Depósito Legal ppi 201502ZU4668

CIENCIA

Vol. 23, Nº 3
Julio-Septiembre 2015

An International Refereed Scientific Journal of
the Facultad Experimental de Ciencias
at the Universidad del Zulia
Maracaibo - Venezuela

Esta publicación científica en formato digital
es continuidad de la revista impresa
Depósito Legal: pp 199302ZU47
ISSN:1315-2076

CIENCIA 23 (3), 126-133, 2015
Maracaibo, Venezuela

Mecanismo de seguridad implementado en sistemas operativos de código cerrado para corregir ataques tipo Spyware

David Bracho Rincón*, Emmanuel Colina Chirinos, Eugenio Ferrer, Alfredo Acurero Álvarez, Olinto Rodríguez Atencio y Carlos Rincón Castro
Unidad de Redes e Ingeniería Telemática, Departamento de Computación, Facultad Experimental de Ciencias, Universidad del Zulia. Maracaibo, Venezuela

Recibido: 03-02-15 Aceptado: 22-07-15

Resumen

El propósito de la investigación fue desarrollar un mecanismo de seguridad activo en sistemas operativos de código cerrado para proteger de ataques tipo Spyware. La investigación fue experimental según Hernández y col (1). Se utilizó la metodología de seguridad "Análisis de Riesgo de la Seguridad de la Información", de Jarauta y col (2), combinada con la del "Método de Ciclo de Vida" de Senn (3). Se desarrolló una aplicación en Visual Basic v6.0 que resolvió problemas por ataques Spyware tipo Backdoor al sistema operativo Windows XP SP2, tales como: Subseven, CyberGate y Spynet, que analizó registros adulterados, procesos y uso del CPU. Adicionalmente, se agregó un módulo para gestionar los procesos iniciados con el sistema (msconfig). Los resultados en función del rendimiento particular comparando el mecanismo desarrollado con la herramienta NOD32 v6.0 arrojó: el primero fue mejor en el Tiempo Promedio de Detección de Amenazas, el segundo fue mejor en los Registros Corregidos, hubo paridad en los Procesos de Memoria Eliminados y en el Inicio de Procesos Eliminados. En términos generales, la efectividad global favoreció al NOD32, ya que, conteniendo una mayor cantidad de firmas digitales, corrigió y revirtió mayor número de archivos dañados.

Palabras Clave: mecanismo de Seguridad; Spyware; Blackdoor; Windows XP SP2; Ataques Informáticos.

Security mechanism implemented in proprietary operating systems for Spyware-type attacks correction

Abstract

The purpose of the research was to develop an active safety mechanism for proprietary operating systems to protect from Spyware attacks. The research was experimental according to Hernandez et al (1). The methodology "Risk Analysis Information Security" by Jarauta et al (2), combined with the "Method of Life Cycle" of Senn (3) was used. An application in Visual Basic v6.0 was developed, to mitigate backdoor Spyware

* Autor para la correspondencia: drbracho@fec.luz.edu.ve

attacks on Windows XP SP2 operating system such as Subseven, CyberGate and Spynet, checking doctored records, processes and CPU usage. Additionally, a module to analyze processes started by the managed system (msconfig) was included. The results based on the comparison between the developed mechanism and NOD32 v6.0 showed that: the first has lower average threat detection time, the second has higher fixed records ratio, and both were equal for the variables deleted processes and deleted starting processes. In general, NOD32 showed the best overall performance because using more registers of digital signatures was able to fix and rollback more corrupted files.

Keywords: Security Mechanisms; Spyware; Blackdoor, Windows XP SP2; Computer Attacks.

Introducción

El uso de nuevas tecnologías de comunicación brinda nuevas oportunidades de comercio para negocios y organizaciones, pero también crea ventajas para los criminales informáticos. De acuerdo con Ma y col (4), la Web no constituye una excepción y a través de ella millones de delincuentes realizan una gran variedad de estafas por medio de la propagación del malware. El Malware es un término colectivo que se aplica a cualquier software malicioso que ingrese en un sistema sin la autorización del usuario. En consecuencia, este tipo de amenaza sigue creciendo en volumen y evolucionando en complejidad. De hecho, según ESET (5) hoy día el Spyware es uno de los tipos de Malware de mayor difusión y tiene una elevada incidencia en los sistemas informáticos.

En ese sentido, desde la perspectiva de Castillo y col (6), los mecanismos de infección del Spyware se basan en la explotación de vulnerabilidades en el software, principalmente en el sistema operativo. De hecho, a juicio de Acero (7), el Spyware ha evolucionado y ha ido incorporando sofisticados mecanismos que hacen difícil su control y detección. En contraparte, la práctica mono-cultura informática existente hace años, en la que la mayoría de las computadoras del mundo utilizan un mismo sistema operativo (Windows) y casi las mismas aplicaciones informáticas, hace que sea muy rentable y sencillo elaborar estos malware.

Razón por la cual, los sistemas operativos Windows del fabricante Microsoft han sido históricamente los más afectados por el Malware y sus usuarios se han acostumbrado a tomar medidas de seguridad para evitar infecciones en este sistema. En efecto, según ESET (8), a través de Ingeniería Social y de la explotación de vulnerabilidades, las amenazas para la plataforma Microsoft son mayoritarias y preponderantes.

Es por ello que, de acuerdo con Delgado (9) el principal problema es que el riesgo frente a las amenazas aumenta aceleradamente, debido principalmente a la falta de protección robusta, vigente y eficiente, originado principalmente por la marcada obsolescencia, ya que, tanto la arquitectura como la estructura no está preparada para afrontar modernos escenarios de ataques, orientados a nuevos ecosistema de formatos, redes sociales o aplicaciones en la "nube".

En consecuencia, la corporación Microsoft descontinuó los programas de actualizaciones y de correcciones de errores gratuitamente. Por consiguiente, insistir en utilizar Windows XP significa estar propenso a perder sistemáticamente el control del equipo, y con ello, la información confidencial y credenciales del usuario, negándosele la disponibilidad de los recursos, alterando simultáneamente la integridad de la data, lo que representa un fallo grave a la seguridad del equipo.

Sin embargo, advirtió el autor que a pesar de todo lo expuesto anteriormente, que durante el año 2014, Windows XP fue un producto que conservó más del treinta por ciento (30%) del mercado de los sistemas operativos de equipos de escritorios (PC y portátiles) a nivel mundial, presencia que se tradujo en más de quinientos millones (500.000.000) de computadores personales. Por lo tanto, sería ingenuo y optimista pensar que los ataques derivados en el uso de esta plataforma dejarán de suceder en el corto plazo.

Por lo anteriormente dicho, el propósito de esta investigación fue desarrollar un mecanismo de seguridad activo para sistemas operativos de código

cerrado; inicialmente en las versiones de Windows XP SP2, que proveyera e integrara módulos de protección ante una modalidad de ataque conocida como Spyware y corrija los daños causados por éste en el sistema

Motivación

De acuerdo con Wellmeyer (10), el Spyware puede instalar software adicional, redireccionar la actividad del navegador web o cambiar la configuración del equipo. Es por ello que, según el informe de PandaSecurity (11), estos programas-espías se instalan con otras aplicaciones que nada tienen que ver con estas pero que, sin saberlo y de acuerdo a las bases legales de ese programa, el usuario finalmente acepta. Por ende, el Spyware también aparece al descargar algún tipo de contenido de una página Web o de redes P2P, al instalar alguna aplicación gratuita o sencillamente al navegar por páginas Web poco recomendables. Por esto, el propósito de estos programas espías es ilegítimo.

Argumenta Ponne (12) que los fabricantes de sistemas operativos, delegan su confianza a los programas antivirus para protegerse de ataques tipo Spyware. Muchos antivirus del mercado son gratuitos y con ciertas limitaciones de seguridad ya que los fabricantes de estos sistemas utilizan estas versiones como parte de su mercadeo puesto que el usuario, para tener un producto sin restricciones debe pagar el costo del mismo. Casi podría decirse que no existe nada completamente seguro, lo que incluye cualquier sistema informático y que la seguridad de un sistema depende de la fortaleza o debilidad con la que es capaz de reaccionar ante algún ataque. Al respecto, García (13) destaca que un ataque es cualquier interacción no prevista con el entorno que pueda alterar el comportamiento de un sistema. Finalmente, Mieres (14) indica que aunque existen herramientas de seguridad antivirus como ESET NOD32, capaces de detectar códigos maliciosos conocidos y desconocidos (malware que ESET NOD32 detecta de forma proactiva), la realidad es que no existe una versión precisa de aplicaciones de seguridad que detecte el 100% de las amenazas.

Por consiguiente, se intentó desarrollar una solución que incorporara un mecanismo de seguridad en el sistema operativo Microsoft Windows, solución que contempla dentro de sus características y atributos los siguientes: licenciamiento gratuito, no-propietario y de fácil acceso al usuario, todo ello con el propósito de prevenir y minimizar los ataques tipo Spyware, para complementar o sustituir las dependencias de algunos programas que brindan protección limitada y de licenciamiento no gratuito.

Metodología

La metodología de seguridad utilizada se basó en el *Análisis de Riesgo de la Seguridad de la Información*. Esta metodología fue planteada por Jarauta y col (2), la cual fue adaptada a los objetivos de esta investigación, en la que se consideraron sólo cuatro fases. Las fases contempladas se describen seguidamente:

a) Fase 1. Identificación y valoración de los activos. Para la clasificación de los activos, se siguió la metodología planteada por Jarauta y col (2); esta fase también posee la actividad de identificación de los activos. Fase 1.1 Identificación de los activos: Software: Sistema Operativo b) Fase 2. Identificación y valoración de las amenazas: determinación de amenazas que afectas al activo clasificado. Ya que la investigación contempla la amenaza para el activo, la actividad de identificación se consideró ejecutada desde la concesión de la investigación. Fase 2.1. Identificación de la amenaza: La amenaza que presenta e identifica este trabajo de investigación es un ataque tipo Spyware. Fase 2.2. Valoración de la amenaza: Se establece la importancia de poder tomar en cuenta esta amenaza. Esto debido a que un sinnúmero de empresas u organizaciones especializadas en el área de seguridad informática, dan al ataque tipo Spyware entre las amenazas de malware más propagadas de los últimos tiempos c) Fase 3. Identificación y valoración de las vulnerabilidades: Esta etapa es responsable de la identificación de vulnerabilidades que presenta el activo. Fase 3.1. Identificación de las vulnerabilidades: Esta actividad identificó las vulnerabilidades del sistema operativo con respecto a la amenaza. d) Fase 4. Identificación y selección de las medidas de seguridad: Se desarrolló el mecanismo de seguridad propuesto como solución para la investigación.

No obstante, para la creación del mecanismo se contó con el *método de ciclo de vida de desarrollo de sistemas*, planteada por Senn (3). Se utilizó como metodología específica de desarrollo, las siguientes etapas planteadas por dicha metodología: i) Investigación preliminar: Vulnerabilidades de los sistemas operativos, esquemas que utilizan los antivirus para detección de ataques Spyware y otras características relacionadas con seguridad informática. ii) Determinación de los requerimientos: Con las características fijadas, modificar el esquema elegido en torno a éstas. Con base a esto, se obtienen los requerimientos que el mecanismo de seguridad debe cumplir iii) Diseño: Generar los documentos de diseño necesarios para preparar la propuesta, el modelo y evaluación contra los requerimientos iníciales. Se diseña el sistema para cumplir con los requerimientos encontrados en la fase anterior iv) Desarrollo: Desarrollar el mecanismo de seguridad activo propuesto por la investigación v) Prueba: El mecanismo se sometió a una serie de pruebas para determinar su funcionamiento y eliminar sus fallas. Además, que cumpliera con los requerimientos fijados y documentar dichas pruebas.

Para el desarrollo del mecanismo propuesto se utilizó el entorno de desarrollo Visual Basic 6.0 (VB6). Este lenguaje de programación fue elegido ya que facilita la creación de interfaces gráficas y la programación misma. De hecho, facilita la manipulación del registro de Windows, ya que tiene acceso total a la application programming interface (API) o interfaz de aplicación de Windows.

Protocolo de pruebas

Se configuró un computador personal con memoria RAM de 2 GB y disco duro 160 GB, sistema Windows XP Professional Service Pack 2 (SP2) de 32 bits, sin ninguna extensión adicional, ni herramientas de seguridad y/o cortafuegos. En cuanto a los Spyware a evaluados, se obtuvieron las firmas digitales de los Spyware más comunes propuestas por Allienhacker (15) y los que son considerados Spyware por Doruk (16). Por lo cual, se utilizó una base de datos de firmas actualizadas proveniente de sitios confiables como Virus Total y Sophos.

Complementariamente, como medio de infección se utilizó la última actualización de la base de datos de los dominios asociados con descargas de Spyware. Adicionalmente, se utilizó una adaptación de la metodología utilizada por Ponne (12), para realizar los experimentos previstos, tomando en cuenta los mismos factores, duración del ataque por intervalos predeterminados para medir el rendimiento de la computadora bajo un ataque por lapsos.

En efecto, desde la perspectiva de Dewald y col (17), el análisis de un sitio web abarca un rango de entre 0,1 a 6,4 seg., y en función de esto, se dividió el tiempo máximo previsto (6,4 seg.) en tres fracciones para determinar los intervalos de los ataques, que arrojaron como resultado: primer intervalo de 0,1 seg., a 2,13 seg., segundo intervalo de 2,14 seg., a 4,26 seg.; y tercer intervalo de 4,27 seg., a 6,4 seg. Con el fin de reducir la posibilidad de obtener valores fuera de rango, cada escenario fue repetido en tres ocasiones y se tomó como resultado final el promedio de las tres pruebas. Los valores monitoreados fueron: Tiempo de infección del Spyware, CPU, Memoria, registros alterados y procesos creados por Spyware.

Posteriormente, una vez identificados todos estos valores y el tipo de Spyware a usar, se procedió atacar a las computadoras vía puerto USB, uno de los escenarios establecidos. Se observó que el mecanismo desarrollado efectuó su trabajo una vez que la máquina estuvo infectada, ya que ésta no contaba con sistemas de protección en tiempo real. De esta manera, fue posible observar la eficiencia del mecanismo en cuanto a la recuperación de los recursos.

Sin embargo, fue necesario usar herramientas para observar los cambios que desencadenaron las infecciones inoculadas en las máquinas. Éstas fueron: a) Process Monitor v3.04, una herramienta de monitorización que muestra en tiempo real el sistema de archivos, el registro de Windows y la actividad de los procesos y subprocesos. Se utilizó la última versión del producto, la cual posee opciones para solución de problemas del sistema operativo y herramientas de búsqueda de malware b) Administrador de Tareas de Windows XP, proporciona información sobre

procesos y aplicaciones que el computador ejecuta, actividad de red, usuarios y servicios activos del sistema. Permite cerrar las aplicaciones que tienen conflictos de funcionamiento c) Antivirus NOD 32 6.0, una herramienta de seguridad informática que detecta en tiempo real nuevas amenazas o virus nuevos no-catalogados, además; analiza el código de ejecución para encontrar operaciones potencialmente dañinas incrustadas en el malware.

Las primeras herramientas sirvieron para monitorear y analizar el comportamiento del mecanismo durante las pruebas; y se hizo lo mismo con el equipo de prueba; se observó el funcionamiento del equipo bajo posibles ataques e infecciones ocurridas en las pruebas. La última herramienta sirvió para analizar el equipo en búsqueda de posibles infecciones generadas en las pruebas y comparar los resultados obtenidos entre las pruebas. Es importante subrayar, que la herramienta de seguridad fue desactivada durante las pruebas para que no interviniera ni contaminara los escenarios. Los casos de pruebas realizados fueron los siguientes: a) Pruebas para medir el comportamiento del sistema sin Spyware, mecanismo inactivado y sin antivirus b) Pruebas para medir el comportamiento del sistema sin Spyware y con el mecanismo activado c) Generación de un cuadro de comportamiento del sistema sin Spyware y con el programa antivirus más común d) Infección de forma intencional de un computador con los programas maliciosos obtenidos de sitios en internet, sin activar el mecanismo desarrollado e) Infección de forma intencional de un computador con programas maliciosos obtenidos de sitios en internet, posteriormente se activó el antivirus f) Infección de un computador con los programas maliciosos obtenidos de sitios en internet, posterior a ello se activó el mecanismo desarrollado g) Análisis para comparar los resultados del antivirus y el mecanismo activo desarrollado.

Análisis de resultados

El mecanismo realizado se basó en un método de búsqueda de firmas digitales hashMD5 desarrollado por RSA Data Security, Inc., tal cual lo indicó Algredo y col (18), para quienes ésta es una función que toma un mensaje de tamaño arbitrario y produce como salida un resumen del mensaje de 128 bits. Esta codificación del MD5 es representada con 32 dígitos hexadecimales; se ejecuta velozmente en computadoras de 32 bits, no requiere grandes tablas de sustitución y puede ser codificada de forma compacta.

Cuando el mecanismo extrae la firma o huella digital de la amenaza, la compara con la base de datos de Spyware y si ambas firmas coinciden se asume la presencia de una amenaza y se eliminará del sistema. En la figura 1 se muestra el diagrama de flujo del algoritmo usado por el mecanismo desarrollado.

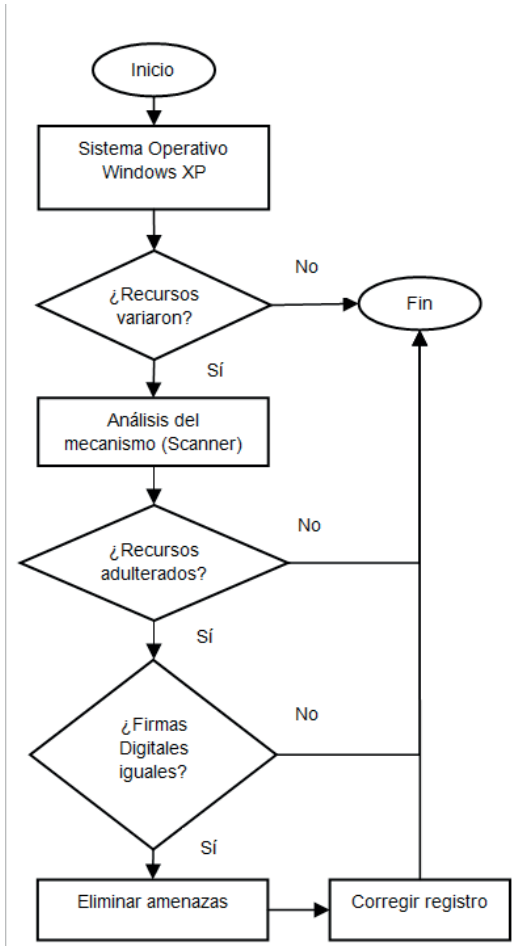

Figura 1. Diagrama de flujo del algoritmo usado por el mecanismo desarrollado

Fuente: Propia (2013).

La presente investigación proporcionó seguridad al sistema operativo Windows XP SP2 ante ataques Spyware tipo tipo Backdoor, tales como: Subseven, CyberGate y Spynet, a través del desarrollo de una API. Para ello, se evaluaron los siguientes parámetros: a) Tiempo de Detección de la Amenaza (TdD) b) Registros Corregidos (RC), Procesos de Memoria Eliminados (PdME), e Inicio de Procesos Eliminados (IdPE). En ese sentido, dichos parámetros fueron medidos en función de determinar el nivel de seguridad ofrecido tanto por la solución individualmente, como cuando fue comparada con la herramienta antivirus NOD32. La tabla 1 muestra el resume de los resultados obtenidos.

Tabla 1. Resultados obtenidos

Software/ Parámetros	NOD32	Mecanismo Desarrollado
Subseven		
TdD (segs)	6,76	4,86
RC	3	2
PdME	1	1
IdPE	1	1
SpyNET		
TdD (segs)	31,39	0,41
RC	4	2
PdME	1	1
IdPE	2	2
CyberGate		
TdD (segs)	30,21	0,38
RC	4	2
PdME	1	1
IdPE	2	2
Totales		
TdD Prom. (segs)	22,79	1,88
RC (Total)	11	6
PdME (Total)	3	3
IdPE (Total)	5	5

Fuente: Propia (2013).

La efectividad promedio del mecanismo de corrección de errores ante los tres ataques para los tres intervalos fue de 54,54%. Éste se obtuvo dividendo la cantidad de registros corregidos por el mecanismo activo (seis), entre la cantidad de registros adulterados (once) por los Spyware. Por otra parte, la efectividad promedio total del mecanismo de corrección de errores ante los ataques, fue del 54,54%. No obstante, la efectividad del mecanismo propuesto con respecto a NOD32 corrección de errores fue de 45,45%. En el mismo orden de ideas, el tiempo promedio total de detección del mecanismo propuesto fue 1,88 seg. En contraparte, el tiempo promedio total de detección obtenido por NOD32 fue 22,79 seg.

Se observó que el tiempo promedio de detección del mecanismo de seguridad fue mucho más bajo que el tiempo de detección de NOD32 debido a la cantidad de firmas que este último presenta. Sin embargo, se advierte que el mecanismo propuesto usó tres firmas digitales, cantidad muy por debajo de las utilizadas por NOD32. Por este motivo, la efectividad arrojada en cuanto al tiempo promedio fue mucho menor favoreciendo al mecanismo propuesto.

Esto no es garantía real de la protección ofrecida por el mecanismo, puesto que, demostró que la cantidad de firmas incidió directamente en los niveles de seguridad integrales de la solución. En definitiva, se aceptó que el mecanismo desarrollado proporcionó protección ante virus Spyware tipo Backdoor, tales como: Subseven, CyberGate y Spynet con las consideraciones antes expuestas.

Conclusiones

1. El módulo msconfig integrado en el mecanismo propuesto sirve para detener procesos maliciosos que se ejecutan al iniciar el sistema Windows XP. Esto permite corregir los errores de registros adulterados por los Spyware.
2. El mecanismo desarrollado registró rendimientos superiores al NOD32 en uno (1) de los cuatro (4) indicadores, correspondiente al Tiempo Promedio de Detección de Amenazas (TdD Prom). En contraparte, dicho mecanismo mostró desempeños inferiores que el NOD32 en uno (1) de los cuatro (4) indicadores, pertenecientes a los Recursos Corregidos (RC). No obstante, tanto el mecanismo, como el NOD32, tuvieron rendimientos similares en dos (2) de los (4) indicadores, concernientes a los Procesos de Memoria Eliminados (PdME),

y al Inicio de Procesos Eliminados (IdPE).

3. La efectividad particular desde la perspectiva del número total de los indicadores evaluados entre el mecanismo desarrollado y el NOD32 evidenció paridad, ya que, ambos fueron superiores con respecto al otro, en un sólo indicador, correspondiente al veinticinco por ciento (25,00%) del total de las métricas analizadas. Sin embargo, se apreció igualdad en dos (2) de los indicadores, equivalente al cincuenta por ciento (50,00%) del total de las métricas evaluadas.

4. La mejora en el rendimiento obtenida por el mecanismo desarrollado en cuanto a los Tiempos Promedio de Detección de Amenazas (TdD Prom), fue consecuencia directa de que la aplicación incluyó una cantidad de firmas digitales significativamente menor a las manejadas por el NOD32. En consecuencia, mientras menos firmas existan, más rápido será el análisis porque hay menor cantidad de elementos que verificar y validar. Sin embargo, hay que destacar que, el factor determinante de la seguridad del mecanismo, no vine dado únicamente por el TdD Prom, sino por la combinación de los TdD Prom y RC.

5. Al ampliar el espectro de firmas digitales se hace complejo el análisis, desacelerándose los tiempos de evaluación notablemente. No obstante, la merma en la velocidad es compensada con la robustez alcanzada, aportando a los procesos de diagnósticos mayor consistencia, integridad y solidez. En consecuencia, el escaso número de firmas digitales gestionadas por el mecanismos incidió en el rezago del desempeño entre los RC de la aplicación desarrollada y del NOD32.

6. El rendimiento en la seguridad depende de la relación TdD Prom y RC, puesto que, a medida que se incorpora mayor cantidad de firmas digitales, se detectan y corrigen mayores RC. Sin embargo, dada la complejidad de los ataques, la magnitud y dimensión de los daños dificulta restablecer y restaurar apropiadamente los RC, por ende, los TdD Prom para dar con soluciones eficientes aumentan proporcionalmente con el esfuerzo hecho.

7. Cuando se valora la relación seguridad – velocidad, la efectividad global esta influenciada primordialmente por la primera, aunque se desmejoren significativamente aspectos concernientes al rendimiento de los TdD Prom, ya que, importa más la confidencialidad, disponibilidad e integridad de los recursos y de los datos, que la rapidez con que se hagan los análisis. Ignorar, desconocer o subestimar amenazas como los ataques Spyware tipo Backdoor conlleva a la pérdida sostenida de la propiedad y de la autonomía de los equipos y de las transacciones. Por consiguiente, en función de lo antes expuesto, se afirma que el mecanismo desarrollado no fue más eficiente que el NOD32, puesto que, no proporcionó el mismo nivel de seguridad.

8. Fue posible desarrollar una herramienta que permitió detectar la presencia de software malicioso en el sistema operativo Windows XP SP2 utilizando herramientas del sistema y API para detectar y corregir ataques Spyware tipo Backdoor tales como: Subseven, CyberGate y Spynet.

9. La aplicación desarrollada es posible ejecutarla en versión posteriores del sistema operativo Windows XP, como SP3, ya que, se valen de la misma API. No obstante, dicha estandarización es al mismo tiempo una desventaja, puesto que, la API puede ser objeto de innumerables ataques Spyware tipo Backdoor, los cuales conociendo el funcionamiento de esta, se aprovechan de las debilidades encontradas, alterando, vulnerando y comprometiendo la seguridad integral del sistema Windows XP, particularmente ahora cuando la corporación Microsoft ha descontinuado el producto y con ello los servicios de actualizaciones del sistemas para corrección de fallas y errores de funcionamiento.

Referencias bibliográficas

1. HERNÁNDEZ SAMPIERI ROBERTO, FERNÁNDEZ COLLADO CARLOS & BAPTISTA LUCIO PILAR, (2010). *Metodología de la Investigación*. Quinta

edición. Edit. McGraw-Hill Editores, S.A. de C V México.

2. JARAUTA, J. SIERRA, J. Y PALACIOS, R. (2006). Instituto de Investigación Tecnológica de la Escuela Técnica Superior de Ingeniería ICAI de la Universidad Pontificia Comillas. *Seguridad Informática: Capítulo 2: Análisis de Riesgos*. http://goo.gl/yCzXnW. Consultada [28-07-2011].
3. SENN, JAMES A. (2001). *Análisis y Diseño de Sistemas de Información*. Segunda Edición. Editorial McGrawHill. México.
4. MA, J. SAUL, L. SAVAGE, S. Y VOELKER, G. (2009). *Identifying Suspicious URLs: An Application of Large-Scale Online Learning*. http://goo.gl/AwRd6K. Consulta [1-11-2013].
5. ESET. (2009). *Un dolor de cabeza llamado Spyware*. http://goo.gl/EDxWdl. Consultada [12-09-2011].
6. CASTILLO, SERGIO. MÚRCIA, JOSÉ. GARCÍA, JOAQUÍN. (2010). *El Spyware como amenaza contra navegadores web*. http://goo.gl/QHWhNO. Consultada [18-07-2011].
7. ACERO, F. (2010). *Los ataques cibernéticos*. http://goo.gl/JQaHTl. Consultada [31-10-2011].
8. ESET. (2011). *Malware para sistemas operativos GNU/Linux y Mac OS*. http://goo.gl/Gxudlo. Consultada [16-11-2011].
9. DELGADO, A. (2013). *¿Debo seguir utilizando Windows XP en 2014?*. http://goo.gl/yNsWml. Consultada [28-06-2015].
10. WELLMEYER, MATTHIAS. (2010). *Spyware development and analysis*. http://goo.gl/Rs2M63. Consultada [06-09-2011].
11. PANDASECURITY. (2011). *Spyware*. http://goo.gl/ZCwYE7. Consultada [07-09-2011].
12. PONNE, J (2010). *Mecanismo de seguridad activos en navegadores web para la protección de ataques tipo Spyware*. (Tesis (de licenciatura) – La Universidad del Zulia (LUZ)), [CD-ROM]. Directorio: Departamento de computación de La Universidad del Zulia.
13. GARCÍA, LINO M. (2009). *El arte de la seguridad*. http://goo.gl/yY2qop. . Consultada [15-09-2011].
14. MIERES, J. (2009). ESET - Latinoamérica. Problemas Comunes Ocasionados por Malware. http://goo.gl/29wxy8. Consultada [25-07-2010].
15. ALLIENHACKER. (2013). *Troyanos 2013*. http://goo.gl/6D5VJ3. Consultada [21-05-2013].
16. DORUK, CUMHUR (2006). *Ghostware and Rootkit Detection Techniques for Windows*. http://goo.gl/Kn34Gd. Consultada [05-09-2012]
17. DEWALD, A.; HOLZ, TH.; FELIX, C. (2009). Secure SystemsLab (isecLAB). Trabajo de investigación titulado *ADSandbox: Sandboxing Javascript to fight Malicious Websites*. Sierre, Switzerland.
18. ALGREDO, IGNACIO. CUMPLIDO, RENÉ. FEREGRINO, CLAUDIA. (2011). *Desarrollo de un módulo MD5 para un sistema criptográfico reconfigurable en un FPGA*. http://goo.gl/aiGNYo. Consultada [23-10-2013].

UNIVERSIDAD
DEL ZULIA

CIENCIA

Vol. 23 Nº 3, Julio-Septiembre 2015

Esta revista fue editada en formato digital y publicada en Septiembre de 2015, por el ***Fondo Editorial Serbiluz, Universidad del Zulia. Maracaibo-Venezuela***

www.luz.edu.ve
www.serbi.luz.edu.ve
produccioncientifica.luz.edu.ve