SOFTWARE ANTIMALWARE

Sistemas Informáticos, 1º DAW

Rubén Bellón, Sergio Bravo, Miguel Ángel Cuadrado
EFA MORATALAZ

SISTEMAS INFORMATICOS.

SOFTWARE ANTI-MALWARE

Índice:

 Rubén Bellón, Sergio Bravo, Miguel Ángel Cuadrado.

1. Introducción.

Muy buenos días a todos, hoy mis compañeros y yo os vamos a exponer nuestro proyecto sobre los Software Anti-Malware el cual daremos los siguientes puntos relacionados con este tema con sus correspondientes videos y explicaciones.

1. ¿Qué es un Software Anti-Malware?
2. ¿Qué es un Malware?
3. Tipos de Malware.
4. Como prevenir el Malware.
5. Como puedo protegerme ante un Malware.
6. Curiosidades.

2. ¿Qué es un Software Anti-Malware?

Se conoce como software antimalware a un tipo de programa o código creado para proteger los sistemas informáticos y los ordenadores personales contra software malicioso o “malware”.

Estos programas antimalware escanean el sistema informático para prevenir, detectar y eliminar el malware.

A continuación, expondremos los tipos más corrientes de Malware y cómo combatirlos.

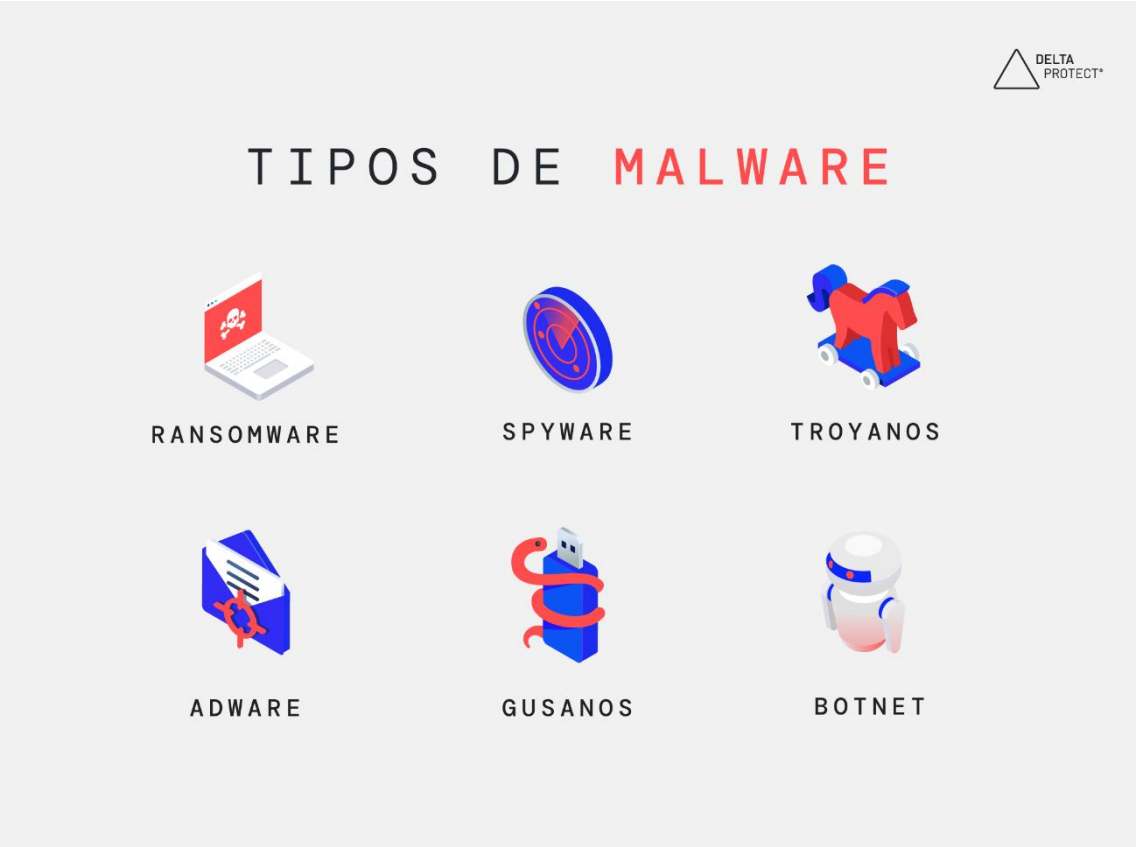
3. ¿Qué es un Malware?

Un "*Malware*" o "*software malicioso*" es un término que describe cualquier programa o código que es dañino para los sistemas.

El "*Malware*" hostil, intrusivo e intencionadamente malicioso intenta invadir, dañar o deshabilitar ordenadores, sistemas informáticos, redes, aunque también pueden estar destinados a alterar o suprimir funciones de nuestro sistema e incluso a recabar información de nuestros equipos.

Hay diferentes tipos de malware, y cada uno infecta o corrompe dispositivos de forma distinta, pero todas las variantes de malware están diseñadas para poner en peligro la seguridad y privacidad de los sistemas informáticos.

A continuación, expondremos los softwares más conocidos y sus características.



4. Tipos de Malware.

a. Phishing:

¿Qué es el phishing?

El Phishing es una técnica de ingeniería social que consiste en enviar correos electrónicos que suplantan la identidad de compañías u organizaciones públicas que solicitan información personal y bancaria de los afectados, logrando conseguir cierta información.
Estos ataques son los más conocidos y en los que más cae la gente, y puede afectar muy negativamente a la persona que cae en esta trampa.

¿Cómo se desarrolla un ataque phishing?

Un ataque de este tipo comienza cuando recibimos un correo, o mensaje en el que una supuesta legítima empresa nos advierte de un problema con nuestra cuenta, con algún pedido o con alguna información faltante para completar una transacción. Suelen ofrecer un link directo a la página de la empresa para que introduzcamos los datos que nos piden, y si accedemos al link, la página es similar o incluso idéntica a la de la empresa, lo que hace que sea difícil darse cuenta de que es un engaño. También hay casos más fáciles de descubrir, como los famosos anuncios que aseguran que hemos ganado un

teléfono móvil o un gran premio y sólo tenemos que introducir nuestros datos en un formulario.

¿Qué objetivo tiene este ataque?

El principal objetivo es recabar algo de información, datos bancarios, información personal (nombre y apellidos, número del DNI, dirección de correo, dirección de nuestra casa,). Una vez los ciberdelincuentes tienen nuestra información, pueden usarla para realizar acciones, normalmente que impliquen gastos monetarios, haciéndose pasar por nosotros. También pueden vender nuestros datos a empresas, y podemos recibir correos basura o anuncios en exceso.

¿Cómo protegernos?

Aunque fundamentalmente depende de nosotros mismos el tener cuidado para no ser víctima de este tipo de ataques, comprobando que los enlaces son fiables o que las páginas son las reales, actualmente nuestros sistemas de correo electrónico o de mensajes de texto comprueban si los mensajes se parecen a otros marcados como spam, y la etiqueta de posible spam en caso de parecerse. De esta manera ayuda a que nos pensemos dos veces si el mensaje que nos han enviado es verídico.

a. Phreaking:

1. ¿Qué es el phreaking?
2. ¿Cómo se desarrolla un ataque phreaking?
3. ¿Qué objetivo tienen estos ataques?

1. ¿Qué es el phreaking?

Este método, también conocido como pirateo telefónico, denomina la actividad en la que nuestro teléfono es explotado sin nuestro conocimiento para que los Phreakers (piratas telefónicos) puedan acceder a servicios como llamadas internacionales o nuestro buzón de voz.
El pirateo telefónico es una disciplina estrechamente vinculada con el hacking convencional. Aunque a menudo es considerado y categorizado como un tipo específico de pirateo informático, en realidad está orientado a la telefonía, está estrechamente vinculado con la electrónica, y fue el germen del pirateo informático puesto que el sistema telefónico es anterior a la extensión de la informática a nivel popular. El pirateo informático surgió del contacto de estos piratas telefónicos con los primeros sistemas informáticos personales y las primeras redes de comunicación.

2. ¿Cómo se desarrolla un ataque phreaking?

Una vez obtienen ese acceso a varios sistemas, los reúnen para crear sus propias redes y usarlas en todo el mundo. Después, cada llamada se enruta a través de una red de estas líneas telefónicas phreaker, lo que hace que sea difícil rastrearlas. Esto desemboca en una factura notable para el propietario de la línea telefónica, con algunas personas perdiendo millones a manos de Phreakers.

3 ¿Qué objetivo tienen estos ataques?

La meta de estos piratas es generalmente superar retos intelectuales de complejidad creciente, relacionados con incidencias de seguridad o fallas en los sistemas telefónicos, que les permitan obtener privilegios no accesibles de forma legal. Estos ataques no suelen ir dirigidos a usuarios puntuales, sino a empresas más bien notables.

A)-Sniffing:

1. ¿Qué es el Sniffing?
2. ¿Qué es un ataque Sniffing?
3. Cómo evitar este tipo de ciberataque.

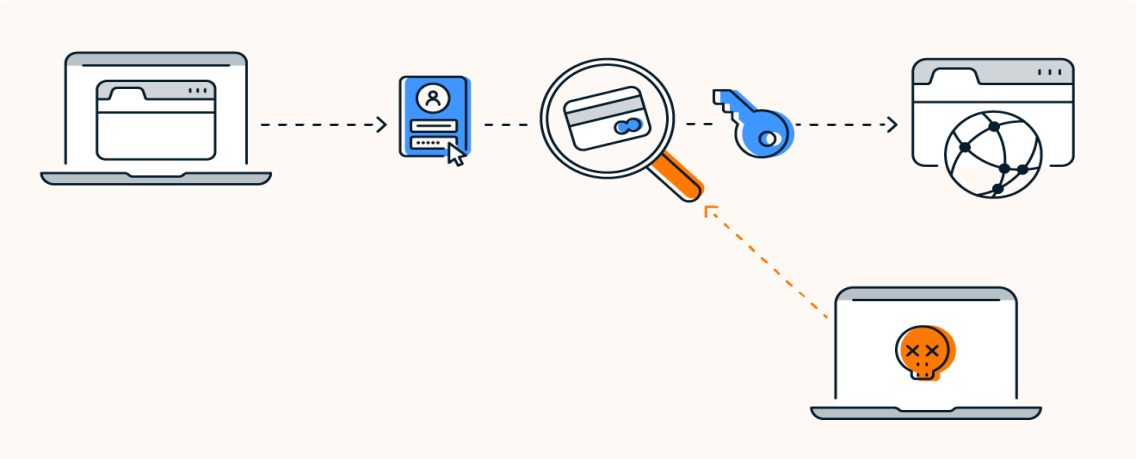
1 - El Sniffing es un tipo de ciberataque que se utiliza para poder escuchar todo lo que sucede dentro de una red, sobre todo en redes internas conocidas como intranet.

2 - Hay dos tipos de ataques de Sniffing:

-El Sniffing pasivo: Se recogen los datos que pasan sobre un nodo, mientras el ciberdelincuente permanece inactivo. Se coloca un dispositivo de rastreo en un HUB para poder capturar todo el tráfico que pasa a través de la red.

-El Sniffing activo: Su objetivo es inundar la memoria de direcciones de contenido (CAM) del switch, que redirige el tráfico a otros puertos, esto le permite al ciberdelincuente espiar el tráfico del switch.

3 - Para evitar este ciberataque es importante que no te metas a redes públicas, usar siempre plataformas de mensajería como (Correo electrónico) que encripta la información, visitar sitios webs que empiezan con HTTPS y como último realizar escaneos de tus redes informáticas.



B)-DDOS:

1. ¿Qué es un ataque DDOS?
2. ¿Cómo funciona un ataque DDOS?
3. ¿Qué objetivo tiene este ataque?
4. Tipos de ataques.

1 - Es un ataque distribuido de denegación de servicio (DDoS), un tipo de ciberataque, que consiste en que el atacante sobrecarga un sitio web, un ataque que sobrecarga un sitio web.

2 - Para lanzar este tipo de ataque, el atacante crea una red de bots, con dispositivos conectados a internet que están infectados con malware, los cuales usan los atacantes para redirigirlos y hacer que una red se sature.

3 - El objetivo de este ataque es disminuir la velocidad o impedir que el tráfico llegue a su destino previsto como por ejemplo impedir que el usuario entre a un sitio web, compre un producto etc.

4 - 1. Ataques a la capa de Aplicación:

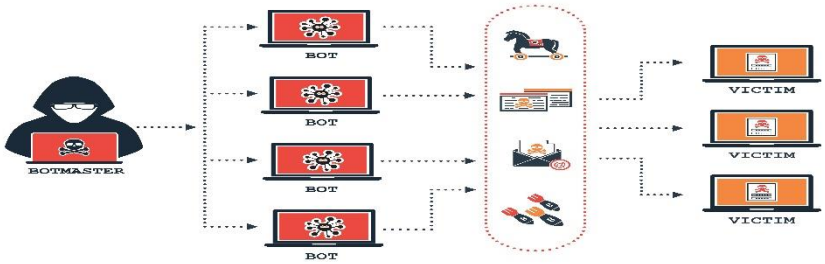
- Los ataques DDoS a la capa 7 (Capa aplicación) se dirigen a vulnerabilidades específicas de un sitio web con el fin de que este ataque impide que funcione el sitio web.

2. Ataques DDoS de protocolo:

- Los ataques de protocolo se dirigen a las debilidades de los protocolos de comunicaciones de internet en la capa 3 y 4 del modelo OSI (Red, Transporte), estos ataques tienen como finalidad consumir y agotar la capacidad informática.

3. Ataques DDoS por amplificación/reflexión de DNS:

- Este tipo de ataque hace que el hacker falsifique la dirección ip de su destino para evitar grandes cantidades de peticiones hacia servidores DNS abiertos.



C)-Virus:

1. ¿Qué es un virus?

Un virus informático es un software que tiene por objetivo alterar el funcionamiento normal de cualquier dispositivo informático, sin el permiso o el conocimiento del usuario, principalmente para lograr fines maliciosos sobre el dispositivo.

2. ¿Cómo funciona un virus?

Estos virus habitualmente reemplazan archivos ejecutables por otros infectados con el código de este mismo. Los virus pueden destruir, intencionadamente, los datos almacenados en un ordenador, aunque existen otros más inofensivos, que sólo producen molestias o imprevistos en el funcionamiento del dispositivo.

3. ¿Cómo se propaga un virus?

Esta propagación puede ocurrir de maneras diferentes, incluido el correo electrónico y la mensajería instantánea. Sin embargo, las redes sociales son la principal vía de propagación de virus informáticos. Todas las actividades disponibles en estas plataformas, como las comunicaciones vía chat, compartir publicaciones o unirse a grupos, permiten a los piratas informáticos atacarlas.

4. Cómo protegernos de un virus

-Métodos activos:

a) Antivirus: Programas que tratan de descubrir las trazas que ha podido dejar un software malicioso, para detectarlo y eliminarlo completamente del dispositivo, y en algunos casos contener o parar la contaminación. Tratan de tener controlado el sistema mientras funciona parando las vías conocidas de infección y notificando al usuario de posibles incidencias de seguridad.

b) Filtros de ficheros: Estos filtros pueden usarse por ejemplo en el sistema de correo o usando técnicas de cortafuegos. Este sistema proporciona una seguridad donde no se requiere intervención del usuario.

c) Actualización automática: Consiste en descargar e instalar las actualizaciones que el fabricante del sistema operativo lanza para corregir fallos de seguridad y mejorar el desempeño de nuestro sistema.

-Métodos pasivos:

Estos métodos dependen más propiamente del usuario, como puede ser no instalar software de dudosa procedencia, o no abrir correos desconocidos ni adjuntos que no se reconozcan. Otros ejemplos podrían ser utilizar un bloqueador de anuncios emergentes, usar la configuración de privacidad del navegador o borrar la memoria caché de internet y el historial del navegador.

D)-Troyano:

1. ¿Qué es un troyano?

   Un troyano es un tipo de malware que a menudo se camufla como software legítimo. Los hackers pueden emplear los troyanos para intentar acceder a los sistemas de los usuarios. Normalmente, algún tipo de ingeniería social engaña a los usuarios para que carguen y ejecuten los troyanos en los sistemas.

2. ¿De dónde viene el término troyano?

   El término troyano deriva de la antigua historia griega acerca del engañoso caballo que provocó la caída de Troya.

   Cuando se trata de nuestro equipo, un virus troyano opera de forma similar:
   se esconde dentro de programas aparentemente inofensivos. El nombre se acuñó en un informe de las Fuerzas Aéreas Estadounidenses en 1974, en el cual se especulaba sobre hipotéticas formas de vulnerar ordenadores.

3. ¿Cómo funcionan los ataques con troyano?

   En estos casos el usuario puede haber sido víctima de phishing primero, siendo engañado para descargar algún archivo aparentemente inofensivo, un software antivirus falso o simplemente alguien con intenciones maliciosas nos ha compartido el archivo troyano.

   Una vez activados, los troyanos pueden permitir a los cibercriminales espiar, robar los datos confidenciales y obtener acceso por una puerta trasera del sistema.

5. Como prevenir el Malware.

Para prevenir que un malware se infiltre en nuestros dispositivos, lo más importante es tener un buen antivirus para protegerlos, otros aspectos importantes que tenemos que tener en cuenta son los siguientes:

- Tener cuidado a la hora de insertar nuestros datos en sitios webs.
- No abrir correos no deseados.
- Tener las últimas actualizaciones de nuestros Software, para evitar nuevas vulnerabilidades.
- Ser precavido a la hora de descargar archivos de sitios web desconocidos.

6. Como puedo protegerme ante un Malware.

Aparte de las anteriores recomendaciones, es importante utilizar herramientas de protección frente al malware, estos antivirus son sencillos de descargar y son capaces de reconocer y advertir al usuario de cualquier tipo de amenazas.

7. Curiosidades.

El primer Software antimalware:

Antes de hablar del primer software antivirus, nos debemos remontar hasta 1971, cuando un empleado de BBN Technologies, **Bob Thomas**, creó el primer virus informático conocido, el virus **Creeper**, que significa “Enredadera” en inglés. A diferencia de los virus que conocemos hoy en día, el virus Creeper no se creó con intenciones maliciosas. Su principal funcionalidad era moverse a través de ARPANET, precursora de Internet, pero aun así tuvo un impacto transcendental en la informática y la ciberseguridad, ya que abrió los ojos al mundo sobre las posibilidades y los riesgos asociados a la autorreplicación y la movilidad de software a través de redes.

Este virus fue concebido en contexto de exploración e innovación tecnológica, en los inicios de la era de la computación interconectada. El objetivo de Creeper era demostrar la capacidad de un software para autorreplicarse y moverse autónomamente a través de una red de ordenadores. Una de las características más distintivas de Creeper era el mensaje que dejaba en cada ordenador que infectaba: “*I’m the Creeper, catch me if you can!*” (Soy la enredadera, ¡atrápame si puedes!). Aunque no causaba daño real, el mensaje era una clara indicación de la presencia del virus.

Como respuesta directa al desafío presentado por el virus, **Ray Tomlinson**, conocido por ser el inventor del correo electrónico moderno, creó **Reaper** (segadora) en 1972. EL objetivo de Reaper era contrarrestar la presencia y la propagación del virus Creeper en la red ARPANET. Este desarrollo fue una iniciativa pionera y crucial en el campo de la seguridad informática, dado que marcó la primera vez que se creó un software específico para combatir otro software malicioso.

La funcionalidad principal de Reaper era detectar y eliminar al virus Creeper de los sistemas infectados. Una vez que localizaba una copia de Creeper en un sistema, el Reaper procedía a eliminarlo. Esta capacidad de reconocer y erradicar un programa específico de un ordenador era un concepto revolucionario en ese momento y sentó un precedente importante para el desarrollo de futuros programas antivirus.

8. Videos.

Sniffing : https://www.youtube.com/watch?v=sxg4sCjdz84

Ddos : https://www.youtube.com/watch?v=7xGdz5Li9Sw

Troyano : https://www.youtube.com/watch?v=2X5mWnmR1g0

Virus : https://www.youtube.com/watch?v=ZHfNaCuVzkg

Phishing : https://www.youtube.com/watch?v=M2HaMR3H0Cg