Ciberdelincuencia y agentes de la Amenaza

Amenazas

- https://www.jesusninoc.com/08/03/adopcion-de-pautas-de-seguridad-informatica-seguridad-y-alta-disponibilidad/#Amenazas_Tipos
- https://www.jesusninoc.com/02/02/auditoria-de-incidentes-de-ciberseguridad-incidentes-de-ciberseguridad/#Taxonomia_de_incidentes_de_ciberseguridad

Botnet

Una *botnet* es el nombre que se emplea para designar a un conjunto de máquinas controladas remotamente con finalidad generalmente maliciosa. Un *bot* es una pieza de *software* maliciosa que recibe órdenes de un atacante principal que controla remotamente la máquina. Los servidores C&C habilitan al atacante para controlar los *bots* y que ejecuten las órdenes dictadas remotamente.

Business E-mail Compromise

El Business Email Compromise (BEC) es una forma dañina de ciberdelincuencia con potencial para costar a las empresas grandes sumas de dinero. Incluso los más astutos pueden ser víctimas de uno de estos sofisticados engaños.

Cartas nigerianas

Las cartas nigerianas son un tipo de fraude informático que tiene como objetivo conseguir solapadamente el acceso a la cuenta bancaria de un usuario, o extorsionarlo para conseguir su dinero de una manera diferente.

Cryptojacking

También llamado Criptominado malicioso o Criptosecuestro, en inglés Cryptojacking, consiste en el secuestro de un dispositivo electrónico sin el consentimiento o conocimiento del usuario, para aprovechar sus recursos en el minado de criptomonedas.

Denegación de servicio

Ataque de denegación de servicio. Ej.: envío de peticiones a una aplicación web que provoca la interrupción o ralentización en la prestación del servicio.

Ingeniería social

Técnicas que buscan la revelación de información sensible de un objetivo, generalmente mediante el uso de métodos persuasivos y con ausencia de voluntad o conocimiento de la víctima.

Inyección SQL

Tipo de explotación, consistente en la introducción de cadenas mal formadas de SQL, o cadenas que el receptor no espera o controla debidamente; las cuales provocan resultados no esperados en la aplicación o programa objetivo, y por la cual el atacante produce efectos inesperados y para los que no está autorizado en el sistema objetivo.

- https://www.jesusninoc.com/10/21/simular-una-inyeccion-de-sql-en-powershell/

Malware

Palabra que deriva de los términos *malicious* y *software*. Cualquier pieza de *software* que lleve a cabo acciones como extracción de datos u otro tipo de alteración de un sistema puede categorizarse como *malware*. Así pues *malware* es un término que engloba varios tipos de programas dañinos.

Pharming

Ataque informático que aprovecha vulnerabilidades de los servidores DNS (*Domain Name System*). Al tratar de acceder el usuario al sitio *web*, el navegador redirigirá automáticamente al usuario a una dirección IP donde se aloja una *web* maliciosa que suplanta la auténtica, y en la que el atacante podrá obtener información sensible de los usuarios.

Phishing

Suplantación de otra entidad con la finalidad de convencer al usuario para que revele sus credenciales privadas.

Spear phishing

Variante del *phishing* mediante la que el atacante focaliza su actuación sobre un objetivo concreto.

Ransomware

Se engloba bajo este epígrafe a aquel *malware* que infecta una máquina, de modo que el usuario es incapaz de acceder a los datos almacenados en el sistema. Normalmente la víctima recibe

posteriormente algún tipo de comunicación en la que se le coacciona para que se pague una recompensa que permita acceder al sistema y los archivos bloqueados.

Skimming

Se denomina Skimming al robo de información de tarjetas de crédito utilizado en el momento de la transacción, con la finalidad de reproducir o clonar la tarjeta de crédito o débito para su posterior uso fraudulento. Consiste en el copiado de la banda magnética de una tarjeta.

Spoofing

La suplantación de identidad□□□ o spoofing en términos de seguridad de redes, hace referencia al uso de técnicas a través de las cuales un atacante, generalmente con usos maliciosos o de investigación, se hace pasar por una entidad distinta a través de la falsificación de los datos en una comunicación.

Spyware

Tipo de *malware* que espía las actividades de un usuario sin su conocimiento o consentimiento. Estas actividades pueden incluir *keyloggers*, monitorizaciones, recolección de datos así como robo de datos. Los *spyware* se pueden difundir como un troyano o mediante explotación de *software*.

Troyano

Tipo de *malware* que se enmascara como *software* legítimo con la finalidad de convencer a la víctima para que instale la pieza en su sistema. Una vez instalado, el *software* dañino tiene la capacidad de desarrollar actividad perjudicial en segundo plano. Un troyano no depende una acción humana y no tiene la

capacidad de replicarse, no obstante puede tener gran capacidad dañina en un sistema a modo de troyanos o explotando vulnerabilidades de *software*.

XSS

Ataque que trata de explotar una vulnerabilidad presente en aplicaciones web, por la cual un atacante inyecta sentencias mal formadas o cadenas que el receptor no espera o controla debidamente.

- https://www.jesusninoc.com/01/09/ejercicios-de-seguridad-simular-un-xss-persistente-almacenando-un-xss-en-un-registro-de-la-base-de-datos/

Zero-day

Un Ataque de día cero es un ataque contra una aplicación o sistema que tiene como objetivo la ejecución de código malicioso gracias al conocimiento de vulnerabilidades que son desconocidas para los usuarios y para el fabricante del producto. Esto supone que aun no hayan sido arregladas.

Cibercriminales

El cibercrimen es una actividad delictiva que se dirige a una computadora, una red informática o un dispositivo en red, o bien que utiliza uno de estos elementos. La mayor parte del cibercrimen está cometido por cibercriminales o hackers que desean ganar dinero.

Crimen as Service

Criminales o cibercriminales que ofrecen sus servicios a otros grupos para el lavado de dinero y “cobro” seguro de las

ganancias derivadas del delito.

Hacktivistas

Un hacktivista es un individuo que abusa de una red o una aplicación web con el fin de promover alguna causa social o política. Los hacktivistas tienden a hacer ataques de denegación de servicio, defacement, exfiltración de datos y más.

Insider threat

Una amenaza interna es una amenaza maliciosa para una organización que proviene de personas dentro de la organización, como empleados, ex empleados, contratistas o socios comerciales, que tienen información interna sobre las prácticas de seguridad, los datos y los sistemas informáticos de la organización.

APTs

Ataques dirigidos contra organizaciones concretas, sustentados en mecanismos muy sofisticados de ocultación, anonimato y persistencia. Esta amenaza habitualmente emplea técnicas de ingeniería social para conseguir sus objetivos junto con el uso de procedimientos de ataque conocidos o genuinos.

Cyber Kill Chain

La *Cyber Kill Chain* está formada por una secuencia de siete pasos, cada uno de los cuales supone una etapa del ataque:

- Paso 1: Reconocimiento.
- Paso 2: Preparación.
- Paso 3: Distribución.
- Paso 4: Explotación.

- Paso 5: Instalación.
- Paso 6: Comando y control.
- Paso 7: Acciones sobre los objetivos.