Universidad Nacional Autónoma de México

Facultad de ingeniería

División de Ingenieria Electrica y Electronica

Ingeniería en Computación

2023 - 1

Sistemas Operativos

Enfermedad y cura: virus y antivirus

Alumno y alumna:

Méndez Sánchez, Erick Jair

Rodriguez Colorado, Carla Elizabeth

Grupo: 6

Profesor: Gunnar Eyal Wolf Iszaevich

Enfermedad y cura: virus y antivirus

I. Introducción

Del 2009 al 2019 las infecciones por malware han incrementado más que el 6500% (Vigderman, A. & Turner, G.) debido al aumento de dispositivos informáticos actuales por lo que este trabajo presenta una revisión sobre el tema de *malware*, enfocado a los virus y antivirus, cómo se propagan y cómo son detectados. También se habla acerca del problema de detención (*Halting problem*) y su relación con la detección de virus y asimismo se discutirá si aún es necesario el uso de antivirus según el sistema operativo. El objetivo de este trabajo es ofrecer una visión de nivel introductorio para cualquier lector con conocimientos básicos sobre computación.

II. Malware

Es importante para este trabajo que el malware es cualquier programa que busca maliciosamente información o dañar el sistema de la persona atacada.

Un virus es un programa que puede replicarse a sí mismo y dañar otros programas. Así se tiene que un virus es un tipo de malware pero no todo el malware es un virus.

Existen diferentes tipos de malware como:

- Spyware: que buscan infiltrarse en el sistema y recolectar información sensible.
- Ransomware: el cual bloquea el acceso a los archivos hasta pagar el rescate.
- Adware: es crear ingresos para el desarrollador sometiendo a la víctima a publicidad no deseada. Algunos tipos comunes de adware son los juegos gratuitos y las barras de herramientas para el navegador.

Tipos de virus

Existen muchos tipos diferentes de virus informáticos, y pueden clasificarse de diferentes maneras según su forma de propagación, su forma de funcionamiento o el daño que causan. Los virus que se clasifican según su método de propagación, entre algunos tipos se encuentran:

- Boot virus: Infecta el sector de booteo del disco de almacenamiento
- Virus parásito: Se “adhiere” a archivos ejecutables como parte de su código, este funciona donde sea que el programa original se ejecute.
- Macrovirus: Es un exploit (aprovecha vulnerabilidades) que ataca un macro lenguaje, se aprovecha de software como Word, Excel, etc.
- Caballo de troya. Los virus de troyano se llaman así porque se esconden detrás de un "caballo de Troya", es decir, un programa o aplicación que parece legítima pero que en realidad es malware. Una vez que se ejecuta el programa o aplicación, el virus de troyano se instala en la computadora y puede hacer cosas como robar información confidencial, destrucción de datos o utilizar la computadora para realizar ataques.

- Virus de archivo: Los virus de archivo son uno de los tipos más comunes de virus informáticos. Se propagan a través de archivos compartidos o descargados de Internet y se activan cuando se abren estos archivos. Una vez activados, pueden dañar el sistema operativo o borrar archivos importantes.
- Gusano: Los virus de gusano son similares a los virus de archivo, pero se propagan de forma más rápida y pueden replicarse sin necesidad de un archivo o programa específico. Pueden utilizar redes y correo electrónico para propagarse y pueden causar daños significativos al sistema operativo.
- Bomba: No se propaga por sí mismo pues este suele ser colocado por un humano o bien, un software, este se activa mediante algún evento.
- Virus polimórfico. Un virus polimórfico es un tipo de malware que se caracteriza por cambiar de forma constantemente para evitar ser detectado por software de seguridad, como los antivirus. Los virus polimórficos utilizan diferentes técnicas para cambiar de forma, como la encriptación, la inversión de bits o la adición de código aleatorio a su estructura.

  Estos virus suelen ser muy difíciles de detectar y eliminar, ya que sus patrones de malware cambian constantemente y pueden evitar ser detectados por las técnicas de detección de malware tradicionales, como la búsqueda de firmas de virus.

  Los virus polimórficos pueden ser peligrosos porque pueden infectar a una computadora o dispositivo móvil sin ser detectados y luego utilizar ese dispositivo como un punto de partida para infectar a otros dispositivos. También pueden utilizar el dispositivo infectado para realizar actividades maliciosas, como enviar spam o participar en ataques de denegación de servicio.

III. ¿Qué es un antivirus?

Un antivirus es un tipo de software que protege a una computadora o dispositivo móvil de virus informáticos y otras formas de malware. El antivirus detecta, evita y elimina el malware evaluando datos, archivos, páginas web y cualquier software. Los antivirus funcionan comparando los archivos contra una base de datos de malware conocido buscando malware conocido y desconocido. Así pues, se utilizan tres métodos de detección: detección específica conocida también como reconocimiento de firma, detección heurística y detección genérica o por descripción general.

Una vez instalado el antivirus es recomendable configurarlo para ser ejecutado en segundo plano para tener protección en tiempo real por lo cual el antivirus siempre estará ‘’vigilando’’ el contenido que se está ejecutando o abriendo en el dispositivo.

Cuando se habla de virus se piensa en los virus que afectan a los humanos y en este caso entre sus coincidencias curiosas se encuentra que los antivirus en ocasiones pueden

mostrar falsos positivos como en el 2019 donde Microsoft Defender malinterpretó el código del buscador Chrome y recomendaba la desinstalación del programa.

Es importante entender que un antivirus no significa que sea antimalware. Para este trabajo se tomó en cuenta que la mayoría de antivirus de terceros cuentan con ambos sistemas.

Un antivirus defiende de los virus informáticos y un anti-malware de otros tipos de malware.

IV. Tecnicas de analisis

El análisis de malware se divide en 3 categorías dependiendo del momento y la técnica utilizada para dicho análisis.

a. Análisis estático

Conocido también como análisis de código, consiste en el análisis de partes de código sin la necesidad de ejecutarlo. Esta técnica se usa ingeniería inversa con el fin de determinar el comportamiento de código malicioso.

Se usan distintas herramientas para el análisis estático, algunos métodos usados para esta técnica son: File Format Inspection, String Extraction, Fingerprinting, etc.

b. Análisis dinámico

También llamado análisis de comportamiento consiste en observar la funcionalidad de un programa ejecutándose, aquí se toman en cuenta aspectos como la llamada a funciones, control de flujos y analizando instrucciones y parámetros de funciones. En este método se realizan las pruebas en un ambiente virtual y es capaz de detectar una gran variedad de malware.

c. Análisis híbrido

Usa el análisis estático y dinámico para obtener mejores resultados, esto es, se combinan las técnicas de forma que se saca el mayor provecho de ambas.

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)

Tahir,R. (2017), *Comparison of Static and Dynamic Analysis*

V. Metodologías usadas por los antivirus para combatir malware

a. Reconocimiento de firma

Los primeros virus creados para las computadoras personales eran principalmente virus parásitos, muchos de las computadoras usaban DOS como sistema operativo y dichos virus atacaban a los archivos ejecutables de este (llamados COM). Dichos virus solían atacar los puntos de entradas (entry points, en muchos lenguajes es la función main), es así que los desarrolladores de antivirus al descubrir dicho comportamiento se enfocaron en la búsqueda de firmas en los archivos ejecutables.

Las firmas utilizadas eran una cadena de código que pueden ser reconocidas como virus, lo anterior al comparar dicha firma con las firmas de virus conocidas (almacenadas en una base de datos).

Actualmente este método se puede implementar de dos formas distintas; en la primera el usuario o administrador puede decidir cuándo realizar una inspección al sistema de archivos, mientras que en la segunda se realiza la metodología en un proceso en segundo plano de forma que todos los archivos a los que se accede son analizados y comparados en la base de datos en busca de firmas que sean potencialmente virus. El segundo método suele ser utilizado para verificar los archivos descargados de internet o bien cuando una aplicación es ejecutada.

El segundo método mencionado adquiere mayor eficacia si cuenta con ciertos permisos del sistema operativo, en Windows en concreto, las APIs son las que tienen esta función. Las API's son un conjunto de software que dan acceso a ciertas funcionalidades del sistema, sin embargo, dichas API's también son víctimas de ataques tales como los realizados por los Macro virus que intentan vulnerar las API's usadas por los macro lenguajes (Excel, Word, etc). Los macro virus son combatidos al almacenar los macros en zonas específicas de forma que el antivirus puede analizarlos de forma temprana.

b. Métodos heurísticos

Este tipo de metodología analiza los patrones de comportamiento de las aplicaciones, se enfoca en descubrir actividades fuera de las normas de operación. Estos métodos se utilizan para encontrar virus para los cuales no se conozca su firma y dado que analizan el comportamiento de los archivos, suelen ser utilizados (en conjunto con otras técnicas) para combatir tipos de virus como los polimórficos.

Los métodos heurísticos se basan en la probabilidad de que un archivo tenga un comportamiento inusual, esto hace que no sean tan precisos en comparación con otros métodos tales como el reconocimiento de firma. Esto puede ser un problema pues debido a que si se obtienen muchos falsos positivos entonces los usuarios eventualmente podrían ignorar las alarmas pensando que todas las sospechas son falsas.

Estos funcionan comparando patrones de comportamiento y características almacenados en una base de datos, misma donde se almacenan indicadores. Dichos indicadores pueden ser datos como fecha de creación de archivo, tamaño de archivo, instrucciones de acceso a recursos del sistema o bien instrucciones para modificar las propiedades de otros archivos.

Los métodos heurísticos consisten en dos pasos: en el primero es observar el comportamiento y almacenar información importante que puede ser verificada en caso de ataque, y en el segundo paso se detecta el malware de una familia de virus.

Los antivirus actuales que implementan los métodos heurísticos pueden configurar el nivel de rigurosidad a la hora de detectar virus, lo que en consecuencia implica un aumento o una

disminución en el número de virus encontrados. Estos métodos pueden ser utilizados en conjunto con otros, siendo esta una de sus mayores ventajas.

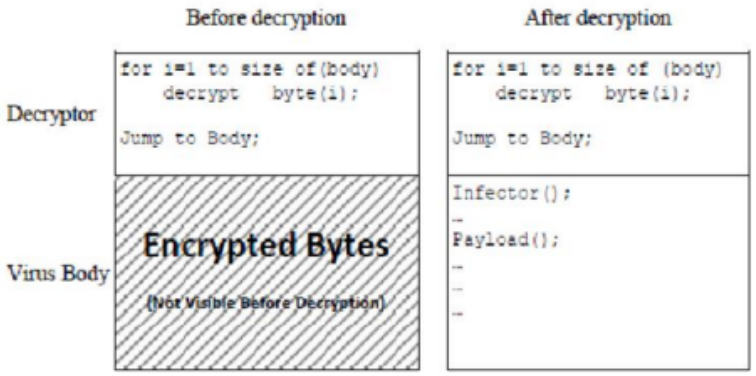
c. Descifrado general

Unos de los virus más complejos son los encriptados (aquí se incluyen los polimórficos y metamórficos), estos se componen de dos partes; En primer lugar, un pequeño código encargado del descifrado y en ocasiones también permite cifrar de nuevo una vez que se propaga y también se tiene el cuerpo de virus encriptado junto con la payload.

Los métodos de descifrado general utilizan tecnología virtual que se compone de tres componentes: un CPU emulado, una base de datos con firmas de virus y un módulo de control emulado. Este tipo de metodología ejecuta los archivos potencialmente malignos dentro del entorno virtual (que replica un entorno real de cómputo) y se observa el comportamiento, es un método muy seguro dado que todo se realiza dentro de un sandbox (entorno de pruebas).

Una vez que ocurre la desencriptación de la payload y se empieza a ejecutar, se busca la firma en la base de datos (componente del método) para determinar si se trata de un virus y actuar en consecuencia de lo obtenido. En caso de encontrar una amenaza, el antivirus se encarga de terminar el hilo de ejecución del malware antes de tener daños en el sistema o los datos.

Dado que la diferencia entre un virus metamórfico y un virus polimórfico es que el primero no tiene una sección de cifrado (pero aun asi cambia cada vez que se propaga), para la detección de virus metamórficos primero se identifica un comportamiento sospechoso con métodos heurísticos.



Tahir,R. (2017), *Structure of Encrypted Virus*

VI. Casos específicos

Ataques al FAT

El virus que ataca el sistema de archivos FAT (File Allocation Table) es un tipo de virus que se propaga a través de archivos compartidos o descargados de Internet y se activa cuando se abren esos archivos. Una vez activado, puede dañar la tabla de asignación de archivos

(FAT) del sistema operativo, lo que puede hacer que los archivos se vuelvan ilegibles o se pierdan.

Los virus que atacan el FAT suelen ser muy peligrosos, ya que pueden causar la pérdida permanente de datos y hacer que el sistema operativo deje de funcionar correctamente. Por lo general, estos virus se propagan a través de dispositivos de almacenamiento externos, como discos duros externos o memorias USB, y pueden infectar a la computadora o dispositivo móvil cuando se conectan a ella.

VII. El malware y los sistemas operativos

Algo que los usuarios pueden llegar a preguntarse, ¿se necesita un antivirus? La respuesta es que si se es un usuario suficientemente cuidadoso no se necesita, la mayoría de sistemas operativos tienen consigo ya antivirus.

Windows tiene el 76% (diciembre, 2020) de computadoras en el mundo de ahí que existen múltiples programas diseñados para este. En este caso el SO viene con Windows Defender que según el AV-Test Institute es lo suficientemente bueno para resguardar el sistema.

En el caso de macOS que tiene menos unidades en marcha globalmente no son el objetivo principal de los hackers pero aun así macOS presenta dos herramientas similares para la protección: XProtect que inspecciona por malware cada aplicación y Gatekeeper que no permite la ejecución de programas sin certificación.

Para ChromeOS donde el sistema solo se encuentra en el 2% del mercado global no se espera que sean un objetivo prioritario en la creación de malware. Además de que este sistema implementa el *sandboxing* que aísla cada aplicación y página web evitando que se pueda acceder directamente a la funcionalidad de nivel de sistema operativo.

Lo implementado por cada sistema operativo, el ser cauteloso al explorar internet y la seguridad que proporcionan los exploradores web vuelven que se vuelva suficiente no instalar un antivirus de terceros.

En el caso de los dispositivos móviles en general se ven menos amenazados que los sistemas como PC y laptops debido a que las aplicaciones que se tienen mayormente son descargadas de una tienda de aplicaciones la cual verifica la existencia de cualquier malware antes de la publicación de la aplicación, además se actualizan automáticamente cuando los desarrolladores encuentran bugs o agujeros en el programa. Es verdad que Android podría verse mayormente amenazado porque permite la instalación de aplicaciones fuera de la tienda a partir de apks que pueden contener malware, en cambio los sistemas iOS solo permiten la obtención de aplicaciones a través de AppStore entonces se encuentra con ningún peligro además que aísla cada app evitando la propagación del virus.

VIII. El problema de Halting y los antivirus

El problema de Halting

El problema de Halting, es un problema teórico en la teoría de la computación que plantea la pregunta de si es posible diseñar un programa de computadora que pueda determinar, para cualquier otro programa dado y cualquier entrada dada, si ese otro programa terminará o seguirá ejecutándose indefinidamente.

El problema de detención es importante porque tiene implicaciones para la teoría de la computación y la complejidad computacional. En particular, demuestra que hay problemas que no pueden ser resueltos por la computadora, independientemente de la velocidad o la capacidad de procesamiento.

El teorema de Halting, que demuestra la imposibilidad de resolver el problema de detención, fue propuesto por el matemático y lógico Alan Turing en 1936.

Aunque el problema de detención y los antivirus parecen no tener relación, en realidad hay una conexión entre ambos. El problema de detención demuestra que hay problemas que no pueden ser resueltos por la computadora, independientemente de la velocidad o la capacidad de procesamiento. Esto significa que, en teoría, no es posible diseñar un antivirus que pueda detectar y eliminar todos los virus o malware con certeza.

Los antivirus se basan en patrones conocidos de malware o en el comportamiento sospechoso para detectar virus y otro tipo de malware. Esto significa que, aunque pueden ser muy efectivos para detectar y eliminar muchos tipos de malware, es posible que no puedan detectar todo el malware que existe.

Además, los creadores de malware a menudo tratan de evitar la detección de los antivirus utilizando técnicas como el polimorfismo, lo que significa que los virus pueden cambiar de forma constantemente para evitar ser detectados. Esto puede hacer que los antivirus sean menos efectivos para detectar y eliminar ciertos tipos de malware.

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/#

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

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/