**CUESTIONARIO VIRUS**

CUESTIONARIO VIRUS

1. **Que é un antivirus?**

É un programa deseñado para detectar e eliminar programas de software malicioso grazas a unha lista que contén os nomes dos diversos virus, métodos e formas de desactivalos. A súa efectividade está na súa capacidade de actualización.

1. **Explica en que consisten os seguintes tipos de antivirus:**

Eliminador

Vacina

Detector

Programa antivirus configurado simplemente para eliminar aos virus.

Programa configurado para detectar e avisar cando exista algunha alteración dos arquivos canto antes.

Programa antivirus configurado para sacar o malware dunha computadora en caso de que pasara desapercibido.

1. **Que é Reaper e Creeper?**

Creeper

Reaper

No ano 1971 apareceu Creeper (enredadeira), o primeiro virus informático da historia desenvolvido por Bob Thomas. Porén, este virus era completamente inofensivo e fora creado para confirmar se podía moverse entre ordenadores.

Tempo despois apareceu Reaper (podadora), o primeiro antivirus da historia. Este antivirus era moi efectivo posto que cando detectaba o ataque de Creeper eliminábao do sistema evitando a súa propagación.

1. **Que é un virus boot?**

É un virus que infecta o sector de arranque dos disquetes ou o rexistro de arranque principal dos discos duros. O seu código execútase cando o sistema se inicia desde un disco infectado e ,despois de cargarse, infecta outros disquetes aos que se accede na computadora infectada.

1. **Que é un virus hijackers?**

É un programa que ten como obxectivo secuestrar o navegador, cambiando a páxina de inicio por unha inxectada de forma directa por un pirata informático ou por un programa malicioso.

1. **Que é o virus keylogger?**

É un software ou hardware que pode interceptar e gardar as pulsacións realizadas no teclado dun equipo infectado. Este virus sitúase entre o teclado e o sistema operativo para interceptar e rexistrar a información sen que o usuario o note.

1. **Que é o virus zombie?**

É unha estratexia para facer uso de computadoras alleas co obxectivo de que estas se convertan en ferramentas que replican e envían cantidades enormes de spam pola rede e formar “botnets” dunha actividade ilegal sen que o usuario se de conta.

1. **Cal é a característica principal do antivirus AVAST?**

A protección segura das contrasinais do usuario xunto coa rede doméstica e a realización frecuente da limpeza do navegador.

1. **Por que se denominan virus aos virus informáticos?**

Un virus informático ten como obxectivo alterar o funcionamento da computadora reemplazando arquivos executables por outros infectados. Como podemos ver, un virus informático actúa da mesma maneira ca un biolóxico, por iso se chama así.

1. **Investiga que é Elk Cloner e quen é Rich Skrenta.**

**Elk Cloner** (1982) é o primeiro virus informático coñecido que tivo unha expansión real desenvolvido por **Rich Skrenta**, un estudante de 15 anos. Este virus orixinouse por unha broma aos seus amigos para que os seus xogos deixaran de funcionar. Este programa acabou propagándose con moita rapidez a través dos disquetes compartidos dos ordenadores Apple II. A característica principal deste virus era a mensaxe que aparecía no arranque 50 cun disco duro infectado.

1. **Por que cres que se fan os virus?**

Principalmente os virus créanse coa intención de **gañar diñeiro** xa sexa enganando ao usuario para comprar ou descargar un software ou forzalo a ver anuncios ou páxinas web. Tamén, ao gravar as pulsacións do teclado, poden facerse con datos persoais como contrasinais ou o número da tarxeta de crédito e roubarlle a súa identidade.

Outra razón sería máis ben **política** para roubar datos importantes do partido contrario.

1. **Cal é a necesidade de actualizar un antivirus?**

Unha das ferramentas que ten un antivirus para impedir ou detectar a tempo un virus é a detección por medio da súa base de datos. O antivirus toma un fragmento de código do virus e incorpórao a súa base de datos para que cando ingrese un novo arquivo compare ese fragmento co arquivo que se estea usando. A eficiencia deste proceso está vinculada ca **calidade da base de datos**.

1. **Que diferencias hai entre a protección dun antivirus gratuíto e un de pago?**

Antivirus gratuíto

Un antivirus gratuíto ofrece protección básica para o ordenador protexéndoo de virus comúns, bloqueando aplicacións e arquivos perigosos e advertindo sobre sitios web sospeitosos.

Antivirus de pago

Mentres que un antivirus de pago ofrece unha protección máis avanzada controlando a forma na que se comportan as aplicacións e os malware para evitar a infección antes de que ocorra.

**Exemplos.**

1. **Que é un antivirus online?**

É un programa o cal non é necesario instalar xa que se pode realizar en determinadas páxinas web. A súa función é escanear o ordenador para comprobar se o noso equipo está infectado con algún virus e logo desinfectalo.

* BitDefender online
* McAffe online
* Kaspersky online.

1. **Indica en que consisten cada un dos seguintes tipos de virus:**

Adware

Spyware

Software non desexado deseñado para mostrar anuncios no monitor do usuario co fin de xerar lucro aos seus autores (software publicitario).

Software malicioso utilizado para recopilar información dun ordenador e transmitir dita información a unha entidade externa sen o permiso do dono do ordenador (programa espía).

Malware

Calquera tipo de software que realiza accións dañinas nun sistema informático de forma intencionada e sen o consentimento do usuario (software malicioso) .

Ransomware

Tipo de programa dañino que restrinxe o acceso a determinadas partes ou arquivos do sistema operativo infectado e pide un rescate (diñeiro normalmente a modo de bitcoins) a cambio de quitar esta restrición (secuestro de datos).

Troianos

Gusanos

Códigos de programa que se reenvían a si mesmos para propagarse polas redes de ordenadores e así bloquear e saturar os sistemas.

Softwares maliciosos que se presentan ao usuario como programas inofensivos, pero que, ao executalo, modifican o sistema deixándoo indefenso para que outros programas poidan acceder ao seu interior.

Porta traseira

Denegación de servicio

Ataque a un sistema de computadoras ou rede que causa que un servizo ou recurso sexa inaccesible aos usuarios lexítimos.

Secuencia especial ou termo traseiro dentro do código de programación, mediante a cal se poden evitar os sistemas de seguridade do algoritmo para acceder ao sistema.

Bombas lóxicas ou de tempo

Phishing

Conxunto de técnicas que perseguen o engano a unha vítima gañándose a súa confianza, facéndose pasar por algo que non é e así manipulala e facer que realice accións que non debería facer.

Parte dun código insertado intencionalmente nun programa informático que permanece oculto ata cumprirse unhas condicións preprogramadas para executarse. Esta acción debe ser indesexada e descoñecida ao usuario do software.

Darknets ou deep web

Comercio de vulnerabilidades

Lugar virtual onde se gardan contidos que non están indexados en ningún dos buscadores existentes debido a que na súa maioría non cumpren as regras de servizos e noticias de Internet.

Actividade económica na que soe haber negocios moi lucrativos como a compra-venta de información sobre vulnerabilidades, a contratación de persoas que se dedican á procura de vulnerabilidades, a venta de produtos que detectan, solucionan ou mitigan o impacto de vulnerabilidades.

1. **Compara os seguintes antivirus e indica as vantaxes de cada un deles:**

McAfee

ESET Nod32

Kaspersky

Kaspersky ofrece unha gran protección fronte o malware, administra contrasinais e controles parentais e autentica dous factores para a conta en liña. Non desacelera case o sistema e é compatible con dispositivos Windows, Android e iOS.

* Protección máxima.
* Moi baixo impacto do rendemento.
* Antivirus máis sinxelo de xestionar.ESET ofrece unha cantidade igual de protección adicional a McAfee. Escanea todas as descargas antes de que se instalen no equipo e detén o proceso se atopa unha ameaza e tamén proporciona filtrado de correo electrónico. É compatible con dispositivos Windows, Android, macOS e Linux.
* Avanzado método antirroubo.
* Baixo impacto co sistema.
* As exploracións fanse durante o tempo de inactividade.

McAfee ofrece protección fronte a unha serie de ameazas, mantén aos usuarios a salvo do malware propagado a través de plataformas de rede e protexe dispositivos ilimitados. Tampouco desacelera tanto o sistema mentres o antivirus funciona e é compatible con dispositivos Windows, Android e iOS.

* Infalible contra calquera ameaza.
* Antivirus que menos recursos gasta.
* Pódese instalar en dispositivos ilimitados.

1. **Investiga en que consistían os seguintes virus:**

Morris (1988)

É o primeiro exemplar de malware autorreplicable que afectou a Internet. Este gusano foi desenvolvido por Robert Tappan Morris, estudante de 23 anos, e infectou a varios servidores conectados á rede incluídos a algúns da NASA. O programa intentaba descubrir as contrasinais de outras computadoras e non foi configurado para causar dano, pero un fallo no seu código fixo que se produciran fallos en centos de computadoras.

CIH/Chernobyl (1998)

No seu momento foi considerado un dos virus máis perigosos e destrutivos, era capaz de eliminar información crítica do usuario e incluso sobrescribir o sistema BIOS impedindo o arranque do equipo. Este virus foi desenvolvido polo estudante Chen Yinghao co obxectivo de deixar en ridículo a algunhas compañías de software que presumían da eficacia dos seus programas antivirus. Cando se propagou o virus, el mesmo publicou un antivirus gratuíto.

Melissa (1999)

É un macrovirus que infecta documentos de Microsoft Office. Este virus era propagado a través de e-mails nos cales se achegaba un arquivo chamado List.doc e que “contiña” unha lista de contrasinais para acceder a 80 páxinas pornográficas. O autor, David L. Smith, declarou que creara o virus en memoria dunha bailarina da cal namorara. Foi condenado e multado.

I love you (2000)

É un gusano escrito en VBS presentado en forma de e-mail co asunto ILOVEYOU e un arquivo achegado co nome de “LOVE-LETER-FOR-YOU.txt.VBS”. Este, ao ser aberto infectaba o ordenador e autoenviábase ás direccións de correo que o usuario tivera na súa axenda de direccións. O virus borraba, copiaba e renomeaba múltiples arquivos do disco duro. Foi desenvolvido por Onel de Guzmán para a aplicación da súa tese.

Mydoom (2004)

É un gusano informático que afecta a Microsoft Windows. Converteuse no gusano de correo electrónico que máis rápido se propagou, récord que non se superou ata 2016. Non se sabe quen foi o autor. Este virus transmítese por correo electrónico aparecendo como un erro de transmisión. O correo contén un arquivo achegado que, se se executa, reenvía o gusano ás direccións de correo electrónico que se atopan nos arquivos locais.

Conficker (2008)

É un gusano informático que ataca o sistema operativo Microsoft Windows explotando unha vulnerabilidade no seu servizo. O gusano propágase a si mesmo a través dunha vulnerabilidade do desbordamento de búter do servicio Server de Windows. Cando infecta un ordenador, desactiva varios servizos e logo contacta cun servidor onde recibe instrucións para propagarse, recolectar información ou descargar malware.

WannaCry (2017)

É un programa dañino de tipo ransomware. Estado Unidos inculpou ao norcoreano Park Jin Hyuok de ser o seu creador. Este virus comezou a través do uso dunha vulnerabilidade nas defensas de rede ou un ataque de phishing ben executado sobre unha primeira vítima. Cando é executado, atopa e localiza unha variedade de arquivos que logo notifica ao usuario de que os arquivos foran encriptados, reclamando un pago en bitcoins para desfacelo.