoy, sigue siendo el principal proveedor de certificados SSL, además de constituir la marca de seguridad en Internet más reconocida en todo el mundo. La reputación que VeriSign ha labrado ante consumidores y negocios por Internet es fruto de muchos años a la cabeza del mercado y con la tecnología más avanzada en todas las soluciones SSL.



Además de la tranquilidad que supone para el cliente contar con un certificado SSL de calidad demostrada, VeriSign se esfuerza constantemente por cubrir todas sus necesidades mediante la ampliación de la oferta de certificados SSL, incorporando nuevos estándares e integrando tecnologías y soluciones adicionales. Ahora, VeriSign da continuidad a esta tradición con la inclusión de un escaneo del sitio web al día para detectar si hay malware, lo que garantiza que su sitio web, su preciada marca y la información privada de sus clientes quedan protegidos de los peligros que nacen y evolucionan constantemente en la red de redes.





CONCLUSIÓN

Las ventas de servicios y productos por Internet han aumentado de manera espectacular durante la última década, aunque ese incremento del uso de la Red en el día a día también se ha traducido en un aumento de las actividades delictivas en este medio. Ahora mismo, el malware tiene una presencia cada vez mayor y está poniendo en peligro el crecimiento del comercio electrónico debido al miedo de los consumidores ante el riesgo que podrían correr sus datos personales. Eso tiene un impacto directo en los resultados de las empresas que comercian por Internet e impide que desarrollen todo su potencial, por lo que es preciso que cuenten con un método eficaz para combatir el malware.

VeriSign ofrece una exhaustiva solución de confianza que contribuirá al éxito de su empresa, ya que combina los mejores certificados SSL con funciones innovadoras que garantizan una supervisión periódica de los sitios web que ven sus clientes para evitar la incorporación de malware. Gracias a esto y al sello de VeriSign, que es la marca de confianza más reconocida mundialmente, el cliente sabrá que puede interactuar con su negocio con total tranquilidad. Así pues, si quiere que sus clientes perciban su sitio web como un comercio electrónico de confianza, elija los certificados SSL de VeriSign.

ACERCA DE VERISIGN

VeriSign es el proveedor de referencia de servicios para infraestructuras de Internet en la era digital. Cada día, nuestra infraestructura de Internet ayuda a empresas y particulares de todo el mundo a comunicarse y establecer relaciones comerciales con plena confianza.

Visite www.Verisign.es si desea obtener más información.

