PRINCIPALES AMENAZAS DE LA SEGURIDAD INFORMATICA

Virus informáticos:

Son las amenazas más conocidas por el público no especializado en temas de informática. Se trata, básicamente, de código con el que se infecta un programa ejecutable y que se propaga copiándose a sí mismo e infectando a otros programas o archivos.

Sus consecuencias y su gravedad varían mucho. Algunos virus solo tienen como finalidad gastar una broma al usuario; otros pueden provocar el mal funcionamiento del software, dañar el hardware o incluso infectar a toda una red de usuarios.

Los virus siempre necesitan de la acción humana para activarse (por ejemplo, ejecutando el usuario software infectado por desconocimiento).

Las pérdidas económicas si llega a dañar el software de la empresa, el sistema operativo o los propios equipos y dispositivos pueden ser muy cuantiosas.

Mantén tu antivirus actualizado, no te puedes imaginar la cantidad de tiempo perdido y el dinero que pierden las empresas teniendo a sus empleados de brazos cruzados por no haber invertido un poco de tiempo y dinero en actualizar su antivirus.

Gusanos:

¿Qué nombre les ponen verdad? pero es que se comportan así y te aseguro que no se convierten en mariposas.A menudo se confunden con los virus. Sin embargo, los gusanos, a diferencia de ellos, no necesitan de la acción humana para activarse, copiarse a sí mismos y propagarse por la red. ¡Porque eso es lo que hacen!

Pueden, por ejemplo, copiarse y enviarse a cada uno de tus contactos mediante tu servicio de correo electrónico o mensajería instantánea, y repetir la operación con la libreta de direcciones de cada uno de tus contactos. Su capacidad de propagación crece de forma exponencial.

Los gusanos suelen colapsar los ordenadores, los servidores y la red, acaparando recursos, consumiendo ancho de banda y provocando serios problemas de rendimiento.

Pero también se pueden utilizar con fines todavía más oscuros, como el de crear grandes redes de ordenadores zombie, controlados por bots que los pueden usar para enviar spam de forma masiva, lanzar ciberataques o descargar todo tipo de malware en el equipo.

¿Imaginas cuánto daño pueden hacer los gusanos en tus equipos informáticos y tu red de trabajo…?

Troyanos:

¿Recuerdas el Caballo de Troya en el que se ocultaron los griegos para entrar en la ciudad de los troyanos y derrotarlos? Pues el malware conocido como troyano hace lo mismo, ¡pero en tu ordenador!

Un Caballo de Troya o troyano informático habitualmente entra en tu equipo o tu dispositivo aprovechando la descarga de software legítimo. (Ojo a la descarga de programas, te recomiendo que lo descargues siempre desde el dominio oficial y cuidado con la palabra gratis en este contexto, casi siempre lleva algo escondido).

De ahí su nombre, porque el Caballo de Troya era supuestamente un inofensivo regalo de los griegos a los troyanos por su valor en la batalla.

¿Su objetivo? Abrir una puerta trasera a los hackers para que puedan controlar tu equipo y su software.

A diferencia de virus y gusanos, el troyano no provoca daños ni se propaga. Por eso pasa inadvertido, algo importante para cumplir su función.

Adware:

Otro campeón de popularidad entre los usuarios. Y es que los efectos de un adware no pasan inadvertidos. ¿Quién no ha sufrido las molestias de navegar por Internet envuelto en un mar de anuncios spam y ventanas emergentes que se abren en el navegador de forma descontrolada?

El adware es un tipo de software aparentemente inofensivo si se compara con alguno de los anteriores tipos de malware, pero que puede bajar drásticamente el rendimiento de los trabajadores que necesitan navegar por Internet para realizar sus tareas.

A veces el adware incluye un “antivirus” o cualquier otra opción de registro mediante pago que elimina el problema. Se trata de un engaño perpetrado por los mismos autores del adware a erradicar.

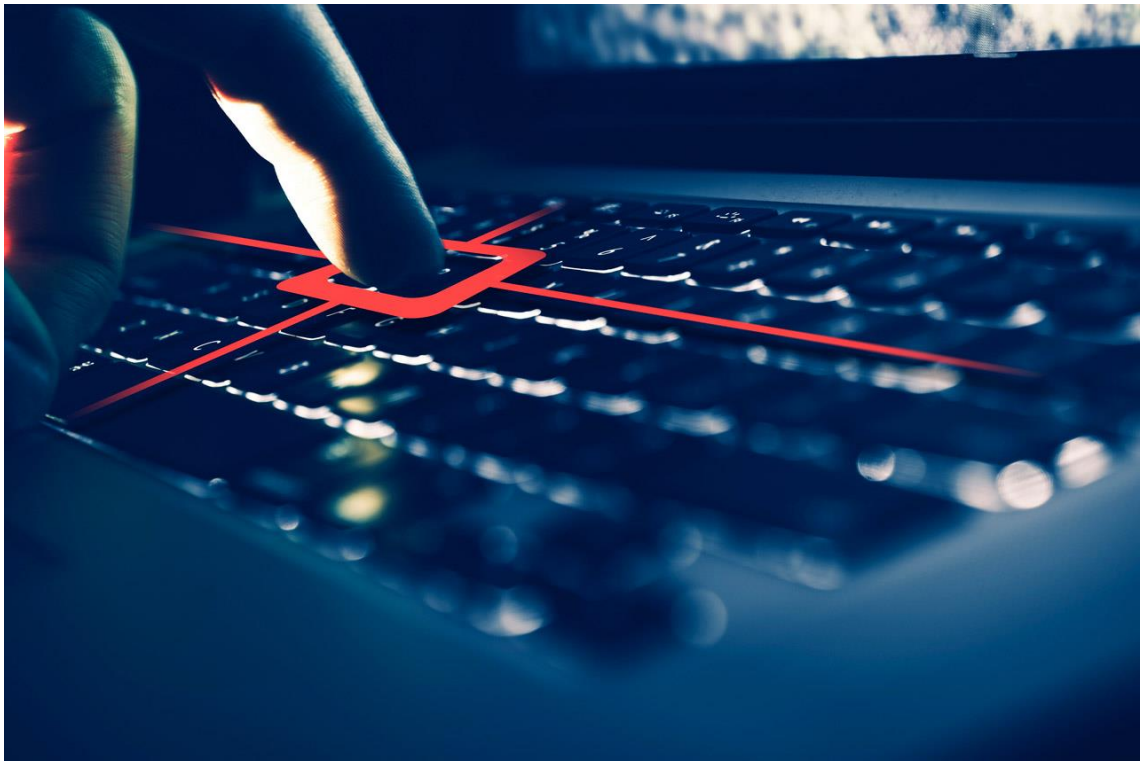
Hace tiempo localicé un limpiador para este software que utilizamos desde hace tiempo y este si es gratuito, eso sí te recomiendo que lo hagas con un técnico especializado,alguna vez que otra borra algún servicio si tocas o activas alguna opción que no debes activar.Se llama adwcleaner.

Rootkit:

Es un software que permite a los ciber intrusos acceder a equipos sin ser detectados para robar información sensible.Los rootkits permiten acceso privilegiado a un usuario (el hacker) ,que se conecta de forma remota, alterando el sistema operativo para ocultar la maniobra.

Un auténtico riesgo para empresas y usuarios, que pueden ver sustraídas sus claves de acceso, datos bancarios, etc.

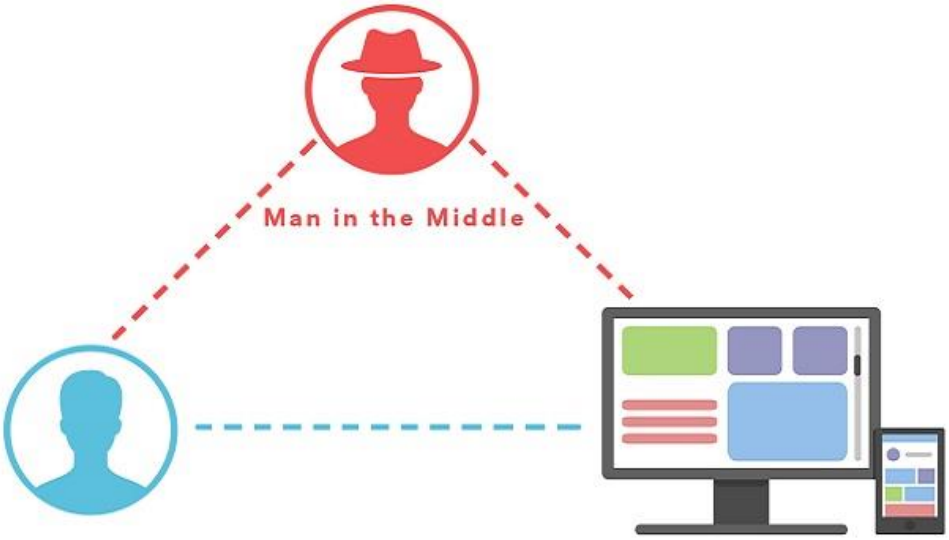
Keylogger:



Aunque también existen versiones que funcionan a través de dispositivos o complementos para hardware, hablamos básicamente de programas que pueden llegar a un equipo a través de virus, troyanos, etc., y que se dedican a memorizar las pulsaciones de teclado que realiza el usuario. La información queda registrada en un archivo y puede ser enviada a través de Internet.

Como puedes imaginar, los ciberdelincuentes pueden hacerse con todo tipo de contraseñas, datos bancarios y cualquier otro tipo de información privada.

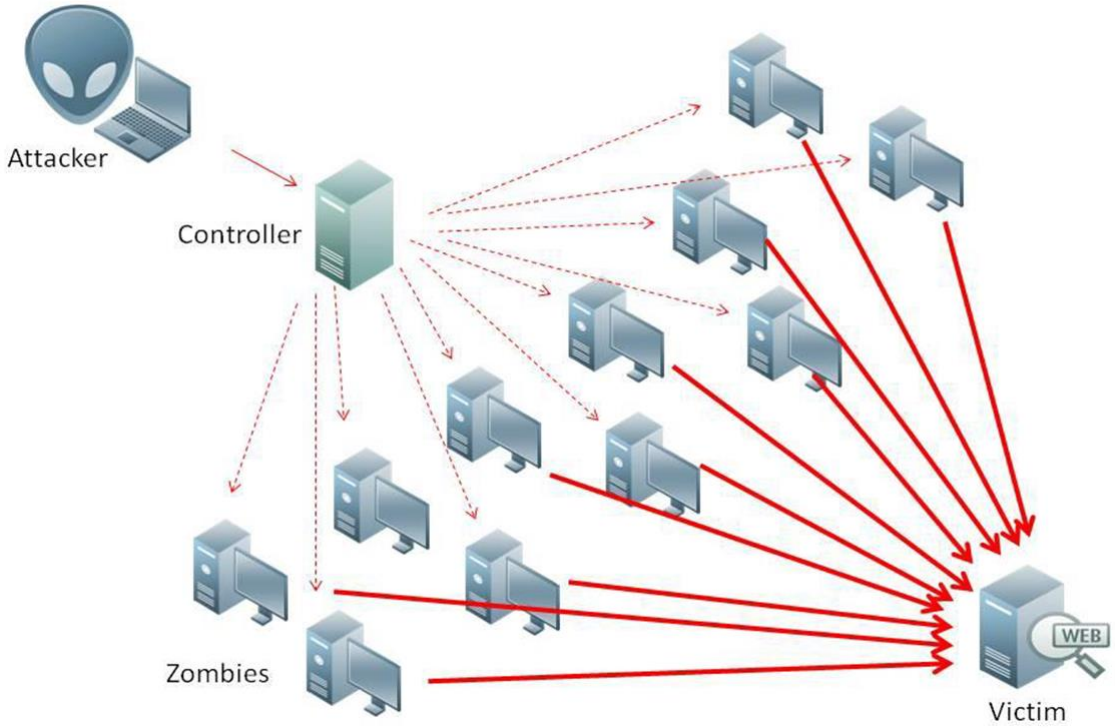
Ataque Man In The Middle (MITM):



Es un tipo de ataque en que el hacker intercepta tráfico que viaja de un equipo emisor a otro receptor. Por eso se llama Man in the middle, que en español significa “Hombre en el medio”.

Al convertirse en un punto intermedio por donde pasa la información desde su lugar de origen (el equipo de un empleado, por ejemplo), a un emplazamiento de destino (supongamos que es el servidor de la compañía), el ciberdelincuente puede descifrar los datos y hacerse con claves y contraseñas.

Ataques DOS:

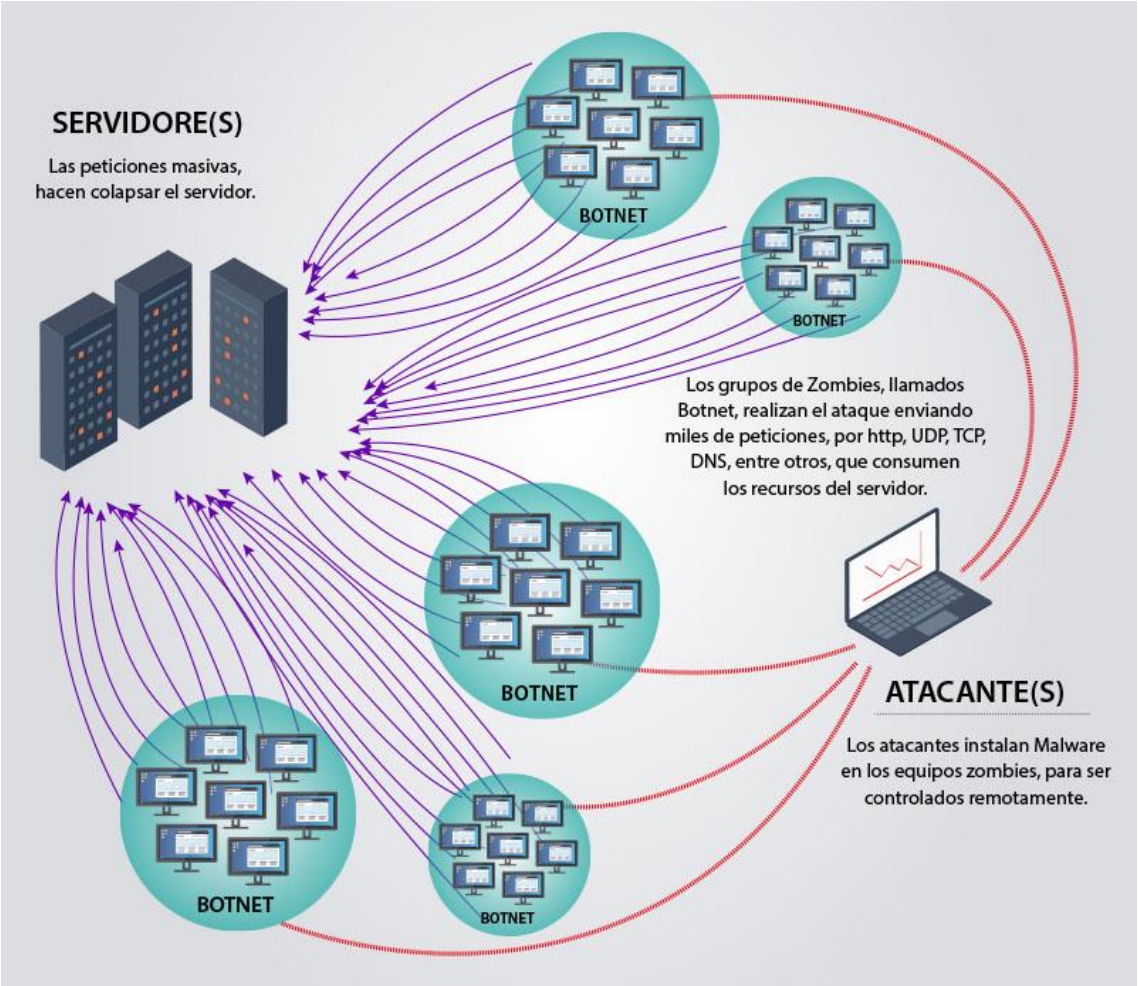


Tener la página web de empresa caída durante algún tiempo puede suponer importantes pérdidas económicas, ¡sobre todo si se trata de una tienda online!

Ese es el objetivo de los ataques de Denial Of Service (DOS), o de “denegación de servicio”. Un ordenador lanza peticiones al servidor en el que se aloja el sitio web hasta que lo satura y empieza a denegar el acceso. La web cae con sus correspondientes pérdidas en ventas, oportunidades de negocio, etc.

Para detener el ataque basta con banear la IP del atacante. Pero si el tiempo en que permanece la web caída es el suficiente, las pérdidas ya han tenido lugar y el daño está hecho.

Ataques DDOS:



El concepto es el mismo que en la amenaza anterior: se realizan peticiones masivas hasta saturar el servidor y hacer caer la web.Sin embargo, el ataque del que hablamos ahora es un Distributed Denial Of Service (DDOS), y es más sofisticado que el anterior.

En lugar de lanzar los ataques desde un único equipo, los ataques DDOS emplean muchos ordenadores para distribuir las peticiones al servidor. A menudo, esos equipos pertenecen a usuarios que no saben para qué se están utilizando sus ordenadores, que han sido añadidos a una red zombie por los hackers infectándolos con malware.

El problema con este tipo de ataques es que al tener un origen múltiple es más difícil averiguar todas las IP de las que parten y, por lo tanto, es más difícil de detener.

Sale Systems. (s. f.). Principales amenazas de la seguridad informatica. Recuperado 8 de abril de 2020, de https://salesystems.es/10-amenazas-la-seguridad-informatica-debes-evitar/