TALENTO TECH

REGIÓN 3

CAUCA – NARIÑO

LECCIÓN 2-UNIDAD 1

TIC

Universidad Tecnológica de Pereira

faceIT

Infracciones de seguridad

Cualquier ataque que da lugar a que alguien obtenga un acceso no autorizado a un conjunto de dispositivos se considera una infracción de seguridad. Es equivalente al ingreso de una persona no autorizada a un edificio. Cuando un atacante logra cometer una infracción de seguridad este intentará instalar programas para hacerse con el control de otros equipos, robar contraseñas, robar datos y cualquier otra acción que pueda provocar daños a la víctima. Casi siempre las infracciones de seguridad van acompañadas de programas que asistan a los atacantes a lograr sus objetivos. A estos programas se les conoce como malware.

El malware tiene dos componentes que son el mecanismo de propagación y la carga del malware a la red o a los sistemas que se quieren afectar.

El mecanismo de propagación es la forma en la que el malware se replica y se instala en varios sistemas. Algunos ejemplos de propagación comunes son:

- **Virus:** son programas que propagan malware. Los atacantes pueden colocar enlaces en correos, en mensajes de texto o en programas alterados de internet, que instalan malware junto con otro software para que el usuario no sospeche que fue infectado.
- **Troyanos:** Su nombre se deriva de la clásica historia del caballo de troya, donde soldados se escondían en un regalo, accedieron fácilmente a la ciudad y atacaron. En la ciberseguridad, estos son componentes de software que vienen junto con programas que el usuario instala, pero, de forma secreta ejecutan acciones malintencionadas como robar información. Existen ejemplos como es el caso de Riot Games. En este caso los usuarios instalan un videojuego, pero con él, se instala un sotfware cuyo propósito es evitar las trampas. Cuando se analizó el trafico de red de ese software, se descubrió que envía a internet la información del usuario, los programas instalados, el uso de CPU, y mucha información privada que no debería estar siendo enviada a servidores remotos. Muchas entidades los clasifican como spyware (software espía).

La carga es el software que se ejecuta en el sistema infectado causando daños. Existen diferentes tipos:

- **Ransomware:** Es software que bloquea sistemas de datos encriptando la información. Los datos encriptados no se pueden leer ni acceder hasta tener una clave. Generalmente los atacantes aprovechan para encriptar todos los archivos a los que se tenga alcance dentro de una red, encriptan los datos y piden ciertas sumas de dinero a cambio de las claves de desencriptado. Incluso es común que los atacantes que reciben el pago del rescate no entreguen ninguna clave de cifrado y bloqueen toda comunicación. También existe ransomware que está programado para borrar los datos en una fecha específica.
- **Spyware:** Es un software que espía un sistema. Por ejemplo, hay programas que graban las pulsaciones de teclado y las envían a dispositivos remotos. Con esta información se pueden obtener fácilmente usuario y contraseñas de portales sin que el usuario se dé cuenta.

- **Puertas traseras:** Son software que abre vulnerabilidades al instalarse. Por ejemplo, se suelen integrar al piratear software, de esta forma cada que una copia pirata del software se instala, abre puertas traseras para que un ciberdelincuente acceda al computador infectado y ejecute programas cuando lo desee.
-
- **Botnets:** Las botnets son software que se instala en los computadores infectados y tiene la capacidad de ejecutar ciertas acciones comandado por un servidor. La botnet consiste en que el atacante tiene muchos equipos infectados y secuestra su capacidad de procesamiento. Puede enviar órdenes a todos los computadores infectados para que calculen claves de criptografía (minería de datos y de criptomonedas) o para que ataquen servidores en internet. Un computador infectado suele ponerse más lento con el tiempo y los usuarios nota que empeoran sus capacidades de procesamiento con el tiempo.

Uso de técnicas de cifrado en la ciberseguridad

En esta lección se estudiarán las técnicas de cifrado y su desempeño en la ciberseguridad. Para las actividades de aprendizaje activo en clase, es necesario orientar a los estudiantes a la instalación de software que les permita escribir código en Python, se recomienda emplear visual studio code y un intérprete de Python desde la versión 3.6 en adelante. Al momento de escritura de este documento, la versión más reciente es Python 3.13, sin embargo, se recomienda continuar con Python 3.10