INTRODUCCIÓN AL CIBERDELITO: CONCEPTOS INTRODUCTORIOS

•Ing. Hernán José Zepeda Castro, Master en Ciberseguridad

¿QUÉ ES LA CIBERSEGURIDAD?

Antes de comenzar a hablar de la Seguridad Informática o Ciberseguridad y ciberdelito debemos reconocer algunos conceptos relacionados:

Ciberespacio: Puede decirse que el ciberespacio es una realidad virtual. No se trata de un ámbito físico, que puede ser tocado, sino que es una construcción digital desarrollada con computadoras, En la actualidad, el concepto de ciberespacio suele asociarse a Internet. Todo aquello que se desarrolla en Internet, a través de sitios web, correos electrónicos, redes sociales, etc., no tiene lugar en un país específico, más allá de la ubicación concreta de los servidores y de los usuarios. El ciberespacio, de todos modos, es más amplio que Internet.

¿QUÉ ES LA CIBERSEGURIDAD?

- **Ciberdefensa:** es el conjunto de acciones de defensa activas, pasivas, proactivas y reactivas para asegurar el uso propio del ciberespacio y negarlo al enemigo.
- **Ciberguerra:** conflicto en el ciberespacio.
- **Cibercrimen:** Acción criminal en el Ciberespacio.
- **Ciberterrorismo:** Acción terrorista en el ciberespacio.

¿QUÉ ES LA CIBERSEGURIDAD?

- Es el conjunto de acciones de carácter preventivo que tienen como objeto el asegurar el uso de las redes propias y negarlas a terceros.

¿DIFERENCIA ENTRE DEEP WEB Y DARK WEB?

- El internet que conocemos y en el que navegamos es realmente **una minúscula parte de lo que es en realidad la red.** Para entender esto debemos conocer dos conceptos importantes y su diferencia:

- **Deep Web**

- **Dark Web**

- Términos que desarrollaremos para explicar y entender un poco mas a que nos enfrentamos y que es lo que vemos en la red.

¿DIFERENCIA ENTRE DEEP WEB Y DARK WEB?

- Para entender los conceptos de **Deep y Dark Web** podemos imaginarnos un iceberg en el océano, del iceberg solo podemos ver el 10% fuera del agua y el 90% esta bajo el agua, lo mismo sucede con la web, ese 10% son los sitios web que las personas visitan habitualmente. Se estima son alrededor de 1000 millones de sitios.

- El 10% de lo que vemos en internet se le conoce como **Surface web** es la parte visible del Internet donde todo esta indexado por los buscadores más habituales como Google, Bing o Yahoo. Cualquier persona puede acceder a esta zona con una conexión a internet, sus dominios mas habituales son **.com, .net, .org** etc.

¿DIFERENCIA ENTRE DEEP WEB Y DARK WEB?

- La **Deep Web** es lo contrario a la Surface web, engloba todo lo que no esta indexado en los buscadores habituales, aquí encontramos contenidos variados, desde publicaciones académicas hasta bases de datos y otras informaciones.

- En la **Dark Web** podemos encontrar literalmente de todo, se desconocen todo lo que puede llegar a albergar, tenemos mercados negros donde se venden de forma ilegal drogas o armas, mensajes y foros de organizaciones terroristas, se pueden contratar servicios de hackers, comprar documentación falsa, sitios para robar nuestros datos o pornografía (tristemente con una gran parte infantil).

SURFACE, DEEP Y DARK WEB

¿QUÉ PROTEGE LA CIBERSEGURIDAD?

- La Seguridad Informática o ciberseguridad protege tanto a nivel personal como corporativo lo siguiente:

- A nivel personal protege:

- La identidad
- Datos personales y,
- Dispositivos informáticos.

¿QUÉ PROTEGE LA CIBERSEGURIDAD?

- A nivel corporativo protege:
- La reputación, los datos y los clientes de la organización.
- A nivel de estado protege:
- La seguridad nacional y,
- La seguridad y bienestar de los ciudadanos.

IDENTIDAD EN LÍNEA Y FUERA DE LÍNEA.

- Primeramente definamos identidad fuera de línea: esa es la persona con la que sus amigos, compañeros y familiares interactúan a diario en el hogar, universidad u oficina.

- La identidad en línea es quien es usted en el ciberespacio, es como se presenta usted ante otros en línea, la cual solo debería revelar una cantidad limitada de información sobre usted.

DISPOSITIVOS INFORMÁTICOS

Sus dispositivos informáticos no solo almacenan sus datos. Ahora estos dispositivos se han convertido en el portal a sus datos y generan información sobre usted.

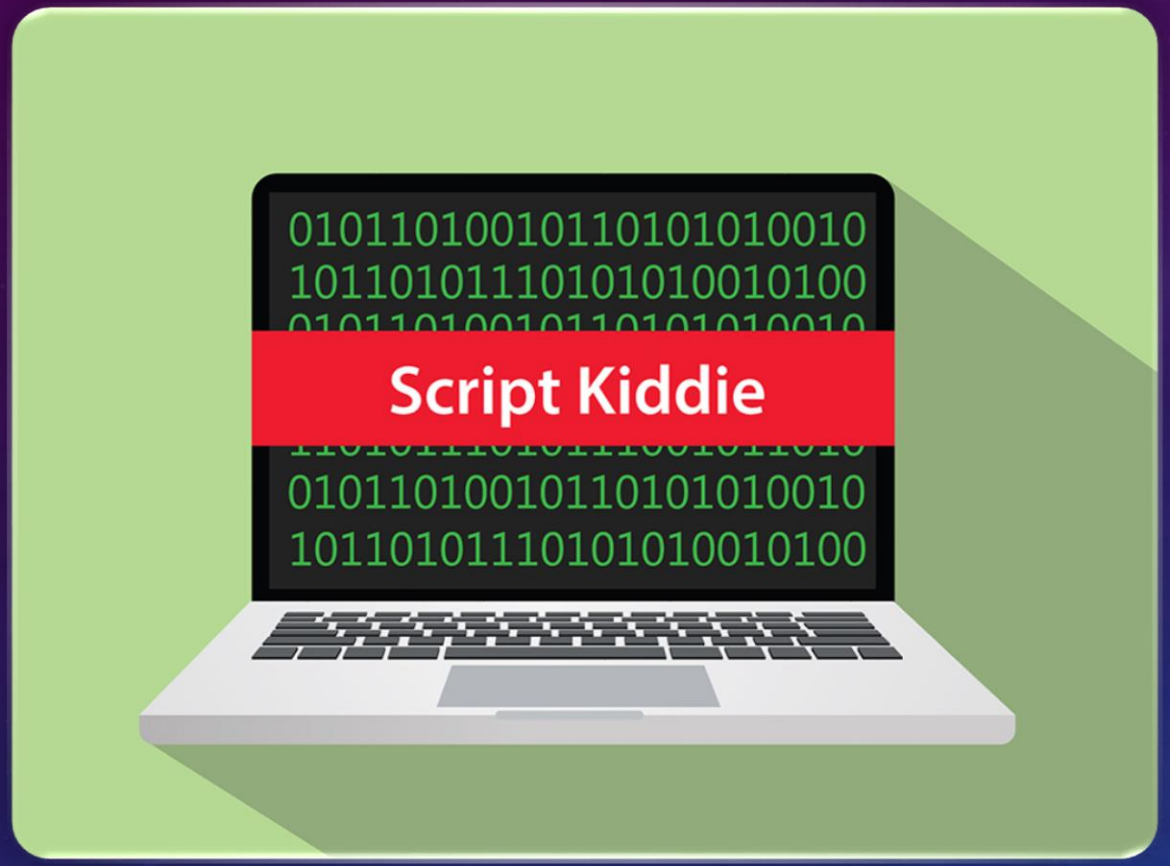
¿CUÁLES SON LOS DATOS IMPORTANTES PARA LOS DELINCUENTES?

- Para los delincuentes cibernéticos todo lo que tenga valor para usted en línea, ellos lo quieren.

- Empecemos por las credenciales en línea, con esta credenciales los delincuentes tendrán acceso a todas nuestras cuentas, los ciberdelincuentes son sumamente creativos, harán de todo para robar no solo su dinero, también su identidad y arruinarle la vida.

TIPOS DE ATACANTES

- Los atacantes son personas o grupos que intentan aprovechar las vulnerabilidades para obtener una ganancia personal o financiera. Los atacantes están interesados en todo, desde las tarjetas de crédito hasta los diseños de producto y todo lo que tenga valor.



TIPOS DE ATACANTES

- Aficionados: a veces, se denominan Script Kiddies. Generalmente, son atacantes con poca o ninguna habilidad que, a menudo, utilizan las herramientas existentes o las instrucciones que se encuentran en Internet para llevar a cabo ataques. Algunos de ellos solo son curiosos, mientras que otros intentan demostrar sus habilidades y causar daños. Pueden utilizar herramientas básicas, pero los resultados aún pueden ser devastadores.

TIPOS DE ATACANTES

- Hackers: este grupo de atacantes ingresa a computadoras o redes para obtener acceso. Según la intención de la intrusión, estos atacantes se clasifican como de sombrero blanco, gris o negro.

TIPOS DE ATACANTES

- Hackers organizados: estos hackers incluyen organizaciones de delincuentes cibernéticos, hacktivistas, terroristas y hackers patrocinados por el estado. Los delincuentes cibernéticos generalmente son grupos de delincuentes profesionales centrados en el control, el poder y la riqueza. Los delincuentes son muy sofisticados y organizados, e incluso pueden proporcionar el delito cibernético como un servicio a otros delincuentes

TIPOS DE ATACANTES

- Los hacktivistas hacen declaraciones políticas para concientizar sobre los problemas que son importantes para ellos. Los atacantes patrocinados por el estado reúnen inteligencia o causan daño en nombre de su gobierno. Estos atacantes suelen estar altamente capacitados y bien financiados, y sus ataques se centran en objetivos específicos que resultan beneficiosos para su gobierno.

HACKERS SOMBRERO BLANCO O WHITE HAT

- Son hackers que utilizan sus habilidades de programación para fines buenos, éticos y legales. Los hackers de sombrero blanco pueden realizar pruebas de penetración de redes con la finalidad de comprometer los sistemas y las redes usando sus conocimientos de los sistemas de seguridad informática para descubrir las vulnerabilidades de la red.

HACKERS SOMBRERO BLANCO O WHITE HAT

- Las vulnerabilidades en la seguridad se informan a los desarrolladores para que las corrijan antes de que puedan ser amenazadas. Algunas organizaciones otorgan premios o recompensas a los hackers de sombrero blanco cuando informan una vulnerabilidad.

HACKERS SOMBRERO GRIS O GREY HAT

- Son personas que cometen delitos y hacen cosas probablemente poco éticas, pero no para beneficio personal o ni para causar daños.
- Un ejemplo sería alguien que pone en riesgo una red sin permiso y luego divulga la vulnerabilidad públicamente.

HACKERS SOMBRERO GRIS O GREY HAT

- Un hacker de sombrero gris puede divulgar una vulnerabilidad a la organización afectada después de haber puesto en peligro la red. Esto permite que la organización solucione el problema.

HACKERS SOMBRERO NEGRO O BLACK HAT

- Son delincuentes poco éticos que violan la seguridad de una computadora y una red para beneficio personal o por motivos maliciosos, como ataques a la red.
- Los hackers de sombrero negro atacan las vulnerabilidades para comprometer la computadora y los sistemas de red.

•TIPOS DE AMENAZAS

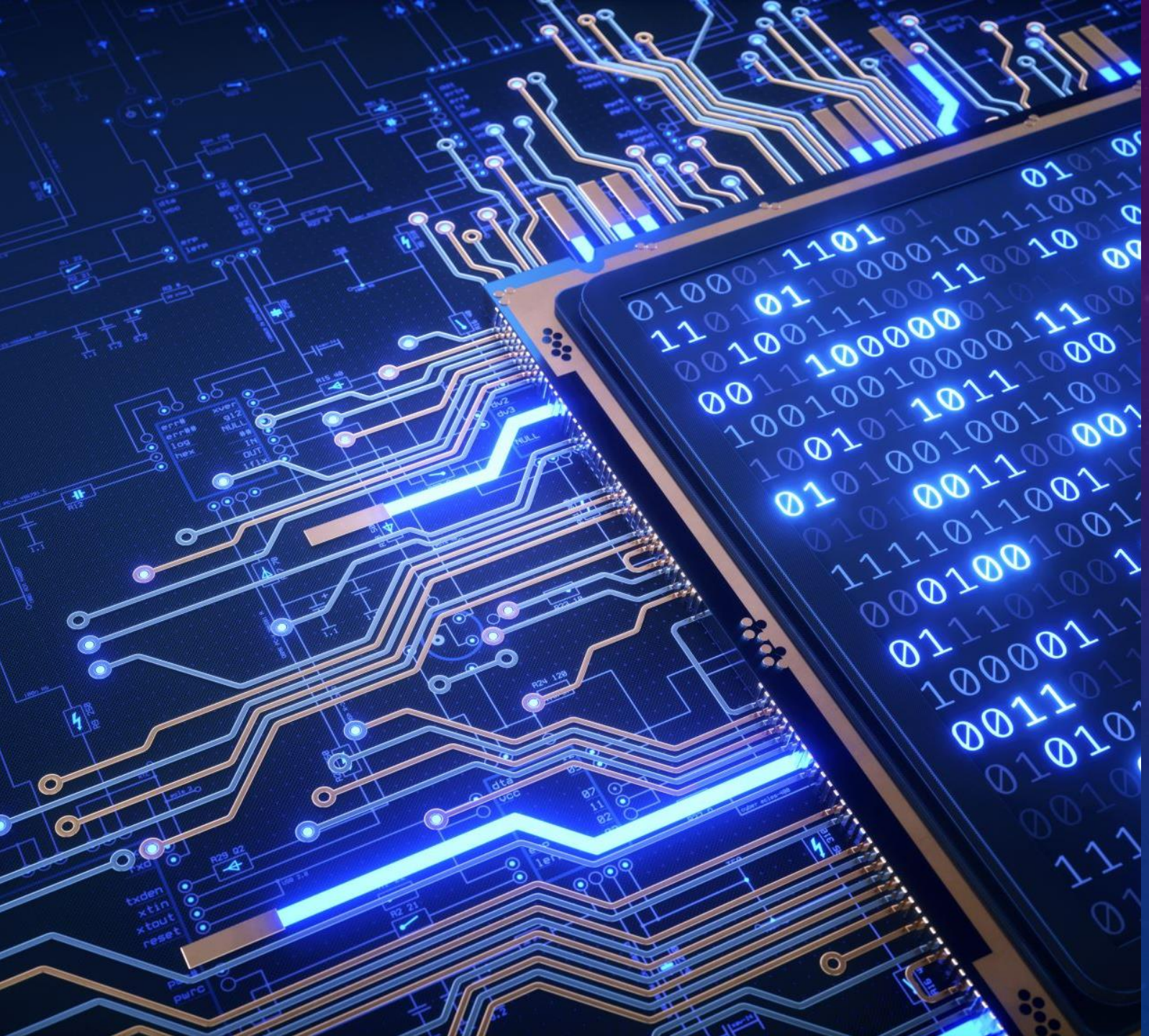
AMENAZAS DE SEGURIDAD INTERNAS

Los ataques pueden originarse dentro de una organización o fuera de ella, Un usuario interno, como un empleado o un asociado contratado, puede de manera accidental o intencional, como ser:

- Manipular de manera incorrecta los datos confidenciales.
- Amenazar las operaciones de los servidores internos o de los dispositivos de la infraestructura de red.
- Facilitar los ataques externos al conectar medios USB infectados al sistema informático corporativo.

AMENAZAS DE SEGURIDAD INTERNAS

- Invitar accidentalmente al malware a la red con correos electrónicos o páginas web maliciosos.
- Las amenazas internas también tienen el potencial de generar mayor daño que las amenazas externas, porque los usuarios internos tienen acceso directo al edificio y a sus dispositivos de infraestructura. Los empleados también tienen conocimiento de la red corporativa, sus recursos y sus datos confidenciales, así como diferentes niveles de usuario o privilegios administrativos.



AMENAZAS DE SEGURIDAD EXTERNAS

- Las amenazas externas de aficionados o atacantes expertos pueden atacar las vulnerabilidades en la red o los dispositivos informáticos, o usar la ingeniería social para obtener acceso.

ATAQUES, CONCEPTOS Y TÉCNICAS

- La mayoría de los ciberataques modernos se consideran ataques combinados. Los ataques combinados usan varias técnicas para infiltrarse en un sistema y atacarlo. Cuando un ataque no puede evitarse, es el trabajo del profesional de ciberseguridad reducir el impacto de dicho ataque

BÚSQUEDA DE VULNERABILIDADES DE SEGURIDAD

- Las vulnerabilidades de seguridad son cualquier tipo de defecto en software o hardware. Después de obtener conocimientos sobre una vulnerabilidad, los usuarios malintencionados intentan explotarla.

- Un ataque es el término que se utiliza para describir un programa escrito para aprovecharse de una vulnerabilidad conocida. El acto de aprovecharse de una vulnerabilidad se conoce como ataque. El objetivo del ataque es acceder a un sistema, los datos que aloja o recursos específicos.

VULNERABILIDADES DE SOFTWARE

- Las vulnerabilidades de software generalmente se introducen por errores en el sistema operativo o el código de aplicación; a pesar de todos los esfuerzos realizados por las empresas para encontrar y corregir las vulnerabilidades, es común que surjan nuevas vulnerabilidades.

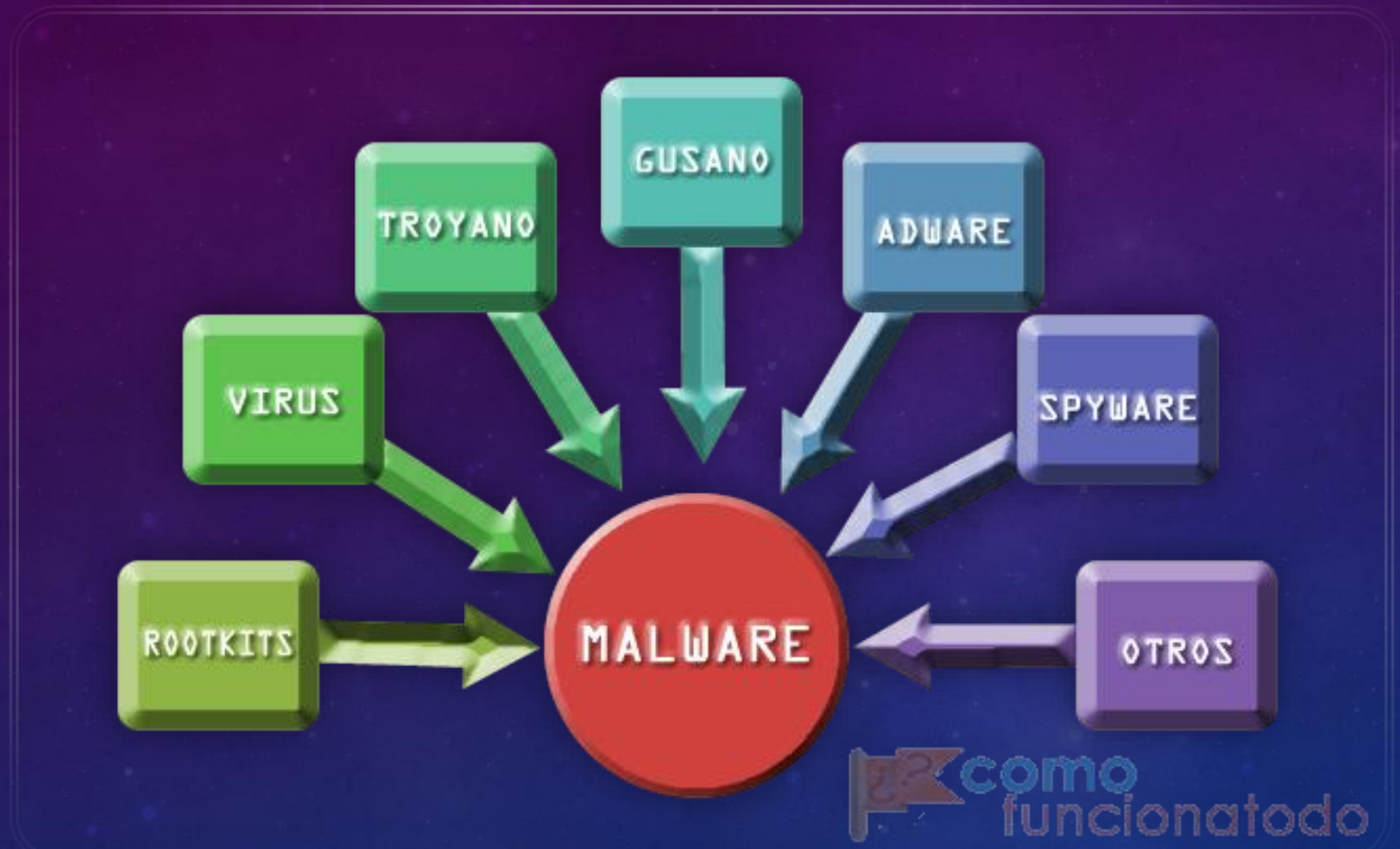
VULNERABILIDADES DE HARDWARE

- Las vulnerabilidades de hardware se presentan a menudo mediante defectos de diseño del hardware.

MALWARE

- Acrónimo para el software malicioso, malware es cualquier código que pueda utilizarse para robar datos, evitar los controles de acceso, ocasionar daños o comprometer un sistema

TIPOS DE MALWARE



- A continuación, veremos algunos tipos comunes de malware:

TIPOS DE MALWARE

- **Spyware:** este malware está diseñado para rastrear y espiar al usuario. El spyware a menudo incluye rastreadores de actividades, recopilación de pulsaciones de teclas y captura de datos. En el intento por superar las medidas de seguridad, el spyware a menudo modifica las configuraciones de seguridad. El spyware con frecuencia se agrupa con el software legítimo o con caballos troyanos.

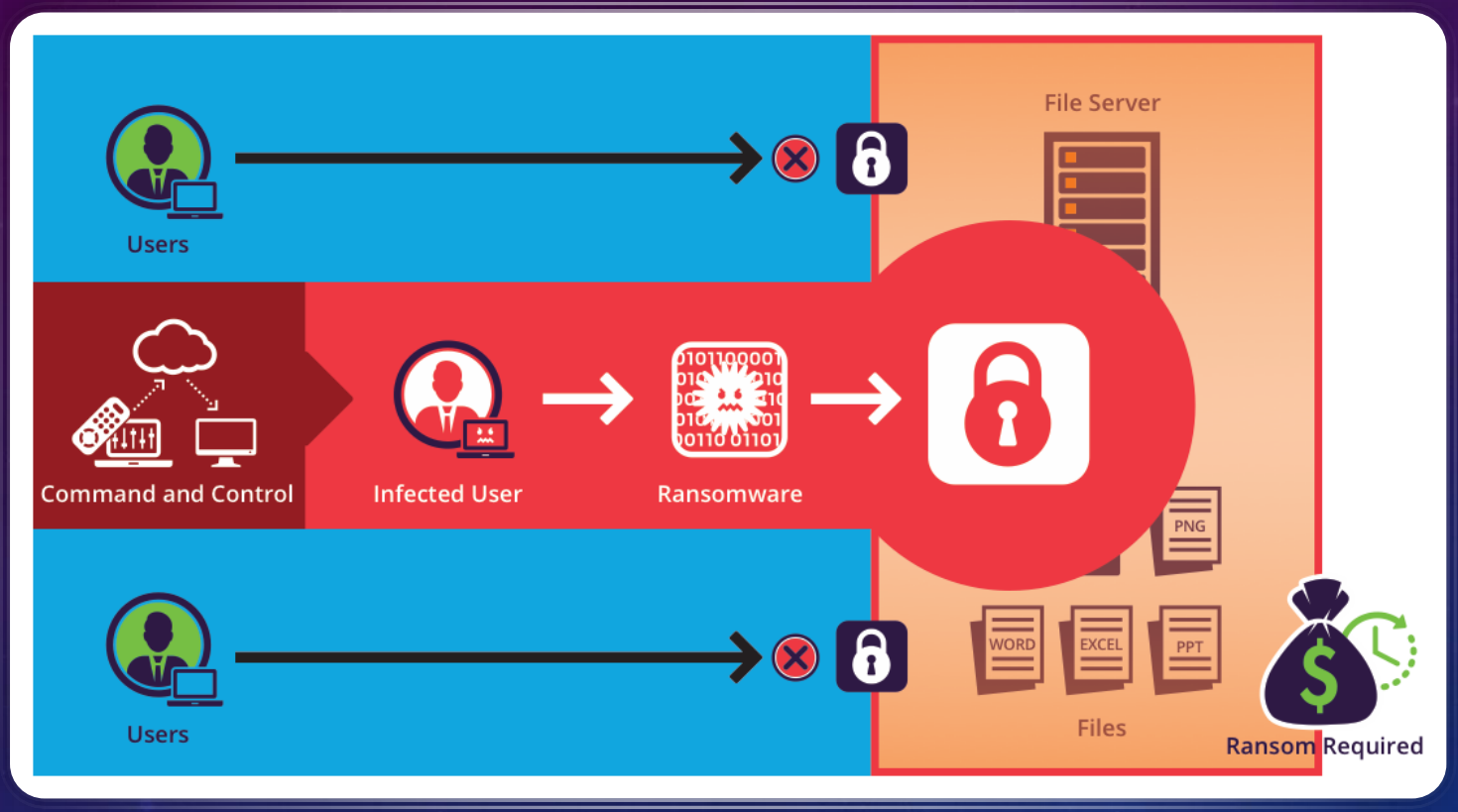
TIPOS DE MALWARE

- **Adware:** el software de publicidad está diseñado para brindar anuncios automáticamente. El adware a veces se instala con algunas versiones de software. Algunos adware están diseñados para brindar solamente anuncios, pero también es común que el adware incluya spyware.

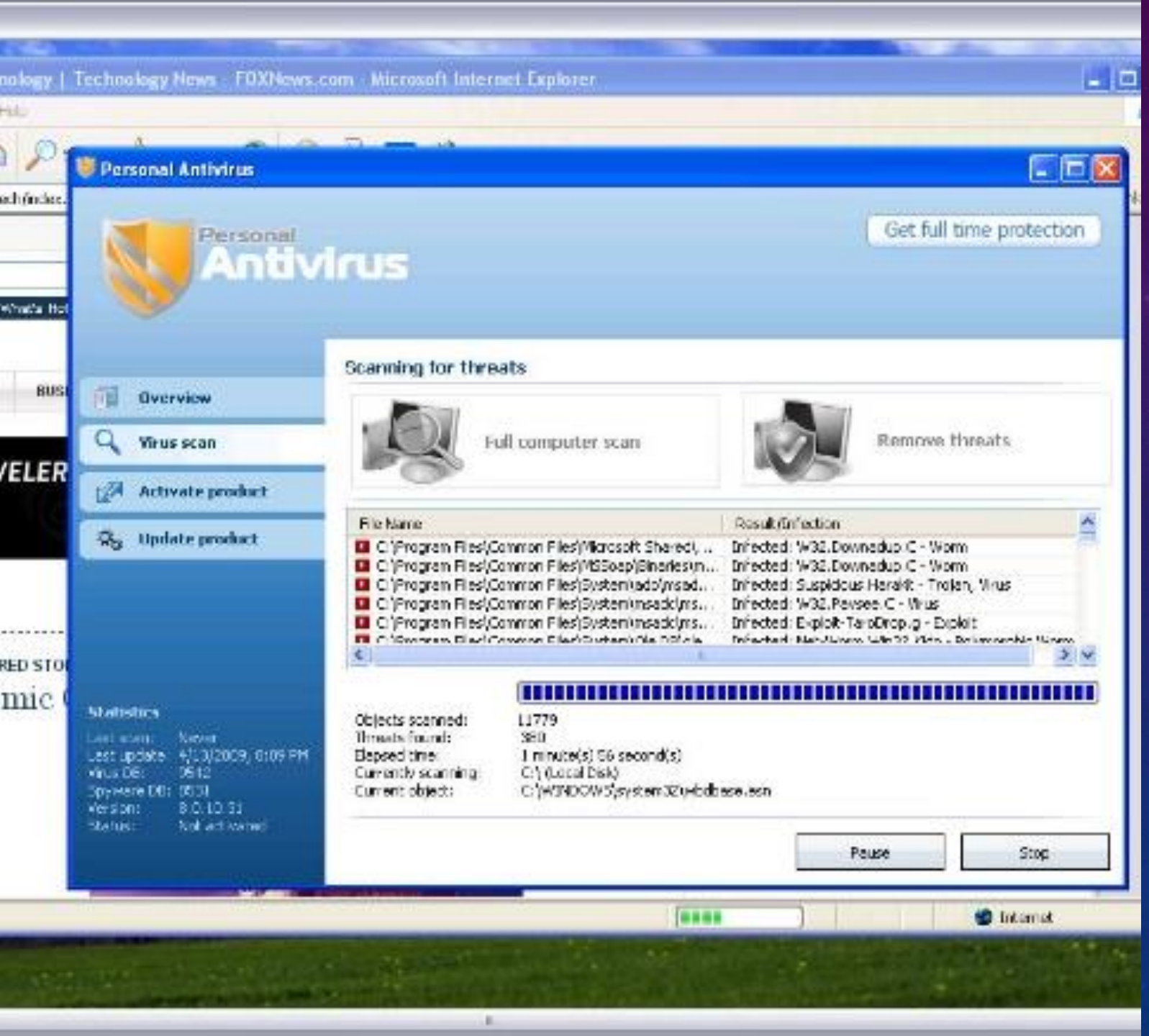
TIPOS DE MALWARE

- **Bot:** de la palabra robot, un bot es un malware diseñado para realizar acciones automáticamente, generalmente en línea. Si bien la mayoría de los bots son inofensivos, un uso cada vez más frecuente de bots maliciosos es el de los botnets. Varias computadoras pueden infectarse con bots programados para esperar silenciosamente los comandos provistos por el atacante.

TIPOS DE MALWARE



Ransomware: Este malware está diseñadp ára mantener captivo un sistema de computación o los datos que contiene hasta que se realice un pago. El ransomware trabaja generalmente encriptando los datos de la computadora con una clave desconocida para el usuario.



TIPOS DE MALWARE

- Scareware: Este tipo de malware esta diseñando para persuadir al usuario de realizar acciones especificas en función del temor. El scareware falsifica ventanas emergentes que se asemejan a las ventanas de dialogo del sistema operativo.
- Estas ventanas muestran mensajes falsificados que indican que el sistema está en riesgo o necesita la ejecución de un programa especifico para volver al funcionamiento normal. En realidad, no se evaluó ni detecto ningun problema y si el usuario acepta y autoriza la ejecución del programa mencionado, el sistema se infecta con malware

TIPOS DE MALWARE

- Rootkit: Este malware está diseñado para modificar el sistema operativo a fin de crear una puerta trasera. Los atancates luego utilizan la puerta trasera para acceder a la computadora de forma remota.
- La mayoría de los rootkits aprovecha las vulnerabilidades de software para realizar el escalamiento de privilegios y modificar los archivos del sistema.

TIPOS DE MALWARE

- **Virus:** un virus es un código ejecutable malintencionado que se adjunta a otros archivos ejecutables, generalmente programas legítimos. La mayoría de los virus requiere la activación del usuario final y puede activarse en una fecha o un momento específico.

- Los virus pueden ser inofensivos y simplemente mostrar una imagen o pueden ser destructivos, como los que modifican o borran datos.

TIPOS DE MALWARE

Tipos de Virus Informáticos

Virus de Arranque
Se ejecutan cuando se enciende la computadora, dañando o borrando información.

Troyanos
Entran al software de la computadora como un programa inofensivo, causando daño a los archivos o robando datos.

Gusanos
Tienen la característica que se copian por sí mismos y se expanden o distribuyen por Internet.

Bomba de tiempo
Virus informático que permanece inofensivo y se activa hasta que se cumpla una condición determinada. Puede ser una fecha, ejecutar un programa o realizar una combinación de teclas.

TIPOS DE MALWARE

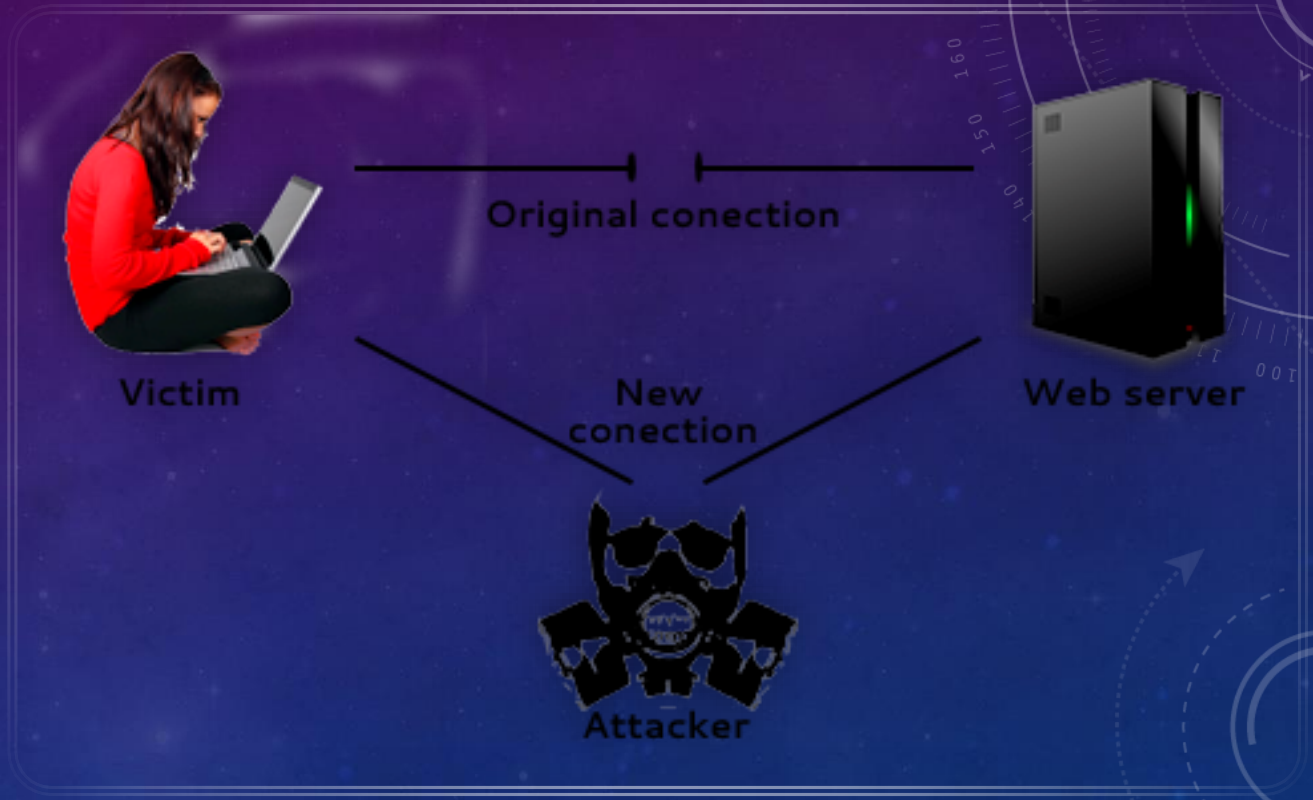
- **Troyano:** un troyano es malware (Virus) que ejecuta operaciones maliciosas bajo la apariencia de una operación deseada. Este código malicioso ataca los privilegios de usuario que lo ejecutan.
- A menudo, los troyanos se encuentran en archivos de imagen, archivos de audio o juegos. Un troyano se diferencia de un virus en que se adjunta a archivos no ejecutables.

TIPOS DE MALWARE

- **Gusanos:** los gusanos son códigos maliciosos que se replican mediante la explotación independiente de las vulnerabilidades en las redes. Los gusanos, por lo general, ralentizan las redes. Mientras que un virus requiere la ejecución de un programa del host, los gusanos pueden ejecutarse por sí mismos.

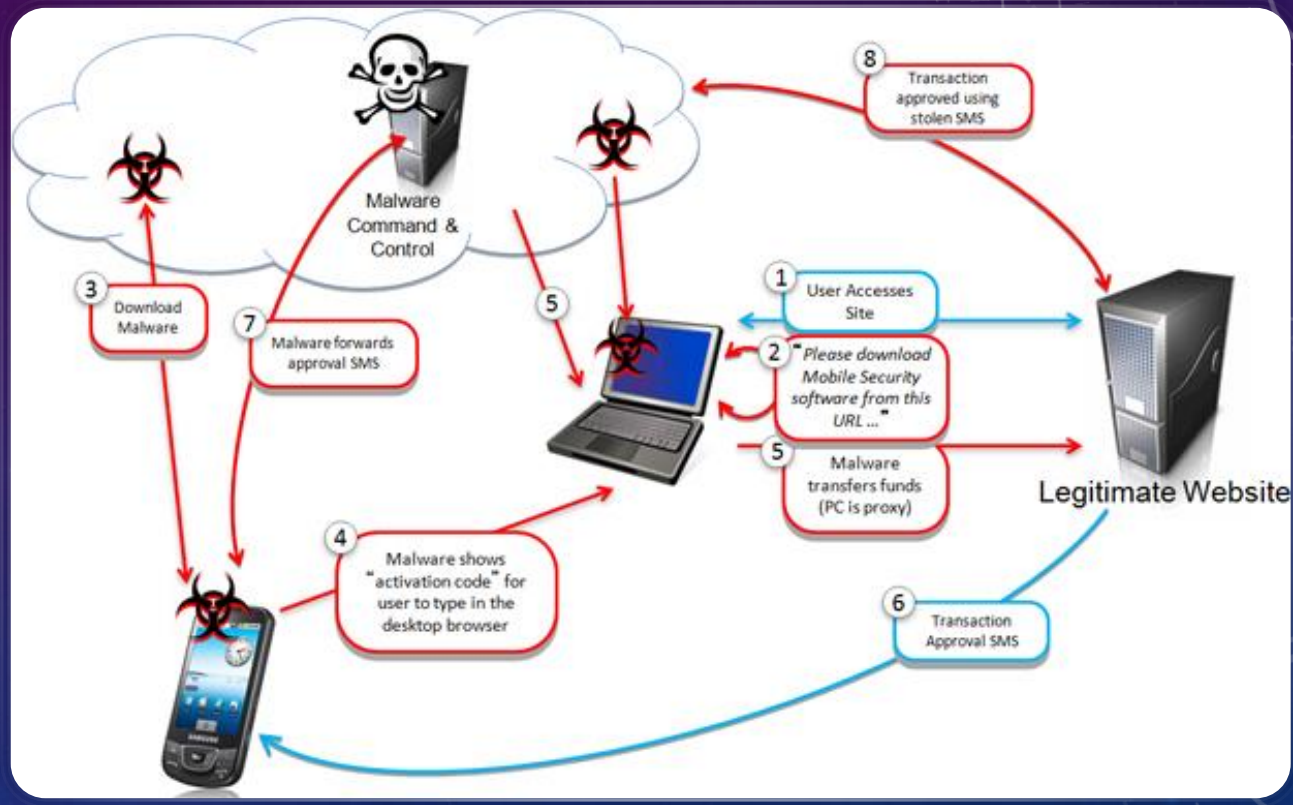
TIPOS DE MALWARE

- **Hombre en el medio (MitM):** el MitM permite que el atacante tome el control de un dispositivo sin el conocimiento del usuario. Con ese nivel de acceso, el atacante puede interceptar y capturar información sobre el usuario antes de retransmitirla a su destino. Los ataques MitM se usan ampliamente para robar información financiera. Existen muchas técnicas y malware para proporcionar capacidades de MitM a los atacantes.



TIPOS DE MALWARE

- **Hombre en el móvil (MitMo):** una variación del hombre en el medio, el MitMo es un tipo de ataque utilizado para tomar el control de un dispositivo móvil. Cuando está infectado, puede ordenarse al dispositivo móvil que exfiltre información confidencial del usuario y la envíe a los atacantes. ZeuS, un ejemplo de ataque con capacidades de MitMo, permite que los atacantes capturen silenciosamente SMS de verificación de 2 pasos enviados a los usuarios.



SÍNTOMAS DE MALWARE

- Independientemente del tipo de malware con el que se ha infectado un sistema, estos son síntomas frecuentes de malware:

- Aumento del uso de la CPU.
- Disminución de la velocidad de la computadora.
- La computadora se congela o falla con frecuencia.
- Hay una disminución en la velocidad de navegación web.
- Existen problemas inexplicables con las conexiones de red.
- Se modifican los archivos.
- Se eliminan archivos.
- Hay una presencia de archivos, programas e iconos de escritorio desconocidos.
- Se ejecutan procesos desconocidos.
- Los programas se cierran o reconfiguran solos.
- Se envían correos electrónicos sin el conocimiento o el consentimiento del usuario.

ATAQUES

INGENIERÍA SOCIAL

- La ingeniería social es un ataque de acceso que intenta manipular a las personas para que realicen acciones o divulguen información confidencial. Los ingenieros sociales con frecuencia dependen de la disposición de las personas para ayudar, pero también se aprovechan de sus vulnerabilidades.
- Por ejemplo, un atacante puede llamar a un empleado autorizado con un problema urgente que requiere acceso inmediato a la red. El atacante podría apelar a la vanidad del empleado, invocar a la autoridad usando técnicas de intimidación por nombres o apelar a la codicia del empleado.

EJEMPLOS DE INGENIERÍA SOCIAL

- **Pretexto:** esto es cuando un atacante llama a una persona y miente en el intento de obtener acceso a datos privilegiados. Un ejemplo implica a un atacante que pretende necesitar datos personales o financieros para confirmar la identidad del objetivo.

- **Seguimiento:** esto es cuando un atacante persigue rápidamente a una persona autorizada a un lugar seguro.

- **Algo por algo (quid pro quo):** esto es cuando un atacante solicita información personal de una parte a cambio de algo, por ejemplo, un obsequio.

DECODIFICACIÓN DE CONTRASEÑAS WI-FI

- La decodificación de contraseñas Wi-Fi es el proceso de detección de la contraseña utilizada para proteger la red inalámbrica.

DECODIFICACIÓN DE CONTRASEÑAS WI-FI

Estas son algunas técnicas utilizadas en la decodificación de contraseñas:

Ingeniería social: el atacante manipula a una persona que conoce la contraseña para que se la proporcione

DECODIFICACIÓN DE CONTRASEÑAS WI-FI

- **Ataques por fuerza bruta:** el atacante prueba diversas contraseñas posibles en el intento de adivinar la contraseña. Si la contraseña es un número de 4 dígitos, por ejemplo, el atacante deberá probar cada una de las 10 000 combinaciones

DECODIFICACIÓN DE CONTRASEÑAS WI-FI

- **Monitoreo de la red:** mediante la escucha y la captura de paquetes enviados por la red, un atacante puede descubrir la contraseña, si la contraseña se envía sin cifrar (en texto plano). Si la contraseña está cifrada, el atacante aún puede revelarla mediante una herramienta de decodificación de contraseñas.

SUPLANTACIÓN DE IDENTIDAD

- La suplantación de identidad es cuando una persona maliciosa envía un correo electrónico fraudulento disfrazado como fuente legítima y confiable. El objetivo de este mensaje es engañar al destinatario para que instale malware en su dispositivo o comparta información personal o financiera. Un ejemplo de suplantación de identidad es un correo electrónico falsificado similar al enviado por una tienda de conveniencia que solicita al usuario que haga clic en un enlace para reclamar un premio. El enlace puede ir a un sitio falso que solicita información personal o puede instalar un virus.

APROVECHAMIENTO DE VULNERABILIDADES

EL APROVECHAMIENTO DE VULNERABILIDADES ES OTRO MÉTODO COMÚN DE INFILTRACIÓN.

LOS ATACANTES ANALIZAN LAS COMPUTADORAS PARA OBTENER INFORMACIÓN.

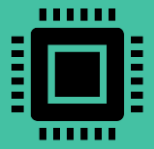
DOS

- Los ataques de denegación de servicio (DoS) son un tipo de ataque a la red. Un ataque DoS da como resultado cierto tipo de interrupción del servicio de red a los usuarios, los dispositivos o las aplicaciones.

DOS

Existen dos tipos principales de ataques DoS:

Cantidad abrumadora de tráfico: esto ocurre cuando se envía una gran cantidad de datos a una red, a un host o a una aplicación a una velocidad que no pueden administrar. Esto ocasiona una disminución de la velocidad de transmisión o respuesta o una falla en un dispositivo o servicio.



Paquetes maliciosos formateados: esto sucede cuando se envía un paquete malicioso formateado a un host o una aplicación y el receptor no puede manejarlo. Por ejemplo, un atacante envía paquetes que contienen errores que las aplicaciones no pueden identificar o reenvía paquetes incorrectamente formateados. Esto hace que el dispositivo receptor se ejecute muy lentamente o se detenga.

- **DDoS**

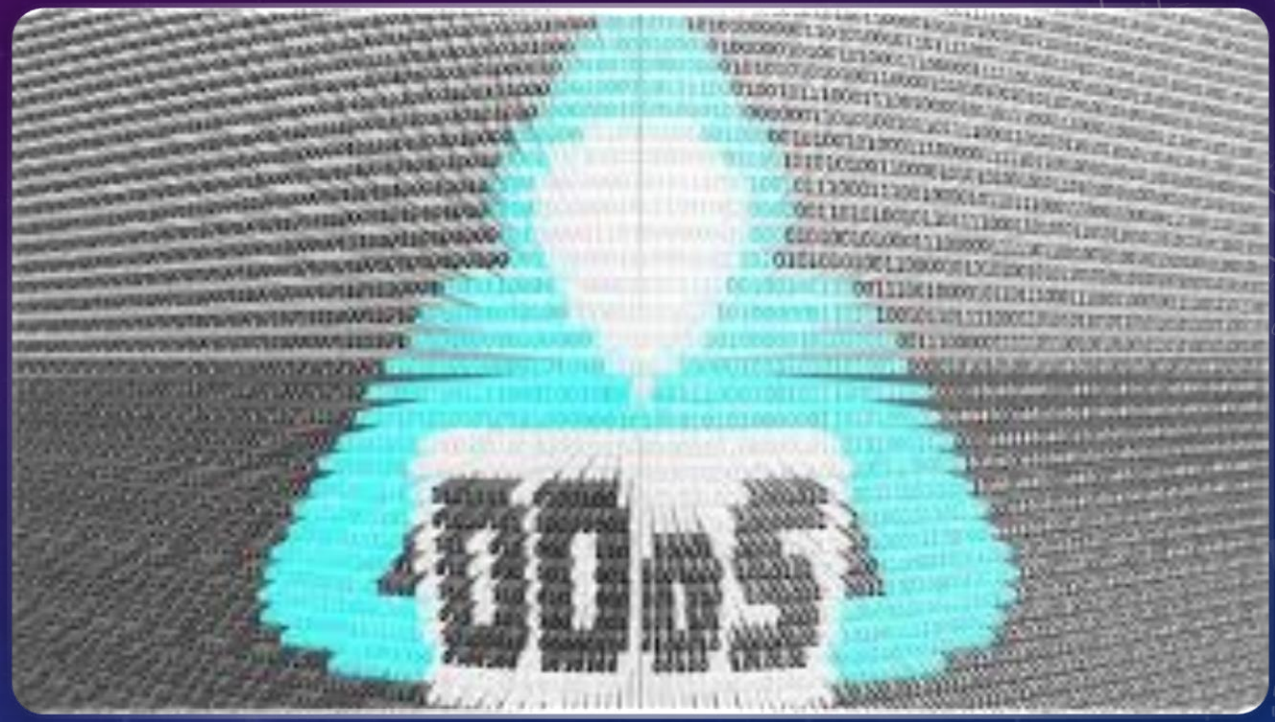
Un ataque DoS distribuido (DDoS) es similar a un ataque DoS pero proviene de múltiples fuentes coordinadas

DDoS

Por ejemplo, un ataque DDoS podría darse de la siguiente manera:

Un atacante crea una red de hosts infectados, denominada botnet. Los hosts infectados se denominan zombies. Los zombies son controlados por sistemas manipuladores.

Las computadoras zombie constantemente analizan e infectan más hosts, lo que genera más zombies. Cuando está listo, el hacker proporciona instrucciones a los sistemas manipuladores para que los botnet de zombies lleven a cabo un ataque DDoS.



ATAQUE COMBINADO

- Los ataques combinados son ataques que usan diversas técnicas para comprometer un objetivo. Mediante el uso de varias técnicas de ataque simultáneas, los atacantes tienen malware que combina gusanos, troyanos, spyware, registradores de pulsaciones, spam y esquemas de suplantación de identidad. Esta tendencia de ataques combinados revela malware más complejo y pone los datos de los usuarios en gran riesgo.

MUCHAS GRACIAS POR SU ATENCIÓN