Integrantes

- Lucas Ayala
- Dana Garcete
- Richard Aguilera
- Ricardo Gamarra

Introducción

Los avances tecnológicos han transformado nuestra sociedad de manera significativa. Uno de los aspectos más destacados de esta revolución es la informática y la conectividad digital. Sin embargo, junto con los beneficios, también han surgido desafíos. Uno de estos desafíos es la amenaza constante de los virus informáticos.

Los virus informáticos son programas maliciosos diseñados para infiltrarse en sistemas informáticos, propagarse y causar daño. Estos pueden afectar desde computadoras personales hasta redes empresariales, y su impacto puede ser devastador. En esta investigación, exploraremos la naturaleza de los virus informáticos, sus métodos de propagación y las medidas de seguridad necesarias para proteger nuestros sistemas.

Que es Virus Informáticos

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.

Tipos de Virus informáticos

Virus de acción directa

Este tipo de virus es uno de los más comunes. Entran e infectan al dispositivo, causan el daño de una vez y en algunos casos se borran después de ejecutar su código. Usualmente usan como programa anfitrión a los archivos ejecutables (aquellos con extensión «.exe»).

Uno de los más conocidos son los keyloggers.

Virus residentes

Como su nombre lo indica, este tipo de virus residen en el ordenador, usualmente se alojan en la memoria RAM del dispositivo. Esto les permite permanecer en la computadora o teléfono, aunque el archivo original de infección haya sido eliminado. Son activados cuando el sistema operativo se ejecuta.

Virus de sobreescritura

Estos virus se caracterizan por sobreescribir o borrar la información del archivo que ha sido infectado. La manera de limpiar el archivo infectado es borrándolo completamente, perdiendo la información contenida en el archivo.

Estos son fáciles de reconocer porque los archivos quedan parcial o totalmente inservibles. Usualmente se propagan por correo electrónico.

Virus FAT

Estos son un sistema de ficheros llamados Tabla de Asignación de Ficheros o File Allocation Table (FAT) en inglés.

Almacenan la información sobre la ubicación de los archivos del sistema, el espacio disponible en el disco, entre otros. Los virus FAT atacan a estos ficheros pudiendo impedir el acceso a ciertas partes del disco o incluso ocasionando la pérdida de directorios completos.

Virus de secuencia de comandos web

Este tipo de virus es capaz de sobrepasar la seguridad del navegador web y puede cambiar configuraciones, alterar o dañar los datos del usuario, hacerse pasar por un usuario, entre otras cosas.

Virus de multipartitos

Este es un tipo de virus bastante avanzado, ya que son capaces de implementar múltiples técnicas de infección y daño de manera simultánea. Pueden atacar los archivos ejecutables e incluso al sistema de arranque. Al alojarse en distintas partes del sistema se hace difícil su eliminación.

Ejemplos de Virus Informáticos

- **Adware**: Software que muestra publicidad no deseada o engañosa, a menudo en forma de pop-ups.
- **Spyware**: Software espía que recopila información del usuario, como datos de navegación, personales y bancarios.
- **Malware**: Códigos maliciosos diseñados para alterar el funcionamiento normal del dispositivo sin permiso del usuario.
- **Ransomware**: Bloquea el dispositivo y solicita un rescate, generalmente en Bitcoin, para liberarlo.
- **Gusanos**: Capaces de replicarse y enviar copias de sí mismos, causando un efecto devastador a gran escala.
- **Troyano**: Se presenta como un ejecutable legítimo, pero al activarlo, permite el acceso remoto al equipo infectado.

Causas de los virus Informáticos

Motivaciones financieras: Muchos virus son creados con el objetivo de robar información financiera o extorsionar a los usuarios para obtener dinero.

Vandalismo digital y desafío técnico: Algunos creadores de virus lo hacen simplemente por el deseo de causar daño y ver el caos que pueden generar o para probar sus habilidades técnicas.

Propaganda o hacktivismo: Algunos virus se crean para difundir un mensaje político o social. Estos pueden redirigir a los usuarios a sitios web específicos, mostrar mensajes en pantalla o incluso dañar sitios web de organizaciones o individuos.

Guerra cibernética: Las naciones pueden desarrollar y usar virus para atacar infraestructuras críticas de otras naciones, recopilar inteligencia o causar daño económico.

- **Distribución de publicidad:** Algunos programas maliciosos, como el adware, están diseñados para mostrar anuncios no deseados al usuario, generando ingresos para el creador del malware.
- **Creación de botnets:** Algunos virus tienen como objetivo infectar tantas máquinas como sea posible para crear una red de bots que luego puede ser utilizada para ataques DDoS, distribución de spam o para otros fines maliciosos.
- **Explotación de vulnerabilidades:** Los virus a menudo se crean para explotar vulnerabilidades específicas en software o sistemas operativos. Cuando se descubre una nueva vulnerabilidad, los ciberdelincuentes pueden apresurarse a crear y distribuir un virus antes de que se lance una solución.

Como funcionan los virus Informáticos

Los virus informáticos pueden entrar al sistema mediante emails a través de los archivos adjuntos de correo, descarga de archivos (como aplicaciones, documentos o *plugins*), servicios de mensajería o redes sociales, o incluso mediante publicidad engañosa.

El proceso de vida de un virus informático se puede comprender a través de las fases por las que pasa dentro del sistema una vez se ha establecido en el programa anfitrión:

- **Fase durmiente:** el virus se esconde en el sistema.
- **Fase de propagación:** el virus se auto-replica en distintos archivos a lo largo del sistema.
- **Fase de activación:** en esta fase, espera una acción específica para ser activado, puede ser una acción del usuario o simplemente un plazo de tiempo determinado.
- **Fase de ejecución:** finalmente, el virus ejecuta su código malicioso, afectando al dispositivo.

Métodos de Propagación de los virus

- **Archivos adjuntos en correos electrónicos**: Los virus a menudo se adjuntan a correos electrónicos y se activan cuando el archivo adjunto es abierto.
- **Descargas de Internet**: Descargar software o archivos de fuentes no confiables puede resultar en la instalación de virus.
- **Mensajería instantánea**: Los virus pueden propagarse a través de enlaces infectados enviados por servicios de mensajería como Skype o Facebook Messenger.
- **Redes sociales**: Vínculos maliciosos en redes sociales pueden llevar a sitios que instalan virus automáticamente.
- **Dispositivos de almacenamiento externos**: Conectar dispositivos infectados como USBs o discos duros externos puede propagar el virus.

- **Aplicaciones móviles sospechosas**: Descargar aplicaciones de fuentes no oficiales puede introducir virus en dispositivos móviles.
- **Ingeniería social**: Mensajes engañosos que incitan a los usuarios a ejecutar programas que contienen virus.
- **Sitios web comprometidos**: Visitar sitios web infectados puede resultar en la descarga automática de virus sin el conocimiento del usuario

Impacto de los Virus Informáticos

- **Rendimiento lento o congelación**: Los virus pueden consumir recursos del sistema, lo que resulta en una disminución del rendimiento o incluso en la congelación del dispositivo.
- **Archivos dañados o eliminados**: Algunos virus están diseñados para dañar o eliminar archivos importantes, lo que puede llevar a la pérdida de datos críticos.
- **Ventanas emergentes constantes o adware**: Los virus pueden generar una cantidad excesiva de publicidad no deseada, interrumpiendo la experiencia del usuario.
- **Fallos del programa y del sistema operativo**: Los virus pueden corromper el software y los sistemas operativos, causando errores y fallos.
- **Mal funcionamiento de aplicaciones, archivos y otros programas**: Los virus pueden interferir con el funcionamiento normal de las aplicaciones y otros programas instalados.

Ejemplos de Virus Notables

- **WannaCry**: Un ransomware que afectó a cientos de miles de computadoras en más de 150 países en 2017, explotando una vulnerabilidad en Windows.
- **Clop Ransomware**: Una variante del CryptoMix ransomware que ataca principalmente a usuarios de Windows, cifrando archivos y deshabilitando aplicaciones y defensas del sistema
- **Cyborg**: Un ransomware que se disfraza como actualizaciones de Windows y cifra archivos y programas, exigiendo un rescate para su descifrado.
- **Zeus Gameover**: Parte de la familia Zeus de malware, este troyano roba información bancaria y fondos sin necesidad de un servidor centralizado de comando y control.

Prevención

- **Descarga software de fuentes confiables**: Evita descargar programas de sitios web desconocidos o sospechosos.
- **No hagas clic en enlaces sospechosos**: Evita abrir enlaces o archivos adjuntos de correos electrónicos no solicitados.
- **Mantén tu sistema operativo actualizado**: Las actualizaciones suelen incluir parches de seguridad para vulnerabilidades recién descubiertas.
- **Realiza copias de seguridad regularmente**: Esto te permitirá recuperar tus datos en caso de que un virus los afecte

Conclusión

Los virus informáticos son programas maliciosos diseñados para alterar el funcionamiento normal de dispositivos informáticos sin el permiso o conocimiento del usuario. Pueden propagarse a través de diversos métodos, como el correo electrónico, la mensajería instantánea y las redes sociales. Algunos virus son inofensivos y solo causan molestias, mientras que otros pueden destruir datos o bloquear redes informáticas. Es fundamental proteger nuestros sistemas con programas antivirus y mantenernos informados para prevenir posibles infecciones.