

Enfermedad y cura: virus y antivirus

Sistemas operativos

Alumno y alumna:
Méndez Sánchez Erick Jair
Rodriguez Colorado Carla Elizabeth

Contenidos

01

Malware

02

Antivirus

03

**Casos
específicos**

04

**Los sistemas
operativos contra
el malware**

05

**Problema de
Halting y
antivirus**



MALWARE

I. Malware

Programa que busca maliciosamente información o dañar el sistema y puede replicarse.

El malware puede ser:

1. Spyware
2. Ransomware
3. Adware
4. Virus
5. Gusanos

VIRUS

El virus es un tipo de malware tiene de características:

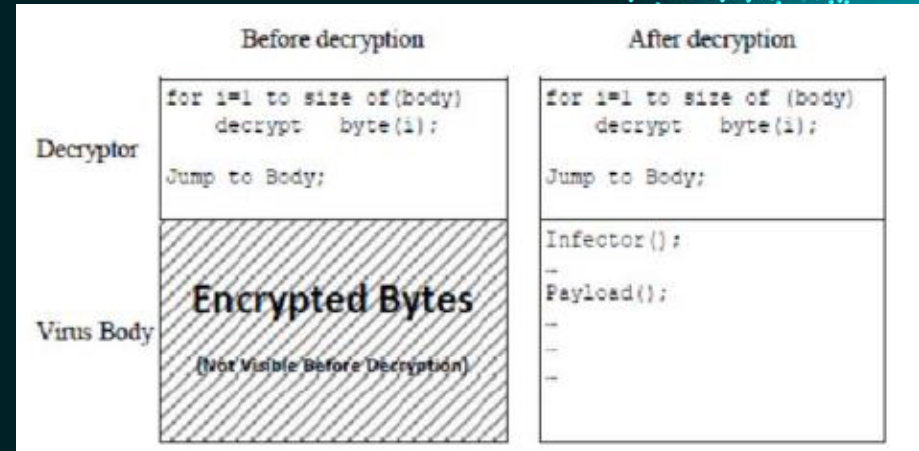
- Propagarse de un host a otro
- Replicarse
- No puede reproducirse ni propagarse sin programar (sin un archivo)

Tipos de virus

Pueden clasificarse por su forma de propagación, de funcionamiento o el daño que causa

Virus clasificados por su forma de propagación

- Boot virus
- Virus parásito
- Macrovirus
- Caballo de troya
- Virus de archivos
- Bomba
- Virus polimórfico





ANTIVIRUS

Antivirus

Software que protege a una computadora o dispositivo móvil de virus informáticos y otras formas de malware.

Un antivirus

- Detecta
- Evita
- Elimina

Se recomienda que ejecute en segundo plano para que siempre “vigile” el sistema.



Antivirus

Comparan los archivos o su comportamiento en ejecución contra una base de datos, buscando malware conocido o desconocido

Tipos de detección

- Reconocimiento de firma
- Métodos heurísticos
- Descifrado general



Técnicas de análisis



Dinámico

Observa
funcionalidad de
programa en
ejecución



JUPITER

Analiza partes de
código sin ejecutar



VENUS

Hace uso de las dos
técnicas anteriores

Static Analysis	Dynamic Analysis
Fast and safe	Time consuming and vulnerable
Good in analyzing multipath malware	Difficult to analyze the multipath malware
Cannot analyze obfuscated and polymorphic malware	Cannot analyze obfuscated and polymorphic malware
Low level of false positive (Accuracy is high)	High level of false positive(Accuracy is low)

Reconocimiento de firma

Primeros virus eran parásitos e infectaban sistema operativo DOS.

Dichos virus atacaban los entry points

- Se le asigna una firma a los virus
- Las firmas son parte de código mediante el cual se puede distinguir un virus
- Base de datos de firmas
- Análisis dinámico e híbrido
- En Windows usan API's

Métodos Heurísticos

Analizan
comportamiento

Probabilidades de que
un archivo tenga
comportamiento inusual

Falsos Negativos

Indicadores como:
fechas de archivo,
tamaño, instrucciones
de acceso a recursos,
etc.

Descifrado general

Usa tecnología virtual: CPU emulado, base de datos con firmas y módulo de control emulado. Se realiza:

- Ejecuta archivos potencialmente malignos en entorno controlado y se observa comportamiento.
- Se espera la descriptación y se ejecuta, buscando firma.
- Métodos heurísticos para virus metamórficos.



An abstract digital graphic on the left side of the image. It features a dense cluster of small, bright blue dots that form a circular, particle-like structure. From the center of this cluster, several bright blue light rays or beams of light extend outwards, creating a sense of motion and energy. The background is a solid dark teal color.

CASOS ESPECÍFICOS

Virus FAT

Es un virus que ataca el sistema de archivos (FAT) que se propaga a través de archivos externos

Daña el sistema de asignación de archivos y los archivos:

- Se vuelven ilegibles
- Se eliminan


Causan pérdidas permanentes y en ocasiones vuelve inservible al SO



Virus de booteo

- Infecta el sector de arranque de disquetes o el registro de arranque principal
- En la actualidad, existen programas denominados "bootkits" escriben su código en el MBR se cargan al principio del proceso de arranque y ocultan las acciones del malware.
- El único criterio para un sector de arranque es que contener 0x55 y 0xAA como sus últimos dos bytes.



An abstract digital background on the left side of the slide. It features a dense field of small, bright blue dots that form a curved, wave-like pattern. From this pattern, several bright blue light rays or beams of light emanate, extending towards the right. The overall color scheme is dark blue and black, with the bright blue elements providing a strong contrast.

Los sistemas operativos contra el malware

Los sistemas operativos contra el malware

Windows (76%)
Microsoft Defender

macOS (16%)
Xprotect
Gatekeeper

ChromeOS
Sandboxing

Android y iOS





El problema de Halting y los virus

Conclusiones

Bibliografía

Avast. (s.f.). ¿Qué es el malware? Avast. <https://www.avast.com/es-es/c-malware>

ChromiumOS. (s.f.). Chromium OS Sandboxing. Chromium OS Developer Guide.

Apple. (s.f.). Gatekeeper y la protección del tiempo de ejecución en macOS. Apple. <https://support.apple.com/es-mx/guide/security/sec5599b66df/web>

Google play. (s.f.). Privacidad, elementos engañosos y uso inadecuado de dispositivos. Google Play. <https://play.google.com/intl/es/about/developer-content-policy/>

Kuenning, G. (2002). How does a computer virus scan work? Scientific American. Springer. <https://www.scientificamerican.com/article/how-does-a-computer-virus/#>

Bibliografía

Windows. (2022). Microsoft Defender Antivirus in Windows. Microsoft.
<https://learn.microsoft.com/en-us/microsoft-365/security/defender-endpoint/microsoft-defender-antivirus-windows?view=o365-worldwide>

NCSC. What is an antivirus product? Do I need one? National Cyber Security Centre. UK.
<https://www.ncsc.gov.uk/guidance/what-is-an-antivirus-product>

Sanok, D. J. (2005). An analysis of how antivirus methodologies are utilized in protecting computers from malicious code. Proceedings of the 2nd annual conference on Information security curriculum development - InfoSecCD '05.
<https://doi.org/10.1145/1107622.1107655>

Bibliografía

- Lucas, S. (2021). The origins of the halting problem. Journal of Logical and Algebraic Methods in Programming. (121). doi.org/10.1016/j.jlamp.2021.100687.
- Phillippo, S. J. (1990). Practical virus detection and prevention. IEE Colloquium on Viruses and their Impact on Future Computing Systems 1990. pp. 2/1-2/4. <https://ieeexplore-ieee.org/pbidi.unam.mx:2443/document/190642/authors#authors>
- Stuart, G. (s.f.). To AV or not to AV? National Cyber Security Centre, UK. <https://www.ncsc.gov.uk/blog-post/av-or-not-av>
- Tahir, R. (2018). A Study on Malware and Malware Detection Techniques. International Journal of Education and Management Engineering, 8(2), 20-30. <https://doi.org/10.5815/ijeme.2018.02.03>
- Vigderman, A. & Turne, G. (2022). How does antivirus software works? Security ORG. <https://www.security.org/antivirus/how-does-antivirus-work/>