MULTICIENCIAS, Vol. 12, Nº 3, 2012 (319 - 326)
ISSN 1317-2255 / Dep. legal pp. 200002FA828

Mecanismo de seguridad activo en navegadores Web para protección de ataques tipo Spyware

David Bracho[1], Alfredo Acurero[1], Carlos Rincón[1], Jhogel Ponne[1] y Eddy Aguirre[2]

[1]*Facultad Experimental de Ciencias,* [2]*Facultad de Ciencias Económicas y Sociales, Universidad del Zulia. Maracaibo, Venezuela*

drbracho@fec.luz.edu.ve; aacurero@fec.luz.edu.ve; crincon@fec.luz.edu.ve; ponne.jhogel@gmail.com; ejaguirre@gmail.com

Resumen

El propósito de la investigación fue desarrollar un mecanismo de seguridad activo en navegadores Web para protección de ataques tipo Spyware. La investigación fue experimental, sustentada en lo planteado por Hernández *et al* (2003). También se utilizó la metodología de seguridad "Análisis de Riesgo de la Seguridad de la Información", de Jarauta *et al* (2006) y como metodología de desarrollo del mecanismo se escogió el "Método de Ciclo de Vida" propuesto por Senn (1992). Se desarrolló una extensión de tipo Browser Helper Object como mecanismo que proporcionó seguridad al navegador Web Internet Explorer versión 6.0 ante ataques Spyware. Los resultados obtenidos determinaron que el mecanismo para la seguridad propuesto presentó una efectividad para detectar sitios Web legítimos del 83,50% y para detectar sitios Web maliciosos del 60,60%. El error obtenido en comparación con la herramienta de seguridad comercial genérica "Spyware Doctor" fue 4,93% y 9,80% respectivamente.

Palabras clave: mecanismo de seguridad Web, Spyware, Internet Explorer Versión 6.0, browser helper object.

Recibido:02-05-2012 / Aceptado:24-09-2012

Active Security Mechanism on Web Browsers for Protection against Spyware Attacks

Abstract

The purpose of this research was to develop an active security mechanism to protect Web browsers from spyware attacks. The research was experimental, based on the methodology of Hernández *et al* (2003); the security methodology, "Risk Analysis for Information Security," proposed by Jarauta *et al* (2006), was also used. To develop the mechanism, methodology based on Senn's "Life-Cycle Method" (1992) was chosen. An extension of the Browser Helper Object type was developed to protect the Internet Explorer 6.0 Web Browser against spyware attacks. Results showed that the proposed security mechanism detected 83.50% of the legitimate URLs and 60.60% of the malicious URLs. The margin of error obtained, compared with the generic commercial security tool, "Spyware Doctor," was 4.93% and 9.90%, respectively.

Keywords: Web security mechanism, spyware, Internet Explorer Version 6.0, Browser Helper Object Web Security Mechanism, Spyware, Internet Explorer Version 6.0, Browser Helper Object.

Introducción

El uso de tecnologías de información y comunicación brinda oportunidades de comercio para los negocios, pero inevitablemente, abre la puerta para los ataques cibernéticos, y la Web no constituye una excepción a este patrón. Hoy día millones de atacantes cibernéticos, avanzan en una amplia variedad de estafas en la que incluyen la propagación, Malware domains (2011).

Según la compañía Websense (2010), en su informe de seguridad, el 52% de los ataques de robo de datos se llevan a cabo en la Web, sobresaliendo el Malware, como software malicioso que entra en el sistema sin autorización del usuario. En ese sentido, el informe identificó un aumento del 111.4% en el número de sitios Web maliciosos entre 2009 y 2010, y precisó que el 79,9% de los sitios Web con código malicioso eran sitios Web legítimos que habían sido comprometidos.

Es por ello que, a juicio de Cova *et al* (2010), del conjunto de posibles aplicaciones vulnerables, el navegador Web, es actualmente el objetivo más popular. Los atacantes crean sitios Web maliciosos que tratan de explotar las vulnerabilidades de éste, y distribuir Malware a través de técnicas de propagación como Javascript Ofuscado, Heurística etiqueta "iframe" y Heurística de URL principal del sitio Web. Ante esta realidad, Marketshare (2011), indicó que entre las versiones de navegadores Web más usados se encuentran el Internet Explorer (IE) versión 6.0 con 11%.

Sin embargo, Castillo *et al.* (2010), señala que los ataques contra navegadores Web pueden comprometer la seguridad y privacidad de los usuarios dada la propagación de software malicioso, como el Spyware. Razón por la cual Vinod *et al.* (2008), advirtió que los métodos de detección de los antivirus funcionaron bien hasta que el Malware evolucionó, eludiendo la detección basada en firmas.

En ese sentido, para Hackworth (2008), el Spyware es muy utilizado por los atacantes en línea y al mismo tiempo, es usado como herramienta para cometer delitos. Es así como, el Spyware puede ser instalado de forma secreta en los navegadores Web y de esa manera robar datos sensibles, tales como identificaciones de usuarios, contraseñas o datos financieros. Por lo tanto, a juicio de Castillo *et al* (2010), los navegadores Web deben incluir mecanismos confiables para garantizar la seguridad y privacidad de sus usuarios.

En función de lo antes expuesto el propósito de esta investigación fue desarrollar un mecanismo de seguridad activo que se incorporó al navegador Web Internet Explorer 6.0 (IE 6.0), para proveer protección ante una modalidad de ataque en Internet tipo Spyware.

Metodología

La metodología de investigación fue experimental, ya que según Hernández *et al* (2003), el diseño de la investigación es experimental cuando se hace un estudio en el que se manipulan intencionalmente una o más variables independientes (supuestas causas-antecedentes), para analizar las consecuencias que la manipulación tiene sobre una o más variables dependientes (supuestos efectos-consecuentes), dentro de una situación de control para el investigador. Adicionalmente, la metodología de seguridad utilizada, se basó en el "Análisis de Riesgo de la Seguridad de la Información" de Jarauta *et al* (2006), adaptada a los objetivos de esta investigación, aplicando 4 fases de 8 posibles. A continuación se explican brevemente en qué consiste cada una de ellas:

1. Identificación y valoración de los activos: consistió en identificar los activos a proteger. Para el presente caso fue seleccionado el navegador Web IE 6.0, ya que desde la perspectiva de Marketshare (2010), todavía es uno de los más utilizados (11%) y vulnerables a la fecha, incluso a pesar de encontrarse versiones actualizadas, robustas y seguras en el mercado.
2. Identificación y valoración de las amenazas: consistió en seleccionar la amenaza a usar en el experimento, escogiendo el ataque Spyware, ya que según Kirda *et al* (2006), es una de las principales amenazas para la seguridad de los usuarios de Internet.
3. Identificación y valoración de las vulnerabilidades: se basó en conocer cómo el ataque Spyware afecta al IE 6.0, y aprovecha la vulnerabilidad de éste. Lo que ocurre gracias al ingreso de vectores de infección que utilizan técnicas de propagación, explotando la seguridad. Castillo *et al* (2010).
4. Identificación y selección de las medidas de seguridad: requirió escoger una entre varias alternativas posibles, tales como: servicios Web, aplicaciones, script, entre otros, seleccionándose una extensión de tipo Browser Helper Object (BHO). De acuerdo con Msdn (2011), esta no son más que componentes ActiveX y Plug-in que se incorporan al IE 6.0, gracias al entorno de desarrollo integrado (IDE) de Microsoft Visual Studio 2008 que permite el desarrollo de un conjunto de plantillas en lenguaje C++ basadas en clases, que crea pequeños y rápidos Component Object Model (COM), los cuales son incorporados y ejecutados en el IE 6.0. Sin embargo, para llevar a cabo este proceso fue necesario utilizar la metodología de desarrollo "Método de Ciclo de Vida", de Senn (1992), la cual consta de un conjunto de actividades (análisis, diseño y pruebas) que los usuarios realizan para desarrollar e implantar un sistema de información.

Protocolo de prueba

El ambiente de prueba se apoyó en una Máquina Virtual (MV) que emuló un hardware con memoria RAM de 512 MB y contó con un Disco Duro de 130,520 MB, sobre el cual se instaló el Sistema Operativo (SO) Windows XP Professional Service Pack 2 de 32 bits con el navegador IE 6.0 (lo trae por defecto), sin ninguna extensión adicional. Aunado a ello, no se contaron con herramientas de seguridad (antivirus y/o cortafuegos activados); esto para observar el comportamiento del ambiente antes expuesto a la hora de un ataque. La MV se ejecutó en una computadora con las siguientes características: Procesador Intel Dual-Core, CPU E5300 @ 2.00GHz 2.60GHz, 1GB de memoria RAM, disco duro 520 GB y como SO Microsoft Windows XP Professional Service Pack 2 de 32 bits, con conexión a Internet, sin antivirus, ni cortafuego alguno.

Los localizadores de recursos uniformes (URLs) maliciosos, utilizados para las pruebas, se seleccionaron del sitio Web: "Malwareurl.com", que permitió descargar un archivo que contiene la lista de URLs maliciosos y actualizados, escogiéndose un porcentaje basado en criterios tomados a conveniencia y planteados por expertos en el área, tales como: a.- Dominios asociados con descargas de Spyware (lista correspondiente al mes de marzo de 2010). McAfee (2010); b.- Los 15 dominios de nivel superior (TLD) más peligrosos. Malwaredomains (2011); c.- El nombre del Host como dirección IP con frecuencia en sitio Web maliciosos. Choi *et al* (2010); d.- El nombre del Host de 2 etiquetas con frecuente en sitio Web maliciosos. Choi *et al* (2010); y 5.- Las URLs con extensión ".exe" con mayor probabilidad de descarga de Spyware. Stamminger *et al* (2009).

Las URLs obtenidas después de la selección fueron 100 y los casos de pruebas realizados todos sobre Navegación por la Web a través del IE 6.0, pero variando los: a.- sitios legítimos sin mecanismo; b- sitios legítimos con mecanismo; c- sitios maliciosos sin mecanismo; y d- sitios maliciosos con mecanismo. Los casos c y d usaron el porcentaje de URL´s indicado por los expertos.

Se utilizó la lista de sitios Web que ofrece "alexa.com", que registra los sitios más populares en Internet. De esta lista se escogieron los primeros 100. La lista es actualizada diariamente, y se usó la del 01 de abril de 2011. El tiempo de duración en la navegación fue de 20 segundos (seg.) como máximo, después que cargara completamente el si-

tio Web, ya que Dewald *et al* (2009), estableció que como tiempo promedio de un análisis estático en un sitio Web, éste no debe superar los 20 seg. En consecuencia, la generación de la prueba simuló la navegación Web, visitando las URLs escogidas, cronometrando el tiempo carga de cada una.

Por otra parte, el software utilizado en la MV fue Microsoft Virtual PC 2007 6.0, aisló el sistema de efectos perjudiciales que el Malware pudiera causar, tal cual lo expuso Aikaterinaki (2009), y con el fin de observar los cambios resultantes de las visitas a las URLs seleccionadas, en los distintos casos de pruebas, se escogieron varias herramientas: a.- "*Process Monitor* 2.94" que es una herramienta de monitoreo. Process (2011); b.- "Wireshark 1.4.4" que es un analizador de protocolos de red. Pctools (2011); c.- "Spyware Doctor 8.0" que es una herramienta de seguridad antispyware. Wireshark (2011). En ese sentido, se utilizaron las últimas versiones disponibles para todas las herramientas antes mencionadas. Las primeras dos herramientas monitorearon y analizaron el comportamiento del mecanismo durante las pruebas, así como al equipo de prueba. La última herramienta analizó el equipo en busca de posibles infecciones generadas en las pruebas y comparó los resultados obtenidos con los del mecanismo desarrollado.

Resultados y discusión

La presente investigación desarrolló un mecanismo de seguridad activo, que se añadió al IE 6.0 y ofreció protección ante ataques Spyware. Colateralmente, el mecanismo disminuye la dependencia en la incorporación de herramientas de seguridad de terceros (antivirus) que por estar desactualizados (bien sea por descuido del usuario, o por no poseer una licencia original) exponen al equipo, y por ende a la información que fluye y son realizadas a través del IE 6.0.

Descripción del funcionamiento del mecanismo propuesto

Desde la perspectiva de Msdn (2011), el IE 6.0, habilita (en su arquitectura), a los desarrolladores para que puedan reutilizar algunos de sus componentes. La arquitectura del navegador Web se basa en COM (una de las muchas formas de extender las capacidades del IE). Razón por la cual, se escogió como modelo del mecanismo la "extensión" del navegador, ya que la funcionalidad de éste permitió que al agregarse al IE 6.0, ésta se ejecuta tantas veces como se invoque al navegador Web. De hecho, y de acuerdo con Msdn (2004), el navegador Web inicializa la extensión y pide determinar la interfaz. Si ésta se encuentra, el navegador utiliza los métodos previstos para pasar el puntero de la interfaz IUNKNOWN del IE 6.0, obteniendo punteros a otras interfaces en un objeto determinado a través del método QueryInterface (consulta). De esta forma, el mecanismo se carga en el contexto del navegador y funciona como un componente del IE 6.0.

En ese sentido, el mecanismo escogido fue una extensión de tipo BHO realizada para el IE 6.0, y se creó para ser ejecutado por el proceso iExplorer.exe. De acuerdo con Msdn (2004), la extensión, es un simple objeto COM que implementa la interfaz iobjectwithsite. Los BHO pueden almacenar el puntero pasado por el IE 6.0 y, posteriormente, utilizarlo para obtener más interfaces específicas. Cuando el IE 6.0 se invoca, el mecanismo inicia su trabajo, es decir, está a la espera de que ocurra un evento originado por éste. El evento en espera carga completamente el documento de lenguaje de marcado de hipertexto (HTML) en el visor del IE 6.0. Al ejecutarse el evento, el mecanismo captura el cuerpo del documento HTML, que utiliza el protocolo de transferencia de hipertexto (HTTP), ya que sólo se consideraron páginas Web que utilizaron en la URL el protocolo HTTP Provos *et al* (2008) determinaron que éste sigue siendo el protocolo con más frecuencia de actividades maliciosas. Adicionalmente, Trend Micro (2007) y Kinkhorst y Kleij (2009), expusieron que las amenazas Web se benefician de los puertos 80 y 8080 de Internet. Los argumentos anteriores permitieron identificar el funcionamiento del mecanismo, el cual se enfocó en analizar la página Web con el protocolo http en la URL, ejecutando para ello los siguientes pasos, especificados por Seifert *et al* (2008), análisis: a- estático; b- del contenido; c- de la estructura.

El mecanismo analizó el documento del sitio Web cargado en el IE 6.0, en busca de características maliciosas, siendo consideradas y analizadas las siguientes: a- Heurística de la URL principal (busca algunos patrones maliciosos en la dirección URL) enfocada en elementos que la componen (nombre de Host; TLD y extensión de la URL); b- Javascript (busca Javascript Ofuscado), que ocultan el verdadero propósito, tal cual lo expuso Seifert *et al* (2008). Las funciones del lenguaje Javascript utilizadas en Javascript maliciosos, basado en las investigaciones de Choi *et al* (2010) y Forest *et al* (2010) quienes determinaron que si una cadena extraída es ofuscada, ésta posee 3 indicadores relevantes (algoritmo de n-gramo, entropía, y longitud de la palabra en la cadena). En consecuencia, las métricas consideradas fueron las siguientes: b.1- si la cadena incluye caracteres especiales en exceso; b.2- si la entropía de la cadena es menor que 1.2 bytes; y b.3- si la longitud de la cadena es más de 350

caracteres. c- Heurística de la etiqueta "iframe" (ubicó varias de las propiedades de la etiqueta tales como: altura, anchura, src y style). El resultado fueron las métricas consideradas: c.1- si el tamaño de la etiqueta es pequeña; c.2- si la visibilidad de la etiqueta es oculta; c.3- si se refiere a otro dominio y el tamaño es pequeño; y c.4- si se refiere otro dominio y la visibilidad es oculta.

En consecuencia, el módulo de defensa del mecanismo contrarrestó los efectos de posibles ataques Spyware, específicamente de los tipos BHO, Toolbars y Browser Hijackers que dañan al IE 6.0 y al sistema como tal. Barwinski *et al* (2005). De esta forma, el mecanismo limpió el sistema y respaldó las claves del registro de Windows y las carpetas modificadas por las amenazas antes mencionadas (Figura 1).

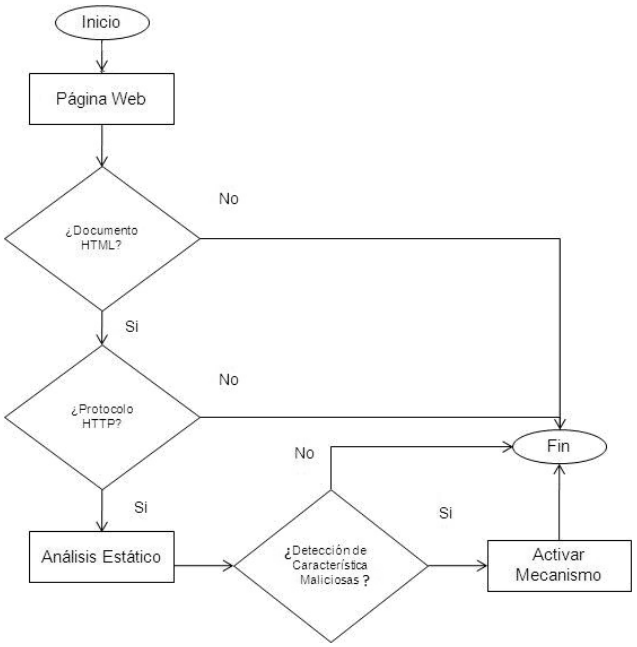
Resultados obtenidos

3.2.1."Caso sin Mecanismo y con URLs Legítimas". De 100 URLs, 97 se encontraban activas, 3 de ellas no (no cargaron una página Web durante las pruebas). El promedio de tiempo de navegación fue de 19,92 segundos (seg.). Las URLs procesadas, promedio de tiempo de detección, Falsos Negativos (FN) y Falsos Positivos (FP), no aplicaron.

3.2.2. "Caso sin Mecanismo y con URLs Maliciosas". De 100 URLs, 51 se encontraban activas, las restantes 49 no (no cargaron una página Web durante las pruebas). El promedio de tiempo de navegación fue de 19,96 seg. Las URLs procesadas, promedio de tiempo de detección, Falsos Negativos (FN) y Falsos Positivos (FP), no aplicaron.

3.2.3. "Caso con Mecanismo y con URLs Legítimas". De 100 URLs, 97 se encontraban activas, 3 de ellas no (no cargaron una página Web durante las pruebas). El promedio de tiempo de navegación fue de 17,09 seg.; el número de URLs procesadas fueron 92; y el promedio de tiempo de detección fue de 0,77 seg. La cantidad de FP fueron 15 y de FN no aplicó (por ser casos de presuntas Web legítimas). Se utilizó la herramienta de seguridad comercial y genérica Spyware Doctor, aplicando las mismas pruebas para comparar resultados (Tabla 1).

Los resultados arrojados en los porcentajes de URLs detectadas en cuanto a FP son similares, es decir, 97 activas de 100 URLs legítimas. El mecanismo procesó 92 y Spyware Doctor 97, esto se debe, básicamente a la diferencia que hay entre las URLs procesadas. En ese sentido, y en cuanto a la detección de FP, el mecanismo arrojó la cantidad de 15 (efectividad de 16,30%), mientras Spyware Doctor encontró 16 (efectividad de 16,49%) representando una diferencia absoluta de 1 URL y relativa de 0,19%. Por su parte, y en cuanto a la detección de sitios Web legítimos, el mecanismo validó 77



Fuente: Ponne (2011).

Figura 1. Diagrama de flujo del mecanismo.

Tabla 1. Comparación Mecanismo y Spyware Doctor con URLs Legítimas.

Características	Herramienta	Mecanismo
URLs Inactivas	3	3
URLsActivas	97	97
URLsProcesadas	97	92
Falsos Positivos	16	15
Falsos Negativos	N/A	N/A
Sitio Web Legítimo	81	77

Fuente: Ponne (2011).

URLs (efectividad de 83,69%) y Spyware Doctor validó 81 URLs (efectividad de 83,50%). La diferencia absoluta fue 4 URLs y la relativa 4,93%, es decir el mecanismo fue efectivo en el 95,06% de los casos donde "Spyware Doctor" también lo fue.

3.2.4. "Caso con Mecanismo y con URLs Maliciosas". De 100 URLs, 51 se encontraban activas y 49 URLs no (no cargaron una página Web durante las pruebas). El promedio de tiempo de navegación y de detección fue de 9,36 seg., y de 0,54 seg., respectivamente; la cantidad de FN fueron 23. Los casos de FP no aplican dado el tipo de prueba (Tabla 2).

Los resultados mostraron que el mecanismo arrojó 54,90% de efectividad. En contraparte, Spyware Doctor

Tabla 2. Comparación Mecanismo y Spyware Doctor con URLs Maliciosas.

Característica	Herramienta	Mecanismo
URLs Inactivas	49	49
URLs Activas	51	51
Falsos Positivos	N/A	N/A
Falsos Negativos	18	23
Sitio Web Malicioso	33	28

Fuente: Ponne (2011).

registró 64,70%, lo que representó una diferencia porcentual de 9,80%. La diferencia se fundamentó en el número de FN encontrados, puesto que para ambos casos el número de URLs procesadas fueron las mismas (51). En consecuencia, los criterios asumidos en el mecanismo para detectar sitios Web maliciosos encontró la cantidad de 28. Esto es posible porque Spyware Doctor incorpora muchos más criterios que son aún más precisos, detectando la cantidad de 33 sitios Web maliciosos. En contraparte, los resultados correspondientes a los FN reflejaron una diferencia de 5 casos, equivalente a un 9,80%.

Sin embargo, y a pesar que 28 sitios Web maliciosos fueron detectados por el mecanismo de seguridad, apenas 8 contenían al menos 1 de las características maliciosas consideradas. Spyware Doctor detectó 33 sitios Web maliciosos, la diferencia en la efectividad fue 84,84%. Al descartar los 8 sitios Web no maliciosos clasificados, por el mecanismo, el número real de sitios Web maliciosos se redujo a 20, por lo tanto, la efectividad del mecanismo con respecto a Spyware Doctor fue 60,60%, disminuyendo en 24,24%. Por otra parte, de los 23 sitios Web considerados como FN por el mecanismo, Spyware Doctor detectó que 13 de ellos provocaron al menos 1 infección y el resto de los sitios Web (10), no provocaron infección, es decir 56,52%. Pero, al comparar con los valores obtenidos por Spyware Doctor, la tasa efectiva del mecanismo fue 55,55%, producto de 10 sitios Web "No" clasificados como FN por el mecanismo y "Si" por Spyware Doctor de un total de 18 sitios maliciosos.

En consecuencia, resultó importante comparar los resultados obtenidos entre los casos con y sin Mecanismo cuando las URLs fueron maliciosas; la cantidad de infecciones encontradas por los resultados de los análisis con Spyware Doctor son similares, y la pequeña diferencia encontrada radicó en la eliminación de varias infecciones directamente, puesto que, Spyware Doctor automáticamente desplegó una serie de acciones (adicionales a las del mecanismo) que contribuyó a una mayor eficiencia. Es decir, en el Caso de prueba sin mecanismo, la cantidad de infecciones encontradas fueron 61, generadas por 33 sitios Web maliciosas y para el Caso de prueba con mecanismo, la cantidad de infecciones encontradas fueron 51, provenientes de 33 sitios Web; detectando el mecanismo 28 de 33 sitios posibles (efectividad de 84,84%).

Finalmente, y en lo que respecta al tiempo de navegación, para los casos cuando el mecanismo estuvo activo y las URLs fueron legítimas o maliciosas, fueron de 17,09 seg., y 9,36 seg., respectivamente. Lo que significó que tan pronto el mecanismo completó el análisis de los sitios Web, bloqueó de forma oportuna la navegación. Los tiempos de detección para los casos cuando el mecanismo estuvo activo y las URLs fueron legítimas o maliciosas fueron de 0,77 seg., y 0,54 seg., respectivamente. Lo anterior evidenció que el análisis de sitios Web fue rápido, actuando oportunamente ante la presencia del Spyware.

Consideraciones finales

El resultado final del experimento arrojó las siguientes consideraciones:

Fue posible desarrollar un mecanismo de seguridad activo específico, como extensión del navegador Web IE 6.0 para proteger contra ataques Spyware de tipo Browser Hijackers, BHO y Toolbars. En consecuencia, el mecanismo analizó el contenido de las páginas Web en busca de características maliciosas JavaScript Ofuscado, Heurística etiqueta "iframe" y Heurística de URL principal del sitio Web, alertando al usuario sobre la navegación segura (insegura) del sitio. Adicionalmente, el mecanismo redujo infecciones que no fueron consideradas como Spyware, pero que pueden ser maliciosas.

El tiempo de detección promedio presentado por el mecanismo para el caso de prueba con URLs maliciosas fue de 0.54 seg., siendo menor que el tiempo de detección de 20 seg., fijado por los expertos en el tema. El porcentaje de detección de URLs legítimas por parte del mecanismo fue 83,69% para cuando se analizaron sitios Web legítimos y los FP reencontrados fueron 16,30% equivalentes a 15 URLs. Por otro lado, el 54,90% de los casos analizados por el mecanismo fueron tipificados como URLs maliciosas, equivalentes a 28 de 51 URLs y los FN arrojado por éste para casos de prueba con URLs maliciosas fue de 45,09%, equivalente a 23 URLs de 51 sitios evaluados. Sin embargo, si se excluyen los 10 sitios Web maliciosos que no provocaron infección alguna, la efectividad sería 56,52%.

Al comparar los FN arrojados Spyware Doctor con el mecanismo, la efectividad fue 55,55%, provenientes de 10 FN identificados por el mecanismo (no infecciosos) de un total de 18 FN arrojados por Spyware Doctor. En consecuencia, la diferencia proporcional de los resultados obtenidos entre ambos, así como para los FP propuesto para el Casos de prueba con URLs legítimas fue del 0,19%, y de los 15 sitios Web clasificados como FP por el mecanismo, 4 causaron al menos 1 infección. Siendo la diferencia proporcional de los resultados obtenidos entre ambos, para Casos de prueba con URLs maliciosas de 9,80% y para casos de FP de 10,68%

La efectividad del mecanismo propuesto para casos de detección de URLs maliciosas fue 54,90%, pero al compararse con Spyware Doctor fue 84,84%. Sin embargo, al excluir los casos "No" detectados por el mecanismos y "Si" por Spyware Doctor ésta fue 60,60%. Con respecto al número de FN para casos de URLs maliciosas, se encontraron 23. Spyware Doctor detectó que 13 de 23 provocaron al menos 1 infección (efectividad del 56,52%). Es por ello que, la tasa efectiva del mecanismo con respecto a Spyware Doctor fue 55,55%, producto de 10 sitios Web "No" clasificados como FN por el mecanismo y "Si" por la herramienta Spyware Doctor de un total de 18 sitios Web maliciosos.

La cantidad de infecciones eliminadas por el mecanismo para casos de pruebas con URLs legítimas fueron 3 (efectividad del 20,00% de 15 Casos de FP). Por su parte, la cantidad de infecciones eliminadas por el mecanismo para Casos de pruebas con URLs maliciosas fueron 11 (efectividad del 39,28%, de un total de 23 casos de FN).

Los tiempos de navegación y de detección para Casos cuando el mecanismo estuvo activo y las URLs fueron legítimas o maliciosas fueron de 17,09 seg., 9,36 seg., 0,77 seg., y 0,54 seg., respectivamente. Evidenciándose que el tiempo de detección fue rápido y permitió bloquear oportunamente sitios Web sospechosos, reduciendo la navegación riesgosa.

Referencias

AIKATERINAKI, N. (2009). Instituto Universitario de Londres Royal Holloway. Trabajo de investigación Drive-By Download Attacks: Effects And Detection Methods. Londres, Inglaterra.

BARWINSKI, M.; IRVINE, C.; LEVIN T. (2005). Taxonomy Of Spyware And Empirical Study Of Network Drive-By-Downloads. (Documento en línea). Disponible: Http://www.obermayer.org/~andyo/Data/theses.nps.navy.mil/05Sep_Barwinski.pdf. [Consulta: 2010, septiembre 03].

CASTILLO, S.; MÚRCIA, A.; GARCÍA, J. (2010). El Spyware como amenaza contra navegadores Web. (Documento En línea). Disponible: HTTP://ccd.uab.es/~joaquin/papers/recsi2010-paper28.pdf. [Consulta: 2010, octubre 10].

CHOI, Y.; KIM, T.; CHOI, S. (2010). Automatic Detection for Javascript Obfuscation Attacks in Web Pages through String Pattern Analysis. (Documento en línea). Disponible: HTTP://www.sersc.org/journals/IJSIA/vol4_no2_2010/2.pdf. [Consulta: 2009, octubre 17].

COVA, M.; KRUEGEL, CH.; VIGNA, G. (2010). Detection and Analysis of Drive-by-Download Attacks and Malicious Javascript Code. (Documento en línea). Disponible: Http://www.cs.ucsb.edu/~vigna/publications/2010_cova_kruegel_vigna_Wepawet.pdf. [Consultada 28-11-2010].

DEWALD, A.; HOLZ, TH.; FELIX, C. (2009). Secure Systems Lab (isecLAB). Trabajo de investigación titulado ADSandbox: Sandboxing Javascript to fight Malicious Websites. Sierre, Switzerland.

FOREST, D.; CHOO CH.; KNG POH, L.: HO S. (2010). National University of Singapore. HoneySift: A fast approach for low interaction client based Honeypot. [En línea]. Dirección URL: http://www.nus.edu.sg/. [Consultada 03-12-2010].

HACKWORTH, A. (2008). Computer Emergency Response Team, Spyware. (Documento en línea). Disponible: Http://www.cert.org/archive/pdf/Spyware2005.pdf. [Consulta: 2010, febrero 14].

HERNÁNDEZ R.; FERNÁNDEZ C.; BAPTISTA P. (2003). **Metodología de la Investigación.** Tercera edición. Edit. McGraw-Hill Editores, S.A. de C V México.

JARAUTA, J.; SIERRA, J.; 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. (Documento *e*n línea). Disponible: HTTP://www. iit.upco.es/palacios/seguridad/cap02.pdf. [Consulta: 2009, mayo 07].

KINKHORST, T.; KLEIJ, M. (2009). Detecting the ghost in the browser: Real time detection of drive-by infections. (Documento en línea). Disponible: Https://www.os3.nl/. [Consulta: 2010, enero 06].

KIRDA, E.; KRUEGEL, CH.; BANKS, G.; VIGNA, G.; KEMMERER Richard A. (2006). Behavior-based Spyware Detection. (Documento en línea). Disponible: HTTP://iseclab.org/papers/Spyware.pdf. [Consulta: 2010, marzo 13].

MA, J; SAUL, L.; SAVAGE, S; Y VOELKER, G. (2009). Identifying Suspicious URLs: An Application of Large-Scale Online Learning. (Documento en línea). Disponible: Http://cseWeb.ucsd.edu/~savage/papers/ICML09.pdf. [Consulta: 2010, noviembre 10].

MALWAREDOMAINS (2011). Lista de dominios de Spyware. (Documento en línea). Disponible: Http://www.Malwaredomains.com/. [Consulta: 2010, mayo 25].

MARKETSHARE (2011). Navegadores Web y sus versiones más utilizadas. (Documento en línea). Disponible: Http://marketshare.hitslink.com/. [Consulta: 2011, abril 03].

MCAFEE (2010). Mapping the Mal Web. The world's riskiest domains McAfree. (Documento en línea). Disponible: Http://us.mcafee.com/en-us/local/docs/MTMW_Report.pdf. [Consulta: 2011, febrero 10].

MSDN MICROSOFT (2011). Arquitectura del navegador Web Internet Explorer**.** (Documento en línea). Disponible: Http://msdn.microsoft.com/en-us/library/aa741312 (v=vs.85).aspx. [Consulta: 2009, mayo 03].

MSDN MICROSOFT (2004). Microsoft Corporation. Browser Helper Objects (BHO): The Browser the Way You Want It. (Documento en línea). Disponible: Http://msdn.microsoft.com/en-us/library/bb250436%28v=vs.85%29.aspx. [Consulta: 2009, mayo 03].

PCTOOLS (2011). (Documento en línea). Disponible: Http://www.pctools.com/. [Consulta: 2009, mayo 16].

PROCESS MONITOR (2011). (Documento en línea). Disponible: Http://technet.microsoft.com/en-us/sysinternals/bb896645. [Consulta: 2011, febrero 11].

PROVOS, N.; MAVROMMATIS, P.; RAJAB, MOHEEB A.; MONROSE, F. (2008). Google Technical Report provos. All Your iFRAMEs Point to Us. (Documento en línea). Disponible: Http://cs.unc.edu/~fabian/papers/iframes.pdf. [Consulta: 2009, octubre 16].

SEIFERT, C.; WELCH, I.; KOMISARCZUK P. (2008). Identification of Malicious Web Pages with Static Heuristics. (Documento en línea). Disponible: HTTP://www.citeseerx.ist.psu.edu. [Consulta: 2010, marzo 15].

SENN, J. (1992). **Análisis y Diseño de Sistemas de Información.** Segunda Edición. Editorial McGrawHill. México.

STAMMINGER, A.; KRUEGEL, C.; VIGNA, G.; KIRDA, E. (2009). University of California y Institut Eurecom. Automated Spyware Collection and Analysis. (Documento en línea). Disponible: Http://www.iseclab.org/papers/Spyware_isc09.pdf. [Consulta: 2010, marzo 15].

TREND MICRO (2007). Gestión de Amenazas Web. (Documento en línea). Disponible: Http://es.trendmicro.com/imperia/md/content/es/br09_entWebthreats_071221es.pdf. [Consulta: 2009, junio 03].

VINOD, P.; GAUR, M.; LAXMI, V. (2008). Survey on Malware Detection Methods. [Documento en línea]. Disponible: Http://www.security.iitk.ac.in/contents/events/workshops/iitkhack09/papers/vinod.pdf. [Consulta: 2010, marzo 15].

WEBSENSE (2010). Informe de Amenazas. (Documento En línea). Disponible: Http://www.Websense.com/assets/reports/report-security-labs-threat-report-2010-es.pdf. [Consulta: 2010, agosto 12].

WIRESHARK (2011). [Documento en línea]. Disponible: Http://www.wireshark.org/. [Consulta: 2011, febrero 10].