Ciberdelincuencia y agentes de la Amenaza: Botnet; Business E-mail Compromise; Cartas negerianas; Cryptojacking; Denegación de servicio; Ingeniería social; Inyección SQL; Malware; Pharming; Phishing; Spear phishing; Ransomware; Skimming; Spoofing; Spyware, Troyano; XSS; Zero-day.

Tipos de Hackers

Antes que nada, vamos a ver los tipos de hackers y lo que hacen, también decir que no todo el que sea hacker implica que tiene maldad, como vamos a ver.

Hacker: un Hacker es un apasionado, un entusiasta, un experto de las nuevas tecnologías, una persona que trata de romper los límites de la tecnología para crear algo superior.

White Hat: Son los hackers éticos, se centran en intentar hackear con permiso las redes de los gobiernos y empresas para identificar vulnerabilidades e intentar arreglarlas.

Black Hat: Son los tipos malos, entran sin autorización a las redes para intentar sacar información, para después venderla o simplemente destruir el sistema.

Gray Hat: Están en el medio, tienen buenas y malas intenciones, la diferencia con los otros hackers es que no quieren robar a las personas ni quieren ayudar a alguien en particular.

Blue Hat o Script-kiddies: Son los que no tienen intención de aprender, este tipos de hackers son malos ya que utilizan el hacking como arma para ganar popularidad entre sus semejantes y para ajustar cuentas. Son personas que carecen de conocimientos profundos y de base y solo usan herramientas de forma dañina.

Hacktivistas: Puede ser un individuo o un grupo de hackers sin nombre cuya intención es obtener acceso a sitios web y redes gubernamentales. Los datos obtenidos se suelen utilizar para obtener beneficios políticos o sociales.

Phreaker: Viene de phone freak y tienen conocimientos en telefonía, tanto modular como móvil.

Newbie: es el Novato, alguien que está empezando en el mundo del hacking.

Botnet

Las botnets son conocidas como redes de “ordenadores zombie”, son varios, muchos dispositivos infectados, que controla uno o varios ciberdelincuentes. Son ataques malware.

El modo de infección es desde código malicioso en páginas web hasta correos electrónicos infectados, una vez abierto este tipo de páginas o correos el dispositivo queda infectado sin ser consciente de ello.

El objetivo de estas botnets es muy variado, como, por ejemplo: propagar virus, spam, y cometer delitos y fraudes en internet.

Business E-mail Compromise

Esta diseñado para obtener acceso a información comercial o extraer dinero a través de una estafa por correo electrónico a las empresas.

Cartas nigerianas

También conocidas como 4/19, ya que, es el articulo penal nigeriano que recoge el delito de cartas nigerianas.

Consiste básicamente en intentar engañar a alguien con un a fortuna inexistente, mediante email obteniendo así acceso a la cuenta bancaria de la víctima.

Cryptojacking

Este tipo de hacking está diseñado para poder minar criptomonedas con nuestros dispositivos sin consentimiento ni conocimiento por parte de la víctima. No roban datos, simplemente utilizan los recursos de los dispositivos para minar criptomonedas. Son ataques de malware.

Denegación de servicio

O DDOS, consiste en atacar desde muchos equipos diferentes un servidor web para que deje de funcionar. Hacen que las páginas web caigan y no se puedan usar. Normalmente se usan los dispositivos de un botnet para aumentar la eficacia y potencia del ataque.

Ingeniería social

Son técnicas que no se dirigen a los dispositivos, sino, a las personas. Con el objetivo de que demos información personal o permitir que controlen nuestros dispositivos. Es básicamente engañar y manipular a las personas. Existen muchos tipos de ataques como:

- Phising: Nos envían un mensaje suplantando a una entidad legítima, como un banco, una red social, paquetería, etc… suelen estar escritos de manera urgente o muy atractivo para que no nos pensemos dos veces que estamos haciendo.
- Vishing: Es exactamente igual, pero por llamadas telefónicas.
- Smishing: Es lo mismo, pero por medio de SMS

Spear phishing

Se centra en correos electrónicos, pero con víctimas específicas y escogidas previamente. Como altos directivos de empresas y gubernamentales.

Inyección SQL

SQL es el lenguaje informático en el que están basadas las bases de datos, en estos ataques inyectan códigos maliciosos en la base de datos de la aplicación web, para tener acceso parcial o total a los datos, para poder robarlos, monitorizarlos o destruirlos.

Utilizan elementos Input, cadenas de consultas, cookies y archivos.

Malware

Son programas maliciosos que llevan a cabo acciones dañinas en un sistema informático y contra la privacidad. Existen varios tipos de malware:

- **Spyware:** Está diseñado para recopilar información y supervisar toda actividad para compartirla con un usuario remoto, también puede descargar otro software malicioso.
- **Troyano:** Se camuflan como software legítimo, normalmente la finalidad es controlar el equipo, robar datos, descargar más software malicioso y propagarse a otros dispositivos.
- **Ransomware:** Cifran el acceso a nuestro dispositivo, discos duros o archivos. Piden un “rescate” para descifrar y que podamos acceder de nuevo a nuestro dispositivo. Police ransomware.

Pharming

El pharming, una combinación de los términos "phishing" y "farming", es muy semejante al phishing, en el que el tráfico de un sitio web es manipulado para permitir el robo de información confidencial. Ataca al DNS, de dos maneras al DNS local (archivo hosts), para que cuando ingreses a una página se te redirija a otra normalmente falsa, o directamente atacar a los servidores DNS para que de igual manera redirijan el tráfico. Lo malo de este ataque es que no es necesario que el dispositivo esté infectado.

Skimming

Es el robo de la información de la tarjeta de crédito o débito, copian la banda magnética de la tarjeta para clonarla.

Spoofing

El spoofing es la suplantación de identidad tanto nuestra como de una web o entidad, hacen una copia exacta de una página de login, para tener acceso a nuestras cuentas.

Existen varios tipos:

- IP spoofing: El atacante falsea su IP para que parezca otra.
- Web spoofing: Suplantación de una web por otra falsa.
- Email spoofing: Suplantación de un mail de una persona o entidad.
- DNS spoofing: Como el pharming suplanta el DNS para que nos conectemos donde ellos quieran, redirigiendo el tráfico de la red.

XSS

Es una secuencia de comandos en sitios cruzados o cross-site scripting.

Es típico de las aplicaciones web que permite al atacante inyectar código en javascript, aunque, también se puede encontrar en aplicaciones y hasta el navegador.

Un ejemplo de esto es lo que pasó con FIFA 21, que robaron el código fuente con este método, usando cookies de sesión.

Zero-day

Las vulnerabilidades zero-day o de día cero, es una vulnerabilidad que ha sido descubierta recientemente y que no tiene parche de seguridad para solucionarla. El ejemplo más reciente de esto es Follina, un zero-day de Word, que usando la herramienta de diagnóstico de Microsoft (MSDT) puede cargar y ejecutar código en powershell.

Cibercriminales

Cibercrimen es toda actividad delictiva que abusa de un ordenador o dispositivo y de la red.

También hace referencia a contratar servicios de sicario por internet, compraventas de drogas etc….

En definitiva, es cualquier crimen que involucre computadoras y al mismo tiempo redes informáticas, incluyendo crímenes que no dependen en gran medida de las computadoras.

Crime as service

Consiste en que hackers experimentados venden el acceso a sus herramientas y conocimientos para hacer ataques. Sus servicios más usados es el Phising.

Insider Threat

Es una amenaza interna, personas dentro de la organización, como empleados, exempleados, contratistas o socios comerciales que saben como funciona la seguridad y los sistemas informáticos.

APTs

Es una amenaza persistente avanzada, su objetivo es atacar de forma avanzada (por múltiples frentes) y de forma continuada a un objetivo determinado (empresa, estado).

Normalmente utilizan zero-days. Los grupos organizadores de APT más conocidos son los que, al menos de manera presunta, son apoyados directamente por los gobiernos más activos en el ámbito de la ciberserguridad, Estados Unidos, Rusia, China, la Unión Europea.

El objetivo de APTs es el ciberespionaje, provocar daño o terror en la población o beneficio económico. Algunos ejemplos: Duqu buscaba información del programa nuclear iraní, Campañas de control industrial, como sabotaje.

Cyber Kill Chain

Para hacer frente a todo lo anterior, Lockheed Martin, desarrolló este procedimiento con el cual divide el ataque en siete partes diferenciadas para poder identificar y hacer frente a estos ataques. Los niveles son:

- Reconocimiento: Es la fase en la que el delincuente recopila información sobre el objetivo.

- Preparación: Una vez recopilada la información, deciden por dónde van a atacar, normalmente es el eslabón más débil de la cadena.
- Distribución: Una vez dentro del sistema, el atacante distribuye todo lo que quiera (Malware, spyware, ransomware, etc…), configura los programas para los tipos de ataque, ya sea inmediatos, programados, o bombas lógicas.
- Explotación: Una vez desplegados, empiezan con la explotación del sistema, que dependerá del tipo de ataque, normalmente ofuscan los programas para que no se detecte su actividad y origen.
- Instalación: Si el atacante le parece oportuno puede dejar una puerta abierta (backdoor) para poder acceder al sistema constantemente y sin ser detectado.
- Comando y control: Una vez hecho todo lo anterior el atacante toma el control del sistema y se asegura de mantener el control.
- Acción sobre el activo: Aquí el atacante ya tiene todo lo necesario para llevar a cabo acciones sobre el objetivo (Cifrar los datos, ataques DDOS o monitorizar).2

Algunos términos:

- Flood o flooders: Programa que se utiliza para enviar mensajes repetidamente y de forma masiva, mediante correo electrónico, sistemas de mensajería instantánea, chats, foros, etc. El objetivo de este comportamiento es provocar la saturación o colapso de los sistemas a través de los que se envía el mensaje.
  Flaming: Situación consistente en una discusión que se lleva a cabo en línea (por medio de correos electrónicos, redes, blogs o foros). Y que toma un tono insultante o desagradable hacia una de las personas con el objetivo de crisparla.
- Alertcops: Servicio que permite que, desde un dispositivo móvil “smartphone”, un ciudadano pueda enviar una alerta directamente a los cuerpos policiales, de una forma sencilla e intuitiva, con el objetivo de ser atendido de manera rápida y eficiente por los cuerpos policiales estatales.