Malware, Virus informáticos y mecanismos de defensa

Publicado el El Informatico - 7 de diciembre de 2020 -

¿Cómo funciona un virus informático? ¿Sabrías distinguir entre malware, y virus? ¿Qué tipos de malware existen, y cómo funcionan? ¿Como podrías defenderte frente al malware? En éste artículo se explican las diferencias de lo que es cada cosa, y cómo funcionan los diferentes tipos de malware. También se explicarán algunos mecanismos y técnicas de defensa. Es un artículo muy largo, pero conviene mucho leerlo ya que cubre todo lo básico.

¿Qué es el *malware*?

La gente le llama 'virus' a cualquier cosa que pueda afectar el rendimiento de un equipo informático o incluso dañarlo. La realidad es que no todos los programas maliciosos son 'virus' informáticos. Es más, ni siquiera todos los virus informáticos tienen por qué ser *malware*, ya que algunos de ellos no causan ningún daño ni extraen o modifican ningún tipo de información del usuario.

Para englobar al conjunto de software malicioso que pudiera causar problemas al equipo informático (PC, teléfonos, 'smart' TVs...) o al usuario de cualquier manera, usamos el término ***malware***.

¿Qué es un virus informático?

Un virus informático es un programa que **puede replicarse a otros equipos**, copiando su código en ellos de alguna forma determinada. Se les llama 'virus' porque su funcionamiento se basa en el funcionamiento de los virus biológicos, pero aplicado a la informática.

Por lo general, un virus suele infectar el equipo copiando su código dentro de los distintos ejecutables presentes en el mismo, o en alguna de las memorias del mismo. Por ejemplo, un virus puede copiarse a un ejecutable como **explorer.exe**, de modo que se activaría al iniciar el sistema operativo, o incluso copiarse en el sector de arranque del disco. Entre muchos otros métodos.

Una vez infectado el sistema, **intentará replicarse por algún medio**. El método

más concreto es mediante el **correo electrónico**, obteniendo la dirección de correo de la víctima y sus contactos, e intentando hacerse pasar por la víctima mandando correos a sus contactos con un archivo ya infectado. En teléfonos móviles ésto también se puede conseguir mediante **Whatsapp o telegram**. Muchos virus mandan mensajes a los contactos del dispositivo con un enlace que, al pulsarlo, abren una página infectada en el navegador del dispositivo.

Cuando el virus ya se ha propagado, se activa lo que se denomina un **payload**. Esto es la función 'dañina' del virus. Algunos virus informáticos pueden servir de **puerta trasera** (**backdoor**) para permitir al atacante hacerse con el control del dispositivo, **puede recopilar o modificar los archivos y la información presente en el dispositivo**, o incluso **dañarlo de alguna manera**.

En la mayoría de los casos la presencia del virus pasa desapercibida por el usuario, pero en otros puede mostrar su *payload* de alguna manera.

¿Qué tipos de *malware* existe?

Existe multitud de tipos de malware. Su categorización depende de su funcionalidad y objetivo, así como su propagación. Algunos ejemplos son:

Según su medio de propagación

- **Virus**: El virus informático es la clase de malware estándar. Se propaga infectando otros equipos mediante correos electrónicos, descarga y apertura de archivos infectados, medios de almacenamiento infectados, etc.
- **Gusano (Worm)**: Un gusano actúa como un virus informático, pero su propagación se realiza a través de la **red local**. Esto lo consigue explotando alguna vulnerabilidad en los protocolos o servicios asociados a la red.
- **Troyano (Trojan)**: Un caballo de troya se camufla como un programa o software inofensivo, pero que al ejecutarse puede infectar el equipo con algún otro tipo de malware o incluso ser el mismo troyano el que realice el ataque, bajo un aspecto inofensivo para la víctima.

Según su funcionalidad

- **Spyware**: Conjunto de malware destinado a espiar a la víctima y hacerse con algún tipo de información. **Generalmente contraseñas o datos bancarios**.
- **Ransomware**: Conjunto de malware capaz de secuestrar un equipo informático, o una parte del mismo, para pedir después un rescate monetario por liberar el mismo. Algo así como un secuestro virtual.
- **Adware**: La finalidad del Adware es la de **mostrar publicidad no deseada al usuario de alguna forma mientras usa su dispositivo**. Puede ser mediante **ventanas emergentes (popups)** en el navegador, o de otra manera.

Según su finalidad

- **Rootkit**: Es un programa o conjunto de programas que le permite a un usuario no autorizado realizar operaciones en un equipo remoto. De éste modo el atacante puede hacerse con el control del mismo.
- **Criptolocker**: Es un tipo de ***ransomware*** que infecta un equipo informático y encripta los archivos que encuentre en el **mismo**. A continuación, le pide al usuario un rescate para recuperar la información encriptada, generalmente en **bitcoins**.
- **Keylogger**: Un programa *keylogger* es un tipo de ***spyware*** que se encarga de **registrar las pulsaciones en el teclado de la víctima**. De éste modo, un atacante puede hacerse con las contraseñas de las páginas web que visita la víctima o incluso sus datos bancarios y conversaciones.
- **Puerta trasera (Backdoor)**: Un programa en segundo plano que habilita alguna vía para que un atacante pueda hacerse con el control del equipo informático o instalar otro malware. Normalmente suelen ser parte de algún **troyano**.

¿Cómo se infecta un equipo?

Una infección se puede realizar por muchos medios, generalmente copiando código en algún sitio para que el equipo lo ejecute automáticamente. Un ejemplo es copiando ese código en los ejecutables de un ordenador, las librerías dinámicas de las aplicaciones que se ejecutan, los servicios en segundo plano, programando alguna tarea, copiándose a alguna de las carpetas de autoarranque del sistema, o incluso copiándose al sector de arranque del disco donde se encuentra el sistema operativo.

Antivirus como mecanismo de protección

Los antivirus son programas que intentan eliminar cualquier tipo de malware que pueda copiarse en el equipo. Por lo general suelen tener un proceso “centinela” (rogue) ejecutándose constantemente en segundo plano, que analiza todos los archivos y directorios según el usuario accede a ellos.

De éste modo, si un archivo está infectado, el antivirus lo reconoce y lo elimina al instante. Lo normal es que copie el archivo a una carpeta de “cuarentena” antes de preguntar al usuario qué hacer con el archivo.

Pero para que ésto funcione, el antivirus debe mantener una base de datos con **todo el malware que pueda reconocer**. Esto se hace mediante lo que se denomina una **base de definiciones**, que no es más que una base de datos con todo el malware reconocido por el antivirus, y sus propiedades (para que pueda reconocerlo).

Por éste motivo, **un antivirus solo no es la mejor solución a la hora de protegerse contra éste tipo de amenazas**. Ya que sólo reconocerá el malware

que tenga registrado en su base de definiciones. Si un atacante crea un nuevo malware que no sea reconocido por éstos antivirus, el malware podrá infectar el equipo sin ningún impedimento.

Si estás usando Windows 10 en el ámbito doméstico, Windows incorpora una herramienta llamada Windows Defender, que contiene un Antivirus. Por éste motivo, no es necesario que compres una licencia de Antivirus, que además requiere de una suscripción anual para poder usarlo (Aunque naturalmente, las empresas de antivirus intentarán convencerte de lo contrario).

En el caso de Windows 7, 8 y 8.1, si bien sería buena idea actualizar a Windows 10, puedes descargar Windows Security Essentials de la página oficial de Microsoft. Este programa incorpora un antivirus similar al Defender de Windows 10 y es completamente gratuito.

Si ésto no fuese suficiente y realmente necesitas otra solución, recomiendo Malwarebytes. Si bien éste contiene suscripciones premium con todos los extras típicos de cualquier otro antivirus, la versión gratuita sirve para escanear archivos y unidades y borrar malware. Eso sí, no tiene centinela.

¿Es verdad que Linux y Mac no tienen malware?

Ésto es un mito que viene de los años 90 y que ya se ha desmentido en numerosas ocasiones. El mito viene a raíz de que, por ser sistemas menos extendidos (como ya digo, en los años 90), nadie hace malware para Linux y Mac. Apple incluso llegó a usar éste argumento en alguno de sus anuncios en televisión, pero es algo completamente **falso**.

Este tipo de "seguridad" en el ámbito de la ciberseguridad se llama "seguridad por rareza" (Security by obscurity), y es el peor tipo de seguridad que existe (Si es que se le puede llamar "seguridad"). Se basa en que si el atacante no conoce la existencia o el funcionamiento de algo, entonces no podrá atacarlo o no querrá atacarlo. Naturalmente ésto es algo ridículo porque, en el caso de que haya un interés, aunque sea por simple curiosidad, nada le impide al atacante estudiar una plataforma, y aun en el caso de que un atacante desconociera de su existencia, es muy muy probable que acabe descubriendo su existencia tarde o temprano.

Existe malware para Linux y **una de las principales plataformas atacadas es Android**, que está basado en el núcleo de Linux. De hecho, Linux está muy extendido hoy en día. La mayoría de routers domésticos y equipos que se conectan a internet llevan un firmware basado en éste núcleo, así como numerosos servicios en internet que usan algún tipo de distribución basada en Linux como **Fedora**. Ésto hace que el interés por ésta plataforma sea, en la actualidad, bastante alto, y que el

riesgo de ser objeto de ataques también sea alto.

Los sistemas operativos de Apple **tampoco son una excepción**. Sobre todo si tenemos en cuenta el número de dispositivos móviles que utilizan **iOS**. Pero naturalmente que OS X y Mac OS han sido objeto de ataques en el pasado de igual forma. **Por norma general, si algo existe, puede ser atacado**.

Android y la Play Store

La tienda de aplicaciones de Android, llamada **Play Store**, es un nido de **malware**. Google se encarga de analizar los paquetes que se agregan a la Play Store, pero como ya he dicho, no se puede detectar lo que no se conoce, y ya ha habido numerosos casos en los que se ha tenido que retirar numerosas aplicaciones de la tienda por **contener malware**. Bien sea malintencionadamente, o por accidente al tener algún componente en común infectado.

Pero incluso en el caso de las aplicaciones verificadas, en numerosas ocasiones éstas aplicaciones contienen **spyware** que pasa desapercibido por el usuario, pero que los desarrolladores usan para algo más que "ofrecer una mejor experiencia de usuario".

"El sentido común es la mejor protección"

Esta es una frase que probablemente escuches en más de una ocasión. Hace referencia a que cuando usamos internet o hacemos uso de un equipo informático, sea un dispositivo móvil o un ordenador, debemos usar la cabeza y pensar en las posibles consecuencias de lo que estamos haciendo y analizar si lo que estamos abriendo o ejecutando podría o no ser seguro.

Esta premisa **es parcialmente cierta**. Por ejemplo, **si descargamos un PDF de internet y en la extensión del archivo pone ".pdf.exe" o ".pdf.jar", entonces es un ejecutable y podemos deducir que se trata de algún tipo de malware. Es uno de los trucos que se usan para infectar a los usuarios en páginas de descargas**, donde el usuario piensa que está descargando un archivo de música o un juego, pero en realidad se trata de un ejecutable infectado. Podemos detectar éste tipo de ataques simplemente fijándonos en lo que descargamos.

Pero, **¿Y si el archivo PDF estuviera infectado dentro del mismo?** Incluso aunque estuviésemos seguros de que la página es de confianza, **un atacante podría de alguna manera inyectar código malicioso en los paquetes de la conexión e infectarnos**. O incluso la propia página podría estar infectada, y podría ser complicado para un usuario detectarlo. En éste caso, el sentido común solo podría no ser suficiente.

Por supuesto, hay maneras activas de prevenir éste tipo de ataques. Un antivirus

podría detectarlo, asumiendo que dicho malware se encuentre en su archivo de definiciones. O incluso un firewall o un proxy podría cortar una conexión con un servidor no seguro. Pero si ese no es el caso, siempre se puede ejecutar primero en algún tipo de entorno controlado (sandboxed) y ver los cambios que se realizan en el sistema, antes de ejecutarlo en el sistema principal.

En cualquier caso, **siempre debemos tener sentido común a la hora de usar internet, ya que mucha gente intentará engañarnos de alguna manera para atacarnos y conseguir algo de nosotros**, sea información o dinero.

NO uses cuentas de Administrador en el equipo

Una de las malas prácticas de la mayoría de usuarios en general es la de utilizar el equipo con **una cuenta de administrador**. En todos los sistemas, salvo en Android e iOS (donde no hay cuentas de administrador), se permiten crear cuentas de usuario con distintos niveles de acceso al sistema. Por lo general, usuario y administrador.

Las cuentas de usuario sólo permiten el acceso a los archivos que se encuentran en la carpeta del usuario, así como la ejecución de aplicaciones que se hayan instalado para todos los usuarios. En cualquier caso, las aplicaciones que se ejecutan como un usuario regular, no tendrán acceso a las carpetas del sistema ni a la configuración del mismo. **Sólo podrán acceder a las carpetas y archivos del usuario que lo ha ejecutado**.

Sin embargo, un usuario administrador **tiene acceso a todo el sistema**. Eso quiere decir que puede acceder a todas las carpetas del sistema, a todos sus archivos, y realizar cambios en el equipo.

Por éste motivo, si un ejecutable infectado se ejecuta como usuario normal e intenta acceder a una carpeta del sistema o intenta realizar una modificación en el mismo, en Windows saltará el mensaje de UAC pidiendo la contraseña del administrador para realizar dichas acciones. Pero si de alguna manera consiguiese infectar el sistema pasando desapercibido para el mismo, en ningún caso tendría permisos de administración. Con lo que sólo afectaría al usuario que lo ha ejecutado.

Pero si se ejecuta como administrador, aunque también salta el UAC con un mensaje de “Sí” o “No” a la hora de realizar cualquier acción, si el malware pasase desapercibido de alguna manera, **podría conseguir hacerse con el control del sistema**.

En Linux, éste es el funcionamiento estándar del sistema. Los usuarios, por defecto, no tienen permisos de administración. Motivo por el cuál se usan los comandos *sudo* o *su* para realizar cambios en el sistema. **En Windows, sin embargo, al instalar el sistema se activa por defecto una cuenta de administrador**, que

es la que usa todo el mundo.

Por este motivo, **recomiendo crear una cuenta de usuario estándar nada más instalar el sistema operativo**, y usar esa cuenta en lugar de la del administrador. La única diferencia es que para instalar programas o acceder a ciertas configuraciones y carpetas, tendremos que introducir la contraseña del administrador. Es algo molesto, por supuesto. **Pero también es mucho más seguro**.

Cuidado con lo de "rootear" el móvil o la tablet

Los dispositivos Android o iOS no incorporan cuentas de administración, ya que son sistemas basados en Unix y/o Linux. Pero los usuarios no tienen ningún privilegio de administración en el sistema ni tampoco manera alguna, por defecto, de obtener esos privilegios.

Es por eso que en muchas ocasiones, para poder instalar aplicaciones que requieran de permisos de administración en el sistema, lo que hacen es modificar el sistema de tal manera que ganan privilegios de administración. A ésto se le llama "rootear" (viene del usuario 'root' que en los entornos UNIX es el administrador del sistema).

Ni qué decir que ésta práctica es una bomba de relojería. Al igual que no usarías una cuenta de administrador en un ordenador normal, tampoco lo harías en un dispositivo Android. **Menos en un teléfono, donde la gente tiene además datos bancarios, datos de acceso a redes sociales, etc**. Simplemente, no te la juegues.

Si lo que quieres son teléfonos con software totalmente libre donde puedas tener tú el control y que además respeten tu privacidad, prueba los Pinephone o los Librem.

Cuidado con las máquinas virtuales

Una de las prácticas de algunas personas es la de ejecutar un archivo en un entorno controlado usando algún tipo de software de virtualización como VirtualBox, VMWare o qEmu. Pero hay que tener mucho cuidado con ésto.

El software de virtualización crea un **ordenador virtual**, que podemos usar dentro de nuestro ordenador como si fuese un ordenador más. Pero ese ordenador virtual **también puede estar conectado a la red**. **Y existe malware que podría propagarse por la red**. Esto se puede conseguir o bien mediante la propia red en la que se encuentra el 'host', o **incluso a traves de las carpetas compartidas**.

Pero aunque deshabilitáramos la red y las carpetas compartidas en la máquina virtual, existe la posibilidad de que el software de virtualización pudiera tener algún tipo de vulnerabilidad que le permita a un atacante exponer la máquina 'host' a

través del equipo virtualizado (guest). Es algo que suena descabellado (Y desconozco si se ha dado alguna vez algún ataque de éste tipo), pero no es imposible y dado que los programas mencionados son bastante populares, es muy probable que haya interés en buscar un *exploit* de éste tipo y que incluso alguien se haya hecho ya con uno.

Nota: Cuando existe una vulnerabilidad que es desconocida para los usuarios y desarrolladores, se le llama '***0day* exploit**'.

ANTERIOR

Chatbots en Python 3.x

SIGUIENTE

Encriptación de correos electrónicos con GnuPG (GPG) y OpenPGP

Opinion | Otros | Personal | Privacidad | Programación | Tecnología | Time Machine | Tutoriales

RSS

Subscribirse al feed RSS