



SEGURIDAD LÓGICA

Ing. Alvaro Antezana
ARAM © 2021



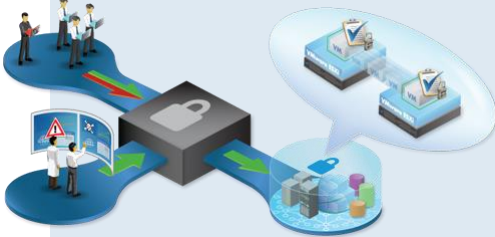
- Clasificar, identificar las amenazas lógicas por su procedencia.
- Describir e identificar los distintos tipos de Malware y Atacantes.
- Caracterizar las herramientas disponibles para proteger la información de virus y ataques de Malware, spam, phishing, etc.

Seguridad lógica

Se refiere a la seguridad en el uso de software y los sistemas, la protección de los datos, procesos y programas, así como la del acceso ordenado y autorizado de los usuarios a la información digital. (Wikipedia, 2020)

Vulnerabilidades lógicas:

- Configuración
- Actualización
- Desarrollo







Vulnerabilidades de actualización:

Se derivan por la utilización de SO, sistemas o servicios informáticos, que se encuentran desatendidos y no siguen un ciclo adecuado de aplicación de parches de seguridad y de actualización principalmente o que concluyo su ciclo de soporte y mantenimiento por parte del fabricante.





Vulnerabilidades de desarrollo:

Se derivan por la carencia de aplicación de buenas prácticas y principios de seguridad en el ciclo de vida del software, que minimicen los fallos de seguridad que pueden ocasionar grandes pérdidas de dinero, tiempo, información, estabilidad entre otros.



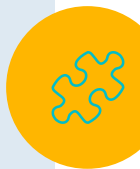
Tipos de atacantes



Son personas que utilizan herramientas o poseen conocimientos específicos para vulnerar y explotar sin autorización los SO, servicios y sistemas informáticos con el fin de obtener algún un beneficio o rédito personal.

PRINCIPALES TIPOS:

- ☐ Hacker
- ☐ Craker
- ☐ Phreaker
- ☐ Lamers
- ☐ Newbie
- ☐ Script kiddies
- ☐ Hacktivistas
- ☐ Personal interno





Tsutomu Shimomura



Hacker



Takedown

Persona élite en la que los méritos se basan en su habilidad, conocimientos, capacidad y el reconocimiento proviene de terceros.

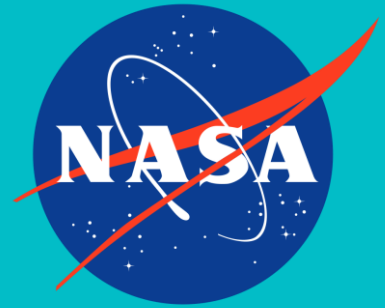
(Kevin Mitnick, arrestado en 1995 liberado 2002)



Defense Threat
Reduction Agency



Cracker



National Aeronautics
and Space
Administration

Persona con grandes conocimientos de informática que se dedica a acceder ilegalmente a sistemas informáticos ajenos y a manipularlos, con el objetivo de crackearlos, es decir utilizar un sistema privativo evadiendo la licencia.

(Jonathan James, susidio 18/05/2008)



26000 Hz rutar
AT&T



Phreaker



Steve Jobs y Steve
Wozniak, cajas
azules

Poseen conocimientos profundos para vulnerar los sistemas de telefonía fija y móvil, centrales telefónicas, radio basé, tarjetas prepago e informática.

(John Draper , arrestado 1976 hasta 1978)





SONY PS3



Jailbreak



Dispositivos móviles

Poseen conocimientos profundos para vulnerar software y hardware que evita la instalación de software no legítimo en dispositivos móviles o consolas de juego.

(George Hotz , acuerdo extrajudicial Sony)




Otros Tipos



LAMERS, Carecen de conocimiento técnicos profundos, son por lo general internautas obsesivos que rebuscan información de interés y que se puede encontrar en Internet que les da la posibilidad de entrar en sistemas informáticos remotos.

NEWBIE, Es un novato en el hackeo que al contrario que los Lamers, aprenden el Hacking siguiendo todos los cautos pasos para lograrlo y sin jactarse de sus logros, con el objetivo de aprender y mejorar su nivel.



SCRIPT KIDDIE, Son fanáticos de temas de hacking y cracking, pero carecen de las bases necesarias para comprenderlos, se limitan a recopilar información de Internet y buscan programas de Hacking para ejecutarlos sin entender su uso, alcance y consecuencias de las mismas.

HACKTIVISMO, Se refiere a una agrupación de Hackers y activistas, que emplean la utilización no violenta de herramientas digitales persiguiendo fines políticos o ideológicos; estas herramientas incluyen desfiguraciones de webs, redirecciones, ataques de denegación de servicio, robo de información, parodias de sitios web, sustituciones virtuales, sabotajes virtuales y desarrollo de software.

PERSONAL INTERNO, Personal o empleado de una organización que puede caer en los anteriores tipos, que busca vulnerar los sistemas informáticos internos con algún fin personal, casusa, espionaje o sabotaje.



Hacktivismo





Hacktivismo

14

LulzSec Ataque a la Red de la OTAN

INTERNET | 7 junio 2011

tweet

El grupo de hackers LulzSec ha proclamado su autoría del ataque a la red de la OTAN. El grupo se autoproclamaba "autónomo" y no estaba relacionado con el FBI.

LulzSec ha penetrado en la red de la OTAN, abriendo un agujero de seguridad en la configuración de sus sistemas. El grupo ha asegurado que no quiere dañar a la OTAN, pero que se comprometió a revelar las vulnerabilidades de su sistema.

En el caso de la OTAN, el grupo asegura que se ha comprometido a revelar la información que se haya comprometido a revelar.

PORTADA >> SOCIEDAD Y CULTURA

Anonymous posee datos cibernéticos de la OTAN

26/07/2011 - 11:51
IBLNEWS, AGENCIAS

Envía

El grupo Anonymous, encabezado por el activista italiano, se adelanta con la operación OTAN. En esta ocasión, el grupo ha asegurado que no quiere dañar a la OTAN, pero que se comprometió a revelar la información que se haya comprometido a revelar.

"AntiSec"(movimiento anti-seguridad online industrial) ha desarrollado varios ataques a la OTAN. Anonymous ha coordinado el ataque pasado jueves, cuando el grupo se comprometió a revelar la información que se haya comprometido a revelar.

La incursión en Colombia, donde el grupo se comprometió a revelar la información que se haya comprometido a revelar.

Opinión

INICIO COCHABAMBA EL PAÍS

Ciencia y Tecnología

Anonymous invade la red sudamericana

El ataque es atribuido por el grupo a la OTAN.



La escalada de guerra cibernética entre los hackers de toda índole, han inhabilitado a los gobiernos de Perú, Colombia, Chile y Argentina.

La incursión en Colombia, donde el grupo se comprometió a revelar la información que se haya comprometido a revelar.

Mundo Domingo 06 de Noviembre 2011

Ataque cibernético a la red de la OTAN y del Shabab

El ataque es atribuido por el grupo a la OTAN.



SIPSE.com SIPSE.com en tu Móvil

Inicio Yucatán Quintana Roo

Anonymous ataca la red de la OTAN

CANCÚN, Q.Roo.- Se reveló que el grupo de hackers Anonymous ha atacado la red de la OTAN, lo que ha causado la caída de la red de la OTAN.



Ayer Anonymous mediante un correo electrónico a Twitter y Facebook, comenzó una campaña de información sobre diputados y senadores de México. (homozapping.com)

guerrero, Diputados del PAN, página de Facebook.

Se revelaron, entre otras cosas, datos personales de los diputados y senadores.

La llamada Operación Corrupción en Yucatán, donde el grupo se comprometió a revelar la información que se haya comprometido a revelar.

Sexenio

EXTRAORDINARY LIFE

2 y 3 de Noviembre

Nacional Política Mundo Economía Empresas Seguridad LifeStyle G

Sexenio por Estados Puebla Querétaro Sinaloa Veracruz Oaxaca Tlaxcala Jalisco

Ingresar a Sexenio con Facebook

13 de noviembre de 2011

Detenidos 14 Anonymous en EE.UU.

El FBI detuvo a 14 activistas relacionados con la red de piratas informáticos Anonymous. Las penas que pueden enfrentar son de diez años de cárcel y 250 mil dólares en multas.

19 de julio de 2011 por Josué Cantorán Viramontes Sección Internacional

Fueron detenidos en Estados Unidos 14 hackers vinculados con la red internacional Anonymous. Todos varones y de entre 20 y 42 años, quienes pueden enfrentar sanciones de hasta diez años de cárcel y 250 mil dólares en multas.

El FBI anunció que, en una magnánima operación que englobó más de 40 operativos en diez estados diferentes, fueron capturados 14 sujetos relacionados directamente con la famosa red de piratas informáticos.

Los nombres e identidades de todos los involucrados, excepto uno, pueden leerse en el comunicado que el propio departamento de seguridad estadounidense publicó para dar a conocer esta información.

"Catorce personas fueron arrestadas hoy por el FBI, debido a cargos relacionados con su presunta implicación en el ataque cibernético al sitio web de PayPal, una acción que ha sido adjudicada por el grupo Anonymous", informó el FBI en el referido comunicado.

El boicot perpetrado a PayPal por Anonymous se debió a que esta empresa se manifestó en contra de WikiLeaks y WikiLeaks.





Amenazas lógicas



Son programas o aplicaciones (software), que pueden comprometer los sistemas informáticos, de forma intencionada (malware) o fortuita (bugs).



CONSECUENCIAS

- Disponibilidad de la información o de los servicios.
- Modificación, robo o pérdida de información no autorizada.
- Manipulación del procesamiento o distorsión de resultados.
- Explotación no autorizada de los recursos hardware y/o software.
- Afectación de la imagen corporativa.
- Pérdida de confianza e ingresos.

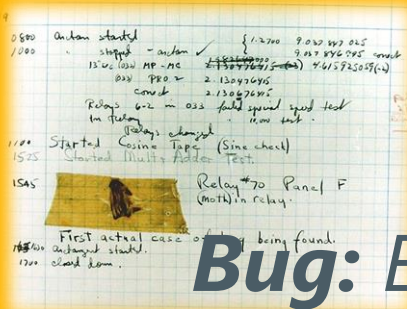




Malware: (del inglés *malicious software*), también llamado *badware* o código maligno.

Tipo de software que tiene como objetivo infiltrarse o dañar una computadora sin el consentimiento de su propietario.





Bug: Error, fallo o problema dentro de un programa o software que desencadena un resultado indeseado o no previsto.

Debug: Depuración de errores en el código de programa o software





Virus

Secuencia de código que se inserta en un archivo (huésped), que al ejecutarse (mediante la intervención del usuario), se inserta a sí mismo en otros archivos.



Troyanos

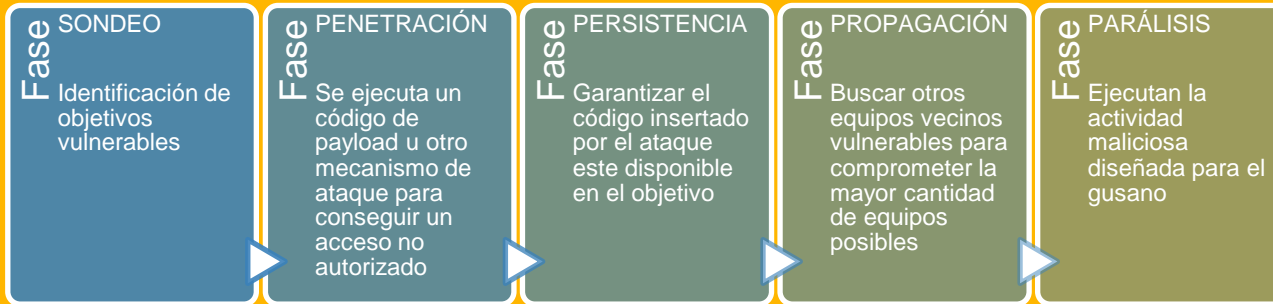
Se presenta al usuario como un programa o archivo aparentemente legítimo e inofensivo, pero al ejecutarlo o accederlo ocasiona daños o otorga accesos no autorizados a un atacante.



Gusanos

Se replican así mismos mediante la red, no requieren la intervención del usuario, utilizan partes automáticas de los sistemas operativos y residen en la memoria.

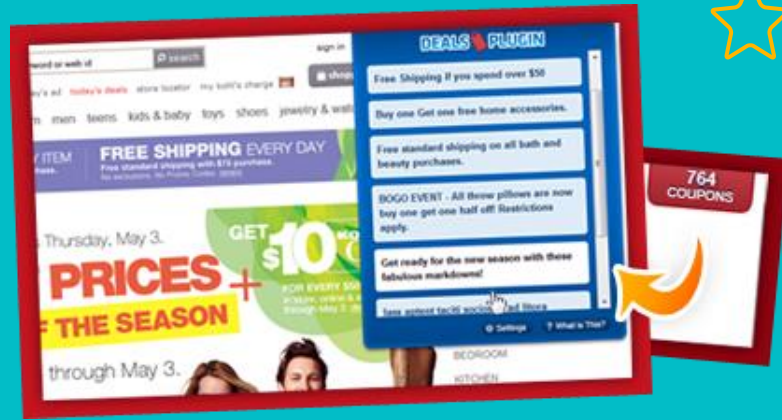
Fase básicas de ataque Gusanos/Virus



Gusanos

23





Adware

Diseñados para mostrar publicidad, redirigir solicitudes de búsqueda a sitios web de publicidad y recopilar datos comerciales para mostrar avisos personalizados.



Spyware

Recopila información sensible y la transmite a una entidad externa, sin el consentimiento o conocimiento del dueño, se encuentra en ejecución permanente en el ordenador.



Bombas lógicas

Son piezas de código que se activan en un momento o bajo condiciones predefinidas, para ejecutar acciones dañinas sobre la información o servicios informáticos.





Backdoor

Secuencia especial dentro del código de programa, por el cual se pueden saltar mecanismo de seguridad (como autenticación) para acceder a un sistema.



Botnet

Ordenadores infectados y controlados por un atacante de forma remota, para explotar sus recursos de procesamiento.

Botnet

29





Ransomware

Secuestra (bloquea) el acceso, al ordenador, unidades de almacenamiento o archivos, utiliza técnicas criptográficas, con el objetivo de solicitar un rescate.

Ransomware

31



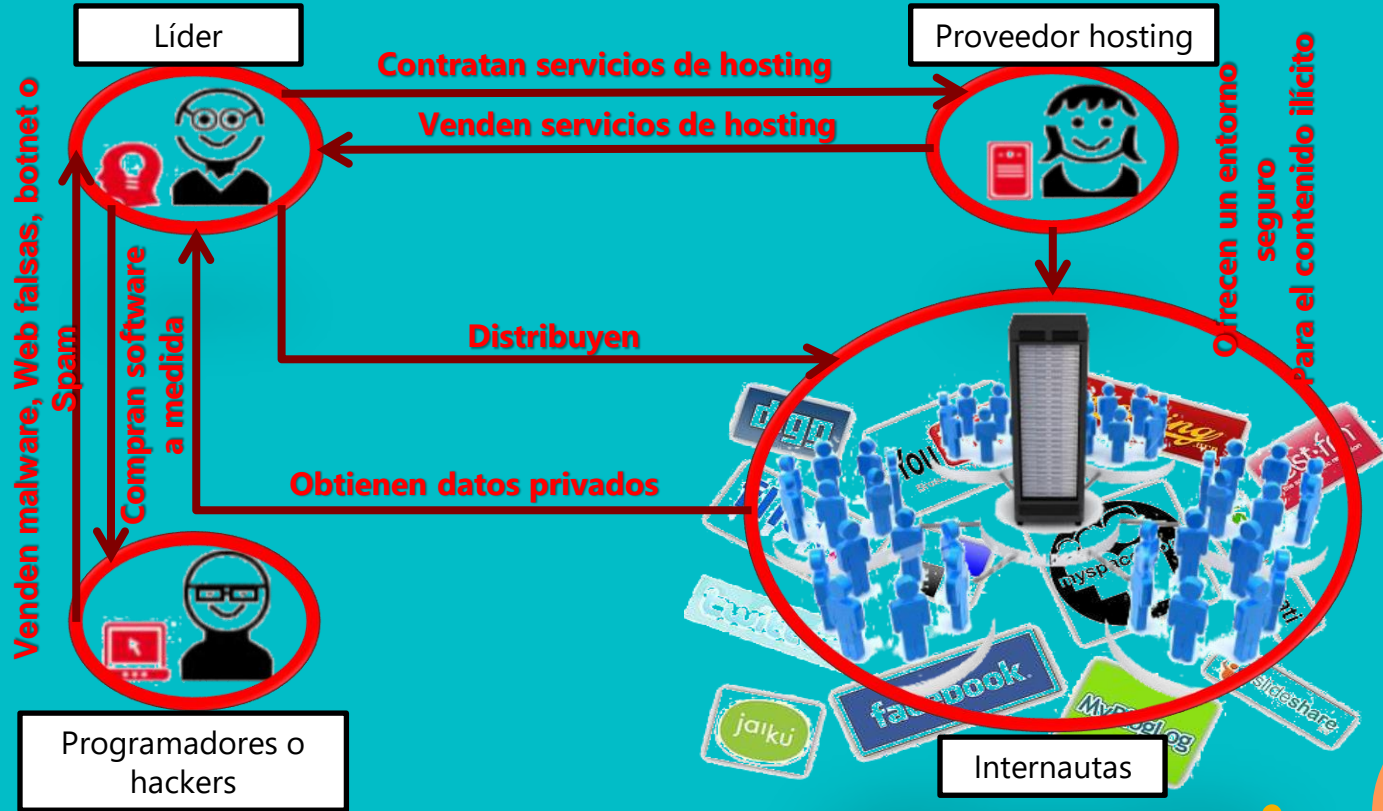


Rootkit

Conjunto de herramientas que esconden los procesos y archivos por el medio de los cuales un intruso mantiene el acceso a un sistema

Ciberdelincuencia

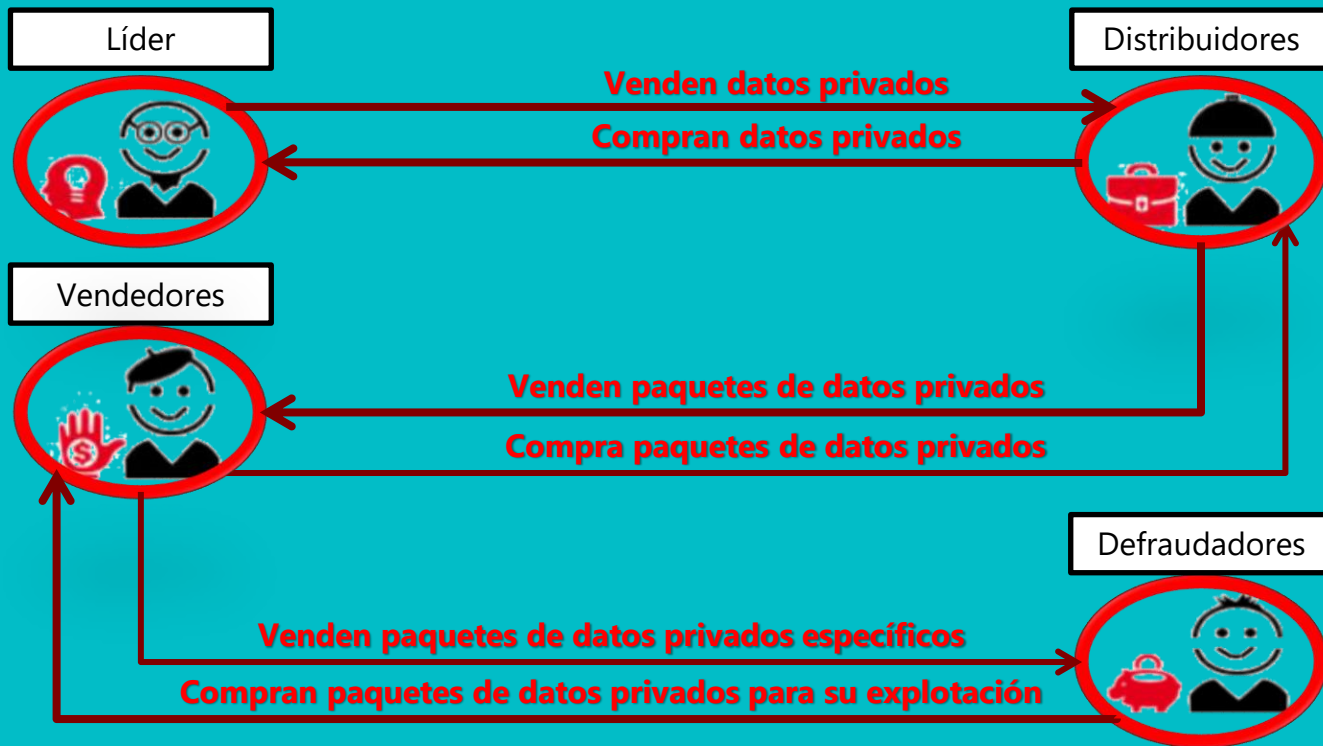
33



Paso 1: Creación de malware y búsqueda de víctimas

Ciberdelincuencia

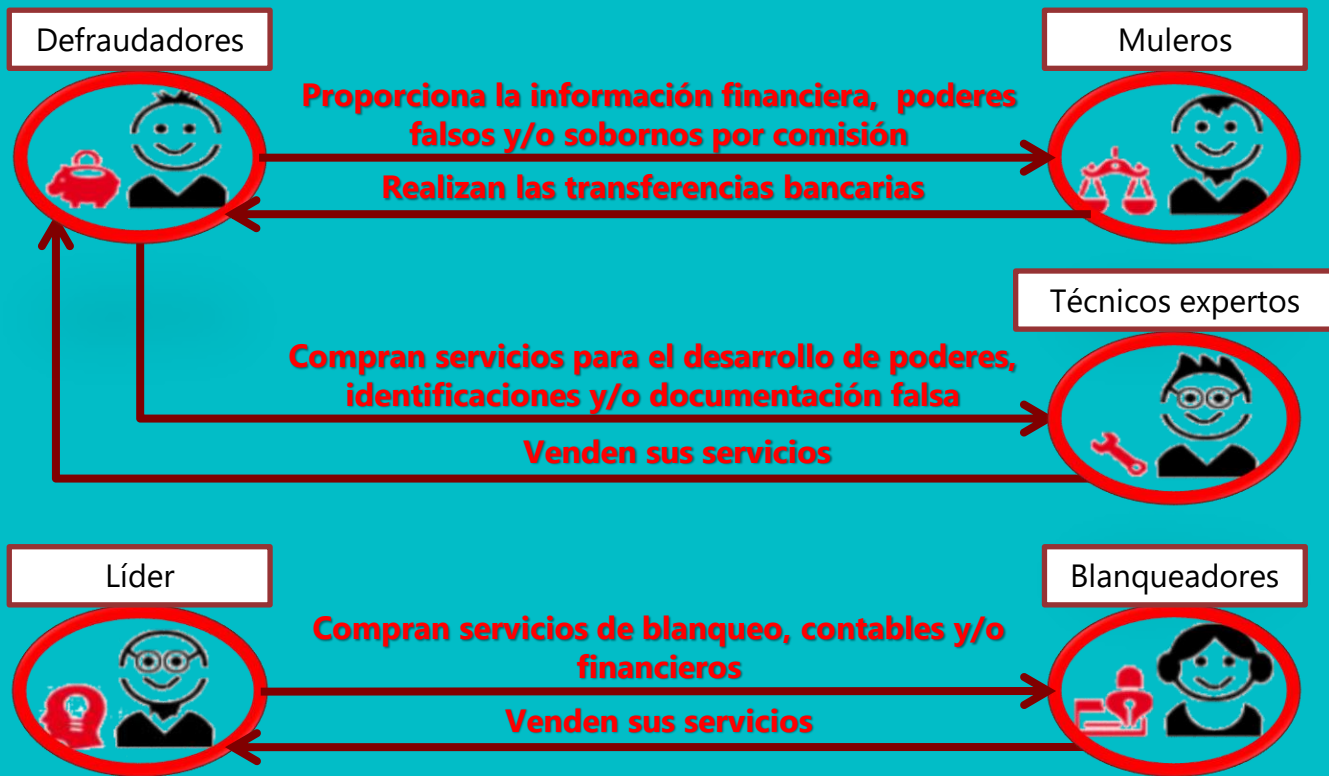
34



Paso 2: Venta de datos privados

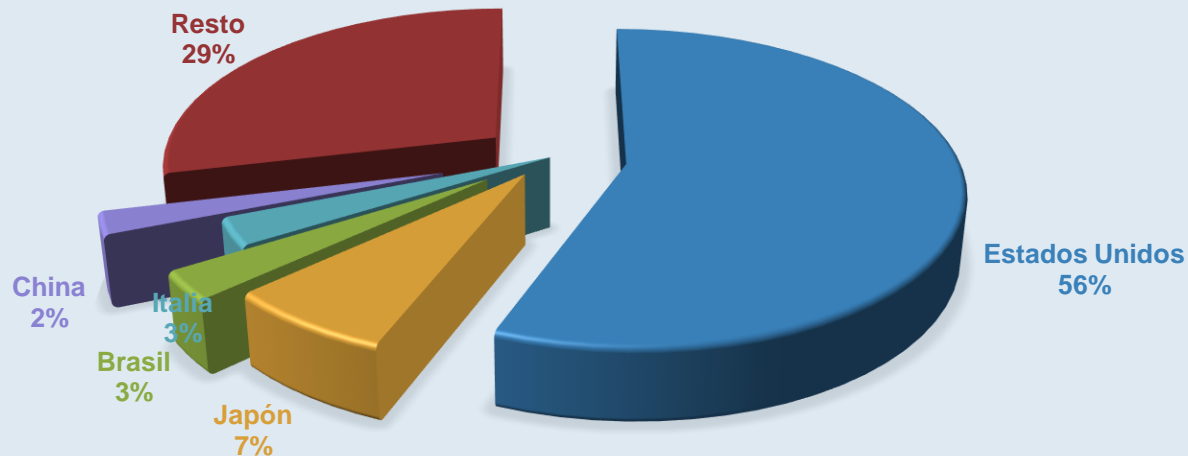
Ciberdelincuencia

35



Paso 3: Blanqueo de dinero

FUENTE CIA WORLD FACTBOOK 2020



Ubicación de Servidores Publicados
en Internet por País




Que es un CVE?

Las vulnerabilidades y exposiciones comunes (CVE), es una forma de publicar e identificar mediante un ID único una lista determinada vulnerabilidades, su descripción, las versiones de software afectadas, posibles soluciones o medidas de mitigación si existen, y otra información de referencia.

El rango de puntuación oscila entre 0 y 10, donde las cifras más altas representan un mayor nivel de gravedad. Muchos proveedores de seguridad crean sus propios sistemas de calificación.







¿Cómo funciona el Sistema CVE?

MITRE Corporation es responsable de gestionar los CVE con el financiamiento de la Agencia de Seguridad de Infraestructura y Ciberseguridad, que forma parte del Departamento de Seguridad Nacional de Estados Unidos.

Los CVE son resumidas y no incluyen datos técnicos ni información sobre riesgos, efectos o soluciones. Ese tipo de información aparece en otras bases de datos, incluidas la National Vulnerability Database de Estados Unidos, la CERT/CC Vulnerability Notes Database y varias listas que mantienen los proveedores y demás empresas fabricantes de software. Los números de identificación de CVE ofrecen a los usuarios una forma confiable de diferenciar cada falla de seguridad en los distintos sistemas.



Fases de un ataque





Dudas y consultas?



tj.alvaro.antezana.m@upds.net.bo



+591 69304565

Este material es facilitado con fines didácticos solo a los estudiantes que cursan alguna asignatura con el autor, su distribución o comercialización sin autorización esta prohibido.

Ing. Alvaro Antezana
ARAM © 2021

