UD1 A11 Cuestionario

Antonio Teixeira Vázquez

**¿Qué es un antivirus?**

Es un programa cuya finalidad es descubrir y borrar virus informáticos.

**Explica en qué consisten los siguientes tipos de antivirus:**

* Vacuna: Busca en el equipo un tipo determinado de virus para eliminarlo o ponerlo en cuarentena.
* Detector: Avisa al usuario de la presencia de un virus, pero no lo elimina.
* Eliminador: Eliminan las amenazas de las partes afectadas además de reparar el equipo devolviéndolo a su estado previo.

**¿Qué es Reaper y Creeper?**

Creeper fue un programa auto replicante creado por Bob Thomas en el año 1971 como experimento.

Creeper se extendía por ARPANET, copiándose así mismo en los equipos que encontraba, mostrando el mensaje:

*“I’m the creeper, catch me if u can!”*

Reaper por su parte, fue creado en el año 1972 con una función, buscar y eliminar a Creeper de los PCs, siendo el primer antivirus.

**¿Qué es un virus boot?**

Es un tipo de virus que ataca el sector de arranque de una unidad, solo se ponen en marcha una vez el equipo se iniciaba con una unidad infectada.

**¿Qué es un virus hijacker?**

Es un tipo de virus que secuestra el navegador, impidiendo acceder a algunas páginas web e instalando basura en el navegador.

**¿Qué es un virus keylogger?**

Es un tipo de virus que una vez en el equipo, registra todas las pulsaciones del teclado con la finalidad de que el autor pueda ver los usuarios y las contraseñas de la víctima.

**¿Qué es un virus zombie?**

Es un tipo de virus que cede el control de la máquina a un tercero para usarla de difusor de otros virus o en tareas como un ataque DDOS.

**¿Cuál es la característica principal del antivirus Avast?**

Que tiene una versión gratuita muy utilizada.

**¿Por qué se denominan virus a los virus informáticos?**

Porque su forma de actuación es muy similar a la de los virus.

**Investiga que es Elk Cloner y quien es Rich Skrenta.**

Elk Cloner fue el primer virus informático que no nació como un experimento de laboratorio.

Creado en el año 1982 para el Apple II, se propagaba infectando los disquetes y difundiéndose a otros equipos a través de estos.

Aunque no tenía una finalidad destructiva, podía llegar a corromper los datos de algunos discos y en el arranque N. º50 del disco, mostraba el siguiente mensaje:

*“Elk Cloner: The program with a personality*

*It will get on all your disks*

*It will infiltrate your chips*

*Yes, it's Cloner!*

*It will stick to you like glue*

*It will modify RAM too*

*Send in the Cloner!”*

Rich Skrenta, el creador de Elk CLoner, era un estudiante de 15 años que desarrollo Elk CLoner como broma a sus amigos cuando compartía juegos.

**¿Por qué crees que se hacen los virus?**

Hay muchas razones que llevan a la gente a desarrollarlos, desde un desarrollador que está haciendo experimentos, hasta una organización con la finalidad de robar datos o causar estragos.

**¿Cuál es la necesidad de actualizar un antivirus?**

Es conveniente actualizar el antivirus para que estos puedan añadir a las listas nuevos virus que vayan encontrando y así ser más eficaces a la hora de detectarlos.

**¿Qué diferencias existen entre la protección de un antivirus gratuito y uno de pago?**

Las diferencias cambian de antivirus a antivirus, la más común es o bien que el gratuito no ofrezca protección en tiempo real, o que la base de datos de virus no esté tan completa.

**¿Qué es un antivirus online? Pon algún ejemplo**

Es un tipo de antivirus, que no necesita ser instalado, es decir, escanea el equipo en búsqueda de amenazas desde el navegador.

Un ejemplo sería Kaspersky online.

**Indica en que consiste cada uno de los siguientes tipos de virus**

* Adware: *Muestra anuncios indeseados.*
* Spyware: *Software espía, recopila información del equipo.*
* Malware: *Alteran el comportamiento del equipo sin el permiso del usuario.*
* Ransomware: *Se bloquea el equipo, y se pide un rescate para desbloquearlo.*
* Gusanos: *Se auto replican y se envían a otros PCs.*
* Troyano: *Virus camuflados dentro de otros programas.*
* Denegación de servicio: *Ataque que satura a la red o equipos que lo reciben imposibilitando su buen funcionamiento.*
* Puerta trasera: *Parte del código de un programa que permite el acceso al equipo a través de él.*
* Phishing: *Páginas web y correos falsos para engañar al usuario y robarle sus datos.*
* Darknets o Deep web, comercio de vulnerabilidades: *Venta de guías que permiten a gente sin experiencia realizar ciberataques.*
* Bombas lógicas o de tiempo: *Fragmentos de código que permanecen ocultos hasta que se cumple una condición, en ese momento ejecutan la acción.*
* Hoax: *Alarma falsa sobre un virus*.

**Compara los siguientes tipos de antivirus e indica las ventajas de cada uno de ellos.**

* Kaspersky:
  + Protección contra una amplia lista de virus.
  + Bajo impacto en el rendimiento.
  + Interfaz sencilla.
* Nod 32:
  + Muy sencillo
  + Base de datos muy amplia.
* Mcafee:
  + De los más utilizados.
  + Permite un número ilimitado de dispositivos.
  + Muy poco impacto en el rendimiento.

**Investiga en que consistían los siguientes virus.**

* Morris (1988):

Morris fue el primer gusano en afectar a internet. Se especula que infectó alrededor de 6000 sistemas por todo EEUU.

El programa aprovechaba defectos en los sistemas UNIX de la universidad de Berkley.

Aunque no fue creado con fines destructivos, pero un bug en el código causo efectos catastróficos, esto hizo que se arrestara al creador, Robert Tappan Morris, un estudiante de 23 años.

* CIH / Chernobyl (1998):

Fue un virus que surgió en el año 1998 y atacaba a los sistemas con Windows 9x (Windows 98,95…)

En su época se consideró como uno de los virus mas peligrosos pudiendo incluso corromper los datos de la BIOS imposibilitando que los equipos arrancaran correctamente.

Su creador Chen Ing Hau, un estudiante de la universidad Tatung de Taipéi, lo creó para dejar en ridículo a las compañías que presumían de sus softwares antivirus.

* Melissa (1999):

Fue un virus creado en el año 1999 que infectaba documentos de Microsoft Office.

Hay muchas variantes, aunque todas tienen una forma de actuar similar, infectan un equipo, y acto seguido envían un email a los 50 primeros contactos en Outlook, con archivos que una vez abiertos repetían todo el proceso de nuevo.

Causó millones de dólares en pérdidas, lo que acarreo que el autor, David L. Smith, fuera condenado a 10 años y una multa de 5000 dólares.

* I love you (2000):

Se creó en el año 2000 e infectó a unos 50 millones de equipos causando perdidas de más de 5500 millones de dólares.

Se propagaba en cuestión de segundos, entrando en la máquina infectada y remplazando diversos archivos con su propio código, después se reenviaba a los 50 primeros contactos de la lista de correo y también se reenviaba por IRC.

* Mydoom (2004):

Es un gusano que apareció por primera vez a principios del año 2004.

Se transmitía a través de correo electrónico en un archivo acompañado de mensajes de error y similares, al ejecutarse creaba puertas traseras que permitían utilizarlo para un ataque remoto programado el 1 de febrero de 2004 al sitio web de SCO Group, además, también le servía para replicarse por servidores p2p, aunque donde realmente se propagó fue a través de los susodichos emails.

Hubo una segunda versión, pero su propagación fue prácticamente nula.

* Conficker (2008):

Fue un gusano que apareció en el año 2008 y que aprovechaba una vulnerabilidad del servicio Server de Windows para propagarse.

Su forma de actuar era, una vez infectado el equipo, deshabilitaba servicios como Windows update, Windows defender… una vez deshabilitados, contactaba con un servidor para recibir instrucciones para propagarse, recolectar datos del equipo e instalar más malware.

* WannaCry (2017):

Fue un Ransomware que se propagó por millones de equipos en el año 2017.

WannaCry infectaba a equipos que utilizaran versiones de Windows sin actualizar aprovechando la vulnerabilidad EternalBLue desarrollada por la NSA.

Una vez infectado el equipo, se bloqueaban los archivos y se mostraba en pantalla un mensaje exigiendo un rescate de 300 dólares.