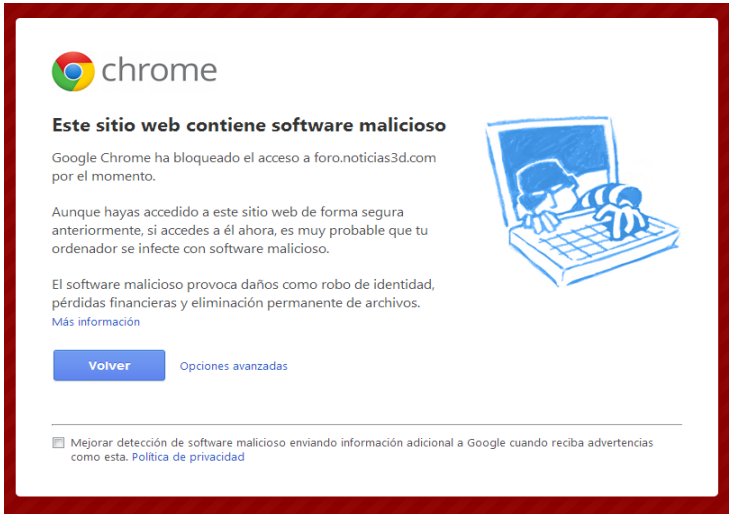
Software Malicioso o Malware

Grupo_16

Septiembre 2017

Software Malicioso

El software malicioso, también conocido como programa malicioso o malware, contiene virus, spyware y otros programas indeseados que se instalan en su computadora, teléfono o aparato móvil sin su consentimiento.



Estos programas pueden colapsar el funcionamiento de su aparato y se pueden utilizar para monitorear y controlar su actividad en internet. Además, con estos programas su computadora puede quedar expuesta al ataque de virus y enviar anuncios indeseados o inapropiados.

Generalmente, el malware se propaga a través de dos vulnerabilidades:

– Vulnerabilidades del software: se trata de explotar debilidades del sistema operativo o de algún programa. Algunos tipos de malware se copian a sí mismos y se envían automáticamente a través de la red para infectar la mayor cantidad de equipos.

- Vulnerabilidades asociadas a las personas: : En la mayoría de los casos, son los mismos usuarios que por su desconocimiento y confianza ayudan a su propagación.

¿Qué son los virus?

Los virus son programas maliciosos creados para manipular el normal funcionamiento de los sistemas, sin el conocimiento ni consentimiento de los usuarios .

Los programas maliciosos pueden alterar tanto el funcionamiento del equipo como la información que contienen o se maneja en ella.

Las acciones que realizan estos pueden ser: robo de información sensible o el borrado de datos hasta el uso del equipo como plataforma para cometer otro tipo de actividades ilegales.

Clasificación del Malware

Los distintos códigos maliciosos que existen pueden clasificarse en función de diferentes criterios, los más comunes son:

- Por su capacidad de propagación.

- Por las acciones que realizan en el equipo infectado.

Cabe mencionar que muchas de las acciones que realizan los códigos maliciosos, en algunas circunstancias se pueden considerar legítimas, por lo tanto, sólo se considera que un programa es malicioso cuando actúa sin el conocimiento ni consentimiento del usuario.

Según su capacidad de propagación:

- Virus

Los podríamos considerar los padres de todos los malware. Se trata de un tipo de programa que se instala en tu ordenador sin tu autorización y que altera su funcionamiento. Para defenderte de este malware debes instalar un antivirus.

- Gusanos

Un gusano (o worm) es un tipo de virus particular. Concretamente, son programas capaces de propagarse de un PC a otro a través de redes informáticas y ejecutar ciertas acciones que pueden afectar la integridad del sistema operativo.

- Troyanos

Como su nombre indica, hacen uso del engaño para llegar hasta nosotros sin delatarse. Parece inofensivo pero dentro puede contener la caja de Pandora. Un programa de este tipo puede manipular nuestros archivos, borrarlos e incluso pasar el control del ordenador a un tercero, para pesadilla nuestra. A diferencia de los virus no se propaga de un ordenador a otro.

Según las acciones que realizan en el equipo infectado; algunos de ellos son:

- Adware. Adversting Software, que es la publicidad no solicitada, por lo regular se presenta en forma de pop-ups que presentan algún tipo de publicidad.

- Spyware. Conocidos comúnmente como espías, son programas cuyo objetivo es recolectar información personal tuya sin que lo sepas y enviarla a su creador..

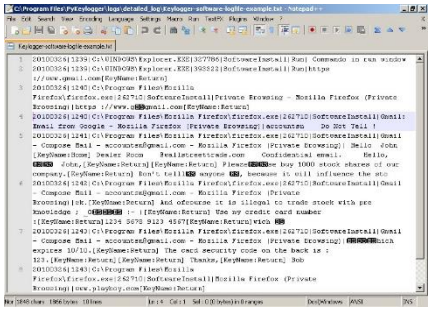
- Hijacking. Cambian la configuración del navegador, por ejemplo, modificando la página de inicio por una página web, que contendrá anuncios o publicidad.

- Jokes o bromas. Aparentemente son inofensivos, pero sólo aparentemente. Son los jokes o bromas informáticas. Se trata de pequeños programas que, en muchos casos, simulan que el ordenador está siendo atacado por un virus.

- Bulo o Hoax (broma o engaño). son mensajes con falsas advertencias de virus, o de cualquier otro tipo de alerta o de cadena (incluso solidaria, o que involucra a nuestra propia salud), o de algún tipo de denuncia, distribuida por correo electrónico.

- Ransomware. Este tipo de malware cifra archivos importantes del disco duro para exigir el pago de dinero a cambio de la contraseña para descifrarlos.

- Rogueware. Es una aplicación que intenta semejarse a otra, por apariencia o nombre, para engañar y timar a los usuarios, generalmente para conseguir dinero de su utilización. También se le llama rogue software, falso antivirus o software bandido.



- Keylogger. Este registra todas las pulsaciones que se realizan sobre las teclas del teclado para robar, por ejemplo, una contraseña.

- Bomba Lógica. Es una parte de código insertada intencionalmente en un programa informático que permanece oculto hasta cumplirse una o más condiciones preprogramadas, en ese momento se ejecuta una acción maliciosa.

Denegación de Servicio

La denegación de servicio o DoS (Denial of Service) se define como la imposibilidad de acceder temporal o permanentemente a un recurso o servicio por parte de un usuario legítimo.

Según el origen de los ataques de denegación de servicio efectuado, distinguimos los siguientes:

- Ataques internos. Se pueden producir de forma casual o intencionada.

- Ataques externos. En este tipo de ataques se aprovechan vulnerabilidades existentes en el sistema, como bugs de los programas o la no autenticación de los usuarios, para acceder a él.

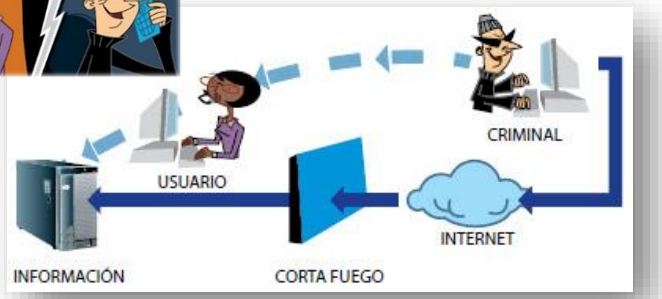
Publicidad y Correo no Deseado

Este correo puede resultar muy molesto porque se trata de correo no solicitado que en algunos casos se envía de forma masiva, llegando a saturar la bandeja de entrada de nuestra cuenta de correo de información no deseada.

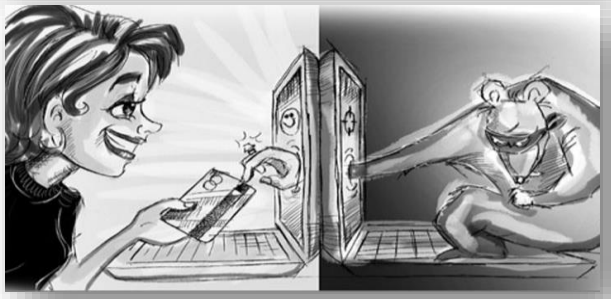
El correo electrónico es una forma de comunicación rápida, gratuita y fácil de utilizar, por lo que muchas empresas lo utilizan masivamente para darse a conocer al público o presentar algún producto, constituyendo una nueva variedad de correo no deseado, el correo basura o spam; se aplica el término spam para el correo no deseado que tiene fines publicitarios o económicos

Ingeniería social. Fraudes informáticos

La mayor parte de las veces, los piratas informáticos no necesitan desarrollar complejos programas para conseguir las contraseñas o los datos bancarios de los usuarios, ya que son estos los que facilitan esta información a los atacantes.



La ingeniería social es una forma de fraude informático muy utilizado por piratas informáticos y consiste en manipular el comportamiento natural de los usuarios mediante engaños y mentiras.



Existe una gran variedad de técnicas destinadas a engañar a los usuarios: phishing, vishing, smishing, grooming, ciber-bulling, cadenas de correos o correos millonarios.

- Escrivá, G. G., Romero, S. R. M., & Ramada, D. J. (2013). Seguridad informática (unidad 6). Madrid, ES: Macmillan Iberia, S.A.. Retrieved from http://www.ebrary.com

- Costas, S. J. (2014). Seguridad informática (capitulo 4). Madrid, ES: RA-MA Editorial. Retrieved from http://www.ebrary.com

- Informático, M. A. (16 de junio de 2016). Mi amigo el informático. Obtenido de https://blog.miamigoelinformatico.com/tipos-software-malicioso-y-sus-cracteristicas/

- Villagomez, C. (23 de abril de 2015). CCM. Obtenido de http://es.ccm.net/faq/2809-diferentes-tipos-de-programas-maliciosos

Universidad Nacional Abierta y a Distancia

GRACIAS POR SU ATENCIÓN