

Exploits en la red: del problema a la solución

Resumen

Este documento discute el problema de los *exploits* en la red, y los peligros asociados con ellos. También detalla las precauciones que deberían tener en cuenta los usuarios para minimizar su exposición a los riesgos causados por estos programas que se aprovechan de las vulnerabilidades del sistema.

Prefacio

La expansión de las aplicaciones maliciosas es uno de los principales problemas que afectan hoy día a los usuarios de Internet.

A diferencia de los virus antiguos, cuya presencia en el sistema era muy visible, los códigos maliciosos actuales son silenciosos y trabajan sigilosamente. A continuación presentamos un caso que resultará demasiado familiar para muchos usuarios de ordenadores:

Después de navegar por Internet durante un par de meses usando un nuevo ordenador portátil o de escritorio —o incluso en un ordenador antiguo donde se ha hecho una instalación nueva de Windows— notamos que este se comporta de manera extraña.

Aparecen ventanas emergentes y alertas sobre errores de Windows u otras aplicaciones. Además, comienzan los problemas para iniciar el sistema y una serie de actividades extrañas que no se habían registrado anteriormente. Desafortunadamente, no habíamos tenido la precaución de instalar una aplicación de seguridad antes de navegar por la red.

Tratamos entonces de recuperar el tiempo —y la seguridad— perdidos, instalando un programa antivirus. No será sorprendente que el primer análisis detecte amenazas activas en la memoria y varios códigos maliciosos en el disco duro.

Al ver este resultado, intentamos descubrir qué hemos hecho o qué sitios hemos visitado, para que nuestro ordenador se haya llenado de estos elementos indeseables.

¿Hemos descargado archivos ejecutables de un sitio sospechoso? ¿Participamos de algún tipo de intercambio de información en una red punto a punto?

¿Respondimos a algún mensaje de correo electrónico no solicitado, o que pudiera ser fraudulento?

¿Ha tenido acceso a nuestro ordenador otra persona (familiares, compañeros de trabajo) que haya realizado alguna de las acciones mencionadas?

Todo puede ser posible. La cuestión es, en realidad, cómo prevenir que estas infecciones ocultas vuelvan a ocurrir.

Una introducción a los *exploits* de la red

Si bien no existe una definición universal de exploit, esencialmente el término se refiere a cualquier código diseñado para exponer las vulnerabilidades de otras aplicaciones, o aprovecharse de ellas.

Los *exploits* de la red trabajan aprovechándose de las fallas de los navegadores o sus complementos, y de otros programas con acceso a Internet, incluyendo Microsoft Word, Adobe Acrobat y otras aplicaciones de uso habitual.

Estas amenazas pueden tomar muchas formas diferentes: descargas forzadas, instalación de códigos maliciosos ocultos, infecciones silenciosas o automatizadas, pero todas tienen el mismo resultado: el ordenador se infecta solamente navegando por Internet, sin que sea necesario hacer nada especial como, por ejemplo, descargar un archivo.

Los *exploits* permiten que los códigos maliciosos se instalen silenciosamente en el sistema, sin el conocimiento del usuario. Esto puede tener como consecuencia el robo de información, el mal funcionamiento del ordenador o su incorporación a una *botnet*, y otros problemas serios.

Ciclo de vida de la vulnerabilidad

El diagrama que está a continuación ilustra el ciclo vida de la vulnerabilidad de una aplicación, y del *exploit* que depende de ella [1]:



1. La aplicación es lanzada al público.
2. Un investigador corrupto, o un delincuente informático descubre una vulnerabilidad en el programa, pero no da aviso al desarrollador. En lugar de esto, entrega esta información a los escritores de códigos maliciosos a cambio de dinero u otro tipo de recompensa. Se crea entonces una aplicación que se aprovecha de dicha vulnerabilidad. Los desarrolladores de soluciones de seguridad aún no conocen estos programas dañinos, de modo que no pueden detectarlos. Generalmente, este tipo de amenazas se conoce como **código malicioso de día cero**.
3. El desarrollador de la aplicación vulnerable se entera del error a través de canales públicos. Esto puede ocurrir de varias formas. La más común es que información sobre el hallazgo se filtre en foros clandestinos que los piratas comparten. También puede tomar conocimiento por medio de los propios usuarios, por comunicaciones de otros desarrolladores, o por trabajos de investigación paralelos realizados por investigadores honestos.
4. El código de prueba de concepto no lleva una carga maliciosa. Su función es, simplemente, probar la viabilidad de los hallazgos, y demostrar que, sin el parche adecuado, la vulnerabilidad realmente podría ser explotada. Un **POC** (*Proof-of-concept*, código de prueba de concepto) se usa principalmente para convencer de esto al desarrollador del programa en riesgo.
5. Una vez que el desarrollador evalúa el informe de vulnerabilidad, y concluye que es necesario crear un parche, comienza a trabajar en ello.
6. El desarrollador crea un parche para corregir la vulnerabilidad detectada. Posteriormente se distribuye la actualización de seguridad, usando el procedimiento estándar de la aplicación en cuestión.
7. El usuario instala el parche del fabricante, para proteger la aplicación contra posibles explotaciones de la vulnerabilidad.

En algún punto entre las etapas dos y siete, el *exploit* sale a la luz y comienza a infectar usuarios vulnerables.

Este período se denomina **ventana de oportunidad**, ya que los piratas informáticos pueden adueñarse de los sistemas de los usuarios sin que estos lo sepan, aprovechándose de las vulnerabilidades que no fueron detectadas o solucionadas.

[1] Cuando un investigador de seguridad informa la existencia de una vulnerabilidad a un desarrollador de aplicaciones, sin difundir este dato a otras personas, se reduce enormemente la probabilidad de que la falla del programa sea aprovechada con fines maliciosos.

Después que la vulnerabilidad ha sido corregida con el parche correspondiente, se pueden divulgar los detalles del error sin poner en riesgo a los usuarios, siempre que estos hayan actualizado sus sistemas. Las investigaciones muestran que aquellos usuarios que no instalan prontamente los últimos parches disponibles, corren un alto riesgo de que sus ordenadores se infecten con algún *exploit* que circula por la red.

Cómo funcionan los exploits

Tan pronto como los delincuentes informáticos se enteran de la existencia de una vulnerabilidad, comienzan a escribir códigos maliciosos para aprovecharse de ella. Esto podría implicar el esfuerzo colectivo de varios grupos de piratas o el trabajo de un solo individuo altamente cualificado, que en algunas ocasiones es también el descubridor del error.

En ocasiones, se lanzan a la venta en el mercado clandestino paquetes de herramientas para crear *exploits*. Estas aplicaciones cuestan entre 350 y 700 euros y cuentan con un servicio de actualizaciones de muy bajo coste, que son distribuidas a los usuarios cada vez que aparecen *exploits* nuevos y se agregan automáticamente al paquete, siguiendo el mismo método que las aplicaciones legítimas.

Los ejemplos más destacados de tales paquetes incluyen los programas **WebAttacker**, de origen ruso, y **MPack**. Estos conjuntos de herramientas contienen un grupo de *exploits* que se aprovechan de las vulnerabilidades conocidas en complementos desarrollados por otras compañías, o en funciones del navegador (las cuales van desde la vulnerabilidad del [cursor animado de Microsoft](#), hasta la sobrecarga de la memoria intermedia de QuickTime de Apple, o múltiples errores descubiertos en los controles ActiveX, JavaScript, y otras extensiones de Internet Explorer).

Una vez que los atacantes obtienen un *exploit*, necesitan esconderlo de forma tal que los usuarios que visitan ciertos sitios —ya sea de manera deliberada, o accidentalmente— sean infectados automáticamente, y sin que tomen conocimiento de esto.

Existen varias formas de atraer víctimas a un sitio malicioso, pero típicamente los piratas usan uno o más de los siguientes recursos:

- Envían mensajes de correo electrónico no solicitados para hacer que los usuarios visiten un sitio mantenido por el delincuente informático. Para conseguir este objetivo también se utilizan otras técnicas sofisticadas, como la suplantación de direcciones DNS (*Domain Name Service*, servicio de nombres de dominio), los ataques de ingeniería social y otras tácticas predatorias.
- Crean una serie de sitios infecciosos cuyos nombres sean similares a los de entidades legítimas, registrando direcciones en Internet que apenas se diferencien de las originales (por ejemplo, [microsooft.com](#) o [dowload.com](#)).
- Infectan sitios web pertenecientes a entidades legítimas, infiltrando los códigos maliciosos antes de que sus administradores puedan bloquear la intrusión. El Banco de la India sufrió un ataque de este tipo recientemente.
- Ponen enlaces a elementos multimedia en sitios de encuentros sociales, tales como FaceBook o MySpace, que en realidad apuntan a códigos maliciosos externos. Estos se aprovechan de las vulnerabilidades de los complementos desarrollados por otras empresas y que son necesarios para ejecutarlos.

Ganando dinero con los *exploits*: un modelo de negocio

Los *exploits* pueden generar un rédito importante para sus desarrolladores.

Algunas fuentes estiman que las ganancias de la delincuencia informática superan a las del contrabando de drogas, y un gran porcentaje de este dinero proviene de la venta de este tipo de programas.

Existen varias opciones para obtener beneficios económicos gracias a los *exploits*:

1. Infectar los ordenadores de los usuarios con todo tipo de códigos maliciosos que pueden ser usados para generar ingresos a través de chantaje, la venta de falsas aplicaciones contra programas espía o de información personal adquirida por medio de registradores de pulsaciones, etc.
2. Vender estos programas maliciosos a otros delincuentes.
3. Utilizarlos como medio de extorsión a un desarrollador de programas.

Combatiendo la amenaza de los *exploits*

Existe una serie de pasos muy sencillos que los usuarios pueden seguir para proteger sus ordenadores de la amenaza de los *exploits*:

1. Mantener actualizados los parches del sistema, y utilizar siempre la última versión del navegador.
2. Desactivar funciones de programación innecesarias, como códigos ActiveX, o permitir solamente que estas sean usadas en sitios previamente revisados y confiables.
3. No visitar sitios desconocidos, o que puedan resultar poco confiables.
4. Usar programas que examinan el contenido de los sitios web en tiempo real, antes de permitir que el usuario acceda a ellos. Programas como [Link Scanner Pro](#), revisan el código HTML del sitio de destino, para asegurarse de que no tiene amenazas ocultas. La extensión [Finian SecureBrowsing](#) realiza una evaluación del código y de la reputación del sitio, para estimar así la amenaza potencial.
5. Utilizar un cortafuegos que proteja el sistema contra códigos maliciosos del tipo día cero, bloqueando cualquier actividad inadecuada dentro de la red o de las aplicaciones locales. Outpost Firewall Pro 2008 incluirá la posibilidad de armar y personalizar una base de datos de sitios peligrosos cuyo acceso estará bloqueado.

Conclusión

Los *exploits* representan un riesgo real y concreto para los ordenadores, pero mientras los usuarios cuenten con el conocimiento, el sentido común y las aplicaciones de seguridad apropiadas, pueden estar seguros de que estos programas no interferirán en sus vidas digitales.