CONCEPTO DE SOFTWARE MALICIOSO

Malware:MALicious software

El software malicioso puede modificar el funcionamiento de un equipo informático o alterar la información que procesa, ya sea borrándola, modificándola o enviándola sin nuestro conocimiento a terceras personas.

Utiliza dos vulnerabilidades:

* Vulnerabilidades del software: explota debilidades del sistema operativo o de algún programa. Algunos se pueden copiarse a sí mismos y enviarse automáticamente a través de la red.
* Vulnerabilidades asociadas a las personas: desde el desconocimiento o del exceso de confianza de los usuarios, contribuyen a la propagación del software malicioso

CLASIFICACIÓN DEL MALWARE

* Según el impacto producido sobre la víctima: hay 3 niveles de peligrosidad, bajo, medio, elevado. Para evaluar el grado de peligrosidad, se estudia la gravedad de las acciones que produce sobre un equipo infectado, su velocidad y facilidad de propagación y la cantidad de infecciones producidas recientemente.
* Según su forma de propagación: hay virus, gusanos y troyanos:
  + Virus: es un software malicioso que tiene por finalidad alterar el funcionamiento de un equipo informático, corrompiendo o destruyendo archivos.

Una vez que se ejecuta, se propaga infectando a otros ficheros y se almacena en ficheros ejecutables para ejecutarse.

* + Gusanos: es un tipo de malware que se propaga automáticamente, ya que puede duplicarse a sí mismo. Su finalidad no es destruir archivos o equipos, sino que están pensados para consumir recursos de un sistema o una red de comunicaciones hasta saturarlo y provocar su caída.

La desinfección de un gusano es más sencilla que la de un virus porque los gusanos no modifican archivos, solo cambian algunos parámetros.

* + Troyanos es un software malicioso y es un programa inofensivo, pero su finalidad es permitir a un usuario no autorizado tomar el control de una máquina infectada. Las infecciones se pueden producir cuando un usuario ejecuta un programa infectado, el programa funciona correctamente, pero el troyano se instala en segundo plano.
  + Hay dos tipos de conexiones:
    - Conexión directa: el cliente se conecta al servidor para enviarle órdenes.
    - Conexión inversa: es el servidor el que envía directamente la información al cliente. Es más efectiva ya que los firewalls no suelen analizar la información saliente del ordenador.

Los más habituales son:

* Backdoor: permite el acceso remoto a un atacante sobre el sistema operativo, una aplicación, una página web o un recurso, de ahí el significado de su nombre
* Keylogger: captura las pulsaciones de las teclas realizadas en el equipo de la víctima para proporcionársela al atacante, con lo que se podría obtener las claves del banco o las conversaciones que ha tenido con otras personas.
* Downloader: su misión es descargar archivos maliciosos y ejecutarlos en el equipo infectado.
* Proxy: el intruso utiliza la red infectada como un servidor proxy, accediendo a la web a través del mismo y encubriendo su verdadera identidad
  + Según las acciones que realiza:
    - Software malicioso no dañino:
      * Spyware: su función es conseguir información del usuario
      * Adware: muestra publicidad de forma intrusiva, por ejemplo, en forma de ventanas emergentes. Suelen camuflar las acciones de otros malware y se suele combinar con spyware.
      * Hijacking: cambian la configuración del navegador, por ejemplo, modificando la página de inicio por una página web, que contendrá anuncios o publicidad. También puede modificar los enlaces de la carpeta “Favoritos” o añadir nuevas barras de herramientas.
      * Jokes: no realiza ninguna acción dañina sobre el equipo infectado, se limita a hacer creer al usuario que se va a borrar el contenido del disco o a enviar información personal por la red, pero no lo hace.
      * Bulos: suele propagarse por correo electrónico y alerta a los usuarios de alguna amenaza no real, como, por ejemplo, un virus, una estafa, un fallo de seguridad, etc. Utilizan técnicas de ingeniería social.
    - Software malicioso dañino:
      * Ransomware: cifra archivos importantes del disco duro para exigir el pago de dinero a cambio de la contraseña para descifrarlos.
      * Rogueware: hace creer al usuario que sui equipo está infectado por algún virus, cuya solución es descargar un supuesto antivirus, dando control total a un atacante remoto.
      * Password stealer: se aprovechan de las herramientas que tienen los navegadores para crear cuentas de correo o redes sociales y modifican el navegador para que capture y envíe las contraseñas cuando la víctima las introduce, obteniendo los datos de sesión.
      * Bombas lógicas: se pone en marcha cuando se cumple alguna condición, como que sea un día concreto, que se cambie algún dato en una base de datos o que se modifique un archivo del disco duro.
      * Keylogger y backdoor:

Denegación de servicio: se define como la imposibilidad de acceder temporal o permanentemente a un recurso o servicio por parte de un usuario legítimo.

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

Ataques de denegación de servicio:

* Ataques internos: provocados por usuarios legítimos de la organización que, ya sea por desconocimiento o de forma intencionada, provocan la degradación de un recurso o servicio, impidiendo su acceso a otros usuarios y a ellos mismos.
* Ataques externos: en este caso, el atacante es una entidad ajena a la organización, es decir, lo provocan usuarios ilegítimos. Se aprovechan las vulnerabilidades del sistema para acceder a él.

Publicidad y correo no deseado

Es todo correo no esperado por el usuario que lo recibe.

Ingeniería social. Fraudes informáticos

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.

* + Suplantación de la identidad: es un tipo de fraude que consiste en hacerse pasar por otra persona. Hay varias categorías:
* Phising: el atacante suele crear una página web falsa aparentemente idéntica a la de una empresa que requiere autenticación y el cliente, al introducir sus datos, le revela esa información al atacante. Una de las técnicas del phishing es el pharming, que es fraude informático que suplanta el sistema de resolución de nombres de dominio (DNS).
* Vishing: es parecida al phishing, pero utiliza como vehículo el protocolo de voz sobre IP (VoIP). La víctima recibe una llamada en la que se le indica que debe teclear en su terminal un determinado dato para realizar alguna acción.
* SMShing: se engaña a las víctimas a través del envío de mensajes SMS a tus teléfonos móviles para conseguir sus contraseñas. Se les pide que accedan a una determinada página web para, por ejemplo, desbloquear su tarjeta de crédito.
* Grooming: consiste en el acoso a menores por parte de un adulto que trata de ganarse su confianza o la coacciona de alguna forma para que realice alguna acción de tipo sexual.
  + Cadenas de correos: son mensajes en los que se incita a su destinatario a difundirlos al mayor número de personas posible bajo promesas o amenazas, con el ánimo de conseguir direcciones de correo.
  + Correos millonarios: es el envío de correos prometiendo a los usuarios que pueden hacerse ricos fácilmente.