Fraudes, intrusión y malware

Álvaro González Sotillo

19 de enero de 2019

Índice

1. El origen del fraude.

El fraude informático puede presentarse de muchas maneras y desde muchos puntos de vista. Entendemos como fraude una acción deliberada, que tiene como objetivo perjudicar de alguna manera a alguien contra quien se comete. En el ámbito de la seguridad informática, esto incluye una posible disminución de cualquiera de las tres propiedades seguras básicas de un sistema de información (confidencialidad, disponibilidad, integridad). Aunque por supuesto, un fraude también puede atentar a través de medios informáticos contra la integridad de las personas, bien en su ámbito moral o financiero. Los medios por los que se suele realizar un fraude en la seguridad informática incluyen:

- Un mensaje, de e-mail o a través de redes sociales, programas de chat o de móvil.
- A través de la web
- Por una intrusión directa de una persona
- Por la actuación de malware.

Por supuesto, éstos cuatro medios pueden combinarse, y de hecho normalmente lo hacen. Por ejemplo,

- una gran mayoría de los fraudes que vienen por mensaje, indican una dirección web,

que da continuidad al fraude

- Los e-mail son a menudo fuente de propagación de malware
- El malware puede ayudar a un intruso a "colarse"
- etc. . .

A menudo, también se combinan con las habilidades personales para extraer información, a esas habilidades las denominamos ingeniería social.

2. Ingeniería social.

La ingeniería social es la práctica de obtener información confidencial a través de la manipulación de usuarios legítimos. Es una técnica que pueden usar ciertas personas para obtener información, acceso o privilegios en sistemas de información que les permitan realizar algún acto que perjudique o exponga la persona u organismo comprometido a riesgo o abusos. El principio que sustenta la ingeniería social es el que en cualquier sistema los usuarios son el eslabón débil. En la práctica, un ingeniero social usará cualquier medio de comunicación, no necesariamente informático, para engañar a la gente, fingiendo ser, por ejemplo, un empleado de algún banco o alguna otra empresa, un compañero de trabajo, un técnico o un cliente.

Vía Internet y la web también se usa, por ejemplo, de manera frecuente, el envío de solicitudes falsas de renovación de permisos de acceso a páginas web, correos falsos que solicitan respuestas o dinero e incluso las famosas çadenas", llevando así a revelar información sensible, o a violar las políticas de seguridad típicas. Con estos métodos, los ingenieros sociales aprovechan la tendencia natural de las personas a confiar y reaccionar de manera predecible en ciertas situaciones (por ejemplo proporcionando detalles financieros a un aparente empleado de un banco). Así, la ingeniería social ahorra procedimientos complejos y engorrosos para perpetrar el fraude, como tener que encontrar vulnerabilidades técnicas de seguridad en los sistemas informáticos.

3. Los mensajes, la web.

Mensajes, web e ingeniería social están íntimamente ligados. El correo electrónico (e-mail) y otras fuentes de mensajería es el origen y una herramienta más en el fraude.

3.1. SPAM

Genéricamente se llama así a todos los correos que se reciben sin ser solicitados.

Normalmente, su remitente es desconocido, en algunos casos falsos, y en otros, es una dirección usurpada. La mayor parte del SPAM es publicidad acerca de productos de dudosa calidad y procedencia. Vamos a hablar de algunos tipos de SPAM característicos.

3.2. HOAXES

Son correos cuyo contenido es falso. Hoax en inglés significa "bulo" o "broma". No obstante, a pesar de ser falsos, la mayor parte de ellos tienen un punto de verosimilitud o alguna otra característica que hace que se propaguen rápidamente. Suelen tratar acerca de:

- Alertas sobre virus incurables
- Mensajes de temática religiosa
- Temas solidarios
- Temas relacionados con la suerte

- Leyendas urbanas
- Métodos para hacerse millonario
- Regalos de grandes compañías

Algunos son simples bromas, otros, llevan una intencionalidad concreta. En algunos de ellos se mencionan datos falsos, como nombres de personas, teléfonos, direcciones matrículas de vehículos. En esos casos probablemente, los datos corresponden a personas a las que se quiere molestar. En otros casos, se pretende dañar la imagen pública de una compañía, o una determinada opción política. En otros, el objetivo es la recopilación de direcciones de correo electrónico.

Se pueden ver algunos de los últimos hoax en sitios como rompecadenas.com.ar o @malditobulo

3.3. Correo en cadena

Es un tipo especial de HOAX. Contienen textos sensibleros o de amenaza. Finalmente, se pide explícitamente que se envíe a varias personas A menudo amenazan con consecuencias graves si no se envía el correo. Su finalidad es siempre recopilar direcciones de correo. Estafas Una estafa es un engaño deliberado, para obtener un beneficio económico de una "víctima" sin una contraprestación legítima. Por ejemplo, un tipo de estafa bastante común consiste en los "correos millonarios" Son mensajes que avisan al destinatario de que debe

- Recoger una herencia
- Recoger un premio de lotería
- Recoger un regalo

- Presentarse a un puesto de trabajo
- Propuestas de negocios ilegales (blanqueo de dinero)

Siempre poniéndose previamente en contacto con un teléfono de pago, o bien, ingresando cierta cantidad de dinero en concepto de gasto En general, suele tratarse de pequeñas estafas, en las que la persona objeto del fraude no obtiene nada a cambio, y se le estafa una pequeña cantidad de dinero. Perseguir una pequeña estafa es complicado, en eso se escudan los estafadores. Las estafas de mayor valor recurren a otra artimaña: hacer que la "víctima" realice alguna acción ilegal... es decir, hacer creer a la víctima que participa en un asunto "turbio" en el que se engaña a un tercero. Por supuesto, no es así. La víctima cree que va a obtener un gran beneficio económico participando en una estafa, en la cual debe invertir una cierta cantidad de dinero, pero ella es la única estafada. A este tipo de estafas en la que la victima cree que participa como estafador se le llama a menudo timo. El timo es difícilmente denunciable, ya que la víctima tendría que admitir su intención de estafar a un supuesto tercero.

La estafa nigeriana. Via wikipedia

3.4. Publicidad, más o menos legítima.

La mayor parte del SPAM que se mueve por el mundo es, sin duda, publicidad. Los grandes anunciantes suelen prestar atención a los intereses de sus posibles clientes, tratando de no bombardearlos con demasiada publicidad por e-mail.

Sin embargo, anunciantes de menor prestigio no tienen escrúpulos en ofrecer todo tipo de productos y servicios por e-mail:

- Productos de electrónica (relojes, etc)
- Ropa y complementos de imitación de otras marcas
- Productos relacionados con el sexo.
- Productos de farmacia, herbolario, parafarmacia.

Quizá alguno de ellos sea de un vendedor legítimo, pero buena parte son de dudosa procedencia, y no se puede saber exactamente si es un vendedor de garantía. [Ej: Cómo funciona el spam de la Viagra. ¿Narcotraficantes virtuales o genios de la mercadotécnia?]

3.5. Phishing

El phishing (Password fISHING: pescar contraseñas) es la técnica por la cual el usuario entrega voluntariamente sus contraseñas u otros datos identificativos de cualquier servicio, aunque promovido por un engaño. Suele realizarse combinando e-mail y web. El ataque de phishing más típico consiste en enviar un e-mail haciéndose pasar por, una entidad bancaria o financiera, un grupo de accion solidaria... alguna organización legítima, informando de que por algún motivo el usuario debe acceder a la web de la organización para alguna cosa. En el mensaje se incluye un enlace, pero no al sitio web legítimo, sino a uno falso. El usuario introduce voluntariamente sus contraseñas. Luego, el portal falso puede marearlo con cualquier excusa, o redirigirlo al portal auténtico sin que se note el ataque. [Ej: Phishing con paypal y Gmail. Via spamloco.net]

3.6. Malware por correo.

El malware es el software con objetivo malicioso que se propaga por distintos medios. El e-mail y otros sistemas de mensajes son frecuente fuente de transmisión de malware. De todas formas, cualquier sistema de transferencia de ficheros puede ser utilizado para transmitir malware: páginas de descargas, BitTorrent, eMule,...

3.7. Las cifras del spam

La cantidad de spam que se propaga por internet a través del e-mail es realmente enorme. A través de otras redes de chat o sociales (messenger, facebook, etc...) las cifras son mucho menores.

El motivo es probablemente doble:

- Por un lado, esas redes de chat y sociales pertenecen a empresas privadas, que pueden poner algún mecanismo para filtrar el spam
- Por otro lado, tecnológicamente, el e-mail es bastante vulnerable y tiene un reparto descentralizado.

Durante el **2010**, en el informe conjunto de algunas empresas de antivirus con sede estadounidense, el tráfico de correos electrónicos alcanzó los 107 billones de correos electrónicos (107.000.000.000.000)

De ellos, el 89.1 % fueron SPAM: 262000 millones de correos electrónicos diarios 1 de cada 284 correos electrónicos contenía malware 2/3 del spam tuvo que ver con productos farmacéuticos 1 de cada 445 correos trataba de Phishing

Desde **2011**, el INCIBE con fuente de origen Symantec informa de una notable caida en la cantidad de SPAM, debido a la desarticulación de redes internacionales de difusión de spam

En 2017, el nivel de SPAM ha bajado al 55 % (Spam y Phising en 2017). Posiblemente el SPAM haya dejado de ser tan lucrativo como antes, debido a los mejores sistemas de detección y al aumento de otros tipos de comunicaciones por medio de las redes sociales.

4. Intrusiones por la red.

Las intrusiones suponen un intento deliberado de una persona de obtener el acceso a información para la cual no tiene permiso, alterar datos sin permiso, o lograr que algunos datos estén o no disponibles para sus usuarios legítimos. Dicho de otro modo, un intruso por la red es una persona que con procedimientos manuales, y sin acceso físico al sitio donde está almacenada alguna información, compromete la confidencialidad, la integridad o la disponibilidad de ésta información. Recuerda que si sólo se compromete la confidencialidad hablamos de un ataque pasivo. Si se compromete cualquiera de las otras dos propiedades, hablamos de un ataque activo.

La intrusión utiliza procedimientos manuales (no automáticos), aunque a menudo se combina una intrusión automática con malware y una intrusión manual. Uso de las redes Los intrusos hacen especial uso de las redes. Pueden utilizar técnicas y herramientas basadas en cualquiera de los niveles de:

- Físico/Enlace
- Red/Transporte
- Aplicación

4.1. Nivel Físico/enlace

En el nivel de enlace, se puede actuar consiguiendo interceptar el acceso físico a las redes:

- En redes cableadas, supone interceptar el cable, lo cual implica un desplazamiento físico de personas a algún punto de la instalación
- En redes inalámbricas, con poca protección, se puede lograr un enlace a un punto de acceso de una red, o lograr examinar el interior de las tramas.

4.2. Nivel Red/transporte

En el nivel de red y transporte, es especialmente delicada la conexión de ordenadores a Internet.

Dado que internet es una interconexión de redes en el nivel de red, se puede lograr interceptar o abrir un transporte remotamente

4.3. Nivel Aplicación

En el nivel de aplicación, el software se comunica utilizando protocolos de aplicación, que a menudo plantean vulnerabilidades. Esas vulnerabilidades son aprovechadas por los intrusos. Las herramientas del intruso. Es muy difícil catalogar a los intrusos y saber qué herramientas necesitan. Aunque, realmente, si se distinguen dos grandes grupos.

- Por un lado, el intruso que no tiene una intención concreta, sino que simplemente prueba a ver de qué es capaz... A veces se cuelan en algún sitio, a veces comprometen la disponibilidad de algún servicio, a veces obtienen acceso a información... pero su comportamiento es irregular y errático.
- Por otro lado, el intruso profesional que sabe lo que hace: tiene un objetivo concreto y no se desvía de él. Actúan como detectives: con paciencia, recopilando información, ordenándola, haciendo deducciones lógicas... y no dejando huellas de su actividad.

Cuando se deciden a atacar son rápidos y fulminantes. En este grupo podemos encontrar:

- A los intrusos con algún objetivo idealista (ej: vulnerar la seguridad de algún sitio por el orgullo de hacerlo; vulnerar la seguridad de alguna entidad como protesta por algún hecho relacionado con ella)
- A los intrusos con algún objetivo relacionado con el crimen (ej: obtener información valiosa de gobiernos, empresas, particulares, famosos, etc.) En algunos casos se trata de individuos solos y en otros pertenecen a bandas de crimen organizado Las herramientas que utiliza un intruso son básicamente tres: ingeniería social, malware y vulnerabilidades.

4.4. La ingeniería social

Es crucial para la actividad intrusa. Como siempre, las personas son el eslabón más débil, y a un intruso:

- Proporcionan contraseñas y accesos
- Informan acerca de estructuras
- Descuidan medidas de seguridad

4.5. Las vulnerabilidades del software.

Los intrusos utilizan las redes, que están controladas por software que responden a protocolos de comunicación.

Un intruso hace un uso irregular de éste software, y debe conocer las vulnerabilidades de cada software que utilice: es decir, aquella forma de utilizar un software que empieza a producir un comportamiento anómalo y que permite un avance del intruso. Todo el software (navegadores, servidores, el firmware de una wifi o de una tarjeta de red, los sistemas operativos) se programa teniendo en mente en primer lugar su funcionalidad, y suponiendo un uso predecible y regular de él. En segundo lugar, los programadores implementan algunas medidas de seguridad para aquellas situaciones irregulares que se les ocurren. Parte de las situaciones irregulares son predecibles y otra parte no puede ser ni imaginada por los desarrolladores del software. Esas

situaciones son, en principio, las vulnerabilidades. Los intrusos exploran formas de utilizar irregularmente el software y que no hayan sido previstas por los programadores. No obstante, a medida que los intrusos investigan, los desarrolladores van implementando medidas de seguridad nuevas para paliar las vulnerabilidades encontradas. Por eso es importante mantener el software actualizado: sistemas operativos, drivers, firmware y las aplicaciones relacionadas con la red.

4.6. Amenazas por la red.

Son muchas las formas en las que puede venir una amenaza. No obstante, caen en seis grandes categorías:

- SUPLANTACIÓN: Un atacante se hace pasar por un tercero, para dar información falsa o fraudulenta (spoofing –IP,DNS, ARP, e-mail,web. . .)
- INTROMISIÓN: Alguien consigue "colarse" a través de la red, y por ella, acceder a servicios que le permiten obtener información (archivos, mensajes, datos). (Phishing / Fuerza bruta / Diccionarios / Code Injection)
- MODIFICACIÓN: Se modifica información (archivos o documentos). Normalmente,tras una intromisión, haciendo uso de servicios de aplicación
- INTERCEPTACIÓN: La información que viaja por la red es desviada hacia otro destino (con técnicas conocidas como "secuestro" – Hijacking)
- ESPIONAJE: Se observa el tráfico de una red para obtener información cuando viaja. (sniffing)
- DENEGACIÓN DE SERVICIO (DoS / DDoS). Intenta impedir el correcto funcionamiento de un servicio (con técnicas como la "inundación" – flooding), de tal manera que el servicio no pueda atender a las peticiones legítimas.

4.7. Técnicas de intrusión

Comentamos algunas de las técnicas de intrusión más habituales

- SPOOFING también llamado poisoning(Del inglés spoof: parodia, representación teatral, o poisoning: envenenar) Consiste ensuplantar la identidad, en aquellos servicios de red donde sea posible.
- E-mail spoofing: falsear el remitente de un e-mail, cambiando las cabeceras del interior dele-mail.
- DNS spoofing: introducir nombres falsos en un sistema DNS legítimo, de tal manera que se resuelvan a una IP no legítima, o bien, lograr montar un DNS falso, y que algún cliente lo utilice. IP spoofing: sustituir la dirección IP del remitente de un paquete por otra
- ARP spoofing: En una red local con con hubs es posible hacer sniffing de las tramas de otros ordenadores, porque el hub reenvía las tramas a todos. En una red con switches o APs no se puede. El ARP spoofing consiste en la emisión desde un ordenador ilegítimo de tramas falsas que logren confundir a la caché ARP de otros ordenadores y del switch o AP, para que seenvíen las tramas al ordenador ilegítimo.
- DHCP spoofing: hacerse pasar por un DHCP legítimo en una LAN, y servir información de configuración falsa a los nuevos clientes, en especial la de la puerta de acceso o los DNS, con intención de desviar sus comunicaciones.

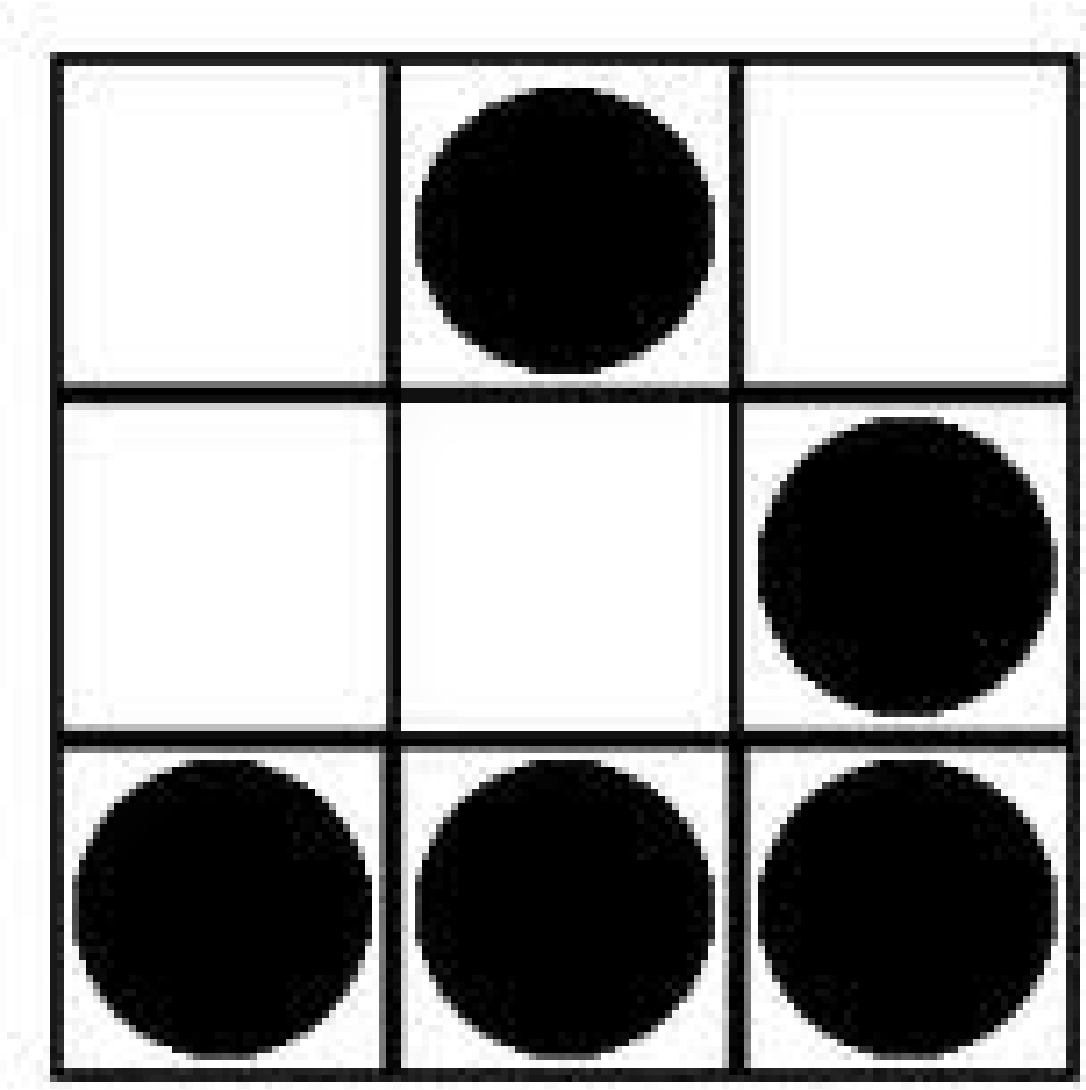
4.8. Man-in-the-middle

Es una expresión que significa que un intruso logra un acceso a algún punto intermedio de una comunicación, en cualquiera de los niveles de red. Normalmente se logra mediante alguna técnica de spoofing, y permite hacer sniffing.

4.9. El malware en la intrusión

El malware también desempeña un papel muy relevante en la intrusión, dado que si logra instalarse en un ordenador en el interior de una red local puede ayudar «desde dentro» a que un intruso logre internarse desde Internet en la red local.

5. La cultura de la intrusión: Hackers



Existe toda una cultura en la intrusión. Es la "cultura hacker" o "movimiento hacker". Entre ellas se encuentran todo tipo de personas y resulta difícil establecer clasificaciones.

En general, se necesita mucha destreza y conocimientos técnicos de un montón de vulnerabilidades... pero desde el punto de vista de la Seguridad Informática, tanta amenaza representa alguien diestro como alguien inexperto.

el logo del movimiento hacker es el de la ilustración, corresponde a una determinada posición de fichas "the glider" en un juego propuesto por el matemático John Horton Conway llamado "Juego de la vida".

5.1. Terminología hacker

- Black Hat: Por un lado muchos de los autodenominados hackers intentan intrusiones no autorizadas a través de redes, con el objeto de vulnerar alguna de las propiedades seguras, en muchas ocasiones, con intención de perjudicar u obtener provecho. A menudo se les llama crackers, aunque también se conoce con ese nombre a los que se saltan sistemas de seguridad del software (es decir, a los que programan cracks, o keygens, u obtienen serials).
- White Hat: Por otro lado, algunos hackers proclaman que sus intenciones no son vulnerar las propiedades seguras, sino descubrir vulnerabilidades, e informar a los propietarios de los sistemas de éstas. En cualquier caso, una intrusión no es deseable en ningún sistema, independientemente de las intenciones que declare el intruso.
- Samurai: En la cultura hacker se llama SAMURAI al especialista en seguridad, que conoce las técnicas de hackers y crackers, y que normalmente las utiliza para instalar, probar o configurar sistemas seguros. Algunos samurais de prestigio previamente fueron black o white hats. [Ej: Kevin Mitnick]
- script-kiddie, newbie: Son términos para referirse a los novatos en la materia.
- Lamer: es un término absolutamente despectivo para referirse a alguien con un comportamiento o actitud molesta
- wannabe: otro término despectivo para un novato con aspiraciones.
- nerd: difícil de describir en nuestra cultura, el término es puramente estadounidense.

5.2. FUERZA BRUTA

Consiste en probar todas las combinaciones posibles de contraseñas o palabras de paso para acceder a un determinado servicio

5.3. ATAQUES DE DICCIONARIO

Consiste en suponer que el comportamiento de un usuario a la hora de elegir una contraseña es predecible, y probar una lista más o menos larga de contraseñas comunes. Normalmente incluyen palabras de uso común del idioma del usuario, del inglés, combinaciones de números, fechas.... y nombres propios... incluyendo artistas, cantantes, lugares, marcas comerciales...

5.4. CODE INJECTION

(Inyección de código) Consiste en aprovechar un tipo concreto de vulnerabilidad de algunos sistemas, en los cuales, es posible conseguir que se ejecute código introduciéndolo en algunos lugares concretos y de una manera determinada. Todos los sistemas informáticos están formados por largas colecciones de código: los programas y scripts. Los ordenadores están permanentemente ejecutando código que reciben por los canales adecuados. No obstante, y por falta de previsión, en algunas partes de un sistema, en principio no aptas para recibir código, se puede escribir código que cumpla ciertas condiciones y resulta que es ejecutado. Conocer esos sitios donde quizá se ejecute código, y escribir y enviar ese código y aprovechar lo que éste pueda hacer es el code injection. Por ejemplo, es un ataque común a las páginas web la inyección de SQL (SQL injection) en el campo de texto del formulario que se utilice para pedir un nombre de usuario y contraseña. A veces, se logra que la página ejecute una orden SQL, pudiendo obtener algún login de usuario o contraseña, o al menos una pista acerca de ellos. Otro ejemplo: el php injection. En algunos sitios web escritos en el lenguaje PHP y que permitan subir ficheros (ej... un foro que permita subir fotos)... se sube en lugar de una foto un programa en PHP, y se ejecuta a través peticiones HTTP pasando parámetros por GET.

5.5. HIJACKING

(secuestro) Consiste en desviar una comunicación en marcha hacia un tercero -un man-in-the- middle, que dejaría de estar en medio para pasar a ser receptor final-. Por ejemplo es bastante frecuente el secuestro de sesión, interceptando la cookie que lleva la información de la sesión de un tercero. Cuando un sitio web (por ejemplo, un foro) reconoce a un usuario por su nombre y contraseña le envía a su navegador un identificador de sesión a través de una cookie del navegador. Si se logra interceptar la cookie con ese código, un tercero puede lograr continuar con la sesión abierta en el foro por el usuario legítimo sin necesidad de saber su contraseña.

5.6. SNIFFING

(Del inglés: "husmear"). Consiste en interceptar una comunicación (tramas o paquetes, según el nivel) y examinar su contenido, averiguando información sobre destinatario, remitente y el contenido de sus comunicaciones

5.7. DoS

(Del inglés Denial of Service - Denegación de Servicio). Consiste en enviar muchas peticiones falsas a un servicio, logrando que se colapse y deje de servir a las peticiones legítimas. A veces se logra un colapso temporal (mientras dure el ataque) y a veces, por falta de previsión en la programación se logra un colapso definitivo, hasta que se detecte el colapso y se reinicie el servicio. Si el ataque se produce simultáneamente por varios atacantes a la vez se le denomina DDos (Distributed Denial of sevice) La DoS más común en nuestros días va dirigida hacia servidores web, en forma de peticiones http. El flooding (inundación) es una técnica concreta para logar un DoS, inundando de peticiones las redes. Normalmente se intenta provocar un colapso en la red, más que en un servicio concreto.

5.8. Exploit

Llamamos así a cualquier pieza de software que ayuda a vulnerar una medida de seguridad, seguramente aprovechando vulnerabilidades de los sistemas Ej:

- Aplicaciones que ayudan a hacer DoS
- Aplicaciones que prueban diccionarios sobre sistemas
- Aplicaciones que intentan descubrir la contraseña de una Wifi criptoanalizando tramas cifradas
- El trocito de código que un intruso escribe en un formulario de una web para hacer SQL injection
- Algún script que se sube a un servidor web para tomar el control del navegador de un usuario

El malware, que veremos a continuación, se diferencia de los exploits en que se distribuye de manera autónoma. Un exploit debe ser ejecutado y/o distribuido manualmente.

5.9. Zero day

Cuando se descubre una vulnerabilidad en un sistema, se suele informar de ella al fabricante de forma que sea solucionada en las siguientes actualizaciones. Si el descubridor de esa vulnerabilidad decide no informar, y aprovechar dicha vulnerabilidad (manualmente, utilizando malware o un exploit), se dice que el ataque es un ataque de día cero. Estos ataques son especialmente peligrosos, ya que ningún administrador de sistemas ni ningún antivirus están preparados para el mismo.

6. Malware

Llamamos genéricamente "malware" (del inglés malicious software), a todo el código con intención maliciosa u oculta que intenta deliberadamente vulnerar cualquiera de las tres propiedades sin el consentimiento de su propietario El software es considerado malware en base a las intenciones del autor a la hora de crearlo El malware tiene dos objetivos fundamentales:

1. PROPAGARSE: el malware debe llegar a un gran número de máquinas y usuarios. Está programado y diseñado para propagarse al máximo posible
2. REALIZAR ALGUNA ACCIÓN MALICIOSA: A esa acción le denominamos la carga (payload, en inglés). Consiste en alterar el normal funcionamiento de la computadora, sin el permiso o el conocimiento del usuario

6.1. Los sistemas operativo objetivo

Windows y sus usuarios son, sin duda, los objetivos más claros de todo el malware. Los constructores de malware, en general, pretenden que el malware se propague llegando a la mayor cantidad posible de lugares. En ese caso, está claro que Windows es una apuesta ganadora, ya que se mantiene entre el 80 % o 90 % de los usuarios de Internet.

El resto es para los usuarios de tipo Unix: Mac OS y Linux.

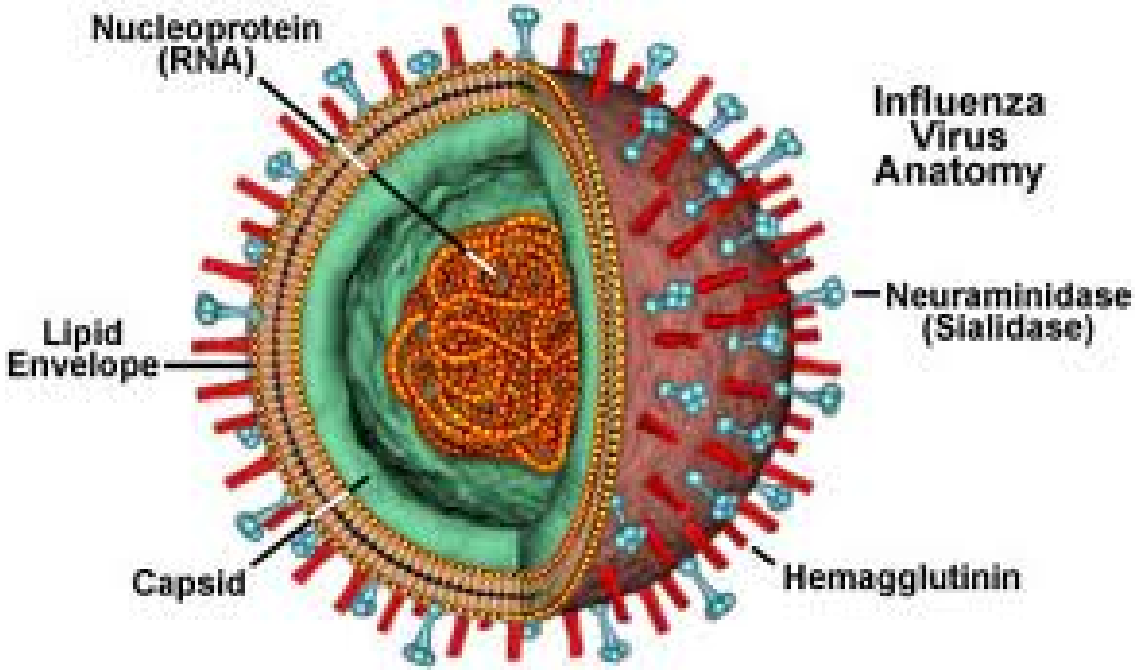
En dispositivos móviles y portátiles están irrumpiendo con tremenda fuerza en los últimos dos años iOS (de Apple) y Android (de Google), con lo que la cantidad de malware para ellos se ha visto multiplicada en el mismo factor que su expansión.

6.2. Clasificación por la forma de propagarse

Según la forma de propagarse, denominamos al malware como virus, gusano o troyano.

A continuación vamos a ver las tres formas básicas de propagación del malware, pero hoy en día es común que un malware utilice más de una de manera combinada para propagarse.

6.2.1. VIRUS



La forma de propagarse es e propagarse a través del software lícito, alterando ficheros y otros códigos. Los virus entran en una computadora mediante la ejecución de un programa infectado. Con esa acción, el virus logra ser ejecutado también. El usuario no detecta nada visualmente en ese primer momento, pero de forma transparente, el virus busca una ubicación en memoria secundaria donde poder duplicarse. El virus busca código ejecutable en dispositivos de memoria secundaria, y graba su propio código junto a él. Por ejemplo, objetivo frecuente de los ataques de virus son los ficheros ejecutables que pueda haber instalados en un entorno Windows (los .exe). Si en un ordenador se ejecuta un virus (por ejemplo, porque viene en un programa infectado que me ha pasado alguien en un pendrive)... el virus buscará otros ficheros .exe donde "pegarse". Al apagar el ordenador, el virus ya no estará activo, pero como se ha propagado a ficheros .exe, tarde o temprano lo volverán a ejecutar, continuando con el proceso de infección. No sólo hay código ejecutable en los .exe: en windows también hay en .dll y otros muchos tipos de archivo. También es código ejecutable los sectores de arranque y algunas partes del sistema operativo, como los drivers. Hay otros tipos de ficheros, que no son directamente ejecutables por el S.O., pero se interpretan por algunos programas: macros del Office, ficheros por lotes (BAT, SH), que también podrían ser infectados.

El término de "virus" se debe a Fred Cohen (en la foto), que en 1986 desarrolló como trabajo para clase un programa que se "propagaba" de un ordenador a otro infectando el sector de arranque de los disquetes, en un tiempo en el que los ordenadores no tenían discos duros. El profesor de Cohen en esa clase en la Universidad

de California era Leonard Adleman (la "A" de RSA). El virus de Cohen no llevaba payload.

6.2.2. GUSANOS

Un gusano tiene la propiedad de duplicarse a sí mismo pero no altera ficheros ejecutables ni otros códigos. Utiliza las vulnerabilidades del S.O. como vía de duplicación. La diferencia fundamental con un virus es que un gusano es un trozo de código que se duplica entero, y no "se pega" a otros ejecutables. Reside en memoria e intenta propagarse a través de servicios de red, y dispositivos de memoria secundaria. No suele requerir

intervención del usuario. Por ejemplo, son bastante comunes los gusanos de pendrive. Intentan propagarse a través de los pendrives que insertamos en una y otra máquina. El gusano se copia en el pendrive entero (es decir, en uno o más ficheros), y luego debe utilizar alguna vulnerabilidad para lograr ser ejecutado: en el caso de los pendrives, alterando el fichero autorun.inf, y esperando que alguna máquina Windows lo ejecute automáticamente. También hay gusanos de red, que se propagan utilizando algún protocolo de compartición de archivos, y luego aprovechan alguna vulnerabilidad del sistema operativo destino para ser ejecutados. En resumen, los puntos clave para identificar a un gusano:

1. Se duplica entero, normalmente como un fichero individual... Directo desde la memoria principal a una secundaria (como un pendrive), o utilizando alguna aplicación relacionada con la red (compartir ficheros, ftp, nfs, e-mail, web...)

2. Debe aprovechar alguna vulnerabilidad en la máquina de destino para lograr ser ejecutado allí. (Si no es ejecutado no estará "activo").

El primer gusano famoso se debe a Robert Morris , que en 1988 diseñó un pequeño programa que se propagaba utilizando una vulnerabilidad del módulo de envío de e-mail en los sistemas unix de la Internet de la época mplementados en máquinas fabricadas por DEC y Sun. Como payload, el gusano intentaba averiguar contraseñas de correo y de acceso al sistema utilizando técnicas similares al ataque de diccionario. Un fallo en su programación hizo que se replicase más de la cuenta consumiendo la memoria de las máquinas y causando denegaciones de servicio masivas (disponibilidad). Se estima que infectó a unas 6000 de las 60000 máquinas conectadas a Internet en aquel momento. Muchas de ellas pertenecían a organizaciones gubernamentales de EEUU y sus contratistas, con lo que Morris fue acusado de ataque contra el gobierno de los Estados Unidos, y aunque sus abogados alegaron que intentaba ayudar a la seguridad de Internet cuando su programa se salió de su control por accidente (white hat) fue encontrado culpable. Erradicar el gusano costó casi un millón de dólares, sumado a las pérdidas por haberse detenido casi toda la red, siendo estimadas las pérdidas totales en 96 millones de dólares

6.2.3. TROYANO

Se presenta al usuario como un programa aparentemente legítimo e inofensivo (juegos, utilidades, animaciones...) pero al ejecutarlo ocasiona alguna acción encubierta (payload), o inicia algún otro tipo de propagación (se comporta como virus o gusano). El término troyano proviene de la historia del caballo de Troya mencionado en la Odisea de Homero.

6.3. El payload (la carga)

Los posibles payloads de los malwares son variadísimos, pero vamos a mencionar tan solo algunos términos que se utilizan comunmente para designarlos. Por supuesto, la carga de un determinado malware puede caer en más de una de éstas categorías.

6.3.1. SPYWARE

Software “espía”: recopila información sobre las actividades realizadas en un ordenador. La función más común que tienen estos programas es la de recopilar información sobre el usuario y distribuirlo a empresas publicitarias u otras organizaciones interesadas, aunque consideramos spyware al software que espía cualquier

cosa. Ej: Mensajes, Contactos, contraseñas datos sobre la conexión a Internet, como la dirección IP, el DNS, el teléfono y el país; direcciones web visitadas, tiempo durante el cual el usuario se mantiene en dichas web y número de veces que el usuario visita cada web; software que se encuentra instalado; descargas realizadas cualquier tipo de información intercambiada, como por ejemplo en formularios, con sitios web, incluyendo números de tarjeta de crédito y cuentas de banco, contraseñas, etc.

6.3.2. ADWARE

Intenta propagar publicidad no deseada, por canales no legítimos. (Ej: ventanas emergentes, cambiando la publicidad "legítima" de las páginas que vemos por otras...)

6.3.3. CRIMEWARE

Ayuda a realizar actividades que enriquezcan a quien controla el software de manera ilícita. Ej: Ayudando a estafas, suplantando personalidad, etc...

6.3.4. RANSOMWARE

El malware *secuestra* la información del ordenador, generalmente encriptando los ficheros del disco duro. Después, envía la contraseña que ha usado para el cifrado a algún servidor de Internet y muestra un mensaje pidiendo dinero para recuperar dicha contraseña.

Los pagos exigidos suelen ser en Bitcoins u otra moneda virtual, para intentar ocultar su rastro. Además, los pagos suelen ser negociables.

Hay que tener en cuenta que, como en los secuestros reales, el pago del rescate no garantiza que el hacker devuelva la clave de encriptación, o que ésta funcione.

En ocasiones, la clave de cifrado puede recuperarse del ordenador infectado. Los fabricantes de antivirus tienen varias herramientas para recuperar los datos de un ordenador infectado.

6.3.5. KEYLOGGERS

Registran pulsaciones de teclas, para posteriormente transmitirlas a algún otro lugar, permiten espiar documentación que se teclea, datos confidenciales, etc. [Culturilla: Si se tiene acceso físico a una máquina también existen los keyloggers hardware. Se colocan en el cable del teclado y registran las pulsaciones en una memoria flash interna. Luego, puede retirarse y leerse la información También los hay que transmiten la información por la red, o módulos electrónicos para integrar en el interior de un teclado, y no ser visibles por una inspección ocular superficial] http://www.keelog.com/es/

6.3.6. SCREENLOGGERS

Evolución de los anteriores, capturan la pantalla entera, o trozos de pantalla, para posteriormente transmitirlas a algún otro lugar. Dado que una captura de pantalla consta de muchos más bytes que una pulsación de teclado, no están constantemente capturando. Actúan a petición, o ante determinados eventos, como pulsaciones de ratón. CULTURILLA: También hay screenloggers por hardware. http://www.keelog.com/es/hardware_video_logger.html

6.3.7. Mineros

La carga intenta utilizar la potencia del ordenador infectado para minar alguna determinada criptomoneda, a favor del intruso que ha programado el malware. Las criptomonedas se obtienen realizando muchas operaciones matemáticas, con lo que hace falta potencia de cálculo, que es bastante cara. A menudo, el gasto energético necesario para minar una unidad monetaria es mayor que el valor de la unidad obtenida.

6.3.8. ROOTKIT

Es una herramienta, o un grupo de ellas que tiene como finalidad esconderse a sí misma y esconder otros programas, procesos, archivos, directorios, claves de registro, y puertos que permiten al intruso mantener el acceso a un sistema para remotamente comandar acciones o extraer información sensible. Permite un acceso de privilegio continuo a una computadora pero mantiene su presencia activamente oculta al control de los administradores y del propio sistema al corromper el funcionamiento normal del sistema operativo o de otras aplicaciones. El término proviene de una concatenación de la palabra inglesa "root" que significa raíz (nombre tradicional de la cuenta privilegiada en los sistemas operativos Unix) y de la palabra inglesa "kit" que significa conjunto de herramientas (en referencia a los componentes de software que implementan este programa). En otras palabras, usualmente se lo asocia con que se esconde a sí mismo y a otros programas, procesos, archivos, directorios, claves de registro, y puertos. Puede ser la puerta de entrada de una intrusión o de nuevo

malware. Algunos no son muy dañinos... Otros, como el gusano conficker fueron astutamente concebidos y causaron tremendos estragos.

6.3.9. BOTs y RATs

Un BOT (de roBOT) es la evolución de un RAT (remote administration tool)

Un RAT es un software que permite administrar remotamente un ordenador, pero si se usa de carga de un malware, un intruso puede entonces realizar gran cantidad de tareas sobre el ordenador infectado:

- Capturar teclas o pantalla
- Cambiar el registro
- Escribir en memoria secundaria

- Instalar programas
- Realizar acciones de red, Etc

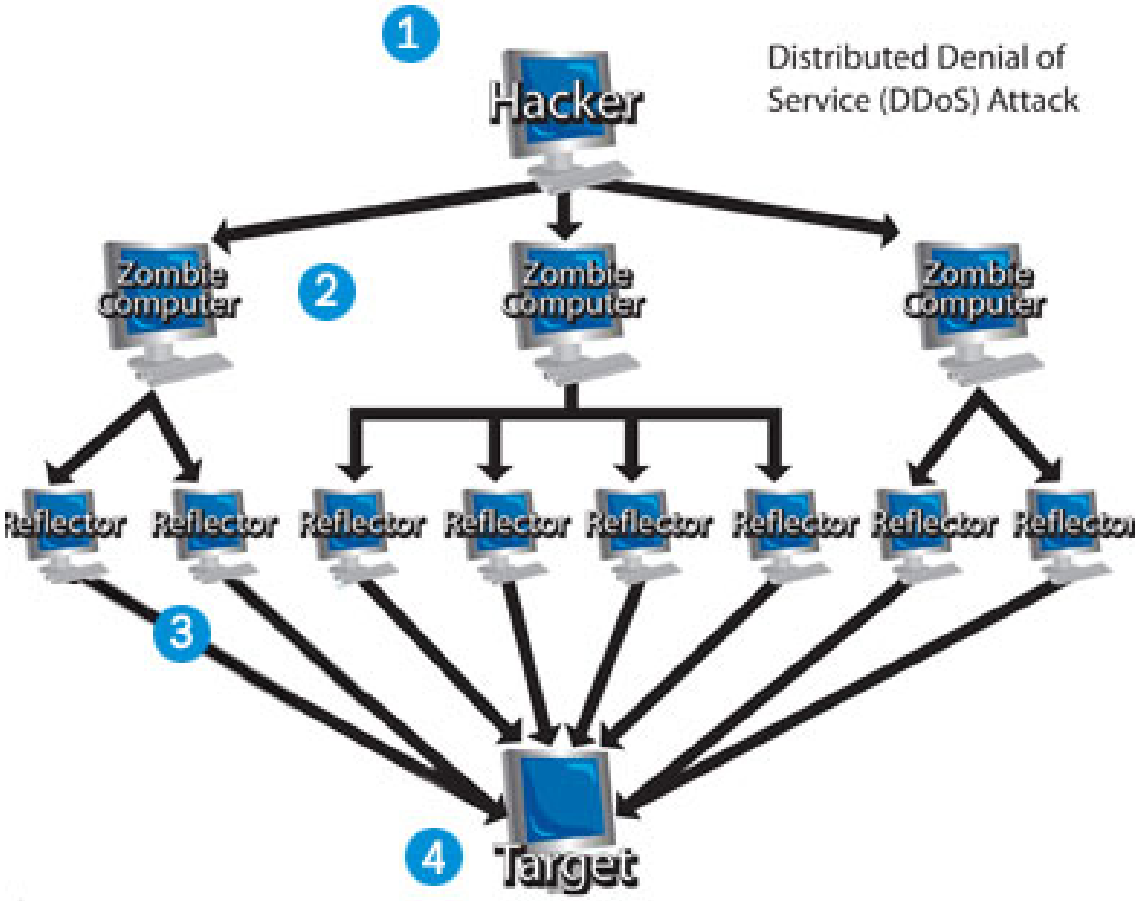
No obstante, los RAT han evolucionado en BOTS, que son capaces, además, de ejecutar scripts de instrucciones.

Cuando un BOT infecta un ordenador, se intenta conectar a una dirección que tiene programada, en la que el intruso le va a dejar un script con instrucciones. El bot se conecta periódicamente a ver si le han dejado instrucciones, y hace lo que se le pida remotamente.

6.3.10. IMPORTANTE: la “llamada a casa”.

Los más antiguos o rudimentarios de los RAT se quedan "escuchando" por un puerto TCP o UDP, esperando a que se conecte el intruso. Eso no es práctico, dado que si el RAT llega a un equipo con una IP privada y que está tras un router con NAT/PAT, un intruso no puede acceder desde el exterior de la LAN al ordenador, ya que no hay rutas para llegar a una IP privada. Los RAT más modernos son activos y utilizan la técnica de la llamada a casa. Una vez instalados, ellos intentan abrir un transporte hasta un servicio alojado en una IP pública en el que espera el intruso. El router con NAT/PAT sí abrirá el transporte hacia la IP pública. Por supuesto, el intruso utiliza una dirección IP dinámica

6.4. BotNets o "Redes Zombi".



Un conjunto de ordenadores infectados por un determinado Spybot se denomina una Botnet, o red zombi. Una red zombi representa una amenaza en sí misma, dado que es una fuerza bruta disponible para una finalidad en principio, desconocida., al servicio del intruso que la controla. Los usuarios de un ordenador que pertenece a una red zombi no son conscientes de ello, ni del uso que le pueda estar dando el intruso que la controle. Las actividades más comunes para una red zombi son el envío de spam, o los ataques de denegación de servicio.

7. Prevención

Las medidas de seguridad activas contra el fraude, intrusiones y amenazas es muy variada, y depende del momento, pero a rasgos generales, hay tres puntos de especial incidencia:

- EDUCACIÓN DEL USUARIO:
  - Instalar software sólo de procedencia legítima, y sólo si realmente se necesita, y, en ese caso, estar pendiente de mantenerlo actualizado para evitar la explotación de vulnerabilidades.
  - Convencer al usuario de que en general, cualquier cosa que venga por correo electrónico u otros medios de mensajería digital, y de la que se pueda sospechar mínimamente que es falsa, probablemente lo sea.
  - Informar al usuario de que los servicios en los que esté registrado (bancos, entidades financieras, redes sociales, etc....) NUNCA le van a pedir sus contraseñas por correo.
  - Informar al usuario de que si recibe por correo electrónico un aviso de su banco, o red social o foro o algo similar que le sorprenda, NUNCA debe seguir ningún enlace incluido en el correo.
  - Escoger contraseñas de longitud y complejidad adecuadas, mantenerlas en secreto y cambiarlas con frecuencia. En la medida de lo posible, mantener contraseñas diferentes para servicios diferentes, especialmente para aquellos más sensibles.
  - Intentar no acceder a sistemas sensibles desde máquinas o redes desconocidas: -Hotspots (puntos de acceso públicos) -Ordenadores "prestados" -ej, el del colegio, el de un cybercafé o locutorio-
  - Utilizar el antivirus instalado para escanear pendrives y discos extraíbles.
  - Informar al administrador cuanto antes de cualquier sospecha.
  - Utilizar privilegios de usuario normal para el trabajo diario. Los privilegios de administración deben dejarse sólo para tareas de administración.
- EL TÉCNICO INFORMÁTICO:
  - Los usuarios que trabajen con una máquina deben tener el menor nivel de permisos con que se les permita trabajar.
  - Los permisos se basarán en una whitelist, no en una blacklist: se van otorgando permisos necesarios, pero por defecto no debe estar otorgado ningún permiso.
  - Los datos, documentos, etc., que se elaboren deben ir a una carpeta de red en un servidor desatendido, o a través de cualquier otro medio de sincronización de información. El hecho de que el servidor esté desatendido minimiza el riesgo relacionados con el usuario como eslabón más débil.
  - Debe programarse una copia de seguridad, para que en caso de un ataque activo con pérdida de integridad pueda restaurarse a un estado anterior
  - Debe cambiarse en el BIOS el orden de los dispositivos de arranque, para colocar en primer lugar el disco duro principal, y evitar la ejecución del sector de arranque de un CD/DVD o una unidad portátil.
  - Revisar las políticas de seguridad del sistema operativo, para desactivar posibles puntos de entrada de intrusos o malware.
    - Por ejemplo, Autoplay de Windows, o el equivalente en otros sistemas operativos
  - Debe mantenerse un antivirus y asegurarse de que se mantiene totalmente actualizado.
  - Periódicamente es necesario programar un escaneo de malware previo al arranque del sistema operativo, para detectar rootkits.

- Deben realizarse auditorías en las que se intentará descifrar las contraseñas de los usuarios. Cualquier contraseña descubierta se considerará débil y deberá ser cambiada.
- Cuando se produzcan cambios en los usuarios (rotación de personal) deben desactivarse cuanto antes los usuarios que ya no se usarán.
- Debe prestarse atención a la configuración de la red local, y de los enrutadores (Las redes Wifi siempre deben configurarse con el mayor nivel de seguridad posible. Para evitar la llamada a casa puede utilizarse configuraciones de red seguras, en el nivel de red y aplicación, mediante la combinación de un firewall y un proxy. - ésto lo trataremos en los temas siguientes-).

- EL ANTIVIRUS
  - Hoy en día es imprescindible que todos los ordenadores conectados a internet cuenten con uno.
  - Al nivel coloquial, a todo el malware se le llama "virus"... por eso este tipo de programas se llaman así, aunque realmente intentan proteger de todo tipo de malware.
  - Un antivirus funciona buscando estadísticamente trazas de malware conocido en memoria secundaria, principal y comunicaciones. Para ello, disponen de una base de datos de indicadores de malware, que debe estar actualizada. Son indicadores numéricos... "huellas" heurísticas que pueden indicar la presencia de un determinado malware.
  - Tienen varias formas de actuar:
    - Al vuelo: buscan malware mientras se ejecutan programas (pasan de memoria secundaria a principal), cuando se insertan dispositivos de memoria secundaria o en el tráfico de red.
    - A propósito: buscan malware por indicación del usuario en memoria secundaria
    - Durante el arranque: cuando todavía no está cargado el sistema operativo, buscando rootkits en el sistema de ficheros.

8. Conclusión

Fraude, intrusión y malware son hoy en día tres conceptos interrelacionados. En este tema hemos intentado hacer un acercamiento a ellos y tener idea de cuales pueden ser los principales puntos de prevención. Es importante saber que los fraudes e intrusiones existen, y que tarde o temprano seremos un objetivo. En thehackernews.com puede verse como empresas y particulares de todo tipo son afectados a diario. La participación de un antivirus es casi imprescindible, pero, en un ámbito empresarial puede ser conveniente prestar también atención a la configuración de red, y a evitar que los usuarios trabajen en los sistemas operativos con privilegios de administración. La configuración basada en estaciones de trabajo y servidores garantiza un mayor control sobre la información. No obstante, el punto clave siempre es la educación de los usuarios (y la formación de nosotros mismos), para que las acciones del día a día se realicen desde una perspectiva segura, lo que suele repercutir en mayor tranquilidad, tanto para usuarios de la empresa, como para los técnicos. En España, los técnicos contamos con la ayuda de:

8.1. Instituto Nacional de Ciberseguridad

El Instituto Nacional de Ciberseguridad (INCIBE), dependiente del Ministerio de industria, energía y turismo, cuyo sitio web es incibe.es . Es una buena fuente de información para la formación y concienciación en seguridad informática

El CERTSI está más orientado al personal técnico -tú-. En esta página encontrarás:

- Información actualizada sobre incidencias de seguridad en España

- Formación
- Herramientas
- Avisos vulnerabilidades y de actualizaciones de software
- Estadísticas en tiempo real mediante la red de sensores
- etc.

8.2. La Oficina de Seguridad del Internauta

dependiente del INTECO, pero con sitio web propio. osi.es Está dirigida a los usuarios de internet en general, y nos ayuda porque da respuesta a muchas de las preguntas y situaciones comunes con las que nos encontramos.

8.3. Otros recursos

Las compañías dedicadas a la ciberseguridad aportan también publicaciones de interés para la formación de empleados y técnicos, como este informe de seguridad de Panda.

9. Referencias

- Adaptado de Víctor J. Fernández
- Versión en PDF