¿Qué es un antivirus?

Es un programa de computadora cuyo propósito es combatir y erradicar los virus informáticos. Es importante que configurarlo adecuadamente. Su uso permite minimizar los riesgos pero nunca será una solución definitiva para que sea más eficaz se deben tomar siempre medidas preventivas y correctivas.

Explica en qué consisten los siguientes tipos de antivirus

- ✓ **Vacuna:** Es un programa instalado en la memoria, actúa como "filtro" de los programas que son ejecutados, abiertos para ser leídos o copiados, en tiempo real.
- ✓ **Detector:** Es el programa que examina todos los archivos existentes en el disco. Tiene instrucciones de control y reconocimiento exacto de los códigos virales que permiten capturar sus pares, debidamente registrados y en forma sumamente rápida desarman su estructura.
- ✓ **Eliminador:** Es el programa que una vez desactivada la estructura del virus procede a eliminarlo e inmediatamente después a reparar o reconstruir los archivos y áreas afectadas.

¿Qué es Reeper y Creeper?

Reeeper virus, Creeper antivirus.

¿Qué es virus boot?

Este virus se activa cuando la computadora es encendida y el sistema operativo se carga.

¿Qué es un virus hijackers?

Son programas que secuestran a navegadores de internet.

¿Qué es el virus keylogger?

Es un capturador de teclas

¿Qué es el virus zombie?

Es cuando el computador está siendo controlado por terceros.

¿Cuál es la característica principal del antivirus AVAST?

El antivirus AVAST tiene la protección antes de ingresar al sistema.

¿Por qué se denominan virus a los virus informáticos?

Porque es como los virus "normales", se meten en un organismo e intentan destruirlo desde dentro.

Investiga que es Elk Cloner y quien es Rich Skrenta.

El primer virus informático fue Elk Cloner, un gusano, hecho por Rich Skrenta de 15 años.

¿Por qué crees que se hacen los virus?

Los que hacen virus se sienten poderosos cuando crean un virus, otros los hacen para robar información personal.

¿cuál es la necesidad de actualizar un antivirus?

Hay que actualizar los antivirus diariamente pues, cada día se fabrican miles y miles de virus, entonces, cuando éstos se fabrican, dejan una firma digital, esa firma digital, la tienen que tener los antivirus para poder detectar esos virus nuevos.

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

En algunos casos, el de pago te ofrece unas herramientas más de protección, muchas veces viene con un firewall. En otros casos el gratuito y el de pago no tienen mucha diferencia.

¿Qué es un antivirus online? Pon algún ejemplo

Es un antivirus en una web, que escanea tu ordenador desde la misma web, pero no te ofrece tanta seguridad como si lo tuvieras instalado.

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

- ✓ **1 – Adware:** Un adware es un software que muestra anuncios. “Los adware se instalan generalmente sin que nosotros lo deseemos. Nadie quiere que le machaquen con publicidad constantemente mientras usa el ordenador”, explica Félix de Molina, responsable de Consultoría de Seguridad de VASS. “Los adware suelen rastrear nuestro uso del ordenador para mostrar publicidad que tiene que ver con nuestras búsquedas en diferentes buscadores o relacionados con los sitios que visitamos”.

- ✓ **2 – Spyware:** El spyware se trata de un software espía que recopila información de un ordenador. “Tras obtener los datos, los transmite a una entidad externa sin el conocimiento o el consentimiento del propietario del ordenador”, afirma Félix de Molina.

- ✓ **3 – Malware:** Se trata de códigos diseñados por ciberdelincuentes que tienen por objeto alterar el normal funcionamiento del ordenador, sin el permiso o el conocimiento del usuario. Este tipo de virus pueden destruir archivos del disco duro o corromper los archivos que tenemos albergados con datos inválidos.

- ✓ **4 – Ransomware:** “Esta práctica se cree que crecerá en 2015, especialmente enfocada a móviles”, advierte Félix de Molina, responsable de Consultoría de Seguridad de VASS. Consiste en que el pirata bloquea el smartphone con un mensaje en el que solicita un rescate para liberarlo. El usuario debe pagar dicho rescate en la moneda digital Bitcoin, para que no se pueda rastrear y se mantenga el anonimato del hacker.

- ✓ **5 – Gusanos:** Tiene la capacidad para replicarse en tu sistema, por lo que tu ordenador podría enviar cientos o miles de copias de sí mismo, creando un efecto devastador a gran escala.

- ✓ **6 – Troyano:** Se trata de un tipo de programa que, al ejecutarlo, le brinda a un atacante acceso remoto al equipo infectado.

- ✓ **7 – Denegación de servicio:** "Consiste en un ataque a un sistema de ordenadores o de red que causa que un servicio o recurso sea inaccesible a los usuarios legítimos", explica el responsable.

- ✓ **8 – Puerta trasera:** Es una secuencia especial dentro del código de programación, mediante la cual se pueden evitar los sistemas de seguridad del algoritmo (autentificación) para acceder al sistema.

- ✓ **9 – Phishing:** Se trata de una modalidad de ataque a través de un email. Los hackers son capaces de adaptarse a ti y/o a tu negocio para convencerte de hacer clic en links o para ingresar datos confidenciales que terminarán por instalar un código malicioso en tu ordenador. "Educar a los empleados acerca de los riesgos de abrir esos mails sospechosos puede prevenir un ciberataque", advierte de Molina.

- ✓ **10 – Darknets o deep web, comercio de vulnerabilidades:** Félix de Molina augura un crecimiento en la venta de "exploits" o guías de vulnerabilidades, mediante los cuales personas sin experiencia podrán llevar a cabo ciberataques.

- ✓ **11 - Bombas lógicas o de tiempo:** estos programas se activan al producirse un acontecimiento determinado. La condición es una fecha, si no se produce la condición permanece oculto al usuario.
- ✓ **12- Hoax:** son virus y no tienen la capacidad de reproducirse a sí solos. Son mensajes que incitan al usuario a hacer copias y enviarlas a sus contactos. Suelen apelar a los sentimientos morales ejemplo: (ayuda a un niño enfermo de cáncer).

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

- ✓ **Kaspersky** ofrece más seguridad ante el peligro de virus gusanos
- ✓ **Nod 32** ofrece más seguridad escaneando online las webs
- ✓ **Mcafee** escanea las descargas sin previo aviso al usuario

Investiga en que consistían los siguientes virus.

1. Morris (1988)

Uno de los primeros grandes ataques que se recuerdan. En 1988 apenas había cerca de 60.000 ordenadores con conexión a internet en todo el mundo, pero este gusano infectó a más del 10% de esos usuarios. Su balance de víctimas no fue poca cosa: en su momento, los daños fueron estimados en cerca de 96 millones de dólares.

Este gusano marcó el inicio de una época: "Morris es un clásico", nos reconoce Víctor Escudero, especialista en ciberguridad de Necsia IT Consulting. "Por aquella época apareció

también el virus Viernes 13, que fue mucho más conocido, pero Morris marcó el camino de cómo se desarrollarían otros muchos gusanos posteriores".

Un disquete con el código del virus Morris

Un disquete con el código del virus Morris (Wikimedia)

2. CIH/Chernobyl (1998)

El virus CIH supuso un auténtico quebradero de cabeza para millones de usuarios de Windows 95, Windows 98 y Windows ME. Una vez instalado dentro del ordenador, acababa infectando y eliminando la información de todo el equipo. En ocasiones incluso llegaba a afectar a la BIOS, con lo que el ordenador, una vez infectado, era incapaz de arrancar.

CIH afectó a más de 60 millones de usuarios en todo el mundo y provocó unos daños económicos cercanos a los 1.000 millones de dólares. Por aquel entonces, el mundo empezó a conocer el verdadero potencial y la verdadera amenaza de este tipo de infecciones.

Captura de pantalla del virus CIH/Chernobyl

Captura de pantalla del virus CIH/Chernobyl (Wikimedia)

3.- Melissa (1999)

Casi llegados a la burbuja puntocom apareció Melissa, uno de los primeros virus que implicó la acción de sus propios usuarios, que fueron los que lo abrieron. La trampa: un archivo llamado List.doc que contenía un sinfín de contraseñas y registros para acceder de manera gratuita a diversas webs pornográficas.

Melissa hizo del correo electrónico su mayor fuerza: en cuanto abrías el documento, el virus accedía a tus contactos y reenviaba el correo a otras 50 personas. Además, infectaba todos tus archivos de Word, con lo que el virus no solo fue destructivo, también viral.

4. I love you (2000)

De lejos, el virus más conocido de nuestra historia reciente. Y es que ahora todos estamos acostumbrados a ignorar cualquier correo electrónico con cierta apariencia de sugerencia sexual, pero hace 17 años la cosa era muy distinta, con lo que el envío de una aparente carta de amor no hizo sospechar a casi nadie.

¿El resultado? El virus I love you, que eliminaba todos los archivos jpg del ordenador, afectó a más de 50 millones de usuarios y generó unas pérdidas aproximadas de 5.500 millones de dólares. Y los 'ingenuos' no solo fueron los usuarios corrientes y molientes: grandes instituciones como el Parlamento Británico o el mismísimo Pentágono también sucumbieron a I love you.

El virus I love you se adjuntaba en un correo electrónico

El virus I love you se adjuntaba en un correo electrónico (Wikimedia)

5.- Mydoom (2004)

Una de las mayores pesadillas de nuestra historia reciente. Mydoom inutilizaba gran parte de las herramientas de seguridad de Windows, con lo que era capaz de moverse a sus anchas por todo el sistema operativo y el ordenador del usuario infectado. La histeria llegó hasta tal punto que Microsoft llegó a ofrecer 250.000 dólares a quien encontrase al responsable de este ataque informático.

Mydoom es uno de los virus que se ha propagado más rápidamente: durante su época de mayor actividad, redujo hasta en un 10% el tráfico global en internet. Hasta su eliminación, este virus generó unos daños cercanos a los 40.000 millones de dólares, según las estimaciones llevadas a cabo en aquella época.

Mydoom fue un auténtico dolor de muelas para Microsoft

Mydoom fue un auténtico dolor de muelas para Microsoft (Wikimedia)

6.- Conficker (2008)

Otra de las grandes pesadillas de Microsoft. Conficker se dio a conocer en octubre de 2008, cuando atacó directamente a la columna vertebral de los sistemas de seguridad de Windows para infectar a todos sus equipos.

Una vez dentro del ordenador, Conficker desactivaba herramientas como Windows Automatic Update, Windows Security Center, Windows Defender y Windows Error Reporting. Además, su ámbito de actuación era casi ilimitado: se difundía entre contactos, recolectaba información y datos personales del usuario e infectaba otros archivos. Como en el caso de Mydoom, Microsoft también ofreció una recompensa de 250.000 dólares para encontrar a su responsable.

7.- WannaCry (2017)

El culmen de todo. El malware WannaCry es el último que ha lanzado un aviso a nivel global: ya no se trata de infectar a usuarios aislados, sino de meterse en las entrañas de grandes corporaciones e instituciones públicas, infectar sus equipos y robarles información, creando un pánico que plantea casi más preguntas que respuestas.

La principal cuestión ahora está clara: ¿ha tocado techo WannaCry? ¿Se propagará aún más? ¿Habrá nuevos ataques? ¿Qué o quiénes se verán afectados? ¿Quién está detrás de todo esto? ¿Deberían preocuparse los estados y grandes corporaciones por el progresivo aumento de este tipo de prácticas?

Un programador muestra la captura de pantalla en la que se pide un rescate en bitcoins por los documentos encriptados por un virus del tipo WannaCry

Un programador muestra la captura de pantalla en la que se pide un rescate en bitcoins por los documentos encriptados por un virus del tipo WannaCry (Ritchie B. Tongo / EFE)

Lo peor es que no sabes quién te está atacando

Víctor Escudero ve un cambio de tendencia: “Antes los ataques eran genéricos y tenían una motivación clara: infectar a toda la gente que fuera posible. Ahora es distinto: se trata de lanzar ataques dirigidos, con una víctima clara e identificada, para robar información o afectar al funcionamiento de los servicios de grandes empresas o instituciones públicas”.

Escudero lo tiene claro: “Quizá las grandes empresas no están invirtiendo todo el dinero que pueden en ciberseguridad, pero están muy activas, porque saben de sobra que el daño económico al que se enfrentan puede ser mucho mayor”. En cuanto a los estados, “todos saben que se enfrentan a una amenaza real y que tienen que ponerse las pilas. Muchas de las nuevas ‘guerras’ van a venir por internet, a través de ciberataques”.

Antes en las guerras tenías que dominar el espacio aéreo; ahora debes dominar el digital”

VÍCTOR ESCUDERO Especialista en ciberguridad deNecsia IT Consulting

Se trata, por tanto, de un cambio en el terreno de batalla: “Antes, en las grandes guerras, tenías que tener el dominio del espacio aéreo. Ahora lo que los estados tiene que hacer es aprender a dominar el terreno digital, porque es ahí donde se van a generar los futuros problemas de seguridad”, asegura Escudero.

Quizá lo peor de todo, en su opinión, es que en este nuevo escenario ni siquiera sabes contra quién luchas: “En las guerras de toda la vida, los contrincantes se identifican entre sí y está todo delimitado, pero ahora no es así. ¿Cómo puede saber un estado quién le está atacando? Puede haber sospechas o incluso puede que lo tenga claro, pero no podrá acusar a un país de manera directa”.

Hay que invertir en defensa... y en ataque

Víctor Escudero nos describe un panorama inquietante: “Ahora que un estado no puede acusar a otro de atacarle si no lo tiene claro, al 100%, ya no solo se trata de defenderse. Ahora los países están invirtiendo en hacer lo mismo que sus enemigos: atacar sin que les descubran. Estados Unidos invierte mucho dinero en defensa, pero también en ataques, incluso contra sus propios ciudadanos”.