Tipos de amenaza

Existen infinidad de modos de clasificar un ataque y cada ataque puede recibir más de una clasificación. Por ejemplo, un caso de *phishing* puede llegar a robar la contraseña de un usuario de una red social y con ella realizar una suplantación de la identidad para un posterior acoso, o el robo de la contraseña puede usarse simplemente para cambiar la foto del perfil y dejarlo todo en una broma (sin que deje de ser delito en ambos casos, al menos en países con legislación para el caso, como lo es España).

Amenazas por el origen

El hecho de conectar una red a un entorno externo nos da la posibilidad de que algún atacante pueda entrar en ella, y con esto, se puede hacer robo de información o alterar el funcionamiento de la red. Sin embargo el hecho de que la red no esté conectada a un entorno externo, como Internet, no nos garantiza la seguridad de la misma. De acuerdo con el Computer Security Institute (CSI) de San Francisco aproximadamente entre el 60 y 80 por ciento de los incidentes de red son causados desde dentro de la misma. Basado en el origen del ataque podemos decir que existen dos tipos de amenazas:

- Amenazas internas: Generalmente estas amenazas pueden ser más serias que las externas por varias razones como son:
    - Si es por usuarios o personal técnico, conocen la red y saben cómo es su funcionamiento, ubicación de la información, datos de interés, etc. Además tienen algún nivel de acceso a la red por las mismas necesidades de su trabajo, lo que les permite unos mínimos de movimientos.
    - Los sistemas de prevención de intrusos o IPS, y *firewalls* son mecanismos no efectivos en amenazas internas por, habitualmente, no estar orientados al tráfico interno. Que el ataque sea interno no tiene que ser exclusivamente por personas ajenas a la red, podría ser por vulnerabilidades que permiten acceder a la red directamente: rosetas accesibles, redes inalámbricas desprotegidas, equipos sin vigilancia, etc.
- Amenazas externas: Son aquellas amenazas que se originan fuera de la red. Al no tener información certera de la red, un atacante tiene que realizar ciertos pasos para poder conocer qué es lo que

hay en ella y buscar la manera de atacarla. La ventaja que se tiene en este caso es que el administrador de la red puede prevenir una buena parte de los ataques externos.

Amenazas por el efecto

El tipo de amenazas por el efecto que causan a quien recibe los ataques podría clasificarse en:

- Robo de información.
- Destrucción de información.
- Anulación del funcionamiento de los sistemas o efectos que tiendan a ello.
- Suplantación de la identidad, publicidad de datos personales o confidenciales, cambio de información, venta de datos personales, etc.
- Robo de dinero, estafas,...

Amenazas por el medio utilizado

Se pueden clasificar por el *modus operandi* del atacante, si bien el efecto puede ser distinto para un mismo tipo de ataque:

- Virus informático: malware que tiene por objeto alterar el normal funcionamiento de la computadora, sin el permiso o el conocimiento del usuario. Los virus, habitualmente, reemplazan archivos ejecutables por otros infectados con el código de este. Los virus pueden destruir, de manera intencionada, los datos almacenados en un computadora, aunque también existen otros más inofensivos, que solo se caracterizan por ser molestos.
- *Phishing*.
- Ingeniería social.
- Denegación de servicio.
- *Spoofing*: de DNS, de IP, de DHCP, etc.

Amenaza informática del futuro

Si en un momento el objetivo de los ataques fue cambiar las plataformas tecnológicas ahora las tendencias cibercriminales indican que la nueva modalidad es manipular los certificados que contienen la información digital. El área semántica, era reservada para los humanos, se convirtió

ahora en el núcleo de los ataques debido a la evolución de la Web 2.0 y las redes sociales, factores que llevaron al nacimiento de la generación 3.0.

- Se puede afirmar que "la Web 3.0 otorga contenidos y significados de manera tal que pueden ser comprendidos por las computadoras, las cuales -por medio de técnicas de inteligencia artificial- son capaces de emular y mejorar la obtención de conocimiento, hasta el momento reservada a las personas".
- Es decir, se trata de dotar de significado a las páginas Web, y de ahí el nombre de Web semántica o Sociedad del Conocimiento, como evolución de la ya pasada Sociedad de la Información

En este sentido, las amenazas informáticas que viene en el futuro ya no son con la inclusión de troyanos en los sistemas o softwares espías, sino con el hecho de que los ataques se han profesionalizado y manipulan el significado del contenido virtual.

- "La Web 3.0, basada en conceptos como elaborar, compartir y significar, está representando un desafío para los hackers que ya no utilizan las plataformas convencionales de ataque, sino que optan por modificar los significados del contenido digital, provocando así la confusión lógica del usuario y permitiendo de este modo la intrusión en los sistemas", La amenaza ya no solicita la clave de homebanking del desprevenido usuario, sino que directamente modifica el balance de la cuenta, asustando al internauta y, a partir de allí, sí efectuar el robo del capital".
- Obtención de perfiles de los usuarios por medios, en un principio, lícitos: seguimiento de las búsquedas realizadas, históricos de navegación, seguimiento con geoposicionamiento de los móviles, análisis de las imágenes digitales subidas a Internet, etc.

Para no ser presa de esta nueva ola de ataques más sutiles, se recomienda:

- Mantener las soluciones activadas y actualizadas.
- Evitar realizar operaciones comerciales en computadoras de uso público o en redes abiertas.
- Verificar los archivos adjuntos de mensajes sospechosos y evitar su descarga en caso de duda.