SOPHOS
Security made simple.

Exploits. Interceptados.

Manual sobre el uso de exploits y vulnerabilidades de software

La explotación de vulnerabilidades es una de las principales técnicas que utilizan los cibercriminales para propagar el malware. Aprovechan los puntos débiles de productos de software legítimos, como Flash y Microsoft Office, a fin de infectar ordenadores para sus fines delictivos. Un único exploit puede ser utilizado por innumerables programas de malware, todos ellos con un propósito malicioso distinto.

Las soluciones antivirus se centran en detener el malware que utiliza el exploit como vehículo portador en lugar de detener los exploits directamente. Si bien existen millones de programas maliciosos diferentes, los atacantes utilizan solo algunas decenas de técnicas distintas para explotar las vulnerabilidades de los programas de software. Al bloquear estas técnicas de explotación, puede detener un ataque antes de que se inicie.

Lea este monográfico para obtener más información sobre los exploits y cómo detenerlos. Explica cómo funcionan los exploits, la industria de los exploits, qué hace que un exploit sea bueno a ojos de los cibercriminales y cómo la tecnología antiexploits ofrece una forma muy efectiva de proteger su organización contra amenazas avanzadas y desconocidas.

Exploits y kits de exploits

Exploits

En la mayoría de los ciberataques hay involucrado un criminal que aprovecha alguna debilidad en la seguridad. Esta debilidad puede ser una contraseña seleccionada con poco celo, un usuario que cae en el engaño de un inicio de sesión falso, un adjunto abierto sin pensarlo dos veces o sencillamente la mera visita a un sitio infectado sin siquiera hacer clic en nada. Los ataques son sofisticados e incluso los usuarios más precavidos son vulnerables a los ataques avanzados. Sin embargo, en el campo de la seguridad informática, la palabra exploit tiene un significado específico: un**exploit** es un método para aprovechar un error de software con el objetivo de hacer que un sistema se comporte como pretende un atacante.

Los errores de software que se pueden explotar de esta forma se conocen como **vulnerabilidades**, por razones obvias, y pueden presentarse de muy distintas formas. Por ejemplo, un router doméstico puede tener una página de contraseña con un "código de puerta trasera" secreto que un criminal puede usar para iniciar sesión, incluso cuando para la contraseña oficial se ha establecido de forma deliberada una contraseña especial. Un producto de software que usa puede tener un error que provoque que se bloquee con entradas inesperadas como nombres de usuario súperlargos o una imagen de tamaño excesivo.

Muchos errores de software causan fallos que son fastidiosos, pero que son detectados y manejados con seguridad por el sistema operativo. Sin embargo, una vulnerabilidad es un error que se puede orquestar o controlar de forma que haga algo no autorizado o inseguro cuando el programa se bloquea, antes de que el sistema operativo pueda intervenir o protegerle.

Cuando los atacantes aprovechan una vulnerabilidad de este tipo, normalmente lo hacen engañando alguna de sus aplicaciones que está utilizando, como su navegador o procesador de texto, para que ejecute un pequeño programa o fragmento de programa enviado desde el exterior. Usando lo que se denomina un exploit de ejecución de código remoto, o RCE por sus siglas en inglés, un atacante puede eludir cualquier cuadro de diálogo emergente de seguridad o del tipo "¿Está seguro?", evitando así que pueda detenerlo.

Los exploits de día cero son aquellos en que los atacantes se aprovechan de una vulnerabilidad todavía desconocida y para la que no hay disponible ningún parche en ese momento.

Como los exploits se aprovechan de debilidades frecuentemente desconocidas en software legítimo, frecuentemente resulta difícil evitarlos, incluso cuando se aplican las mejores prácticas de seguridad.

Kits de exploits

Un **kit de exploits** es un kit de herramientas preensamblado de páginas web o software maliciosos que los ciberdelincuentes pueden comprar, otorgar licencias o arrendar con el fin de distribuir malware. En otras palabras, si tiene algún malware novedoso (a lo mejor ransomware o un troyano o ladrón de contraseñas), puede usar un kit de exploits para hacer llegar ese malware a víctimas incautas.

En lugar de intentar cargar su propia página web con códigos maliciosos para que los visitantes se infecten, los hackers recurren a un código de ataque ya preparado en un kit de exploits para probar una serie de brechas de seguridad conocidas con la esperanza de tener éxito con alguna de ellas.

Normalmente, los kits de exploits se suministran directamente al navegador de una víctima potencial en forma de un JavaScript enrevesado y difícil de seguir. Automáticamente intenta una serie de ataques por orden de probabilidades de éxito hasta que uno funcione o todos fallen. Algo similar al ejemplo siguiente:

```
if java installed then
   try java exploit 1
   if exploit worked then install malware end
end
if silverlight installed then
   try silverlight exploit 1
   if exploit worked then install malware end
   try silverlight exploit 2
   if exploit worked then install malware end
end
if flash is installed then
   ...
end
if nothing worked then give up end
```

El mismo kit de exploits se puede usar para entregar distintas muestras de malware, y la misma muestra de malware puede ser entregada por uno o más kits de exploits distintos.

```
<script>var wqncvnhankfhte=(1194000100<780281714?"ie":"rv:1");
var gjxtcjftwwxi=(1149318224+131959385<1122077856+259936926?"gjx":"dk");
var fntzefklgaqvsjy=(1577258313>1944482977?"w":"r");
var wmjsvibonuq=(1293847248>1687638986?"rtr":"\x72\x65\x74\x75\x72\x6e");
wqnctvnankfhte+=(151554506+472333707>363202458?"\x31":"\x68\x74");
var ixgjdotdmfrbi=(160750077+525999200>1876280?"\x5b\x5d":"\x74");
var gfanlterj=(2103263286>2143916270?"czr":"ret");
var wqkbimsjzmmaf=(968162729<189979742?"\x6b":"wq");
var rggshjhsixeofuo=(115809819+1034707353<1078015506+1085801412?"\x72":"c");
fntzefklgasjy+=(77641620+817194218<1256743977+344513278?"\x65\x74":"\x71\x6f");
```

Convoluted JavaScript code from an Angler exploit kit web page

Además de los kits de exploits que aprovechan la web para su distribución, también hay disponible un número de kits de exploits similares para campañas de correo electrónico y phishing. Con estas campañas, el atacante envía adjuntos a usuarios incautos con la esperanza de que abran el adjunto, instalen el kit de exploits o incluso que solo muestren las imágenes en el correo electrónico. Los mecanismos de distribución disponibles son innumerables, y las víctimas desprevenidas pueden hacer poco más que desenchufar su ordenador o sacar la batería del teléfono móvil para evitar los ataques más sofisticados.

La industria de exploit

Gracias a los kits de exploits, los autores de malware no tienen que preocuparse por cómo encontrar errores en Java, Silverlight o Flash, cómo integrar esos errores en exploits activos, cómo encontrar servidores web no seguros para alojar los exploits o cómo atraer víctimas a las páginas web cargadas con código malicioso.

En la misma medida, los autores de kits de exploits no tienen que preocuparse de escribir programas maliciosos completos, no tienen que tener servidores para el seguimiento de los ordenadores infectados ni recaudar dinero de sus víctimas, tampoco tienen que involucrarse en la exfiltración de datos robados ni la venta de estos, etc.

Cada grupo se especializa en uno o más segmentos del panorama de amenazas, en lo que ya se conoce satíricamente como CaaS o Ciberdelicuencia como Servicio. Y entre estos grupos se encuentran los brókeres de exploits.

Los brókeres de exploits compran exploits a los que los descubren y los revenden a cualquiera que esté interesado. Puede tratarse de órganos gubernamentales o hackers infames por igual que, sin embargo, comparten una característica: no revelar sus objetivos. Así lo explicó Kevin Mitnick, fundador de Mitnick's Absolute Zero Day Exploit Exchange, a Wired:

"Cuando tenemos un cliente que quiere una vulnerabilidad de día cero por el motivo que sea, no preguntamos, y de hecho, tampoco nos lo contaría.

Investigadores las encuentran, nos las venden por X, nosotros las vendemos por Y, y nos quedamos con el margen."

Kevin Mitnick, Once the World's Most Wanted Hacker, Is Now Selling Zero-Day Exploits - Wired.com 09.24.14

No es ilegal vender exploits, pero es lucrativo. Una suscripción a un año de 25 vulnerabilidades de día cero puede alcanzar cifras de hasta 2,5 millones de dólares.

La función de los parches

Como hemos visto anteriormente, los exploits aprovechan las vulnerabilidades de productos de software legítimos. Todos los proveedores de software serios crean parches para solucionar las vulnerabilidades una vez detectadas. Probablemente el más conocido sea Microsoft, que publica parches para entre 20 y 30 vulnerabilidades cada segundo martes del mes (Patch Tuesday) Casi siempre transcurre un periodo de tiempo entre la detección de la vulnerabilidad y la creación del parche, incluso cuando se sabe que se usa para actividades criminales, según muestra esta Recomendación de seguridad publicada por Adobe el 14 de junio de 2016:

Existe una vulnerabilidad grave (CVE-2016-4171) en Adobe Flash Player 21.0.0.242 y versiones anteriores para Windows, Macintosh, Linux y Chrome OS. El aprovechamiento de esta vulnerabilidad podría causar un bloqueo y permitir que un intruso se hiciera con el control del sistema afectado.

Adobe tiene conocimiento de que se ha publicado un informe en el que se indica que existe una explotación de la vulnerabilidad CVE-2016-4171 mediante ataques dirigidos limitados. Adobe solucionará esta vulnerabilidad en nuestra actualización de seguridad mensual, que estará disponible a partir del 16 de junio."

Generalmente, una vez que se ha corregido una vulnerabilidad, su efectividad como vector de ataque se ve reducida, ya que, a medida que los usuarios actualizan su software, cada vez son menos los susceptibles de sufrir un ataque del exploit. Sin embargo, todo esto depende de cómo de rápido y con qué eficacia las organizaciones parchean las vulnerabilidades. Las medidas de corrección laxas dejan las puertas abiertas a los ciberdelincuentes, como ejemplifica la vulnerabilidad CVE-2012-0158.

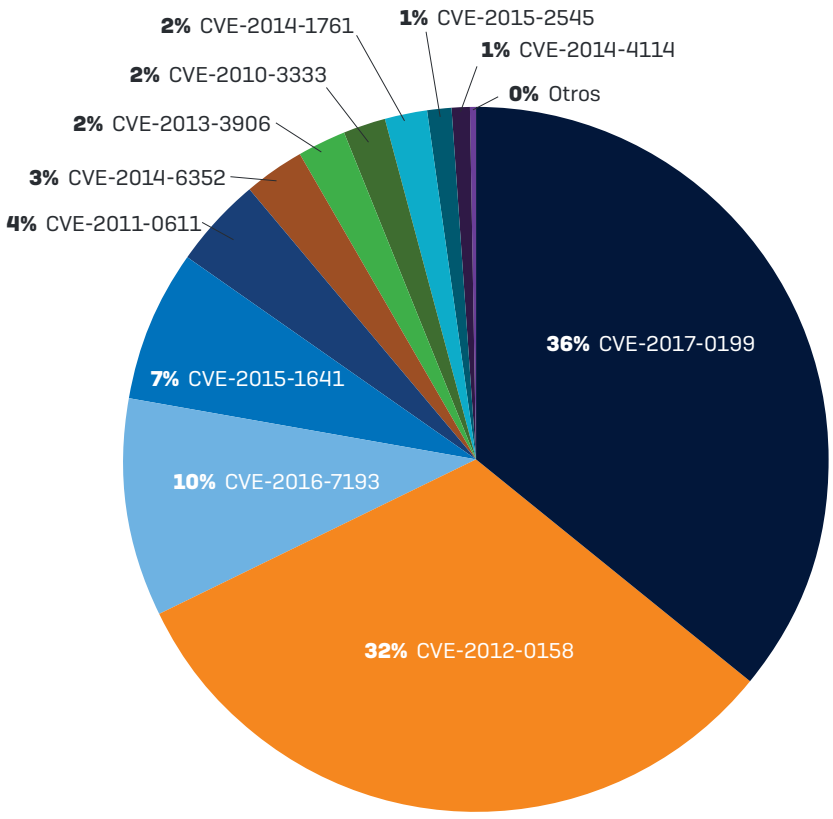
Anatomía de una vulnerabilidad prolífica: la CVE-2012-0158

La vulnerabilidad CVE-2012-0158, posiblemente una de las más explotadas de la última década, esconde una historia de adaptación constante, algo así como una encarnación moderna de "El origen de las especies" de Charles Darwin.

Para el público en general, la CVE-2012-0158 ha ganado notoriedad por una serie de ataques dirigidos bien documentados como el Red October, el FakeM y la campaña Rotten Tomato. El abanico de víctimas de estos casos abarcó desde empresas de logística a empresas de la industria del cuero pasando por organizaciones diplomáticas y gubernamentales. Algo que sugiere que esta vulnerabilidad no solo es muy popular, sino que también es usada por grupos de criminales muy diversos con intenciones distintas.

La CVE-2012-0158, que fue revelada y corregida por Microsoft (MS12-027) ya en el 2012, ha demostrado tener una popularidad perenne entre los cibercriminales. De hecho, y a pesar de existir ya un parche durante más de tres años, la CVE-2012-0158 siguió ocupando las primeras posiciones en las estadísticas de exploits de *SophosLabs* durante el último trimestre de 2015, acaparando un sorprendente 48% de todos los ataques basados en exploits registrados a nivel mundial.

Distribución de exploits



Distribución de exploits, abril-junio de 2017
Fuente: SophosLabs

No es extraño que los ciberdelincuentes apuesten por una vulnerabilidad específica, lo que sí es poco usual es que lo hagan durante tanto tiempo. Parchear una vulnerabilidad normalmente marca el comienzo del final de su utilidad para los cibercriminales, cuanta más gente aplica el parche más débil se vuelve la vulnerabilidad. Teniendo en cuenta que abril de 2017 marcó el quinto aniversario del parche de Microsoft para la CVE-2012-0158, resulta sorprendente que los cibercriminales todavía sean capaces de aprovecharla.

El futuro de la CVE-2012-0158

Siendo realistas, mientras que los kits de exploits para Office no corten sus lazos con ella, parece poco probable que la CVE-2012-0158 desaparezca del panorama a corto plazo. Su uso continuado da más peso a la teoría de que todavía está teniendo éxito, aunque ha tenido que cambiar su forma de actuar pasando de campañas de spam a ataques más concentrados. Mientras que haya ordenadores vulnerables en el mundo, parece dudoso que los autores de kits de exploits lo desechen.

Mientras que su existencia puede que no esté en peligro, sí está en riesgo su posición en la parte alta de la tabla de exploits. Durante el último año han aparecido vulnerabilidades más novedosas y atractivas que ya se han integrado en los kits de exploits y han encontrado aceptación entre los grupos de malware. Las otras dos aspirantes más probables a la corona de la CVE-2012-0158 son la CVE-2015-1641, una vulnerabilidad RTF que explota la forma en que Office procesa el contenido incrustado, y la CVE-2015-2545, que explota el código que Office utiliza para compilar archivos Postscript.

Características de una vulnerabilidad "buena"

La popularidad inicial de la CVE-2012-0158 era comprensible, ya que cumplía muchos de los criterios de los autores de malware a la hora de seleccionar un instalador para sus campañas de spam. Normalmente, las campañas de spam se envían a un número grande de destinatarios aleatorios, de modo que al seleccionar la técnica de ataque no es posible hacer conjeturas sobre el software que tiene instalado la víctima. La consecuencia es que los cibercriminales tienen que jugar con porcentajes de probabilidades y seleccionar una técnica de ataque que funcione en la mayoría de las configuraciones normales. Existen cuatro aspectos clave para determinar lo viable que es una vulnerabilidad:

1. **¿Es el formato de archivo un formato no sospechoso como adjunto de correo electrónico?**

   Una de las primeras líneas de defensa en una solución de seguridad de una empresa es la capacidad de estipular exactamente qué tipo de adjuntos se permiten entrar a la red desde direcciones de correo electrónico externas.

   El código que la CVE-2012-0158 aprovecha está alojado dentro de la biblioteca de control común de Microsoft Windows. La CVE-2012-0158 está centrada específicamente en los controles de ActiveX ListView y TreeView. Ambos controles puede explotarse en documentos de Word y hojas de cálculo de Excel y ninguno de estos dos tipos de archivo parecería extraño en correos electrónicos de conocidos o clientes.

2. **¿Cuál es la probabilidad de que el ordenador de la víctima sea compatible con el ataque?**

   Otra consideración relativa al formato del archivo es si la víctima tiene instalado el software correcto para que el ataque tenga éxito en caso de abrirse el adjunto. La probabilidad de que una infección tenga éxito con un instalador de AutoCAD, por ejemplo, es mucho más baja que si se utiliza un instalador en una presentación de PowerPoint.

   La vulnerabilidad CVE-2012-0158 afecta a Office 2007 y 2010, y esta última era la versión más reciente de Microsoft en el momento de revelar la vulnerabilidad. A pesar de los recientes avances de las alternativas a Microsoft Office, este sigue dominando el mercado, lo que hace de la CVE-2012-0158 una candidata perfecta.

3. **¿Qué funciones permite el ataque?**

   Que el archivo tenga un formato que no levante sospechas y un alto nivel de compatibilidad es bueno, pero a no ser que el método de ataque garantice a los cibercriminales las funciones que necesitan, la técnica no vale para nada.

   La CVE-2012-0158 está clasificada como una vulnerabilidad de "ejecución de código arbitrario". Este tipo de vulnerabilidad se considera como una de las más graves, ya que permite a los cibercriminales secuestrar el programa (en este caso Word/Excel de Microsoft) y obligarlo a cumplir sus órdenes.

4. **¿Qué flexibilidad tiene el método de ataque a la hora de eludir la detección por parte de los antivirus?**

   Un factor clave en decidir cómo de prolífico será un método de ataque es su capacidad de adaptación. Una vez que la industria antivirus descubre un método de ataque, da comienzo el juego del gato y el ratón permanente, en que el malware cambia de forma continuamente a fin de eludir la detección.

   Desafortunadamente, los autores de malware no tardaron mucho en encontrar una serie de soluciones ingeniosas para ocultar la presencia de la CVE-2012-0158, entre ellas:

   - Cifrado de contraseña por defecto
   - Uso del formato RTF
   - Ofuscación de espacios en blanco y grupos incrustados
   - Mezcla de datos binarios

Cómo protegerse frente a exploits

Tecnología antiexploits

Si bien existen millones de programas maliciosos diferentes, los hackers utilizan solo algunas decenas de técnicas distintas para explotar las vulnerabilidades de los programas de software. Bloquear estas técnicas de exploits es una forma muy eficiente y efectiva de bloquear un número masivo de muestras de malware de una sola vez.

Sophos Intercept X es una solución de seguridad para endpoints de última generación sin firmas que ofrece una potente funcionalidad contra exploits. Detecta y bloquea las técnicas de explotación para detener los innumerables programas maliciosos que las utilizan, independientemente de si se trata de variedades de malware conocidas o no.

Intercept X sencillamente reconoce las técnicas de exploit y evita que puedan ser aprovechadas. A diferencia de la tecnología antimalware tradicional, Sophos Intercept X detiene las amenazas antes de que entren en su sistema.

Prácticas recomendadas para la seguridad

Para reforzar sus defensas contra cualquier intento de explotación, le recomendamos:

Desplegar Sophos Intercept X. Se ejecuta junto a su producto antivirus, incluido Sophos Endpoint Protection, para reforzar su protección contra exploits, ransomware y malware nunca visto antes. Al desplegarse junto con Sophos Endpoint Protection, se integra en un único agente de escritorio administrado desde la nube a través de Sophos Central.

Aplicar los parches con prontitud y frecuencia. Si ya ha cerrado las brechas para las que está programado un kit de exploits, todas sus alternativas fallarán y el kit de exploits queda inservible.

Mantener el software de protección actualizado. Un buen antivirus puede bloquear ataques de documentos en muchos puntos; por ejemplo, puede deshacerse de archivos adjuntos de correo electrónico peligrosos antes de que se abran, filtrar sitios web cargados de código malicioso para que no se pueda acceder a ellos y bloquear archivos con programas maliciosos para que no se puedan ejecutar.

Plantearse el uso de un visor de documentos simplificadoo bloquear Microsoft Office. El contenido activo de los documentos de Office se utiliza a menudo para explotar las vulnerabilidades de las aplicaciones. Si utiliza Microsoft Office, es siempre buena idea aplicar controles de seguridad como deshabilitar las macros.

Eliminar plugins de navegador que no utiliza. Si no necesita Java (ni Silverlight, ni Flash) en su navegador, desinstale el plugin. Un kit de exploits no puede atacar un componente del navegador que no está instalado.

Conclusión

Los exploits son herramientas increíblemente potentes usadas ampliamente por los ciberdelincuentes actuales, en las que se aprovecha un solo exploit para distribuir millones de variantes de malware. La buena noticia es que, deteniendo los exploits, puede bloquear la mayor parte de las instancias de ese malware antes incluso de que entre en su sistema.

La probada tecnología antiexploits de Sophos Intercept X permite parar en seco los exploits. Esta solución para endpoints de última generación complementa su protección antivirus existente y le permite proteger su organización con un esfuerzo mínimo.

Más información

Para obtener más información sobre la tecnología antiexploits de Sophos Intercept X, consulte el artículo técnico detallado Los exploits a fondo.

Pruebe Sophos Intercept X gratis:
es.sophos.com/intercept-x

Ventas en España
Teléfono: (+34) 913 756 756
Correo electrónico: comercialES@sophos.com

Ventas en América Latina
Correo electrónico: Latamsales@sophos.com

17-08-16 WPES (NP)

SOPHOS