Backdoor de los antivirus

Víctor Páramo Domínguez
Instituto Tecnológico de Celaya: ITC
v_paramo@hotmail.com

Tomas Antonio Corrales Cortes
Instituto Tecnológico de Celaya: ITC
tomluc2001@hotmail.com

M. T. I. Francisco Gutiérrez Vera
Instituto Tecnológico de Celaya: ITC
francisco.gutierrez@itcelaya.edu.mx

M. C. Claudia Cristina Ortega González
Instituto Tecnológico de Celaya: ITC
claudia.ortega@itcelaya.edu.mx

Resumen

La finalidad del presente artículo es determinar si la seguridad que integran los antivirus más populares de este 2015, cuentan con las herramientas y medidas necesarias para afrontar los diversos tipos de ataques que se encuentran actualmente amenazando la seguridad e integridad de los dispositivos electrónicos en red.

Palabras Clave: Antivirus, malware, seguridad, software.

Abstract

The finality of the present article is determining if the security that integrates the antivirus have the proper measures and tools for diverse types of attacks, which are currently found threatening the security and integrity of the electronical devices on the web.

Keywords: *Antivirus, malware, security, software.*

1. Introducción

La constante evolución de las Tecnologías de la Información y las Comunicaciones (TICs) han tenido un impacto muy positivo en nuestras vidas e inciden directa o indirectamente en prácticamente todos los sectores de la sociedad. El término ciberseguridad define un conjunto de herramientas, políticas, métodos de gestión de riesgos, acciones, formación, prácticas idóneas, seguros y tecnologías que pueden utilizarse para proteger los activos de la organización y los usuarios en el ciberentorno. Este concepto garantiza el cumplimiento de los objetivos fundamentales de la seguridad informática (ISO 27002) las cuales son:

- Confidencialidad.
- Integridad.
- Disponibilidad.

(Nuñez Maturel, Reyes Dixson, Alvarez Zaldivar, & González Torres, 2014).

La ***confidencialidad,*** es un concepto con el que se trata con frecuencia en la vida real. Por ejemplo, se espera que nuestros médicos mantengan nuestros expedientes como confidenciales. En el mundo de los negocios, se define como la característica de un recurso que asegura que el acceso está restringido para ser utilizado únicamente por usuarios, aplicaciones o sistemas informáticos autorizados; es decir, se ocupa de mantener la información, las redes y los sistemas seguros frente a cualquier acceso no autorizado. (Microsoft Official Academic Course).

En este mismo contexto, la ***integridad*** es definida como la consistencia, la precisión y la validez de los datos y la información. Uno de sus objetivos de un programa exitoso de seguridad, es cerciorar que la misma esté protegida frente a cualquier cambio no autorizado o accidental mediante procesos y procedimientos para manejar cambios intencionales, así como la capacidad para detectar cambios; por ejemplo, se pueden utilizar derechos y autorizaciones para controlar quién puede tener acceso a cierta información o recurso. (Microsoft Official Academic Course).

La ***disponibilidad*** es el tercer principio básico de la seguridad y describe un recurso que es accesible para un usuario, una aplicación o sistema informático cuando es requerido. Por lo general, las amenazas de disponibilidad son de dos tipos: *accidental* y *deliberada*. Las primeras, incluyen desastres naturales tales como tormentas, inundaciones, incendios, cortes de energía eléctrica, etc. También, incluye problemas de software, de red o del usuario. La segunda categoría, va relacionada con cortes que son el resultado de la explotación de una vulnerabilidad en el sistema. Algunos ejemplos de este tipo de amenaza incluyen ataques de denegación de servicios o gusanos informáticos que afectan a los sistemas vulnerables y su disponibilidad. (Microsoft Official Academic Course).

De este modo, la seguridad informática se puede definir como un conjunto de procedimientos, dispositivos y herramientas encargadas de asegurar la integridad, disponibilidad y privacidad de la información en un sistema informático e intentar reducir las amenazas que pueden afectar al mismo. (García-Cervigón Hurtado & Alegre Ramos, 2011).

Dentro de la seguridad informática se pueden encontrar elementos y técnicas tanto hardware, como software, así como dispositivos físicos y medios humanos.

La seguridad informática se divide en *activa* y *pasiva*, dependiendo de los elementos utilizados por la misma, así como de la actuación que van a tener en la seguridad de los mismos.

Se entiende por *seguridad activa* a todas aquellas medidas que se utilizan para detectar las amenazas, y en caso de su detección genera los mecanismos adecuados para evitar el problema. Por ejemplo, contraseñas o claves de acceso, uso de antivirus, cortafuegos o firewall.

Por otro lado, la *seguridad pasiva* comprende todo el conjunto de medidas utilizadas para que una vez que se produzca el ataque o el fallo en la seguridad del sistema, hacer que el impacto sea el menor posible, y activar mecanismos de recuperación del mismo. Por ejemplo, copias de seguridad de los datos del sistema, uso de redundancia

en discos o discos RAID (**R**edundant **A**rray of **I**nexpensive **D**isks). (García-Cervigón Hurtado & Alegre Ramos, 2011).

Desde el punto de vista de la naturaleza de las amenazas, se pueden clasificar en *nivel físico* o *nivel lógico*.

El ***nivel físico***, se utiliza para proteger el sistema informático utilizando barreras físicas y mecanismos de control; algunas de ellas son los guardias de seguridad del edificio, alarmas, cámaras de seguridad, extintores, etc.

El ***nivel lógico*** se encarga de asegurar la parte del software de un sistema informático; es decir, se encarga de asegurar los programas y los datos. Además, controla que el acceso al sistema informático se realice correctamente y por usuarios autorizados, ya sea desde la misma red donde éste se encuentre o desde una red externa, usando una VPN (protocolos PPP, PPTP, etc.), la web (protocolos HTTP, HTTPS), transmisión de ficheros (FTP), conexión remota (SSH, Telnet), etc. (García-Cervigón Hurtado & Alegre Ramos, 2011).

Por ende, los tipos de amenazas al sistema informático más destacadas son:

Amenazas software

Dentro de este tipo de amenaza podemos encontrar el ***software malicioso*** (malware), el cual es un software que está diseñado para infiltrarse o afectar al sistema de una computadora sin la aceptación informada del propietario. Actualmente, el *malware* puede ser usado para lanzas ataques de negación de servicio (DoS) en contra de otros sistemas, redes o sitios Web causando que dichos sistemas tengan problemas de desempeño o que se vuelvan inaccesibles.

El *malware* puede ser dividido en diversas categorías, incluyendo las siguientes:

Virus*.* Es un programa que puede copiarse por sí mismo e infectar una computadora sin la aprobación o el conocimiento del usuario.

Gusanos. Es un programa auto-reproducible que se copia a sí mismo en otras computadoras en una red sin ninguna intervención del usuario. A diferencia de un *virus*, un *gusano* no corrompe ni modifica archivos en la computadora objetivo. En vez de esto, consume su ancho de banda, los recursos de su procesador y su memoria, reduciendo la velocidad del sistema o causando que este sea inutilizable.

Troyanos*.* Es un programa ejecutable que aparece como un programa deseable o útil. Sin embargo, cuando es cargado puede causar que la computadora de un usuario se vuelva inutilizable, o puede evadir la seguridad de un sistema, permitiendo que la información privada (tarjetas de crédito, contraseñas, número de seguro social, etc.) sea accesible por una persona externa. En algunos casos, también puede ejecutar *adware*.

Spyware*.* Es un tipo de *malware* que es instalado en una computadora para reunir información personal de un usuario o detalles sobre sus hábitos de exploración, con frecuencia sin conocimiento del usuario. Además, puede instalar software adicional, redirigir su explorador Web a otros sitios o cambiar su página de inicio. Un ejemplo es el capturador de teclado (keylogger), que cuando se instala en un sistema, registra cada tecla presionada por un usuario permitiendo saber los números de la tarjeta de crédito, los números del seguro social, o contraseñas, para posteriormente registrarla y enviarla a alguien sin autorización.

Adware. Es cualquier paquete de software que reproduce, muestra o descarga automáticamente anuncios a una computadora después de que el software es instalado o mientras la aplicación está siendo usada.

Puerta trasera (back door). Es un programa que le da a alguien control remoto no autorizado de un sistema o inicia una tarea no autorizada. Algunas *puertas traseras* son instaladas por virus u otras formas de *malware*.

Los virus y gusanos con frecuencia explotan lo que se conoce como *buffer overflow* (búfer). En todos los programas de aplicación, incluyendo Windows, existen buffers que contienen datos y tienen un tamaño fijo. Por tanto, si se envían demasiados datos a estos buffers, ocurre un *buffer overflow* (desbordamiento). Dependiendo de los datos

enviados al desbordamiento, un hacker puede ser capaz de usar el desbordamiento para enviar contraseñas a sí mismo, alterar archivos del sistema, instalar *back doors*, o causar errores en la computadora.

(Microsoft Official Academic Course).

Amenazas físicas

Como ya se ha mencionado, dentro de este tipo de amenazas se pueden encontrar todos aquellos posibles daños causados al sistema informático por razones físicas y naturales.

Amenazas humanas

Las amenazas puramente humanas, pueden venir desde dos tipos de amenazas:

1. ***Intrusos***, como piratas informáticos, que pueden entrar vía web, es decir, de forma remota, o físicamente al sistema.
2. ***Fallos humanos*** de los propios usuarios del sistema informático.

(García-Cervigón Hurtado & Alegre Ramos, 2011).

La aspiración de este artículo es la de incentivar al lector en un aspecto tan importante como es la seguridad informática; además, explica por qué los antivirus tradicionales han pasado a ser una tecnología obsoleta.

2. Metodología

Para el desarrollo de la investigación se efectuó una verificación bibliográfica con el fin de analizar, sintetizar y esclarecer los puntos más importantes de las bibliografías consultadas. También, se consultaron diferentes libros, artículos y revistas electrónicas referentes a la ciencia y tecnología, así como de portales Webs de empresas líderes en seguridad informática de vanguardia.

Para fundamentar la investigación se tomó una muestra del 10% de la población del Instituto Tecnológico de Celaya para posteriormente aplicarles una encuesta con el fin de determinar que antivirus utilizan actualmente, que nivel de protección aportan y cómo se sienten los usuarios al respecto.

Por otro lado, las pruebas de seguridad a las que se sometieron los antivirus más populares de este 2015, son las proporcionadas por ***SSTS (S****ecurity* ***S****oftware* ***T****esting* ***S****uite****)*** *de Matousec*:

1. **Schedtest:** Determina si el software de seguridad probado permite la comunicación con otro programador de tareas de procesos para establecer una nueva tarea, por ejemplo, la ejecución de código malicioso.

2. **BITStest:** Determina si el software de seguridad probado permite descargar un archivo desde internet, por ejemplo, para actualizar el malware albergado en la computadora. Esta prueba usa IBackgroundCopyManager organizada por servicios BITS Windows para realizar dicha acción.

3. **Kill5:** Es uno de los métodos que el malware puede utilizar para matar un proceso de algún software de seguridad.

4. **Zero-Day (Anti-Keylogging):** Determina si el software de seguridad probado permite la ejecución de algún keylogger.

5. **CLT:** Básicamente, muestra como el equipo está protegido contra RAT's, rootkits y las inyecciones.

Cabe mencionar que existen varios niveles de pruebas en *SSTS.* Cada nivel contiene un conjunto seleccionado de pruebas y también contiene un límite de puntuación que es necesario para pasar el nivel. Todos los productos son probados con el nivel 1 del conjunto de pruebas. Los productos que llegan al limite de la puntuación del nivel 1 pasan al nivel 2 y así sucesivamente hasta llegar al nivel más alto o hasta que falle el limite de un cierto nivel.

(matousec, s.f.).

A continuación, se describen los materiales que se utilizaron para realizar las pruebas:

- Sistema Operativo Microsoft Windows 10 con arquitectura basada en 64 bits.
- VMware para contar con un entorno controlado de virtualización.
- Firma de base de datos del antivirus actualizado.

Los pasos que se siguieron para realizar las pruebas correspondientes son:

1. Descargar el software a utilizar:
    - **Microsoft Windows 10:** Microsoft DreamSpark for Academic Institutions
    - **VMware:** *CHECAR*
    - **SSTS:** http://www.matousec.com/downloads/
    - **Antivirus:** Sitio Web correspondiente al software.
2. Instalar VMWare.
3. Configurar el entorno virtual e instalar el SO mencionado.
4. Instalar el software antivirus a probar.
5. Ejecutar SSTS.
6. Verificar si el antivirus detecto la amenaza.
7. Documentar el resultado.
8. Repetir el paso cinco (5) hasta que hallamos concluido las cinco (5) pruebas correspondientes de seguridad.
9. Desinstalar el antivirus.
10. Repetir el paso cuatro (4) hasta que hallamos verificado los cinco (5) antivirus propuestos.

11. Analizar y comparar los resultados obtenidos en la encuesta con los resultados obtenidos en las pruebas.
12. Interpretación de resultados.

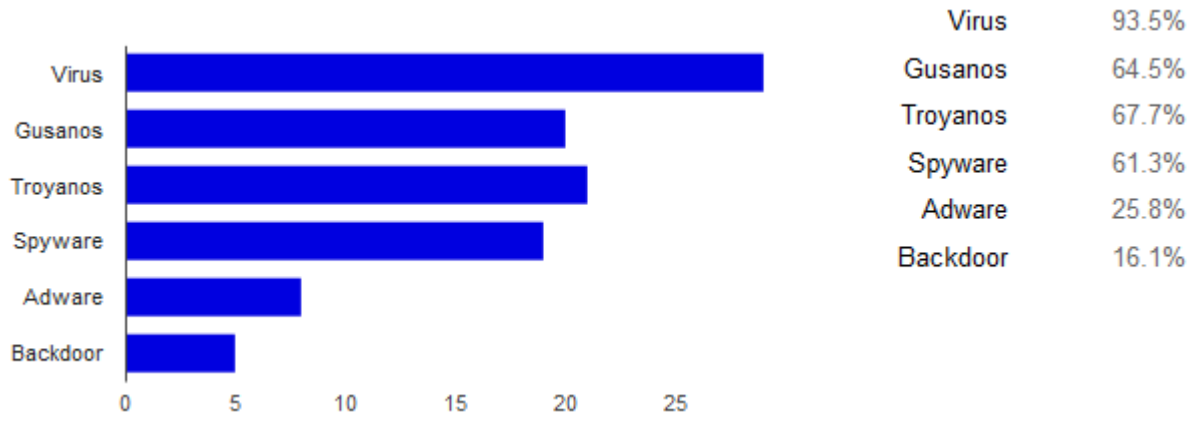
3. Resultados

En cuanto a la encuesta aplicada para esquematizar o caracterizar a la población referente a los antivirus que utilizan en el Instituto Tecnológico de Celaya, se obtuvieron datos estadísticos de la población y de ello se muestran los siguientes resultados:

Como se muestra en la gráfica 1.1 con un 45.3% de preferencia, el software de seguridad más usado es *Avast Free Antivirus 2015*, seguido de AVG Internet Security y ESET Smart Security los cuales cuentan con un 12.9% de preferencia.

GRÁFICA 1.1 Software antivirus más utilizado por la comunidad estudiantil del ITC.

Como se muestra en la gráfica 1.2 con un 93.5% de ocurrencia, los virus son el tipo de amenza que comúnmente detectan los usuarios, seguido de los troyanos con un 67.7% de ocurrencia y gusanos con un 64.5% de ocurrencia.



GRÁFICA 1.2 Índice de amenazas detectadas por la comunidad estudiantil del ITC.

Como se muestra en la gráfica 1.3 con un 35.5% de ocurrencia, los usuarios que utilizan algún software antivirus no sienten una protección óptima ante las amenazas de la red. Por ello, recurren a instalar software adicional para completar la seguridad o sentirse más seguros.

GRÁFICA 1.3 Índice de satisfacción de la comunidad estudiantil del ITC al uso de algún software antivirus.

Como se muestra en la gráfica 1.4 con un 58.1% de ocurrencia, los usuarios cercioran que no han sido víctimas de alguna amenaza.

GRÁFICA 1.4 Tasa de infecciones en los equipos de algún miembro de la comunidad estudiantil del ITC.

Como se muestra en la gráfica 1.5 con un 71% de ocurrencia, los usuarios cercioran que un antivirus no es una herramienta de seguridad suficiente para protegerse de las diversas amenzas que se encuentran actualmente acechando en la red.

GRÁFICA 1.5 Tasa de infecciones en los equipos de algún miembro de la comunidad estudiantil del ITC.

Por ello, como se muestra en la gráfica 1.6 el 80.6% de los usuarios creen que los antivirus tradicionales han pasado a ser obsoletos y por ende, necesitan una reinvención para satisfacer y aumentar el rango de protección.

GRÁFICA 1.6 índice de las opiniones de la comunidad estudiantil del ITC referente a la reinvención del software antivirus.

Por otro lado, al realizar las pruebas de seguridad en los antivirus seleccionados, se presentaron los siguientes valores:

TABLA 1.1 Resultados de las pruebas de seguridad en los antivirus..

SOFTWARE ANTIVIRUS	PRUEBA REALIZADA					FECHA	PUNTUACIÓN
	Schedtest3	BITStest	Kill5	CLT (PUNTUACIÓN)	Zero-Day		
Comodo Internet Security Pro	Fracaso	Fracaso	Pasado	340/340	Pasado	11/09/2015	60%
AVG Internet Security	Fracaso	Fracaso	Pasado	220/340	Fracaso	11/09/2015	22%
ESET Smart Security	Fracaso	Fracaso	Pasado	210/340	Fracaso	11/09/2015	20%
Kaspersky Total Security 16	Fracaso	Fracaso	Pasado	210/340	Fracaso	11/09/2015	20%
BitDefender Total Security 2015	Fracaso	Fracaso	Fracaso	230/340	Fracaso	11/09/2015	4%

Con base a los valores obtenidos de la tabla 1.1 se interpreta que:

- Al no superar las pruebas Schedtest3 y BITStest, los antivirus *Comodo*, *AVG*, *ESET*, *Kaspersy* y *BitDefender* permiten tanto la ejecución de código malicioso como la actualización de los mismos.

- Al superar la prueba Kill5, los antivirus *Comodo*, *AVG*, *ESET* y *Kaspersky* evitan que el malware deshabilite algún proceso de seguridad. Sin embargo, el antivirus *BitDefender* es vulnerable a dicha amenaza.

- Al superar la prueba CLT, el antivirus *Comodo* es el único que protege al dispositivo de rootkits, RAT's e inyecciones.

- Al no superar la prueba Zero-Day, los antivirus *AVG*, *ESET*, *Kaspersy* y *BitDefender* permiten la ejecución de keylogger y por ende, el robo de datos. A excepción del antivirus *Comodo* el cual, es fuerte ante estas amenazas.

Finalmente, al no haber aprobado las pruebas de seguridad básicas, se concluye que en la actualidad los antivirus, no tienen la capacidad necesaria para afrontar las nuevas generaciones de amenazas, ya que dichas amenazas están en una constante evolución y cada vez tienen técnicas de penetración más robustas y eficientes.

Cerciorando la hipótesis planteada, se obtiene la conclusión plasmada, las empresas de seguridad informática no han tomado los esfuerzos ni medidas suficientes para contrarrestar este avance significativo y continuo respecto a los ataques cibernéticos y su amplia gama de amenazas.

4. Discusión

Con el fin de corroborar la hipótesis planteada y los resultados obtenidos, se propone efectuar las pruebas proporcionadas por *SSTS* en el mes de diciembre, de tal manera que se cubra una mayor gama de software antivirus y una firma de base datos actualizada para contar con una visión más amplia del problema detectado. Además, para contar con una protección más robusta en el sistema, se pretende anexar otros tipos de software que sirvan como complemento al antivirus, por ejemplo, anti-malware y firewalls.

Una vez realizado el nuevo análisis, se compararán los resultados obtenidos con los resultados expuestos en este artículo para comprobar la eficiencia del software de seguridad informática y por ende, si las empresas involucradas han hecho algo al respecto o si necesitan reinventar el software antivirus con el único objetivo de brindar una mayor protección en tiempo real ante el ritmo en que las amenazas informáticas evolucionan.

Bibliografía

[1] García-Cervigón Hurtado, A., & Alegre Ramos, M. D. (2011). *Seguridad Informática* (Primera ed.). (M. J. López Raso, Ed.) Navalcarnero, Madrid, España.

[2] matousec. (s.f.). *matousec*. Obtenido de http://www.matousec.com/

[3] Microsoft Official Academic Course. (s.f.). Fundamentos de Seguridad.

[4] Nuñez Maturel, L., Reyes Dixson, Y., Alvarez Zaldivar, Y., & González Torres, M. D. (Julio de 2014). Selección de productos antivirus. Una mirada actual desde el sector de la salud en Cuba. *Revista Cubana de Informática Médica, VI*(2). Obtenido de http://scielo.sld.cu/scielo.php?script=sci_arttext&pid=S1684-18592014000200003