UNIVERSIDAD DE ALCALÁ

Escuela Politécnica Superior

GRADO EN SISTEMAS DE INFORMACIÓN

Trabajo Fin de Grado

Definición de metodología para el descubrimiento del Zero Days

Autor: Cristina Fernández Rivas

Director: D. Manuel Sánchez Rubio

TRIBUNAL:

Presidente:

Vocal 1º:

Vocal 2º:

CALIFICACIÓN: ……..

FECHA: ……..

A mis padres por el apoyo recibido,

A mis abuelos,

Y a todas las personas que han confiado en mí.

Me lo contaron y lo olvide; lo vi y lo entendí; lo hice y lo aprendí.

Confucio

Índice de Contenidos

Índice de Figuras, Tablas y Diagramas

1. Resumen

1.1 Resumen

El objetivo de este proyecto es definir la metodología de un ataque de día cero, desde que se detecta la vulnerabilidad hasta que se consigue el parche. También se describe el resto de amenazas avanzadas persistentes en las organizaciones, en la que los atacantes emplean un malware sofisticado.
Para evitar estos ataques muchas organizaciones utilizan soluciones tradicionales como son la detección de intrusos, antivirus, antibots y sandboxing. Sin embargo los avances en las técnicas de malware han hecho que estos sistemas sean mucho menos eficaces. Por ello se describe una nueva tecnología efectiva en los puntos finales de la empresa, llamada Stateful Application Control.

1.2 Summary

The objective of this project is to define the methodology of a zero-day attack, since the vulnerability is detected until you get the patch. It also describes the rest of advanced persistent threats in organizations, in which the attackers used a sophisticated malware. To prevent these attacks, many organizations used traditional solutions such as the detection of intruders, antivirus, antibots and sandboxing. However advances in malware techniques have made that these systems are much less effective. This describes a new effective technology in the end points of the company, called Stateful Application Control.

1.3 Palabras Clave

Vulnerabilidad es una debilidad en un sistema permitiendo a un atacante violar la confidencialidad, integridad, disponibilidad, control de acceso y consistencia del sistema o de sus datos y aplicaciones.

Exploit es un fragmento de software, fragmento de datos o secuencia de comandos o acciones, utilizada con el fin de aprovechar una vulnerabilidad de seguridad de un sistema de información para conseguir un comportamiento no deseado del mismo.

Arma significa que el archivo o sitio web contiene código malicioso conocido como un exploit.

Malware es un tipo de software que tiene como objetivo infiltrarse o dañar una computadora o sistema de información sin el consentimiento de su propietario.

Falla es un error o fallo en un programa de computador o sistema de software que desencadena un resultado indeseado.

1.4 Resumen Extendido

Las motivaciones que tienen los ciberdelincuentes para atacar a las organizaciones están creciendo, esto va a suponer una gran amenaza. Algunas de estas motivaciones son: la adquisición de dinero, el espionaje industrial, político y militar, y también la capacidad para deshabilitar en línea a las organizaciones en la que los atacantes no están de acuerdo con algún nivel ideológico.

A lo largo del tiempo el malware ha ido avanzando y adquiriendo más fuerza, entre ellos se encuentra:

- Troyanos de acceso remoto (RAT): permiten acceder de forma remota y controlar el sistema de destino, sin el conocimiento del usuario.

- Robo de información: está diseñado para robar credenciales de acceso así como información de tarjetas de pago.

- Botnets: permiten el control de forma remota de un gran número de máquinas y las usan para transmitir a las organizaciones spam o ataques de destino en un ataque de denegación de servicio.

- Cryptolocker o ransomware: Infecta el pc y secuestra, con una clave secreta, los documentos y a cambio pide dinero para recuperarlos.

Las organizaciones han desarrollado y adoptado muchas herramientas, técnicas y procesos con el fin de resistir el malware y los ataques. Algunas técnicas han tenido éxito pero este éxito lo que ha hecho es motivar a los atacantes a que desarrollen mejores técnicas para eludir defensas persistentes (APT). Aquí se abren tres frentes para detener estas amenazas avanzadas:

- La primera de ellas es la educación del usuario: es muy importante la conciencia de la seguridad para que el personal interno evite ataques como el phishing.

- La segunda es como evitar vulnerabilidades de día cero: para ello hay que evitar el phishing, descargas y ataques que van a depender del usuario que carecen de parches de seguridad. Sin estos parches las estaciones de trabajo pueden ser vulnerables a ataques, aunque también hay vulnerabilidades para las que un parche no está disponible, ya sea porque el proveedor no lo ha desarrollado o simplemente no conoce la vulnerabilidad.

- La tercera es la detección de malware: las organizaciones han utilizado soluciones tradicionales como sistemas de detección de intrusos (IDS e IPS), antivirus y antibots, las cuales no son suficientes. A estas tres soluciones necesitamos añadir una más llamada sandboxing**,** es un mecanismo que implementan varias aplicaciones para ejecutar aplicaciones y programas con seguridad y "aislarlas" del resto del sistema dentro de una especie de contenedor virtual desde el cual controlan los distintos recursos que solicita dicha aplicación (memoria, espacio en disco, privilegios necesarios, etc.).

Los expertos en seguridad van a tener dificultades para detectar las amenazas denominada *día cero* o en ingles *Zero Days*. Un ataque de día cero es aquel ataque que se realiza contra una aplicación o sistema, aprovechando una vulnerabilidad desconocida por los usuarios, la cual no ha sido revelada públicamente. Se caracteriza porque estas amenazas combinan las características de los virus, gusanos, troyanos y código malicioso con el servidor y las vulnerabilidades de Internet para iniciar, transmitir y difundir un ataque. El tiempo para la explotación es el tiempo entre el descubrimiento de una vulnerabilidad y la realización de amenazas que podrían explotarlo. En el momento en el que el proveedor de la aplicación lanza parches y lo hace disponible, es probable que los ataques ya estén explotando la vulnerabilidad. El ciclo de vida típico de una vulnerabilidad comienza mucho antes de los anuncios públicos de su existencia. Es común que un fabricante de software o hardware espere varios meses o incluso años después de haber sido notificado de una vulnerabilidad antes de publicar un parche para ello. Los siguientes sucesos marcan este ciclo de vida:

- Vulnerabilidad introducida: Un error se introduce en el software que más tarde se liberará y se implementará (tiempo= tv).

- Exploit liberados en su hábitat natural: Se descubre la vulnerabilidad para llevar a cabo ataques contra objetivos seleccionados (tiempo=te).

- Vulnerabilidad descubierta por el proveedor: El proveedor se entera de la vulnerabilidad y evalúa su peligrosidad y comienza a trabajar en un parche (tiempo=td).

- Vulnerabilidad divulgada públicamente: La vulnerabilidad se divulga, ya sea por parte del vendedor o en foros. El identificador CVE se asigna a la vulnerabilidad. (tiempo=t0)

- Firmas de antivirus liberadas: La vulnerabilidad se da a conocer, entonces los fabricantes de antivirus liberan nuevas firmas de ataques en curso y las detecciones heurísticas creadas para la explotación. (tiempo= ts)

- Parche liberado: En la fecha de divulgación, el proveedor de software libera un parche para la vulnerabilidad. (tiempo= tp).

- Parche completado: Todos los ordenadores vulnerables en todo el mundo están revisados y la vulnerabilidad deja de tener un impacto (tiempo=ta).

Las amenazas de día cero se han ido propagando a lo largo del tiempo en diferentes navegadores, reproductores multimedia, y visores de documentos. Estos programas de software con una larga historia de defectos de seguridad a menudo son objeto de explotación, lo que resulta un compromiso completo de los puntos finales. Algunos ejemplos son:

- Internet Explorer: fue atacado por un exploit de día cero conocido como caballo de Troya, el cual ataco el objeto de datos de la vulnerabilidad de ejecución remota.

- Adobe Acrobat y Reader: se utiliza un nuevo PDF de explotación que no pasa por las características de seguridad sandbox en Adobe Reader X y XI, con el fin de instalar malware bancario en las computadoras.

- Google: el nacimiento de google Project zero sirvió para auditar en busca de vulnerabilidades en aplicaciones de otros fabricantes, incluyendo en esta lista software libre y software de código cerrado. Dos casos la publicación de vulnerabilidades de 0days de Windows y de 0days OS X.

- Java: es el principal blanco de los hackers que buscan una manera de romper con los sistemas. Esta plataforma de software de Java, que está presente en casi todos los dispositivos, tiene muchas vulnerabilidades y exploits críticos.

Un informe de Advanced Threat Report 2013 creado por FireEye explica que las empresas sufren de media un ciberataque cada 1,5 segundos. También revela que durante el primer semestre de 2013 la plataforma Java fue el principal objetivo más frecuente para ataques de día cero, mientras que en el segundo semestre se centraros más en el navegador Internet Explorer (IE), mediante ataques conocidos como "watering hole".

Los exploits entregados a través de ataques de contenido y abrevadero en armas permiten descargas silenciosas de malware en los equipos de los usuarios y de un punto de entrada sigilosa.

Por contenido en armas entendemos que es un documento de Word o PDF, una hoja de cálculo Excel, o un objeto flash. Estos archivos pueden incluir ocultos códigos de exploits que se ejecutan cuando el contenido se abre por la aplicación de visualización.

El contenido en armas a menudo se entrega a través de un correo electrónico que lanza un phishing para convencer al usuario de abrir un archivo adjunto o de que haga clic en una URL para un sitio de explotación. El lanzamiento de phishing requiere que el atacante diseñe un mensaje convincente para que el usuario pueda confiar y lo abra.

En cuanto a un ataque de abrevadero o watering hole, los atacantes investigan el perfil de la víctima y el tipo de sitios web que visitan. Entonces el atacante prueba las vulnerabilidades de dichos sitios web, cuando el atacante encuentra un sitio web que puede comprometer, inyecta el código, redirigiendo a la víctima a un sitio por separado que alberga el código para explotar la vulnerabilidad elegida. Por tanto el sitio web comprometido está esperando a infectar a la víctima con un ataque del día cero.

El malware se utiliza para obtener acceso a datos sensibles y un control total sobre el sistema comprometido, y que permite al atacante romper con éxito la organización. Cuando el malware se ha introducido en un punto final, comenzara a llevar a cabo el robo de información. Las técnicas que han utilizado para robar datos son las siguientes:

- Clave: Puede interceptar las pulsaciones de teclado del sistema, para averiguar la clave.

- Captura de pantalla: Puede tomar imágenes de la pantalla en el punto final, como cuando se visualiza en cuentas bancarias o tarjetas de crédito.

- Formar acaparamiento: Adquiere información sobre los formularios web dentro del navegador del usuario.

- Espionaje de red: Puede espiar las comunicaciones de red del sistema de destino, obteniendo lo que quiere cuando lo encuentra.

- Sistemas de archivos: Busca el sistema de archivos de la máquina de destino, buscando patrones, palabras clave.

- Control remoto: Proporciona al atacante el control remoto completo sobre la máquina.

Cuando el malware ha obtenido la información, el atacante tiene que enviarlo de vuelta. Los métodos que utilizan para la ex filtración dependen tanto de lo que está disponible para el atacante y que método es menos probable que se detecten. El canal de comunicación de intercambio entre los programas maliciosos instalados y los ordenadores centrales se realiza mediante C & C.

Como las herramientas tradicionales han resultado ser ineficaces se va describir una nueva tecnología prometedora llamada Stateful Application Control. Este va analizar el estado de una aplicación para determinar lo que está haciendo y por qué lo está haciendo, validando así el estado de la aplicación. Va a establecer con precisión si la acción de la aplicación es legítima y va a bloquear archivos no autorizados que se descargan a través de acciones ilegitimas (exploits). Además, bloquea los comandos maliciosos y controla la comunicación (C&C) y el robo real de datos (ex filtración).

También hay que mencionar la tecnología Trusteer Apex, ya que monitorea el estado de la aplicación cada vez que está realizando operaciones sensibles como escribir al sistema de archivos o la apertura de un canal de comunicaciones. Por ejemplo cuando la aplicación utiliza una interfaz de aplicación, Stateful Application Control se activa para validar el estado de la aplicación que actualmente se observa en contra de todos los estados de aplicación conocidas. Mientras el estado de la aplicación coincide con un estado de la aplicación legítima conocido, se permite a la aplicación proceder con la operación. Sin embargo, si el estado de la aplicación no coincide con ninguno de los estados de aplicación válidos, como sucede cuando un exploit se lleva a cabo, entonces Trusteer Apex impide que el archivo descargado se ejecute y ponga en peligro a la máquina. También genera una

alerta para notificar al usuario que un intento de exploit ha sido detectado y que el archivo descargado fue bloqueado.

Por otra parte Trusteer Apex incluye capas de seguridad específicamente diseñadas para proteger las credenciales de acceso corporativo contra el robo y la exposición:

- Una parte de la solución evita que los registradores de claves capturen las credenciales del usuario.

- La segunda parte de la solución evita que los usuarios expongan sus credenciales corporativas en los sitios de phishing.

- La tercera parte de la solución evita que los usuarios reutilicen sus credenciales corporativas en los sitios de consumo y redes sociales.

Trusteer Apex notifica a los usuarios cuando no están autorizados a utilizar credenciales corporativas y envía una alerta a la seguridad de TI acerca de estos eventos.

Las cinco consideraciones a tener en cuenta para la protección contra las amenazas avanzadas pueden ser:

- Capacidad para detener el malware entregado por exploits.
- Prevención precisa de ex filtración
- Impacto mínimo sobre los usuarios (usabilidad, rendimiento)
- Mínimo mantenimiento continuo (Automated)
- Escalas para la protección de todos los empleados de la empresa

2. Memoria

2.1 Introducción

Los ataques de día cero y las amenazas avanzadas persistentes (APT) están creciendo, esto va a suponer serias amenazas para las organizaciones.

Por ataque de día cero entendemos que es un ataque **contra una aplicación o sistema, aprovechando una vulnerabilidad desconocida por los usuarios**, la cual no ha sido revelada públicamente. Casi no hay defensa contra un ataque de día cero, mientras que la vulnerabilidad sigua siendo desconocida.

Por desgracia, muy poco se sabe sobre los ataques de día cero porque, en general, los datos no están disponibles hasta después de que los ataques son descubiertos.

Las organizaciones de ciberdelincuentes parecen estar más motivados y más hábiles todos los días.

Las técnicas de evasión avanzadas de malware están haciendo que las soluciones de detección sean ineficaces para la prevención de infecciones, ya que roba información avanzada de malware utilizando técnicas en constante avance de explotación de vulnerabilidades de aplicaciones, infectando a los puntos finales específicos, y el robo de información.

Hoy en día la mayoría de los expertos en seguridad están de acuerdo en que la detección de las amenazas ya no es la respuesta. Los sistemas de detección tradicionales están disminuyendo en eficacia y los programas antimalware bloquean solo una minoría de malware. A pesar de las mejoras en las herramientas de implementación de punto final y los procesos de gestión de parches, la mayoría de las organizaciones todavía tardan semanas o más para implementar parches de seguridad críticos. Y los ciberdelincuentes desarrollan continuamente nuevos métodos para eludir las reglas de detección.

Este proyecto trata de ataques de día cero y amenazas adicionales que se utilizan para poner en peligro los puntos finales de la empresa y así permitir amenazas avanzadas

persistentes (APT) y ataques dirigidos. En él se describe una nueva tecnología prometedora llamada Estado de control de aplicaciones, lo que proporciona una protección transparente y efectiva en los puntos finales de la empresa.

2.2 Investigación Aplicada

2.2.1 Análisis de la situación de la amenaza

Entendiendo a los ciberdelincuentes y sus motivaciones

¿Por qué los ciberdelincuentes y adversarios atacan organizaciones?

Las motivaciones de los ciberdelincuentes y adversarios encajan en las siguientes categorías:

- **El espionaje industrial**: Las organizaciones se espían unos a otros para robar secretos industriales, para su propio beneficio, o para atenuar las habilidades de sus competidores.

- **Espionaje político**: Siempre los estados de la nación y las naciones van a espiar a los demás, para saber más sobre ellos. La ultima técnica disponible será irrumpiendo en las computadoras.

- **Militar:** Al igual que el anterior, las organizaciones militares desean conocer más sobre sus adversarios militares, y se han añadido ciberataques como otro medio para obtener la inteligencia necesaria o para sabotear instalaciones militares o industriales.

- **Ganancia financiera**: Muchas organizaciones criminales cibernéticas organizadas están en esto por el dinero, directa o indirectamente. Un ejemplo de ello es la ciberdelincuencia en todo el mundo, que supero el tráfico de drogas como la mayor fuente de ingresos penal.

- **Activismo y el hacktivismo:** Gran cantidad de ataques cibernéticos están dirigidos a deshabilitar las capacidades en línea de las organizaciones, en la que los atacantes no están de acuerdo con algún nivel social o ideológico.

Un método popular para infectar los equipos de destino con malware son los exploits, debido a que operan en silencio, sin la ayuda o conocimiento del usuario. Estos exploits están creados para atacar a una vulnerabilidad que tengan los sistemas de destino, si se descubre esta vulnerabilidad, el exploit se instalara en cualquier software malicioso que el atacante haya elegido.

El principal riesgo de exploits y malware en las organizaciones es el robo de información y obtención del control de las máquinas de los empleados, lo que va a suponer una violación de datos. El malware utiliza los siguientes métodos para comprometer una máquina, entre ellas:

- **Web raspado y pantallas de aplicación**
- **Robo de credenciales**
- **Registro de pulsaciones de teclado**
- **Documentos de ex filtración, correos electrónicos y otros datos de recursos directamente desde la maquina infectada.**
- **Proporcionar acceso remoto para un atacante que desea examinar directamente los sistemas y redes de destino.**

El malware avanzado permite APT y los ataques dirigidos

Los hackers tienen como objetivo desarrollar un ataque preciso dirigido a las organizaciones que posean datos de valor.

Cuando un adversario elige una organización, su objetivo va a ser utilizar técnicas para mentir en uno o más sistemas informáticos de la organización. La organización de destino en lugar de hacer un ataque directo frontal, que va a ser imposible, puede tener defensas contra los adversarios.

En cambio, muchos adversarios deciden penetrar en una organización mediante la ayuda del desconocimiento del personal. Un ataque característico puede producirse a través de los siguientes pasos:

1. **Reconocimiento:** la organización recoge información sobre el objetivo del adversario, a través de la ingeniería social y la información a disposición del público.

2. **La planificación y el desarrollo de herramientas de ataque:** El adversario cuando ya posee algunos de los detalles de la organización y de sus empleados, comienza a idear su ataque con técnicas y herramientas específicas. A menudo, estas herramientas incluyen el desarrollo de mensajes y sitios web destinados a parecerse a los sitios utilizados por el personal de la organización de destino.

3. **Gancho de ataque:** El adversario lanza su ataque inicial dirigido al personal, utilizando un mensaje de *lanzamiento de phishing*, que contiene un archivo adjunto en armas, o el uso de un *ataque de abrevadero* en un sitio legítimo donde los usuarios de la organización visitan a menudo. El objetivo es conseguir que los empleados de la organización de destino abran el archivo en armas o visiten el sitio web para lograr infectar sus computadoras con malware. Si la infección es exitosa el adversario podrá continuar con su operación de ataque.

   Normalmente, el malware es un troyano de acceso remoto (RAT) que da el mando a distancia al adversario del ordenador de la víctima o malware que roba información como los credenciales, información de tarjetas de crédito, documentos del usuario, correos electrónicos, etc.

4. **Reconocimiento interno:** En este momento el adversario tiene el control de una o más estaciones de trabajo de la organización de destino, mediante estas estaciones se puede obtener el reconocimiento interno, lo cual va a implicar el seguimiento de mensajes de correo electrónico o la observación de tráfico de la red, con el fin de descubrir la ubicación de los servidores que contienen la información final (robo de dinero, de información o incluso la interrupción de las operaciones del sitio). Algunos de los reconocimientos internos pueden incluir la observación del registro inicial para saber si fue notado o por el contrario no.

5. **Final del compromiso:** El adversario está preparado con el conocimiento y las herramientas necesarias para lanzar su compromiso primario, que puede ser una violación de datos o el robo de propiedad intelectual, para así llegar a perjudicar un sistema de destino.

6. **Cubrir las pistas:** El atacante seguirá siendo desconocido para la organización ya que mantendrá una serie de operaciones destinadas para cubrir sus pistas.

   Estas operaciones pueden durar desde varias semanas hasta un año o más. Cuanto mayor sea la recompensa potencial, el atacante debe evitar ser detectado siendo más sigiloso, así alcanzara su objetivo con más éxito.

Este tipo de amenazas persistentes, están presentes en los siguientes sectores según un informe de amenazas avanzadas de 2013 de FireEye:

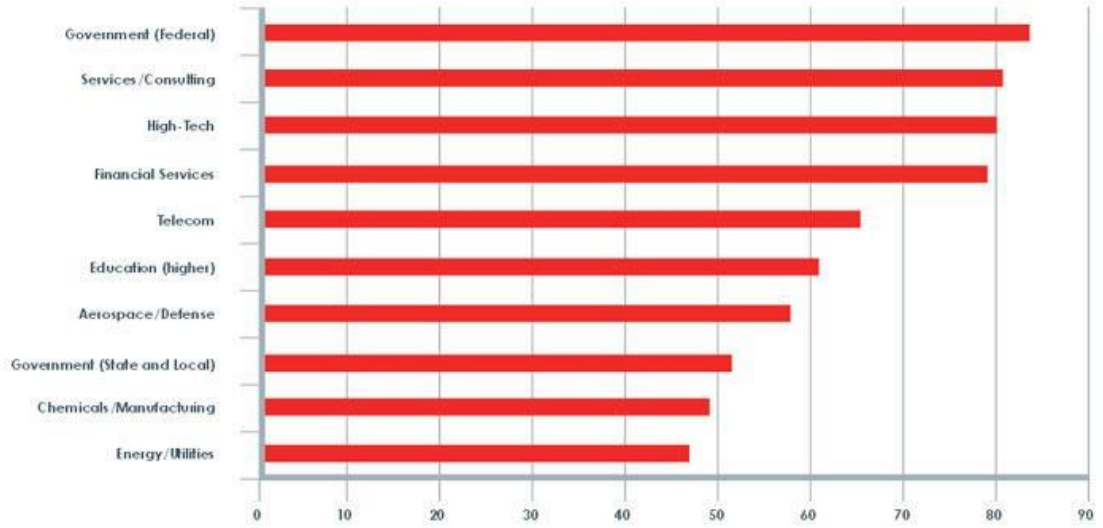


Imagen 1: Amenazas APT por sectores verticales 2013 (www.fireeye.com)

Desarrollo de malware avanzado

Los hackers al conocer que las organizaciones han desarrollado más capacidades para la realización de negocios en Internet, han sacado nuevas formas de atacar a los ciudadanos, empresas y gobiernos para el robo de información valiosa.

Algunas de las innovaciones de malware que se han desarrollado a través del tiempo son las siguientes:

- **Troyanos de acceso remoto o RAT:** Estos son programas maliciosos que dan a un atacante la posibilidad de acceder de forma remota y controlar el sistema de destino, sin el conocimiento del usuario, en cualquier momento. El objetivo puede ser para observar las acciones del usuario, o para utilizar el sistema como un punto de partida para encontrar y comprometer otros sistemas en una organización.

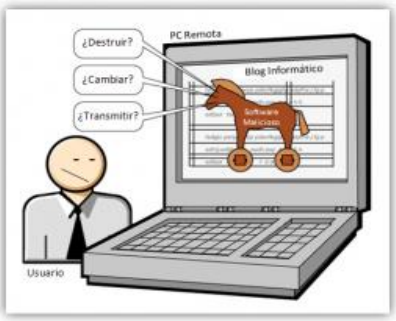


Imagen 2: Troyanos de acceso remoto

- **Robo de información:** Este es el malware que está diseñado particularmente para robar credenciales de acceso, información de tarjetas de crédito, u otros datos sensibles de aplicaciones de alto valor, tales como las aplicaciones corporativas y aplicaciones de banca en línea.

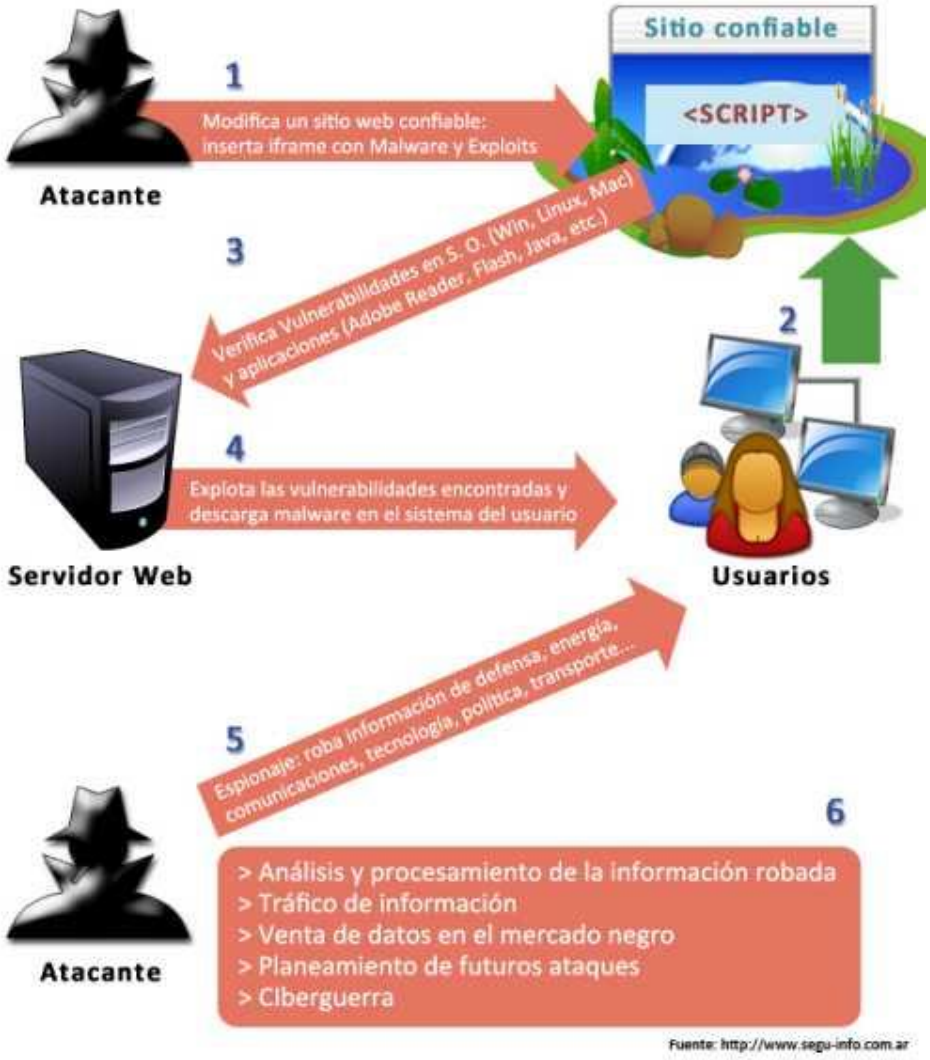


Imagen 3: Robo de información

- **Botnets:** Los atacantes controlan de forma remota un gran número de máquinas comprometidas y las usan para transmitir a las organizaciones, spam o ataques de destino en un ataque de denegación de servicio (DDos).

  La forma más habitual de expansión de una botnet en un **sistema de Windows** suele ser el uso de cracks y archivos distribuidos descargados con algún tipo de cliente P2P. Este tipo de software suele contener malware. Una vez el programa se ejecuta, puede escanear su red de área local, disco duro y también puede intentar propagarse usando vulnerabilidades conocidas de Windows.

  En **entornos como UNIX, GNU/Linux** la forma más clásica de ataque a servidores para construir y expandir una Bonet es por telnet o SSH por medio del sistema prueba-error: probando usuarios comunes y contraseñas al azar contra todas las IPs que se pueda de forma sistemática o bien mediante ataques a bugs muy conocidos, que los administradores pueden haber dejado sin enmendar.

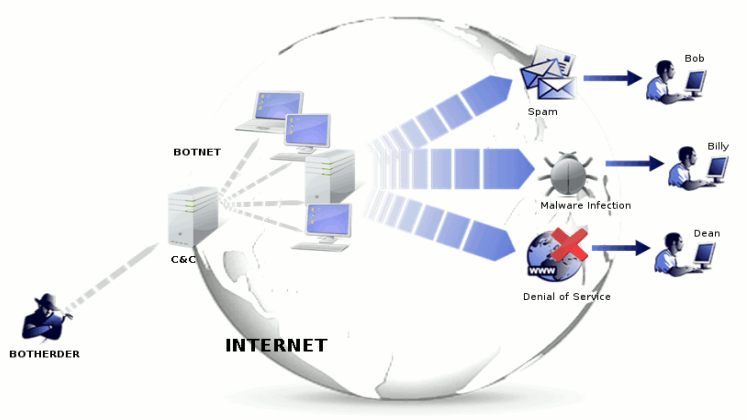


Imagen 4: Botnets

- **Cryptolocker o también llamado ransomware:** Es uno de los **malware más peligrosos de los últimos años, denominado malware secuestrador.** Al infectar el PC, secuestra documentos y pide dinero a cambio de recuperarlos. Los programas antivirus están diseñados para detectar estas amenazas, pero no terminan de conseguirlo o tal vez lo hagan cuando está cifrando archivos, o incluso cuando ya lo finalizo. Esto suele ocurrir cuando se distribuye una versión nueva del malware, como un **ataque de día cero**.
  Cryptolocker secuestra documentos con una clave secreta. Cuando se ejecuta, se instala en la carpeta de programas y empieza a cifrar documentos de Office, archivos PDF, fotos e ilustraciones, que se vuelven inaccesibles. Los archivos se cifran con una clave que solo conocen los autores de Cryptolocker, lo que hace más difícil su recuperación. En este momento, Crytolocker lanza su amenaza, la cual consiste en que si el propietario no paga una suma de dinero en el plazo de tres días o cuatro, la clave con la que se bloquearon los archivos será borrada para siempre, por lo que los archivos ya no podrán recuperarse.

  Como el proceso de cifrado tarda un tiempo, si el malware es eliminado tempranamente, limitaría su daño. Los expertos sugieren tomar ciertas medidas preventivas, como usar aplicaciones que no permitan la ejecución del código de Crytolocker.

Imagen 5: Ransomware

Los tipos de malware explicados anteriormente se resumen en el siguiente cuadro:

Tipo de malware	Ataque	Objetivo
Troyanos de acceso remoto	Acceder de forma remota y Controlar el sistema de destino, sin el conocimiento del usuario.	observar las acciones del usuario Utilizar el sistema como un punto de partida para encontrar y comprometer otros sistemas
Robo de información	Robo de información	Robo de credenciales de acceso Información de tarjetas de crédito Otros datos sensibles
Botnets	Controlan de forma remota un gran número de máquinas comprometidas y las usan para enviar: spam, virus y software espía Lanzan ataques de denegación de servicio (DoS) contra un objetivo específico.	Robar información privada y personal y la comunican al delincuente: - números de tarjeta de crédito - credenciales bancarias
ransomware	Infecta el PC y secuestra documentos.	Cifra documentos con una clave secreta para obtener dinero a cambio.

Tabla 1: Tipos de malware avanzado

El uso de lanzamiento de phishing e ingeniería social para la entrega de malware avanzado

La mejor manera de robar algo de alguien es convencer a un objetivo a confiar en ellos. Mediante el uso de ingeniería social los atacantes podrán convencer a los usuarios a confiar en el contenido que ofrecen. Por ejemplo:

- **Notificaciones de transacción**: Un mensaje que proviene de un banco o comerciante, convencerá al destinatario de una transacción ficticia que acaba de tener lugar. Este mensaje puede contener un archivo adjunto en arma o un enlace a un sitio web de phishing malicioso lo que va a indicar al usuario más información acerca de la transacción o la posibilidad de cancelarlo.

- **Falsas alertas de seguridad y de noticias:** Un mensaje que proviene de un proveedor de servicios, intentara convencer al destinatario de que alguna noticia sobre seguridad requiere su atención y acción inmediata, de esta manera ingresará a un sitio falso. Este sitio puede ser una web de phishing creada para el robo de sus credenciales o también puede ser un sitio inyectado con exploit.

- **Avisos de Gobierno:** Un mensaje que proviene de una agencia del gobierno intentará convencer al destinatario de que algún asunto urgente requiere de su atención. Esto podría ser por ejemplo una factura de un recaudador de impuestos o el cumplimiento de una ley.
  De esta manera se consigue el acceso a la información, esto se conoce como ingeniería social. Las técnicas más utilizadas son las siguientes:

  - **Ataques de phishing y lanzamiento de phishing:** El objetivo de los atacantes es engañar a los destinatarios para instalar malware en las computadoras de destino mediante la creación de mensajes de correo electrónico o sitios web de aspecto realista. Por ejemplo:

    - **Visitar un sitio con exploit.** Estos sitios contienen exploits que pueden infectar sistemas vulnerables con malware.

    - **Abrir un documento adjunto en armas.** Un documento o programa contiene código malicioso que descarga malware a la máquina del usuario, lo que permite al adversario robar información, capturar pulsaciones de teclado utilizando un

malware llamado capturador de teclado, lo que da al adversario el control remoto del ordenador.

- **Visitar un sitio de phishing**. El sitio web es una copia convincente de un sitio web real. Cuando la víctima se conecte al sitio, los credenciales de inicio de sesión pueden ser vistos, lo que va a creer que está visitando la página original. De esta manera, el atacante puede utilizar esas credenciales para robar dinero o información de la víctima.

Los ataques de Phishing y lanzamientos de phishing son básicamente los mismos, salvo que un ataque lanza phishing cuando se dirige a personas específicas o a una organización específica. Además, el malware carga información útil que pueden orientar en el uso de tecnologías conocidas para la organización.

2.2.2 El Estudio de tres frentes para detener las amenazas avanzadas

Las organizaciones con el fin de resistir el malware y los ataques cibernéticos han creado muchas herramientas, técnicas y procesos. Algunas de estas técnicas no han tenido todo el éxito esperado y para lo único que han servido es para motivar a que los atacantes desarrollen aún mejores técnicas de ataque para evitar las defensas.

La actual guerra cibernética se libra en muchos frentes, tres de estos frentes no han demostrado ser eficaces para detener las amenazas avanzadas.

Educación del usuario

Las organizaciones llaman formación de conciencia de seguridad, a un medio para la capacitación de personal interno de las reglas de la seguridad informática para evitar y resistir los ataques como el phishing.

En las organizaciones hay personas que por ignorancia, falta de olvido, juicio o solo por pura curiosidad, pueden abrir un phishing. Los empleados, con Internet pueden ser engañados por los ataques de phishing altamente sofisticados que han sido desarrollados. Y a su vez, esto puede conducir a un éxito de campaña criminal cibernético que no puede ser detectado por un largo tiempo.

Según un estudio de la ONTSI de 2013, si el usuario no adquiere una educación en seguridad, pueden ocurrir los siguientes problemas:

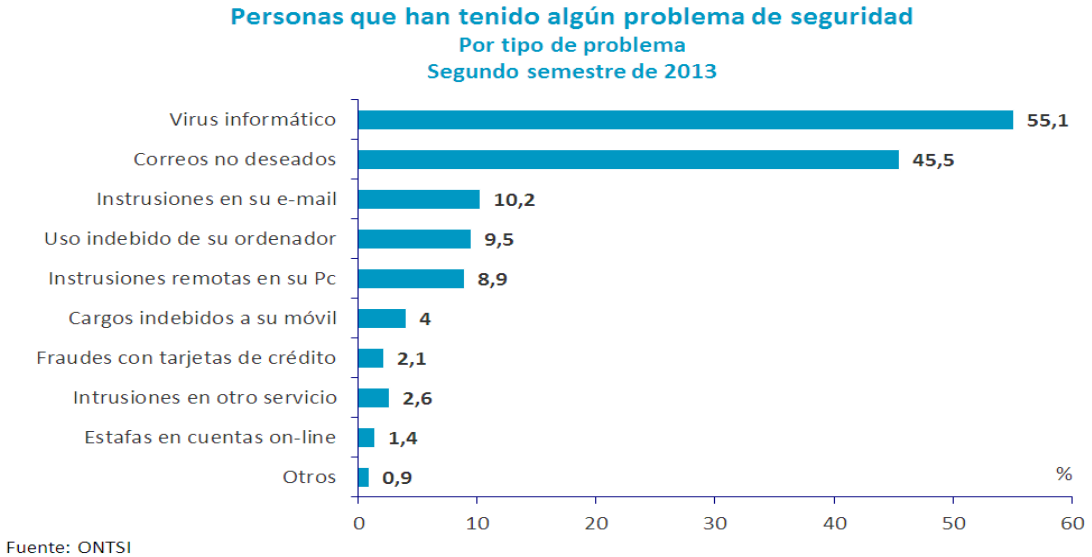


Imagen 6: Personas que han tenido problemas de seguridad (ONTSI)

Como se observa en la imagen los videos informáticos están por encima con un 55,1% detrás le sigue los correos no solicitados ni deseados denominados como spam con un 45,5%.

Evitar vulnerabilidades de día cero

La mayoría de phishing, descargas y ataques dependen de los ordenadores de la víctima que carecen de parches de seguridad esenciales. Sin estos parches, las estaciones de trabajo pueden ser vulnerables a ataques, que son capaces de tomar el control completo del sistema de un usuario sin su conocimiento.

La gestión eficaz del parche consiste en el despliegue oportuno de los parches de seguridad. Pero a menudo hay tantos parches de seguridad emitidos por los proveedores de software en un mes determinado que los equipos de seguridad, que están bien financiados tienen problemas para mantenerlos. También hay muchas vulnerabilidades para las que un parche no está disponible, ya sea porque el proveedor simplemente no lo ha desarrollado, o porque no es consciente de la vulnerabilidad.

Detección de malware

Muchas organizaciones han confiado en las soluciones de detección de malware tradicionales como los **sistemas de detección de intrusos (IDS e IPS), antivirus y antibots** para detectar y eliminar el malware. Sin embargo, los avances en las técnicas de malware y de evasión han hecho que los controles de seguridad tradicionales sean mucho menos eficaces.

Un ejemplo que demostró la incompetencia de los antivirus tradicionales se demostró en el 2013 en el New York Times, donde la solución antivirus detectó sólo 1 de cada 45 archivos maliciosos en los equipos de los empleados.

Diagrama 1: Soluciones de detección tradicionales

IDS e IPS

Estas soluciones tradicionales como los **IPS** buscan el control de acceso en una red informática para proteger a los sistemas computacionales de ataques y abusos.

Entre sus principales funciones, no solo está la de identificar la actividad maliciosa sino que también intenta detener esta actividad. Siendo esta última una característica que distingue a este tipo de dispositivos de los llamados Sistemas de Detección de Intrusos (IDS).

Las funciones de un **IDS son alertar al administrador ante la detección de intrusiones o actividad maliciosa**, mientras que de un **Sistema de Prevención de Intrusos (IPS) establece políticas de seguridad para proteger al equipo o a la red de un ataque.**

Por ello se dice que un **IPS protege a un equipo o red de manera proactiva** mientras que un **IDS lo hace de manera reactiva**.

Existen cuatro tipos diferentes de IPS, son los siguientes:

1. **Análisis de comportamiento de red (NBA):** Este tipo analiza el tráfico de red para identificar amenazas que generan tráfico inusual, como ataques de denegación d servicio ciertas formas de malware y violaciones a políticas de red.

2. **Basados en Host (HIPS)**: Este tipo se genera mediante la instalación de paquetes de software que monitorean un host único en busca de actividad sospechosa.

3. **Basados en Red LAN (NIPS):** Este tipo monitorea la red LAN en busca de tráfico de red sospechoso mediante el protocolo de comunicación LAN, de esta manera analizan todas las actividades.

4. **Basados en Red Wireless (WIPS):** Este tipo monitorea la red inalámbrica en busca de tráfico de red sospechoso mediante el protocolo de comunicación inalámbrico, de esta manera analizan todas las actividades.

La forma en la que los IPS detectan el tráfico malicioso se clasifica en:

Detección basada en políticas

El IPS requiere que se declaren muy específicamente las políticas de seguridad. Por ejemplo, determinar que host pueden tener comunicación con determinadas redes. El IPS reconoce el tráfico fuera del perfil permitido y lo descarta.

Detección basada en firmas

Cuando una firma reconoce una determinada cadena de bytes en cierto contexto, entonces lanza una alerta. Por ejemplo, los ataques contra los Servidores Web, que suelen tomar la forma de URLs. Por lo tanto se puede buscar utilizando un cierto patrón de cadenas que pueda identificar ataques al servidor web. Pero, como este tipo de detección funciona parecido a un antivirus, el administrador debe verificar que las firmas estén continuamente actualizadas.

Detección basada en anomalías

En este tipo de detección es muy difícil determinar y poder medir una condición normal ya que tiende a generar muchos falsos positivos. Dos opciones:

1. **Detección estadística de anormalidades:** El IPS crea una línea base de comparación y analiza el tráfico de red por un determinado periodo de tiempo. Cuando el tráfico varía demasiado con respecto a la línea base de comportamiento, se genera una alarma.

2. **Detección no estadística de anormalidades:** Aquí, es el administrador quien defiende el patrón “normal” de tráfico. Sin embargo, debido a que no se realiza un análisis dinámico y real del uso de la red, es susceptible a generar muchos falsos positivos.

Antivirus

Por otro lado los **antivirus** ayudan a proteger la computadora contra la mayoría de los virus, worms, troyanos y otros invasores indeseados que puedan infectar su ordenador.

Entre los principales daños que pueden causar estos programas están: la pérdida de rendimiento del microprocesador, borrado de archivos, alteración de datos, información confidencial expuesta a personas no autorizadas y la desinstalación del sistema operativo.

Normalmente, los antivirus monitorizan actividades de virus en tiempo real y hacen verificaciones periódicas, o de acuerdo con la solicitud del usuario, buscando detectar y, entonces, anular o remover los virus de la computadora.

Los antivirus actuales cuentan con vacunas específicas para decenas de miles de plagas virtuales conocidas, y gracias al modo con que monitorizan el sistema consiguen detectar y eliminar los virus, worms y troyanos antes que ellos infecten el sistema.

Esos programas identifican virus a partir de "firmas", patrones identificables en archivos y comportamientos del ordenador o alteraciones no autorizadas en determinados archivos y áreas del sistema o disco rígido.

El antivirus debe ser actualizado frecuentemente, pues con tantos códigos maliciosos siendo descubiertos todos los días, los productos pueden hacerse obsoletos rápidamente.

Antibots

Y los **antibots** son diseñados para ser usados en conjunto con otros programas antivirus. A diferencia de los antivirus tradicionales, un AntiBot no utiliza firmas, hay un retraso entre el momento que un proveedor descubre un virus y distribuye la firma. Durante el retraso, los ordenadores pueden verse afectados. En cambio, Antibot intenta identificar un virus a través de sus acciones. Los virus son maliciosos por naturaleza.

A estas soluciones necesitamos añadir una más llamada **sandboxing** ya que esta permite el aislamiento de procesos, es decir, es un mecanismo que implementan varias aplicaciones para ejecutar aplicaciones y programas con seguridad y "aislarlas" del resto del sistema dentro de una caja virtual desde el cual controlan los distintos recursos que solicita dicha aplicación (memoria, espacio en disco, privilegios etc.). Este control al que se somete el proceso sirve para distinguir si el código a ejecutar es malicioso o no, ya que por norma general, se restringirá cualquier tipo de acceso a dispositivos de entrada del sistema anfitrión.

Ya sea que un archivo se envié a través de la web o por correo electrónico, el sandboxing lo ejecuta en un entorno virtual que está completamente separado de todos los demás entornos y redes. Esto permite que el archivo se ejecute en su totalidad y por tanto que el

sandboxing monitoree el ciclo de vida de la infección por completo. Un sandboxing típico incluye no solo un sistema operativo sino también las aplicaciones comerciales más comúnmente usadas.

Para monitorear el ciclo de vida de la infección del malware se requiere del análisis de la actividad de ambos sistemas que incluyen todo, desde modificaciones del sistema de archivos y procesos a cambios de registro. Al usar el nuevo entorno virtual para cada análisis, el sandboxing siempre empieza desde el mismo punto, y esto permite que los análisis subsiguientes sean muy específicos sobre los cambios que se realizan. Conocer este listado de cambios del sistema es crucial para los profesionales de seguridad para comprender la naturaleza del malware y para reparar la infección.

Es igual de importante comprender la actividad del sistema que monitorear la comunicación del malware. La actividad del sistema sienta las bases para el daño real, generalmente al descargar componentes adicionales o extraer datos. En ambos casos es de vital importancia que se analicen todos los protocolos de comunicación, los hosts o IP de destino o las solicitudes de DNS y los tipos de datos transferidos.

Es necesario hacer un seguimiento tanto de la actividad como de la comunicación del sistema para comprender el ciclo de vida completo de la infección, pero es solo el punto de partida.

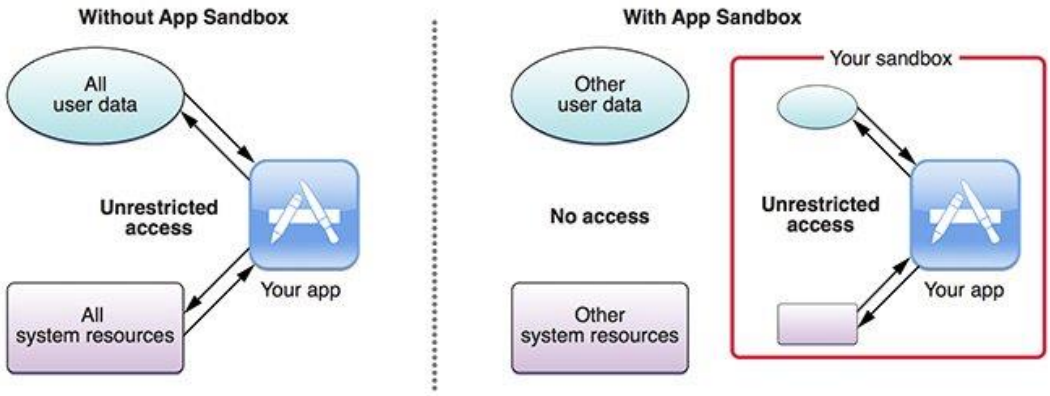


Imagen 7: Sandbox

El malware de hoy también utiliza técnicas avanzadas para evitar la detección y también para sabotear antivirus y programas de instalación de parches.

2.2.3 Malabares en seguridad

La seguridad debería permitir el crecimiento de la productividad de la empresa y del usuario y no obstaculizarlo.

En la profesión de seguridad y en la TI, están obligados a que la gente equilibre la seguridad contra muchas otras necesidades.

Equilibrio de usabilidad y seguridad

El término de usabilidad se refiere a la facilidad en la que un sistema puede ser utilizado. En seguridad un sistema ya no se considera útil si los usuarios del sistema no hacen el esfuerzo para utilizar los controles de seguridad del mismo, o también si el sistema se vuelve tan sobrecargado que se termina haciendo inutilizable.

Los problemas de usabilidad incluyen:

- **Recurso excesivo de máquinas gastado en seguridad:** Los antivirus cada cierto tiempo realizan una exploración de todo el disco duro, los cuales consumen todos los recursos del sistema mientras estamos tratando de hacer otro trabajo.

- **Restricciones de conectividad:** Para prevenir la fuga de datos se utilizara un dispositivo USB conectado a almacenamiento externo, correo electrónico o imprimir y guardar documentos en un sistema de archivos locales. Estos controles pueden ayudar pero por otro lado obstaculizaran la capacidad del trabajador para conseguir cualquier trabajo hecho.

- **Mensajes pop-up preguntando al usuario de las acciones que deben ser permitidos o bloqueados:** Para la mayoría de los usuarios, estos mensajes pop-up son solo una molestia y, hacen clic a través de ellos, independientemente de las circunstancias. La mayoría de los usuarios no saben y no les importa este tipo de mensajes.

La gestión de los gastos generales de TI de seguridad

Si una solución es difícil de implementar y requiere de actualizaciones y administración continúa, entonces el departamento de TI tendrá que invertir una gran cantidad de recursos profesionales con el fin de hacer funcionar correctamente esta solución, en lugar de permitir el crecimiento de la empresa.

Muchas organizaciones si ven que el gasto de la seguridad es muy alto, van a terminar eliminando parte de la seguridad, o van hacer que la solución se desplegué de forma diferente utilizando menos seguridad.

Imagen 8: Equilibrio correcto de los gastos en seguridad

2.2.4 Explicación de día cero y otros exploits

Los expertos en seguridad de datos utilizan términos y asignan nuevos significados a ellos. Dos de estos términos que se discuten en este apartado son el de día cero y el de exploit. El malware se utilizara para recopilar información y permitir una amenaza persistente de ataque avanzado. Los exploits son una forma común de infectar los puntos finales de los usuarios con malware. Esto va a suponer una amenaza significativa para las organizaciones, ya que un tipo de exploit llamado *día cero* o del inglés *Zero Day* puede ser considerablemente difícil de detectar.

Despliegue de la amenaza de día Cero

Los programas de software están llenos de vulnerabilidades que están esperando a ser descubiertos. Cuanto más complejo es un sistema, va a ser más probable que haya vulnerabilidades, y que más de una de ellas sea grave. Este tipo de **vulnerabilidades de día cero son desconocidas** en una aplicación o un sistema operativo de la máquina.

Un **exploit de día cero es un código que no se ha examinado antes** y que aprovecha una vulnerabilidad que no ha sido descubierta. Una **amenaza de día cero es una nueva amenaza que aprovecha una vulnerabilidad** de día cero o un exploit de día cero. El tiempo de las amenazas de día cero ha cambiado en los últimos años.

Desde el punto de vista técnico, el tiempo para la explotación es el tiempo entre el descubrimiento de una vulnerabilidad y la realización de amenazas que podrían explotarla. Frecuentemente, debido a la extensa investigación, los hackers de sombrero negro saben acerca de las vulnerabilidades antes que el proveedor de software (el proveedor a veces sabe que la vulnerabilidad existe, pero no se desarrolla un parche de inmediato). Esto proporciona a los desarrolladores el tiempo suficiente para desarrollar el código de explotación, el cual está diseñado para aprovechar la vulnerabilidad y alterar el comportamiento diseñado de la aplicación.

Cuando el proveedor de la aplicación lanza parches y lo hace disponible, es probable que los ciberdlincuentes ya estén explotando la vulnerabilidad, por lo que ya se han desarrollado y se están utilizando exploits para cualquier revisión de seguridad recién publicado.

¿Qué entendemos por hacker de sombrero blanco y hacker de sombrero negro?

Un ***hacker de sombrero blanco*** **o en ingles** ***White Hat Hackers***, se refiere a una ética hacker que se centra en asegurar y proteger los sistemas de TIC, ya que estos penetran en la seguridad de los sistemas para encontrar vulnerabilidades. Estas personas suelen trabajar para empresas de seguridad informática las cuales los denominan, «zapatillas o equipos tigre».

Por el contrario, los ***hackers de sombrero negro*** **o en ingles** ***Black Hat Hackers***, también conocidos como "crackers" muestran sus habilidades en informática rompiendo sistemas de seguridad de computadoras, colapsando servidores, entrando a zonas restringidas, infectando redes o apoderándose de ellas, entre otras muchas cosas utilizando sus destrezas en métodos hacking.

Por curiosidad esta clasificación de hackers proviene de los héroes en las películas antiguas del viejo oeste ya que típicamente usaban sobreros para distinguirse.

¿Desde cuándo la vulnerabilidad de día cero?

Un exploit de día cero es una nueva amenaza que nunca se ha visto antes, y solo se ha descubierto e investigado ahora.

Después de haber sido notificado de una vulnerabilidad un fabricante de software o hardware va a esperar varios meses o incluso años antes de publicar un parche para ello. El ciclo de vida típico de una vulnerabilidad comienza mucho antes de los anuncios públicos de su existencia.

El protocolo acordado es notificar a un proveedor y darle un periodo razonable para corregir la vulnerabilidad, y permitir que el proveedor pueda controlar la publicación. Sin embargo, hay muchos que no siguen las siguientes reglas:

Si los hackers descubren una vulnerabilidad, pueden o bien desarrollar un exploit por su propia cuenta o vender información sobre la vulnerabilidad al mejor postor.

Aunque los hackers de sombrero negro participen activamente en la investigación con la esperanza de encontrar nuevas vulnerabilidades, los hackers de sombrero blanco hacen lo mismo con la esperanza de ser los primeros en descubrir las vulnerabilidades para poder notificar a los proveedores de software antes de que dichas vulnerabilidades se exploten con exploits de día cero.

Imagen 9: Proceso de una amenaza de día cero

En la imagen se explica el proceso desde que el proveedor lanza una aplicación al mercado hasta que se consigue detectar la vulnerabilidad y lograr poner un parche.

Ciclo de vida de un ataque de Día Cero

El consorcio de Vulnerabilidades y Exposiciones Comunes (CVE) mantiene una base de datos con amplia información acerca de las vulnerabilidades, incluyendo los detalles técnicos y las fechas de divulgación, que es un estándar ampliamente aceptado para el mundo académico, las organizaciones no gubernamentales y de la industria de la seguridad cibernética.

La carrera entre los ataques y las medidas de corrección introducidas por la comunidad de seguridad puede continuar durante varios años, hasta que la vulnerabilidad finalice.

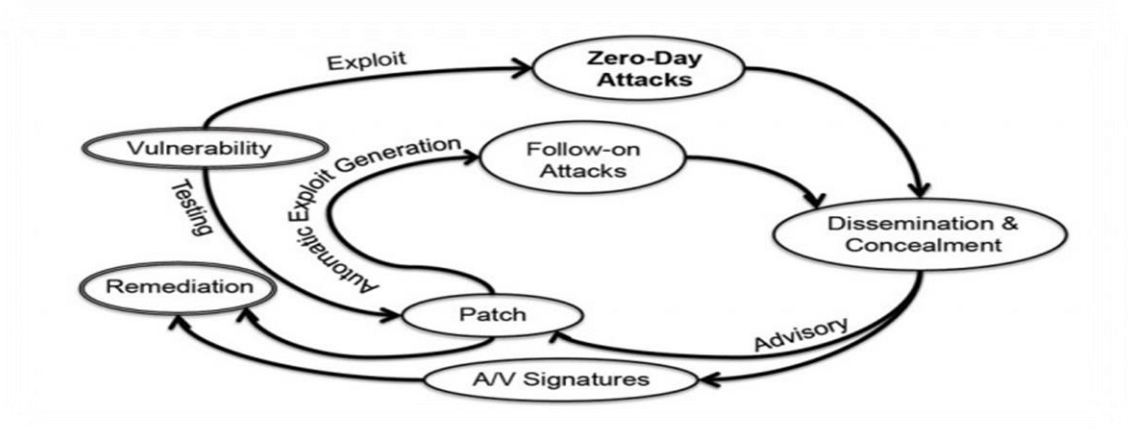


Imagen 10: Ciclo de vida de un ataque de día cero

Los siguientes eventos marcan este ciclo de vida:

- **Vulnerabilidad creada.** Un error, como error de programación, la mala gestión de memoria, se introduce en el software que se libera más tarde y se implementará en los ejércitos de todo el mundo (tiempo = tv).

- **Exploit liberados a la red.** Se descubre la vulnerabilidad para llevar a cabo ataques contra objetivos seleccionados. (tiempo = te).

- **Vulnerabilidad descubierta por el proveedor.** El proveedor se entera de la vulnerabilidad (ya sea mediante el descubrimiento a través de las pruebas o de un informe de terceros), evalúa su peligrosidad, y comienza a trabajar en un parche (tiempo = td).

- **Vulnerabilidad hecha pública.** La vulnerabilidad se divulga, ya sea por parte del vendedor o en foros y listas de correo. Un identificador CVE (por ejemplo CVE-2010-2568) se asigna a la vulnerabilidad (tiempo = t0).

- **Firmas de antivirus liberadas**. Una vez que la vulnerabilidad se da a conocer, los fabricantes de antivirus liberan nuevas firmas de ataques en curso y las detecciones heurísticas creadas para la explotación. Después de este punto, los ataques pueden ser detectados en anfitriones finales con actualización de firmas (tiempo= ts).

- **Parche liberado.** En la fecha de divulgación o después, el proveedor de software libera un parche para la vulnerabilidad. Después de este punto, los hosts que han aplicado el parche ya no son susceptibles al exploit. (tiempo = tp).

- **Despliegue de parche completado.** Todos los ordenadores vulnerables en todo el mundo están revisados y la vulnerabilidad deja de tener un impacto (tiempo = ta).

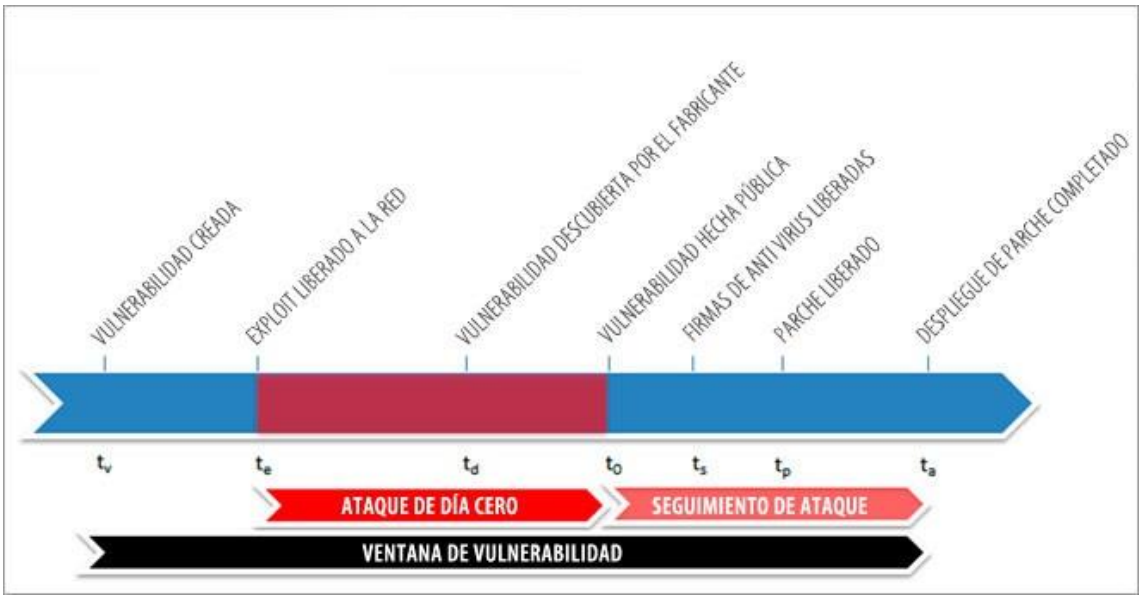


Imagen 11: Ataque y defensa cronológica

Características de los ataques de día cero

Los ataques de día cero se caracterizan porque son amenazas de ataques combinados, los cuales provocan daños. El vector más peligroso y probable de propagación de amenazas de día cero es una amenaza combinada. Estas amenazas combinan las características de los virus, gusanos, troyanos y código malicioso con el servidor y las vulnerabilidades de Internet para iniciar, transmitir y difundir un ataque.

Estos ataques provocan muchos daños a los usuarios finales, se suelen propagar por varios métodos y desde múltiples puntos. Y también permiten la explotación de vulnerabilidades.

La propagación de las amenazas de día cero

Internet Explorer

En los últimos años han aparecido muchas amenazas de día cero. En Octubre de 2003, un exploit de día cero conocido como el caballo de Troya, ataco el objeto de datos de la vulnerabilidad de ejecución remota de Internet Explorer.

El caballo de Troya seria automáticamente descargado y ejecutado en el sistema de una víctima inocente solo cuando se acceda a código específico integrado en un banner con Internet Explorer.

Con frecuencia, los caballos de Troya se utilizan como primera fase de un ataque y su objetivo fundamental es **mantenerse ocultos mientras se descargan e instalan amenazas más poderosas.** A diferencia de los virus y los gusanos, los caballos de Troya no pueden propagarse por sí solos. A menudo, **llegan a la víctima por medio de un mensaje de correo electrónico en el que se hacen pasar por una imagen, o también a través de un sitio web dañino que instala el caballo de Troya en un equipo mediante las vulnerabilidades existentes en el software del navegador web,** como Microsoft Explorer.

Tras su instalación, el caballo de Troya merodea sigilosamente por el equipo infectado y de manera invisible comete sus fechorías, como descargar software espía mientras la victima continua realizando sus actividades cotidianas.

Según la fábula griega el término “caballo de Troya” procede de los griegos, estos ofrecieron a los troyanos un caballo de madera gigante como símbolo de paz. Sin embargo, los troyanos se llevaron una ingrata sorpresa cuando del interior del caballo de madera surgieron tropas de soldados griegos que capturaron Troya. De manera similar, un programa de caballo de Troya se presenta a sí mismo como un programa informático de utilidad, mientras que lo que hace en realidad es causar trastornos y daños en el equipo.

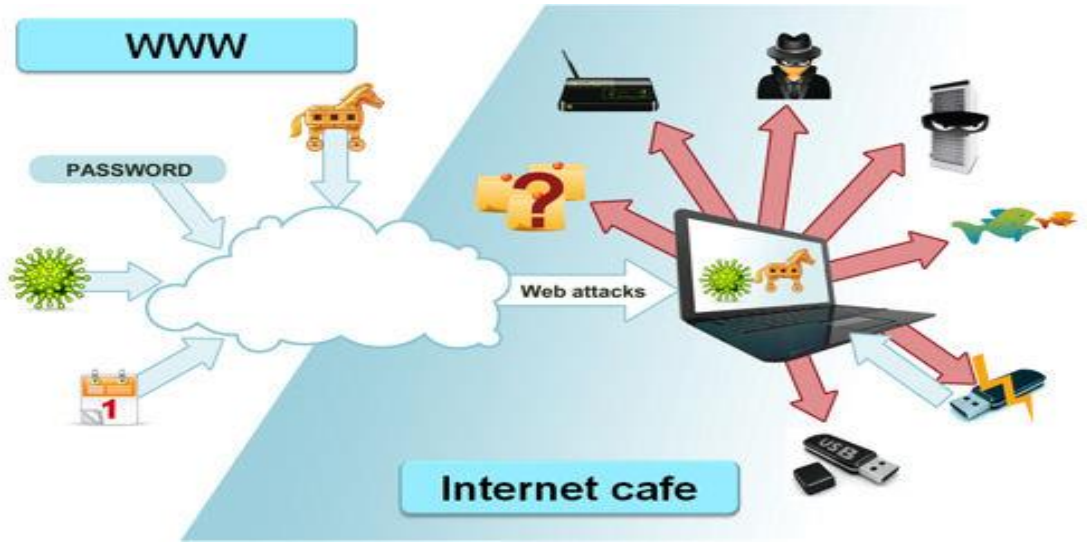


Imagen 12: Ataque de un “caballo de Troya”

Adobe Acrobat y Reader

Los ciberdelincuentes están utilizando un **nuevo PDF de explotación que no pasa por las características de seguridad sandbox** en Adobe Reader X y XI, con el **fin de instalar malware bancario en las computadoras.**

El ataque falla en Google Chrome porque Chrome ofrece una protección adicional para el componente de Adobe Reader, mientras que el ataque tiene éxito usando Internet Explorer o Firefox.

Existen multitud de vulnerabilidades en Adobe, por ejemplo hay dos vulnerabilidades en las últimas versiones de su software, incluyendo Adobe Reader y Acrobat XI (11.0.01 y versiones anteriores) para Windows y Macintosh, X (10.1.5 y anteriores) para Windows y Macintosh, 9.5.3 y versiones anteriores para Windows y Macintosh, y Adobe Reader 9.5.3 para Linux.

La empresa Adobe es consciente de los informes de que estas vulnerabilidades están siendo explotadas en el medio de los ataques dirigidos, **diseñados para engañar a los usuarios de Windows a hacer clic en un archivo PDF malicioso enviado en un mensaje de correo electrónico.** El fabricante de software está en el proceso de trabajar en una solución para estos problemas.

Mientras tanto, los usuarios de Windows de Adobe Reader y Acrobat XI pueden protegerse de la seguridad explotando mediante la activación de *Vista protegida*.

Imagen 13: Ataque mediante un archivo PDF con exploit

Google

Una iniciativa de seguridad de Google fue la creación de Google Project Zero para auditar en busca de vulnerabilidades en aplicaciones de otros fabricantes, incluyendo en esta lista software libre y software de código cerrado. Google montó su equipo en busca de fallos en el software que ellos utilizan, entre ellos hay hackers de gran nivel y reconocimiento internacional.
¿Cuándo debe parchearse algo? Cuanto antes, y es el fabricante del software el que lo debe hacer. **¿Cuál es el límite de tiempo que el investigador debe darle al fabricante antes de decir basta?** El equipo de Google Project Zero ha determinado que 90 días.

A partir de ese momento, para forzar a la actualización se hace público, **aumentando masivamente el riesgo de los clientes,** pero al mismo tiempo **transfiere a ellos la responsabilidad, y la oportunidad, de hacer algo para protegerse contra un fallo que puede que esté siendo explotado actualmente.**

Tenemos **dos casos** la publicación de vulnerabilidades de **0days de Windows** y **de 0days OS X.**

En el caso de **Zero days de Windows**, la vulnerabilidad se encuentra en las versiones de 32 y 64 bits de Windows 8.1. Esto va a ocasionar la ejecución remota de código, la elevación de los privilegios y la denegación de servicios. Estuvo expuesto **más de 90 días, por lo que Google publicó la vulnerabilidad debido a la tardanza de Microsoft en parchearla.**

- MS15-001 – Importante – Una vulnerabilidad en Windows Application Compatibility Cache podría permitir la elevación de privilegios (3023266)
- MS15-002 – Crítica – Vulnerabilidad en el servicio Telnet de Windows podría permitir la ejecución remota de código (3020393)
- MS15-003 – Importante – Vulnerabilidad en el servicio Windows User Profile podría permitir la elevación de privilegios (3021674)
- MS15-004 – Importante – Vulnerabilidad en Windows Components podría permitir la elevación de privilegios (3025421)
- MS15-005 – Importante – Vulnerabilidad en el servicio Network Location Awareness que podría relajar las políticas del firewall y servicios relacionados (3022777)
- MS15-006 – Importante – Una vulnerabilidad en Windows Error Reporting el acceso a la memoria en procesos protegidos (3004365)
- MS15-007 – Importante – Una vulnerabilidad en la directiva de red del servidor RADIUS podría provocar la denegación de servicio (3014029)
- MS15-008 – Importante – Una vulnerabilidad en el Windows Kernel-Mode Driver podría permitir la elevación de privilegios (3019215)

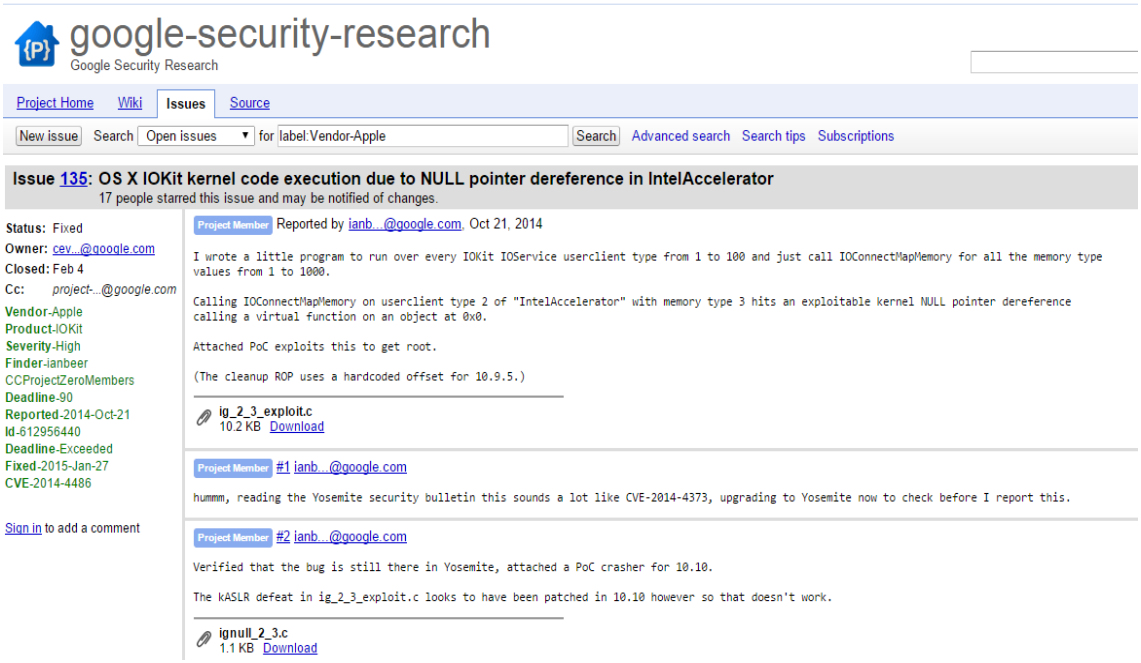
Imagen 14: Parche y vulnerabilidades

Por otro lado en **Zero days OS X**, hay tres vulnerabilidades:

- La primera afecta al servicio XPC de networkd, es lo que usa OS X para manejar las redes.
- La segunda afecta a la ejecución de IO/Kit, que se encuentra en el kernel, debido a que una referencia a un puntero nulo en el componente de IntelAccelerator.
- La tercera también afecta a la ejecución IO/kit, que es **una corrupción de memoria provocada por el uso de la conexión a través Bluetooth.**

Esto va a ocasionar la elevación de los privilegios y así poder controlar el ordenador. Estuvo **expuesto más de 90 días, por lo que Google decidió hacerlas públicas pasado ese periodo de tiempo.**

Imagen 15: Vulnerabilidad XPC de networkd



google-security-research
Google Security Research

Project Home | Wiki | Issues | Source

New issue | Search | Open issues | for label:Vendor-Apple | Search | Advanced search | Search tips | Subscriptions

Issue 135: OS X IOKit kernel code execution due to NULL pointer dereference in IntelAccelerator
17 people starred this issue and may be notified of changes.

Status: Fixed
Owner: cev...@google.com
Closed: Feb 4
Cc: project-...@google.com
Vendor-Apple
Product-IOKit
Severity-High
Finder-ianbeer
CCProjectZeroMembers
Deadline-90
Reported-2014-Oct-21
Id-612956440
Deadline-Exceeded
Fixed-2015-Jan-27
CVE-2014-4486

Sign in to add a comment

Project Member Reported by ianb...@google.com, Oct 21, 2014

```
I wrote a little program to run over every IOKit IOService userclient type from 1 to 100 and just call IOConnectMapMemory for all the memory type
values from 1 to 1000.

Calling IOConnectMapMemory on userclient type 2 of "IntelAccelerator" with memory type 3 hits an exploitable kernel NULL pointer dereference
calling a virtual function on an object at 0x0.

Attached PoC exploits this to get root.

(The cleanup ROP uses a hardcoded offset for 10.9.5.)
```

ig_2_3_exploit.c
10.2 KB Download

Project Member #1 ianb...@google.com

```
hummm, reading the Yosemite security bulletin this sounds a lot like CVE-2014-4373, upgrading to Yosemite now to check before I report this.
```

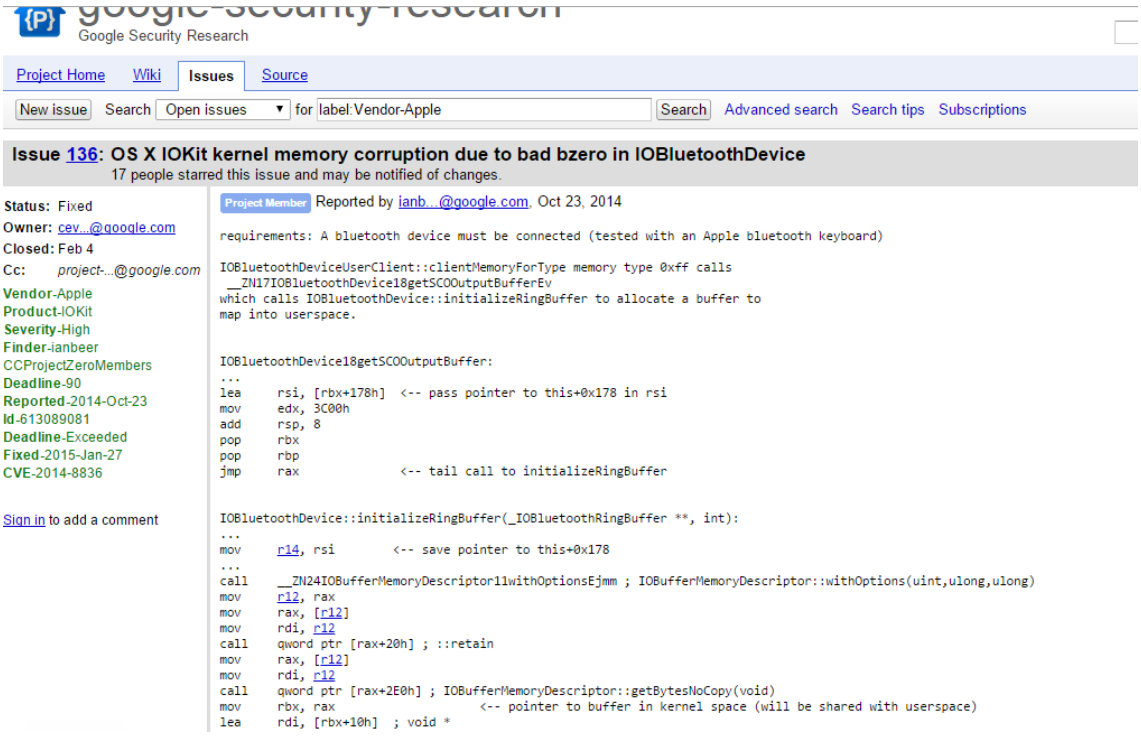
Project Member #2 ianb...@google.com

```
Verified that the bug is still there in Yosemite, attached a PoC crasher for 10.10.

The kASLR defeat in ig_2_3_exploit.c looks to have been patched in 10.10 however so that doesn't work.
```

ignull_2_3.c
1.1 KB Download

Imagen 16: Vulnerabilidad ejecución de IO/Kit



Google Security Research

Project Home | Wiki | Issues | Source

New issue | Search | Open issues | for label:Vendor-Apple | Search | Advanced search | Search tips | Subscriptions

Issue 136: OS X IOKit kernel memory corruption due to bad bzero in IOBluetoothDevice
17 people starred this issue and may be notified of changes.

Status: Fixed
Owner: cev...@google.com
Closed: Feb 4
Cc: project-...@google.com
Vendor-Apple
Product-IOKit
Severity-High
Finder-ianbeer
CCProjectZeroMembers
Deadline-90
Reported-2014-Oct-23
Id-613089081
Deadline-Exceeded
Fixed-2015-Jan-27
CVE-2014-8836

Sign in to add a comment

Project Member Reported by ianb...@google.com, Oct 23, 2014

```
requirements: A bluetooth device must be connected (tested with an Apple bluetooth keyboard)

IOBluetoothDeviceUserClient::clientMemoryForType memory type 0xff calls
 __ZN17IOBluetoothDevice18getSCOOutputBufferEv
which calls IOBluetoothDevice::initializeRingBuffer to allocate a buffer to
map into userspace.


IOBluetoothDevice18getSCOOutputBuffer:
...
lea     rsi, [rbx+178h]  <-- pass pointer to this+0x178 in rsi
mov     edx, 3C00h
add     rsp, 8
pop     rbx
pop     rbp
jmp     rax              <-- tail call to initializeRingBuffer


IOBluetoothDevice::initializeRingBuffer(_IOBluetoothRingBuffer **, int):
...
mov     r14, rsi        <-- save pointer to this+0x178
...
call    __ZN24IOBufferMemoryDescriptor11withOptionsEjmm ; IOBufferMemoryDescriptor::withOptions(uint,ulong,ulong)
mov     r12, rax
mov     rax, [r12]
mov     rdi, r12
call    qword ptr [rax+20h] ; ::retain
mov     rax, [r12]
mov     rdi, r12
call    qword ptr [rax+2E0h] ; IOBufferMemoryDescriptor::getBytesNoCopy(void)
mov     rbx, rax                        <-- pointer to buffer in kernel space (will be shared with userspace)
lea     rdi, [rbx+10h]  ; void *
```

Imagen 17: Vulnerabilidad ejecución de IO/Kit

La explotación de Java y otras aplicaciones vulnerables

Actualmente los criterios de valoración tienen una gran cantidad de componentes integrados adicionales de software. Estos componentes de software a menudo incluyen vulnerabilidades debido a errores de codificación, de negligencias, y algunos podrían estar allí debido a fallas de diseño. Estas vulnerabilidades se vuelven peligrosas cuando se encuentran en aplicaciones populares de usuario final, en un formato que permite a los hackers la explotación.

Las características comunes que se comparten entre aplicaciones explotables son:

- **Reciben contenido externo:** El atacante de alguna manera necesita entregar el código de explotación de la máquina. Este va a ocultar el código dentro de un contenido externo que recibe el usuario. Dicho contenido puede ser documentos adjuntos de correo electrónico, contenido en HTML en las páginas web, etc.

- **Tiene vulnerabilidades:** El hacker mediante estas debilidades va a escribir código de explotación para alterar el comportamiento diseñado de la aplicación.

- **Usados por los usuarios finales:** Para el atacante es más fácil desarrollar y entregar un exploit a través de una aplicación común, que se puede encontrar en la mayoría de los equipos de los usuarios, que diseñar y entregar un exploit a una aplicación única personalizada.

Java

La plataforma de software de Java que está presente en prácticamente todos los dispositivos, tiene muchas vulnerabilidades y exploits críticos. Oracle ha sido tachado por ser lenta para responder de manera oportuna a estas vulnerabilidades. Por todo esto Java es el principal blanco de los hackers que buscan una manera de romper con los sistemas de punto final.

Los temas problemáticos de Java que lo convierten en un objetivo favorable para los adversarios, incluyen:

- **Empresa rígida**: Muchas de las organizaciones dependen en gran medida de una o más aplicaciones de negocios que requieren Java. Si se cambia a otras aplicaciones de negocios que no requieren Java podría ser más caro.

- **Versión anterior bloqueada:** Muchas aplicaciones de software se incluyen con versiones antiguas de Java, las cuales contienen muchas vulnerabilidades explotables.

- **Plataforma múltiple**: En muchos sistemas operativos se ha sido implementado la plataforma de software de Java. El código de Java se ejecutara en cada sistema con el Java Virtual Machine (JVM). Esto significa que pueden tener exploits capaces de afectar gran parte de la instalación.

- **Código abierto**: Java es un software de código abierto. Su código fuente está disponible tanto para hackers de sombrero negro y como para hackers de sombrero blanco por igual. Y aunque los hackers de sombrero blanco traten de asegurarse de que las vulnerabilidades que encuentran sean fijas, los hackers de sombrero negro crearan exploits para vulnerabilidades que encuentren.

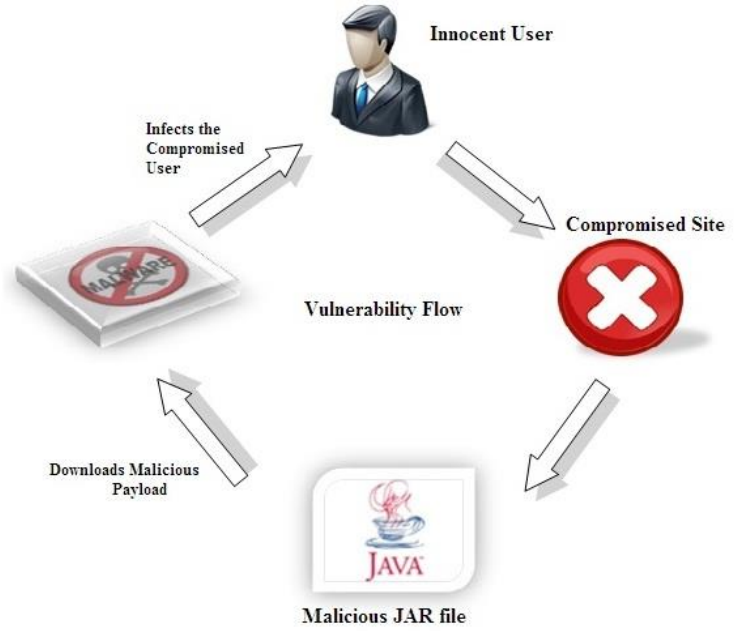


Imagen 18: Ataque mediante un archivo malicioso JAR

Los navegadores y otras aplicaciones específicas

Los reproductores multimedia, navegadores y visores de documentos como Adobe Acrobat y Microsoft Word representan la mayor parte de la interacción humana entre las computadoras e Internet. Al igual que Java, navegadores, plu-gins, reproductores multimedia, y visores de documentos son objeto de investigación de vulnerabilidades y numerosos ataques de día cero. Son programas de software con una larga historia de defectos de seguridad bastante críticos, que a menudo son objeto de explotación, lo que va a poner en peligro los puntos finales del usuario.

Los reproductores multimedia más conocidos y lectores de documentos con una larga historia de exploits son y Adobe Reader, Adobe Flash Player y Adobe Shockwave Player.

Los desarrolladores de malware van a atacar a este tipo de programas más utilizados, que se encuentran en los puntos finales de los usuarios, con el fin de aumentar sus tasas de éxito y maximizar el retorno de su inversión.

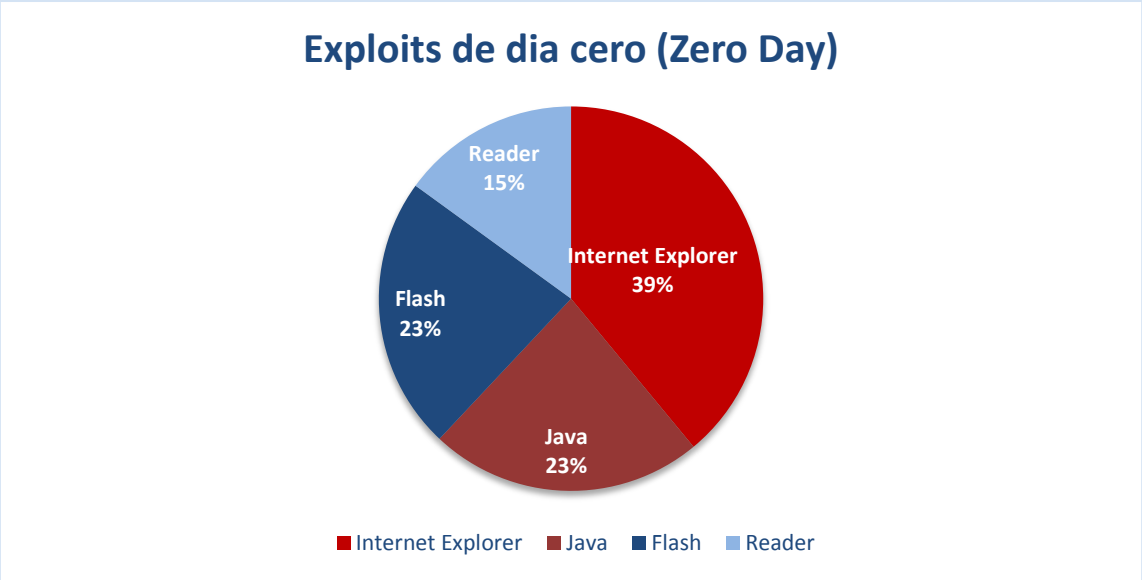


Imagen 19: Informe Advanced Threat Report 2013 de FireEye (www.fireeye.com)

El informe Advanced Threat Report 2013 creado por FireEye concluye que **las empresas sufren de media un ciberataque cada 1,5 segundos**. Además, la expansión global de los ataques de malware ya afecta a 206 países de todo el mundo. El estudio está basado en **40.000 ataques cibernéticos únicos** (más de 100 por día) y más de 22 millones de comunicaciones de malware comando y control (CNC).

Asimismo FireEye revela que durante el primer semestre de 2013 la plataforma Java fue el objetivo principal más frecuente para ataques de día cero, mientras que en el segundo semestre se centraron más en el navegador Internet Explorer (IE), mediante ataques conocidos como “watering hole”.

2.2.5 El uso de contenido en armas y Ataque de abrevadero

El objetivo del ciberataque de hoy en día es realizar ataques sigilosos. Si se realiza una violación muy larga no se detectara, entonces el atacante podrá penetrar con más profundidad en la organización.

Los exploits entregados a través de ataques de contenido en armas y abrevadero permiten descargas silenciosas de malware en los equipos de los usuarios y un punto de entrada sigilosa.

Contenido en armas

El término contenido en armas se refiere a un documento, archivo adjunto o un enlace a un sitio web que contiene oculto el código de exploit, por ejemplo, un documento de Word o PDF, una hoja de cálculo Excel, etc. Estos archivos pueden incluir ocultos código de exploits que se ejecutan cuando el contenido se abre por la aplicación de visualización, por ejemplo, cuando un archivo de Word en arma es abierto por una aplicación de Word vulnerable.

Un sitio web con contenido en armas se conoce como un sitio de exploits. Este es un sitio web que contiene código oculto de explotación, puede ser un sitio malicioso, creado por un atacante o un sitio legítimo que ha sido comprometido e inyectado con código de exploits. Por ejemplo un usuario navega por el sitio web que aprovecha una vulnerabilidad, como un complemento o plugin del navegador, de esta manera se descarga malware en el punto final.

Lanzamiento de ataques de phishing

EL contenido en armas a menudo se entrega a través de un correo electrónico que lanza un phishing para convencer al usuario de abrir un archivo adjunto o de que haga clic en una URL de un sitio de exploits. EL lanzamiento de phishing requiere que el atacante diseñe un mensaje convincente para que el usuario pueda confiar y lo abra. Esto no es una tarea simple.

Pero mediante la mediante la utilización de ingeniería social y mensajes personalizados, los atacantes encuentran maneras de ganar la confianza del usuario. Esto refleja una subida significativa de la potencia y la sofisticación de los ataques de malware.

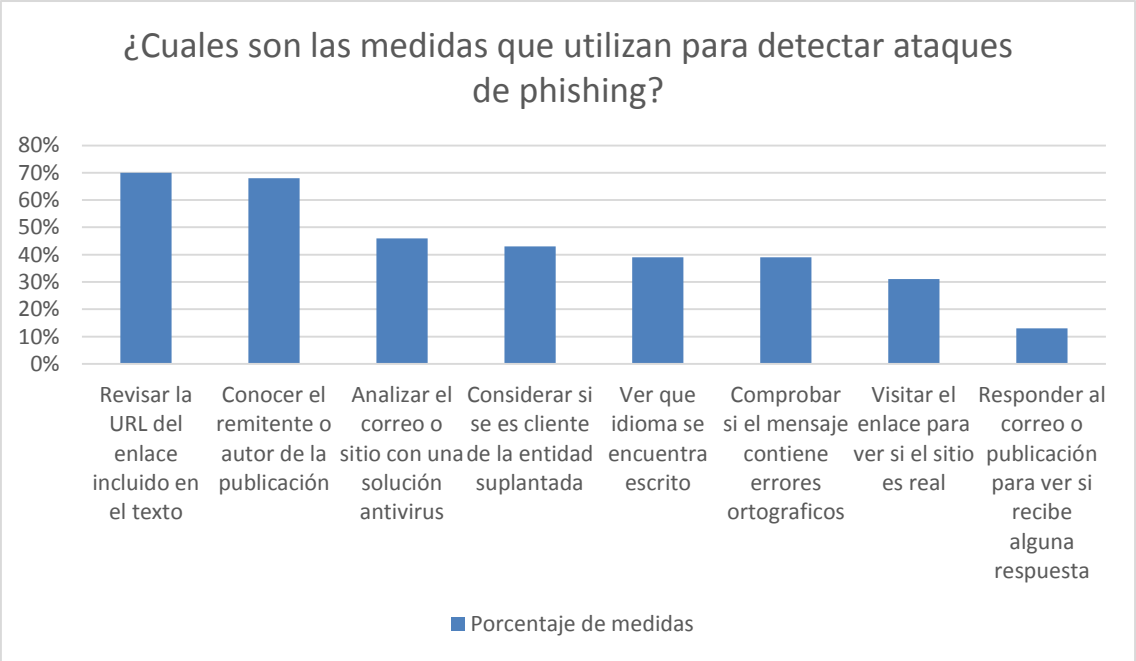


Imagen 20: Medidas para detectar phishing

Ataque de abrevadero

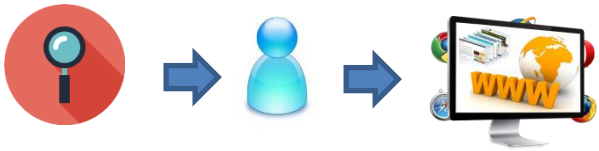
El término ataque de abrevadero o *"watering hole"* proviene de la técnica utilizada por los depredadores que esperan a sus presas a visitar el abrevadero. En lugar de perseguir a la presa, el depredador simplemente espera en un lugar donde la presa irá.

En un *ataque de abrevadero*, los atacantes se dirigen a sitios web legítimos que son visitados frecuentemente por el personal de la organización de destino.

Los atacantes ponen en peligro uno de estos sitios web, convirtiéndolo en un sitio de explotación, con el código de explotación diseñado aprovechan las vulnerabilidades de plugin del navegador y así descargan el malware al visitar la máquina del usuario.

Debido a que el sitio comprometido es un sitio legítimo, que a menudo es utilizado por los empleados, no es práctico para la organización bloquear el acceso a este sitio.

1. El atacante traza un perfil de las víctimas y del tipo de sitios web que visita.



2. Entonces, el atacante prueba las vulnerabilidades de dichos sitios web.

3. Cuando encuentra un sitio web que puede comprometer, inyecta un código JavaScript o HTML, redirigiendo a la víctima a un sitio por separado que aloja el código para explotar la vulnerabilidad elegida.

4. El sitio web comprometido esta "esperando" a infectar a la víctima con un ataque de día cero. *Se puede comparar como cuando un león espera en un abrevadero.*

Diagrama 2: Ataques del tipo "Abrevadero"

2.2.6 Punto final de compromiso y ex filtración de datos

En esta parte, se describe como el malware se utiliza para obtener acceso a datos sensibles y como obtiene un control total sobre el sistema comprometido, lo que va a permitir al atacante destruir con éxito la organización.

Robo de información de malware y credenciales

Información malware de robo

Una vez que el malware se ha establecido en un punto final, comenzara a llevar a cabo su misión: robar información y transmitir esa información robada de nuevo al dueño del malware.

Los desarrolladores de malware han creado muchas técnicas para robar datos de un sistema de punto final. Las técnicas incluyen lo siguiente:

- **Captura de pantalla:** El malware puede tomar imágenes de la pantalla en el punto final, a intervalos de tiempo o cuando se producen eventos específicos, como cuando el usuario visualiza cuentas bancarias o tarjetas de crédito. También puede capturar grabaciones de video de la pantalla.

- **Clave:** El malware puede interceptar las pulsaciones de teclado de controladores de teclado del sistema, para el robo de credenciales.

- **Formar acaparamiento:** El malware puede obtener información sobre los formularios web dentro del navegador del usuario. La información que desean adquirir son por ejemplo, credenciales de acceso, números de tarjetas de crédito y números de cuentas bancarias.

- **Espionaje de red:** El malware puede espiar las comunicaciones de red del sistema de destino, obteniendo todo lo que le interese cuando lo vea. Pero el malware también puede convertir un sistema focalizado en un sniffer de red y capturar las comunicaciones de red de otros sistemas en la misma red local.

- **Sistema de archivos:** El malware puede buscar el sistema de archivos de la máquina de destino, buscando patrones, palabras clave, o lo que sea de interés para el atacante.

- **Control remoto:** Algunos malware pueden proporcionar al atacante el control remoto completo sobre la máquina.

Puede ser necesario comprometer los sistemas y la ex filtración de datos antes de que se haya obtenido la información específica del atacante. Por ejemplo, la primera máquina comprometida puede haber proporcionado credenciales de inicio de sesión, que permite al atacante obtener acceso a otros sistemas desde el cual se puede obtener más información para ayudar al atacante a determinar la ubicación real de los datos que desea robar.

Una máquina que ha sido comprometida puede proporcionar al atacante acceso a otros sistemas, a las redes corporativas, y, finalmente, a los recursos corporativos que contiene datos valiosos.

Ex filtración de la información robada

Si el malware ha obtenido la información, el atacante tiene que enviarlo de vuelta. Las técnicas utilizadas por los atacantes para la ex filtración dependen de lo que está disponible para el atacante y de que método es menos probable que se detecten. Las opciones incluyen HTTP, HTTPS, FTP, correo electrónico e Internet Relay Chat (IRC). Si el atacante cree que la organización de destino tiene un sistema de prevención de fuga de datos (DLP), entonces el atacante puede elegir cifrar la información de modo que no se detecte la ex filtración.

Comunicación de Malware C & C

C & C se define como *Comunicaciones de comando y control*, tienen que ver con el intercambio que tiene lugar entre los programas maliciosos instalados y sus ordenadores centrales. La comunicación C & C se utiliza para:

- **Ex filtración de datos:** Un programa de malware instalado puede enviar periódicamente datos robados, como pueden ser credenciales de acceso, datos sensibles etc. de vuelta al ordenador central del adversario. Este es el punto central del malware.

- **Acceso y control remoto:** Permite al adversario acceder de manera ilícita al sistema infectado, explorar sus datos y programas, y controlar el sistema.

- **Actualizaciones de software de malware:** Los desarrolladores de malware, incluso a veces quieren mejorar sus programas para ello se realizan actualizaciones de software.

- **El trabajo sucio:** Los adversarios pueden dirigir los equipos infectados para que hagan todo tipo de tareas, como sitios de phishing anfitrionas, retransmitir correo no deseado, o participar en ataques de denegación de servicios distribuidos (DDoS).

Para comunicarse con el atacante, el malware intentara abrir un canal de comunicación externa. La forma más sencilla de hacerlo es mediante la apertura de un canal de comunicación directa, pero los canales de comunicación directos son muy sensibles.

Los controles de seguridad basados en host, como firewalls personales, pueden identificar fácilmente que se trata de nuevos canales de comunicación, muy maliciosos y los llegan a bloquear.

El malware intentará ocultar su comunicación para evitar estos controles de seguridad de detección y derivación. Una técnica popular para ocultar la comunicación externa es comprometer canales de comunicación legítimos. Por ejemplo, el malware pondrá en marcha un proceso en un navegador legítimo, como Microsoft Internet Explorer (IE). Si bien el proceso está comenzando, el malware congela el proceso e inyecta código malicioso en él, sustituyendo el código legítimo. Cuando se reanuda el proceso, todo lo que queda es un proceso de Shell que parece legítimo, de hecho se parece a cualquier otro proceso del navegador de IE, pero en realidad no es un proceso regular. No hay ni siquiera una interfaz de la ventana de IE en la máquina. Esto es porque ahora es un proceso malicioso utilizado para la ex filtración de datos. Para evitar ser detectados por las soluciones de seguridad de red que buscan comunicación conocida como C & C, el malware también puede comunicarse con C & C sobre sitios web legítimos como Google Docs y foros de usuarios.

Estas técnicas de evasión hacen que sea muy difícil identificar el canal de comunicación malicioso ya que se ve como un proceso habitual y permite comunicarse externamente. Los firewalls y soluciones de seguridad de red no son capaces de identificarlo como malicioso, lo que va a permitir al atacante comunicarse libremente con el malware, operar, y utilizarlo para la ex filtración de datos.

2.2.7 Descubriendo Stateful Application Control

Como se ha comentado anteriormente en otras secciones el malware es malo tan malo que todos los medios tradicionales para combatirla han resultado ser prácticamente inútil. Esta parte trata de Stateful Application Control en general y también sobre lo que ofrece la tecnología Trusteer Apex.

Introducción a Stateful Application Control

El **Estado de control de aplicaciones** o en inglés ***Stateful Application Control*** es un nuevo enfoque para la prevención de la ejecución de malware entregado por exploits y para frenar el malware avanzado de los puntos finales de los usuarios. Este va **analizar el estado de una aplicación para determinar lo que está haciendo y por qué lo está haciendo.** Con este enfoque, es posible establecer con precisión si la acción de la aplicación es legítima y bloquear archivos no autorizados, maliciosos, que se descargan a través de acciones ilegítimas (exploits).

Trusteer a través de los años, ha encontrado que las acciones de aplicaciones legítimas crean conocidos estados de aplicación. Al analizar el estado de la aplicación, es posible entender el contexto de una acción, de averiguar por qué se está llevando a cabo. Por ejemplo, mediante la comprensión del estado de la aplicación, es posible determinar que la aplicación está escribiendo un archivo en el sistema de archivos debido a que el usuario solicitó Guardar archivo.

Con estado de control de aplicaciones rápida y automáticamente identifica estados de aplicación inválidas que no coinciden con las acciones de aplicación legítimos conocidos. Esto permite la detección precisa de los exploits y la protección contra el malware, entregada a través de la explotación de vulnerabilidades de aplicaciones conocidas y desconocidas.

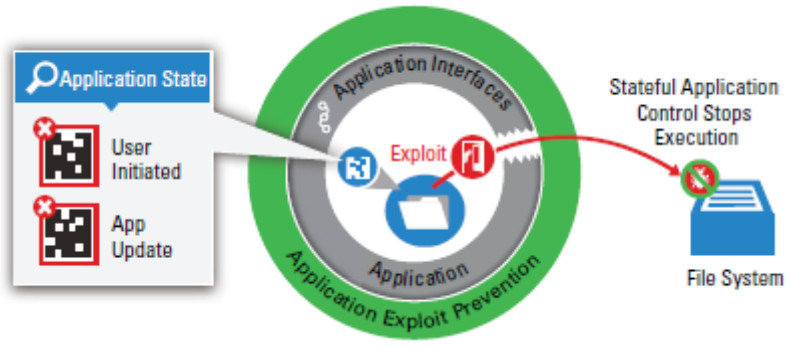


Imagen 21: Funcionamiento de Stateful Application Control

Detener exploits de día cero y los ataques dirigidos

Se va a utilizar un medio eficaz llamado estado de control de aplicaciones para bloquear exploits de día cero y otras amenazas persistentes avanzadas (APT) que son capaces de pasar por alto el radar. Esto es porque el estado de control de aplicaciones no detiene el malware y no requiere de una actualización diaria de firmas de malware. Tampoco necesita ninguna información previa sobre la amenaza, su fuente, o el malware que está tratando de descargar, debido a que no intenta detectar la amenaza, sino **validar el estado de la aplicación**. Stateful Application Control es capaz de bloquear con precisión las amenazas, ya sea conocido o desconocido.

Así es como funciona: Trusteer Apex monitorea el estado de la aplicación cada vez que está realizando operaciones sensibles como escribir al sistema de archivos o la apertura de un canal de comunicaciones. Cuando la aplicación utiliza una interfaz de aplicación, **Stateful Application Control se activa para validar el estado de la aplicación que actualmente se observa en contra de todos los estados de aplicación conocidas**. **Mientras que el estado de la aplicación coincida con un estado conocido de la aplicación legítima,** la operación es conocida**, se permite a la aplicación continuar con la operación.** En cambio**, si el estado de la aplicación no coincide con ninguno de los estados de aplicación válidos,** como sucede cuando un exploit se lleva a cabo**, entonces Trusteer impide que el archivo descargado se ejecute y ponga en peligro a la máquina.**

También genera una alerta para notificar al usuario y al administrador de seguridad que un intento de exploit ha sido detectado y que el archivo descargado fue bloqueado.

Stateful Application Control protege a las organizaciones del malware mediante la prevención de la ejecución de este entregado a través de la explotación de vulnerabilidades en aplicaciones de punto final.

Las organizaciones van a estar protegidas de exploits prácticamente conocidos y desconocidos, aunque tengan parche disponible o no. Esta es una defensa especialmente eficaz contra los ataques de día cero y APT que pretenden pasar por encima del radar de soluciones de detección de malware, como antivirus y sistemas de detección de intrusos.

A diferencia de las soluciones de detección de malware, Trusteer Apex no requiere información avanzada sobre la amenaza con el fin de identificar y bloquearlo.

Para explicar mejor cómo con estado de control de aplicaciones evita el compromiso por el malware entregado a través de exploits, los siguientes ejemplos enseñan la diferencia entre las acciones legítimas que crean estados de aplicación válidos, y exploits que alteran el comportamiento de la aplicación, creando estados de aplicación desconocidos y no válidos:

- Una acción legítima que crea un estado de la aplicación conocida es si un usuario utiliza un navegador para acceder a un sitio web y descarga un archivo. Pero si el sitio contiene código oculto malicioso que aprovecha una vulnerabilidad sin parchear en un navegador para realizar un ataque drive-by download, entonces se crea un estado de aplicación no valido desconocido.

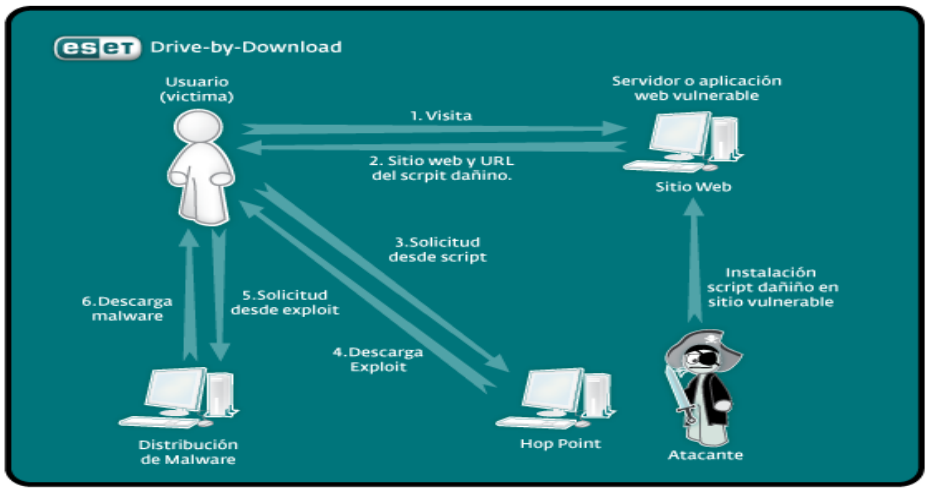


Imagen 22: Ataque drive-by-dowload

- Si un usuario trabaja con Adobe Acrobat y la aplicación se actualiza solo al escribir archivos en el sistema de archivos, entonces se crea un estado de la aplicación legítima. Pero si un usuario abre un documento PDF que recibió por correo electrónico, y el documento contiene oculto código de explotación, el código de explotación alterará el comportamiento de la aplicación para descargar archivos maliciosos para el sistema de archivos, ahora se crea un estado de aplicación no válido desconocido.

La prevención de Datos de ex filtración

El estado de control de aplicaciones proporciona una defensa en profundidad para el bloqueo de malware. Esto significa que bloquea la ejecución inicial de malware si su intrusión fue a través de la explotación de la aplicación de vulnerabilidades. También bloquea los comandos maliciosos y controla la comunicación (C&C) y el robo real de datos (exfiltración). Cualquier intento por parte de malware para trasmitir datos robados de distancia de la máquina de la víctima se bloquea. Esto se entiende mejor con un ejemplo:

El malware se ha infiltrado con éxito en el equipo de un usuario. Ahora lo que necesita es obtener más instrucciones de su operador. Para ello, el malware necesita establecer un canal de comunicación externa. Debido a que el malware no debe permitir comunicarse externamente, este canal de comunicación deber ser bloqueado.

Es más fácil para el malware abrir un canal de comunicación directo desde la maquina infectada a Internet, y lo utilizan para la comunicación con el atacante, normalmente a través de un servidor C & C. Sin embargo, como los canales de comunicación directos son muy visibles, es muy fácil de bloquear, y la mayoría de los cortafuegos personales serán capaz de identificar estos canales y bloquearlos.

Para evitar la detección y permitir la comunicación de malware, los desarrolladores de malware han creado sofisticadas técnicas de evasión para eludir estos controles. El malware avanzado utilizara mejores técnicas para comunicarse con su operador. Sabiendo que algunos sistemas de seguridad evitaran programas desconocidos desde la apertura de las comunicaciones directas, el malware intentará utilizar un programa legítimo para comunicarse.

EL malware avanzado puede, por ejemplo, poner en peligro otros procesos legítimos para ocultar su comunicación maliciosa:

El malware iniciara un proceso que le permite comunicarse externamente, por ejemplo, Internet Explorer (IE).

Cuando el proceso se lanza, el malware congelará el proceso, inyectara el código en el proceso, en sustitución de código malicioso existente, y reanudara el proceso. Ahora es un proceso que se parece al sistema operativo como un proceso de IE, pero en realidad es solamente una parte de ese proceso en el que se ejecuta el código malicioso. Se parece a cualquier otro proceso de IE. Debido a que no hay indicios de que este proceso es un proceso comprometido, los controles de firewalls personales, le permiten comunicarse externamente.

El malware utilizará un navegador para comunicaciones en lugar de comunicarse directamente esto es debido a que se elimina el riesgo de que los controles de seguridad identifiquen las comunicaciones salientes de un programa desconocido y lo bloqueen. Pero si el proceso parece legítimo, quien se encargara de bloquearlo.

Otra técnica de evasión utilizada junto con el compromiso de un proceso legitimo es el uso de sitios web legítimos para la comunicación de C & C. Debido a que los controles de seguridad no pueden identificar procesos comprometidos, tratan de determinar si el canal de comunicación es malicioso en función de su destino. Si se comunica con un sitio C & C conocido, debe ser bloqueado. Para evadir la detección, el malware puede comunicarse con C & C sobre sitios legítimos como foros de usuarios y Google Docs.

Debido a que estos son sitios legítimos, y es imposible distinguir entre la comunicación legítima y la maliciosa, este tráfico no se bloquea.

El estado de control de aplicaciones bloquea los intentos de malware para establecer canales de comunicación directos. También identifica que el malware está tratando de poner en peligro los procesos legítimos y lo bloquea. Esto evita que el malware sea capaz de ocultar sus canales de comunicación y se comunique libremente con el atacante de datos de exfiltración. Porque con estado de control de aplicaciones se tiene una profunda visibilidad de las operaciones de código malicioso en la misma máquina, y es capaz de bloquear con precisión el malware en una etapa temprana, evitando el uso de las técnicas de evasión previamente mencionados.

La protección de credenciales corporativas

Las credenciales corporativas proporcionan el acceso al sistema. Con las credenciales robadas, los adversarios pueden simplemente conectarse a los sistemas corporativos, esto no será visto como la entrada no autorizada sino como el acceso legítimo.

Las maneras en la que los atacantes obtienen contraseñas corporativas son:

- **El uso de sitios de phishing.** Los sitios falsos se utilizan para convencer a los usuarios a introducir sus credenciales, este tipo de sitios se parecen a los legítimos como Google Apps o sitios de banca en línea.

- **El uso de los registradores de claves para robar los credenciales fuera de la máquina del usuario.** Numerosas variantes de malware incluyen funciones de registros de claves que permiten al atacante tomar las credenciales de los usuarios.

- **Piratería en sitios web públicos de consumo o redes sociales y el robo de la base de datos de usuario.** Los usuarios no quieren recordar muchas contraseñas por ello mucha gente recuerda una o dos contraseñas y las utilizan en tantos sitios como sea posible. Los usuarios tienden a utilizar una contraseña compleja en todos sus sitios personales y de negocios, sin

saber que existe un riesgo inherente en hacer esto. Todo esto lo saben los ciberdelincuentes. Si una tabla de contraseñas de un sitio es robado y con éxito descifrado, sus valores hash rotos o sus credenciales de inicio de sesión están en peligro, los adversarios trataran esas credenciales robadas en otros sitios, y son frecuencias las reunirán con éxito.

Trusteer Apex incluye capas de seguridad particularmente diseñadas para proteger las credenciales de acceso corporativo contra el robo y la exposición:

- Una parte de la solución evita que los registradores de claves capturen las credenciales del usuario mediante el engaño de las pulsaciones del teclado del usuario. Cualquier malware que está interceptando las pulsaciones del teclado va a leer las pulsaciones del teclado ofuscados, que harán que el atacante no sea bueno.

- La segunda parte de la solución evita que los usuarios expongan sus credenciales corporativas en los sitios de phishing. Trusteer Apex permite a los usuarios introducir sus credenciales corporativas solo en sitios web corporativos validos con aprobación previa. Si Trusteer Apex reconoce que el usuario no se encuentra en una página web corporativa aprobada, impide la presentación de las credenciales corporativas. De esta manera el usuario cree que está accediendo a un sitio corporativo, pero en realidad es un sitio de phishing diseñada para parecerse a la web corporativa, en la cual no se le permitirá identificarse.

- La tercera parte de la solución evita que los usuarios reutilicen sus credenciales corporativas en los sitios de consumo y redes sociales, debido a que estos sitios no están en la lista de sitios corporativos aprobados, los usuarios no pueden utilizar sus credenciales corporativas que tendrán que usar diferentes credenciales para tales sitios, evitando el riesgo de exposición de credenciales corporativas a través de un sitio web de terceros.

Cuando los usuarios no están autorizados a utilizar credenciales corporativas Trusteer Apex lo notifica y envía una alerta a la seguridad de TI acerca de estos eventos. En caso de que una nueva página web corporativa tenga que ser aprobado para la conexión del usuario, los administradores de seguridad pueden agregar fácilmente el sitio a la lista de la página web corporativa aprobada con un clic de un botón.

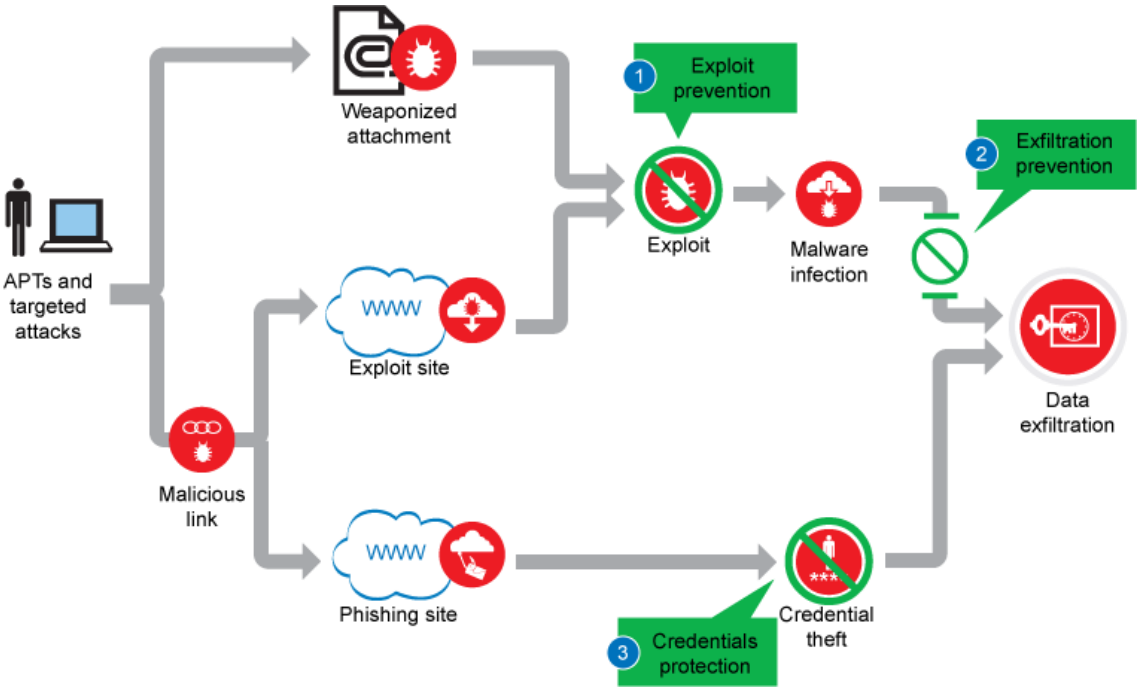


Imagen 23: Prevención de exploits, prevención de ex filtración y protección de credenciales

En cuanto a las opciones de implementación

Una herramienta de gran eficacia como Stateful Application Control seria poco productiva si no hay una manera más fácil de obtener el software en los puntos finales. Trusteer pensó en esto y ha llevado a cabo una solución para que sea lo más fácil posible lograr que se instale en todos los puntos finales tanto administrativo como no administrativo. Las opciones funcionan así:

- **Implementación para los puntos finales administrados.** El software de Trusteer Apex puede ser empujado a todos los puntos finales administrados usando herramientas de distribución de software de la empresa común. Muchas herramientas diferentes de implementación de la empresa se pueden utilizar, incluyendo SMS Microsoft o IBM Endpoint Manager.

- **Implementación de dispositivos no administrados.** Las organizaciones pueden introducir un fragmento de detección en los sitios web corporativos y SSL VPN páginas de inicio de sesión para asegurar que la maquina desde la que el usuario está tratando de conectarse está protegido por Trusteer Apex, antes de conceder el acceso. Si Trusteer Apex

no está presente, el fragmento de detección aparecerá un mensaje que requiere que los usuarios descarguen e instalen el software. El usuario tendrá que descargar el agente de software con el fin de proceder, un proceso que toma solo un par de minutos y no requiere el reinicio de la máquina. A continuación de que Trusteer Apex está instalado y en ejecución, los usuarios podrán acceder a la red o a la empresa web que necesiten.

La tecnología de agente de software se puede instalar en una amplia variedad de plataformas y es compatible con otras aplicaciones de software que ya están ejecutando en la máquina. Esto se ha demostrado en decenas de máquinas protegidas en todo el mundo ya que ejecutan el software de agente.

Comprensión del impacto para el usuario final

Stateful Application Control está diseñado para ser ligero y discreto, al tiempo que protege de forma transparente los puntos finales de usuario y la prevención de la explotación de las debilidades de la aplicación y ex filtración de datos.

Esta tecnología ha sido comprobada en muchos puntos finales, y no interfiere con aplicaciones de negocios u otros productos de software de seguridad, como antivirus, filtrado de Web, IPS (sistemas de prevención de intrusiones basado en host) o firewalls.

Aumentar la protección de la amenaza en tiempo real

Trusteer investiga y ofrece extensa información sobre amenazas en su gran laboratorio. En parte, esta inteligencia proviene de los puntos finales protegidos por Trusteer.

Este proporciona el estado en tiempo real sobre las amenazas que están en ese momento. Las intrusiones de malware y extrusiones se bloquean en tiempo real. Trusteer Apex actualiza de manera automática todos los puntos finales protegidos con nuevos estados de aplicación legítima y nuevas amenazas avanzadas.

Como Trusteer ofrece las actualizaciones, los profesionales de la seguridad de TI no necesitan actualizar continuamente las reglas o políticas, y no hay experiencia interna necesaria para asegurar que la solución está actualizada contra las últimas amenazas. Esto permite a la organización enfocar sus recursos en proyectos de TI que soportan el negocio principal.

Aprovechando Administración basada en Web

Trusteer Apex es una solución alojada, lo que significa que no hay servidores internos o aparatos para instalar y gestionar. Lo bueno de una solución alojada es que Trusteer gestiona toda la infraestructura de gestión para que no tenga que hacerlo un profesional de seguridad de TI.

2.2.8 Cinco consideraciones a tener en cuenta para la protección contra las amenazas avanzadas

Capacidad para detener el malware entregado por Exploits

Una solución avanzada de amenazas deber ser capaz de detener la ejecución de malware incluso si estaba en silencio entregado por un exploit.

Se debe detener el malware independientemente de que la aplicación de la vulnerabilidad este explotada para su entrega, el tipo de malware, su origen o su destino. La solución debe ser capaz de proteger contra el malware entregado de día cero y ataques conocidos.

Prevención Precisa de ex filtración

Cuando el malware infecta un punto final, se va a establecer un canal de comunicación externa lo que va a permitir la comunicación con el atacante.

Más tarde, este canal de comunicación será utilizado para la ex filtración de datos. Las soluciones avanzadas de protección de amenazas deben impedir las comunicaciones de malware y ex filtración de datos, independientemente de las técnicas de evasión.

Para evitar el compromiso, las soluciones avanzadas de protección contra amenazas necesitan prevenir la ex filtración de datos en las maquinas infectadas.

Impacto mínimo sobre los usuarios (usabilidad, rendimiento)

La mejor protección es del tipo que es transparente para los usuarios, lo que quiere decir que los usuarios son conscientes de ello. La mayoría sabe que los usuarios solo realizan su trabajo y ellos si se les pide no van hacer ninguna de las tareas relacionadas con la seguridad.

La confianza en los usuarios finales a que tomen decisiones de seguridad como “¿Se debe permitir esta aplicación para cambiar estas claves del registro y guardar estos archivos en el sistema de archivos?” La mayoría de los usuarios no son expertos en seguridad de la información, ni deben necesitar serlo. En la mayoría de los casos, los usuarios no pueden entender el significado de las alertas de seguridad técnica y, por tanto, no pueden tomar la decisión correcta.

Mínimo mantenimiento continuo (Automated)

Los departamentos de TI tienen mucho trabajo, por lo que lo último que van a querer escuchar es que una herramienta más de seguridad necesita un cuidado constante. Esa es una falla. Además, la mayoría de las organizaciones no tienen la experiencia interna para investigar las últimas amenazas y asegurar que la solución es la correcta.

Por otro lado, hoy en día las organizaciones de TI necesitan soluciones que requieren un mantenimiento mínimo y tienen un proveedor para administrar las actualizaciones automáticas, infraestructura, alertas y todos los demás que hace que funcione.

Escalas para la Protección de todos los empleados de la empresa

Un sistema de protección avanzada contra amenazas efectiva va a ser un éxito sólo si se trabaja en organizaciones de cualquier tamaño, ya sea 100 empleados o muchos millones. Su entorno constantemente va a crecer y a cambiar.

Los puntos finales de los empleados en consultorios, oficinas remotas, que viajan, deben ser protegidos.

2.3 Descripción Experimental

La experimentación realizada ha consistido en la investigación de ataques de día cero y las amenazas que conllevan este tipo de ataques, ya que desde que se descubre la vulnerabilidad hasta que se lanza el parche pasa un tiempo.

Durante ese tiempo los ciberdelincuentes aprovechan esa vulnerabilidad para llevar a cabo ataques contra objetivos seleccionados.

El malware utilizado permite el robo de información y la transmisión de esa información robada de nuevo al dueño de malware.

Se ha investigado acerca de cómo evitar este tipo de ataques haciendo hincapié en la educación del usuario, en el desarrollo de un parche y en el uso de diferentes soluciones tradicionales como IDS, antivirus etc. Pero han resultado ser ineficaces a la hora de evitar estos ataques.

Se ha observado que existen otros tipos de tecnologías como Stateful Application Control de Trusteer Apex que proporcionan protección contra amenazas desconocidas y de día cero y programas maliciosos avanzados, los cuales podrían ser la solución adecuada frente a estos problemas.

2.4 Conclusiones

La principal conclusión obtenida del proyecto es que un ataque de día cero va a suponer una seria amenaza para las organizaciones, ya que realiza un ataque contra una aplicación o sistema, aprovechando una vulnerabilidad desconocida por los usuarios. Además poco se sabe sobre este tipo de ataque debido a que los datos no están disponibles hasta después de que los ataques son descubiertos.

El tiempo que transcurre entre el descubrimiento y la publicación del parche, supondrá un riesgo para las organizaciones, ya que los ciberdelincuentes utilizaran técnicas de malware avanzadas para infectar los puntos finales y el robo de información. Estos ciberdelincuentes intentaran convencer al usuario, mediante el phishing y la ingeniería social, para lograr sus objetivos.

Por otro lado, los ciberdelincuentes utilizaran ataques más sofisticados para penetrar con más profundidad en la organización, mediante el uso de contenido en armas y el ataque de abrevadero que permiten descargas silenciosas de malware en los equipos de los usuarios y de un punto de entrada sigilosa.

Cabe destacar que las soluciones tradicionales no han logrado la detección del malware avanzado y por ello es necesario utilizar una tecnología que da un nuevo enfoque para el bloqueo de amenazas de día cero, llamada Stateful Application Control.

3 Diagramas

El siguiente diagrama muestra cómo actúa un ataque de día cero:

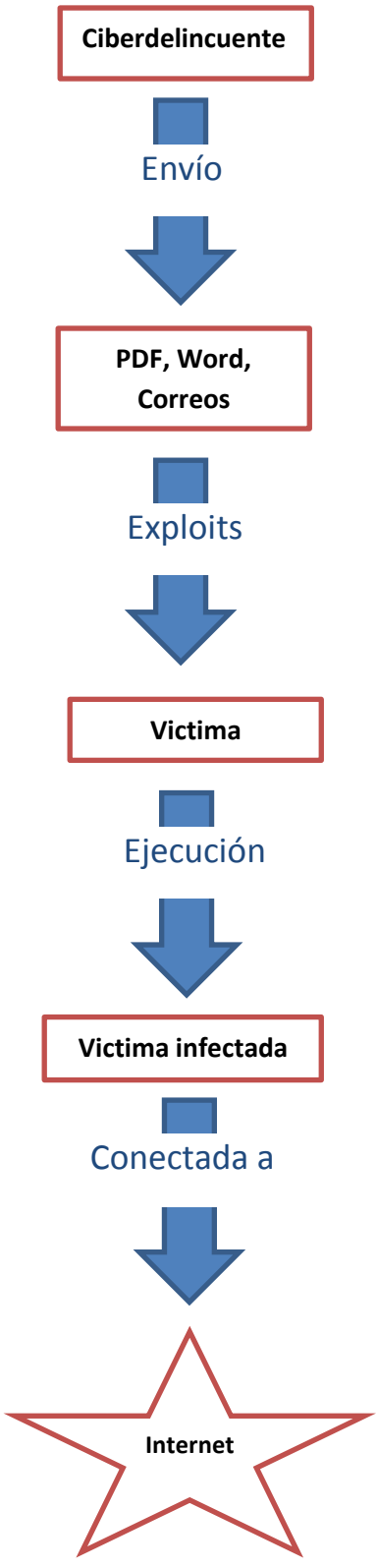


Diagrama 3: Ataque de día cero

4 Bibliografía

Peter H. Gregory, CISA, CISSP, CRISC. (2014). Stopping Zero-day Exploits. New Jersey: Dummies.

Users.ece.cmu.edu: https://users.ece.cmu.edu/~tdumitra/public_documents/bilge12_zero_day.pdf

El lado del mal: http://www.elladodelmal.com/2015/01/es-google-project-zero-irresponsable.html

Blog-segu-info: http://blog.segu-info.com.ar/2014/02/como-eliminar-cryptolocker-el-troyano.html

Wikipedia: http://es.wikipedia.org/wiki/Sistema_de_prevenci%C3%B3n_de_intrusos

Globbtv: http://globbtv.com/3989/noticias/fireeye-presenta-su-informe-de-amenazas-avanzadas-persistentes-apt-2013

Cronicaweb: http://www.cronicaweb.com/descubre-que-es-un-ataque-informatico-5525/

Channelbiz: http://www.channelbiz.es/2013/04/17/ataques-pymes-multiplicaron-2012/

Hipertextual: http://hipertextual.com/archivo/2012/08/que-es-el-sandboxing/

Norton: http://es.norton.com/cybercrime-trojansspyware