TEMA 6: MALWARE, SOFTWARE MALICIOSO Y MEDIDAS DE PROTECCIÓN

SMR- SEGURIDAD INFORMÁTICA

CONTENIDO

- **Introducción**
- Tipos de malware
- Medidas de protección
- Sistemas de detección
- Métodos de ciberdelincuencia

INTRODUCCIÓN

- **Malware**, software maligno y software malicioso son términos equivalentes que engloba a todo software hostil, intrusivo o molesto, y suele ser confundido con el término virus informático que, en realidad, es solo uno de los diversos tipos de malware existentes.
- El malware es un software que se instala en un sistema informático **sin el consentimiento del usuario y se ejecuta sin su autorización**, el **objetivo** del malware puede ser muy diverso, pudiendo ser desde inofensiva bromas o demostraciones del tipo "he estado aquí", hasta el borrado o secuestro de datos, pasando por el robo de contraseñas. En el 98% de los casos el objetivo es principalmente económico.
- El malware que afecta a servidores puede ser muy diferente del que afecta a equipos sobremesas, dado que el objetivo suele ser la captura de información sensible o la utilización de los recursos del sistema infectado para la realización de alguna actividad delictiva.

CONTENIDO

- Introducción
- **Tipos de malware**
- Medidas de protección
- Sistemas de detección
- Métodos de ciberdelincuencia

TIPOS DE MALWARE: ADWARE

El adware es un software no deseado diseñado para mostrar anuncios en su pantalla, normalmente en un explorador.

Diferenciado del spyware como una forma de PUP (Potentially Unwanted Program) menos dañina.

El adware más famoso: DeskAd, muestra anuncios en el navegador de Internet.

Malvertising (la evolución del adware): Programa malicioso que se oculta en publicidad en páginas de terceros.

Tipos:

- Adware completo o parcial: El software puede ser un programa como cualquier otro instalado en nuestro dispositivo (completo) o, por otro lado, estar instalado en forma de extensión dentro de un programa (parcial).
- Adware oculto o visible: El software puede estar escondido, puede mostrarse con un nombre, pero estar instalado con otra denominación. Esto hace que sea realmente complicado desinstalarlo.
- Adware ético o malware: En la actualidad muchas aplicaciones podemos descargarlas de forma gratuita y algunas se mantienen a base de anuncios. Estos anuncios son mostrados previa aceptación de cookies o política y condiciones hacia el usuario, pero en su mayoría el adware ha servido a modo de software espía y se ha vuelto problemático.

TIPOS DE MALWARE: CRYPTO JACKING

El crypto jacking es una forma de apropiarse de los recursos de un dispositivo ajeno sin el consentimiento ni conocimiento del usuario infectado, para “minar” criptomonedas.

Este robo de sus recursos informáticos reduce la velocidad de otros procesos, aumenta la factura de la luz y acorta la vida del dispositivo.

TIPOS DE MALWARE: GUSANOS

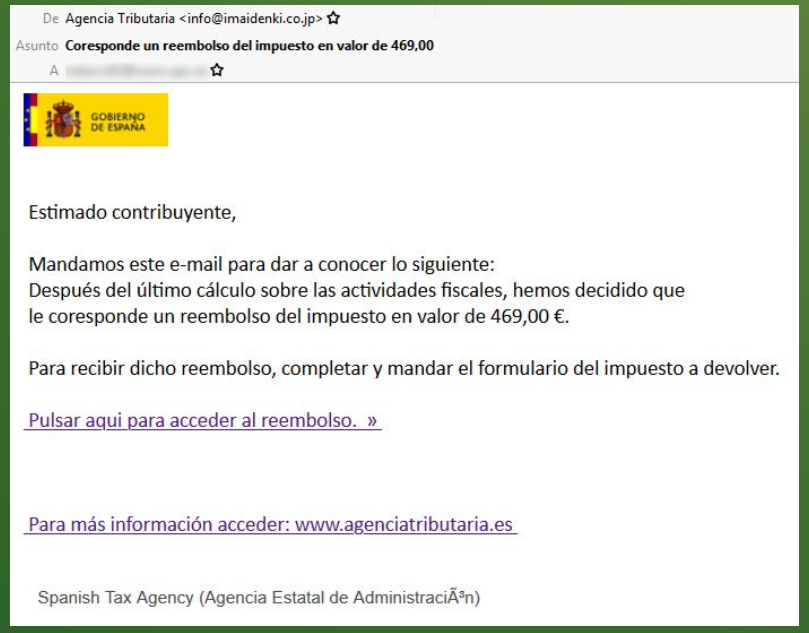
Los gusanos son en realidad una subclase de virus, por lo que comparten características. Son programas que realizan copias de sí mismos, alojándolas en diferentes ubicaciones del ordenador. El objetivo de este malware suele ser colapsar los ordenadores y las redes informáticas, impidiendo así el trabajo a los usuarios. A diferencia de los virus, los gusanos no infectan archivos.

El gusano **Morris** fue el primer ejemplar de malware autorreplicable que afectó a internet, el 2 de noviembre de 1988.

El gusano **ILOVEYOU** instalaba un troyano y destruía todos los archivos de extensión doc , vbs , vbe , js , jse , css , wsh , sct , hta , jpg y jpeg en los ordenadores infectados, sustituyendolos por una copia del script.

TIPOS DE MALWARE: PHISING

El **phishing** es una técnica de engaño que utilizan los piratas informáticos para robar nuestros datos personales y bancarios a través de la página web falsa de alguna institución oficial como la Agencia Tributaria, nuestro banco o cualquier empresa o tienda que consideramos de total confianza.


De Agencia Tributaria <info@imaidenki.co.jp>
Asunto **Coresponde un reembolso del impuesto en valor de 469,00**
A

GOBIERNO DE ESPAÑA

Estimado contribuyente,

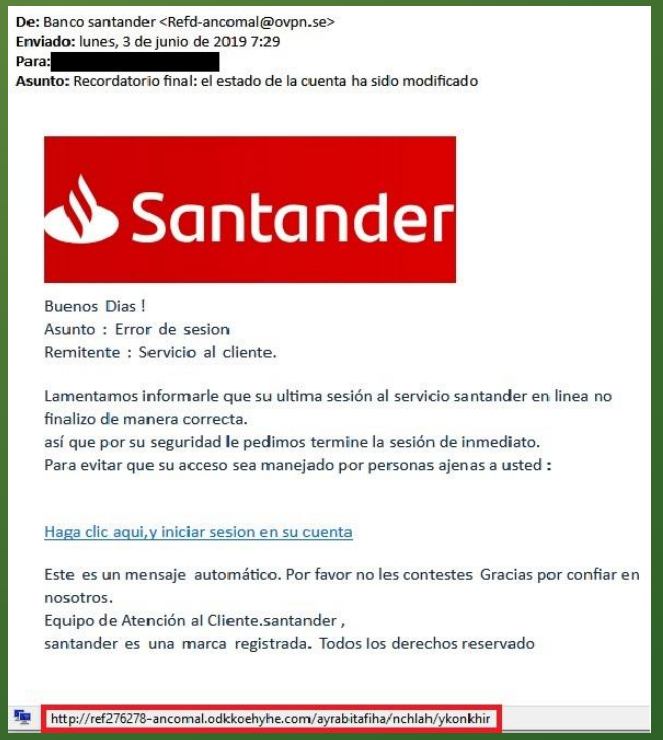
Mandamos este e-mail para dar a conocer lo siguiente:
Después del último cálculo sobre las actividades fiscales, hemos decidido que le coresponde un reembolso del impuesto en valor de 469,00 €.

Para recibir dicho reembolso, completar y mandar el formulario del impuesto a devolver.

Pulsar aqui para acceder al reembolso. »

Para más información acceder: www.agenciatributaria.es

Spanish Tax Agency (Agencia Estatal de AdministraciÃ³n)


De: Banco santander <Refd-ancomal@ovpn.se>
Enviado: lunes, 3 de junio de 2019 7:29
Para: [redacted]
Asunto: Recordatorio final: el estado de la cuenta ha sido modificado

Santander

Buenos Dias !
Asunto : Error de sesion
Remitente : Servicio al cliente.

Lamentamos informarle que su ultima sesión al servicio santander en linea no finalizo de manera correcta.
así que por su seguridad le pedimos termine la sesión de inmediato.
Para evitar que su acceso sea manejado por personas ajenas a usted :

Haga clic aqui,y iniciar sesion en su cuenta

Este es un mensaje automático. Por favor no les contestes Gracias por confiar en nosotros.
Equipo de Atención al Cliente.santander ,
santander es una marca registrada. Todos los derechos reservado

http://ref276278-ancomal.odkkoehyhe.com/ayrabitafiha/nchlah/ykonkhir

TIPOS DE MALWARE: RANSOMWARE

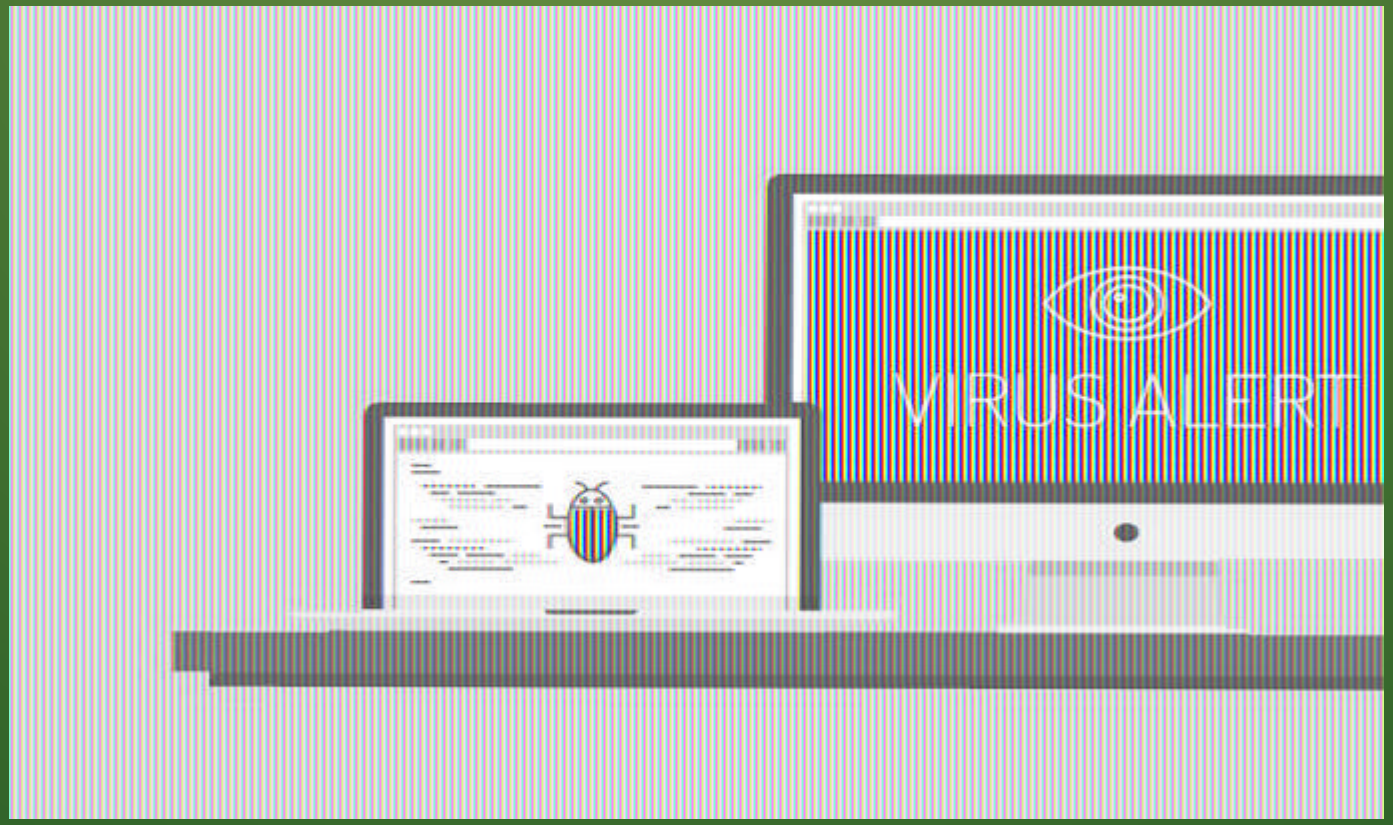
El ransomware es un tipo de malware que impide a los usuarios acceder a su sistema o a sus archivos personales cifrando la información y que exige el pago de un rescate para poder acceder de nuevo a ellos.

WannaCry el 12 de mayo de 2017: https://youtu.be/OuH-1spvOYE

Funcionamiento y daños que realiza: https://youtu.be/YBspSkGF1nM

TIPOS DE MALWARE: ROGUEWARE

Es un software malicioso que simula ser un antivirus que nos lanza una alerta donde indican que algo va mal en nuestro equipo.



TIPOS DE MALWARE: ROOTKIT

Un rootkit o encubridor es un conjunto de software que permite al usuario un acceso de "privilegio" a un ordenador, pero mantiene su presencia inicialmente oculta al control de los administradores.

El funcionamiento de los rootkits se puede generalizar de la siguiente manera:

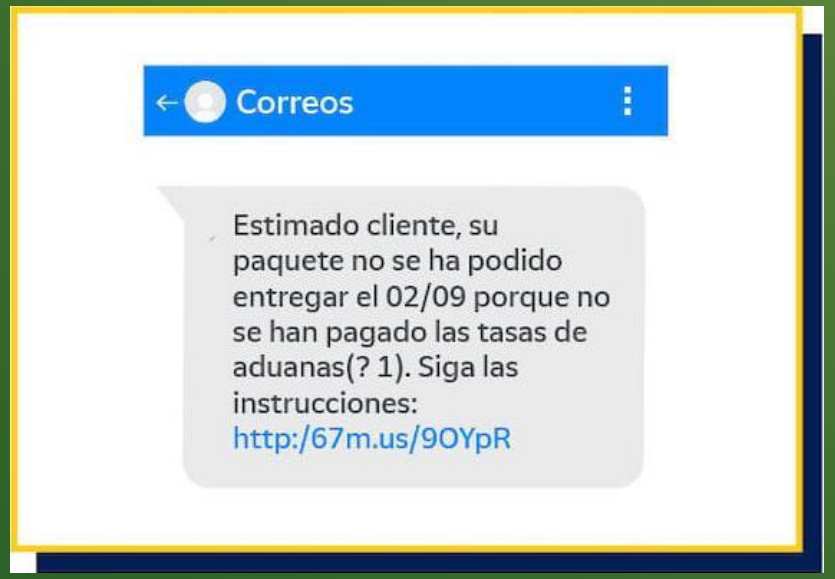
1. Infección del sistema: en primer lugar, el rootkit se instala en el dispositivo e infecta el sistema.

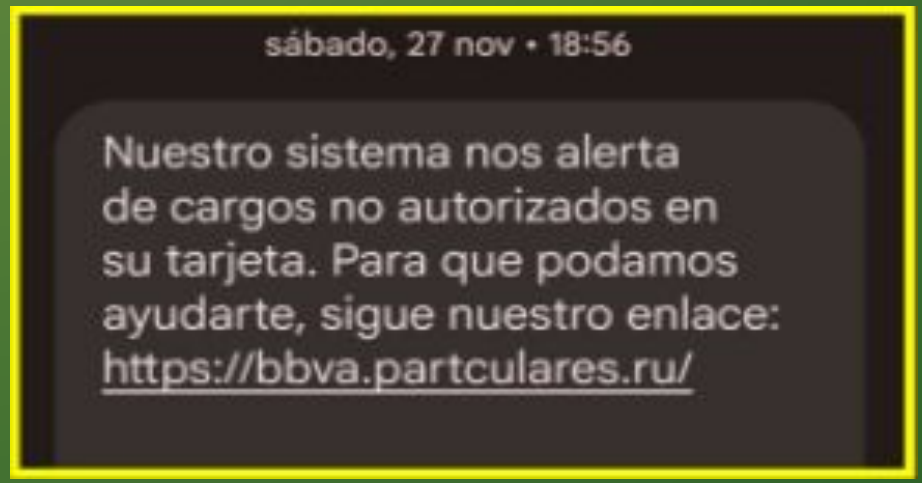
2. El modo encubierto: una vez que el rootkit se haya instalado, pasa al modo encubierto. En otras palabras, el rootkit se oculta en el sistema y empieza a manipular los procesos de intercambio de datos que utilizan los programas y las funciones para mandar falsa información a los programas de seguridad como, por ejemplo, los programas antivirus.

3. Crear una puerta trasera: el último paso consiste en crear una puerta trasera para permitir el acceso remoto al dispositivo. La tarea del encubridor consiste en ocultar los inicios de sesión remotos y cualquier actividad que se pueda clasificar como sospechosa para poder manipular el dispositivo sin dejar ningún rastro.

TIPOS DE MALWARE: SMISHING

El smishing es un tipo de delito o actividad criminal a base de técnicas de ingeniería social con mensajes de texto dirigidos a los usuarios de telefonía móvil. Se trata de una variante del phishing.





TIPOS DE MALWARE: SPYWARE

Un spyware se dedica al robo de la información, esté la recopila y luego se envía a alguien externo del ordenador sin el consentimiento del usuario y sin que este se entere.

Tipos de spyware:

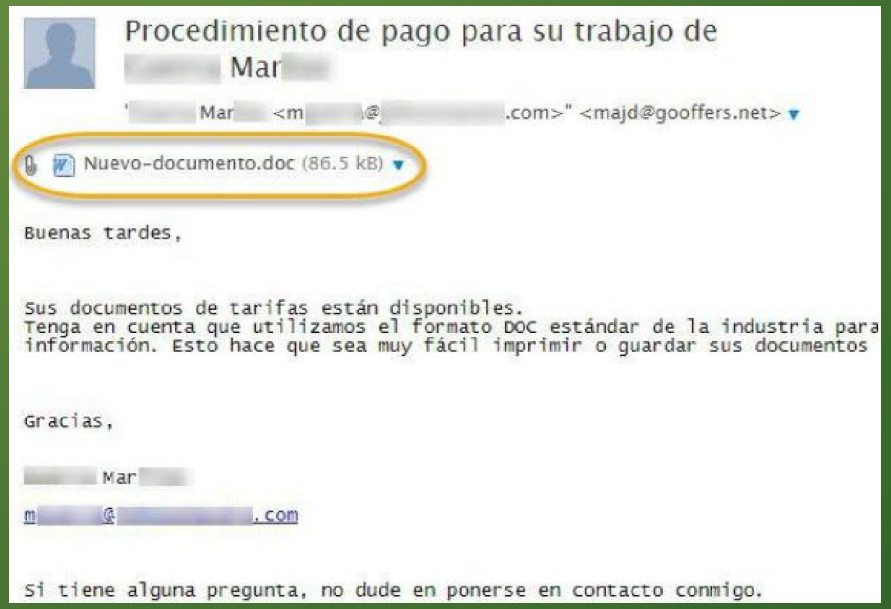
- Keyloggers: registra las teclas que pulsa el usuario desde su ordenador. El mayor riesgo reside en que las contraseñas también pueden quedar registradas cuando se introducen.
- Adware: Genera que aparezcan constantemente anuncios publicitarios en ventanas emergentes. No solamente es molesto, sino que podrá guardarse y transmitirse cualquier información que el usuario proporcione sin su autorización al acceder a alguno de esos sitios.
- Info Stealers: como el keylogger, opera sin que el usuario se dé cuenta de que está recopilando y transmitiendo la información del ordenador. En este caso, recopila indiscriminadamente todos los datos que se introducen en el ordenador: desde el contenido multimedia al historial de búsqueda, incluyendo contraseñas y cuentas de correo electrónico.

TIPOS DE MALWARE: TROYANO

Un troyano es un archivo, programa o fragmento de código que parece ser legítimo y seguro, pero en realidad es un malware. Los troyanos se empaquetan y entregan dentro de software legítimo, y suelen diseñarse para espiar a las víctimas o robar datos.

Tipos de troyanos:

- Troyanos de puerta trasera
- Troyanos bancarios
- Troyanos antivirus falsos



Emotet en 2014 como troyano bancario, se detuvo en 2021:

https://www.europol.europa.eu/media-press/newsroom/news/world%E2%80%99s-most-dangerous-malware-emotet-disrupted-through-global-action

TIPOS DE MALWARE: VIRUS

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

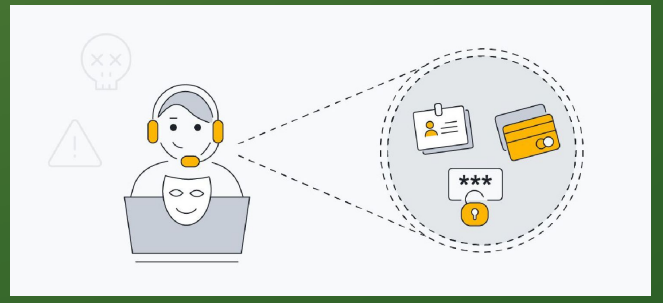
Método de propagación: el usuario, en un momento dado, ejecuta o acepta de forma inadvertida la instalación del virus.

TIPOS DE MALWARE: VISHING

Es una técnica de phishing usando la voz, es decir, una llamada o una doble llamada. Un ejemplo de un caso de vishing: una persona nos llama por teléfono haciéndose pasar por nuestra operadora y nos avisa de un aumento en la tarifa. Acto seguido, recibimos una segunda llamada de alguien que nos ofrece una tarifa más barata con el fin de conseguir información sensible, como un número de cuenta o un DNI.

El vishing es algo relativamente reciente, es una evolución del phishing lo que consistía en engaños mediante mensajes o correos electrónicos, esta técnica nueva utiliza la voz por lo que se hace mediante llamadas telefónicas, y ahora pueden llegar a utilizar la tecnología DeepFake, para conseguir voces falsas de gente conocida.

https://youtu.be/fjDqZ6s38ak



CONTENIDO

- Introducción
- Tipos de malware
- **Medidas contra el malware**
- Sistemas de detección
- Métodos de ciberdelincuencia

MEDIDAS CONTRA EL MALWARE

Una medida básica dentro de las que todo administrador debe adoptar en el terreno de la seguridad activa es la de tener **actualizado el software** que utiliza, tanto sistema operativo como aplicaciones. Desafortunadamente, no todas las actualizaciones ponen remedio a agujeros de seguridad detectados, sino que arreglan pequeños defectos (bugs) o añaden alguna funcionalidad nueva.

Las actualizaciones que corrigen brechas de seguridad reciben el nombre de **actualizaciones de seguridad**, y merecen una especial atención porque:

- Tras actualizar, se estará protegido ante esos agujeros de seguridad descubiertos.
- La información publicada sobre el fallo corregido suele ser utilizada por los hackers para atacar sistemas sin actualizar lo que hace urgente la acción del administrador.

MEDIDAS CONTRA EL MALWARE

No obstante, una actualización también tiene sus riesgos: puede dejar el sistema inestable o en el peor de los casos inservible, a causa de alguna incompatibilidad del nuevo software con otro existente en el equipo o con el hardware subyacente.

Dicho esto, hay que informarse bien de todas las actualizaciones de los sistemas y especialmente de las denominadas críticas.

MEDIDAS CONTRA EL MALWARE

Las 3 medidas imprescindibles para luchar contra el malware son:

1. Usar siempre software legal.
2. Actualizar siempre con presteza el software, empezando por el sistema operativo. En el entorno empresarial es necesario que el administrador defina una política de actualizaciones para servidores y equipos de usuario.
3. Instalar un **software antivirus** actualizado.

Las medidas de seguridad que se deben adoptar están catalogadas como **seguridad activa** pues implican la supervisión constante del administrador del sistema, por ejemplo actualizando el sistema operativo.

Ante el malware, una buena medida de protección, sería la suma de *un antivirus + formación + más sentido común*.

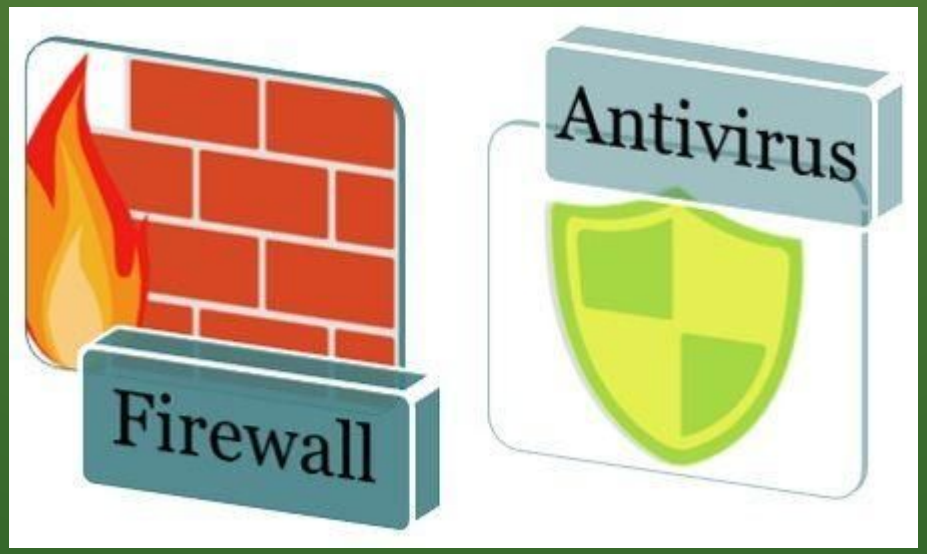
CONTENIDO

- Introducción
- Tipos de malware
- Medidas contra el malware
- **Sistemas de detección**
- Métodos de ciberdelincuencia

SISTEMAS DE DETECCIÓN

A pesar de las distintas características que tienen las tipologías de malware, los sistemas utilizados para su detección y contención son comunes entre ellos:

- IDS/IPS.
- Antivirus.
- *Firewall* o cortafuegos.



SISTEMAS DE DETECCIÓN: IDS/IPS

IDS (“Intrussion Detection System”) – estos sistemas sirven para detectar e informar a los administradores sobre los intentos de intrusión que se producen en un equipo, red o dispositivo. Además, algunos de ellos (IPS “Intrussion Prevention System”) además de detectar intrusiones utilizan otro tipo de mecanismos para evitar que la intrusión se produzca con éxito.

Para su correcta utilización se necesita un alto nivel de experiencia y conocimiento del sistema de modo que sus configuraciones permitan el equilibrio entre la detección de falsos positivos y falsos negativos.

IDS – modo de protección reactiva ante intrusiones (medidas correctivas o reactivas)

IPS – modo de protección proactiva (medidas preventivas)

SISTEMAS DE DETECCIÓN: ANTIVIRUS

Los antivirus son programas que tienen como función detectar y eliminar tanto virus como otros tipos de código malicioso. Para su detección disponen de una base de datos de patrones de modo que comparando cada archivo con los patrones se pueden detectar archivos contaminados.

Además de la comparación de los archivos del sistema con patrones de archivos contaminados, también tienen otras funciones:

- Revisan el correo electrónico
- Revisan el historial de páginas web visitadas para detectar código malicioso oculto
- Revisan los sistemas para detectar si hay algún troyano o gusano
- Realizan tareas propias de los sistemas IDS/IPS y de los cortafuegos

SISTEMAS DE DETECCIÓN: FIREWALL

Los cortafuegos pueden ser elementos hardware o software, que se utilizan en un equipo o en una red de equipos como medida de control de las comunicaciones establecidas, permitiendo o denegando el acceso a los sistemas según las políticas de seguridad determinadas por la organización.

Así, un cortafuegos configurado correctamente funciona eficazmente como barrera para evitar el acceso de código malicioso a los sistemas de la organización, aunque por sí solo no es suficiente: es necesaria la instalación de medidas de protección adicionales como antivirus o sistemas IDS/IPS.

CONTENIDO

- Introducción
- Tipos de malware
- Medidas contra el malware
- Sistemas de detección
- **Métodos de ciberdelincuencia**

MÉTODOS DE CIBERDELINCUENCIA

- La **ciberdelincuencia** o **fraude on-line** es aquel acto deliberado e ilegítimo que causa un perjuicio patrimonial mediante un conjunto de procedimientos que evolucionan y se transforman vertiginosamente y que tienen la intención fraudulenta o delictiva de obtener ilegítimamente un beneficio económico.

MÉTODOS DE CIBERDELINCUENCIA

- Los principales métodos de ciberdelincuencia son:
  - **Botnets**: redes infectadas por bots que pueden controlarse remotamente por la persona que controla el malware instalado en los equipos. El objetivo final es contar con un gran número de máquinas anónimas que reciban órdenes para la distribución de malware, envío de spam, o ejecución de ataques de denegación de servicio (DDoS).
  - **Spoofing**: suplantación de identidad para interceptar, alterar o conseguir comunicación y acceder a los recursos de la red o a la administración de equipos.
    - IP Spoofing: suplantar la dirección IP.
    - ARP Spoofing: falsear la tabla ARP (MAC-IP)
    - DNS Spoofing: falsificar la tabla de resolución de IPs y nombres de dominio en un DNS.
    - Web Spoofing: falsificar parcial o totalmente un sitio web para interceptar la información introducida por el usuario.
    - Mail Spoofing: suplantación de las direcciones de correo.

MÉTODOS DE CIBERDELINCUENCIA

- Los principales métodos de ciberdelincuencia son:
  - **Ataques fuerza bruta:** superación de sistemas criptográficos para conseguir acceder al sistema.
  - **Ataques JavaScript**: Introducción de código adicional en sitios web muy visitados con el objetivo de redirigir a los usuarios hacia webs maliciosas. También se introduce código para descargar componentes diseñados para aprovechar vulnerabilidades en el cliente, conocido como **exploit**.
  - **SQL Injection**: introducción de comandos SQL adicionales a través de formularios de autenticación. Si existen fallos de programación será posible ejecutar sentencias sobre la base de datos, pudiendo alterar sus datos.
  - **Rootkits**: conjunto de herramientas con objetivos maliciosos que ejecutan procesos restringidos a administradores y modifica los archivos del sistema.

MÉTODOS DE CIBERDELINCUENCIA

- ARP Spoofing: monitorizando tramas ARP con Arpwatch

Monitorizando tramas arp con Arpwatch

Instala la herramienta **Arpwatch** en tu máquina Linux. Procede a su configuración para que el administrador de la red reciba alertas arp spoofing.

Comprueba si el proceso está en ejecución.

Evita **arp spoofing** haciendo una entrada estática en la tabla ARP.

MÉTODOS DE CIBERDELINCUENCIA

- ARP Spoofing: monitorizando tramas arp con Arpwatch

Primero se procede a la instalación en Ubuntu ejecutando el comando

```
apt-get install arpwatch
```

Luego, se edita el fichero de configuración que se encuentra localizado en el directorio */etc/arpwatch.conf*. Para indicar el correo al que la herramienta enviará las alertas arp se añade a dicho fichero la línea

```
eth0 -a -n 192.168.1.143/24 -m admon@paraninfo.es
```

En caso de que la interfaz de red que usar no se llame `eth0` o se quiera monitorizar otra tarjeta de red, se indicaría el nombre de la misma en vez de `eth0`.

Se reinicia el servicio para que la nueva configuración tenga efecto

```
/etc/init.d/arpwatch restart
```

Para comprobar que el proceso está activo, se ejecuta

```
ps -ef | grep arpwatch
```

Para contrarrestar este tipo de ataques, se usa configuración ARP estática. La orden que se usa para este cometido es `arp -s`, indicando la dirección IP y la dirección física o MAC, de la forma

```
arp -s 192.168.1.143 9f-4b-0c-9f-14-cb
```

Recuerda que en Linux se usa el carácter delimitador dos puntos, de modo que el mismo comando en Linux es

```
arp -s 192.168.1.143 9f:4b:0c:9f:14:cb
```