KASPERSKY lab

TECNOLOGÍA DE PREVENCIÓN AUTOMÁTICA FRENTE A EXPLOITS DE KASPERSKY LAB

Be Ready for What's Next

www.kaspersky.es

1. LA NUEVA AMENAZA INTERNA

Las aplicaciones de terceros representaron el 87 % de las vulnerabilidades detectadas en 2012.[1] Ese mismo año, Kaspersky Lab registró más de 132 millones de aplicaciones en riesgo.

"Kaspersky Lab cree que la mejor forma de abordar esta amenaza de rápida evolución es utilizar una tecnología especializada que ofrezca su propio nivel de protección único contra los exploits dirigidos a las vulnerabilidades de aplicaciones populares."

Los defectos de Oracle Java, Adobe Flash Player y Adobe Reader, junto con los puntos débiles de Microsoft Office, son los objetivos más populares para los exploits delictivos. Entre marzo y agosto de 2013, los investigadores de Kaspersky Lab registraron 8,54 millones de ataques con exploits de Java, lo que supone un aumento del 52,7 % respecto a los seis meses anteriores.

Kaspersky Lab cree que la mejor forma de abordar esta amenaza de rápida evolución es utilizar una tecnología especializada que ofrezca su propio nivel de protección único contra los exploits dirigidos a las vulnerabilidades de aplicaciones populares. Impedir la ejecución de este código malicioso permite evitar que las aplicaciones y los componentes empresariales esenciales se conviertan en pasarelas para ataques a mayor escala.

1 Secunia Vulnerability Review 2013, Secunia Research Lab, 14 de marzo de 2013.

2. EXISTE UNA LAGUNA AL RESPECTO: EL COMPORTAMIENTO TÍPICO DE LOS EXPLOITS

La finalidad de todo exploit es aprovechar las vulnerabilidades del software muy utilizado para ejecutar varios tipos de código malicioso. Para infectar un sistema mediante esta técnica, los delincuentes adoptan una serie de métodos, incluidos los siguientes:

- Atraer a los usuarios a un sitio web malicioso creado ex profeso o a un sitio web auténtico que haya sido atacado e infectado con código malicioso. Algunos delincuentes dirigen sus ataques a sitios auténticos que son populares entre tipos concretos de usuarios, como desarrolladores en grandes empresas. Son los llamados "ataques de abrevadero".
- Embaucar a los usuarios para que descarguen o abran un documento creado especialmente, aparentemente auténtico, como un PDF, un documento de Office o incluso una imagen de aspecto inofensivo.
- Es muy fácil introducir ilegalmente en las empresas dispositivos de almacenamiento extraíbles, como unidades USB con malware que utiliza exploits. En los últimos años, varios estudios han constatado que los usuarios finales que encontraban memorias USB extraíbles en el aparcamiento de su empresa los conectaban a sus equipos, en especial si llevaban la marca de la empresa.[2]

Normalmente, los ataques dirigidos comienzan con un usuario que abre un archivo adjunto de correo electrónico malicioso especialmente diseñado que parece auténtico a primera vista.

2 Bruce Schneier, "Yet Another 'People Plug in Strange USB Sticks' Story", Schneier on Security, https://www.schneier.com/blog/archives/2011/06/yet_another_peo.html

Para obtener más información sobre los exploits a través de soportes extraíbles, visite: http://www.securelist.com/en/blog/208187475/Another_usb_media_infection

3. LA POPULARIDAD LE HACE VULNERABLE: EL SOFTWARE MÁS ATACADO

Casi todos los programas son vulnerables a errores, algunos de los cuales permiten la ejecución de código malicioso sin autorización. Si tenemos en cuenta que un usuario medio tiene alrededor de 72 programas instalados en su equipo,[3] las empresas tienen muchas vulnerabilidades. No obstante, lo cierto es que los delincuentes tienden a dirigir sus ataques a las aplicaciones más populares, porque de este modo se garantiza un gran número de víctimas potenciales; después de todo, para lograr el objetivo, solo se necesita que una persona haga clic.

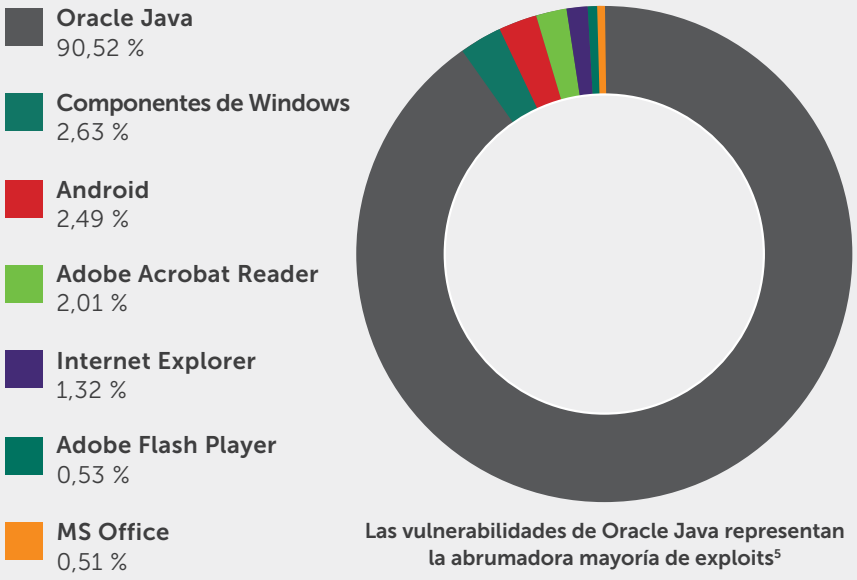
"De los usuarios de Kaspersky Lab que participan en nuestro sistema de inteligencia y detección de amenazas Kaspersky Security Network basado en la nube, el 6,3 % todavía utiliza Windows XP."

Las investigaciones de Kaspersky Lab demuestran que el software más perseguido por los exploits es Oracle Java, que registró el 90,52 % de todos los intentos de explotar vulnerabilidades detectados en 2013. Estas vulnerabilidades son explotadas por ataques ocultos a través de Internet y los nuevos exploits de Java están presentes en muchos paquetes de exploits.[4]

El segundo objetivo más popular de las vulnerabilidades es la categoría de componentes de Windows, incluidos archivos vulnerables del sistema operativo Windows, además de Internet Explorer y Microsoft Office, que Kaspersky asigna a otra categoría. La mayoría de los ataques en esta categoría de componentes se dirigen a una vulnerabilidad descubierta en 32k.sys-CVE-2011-3402, utilizada por primera vez en el famoso exploit Duqu.

3 Secunia Vulnerability Review 2013.

4. Informe de Kaspersky Lab: Java Under Attack – The Evolution of Exploits in 2012-2013, Securelist, 20 de octubre de 2013, http://www.securelist.com/en/analysis/204792310/Kaspersky_Lab_Report_Java_under_attack_the_evolution_of_exploits_in_2012_2013.



Las vulnerabilidades de Oracle Java representan la abrumadora mayoría de exploits[5]

Con el tiempo, la lista de objetivos de software podría cambiar; por ejemplo, Microsoft Office fue el principal objetivo de los ataques en 2010. En abril de 2014, Microsoft empezó a dejar de prestar asistencia a Windows XP y Office 2003, por lo que ya no se desarrollan actualizaciones ni parches de seguridad para este software, lo que deja a algunas empresas expuestas a graves deficiencias que, sin duda, los delincuentes tienen en su punto de mira. De los usuarios de Kaspersky Lab que participan en nuestro sistema de inteligencia y detección de amenazas Kaspersky Security Network basado en la nube, el 6,3 % todavía utiliza Windows XP.

5 http://www.securelist.com/en/images/vlill/stat_ksb_2013_04.png

4. MÉTODOS GENERALES PARA PROTEGERSE FRENTE A EXPLOITS

Las soluciones de Kaspersky Lab utilizan varios métodos de bloqueo de exploits. Por ejemplo, se añaden firmas especiales para el malware que utiliza exploits que permiten la detección de archivos maliciosos (como un archivo adjunto de correo electrónico), incluso antes de que se abra el archivo. La protección proactiva y otras tecnologías permiten la detección y el bloqueo de malware una vez que se abre un archivo vulnerable. Por último, el análisis de vulnerabilidades permite la fácil detección de software vulnerable en cualquier endpoint y puede funcionar de manera coordinada con la gestión de parches y otras funciones de gestión de sistemas para aplicar automáticamente las actualizaciones o impedir la carga de software sin parches.

"Aunque relativamente pocas amenazas escapan a los niveles de seguridad tradicionales, el potencial de daños masivos que un solo exploit podría causar hace imprescindible la introducción de un nivel adicional de seguridad en la empresa."

Por supuesto, las actualizaciones periódicas de los componentes del sistema Windows y otro software instalado es la mejor manera de evitar la mayoría de exploits.

No obstante, en algunos casos, las técnicas cotidianas de protección podrían no ser eficaces. Esto es especialmente cierto en el caso de las vulnerabilidades de día cero, es decir, fallos de software no detectados o que se acaban de descubrir. En estas circunstancias, es difícil para los proveedores de seguridad reconocer los exploits dirigidos a vulnerabilidades de día cero por medio de métodos basados en firmas. Los exploits complejos también pueden utilizar varias técnicas para sortear o superar las tecnologías de protección proactiva. Aunque relativamente pocas amenazas escapan a los niveles de seguridad tradicionales, el potencial de daños masivos que un solo exploit podría causar hace imprescindible la introducción de un nivel adicional de seguridad en la empresa. Ahí es donde entra en juego la prevención automática frente a exploits.

5. PREVENCIÓN AUTOMÁTICA FRENTE A EXPLOITS: FUNCIONAMIENTO

La tecnología para la prevención automática frente a exploits se dirige específicamente contra el malware que aprovecha las vulnerabilidades del software para obtener un punto de apoyo en los endpoints y las redes de la empresa. Incluso si un usuario descarga o abre un archivo malicioso, la tecnología AEP impedirá la ejecución del malware.

Kaspersky ha desarrollado AEP mediante un análisis en profundidad del comportamiento y las características de los exploits más generalizados. Esta función permite a nuestra tecnología diferenciar patrones de comportamiento característicos de los exploits y bloquearlos para que no finalicen su tarea.

Durante el proceso de desarrollo, los equipos de I+D de Kaspersky descubrieron el software y las aplicaciones empresariales que son objeto de ataque con mayor frecuencia, lo que permitió adaptar la tecnología AEP en consonancia. AEP se incluye ahora en las soluciones de seguridad en Internet y antivirus de Kaspersky Lab, donde funciona junto con nuestro módulo estándar Supervisor del sistema para proporcionar un nivel adicional de seguridad que incluye las siguientes capacidades:

CONTROL DE APLICACIONES POTENCIALMENTE VULNERABLES

La tecnología AEP se centra en las aplicaciones atacadas con más frecuencia, como Adobe Reader, Internet Explorer y Microsoft Office. Si estos programas intentan iniciar código o archivos ejecutables inusuales, se activan comprobaciones de seguridad adicionales. A veces, estas acciones son legítimas; por ejemplo, Adobe Reader podría iniciar un archivo ejecutable para buscar actualizaciones. Sin embargo, ciertas características del archivo ejecutable, junto con las acciones asociadas, podrían apuntar a la existencia de actividad maliciosa y, por lo tanto, ser merecedoras de un examen adicional.

SUPERVISIÓN DE LAS ACTIVIDADES ANTERIORES AL INICIO

La manera en que se inicia una aplicación o se ejecuta código y lo que sucede justo antes pueden revelarnos mucha información. Ciertos tipos de comportamiento indican la existencia de actividad maliciosa; la tecnología AEP puede rastrear dicha actividad y detectar el origen del intento de iniciar el código. El origen podría ser el propio software, pero también puede ser el resultado de un exploit. Los datos sobre los comportamientos más habituales de los exploits pueden ayudar a detectar este tipo de actividad, incluso cuando se utiliza una vulnerabilidad de día cero. Por consiguiente, AEP no necesita conocer la naturaleza exacta de la vulnerabilidad explotada para comprender que se está llevando a cabo una actividad maliciosa.

RASTREO DEL ORIGEN DEL CÓDIGO

Algunos tipos de exploits, particularmente los usados en descargas ocultas (es decir, exploits iniciados a través de una página web maliciosa), tienen que ir a buscar su carga desde otro sitio web antes de ejecutarla. AEP puede rastrear el origen de esos archivos, identificar el navegador concreto que ha iniciado la descarga y recuperar la dirección web remota de los archivos.

"La metodología de comprobación y rastreo de Kaspersky, junto a investigaciones continuas y profundas realizadas sobre las aplicaciones empresariales más populares, hace que el riesgo de falsos positivos sea muy bajo. Es posible ejecutar esta función en modo interactivo, si así lo prefiere."

Además, para ciertos tipos de programas, AEP puede distinguir entre los archivos creados con el consentimiento del usuario y los archivos nuevos no autorizados. Cuando se intenta iniciar código sospechoso, esta información puede ayudar a identificar y bloquear un exploit.

IMPEDIR QUE LOS EXPLOITS ACCEDAN A LA VULNERABILIDAD ELEGIDA

AEP puede utilizar una técnica llamada aleatorización forzada del diseño del espacio de direcciones con algunos programas y módulos de software para impedir que los exploits encuentren la vulnerabilidad o el código concretos que necesitan ejecutar.

La tecnología de aleatorización del diseño del espacio de direcciones (ASLR) se ha incluido en el sistema operativo Microsoft Windows desde Windows Vista, pero no todos los programas son compatibles con esta función predeterminada. La tecnología AEP de Kaspersky amplía la funcionalidad de ASLR a programas no compatibles con esta versión predeterminada para bloquear ciertos tipos de exploits impidiendo que determinen la ubicación del código que necesitan para funcionar, por ejemplo, en la memoria. Los repetidos esfuerzos para localizar el código necesario tienen más probabilidades de provocar el bloqueo de la aplicación que la ejecución del código malicioso.

Dónde encontrar AEP

La tecnología de prevención automática frente a exploits está disponible como parte de Kaspersky Endpoint Security for Business. Está activada de manera predeterminada, pero puede desactivarse por separado o junto con todo el módulo Supervisor del sistema (que rastrea la actividad de los programas en el sistema), si lo desea.

De manera predeterminada, AEP bloquea el inicio de cualquier código sospechoso; la metodología de comprobación y rastreo de Kaspersky, junto a investigaciones profundas y continuas realizadas sobre las aplicaciones empresariales más populares, hace que el riesgo de falsos positivos sea muy bajo. Es posible ejecutar esta función en modo interactivo, si así lo prefiere.

6. VENTAJAS PARA LA SEGURIDAD DE IT EMPRESARIAL

La prevención automática frente a exploits reduce significativamente el riesgo de infección de malware generalizado o ataques más dirigidos que utilizan exploits, incluso cuando se emplea una vulnerabilidad de día cero. Durante los exhaustivos procesos de pruebas, investigación y desarrollo internos de Kaspersky Lab, AEP logró bloquear exploits dirigidos a vulnerabilidades populares en Adobe Flash Player, QuickTime Player, Adobe Reader, Java y otros programas.

El enfoque de Kaspersky Lab en materia de seguridad de IT siempre se ha basado en proporcionar varios niveles de protección, junto con el uso eficaz de la inteligencia de amenazas para prever la naturaleza de las amenazas desconocidas hasta el momento. La prevención automática frente a exploits bloquea la ejecución de exploits conocidos y desconocidos. Al hacerlo, complementa el resto de tecnologías de Kaspersky, como el antivirus y los filtros antispam, proporcionando una red de seguridad capaz de atrapar el código más complejo o sofisticado que a veces puede sortear las tecnologías de seguridad de IT tradicionales.

Kaspersky anticipa y previene amenazas de seguridad de IT constantemente, lo que reduce el riesgo en las empresas tanto en el momento actual como en un futuro cada vez más complejo.


Twitter.com/
kasperskyes


Facebook.com/
kasperskyes


Youtube.com/
Kasperskyespana

Kaspersky Lab, Moscú, Rusia
www.kaspersky.es

Todo sobre la seguridad en Internet:
www.viruslist.com/sp

Encuentra un partner próximo:
www.kaspersky.com/buyoffline

KASPERSKY lab