AMENAZAS

CIBERSEGURIDAD Y TIPOS DE AMENZAS

Ciberseguridad

La Ciberseguridad es la disciplina dentro del campo de la informática encargada de la protección de sistemas, redes, programas e individuos de ataques cuyo fin es el de conseguir, destruir o capturar información privilegiada o confidencial a cambio de algún beneficio ya sea económico, social, reputacional, etc.

Estos ataques usualmente son desastrosos ya que no solamente afectan la información de los objetivos, sino que también interrumpen el correcto funcionaniemnto de todos los sistemas que puedan depender de esta información, causando estragos a largo plazo.

TIPOS DE AMENAZAS

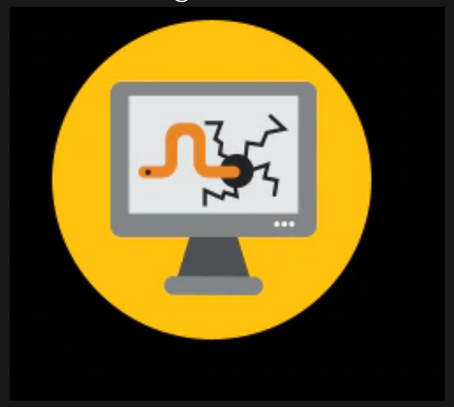
Malware

Malware o “software malicioso” es un término amplio que describe cualquier programa o código malicioso que es dañino para los sistemas.

1

Virus

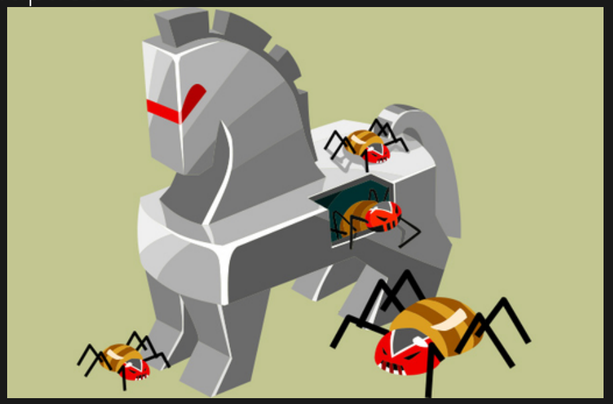
Un virus informático es un tipo de programa o código malicioso escrito para modificar el funcionamiento de un equipo. Además, está diseñado para propagarse de un equipo a otro. Los virus se insertan o se adjuntan a un programa o documento legítimo que admite macros a fin de ejecutar su código.



2

Troyano

Un caballo de Troya o troyano es un tipo de malware que a menudo se camufla como software legítimo. Una vez activados, los troyanos pueden permitir a los cibercriminales espiar, robar datos confidenciales y obtener acceso por una puerta trasera al sistema infectado. Los troyanos no pueden multiplicarse.



TIPOS DE AMENAZAS

3

Gusanos

Los gusanos son en realidad una subclase de virus, por lo que comparten características. Son programas que realizan copias de sí mismos, alojándolas en diferentes ubicaciones del ordenador sin necesidad de interacción por parte del usuario.

El objetivo de este malware suele ser colapsar los ordenadores y las redes informáticas, impidiendo así el trabajo a los usuarios. A diferencia de los virus, los gusanos no infectan archivos.

4

Adware

Adware es el nombre que se da a los programas diseñados para mostrar publicidad en la computadora, redirigir las solicitudes de búsqueda a sitios web de publicidad y recopilar datos comerciales acerca del usuario (como los tipos de sitios web que visitas) para mostrarte avisos personalizados.

Estos pueden ser maliciosos (sin autorización del usuario), o invasivos (autorización del usuario).

TIPOS DE AMENAZAS

5

Spyware

Recopilar información de un ordenador o dispositivo informático y transmitir la información a una entidad externa sin el permiso del dueño del ordenador

6

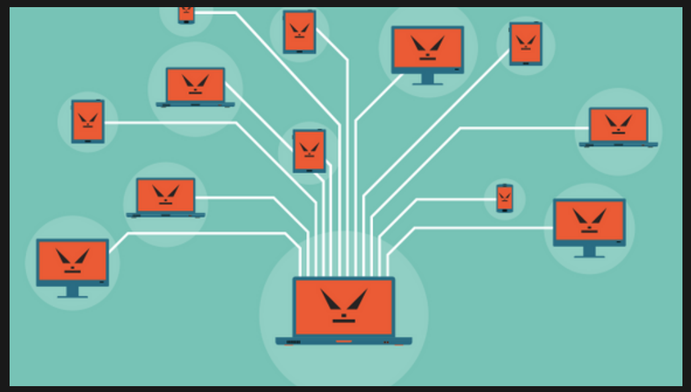
Rootkits

Diseñado para infectar un PC, el cual permite instalar diferentes herramientas que le dan acceso remoto al ordenador. Este malware se oculta en la máquina, dentro del sistema operativo.

7

Botnets

Se utilizan virus troyanos especiales para crear una brecha en la seguridad de los ordenadores de varios usuarios, tomar el control de cada ordenador y organizar todos los equipos infectados que el cibercriminal puede gestionar de forma remota.



TIPOS DE AMENAZAS

8

Crimeware

Diseñado para robar datos financieros. Utiliza la ingeniería social principalmente para lograr su objetivo. Lo que buscan principalmente son las credenciales de acceso a bancos, métodos de pago y todo lo relacionado con las finanzas.

9

Ramsomware

Softwares malicioso diseñados para infiltrarse o dañar una computadora o sistema de información sin el consentimiento de su propietario. El malware puede tomar varias formas, como la de un virus informático, un troyano, un spyware.

PRINCIPIOS DE LA SEGURIDAD DE LA INFORMACIÓN

SEGURIDAD DE LA INFORMACIÓN

Cuando hablamos de asegurar la informacion hay 3 pilares que deben cumplirse para que esta sea consistente.

+ Integridad

es como los datos se mantienen intactos libre de modificaciones o alteraciones por tercero

+ Confidencialidad

se conoce como una forma de prevenir la divulgación de la información a personas o sistemas que no se encuentran autorizados.

+ Disponibilidad

nada hacemos teniendo segura e integra nuestra información, si no va a estar disponible cuando el usuario o sistema necesite realizar una consulta.

PROTECCIÓN DE LA INFORMACIÓN

garantizar los 3 pilares que garantizan su seguridad

Medidas preventivas

Encriptacion <c>
Control de Accesos <c>
Capacitacion <c>
Firmas digitales <i>
Redundancia <d>

Medidas Reactivas

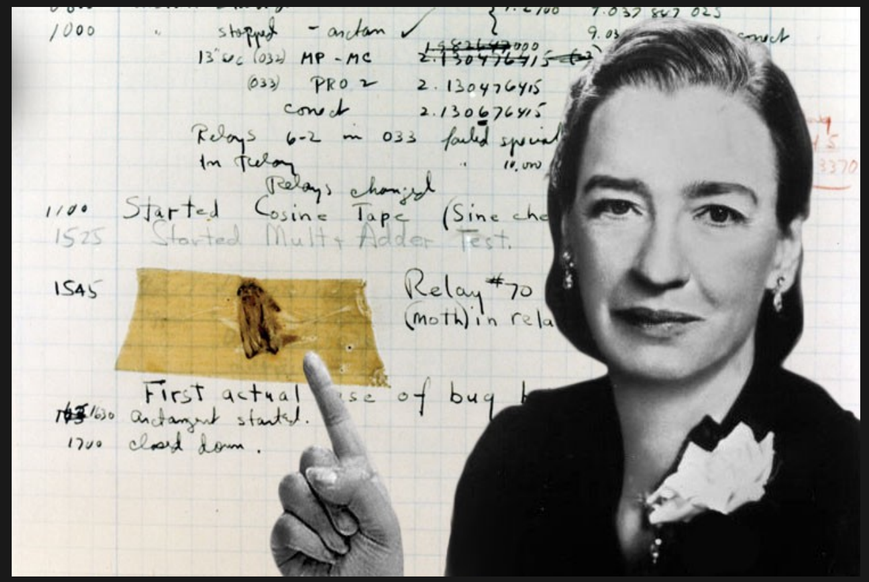
Borrado remoto <c>
Auditorias <i>
Control de Versiones <i>
Deteccion de intrusos <i>
Parches de seguridad <d>

FALLAS Y VULNERABILIDADES

FALLAS

Una falla o bug (insecto) es un error en un programa o S.O. que desencadena un resultado no deseado

El término bug viene desde 1947 cuando la física y matemática Grace Hopper descubre que una polilla había provocado un error en uno de los relés electromagnéticos del Mark II



TIPOS DE FALLAS

Heisenbug

Basado en el principio de incertidumbre de Heisenberg, es un tipo de bug que parece desaparecer o comportarse de otro modo al intentar ser depurado.

Bohrbug

Es un bug que siempre produce una falla al reiniciar la operación que causó la falla. Recibió su nombre del átomo de Bohr porque representa un error sólido y fácilmente detectable que puede aislarse mediante técnicas de depuración estándar.

Mandelbug

Llamado así por el matemático Benoit Mandelbrot, es un tipo de bug muy complejo que es difícil de solucionar debido a su complejidad e imprevisibilidad.

Schrödinbug

Es un error que se manifiesta al ejecutar software después de que un programador se da cuenta de que el código nunca debería haber funcionado en primer lugar.

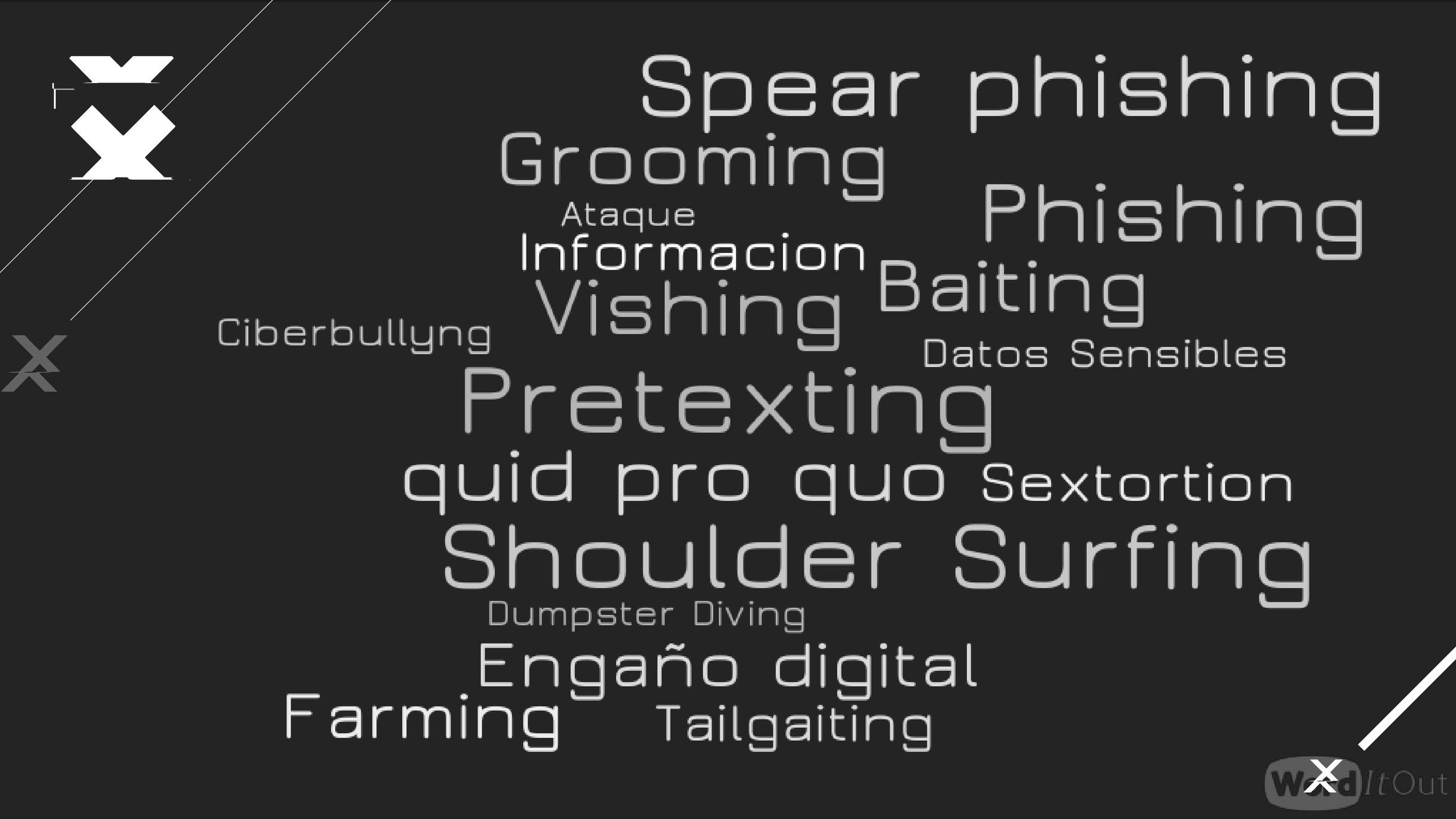
VULNERABILIDADES

Una vulnerabilidad es una debilidad o fallo de un sistema informático que puede poner en riesgo la integridad, confidencialidad o disponibilidad de la información.

PASOS PARA DETECTAR UNA VULNERABILIDAD

1. Evaluar cómo está constituida la red e infraestructura.
2. Delimitar quién puede y debe acceder a la información.
3. Probar que las copias de seguridad realizadas funcionen.
4. Identificar las partes más sensibles y esenciales del sistema.
5. Analizar el estado de la seguridad informática.

INGENIERIA SOCIAL


Spear phishing
Grooming
Ataque
Phishing
Informacion
Baiting
Vishing
Ciberbullyng
Datos Sensibles
Pretexting
quid pro quo
Sextortion
Shoulder Surfing
Dumpster Diving
Engaño digital
Farming
Tailgaiting

AARON SWARTZ

Programador, activista político y hacktivista

Background

Diseñador jefe del proyecto inicial de Open Library
Cofundó el grupo en línea Demand Progress
Estuvo involucrado en el desarrollo de RSS, Markdown, Creative Commons, "web.py" y Reddit.

El 6 de enero de 2011 fue arrestado bajo los cargos de fraude electrónico, fraude informático, entrada ilegal e imprudente.
Por descargar automaticamente publicaciones académicas automáticamente desde JSTOR, con una cuenta de invitado que le proporcionó el mismo Instituto. En la red del MIT.

There is no justice in following unjust laws. It's time to come into the light and, in the grand tradition of civil disobedience, declare our opposition to this private theft of public culture.

MUCHAS GRACIAS

Carrillo, Alexis
Gerardi, Francisco
Gonzalez Olaya, Stiven
Gozzerino Taboada, María Gabriella