INSTITUTO de ENSEÑANZAS a DISTANCIA de ANDALUCÍA

2º de Bachillerato

Tecnologías de la Información y Comunicación

Contenidos

Diseño web funcional.Prevención y buenas prácticas: Seguridad frente a software malicioso

Imagen en Flickrcc de Christoph Scholz

Todos habremos oído alguna vez hablar de virus informáticos, e incluso es probable que tengamos instalado un antivirus en nuestro PC, pero ¿es este el único ataque que puede recibir nuestro equipo?, la respuesta es no.

Los virus no son más que un tipo (de entre otros) de software malicioso que puede instalarse en nuestro ordenador, tablet o móvil, pero veremos que hay más.

Conocerás también alguno de los diferentes mecanismos usados para atacar nuestros equipos, desde correos, suplantar la identidad de otro, capturas tus contraseñas, etc.

Pero no te desesperes, afortunadamente también hay utilidades para detectar y solventar estos problemas, así como una serie de buenas prácticas. También las veremos.

1. Malware (software malicioso)

La palabra **malware** proviene de las palabras (en inglés) MALicious softWARE, que se traduce como software malicioso.

Cuando hablamos de malware, no nos referimos a ningún software defectuoso (un bug en una aplicación no es algo que se haga con intencionalidad ni buscando fines dañinos).

Malware engloba todo aquel software creado para infiltrarse en un equipo informático con la finalidad de modificar su funcionamiento o la información que almacena, modificándola, eliminándola o reenviándola a terceros sin el consentimiento de su propietario.

Los efectos de este tipo de software son muy diversos, y pueden ir desde una simple molestia para el usuario a ser muy perjudiciales y dañinos.

Virus, gusanos, troyanos, spyware, adware y otros, no son más que distintos tipos de software malicioso que iremos conociendo a lo largo de este tema.

Imagen en Pixabay de Antara_Nandybajo licenciaCC0 Public Domain

Un virus es un programa o fragmento de código, que se carga en un equipo sin consentimiento ni conocimiento del propietario.

Algunos son solo molestos pero otros pueden llegar a ser muy dañinos, destruyendo información o tomando el control del sistema. Sus efectos pueden ir desde rotar la pantalla, cambiar nombres de carpetas, cambiar el puntero del ratón hasta modificar valores en el registro y controlar totalmente el equipo infectado, pudiendo también borrar o modificar la información que contiene.

Este código malicioso puede venir en archivos ejecutables descargados de sitios poco fiables, o que nos ha pasado alguien y ya vienen infectados, o en algún archivo adjunto a un correo, etc...

Cuando ejecutemos el programa infectado, el virus se instalará en memoria RAM (es importante tener en cuenta que para que el virus comience a funcionar y a extenderse, debe haber alguien que ejecute ese código). Una vez en la RAM el virus infectará otros archivos ejecutables y los grabará en disco, de forma que aún después de apagar el ordenador, cuando algunos de estos programas se ejecute, se repetirá la acción.

Curiosidad

VIERNES 13

Imagen en Pixabay de J_lloabajo licenciaCC0 Public Domain

Hace ya más de 30 años que este virus hizo estragos.

Recibe también el nombre de **Jerusalem** porque fue descubierto y aislado por una Universidad de esta ciudad en 1.987.

El virus se transmitía principalmente por diskettes infectados (que eran el soporte más utilizado en aquella época) y se instalaba en RAM afectando a los ficheros tipo .exe, .sys y .com. Los ficheros infectados aumentaban su peso en 2k, y como el virus no podía detectar que ficheros ya estaban infectados, entraba en un bucle, que hacía que los ficheros subieran de peso llenando las memorias RAM y discos duros de la época (las RAM no pasaban de 649 KB y los discos duros de 20 o 30 MB). Fue precisamente este "fallo" el que permitió su detección.

El virus tenía como objetivo la destrucción masiva de ficheros todos los viernes 13.

En España este virus destruyo a una de las revistas informática pioneras, Amstrad Users, que difundió junto con la revista un diskette con utilidades shareware infectado con el virus.

Imagen en Pixabay de DirtyOpibajo licenciaCC0 Public Domain

Los gusanos o worms se diferencian de los virus en su forma de propagarse. Este malware no necesita de la ejecución del programa infectado para su propagación, pues puede autopropagarse sin necesidad de infectar otros archivos.

Sus efectos también suelen ser distintos a los de los virus, mientras que los virus pretenden alterar o destruir archivos los gusanos van encaminados a consumir recursos causando generalmente problemas de saturación en la red.

Las vías más comunes de propagación son:

- A través de correo (SMTP), bien en el mismo mensaje, bien en algún adjunto. Estos mensajes suelen tener un asunto interesante para que el usuario lo abra.
- A través de redes P2P (peer to peer) de compartición de archivos (descargamos archivos de múltiples clientes y a la vez compartimos algunos nuestros). En este caso los ficheros suelen tener el nombre de alguna película de estreno o de vídeos cómicos o incluso porno.
- A través de programas de chat (IRC).
- A través de carpetas compartidas en red.

Curiosidad

LAS CENTRIFUGADORAS SE VOLVIERON LOCAS EN LA CENTRAL NUCLEAR DE NATANZ

Ocurrió en enero del 2010, los inspectores de la Agencia Internacional de Energía Atómica visitaban la central nuclear de Natanz en Irán cuando vieron como las máquinas centrifugadoras usadas para enriquecer el uranio comenzaban a fallar, aumentaban su velocidad de giro bruscamente para luego volver a la velocidad normal. El comportamiento se repitió durante varias ocasiones, ocasionando que 1000 máquinas se autodestruyeran (como consecuencia de los cambios bruscos de velocidad).

El motivo de esto fue el gusano Stuxnet, el primero que destacó por no atacar a los PCs directamente infectados, sino a los sistemas PLC, a los que reprogramaban para alterar el funcionamiento de las centrifugadoras.

El gusano entró en la planta a través de una memoria USB conectada a alguno de los equipos, y desde este se propagó a través de impresoras compartidas y aprovechando vulnerabilidades en el sistema Microsoft Windows (solo atacaba a equipos con este sistema operativo).

Como solución Microsoft desarrolló parches de seguridad que impedían el ataque del gusano y su propagación y se prohibió el uso de memorias externas en plantas de este tipo, pues son una posible fuente de infección.

1.3. Troyanos

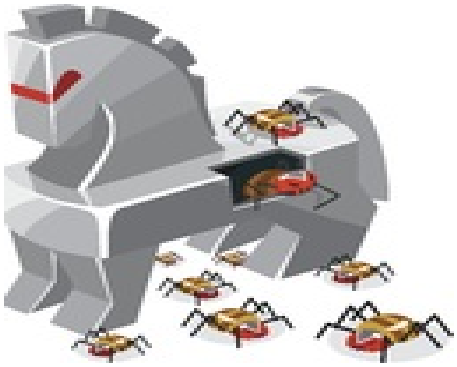

Imagen en WikimediaCommons de Starkus01 bajo licencia Creative Commons Attribution-Share Alike 4.0 International

Los troyanos, toman su nombre del famoso caballo de Troya:

> El caballo de Troya fue un artilugio con forma de enorme caballo de madera que se menciona en la historia de la guerra de Troya y que según este relato fue usado por los griegos como una estrategia para introducirse en la ciudad fortificada de Troya.

Al igual que hicieron los griegos para entrar en la ciudad de Troya ocultos en el caballo de madera, los troyanos son un tipo de malware que se introduce en el equipo camuflado en un programa aparentemente inofensivo.

De hecho al ejecutar el programa en cuestión, este parecerá funcionar correctamente, sin embargo en segundo plano, y sin que nos percatemos de ello, se instalará el troyano, cuya misión no es la de infectar ficheros como los virus para propagarse, ni hacerlo de forma autónoma como los gusanos, sino la de realizar distintas acciones y configuraciones con el fin de facilitar el control externo de nuestro equipo sin nuestra autorización.

El troyano tendrá dos partes, un cliente que es el que se instala en el equipo atacante y un servidor que es el instalado en el equipo atacado, que será el que reciba las ordenes del cliente y realice las operaciones oportunas en el equipo en el que se aloja.

Algunos troyanos son:

Proxy	El equipo atacante usará al infectado como proxy, enmascarando su identidad con la del atacado. De forma que en cualquier operación que realice aparecerá como origen el equipo infectado.
Backdoor o puerta trasera	Este tipo de malware permite que se realicen conexiones a la computadora infectada saltándose todos los mecanismos habituales de autenticación.
Keylogger	Este malware captura las pulsaciones del teclado, obteniendo así claves de acceso. Algunas entidades bancarias, para evitar esto, usan un mecanismo por el que la clave de acceso a su web se introduce a través de una pantalla emergente haciendo click en letras y/o números que aparecen en dicha pantalla y que además varían su orden cada vez que accedemos para evitar la captura de patrones.
Drive-by downloads	Son programas cuya misión es la de instalar otros programas que capturen información de nuestro equipo. Generalmente son scripts maliciosos incluidos en alguna págian web que se descargan aprovechando alguna debilidad en esta.

1.4. Grayware

Engloba a aquellos programas malignos que sin llegara ser dañinos, son bastante molestos o indeseados.

Algunos de sus efectos son:

- Pérdida de privacidad del usuario.
- Reducen el rendimiento del equipo.
- Dificultan el trabajo del usuario.
- Consume de ancho de banda.

Algunos tipos de Grayware son:

Spyware	O software espía (spy), trata de obtener información de la máquina en la que se aloja, a veces es información de uso y estadísticas, pero otras puede ser información más comprometida en cuyo caso dejaría de ser grayware y pasaría a ser malware. Se instala y opera sin que el usuario lo advierta, muchas veces al aceptar las condiciones de algún programa que nos hemos bajado e instalado.
Adware	El término proviene de "ad" (abreviatura de advertisement o anuncio) y software, se trata de software que muestra publicidad de forma intrusiva, generalmente a través de ventanas emergentes o popups. Existen desarrolladores de software gratuito que incluye adware, de forma que deberemos pagar por la versión del programa sin publicidad. Este tipo de malware viene muchas veces acompañado de algún programa tipo espía, de manera que a la vez que se emite publicidad se monitoriza la actividad del usuario.
Hijacking	La palabra hijacking significa secuestro. Este tipo de programas secuestran nuestro navegador, modifican: cambian la página de inicio por otra con publicidad, modifican el motro de búsqueda por otro, modifican los favoritos o marcadores, etc. Su finalidad suele ser el obligarnos a visitar páginas con publicidad.
Bromas o jokes	En este caso el desarrollador del software no busca hacer daño en la máquina instalada, pretende gastar una broma, muchas veces muy pesada. Hay programas que avisan del inminente formateo del disco dura (cosa que luego no ocurre), o rotan la pantalla, o modifican el teclado, etc

1.6. Ransomware

Imagen en Flickr de Pictures of Money bajo licencia Algunos derechos reservados

Su nombre proviene de ransom (rescate) y software.

Este malware "secuestra" archivos y pide un rescate por liberarlos.

Lo que hace es encriptar archivos (también de le conoce como criptovirus) y no facilita la clave para su desencriptación hasta que se paga una determinada cantidad de dinero.

Recomendaciones

Para evitar pérdidas asociadas a este tipo de ataque se recomienda:

- Tener instaladas herramientas de detección de malware, si la amenaza se detecta de forma temprana es posible eliminarla antes de que actúe sobre archivos (encriptándolos) o bloquee el acceso a partes del sistema.
- Tener copias de seguridad de los ficheros importantes en algún tipo de almacenamiento externo.

Curiosidad

Uno de los malware más famosos de tipo ransomware es Cryptolocker, que se distribuye entre otras formas, a través de un adjunto de correo, de forma que al activarlo encripta ficheros almacenados en disco o unidades de red, usando criptografía de clave pública RSA en máquinas con S.O. Windows.
El creador de este malware fue un ruso de 31 años por el cuál el FBI ofrecía una recompensa de tres millones de dólares a quién pudiera informar de su paradero.

1.7. Rootkits

Los rootkits son programas cuya finalidad es ocultar la ejecución de otro, generalmente malware.

Por ejemplo, podría ocultar los puertos por los que se realiza la conexión usando algún backdoor, o no mostrar los procesos reales en ejecución (si no información falsa, ocultando los procesos correspondientes al malware que está protegiendo), o no mostrando sus propios archivos, etc.

Su nombre se debe a que inicialmente eran programas para atacar sistemas Unix, a los que accedían una vez que tenían la clave de root, hoy en día su significado otro, utilizándose para programas que ocultan rutinas maliciosas.

Este tipo de malware es más difícil de detectar, y un simple antivirus no los detectaría. Las herramienta antirrotkit deberán ir analizando todos los procesos que corren en el equipo, hasta encontrar condiciones sospechosas.

2. Correo no deseado y spam

Imagen en Wikimedia Commons de Luis xavi 1630 bajo licencia Creative Commons Attribution-Share Alike 4.0 International

El correo electrónico también puede ser una vía de acceso para posibles amenazas o usos malintencionados.

Muchos de los correos que recibimos son no deseados y no solicitados. A veces son portadores de algún software malicioso adjunto al correo, o provienen de destinatarios desconocidos o anónimos, o la dirección de correo del remitente es falsa, o es una dirección muy parecida a la de algún organismo o persona a la que se quiere suplantar,etc.

A veces tienen como objetivo el hacerse con direcciones válidas de correo, con bromas o un correo en el que se dice que si no se reenvía a cierto número de personas algo malo sucederá, de forma que con cada reenvío van sumándose nuevas direcciones (de tus amigos o contactos), de forma que cuando el mensaje vuelva al remitente tendrá todas esas direcciones. Para evitar esto se recomienda, en primer lugar, no reenviar este tipo de mensajes, y en segundo, en caso de hacerlo, eliminar las cuentas que aparezcan en el mensaje reenviado y las que añadamos ponerlas como CCO (copia oculta) para que no sean visibles (ninguno de los receptores verá la dirección de correo de los demás).

Otas veces el correo puede incluir algún mensaje indicando que pulses en algún enlace para darte de baja de la lista de distribución. El objetivo de estos correos es obtener cuantas de correo "vivas", y al responder, confirmas que la tuya está activa.

La mayoría de las veces la finalidad de estos correos no deseados es la de publicidad, y suelen enviarse de forma masiva, este tipo de correos recibe el nombre de **spam**.

Casi todos los servicios de correo incluyen filtros antispam. Puede ocurrir a veces que un correo que no es spam, sea clasificado como tal y movido a la carpeta de correo no deseado, por lo que debes revisarla de vez en cuando.

Para saber más

Imagen en Wikimedia Commons de Qwertyxp2000 bajo licencia CC BY-SA 4.0

El término spam proviene de la Segunda Guerra Mundial. Las familias de los soldados americanos enviaban a estos comida enlatada, entre la que destacaba una carne en lata, muy famosa en Estados Unidos cuya marca es spam.

3. Suplantación de identidad

Con el uso del correo, redes sociales y las compras o gestiones bancarias online, cada vez aparecen nuevas formas de suplantación de identidad.

Entendemos por suplantación de identidad, el uso de técnicas de ingeniería informática haciéndose pasar por alguna persona o entidad de confianza, para obtener datos privados de la víctima y usarlos de forma fraudulenta

Para saber más

Recuerda que puedes informar o denunciar cualquier delito informático a través de la página del Grupo de Delitos Telemáticos de la Guardia Civil

Imagen en Flickrccde Betacontinua bajo licencia
Algunos derechos reservados

Toma su nombre del inglés phising (pesca), pues se trata de técnicas para conseguir que la víctima "muerda el anzuelo".

Podría llegarnos un correo o mensaje al móvil de nuestro banco informándonos de que se han detectado problemas de seguridad, o de que necesitan verificar nuestros datos o número de cuenta o tarjeta por mantenimiento de la base de datos de clientes, o cualquier otro motivo, y para ello se nos facilita un enlace. Al hacer click en este enlace nos aparecerá una página, falsa, con el mismo aspecto que la de nuestro banco real. Es complicado darse cuenta de que no es la página verdadera puesto que la interfaz es la misma, tan solo si observamos la url o dirección de la página veremos que aunque muy similar, no es exactamente la de nuestro banco. Pero si no nos percatamos de esto al introducir nuestros datos, el atacante los tendrá en su poder y habremos caído en el engaño.

Puesto que la página es falsa, una vez tengan los datos que buscaban, nos saltará alguna página informándonos de algún error en el servidor o en la conexión, para evitar levantar sospechas.

Recomendaciones

- Sospechar siempre de correos o mensajes en que se nos soliciten datos. Las entidades implicadas deberían tenerlos y en caso de necesitar alguna verificación no sería por este medio.
- Nunca pulsar en un enlace que se nos facilite en correos o mensajes, hacerlo siempre desde la web oficial.
- Verificar la URL antes de introducir datos.
- Sospechar de URL con el carácter @ pues lo que hace es dirigirnos de una página a otra.
- Verificar que la conexión es segura (precedida de https).
- Sospechar de mensajes cuyo remitente no provenga del correo oficial de la entidad.
- Utilizar filtros antispam en el correo.

Curiosidad

Algunos ejemplos de fishing son:

ATAQUE DE PHISHING CONTRA LA DIRECCIÓN GENERAL DE TRÁFICO (2.011)

DGT Dirección General de Tráfico

Imagen en Wikimediacommons de Dirección General de Tráfico bajo licencia Creative Commons

Mediante este ataque se enviaba a los usuarios un correo spam, desde una dirección de hotmail (que ya es bastante sospechoso), en el que, con una apariencia totalmente seria y haciendo uso de logos y estilo característicos de la D.G.T. , se nos informaba de la notificación de una sanción.

En el correo se indicaba, si se deseaba más información, la url (real) de la oficina virtual de la Dirección General de Tráfico, con la finalidad de ganar la confianza de la posible víctima y no levantar sospechas-

El correo llevaba dos adjuntos, unos un pdf con la supuesta notificación y otro un word que se debía rellenar con nuestros datos personales (nombre, apellidos, dirección, teléfono, DNI, etc.) para presentar la alegación.

Una vez enviado el mensaje con los datos, se nos enviaba un acuse de recibo, notificando la recepción de los datos (desde un correo aparentemente de la Dirección General de Tráfico, pero que no es el real).

ATAQUE DE PHISHING CONTRA CORREOS (2.016)

En este caso, se recibe un email, aparentemente de Correos España, en el que se indica al usuario que ha recibido una carta y que debe personarse en la oficina de Correos más cercana para proceder a su recogida.

Se proporciona un código CAPTCHA para darse seguridad y ganarse la confianza del receptor, y a la vez se le coacciona indicando que si no recoge la carta en los próximos 30 días, se le cobrarán 8,15 euros por cada día adicional que la carta permanezca allí.

Para recoger la carta hay que rellenar un pdf que se adjunta y entregarlo en la oficina a la que vayamos.

El pdf en cuestión es en realidad un ejecutable, aunque para evitar sospechas lleva el icono de un archivo pdf. Si hacemos click en él, se ejecutará infectando nuestro equipo con Malware.

Si hemos llegado a este punto, se recomienda pasar alguna herramienta antimalware y cambiar las contraseñas (desde otro equipo) de nuestro servicios web.

Imagen en Wikimediacommons deGregbowden bajo licencia GNU Free Documentation License

ATAQUE DE PHISHING CONTRA WHATSAPP (2.016)

Imagen enPixabay de arivera
bajo licencia CC0 Public Domain

Este Malware ataca a dispositivos móviles con Android.

Comienza con la recepción de un SMS de alguna entidad aparentemente fiable como Whatsapp, Mercadona, Zara, etc en el que se nos indica que uno de nuestros mensajes no ha podido ser enviado o que uno de nuestros pedidos tiene algún problema, etc.. y se nos facilita una url para consultar el estado del envío. Al hacer click automáticamente se nos instala del malware, que lo que hace es suplantar a la aplicación Whatsapp (también puede afectar a otras como Uber o Google Play (Play Store).

Cuando abramos Whtasapp, en realidad estaremos ejecutando el malware, con una apariencia tan conseguida que no nos daremos cuenta de que no es la aplicación real.

No sabremos que realmente no hablamos con uno de nuestros contactos y se nos intentará sacar datos personales que permitan el robo de dinero.

En caso de que tu smarthone esté infectado por algún tipo de malware se recomienda ir a las aplicaciones y desinstalar aquellas sospechosas, además de pasar un buen antivirus.

3.2. Pharming

El pharming es otra técnica que al igual que la anterior, nos lleva a páginas web falsas, con apariencia idéntica a las verdaderas.

Es más difícil de detectar porque trabajan modificando DNS, de forma que cuando tecleemos la URL de nuestro banco, en lugar de traducir esa direccción a la IP de la web de la entidad, lo hará a la IP de la web falsa.

Recuerda:

DNS es el sistema que traduce una url o nombre de internet en la dirección IP de una máquina.

Una máquina, para conseguir esta traducción mirara primero en su fichero local **HOSTS,** en caso de no encontrarla, recurrirá a su **DNS primario**, y si no obtiene respuesta de este, recurrirá a su **DNS secundario.**

Para conseguir su propósito se pueden usar diferentes técnicas:

- Atacar directamente a los servidores DNS.
- Hacer uso de algún malware que modifique el fichero hosts para introducir las conversiones falsas.

Recomendaciones:

- Hacer uso de herramientas antimalware.
- Tener actualizados los navegadores.

4. Denegación de servicio

Esta técnica conocida como denegación de servicio o DoS (Denial of Service), tiene por objetivo el impedir el correcto funcionamiento de servidores con presencia en Internet con el fin de dañar la reputación de las empresas que ofrecen esos servicios.

No se pretende capturar, borrar ni modificar datos, sino el saturar a los servidores para que no puedan consultarse ni utilizarse.

Para esto aprovechan vulnerabilidades en el protocolo IP y en los propios sistemas, enviado paquetes IP en formatos, tamaño o frecuencia que saturen el ancho de banda de la conexión o al propio servidor, que se ve incapaz de responder.

Después de conocer algunas de las múltiples amenazas que nos encontramos en la red, podríamos pensar que estamos totalmente desprotegidos, pero no es así, existen multitud de herramientas, que junto con algunas de las buenas prácticas que hemos ido viendo, protegerán a nuestro equipo. Aunque, desgraciadamente, ninguna herramienta protege al 100%, puesto que los desarrolladores de malware están constantemente evolucionando.

Algunas de estas herramientas antimalware son:

- **Antivirus:** que nos permitirán detectar, eliminar y prevenir virus informáticos. Es importante que la base de datos de virus que usa se actualice frecuentemente.
- **Antspyware:** eliminan y previenen frente a software espía.
- **Antirootkit:** estas herramientas van dirigidas a localizar rootkits, que como ya vimos es un tipo de malware que un antivirus no detectaría.
- **Filtros antispam**: analizan los correos de la bandeja de entrada para localizar publicidad no deseada y correos masivos o sospechosos, que mueven a otra carpeta para su posterior chequeo y borrado por parte del usuario.
- **Antiphising**: van más allá de los filtros antispam, analizan los correos para detectar links fraudulentos o dominios falsos.
- **Filtros de contenido:** permiten o deniegan el acceso a páginas en función de su contenido, según reglas previamente establecidas.
- **Control parental:** con el fin de proteger al menor, es posible instalar filtros que permitan o denieguen el acceso a determinadas páginas o utilidades, según la url, según contenido, etc. Que bloqueen el acceso a redes sociales o registren su actividad o que limiten el tiempo y horarios de uso.
- **Firewall**: O cortafuegos, nos permite limitar el acceso desde internet a una parte de la red o a nuestro equipo, estableciendo ciertas reglas de filtrado, por paquetes o aplicaciones.
- **Suites de seguridad:** agrupan todas o varias de las herramientas anteriores con el fin de proteger al equipo.
- **Actualizaciones de los navegadores y sistema operativo:** es recomendable tener siempre actualizados tanto el S.O. como los navegadores que usemos, pues muchas veces estas actualizaciones resuelven problemas detectados en la seguridad del software.
- **Copias de seguridad**: copias de los ficheros y datos más importantes en algún soporte externo, de forma que permanezcan intactos tras cualquier ataque a la máquina original que provoque la destrucción, encriptación o modificación no deseada de estos.

Otras precauciones:

- Desconfiar siempre de correos desconocidos.
- No hacer click en URL sospechosas que se nos adjunten en mensajes o correos.
- No abrir ficheros ejecutables que nos lleguen por correo.
- Jamás dar nuestros datos personales a ninguna "supuesta" entidad. La entidad real (banco, policia, etc.) jamás nos pedirá nuestros datos y menos por esas vías.
- Al entrar en páginas de compras, bancos, etc. verificar que la conexión es segura (https://...)
- No descargar software de páginas no confiables.
- Si vas a instalar un software descargado, lee atentamente todas las pantallas (evita hacer click en siguiente, siguiente). En este tipo de instalaciones suele venir marcada por defecto (hay que desmarcar o elegir instalación personalizada en lugar de típica) la instalación de software adicional, generalmente con fines publicitarios.

MALWARE EN SISTEMAS GNU/LINUX

Hemos oído muchas veces que los sistemas GNU/Linux están libres de virus. ¿Es esto cierto?.

La respuesta en NO, puesto que existe malware para estos sistemas, ahora bien, la protección de estos sistemas frente a ataques es muchísimo mayor que la de un sistema Windows y el software malicioso desarrollado mucho menor. Veamos todo esto con un poco más de detalle.

- Los sistemas GNU/Linux son sistemas multiusuario, y con un fuerte sistema de permisos. Un software malicioso alojado en un fichero no tendrá posibilidad de ejecutarse si el usuario en cuestión no tiene permisos de ejecución sobre ese fichero. En caso de que si los tuviera, podría dañar datos de ese usuario, siempre dependiendo de los permisos, pero no el sistema, salvo si el usuario en cuestión fuera el superusuario o root.

- Debido a que son sistemas menos extendidos, el interés de los programadores de software malicioso a la hora de desarrollar código es menor. Además se encuentran con problemas adicionales como que unos sistemas son diferentes de otros (distinto núcleo, aplicaciones instaladas diferentes, características de seguridad específicas, etc.) lo que dificulta el desarrollo del software.

- Como se trata de software abierto las actualizaciones para solventar vulnerabilidades en el sistema (que pudieran ser aprovechadas para posibles ataques) son relativamente rápidas y eficientes.

- Además, cuenta con un repositorio de software que es verificado por administradores con el fin de verificar que las aplicaciones estén libres de malware.

- Aún así, existen herramientas antimalware para Linux.

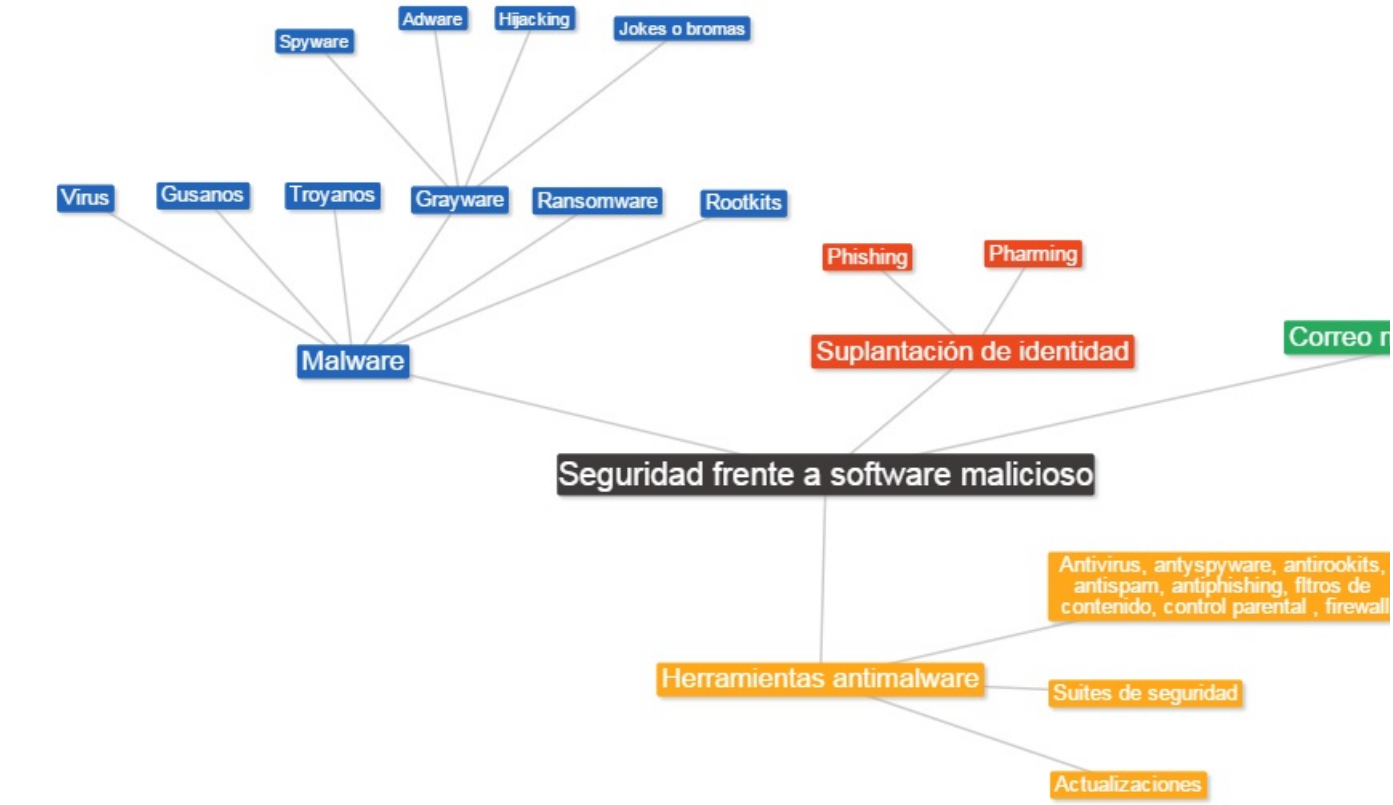

Imagen de creación propia bajo licencia CC

Not Found

The requested URL /adistancia/Aviso_Legal_Andalucia_v04.htm was not found on this server.

Descargar PDF