ISSN: 1317-2255
Deposito Legal: pp 20002FA828
Dep. legal ppi 201502ZU4642

Vol 15, Nº 3
Julio - Septiembre 2015

Multiciencias

RMCs

Universidad del Zulia
Revista Arbitrada Multidisciplinaria

LUZ Punto Fijo

Núcleo LUZ-Punto Fijo
Programa de Investigación y Posgrado
Falcón-Venezuela

Multiciencias / Revista Arbitrada Multidisciplinaria del Núcleo LUZ-Punto Fijo

MULTICIENCIAS, Vol.15, Nº 3, 2015 (339 - 346)
ISSN: 1317-2255 / Deposito Legal: pp 20002FA828 / Dep. legal ppi 201502ZU4642

Optimización del mecanismo de seguridad activo en navegadores web para protección de ataques tipo Spyware

David Bracho, Daniel Núñez, Eugenio Ferrer, Afredo Acurero, Carlos Rincón y Amir Granadillo

Universidad del Zulia. Venezuela. Maracaibo. Edo Zulia. Venezuela.

drbracho@fec.luz.edu.ve; dan88x@gmail.com; eferrer@fec.luz.edu.ve; acurero@fec.luz.edu.ve; crincon@fec.luz.edu.ve; agranadillo@fec.luz.edu.ve

Resumen

El propósito de la investigación fue optimizar el mecanismo de seguridad activo en navegadores Web para protección de ataques tipo Spyware, desarrollado por Ponne (2012). La investigación fue experimental, de tipo proyecto factible según Hernández et al (2012) y Upel (2010). El marco de referencia fue "Análisis de Riesgo de la Seguridad de la Información" de Jarauta et al (2006) y "Método de Ciclo de Vida" de Senn (2001). La optimización resolvió problemas del análisis de páginas Web HTTPS, características maliciosas en Visual Basic Script, Tags Form y Embed no abordados por Ponne (2012). Los resultados evidenciaron que en promedio la efectividad del mecanismo optimizado fue 69,02%, el tiempo de navegación fue 17,25 seg y el de detección fue 2,5 seg. Se experimentó una desmejora en los promedios globales debido al incremento de la complejidad, hecho compensado en la ampliación de la cobertura de protección no analizada por Ponne (2012).

Palabras clave: Spyware; HTTPS; visual basic script; tags form; tags emdeb.

Recibido: 10-11-2014 / Aceptado: 10-03-2015

Optimization of active security mechanism in web browser for protection against Spyware attacks

Abstract

The purpose of the research was to optimize the safety mechanism developed by Ponne (2012) to protect Web browsers against Spyware attacks. The research was experimental (feasible project) according to Hernández et al (2012) and UPEL (2010) respectively. The used framework is a combination of "Risk Analysis of Information Security" and "Method of Life Cycle" of Jarauta et al (2006) and Senn (2001) respectively. The optimization solved problems not addressed by Ponne (2012): analysis HTTPS Web pages, malicious features in Visual Basic Script, Form and Embed Tags. The results showed that on the average the effectiveness of the optimized mechanism was 69.02%, the Web browser time was 17.25 sec and detection time was 2.5 sec. A decrease on the average performance of the mechanism was observed due to complexity, however this is compensated by increasing the security.

Key words: Spyware; HTTPS; visual basic script; tags form; tags emdeb.

Introducción

En el año 2011, Ponne, Jhogel desarrolló un mecanismo activo para prevenir ataques tipo Spyware, Browser Hijackers, Browser Helper Object (BHO) y Toolbars. Este mecanismo fue construido como una extensión del navegador Web Internet Explorer (IE) versión (v) 6.0 para analizar el contenido de páginas Web en busca de características maliciosas Java Script (JS) Ofuscado, Heurística de etiqueta "iframe" y de medio principal de localización de los distintos recursos en Internet (URL) del sitio Web, que usan protocolo Hyper Text Transfer Protocol (HTTP), ya que atentan contra la navegación segura del usuario.

Los resultados de Ponne (2012) evidenciaron en primer lugar, que cuando el mecanismo estuvo activo con URL legítimas, el porcentaje de detección de URLs fue del 83,69% de efectividad (Efec), producto de dividir 77 URLs legítimas entre 92 URLs activas, de un total de 100 URLs consideradas. Adicionalmente, el tiempo promedio de detección (TPD) fue de 0,77 seg, identificando 15 URLs como Falsos Positivos (FP). En segundo lugar, cuando el mecanismo estuvo activo con URLs maliciosas, el porcentaje de detección de URLs fue de 54,90% de Efec, producto de dividir 28 URLs maliciosas de 51 URLs activas, de un total de 100 URLs consideradas. Adicionalmente, el TPD fue de 0,54 seg identificando 23 URLs como Falsos Negativos (FN).

Sin embargo, y a pesar de la seguridad ofrecida el mecanismo desarrollado por Ponne (2012) presentó limitaciones, en cuanto a la robustez y consistencia, ya que, no abarcó aspectos tales como: análisis de páginas Web Hyper Text Transfer Protocol Secure (HTTPS), análisis de las funciones (JS), análisis de las funciones Visual Basic Script, (VBS) análisis de Tags Form (Etiquetas de Formatos) y Embed (Etiquetas Incrustadas), e inclusión de nuevos elementos y claves en backup (respaldos) de registro. En consecuencia, se optimizó el mecanismo de seguridad activo añadido al IE v6.0 desarrollado por Ponne (2012), ampliando el campo de protección originalmente dispuesto por éste, ofreciendo mayor y mejor seguridad ante ataques Spyware, analizando páginas Web HTTPS, funciones JS, funciones VBS, Tags Form y Embed, y nuevos elementos y claves en backup (respaldos) de registro.

Finalmente, para garantizar la homogeneidad de los procesos entre la versión original y la optimizada se utilizó el mismo marco de referencia metodológico como lo fue "Análisis de Riesgo de la Seguridad de la Información" y "Método de Ciclo de Vida" de Jarauta *et al* (2006) y Senn (2001) respectivamente, como se aplicó el mismo protocolo y los escenarios de pruebas.

Metodología

La metodología de investigación fue experimental, según Hernández *et al* (2012) puesto que el diseño experimental manipula intencionalmente una o más variables independientes, con el fin de analizar las consecuencias (impacto o efecto) que dicha manipulación tiene sobre una o más variables dependientes. En ese

sentido, y debido a que el mecanismo original planteado por Ponne (2012) fue de tipo proyecto factible, se dedujo que también la optimización lo sería, puesto que, de acuerdo con UPEL (2010) un proyecto factible responde a la generación de un modelo o propuesta viable que presente soluciones a un problema concreto – práctico, con base a satisfacer las necesidades de una institución o grupo social. Particularmente, la optimización beneficia a todos los usuarios que aún utilizan al navegador Web IE v6.0.

No obstante, podría pensarse que por ser obsoleto el navegador IE v6.0 y al haber sido desincorporado por parte del fabricante Microsoft no tiene relevancia y vigencia práctica. Sin embargo, y desde la perspectiva de w3schools (2014) dicha versión del IE sigue registrando adeptos, arrojando una participación del 12,08% y 0,13% con respecto a otras versiones del navegador IE y de otras marcas de navegadores respectivamente, durante el año 2013 a nivel global. Razón por la cual, los riesgos inherentes al uso del IE v6.0 siguen estando presente y continúan representando en la actualidad una amenaza latente que compromete la integridad, confidencialidad y disponibilidad tanto de los recursos como de las operaciones basadas en Internet.

Adicionalmente, se utilizó la metodología de seguridad como marco de referencia principal "Análisis de Riesgo de la Seguridad de la Información" de Jarauta *et al* (2006), la cual evalúa los activos empresariales y la eficiencia de las medidas de seguridad ante amenazas y vulnerabilidades actuales, cuantificando la exposición al riesgo en función a la disponibilidad, confidencialidad e integridad de la información. Para ello se adaptaron y aplicaron 4 fases de las 8 posibles de acuerdo a la conveniencia de la investigación. a.- Identificación y valoración de los activos: identificó los activos a proteger, seleccionado el navegador Web IE v6.0, ya que, desde la perspectiva de W3schools (2014) su participación a nivel mundial sigue siendo importante. b.- Identificación y valoración de las amenazas: selección de las amenazas usadas en el experimento, escogiendo ataques Spyware, porque según Microsoft (2013) representan un problema que atentan contra páginas con protocolo HTTPS; código VBS y VBS, Tags Form y Tags Embed no desarrollados en la versión original de Ponne (2012). c.- Identificación y valoración de las vulnerabilidades: funcionamiento de los ataques tipo Spyware en el IE v6.0. A juicio de Castillo *et al* (2010) el ingreso de vectores de infección utilizan técnicas de propagación, que explotan la seguridad del IE v6.0. d.- Identificación y selección de las medidas de seguridad: adaptación y ampliación de la solución tipo Browser Helper Object (BHO) implementada por Ponne (2012). De hecho, se aplicó el mismo procedimiento con las variantes del caso, siguiendo la metodología de desarrollo "Método de Ciclo de Vida", de Senn (2001) usada por Ponne (2012) para garantizar la homogeneidad, consistencia y resultados confiables.

Protocolo de prueba

Para garantizar la homogeneidad de las pruebas realizadas entre la versión original y la optimizada, se utilizó el mismo protocolo y los escenarios aplicados por Ponne (2012) asegurando con ello la confiabilidad y consistencia de los resultados. De hecho, se consideraron 100 URLs a analizar, tal cual se estableció para el mecanismo original, siempre y cuando cumplieran con los criterios descritos más adelante, sometiendo así, al mecanismo optimizado a los mismos escenarios por los cuales fue examinado el original. En efecto, se asumió igual patrón de navegación, estandarizando los casos de pruebas entre ambos mecanismos, quedando estructurados en la siguiente forma: a.- "Caso sin Mecanismo y con URLs Legítimas", b.- "Caso con Mecanismo y con URLs Legítimas", c.- "Caso sin Mecanismo y con URLs Maliciosas", y d.- "Caso con Mecanismo y con URLs Maliciosas". Ver Figura 1. Ambiente de Prueba.

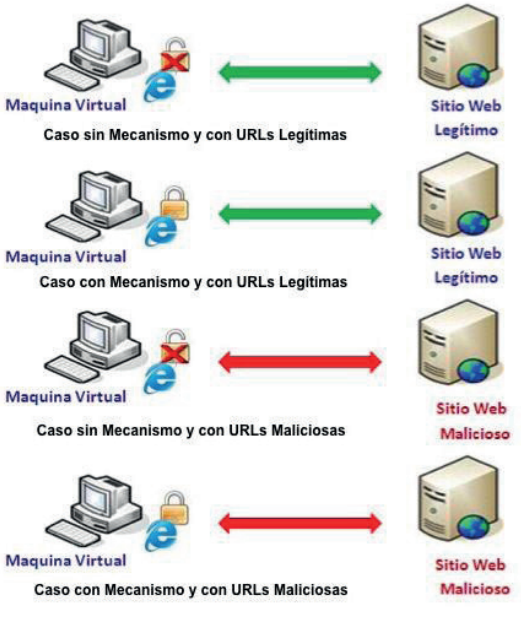

Figura 1. Ambiente de Prueba.
Fuente: Propia (2013).

Los criterios fueron los siguiente: Criterio Nº1: el ambiente de prueba consistió en Máquinas Virtuales (MV) ejecutadas en una computadora con procesador Intel Core 2 Duo, CPU T7500 @ 2.20GHz, 2GB de RAM, 320GB en disco con sistema XP Professional Service Pack 2 de 32 bits (XP SP2), sin software de seguridad instalado. La MV se conformó con 512 MB de RAM, 500MB de disco duro y sistema XP instalando el IE v6.0, sin ninguna extensión adicional según Oldapps (2012), ni herramientas de seguridad como antivirus y/o cortafuegos. Es por ello que, al seleccionar idénticos entornos operativos y herramientas utilizadas por Ponne (2012) se dispuso que el software de la MV según Microsoft (2012) fuese el Microsoft Virtual PC 2007 6.0, lo que aseguró mantener el sistema aislado de efectos perjudiciales ocasionados por el Malware y que pudieran alterar los resultados esperados, aspecto recomendado por Aikaterinaki (2009).

Criterio Nº2: para observar los cambios resultantes de cada visita hecha a las URLs escogidas se actualizaron las siguientes herramientas: "Process Monitor 3.03" herramienta de monitoreo, de acuerdo con Process (2012), "Wireshark 1.8.3" analizador de protocolos de red, según Wireshark (2012), y "Spyware Doctor 9.1" herramienta de seguridad antispyware, a juicio de Pctools (2012). Las dos primeras herramientas monitorearon y analizaron el comportamiento del mecanismo y del equipo durante las prueba. La última herramienta analizó el equipo en busca de posibles infecciones generadas en las pruebas.

Criterio Nº3: los localizadores de recursos de uniformes (URLs) maliciosos utilizados para las pruebas fueron tomados del sitio Web: "www.malwareurl.com", según Malwaredomain (2012), así como los sitios Web con protocolo HTTPS, dominios de nivel superior (TLD) más peligrosos, específicamente .co.cc, .co.cz, .cz.cc, in, .info, .org, .uni, y .me) siguiendo lo estipulado por McAfee (2010), los nombre de Host como dirección IP, frecuentemente vinculado a sitios Web maliciosos según lo establecido por de Kinkhors *et al* (2012), nombre del Host de 2 etiquetas, comúnmente asociado a sitios Web maliciosos a criterio de Kinkhors *et al* (2012), y URLs con extensión ".exe" las cuales poseen mayor probabilidad de descarga de Spyware según Stamminger *et al* (2009).

Sin embargo, para ejecutar dichos escenarios se establecieron varias consideraciones. Consideración general. Para todos los escenarios aplicó lo dispuesto por Dewald *et al* (2009) y Ponne (2012) fijando para el análisis estático como tiempo máximo de navegación los 20 seg y el tiempo máximo de detección los 6,40 seg. Por ello, cualquier sitio Web que superó esa cuota fue clasificado como "página inactiva" y descartado para el cálculo de la Efec y del TPD. Consideración particular Nº1: abarcó los escenarios "a" y "b". Se usó la lista del portal "www.alexa.com" del 01 de Noviembre de 2012, que registra y actualiza los enlaces más populares de Internet diariamente, de acuerdo con Alexa (2012). Consideración particular Nº2: comprendió los escenarios "c" y "d". Se utilizó la lista del portal "www.malwareurl.com" del 01 de Noviembre de 2012, que registra y actualiza los enlaces Web maliciosos diariamente, según Malwaredomain (2012).

Discusión y análisis de resultados

La presente investigación optimizó el mecanismo de seguridad activo añadido al IE v6.0 desarrollado por Ponne (2012), ampliando el campo de protección originalmente dispuesto por éste, ofreciendo mayor y mejor seguridad ante ataques Spyware, analizando páginas Web HTTPS, funciones JS, funciones VBS, Tags Form y Embed, y nuevos elementos y claves en backup (respaldos) de registro.

Descripción del funcionamiento y estructura del mecanismo optimizado

Se mantuvo el funcionamiento y estructura del mecanismo desarrollado por Ponne (2012), es decir el "core", adaptando solo aquellos aspectos particulares necesarios para resolver los ataques nuevos, ya que, la arquitectura del navegador IE v6.0 permite reutilizar componentes "COM" (modelo de componentes de objetos) referido por Msdn (2004) como una de las distintas forma de extender las capacidades de los navegadores. Es por ello que, similarmente a lo que sucedió con el mecanismo de Ponne (2012) el mecanismo optimizado queda a la espera que ocurra un evento originado por él, lo que conlleva a la carga del documento completo en lenguaje de marcado de hipertexto (HTML) en el visor del IE v6.0. No obstante, el mecanismo optimizado captura el cuerpo del documento HTML que utilizan tanto protocolos HTTP como HTTPS.

Es por ello que, se siguió el procedimiento dispuesto por Seifert *et al* (2008) para el estudio de las páginas Web según los criterios: estático, contenido y estructura. Particularmente, y en lo que respecta análisis

estáticos (detección) verificando y validando la dirección URL (maliciosa o no), aplicando técnicas simultáneas de análisis del contenidos y estructuras de la página Web, conservando así la modalidad del formato .DLL (bibliotecas de vínculos dinámicos) como extensión BHO, pero agregando variables nuevas:

a.- Tags Form y Tags Embed: se comparó el atributo "Action" para el Form y el atributo "SRS" (source) para los "iframe" y "Embed", utilizando la lista del sitio "www.malwareurl.com" según Malwaredomain (2012). Por lo tanto, con sólo ubicar un atributo malicioso (el primero), automáticamente se detuvo la navegación advirtiendo al usuario y bloqueando la URL. Ahora bien, los Tags Form presentaron otras características peligrosas señaladas por Dougherty (2012) consideradas en el método de ingreso (GET) y egreso (POST) de información, usadas para capturar datos del usuario sin consentimiento alguno.

b.- Sitios Web con protocolos HTTPS: se consideró la validación de certificados de acuerdo con Pushpendra *et al* (2012) que para el caso del XP se encuentran en un reservorio propio denominado "X509" donde se aloja los certificados válidos, corrigiendo las deficiencias del IE v6.0.

c.- Páginas Web con VBS: se incorporaron diversos registros, métodos y funciones de respaldo para detectar código malicioso del VBS. En ese sentido, las funciones estudiados fueron las identificadas por Bielova (2012) a través de las cuales los Spyware recurren a ellas para extraer información entre el IE v6.0 y los servidores, modificando la configuración del sistema y capturando data sin autorización. Las funciones fueron: Regwrite (escribe en registro de sistema), Regread (lee en registro de sistema), Regdelete (elimina registros), Specialfolders (acceso a carpetas del sistema), Getfolder (acceso a carpetas específicas), Getfile (captura archivos específicos) y Createprocess (crea procesos en el sistema). El método analizó totalmente los Script ubicando elementos maliciosos dentro de las funciones mencionadas, alertando al usuario sobre la peligrosidad del sitio. La lista de registros fueron incorporados al área de respaldo (backup) del XP, según lo dispuesto por Norton (2010).

Variantes del mecanismo optimizado

Ambos mecanismos analizaron el documento del sitio Web cargado en el IE 6.0. N obstante, existen variantes que marcan diferencias entre la versión original y la optimizada, tales como: Heurística de la URL principal enfocada en elementos que la componen incluyendo la certificación del protocolo HTTPS, Análisis estático para determinar VBS Ofuscado, validación y verificación del código VBS, Tags Form y Tags Embed y activando el mecanismo para el respaldados de registros del XP. Es importante acotar que las funciones VBS maliciosas fueron mencionadas por Ponne (2012) más no desarrolladas, siguiendo lo referido por Choi *et al* (2010) y Forest et al (2010), hecho implementado en la optimización. Adicionalmente, el módulo de defensa del mecanismo optimizado se incorporó al Toolbar, integrándose al IE v6.0, pudiendo activarse a conveniencia del usuario. En definitiva, el mecanismo contrarrestó los efectos de los posibles ataques Spyware, tales como: BHO, Toolbars y Browser Hijackers, lo cuales dañan tanto al IE v6.0 y como al XP, limpiando el sistema y respaldando claves del registro del sistema XP, así como, los sitios modificados (carpetas) por los Spyware antes mencionados. A continuación se muestra el Diagramas de Flujo Mecanismo Original y Optimizado. Ver Figura 2. DFD Mecanismo Original y Optimizado.

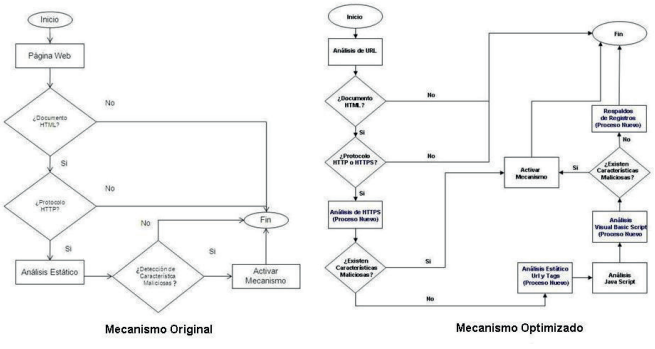

Figura 2. DFD Mecanismo Original y Optimizado.

Fuente: Propia (2013)

Resultados obtenidos

A fin de conocer la Efec, TPN y TPD del mecanismo optimizado, se compararon los valores con los arrojado por el de Ponne (2012), pero sólo en aquellos casos donde el mecanismo optimizado fue ejecutado, correspondiente a los escenarios "b" y "d" descritos en el "Protocolo de prueba". a.- Escenario "b" correspondiente al "Caso con Mecanismo y con URLs Legítimas": Ver Tabla 1. Frecuencias Mecanismos y Tabla 2. Promedios y Porcentajes Mecanismos. b.-

Escenario "d" correspondiente al "Caso con Mecanismo y con URLs Maliciosas": Ver Tabla 1. Frecuencias Mecanismos y Tabla 2. Promedios y Porcentajes Mecanismos. Finalmente, se muestra la Efectividad comparada entre el Mecanismo Original y el Optimizado. Ver Tabla 3. Eficiencia Mecanismos.

Tabla 1. Frecuencias Mecanismos

Frecuencias	URLs Legítimas		URLs Maliciosas	
Características	Mecanismo Original	Mecanismo Optimizado	Mecanismo Original	Mecanismo Optimizado
URLs Inactivas (URLs Inac)	3	8	49	54
URLs Activas (URLs Act)	97	92	51	46
URLs Procesadas (URLs Proc)	92	92	51	46
FP	15	11	No Aplica	No Aplica
FN	No Aplica	No Aplica	23	23
Sitios Web Legítimos (SWL)	77	81	No Aplica	No Aplica
Sitios Web Maliciosos (SWM)	No Aplica	No Aplica	28	23

Fuente: Propia (2013)

Tabla 2. Promedios y Porcentajes Mecanismo

Promedios y Porcentajes	URLs Legítimas		URLs Maliciosas	
Características	Mecanismo Original	Mecanismo Optimizado	Mecanismo Original	Mecanismo Optimizado
% FP (FP / URLs Proc)	16,30%	11,95%	No Aplica	No Aplica
% FN (FN / URLs Proc	No Aplica	No Aplica	45,09%	50,00%
% Sitios Web Legítimos (SWL) (SWL / URLs Proc)	83,69%	88,04%	No Aplica	No Aplica
% Sitios Web Maliciosos (SWM) (SWM / URLs Proc)	No Aplica	No Aplica	54,90%	50,00%
Promedio TPN (Σ PN / URLs Procesadas)	17,09 seg	17,25 seg	9,36 seg	17,25 seg
Promedio TPD (Σ PD / URLs Procesadas)	0,77 seg	3,40 seg	0,54 seg	1,60 seg

Fuente: Propia (2013)

Tabla 3. Eficiencia Mecanismos

Eficiencia	Efec SWL (% SWL)	Efec SWM (% SWM)	Efec Total (Σ Efec SWL + Efec SWM / 2
Características	URLs Legítimas	URLs Maliciosas	URLs Total
Mecanismo Original	83,69%	54,90%	69,29%
Mecanismo Optimizado	88,04%	50,00%	69,02%
Diferencia (Con respecto al Mecanismo Optimizado	4,35%	-4,90	-0,27%

Fuente: Propia (2013)

Consideraciones finales

Se logró optimizar el mecanismo de Ponne (2012) como una mejora que se incorporó como extensión al navegador Web IE 6.0 por medio de la cual se incrementaron los niveles de protección, en especial contra ataques Spyware tipo: Browser Hijackers, BHO y Toolbars. Las funcionalidades garantizaron corregir las características maliciosas: VBS Ofuscado, Heurística etiqueta "iframe" y Heurística de URL principal del sitio Web previstas por Ponne (2012) como parte de una actualización que amplió el espectro de protección original, arribando a una versión optimizada del mecanismo, mejoras que resolvieron problemas inherentes al: análisis de páginas Web con protocolo HTTPS, funciones VBS, Tags Form y Tags Embed, y claves en backup (respaldos) de registro.

De lo anterior se desprenden ciertas consideraciones particulares:

1.- El promedio global de la Efec del mecanismo optimizado agrupando los resultados obtenidos tanto para la detección de sitios Web legítimos como maliciosos fue 69,02%. Por su parte, el promedio global de la Efec del mecanismo original bajo los mismo términos fue 69,29%. En consecuencia, se evidenció una merma en el rendimiento del mecanismo optimizado con respecto al original del 0,27%, ya que, los TPN y TPD globales del mecanismo optimizado agrupando los resultados obtenidos en las condiciones antes mencionadas fueron 17,25 seg y 2,50 seg respectivamente, tiempos mayores a los TPN y TPD globales del mecanismo original, que bajo los mismo términos fueron 13,22 seg y 0,65 seg respectivamente. Razón por la cual, se evidenció una reducción en el rendimiento del mecanismo optimizado con respecto al original en los TPN y TPD en 4,03 seg y 1,85 seg respectivamente. Sin embargo, la disminución del rendimiento total fue compensado por el incremento del desempeño global, puesto que, el mecanismo optimizado abarcó una cantidad mayor de características maliciosas analizadas tales como: protocolos HTTPS, funciones VBS, Tags Form y Tags Embed, y claves de respaldo de registro, lo que redundó en el aumento sostenido de los niveles de seguridad.

2.- No obstante, el rendimiento no se puede medir únicamente por el TPD, ya que, se comete el error de hacer revisiones generales y a la ligera, que omiten, ignoran o subestiman, propiedades, atributos y características no emblemáticas maliciosas, autorizando a que agentes externos potencialmente dañinos ingresen y afecten significativamente la confiabilidad, integridad y disponibilidad de los recursos e información. Ahora bien, los TPD registrado por el mecanismo optimizado no superaron los 6,40 seg establecidos como cuota máxima de eficiencia fijada por investigaciones acreditadas en la seguridad Web.

3.- Indiscutiblemente que la relación velocidad – seguridad está influenciada por la cantidad y calidad de los elementos a inspeccionar, hecho que abarca el número de FP y FN. Es por ello que, al analizar con detenimiento la tasa de los FP y FN detectados por el mecanismo optimizado se evidencia que fue menor o igual que los localizados por el mecanismo original. En consecuencia, mientras menor sea la tasa de los FP y FN, mayor cantidad de sitios Web son evaluados. Por ende, menor cantidad de sitios Web no serán descartados como legítimo o malicioso "por defecto", reduciendo el número de sitios que quedan exentos del diagnostico. En ese sentido, forzar al mecanismo optimizado a revisar mayores elementos evita que se anulen sitios Web cuyo tratamiento a priori puede ser equivocado.

4.- A medida que se incrementan los esfuerzos por descubrir características maliciosas reveladas u ocultas, se aumenta sistemáticamente la complejidad de los procesos inherentes al análisis. Por lo cual, la eficiencia de un mecanismo de protección está determinado más por el desempeño que por el rendimiento. Por ende, garantizar robustez, solidez, consistencia e integridad en la coexistencia de funciones originales, adaptadas y adecuadas para la detección y corrección de nuevas característica maliciosas, y que simultáneamente impone el desarrollo de nuevas funciones propias de la optimización, derivó en un mecanismo mucho más completo y complicado que el de Ponne (2012), evidenciando una desaceleración de los TPN y TPD globales.

5.- A medida que los ataques evolucionan, ocasionan daños de dimensiones y magnitudes importantes a la seguridad de los navegadores. Por lo cual, los procesos para corregir las averías ocasionadas a condiciones donde el navegador IE v6.0 se comportó consistentemente son cada vez más complejas y difíciles de realizar integralmente satisfaciendo patrones en los TPN que sean eficientes. Por ello, condicionar los procesos de seguridad a la velocidad, deteriora la eficiencia global de los mecanismos de seguridad.

6.- La seguridad en la navegación de sitios Web no es una responsabilidad absoluta de la tecnología. Muchas veces los usuarios abusando del exceso de confianza implícito en las herramientas de seguridad, descuidan procesos de actualización de los programas de seguridad, elevando los riesgos, ya que, experimentan una "falsa sensación de seguridad". En consecuencia, dejar de usar el IE v6.0, puesto que, ha sido desincorporado, sin soporte de parte del fabricante Microsoft. Es un paso importante para disminuir las vulnerabilidades de aquellos quienes aún insisten en realizar transacciones Web usando dicho navegador.

7.- Finalmente, ninguna tecnología es 100% segura y la garantía de la seguridad integral eficiente impone que los usuarios finales asuman posiciones críticas y protagónicas donde se deje de subestimar las amenazas y se deje de sobreestimar herramientas de seguridad que han mostrado ser vulnerables a la fecha.

Referencias

AIKATERINAKI, Niki (2009). Drive-By Download Attacks: Effects And Detection Methods. (Documento en línea). Disponible: http://goo.gl/hQQeS7 [consulta: 2012, septiembre 13].

ALEXA (2012). Lista de URLs Asociada a Páginas Legítimas. (Documento en línea). Disponible: http://goo.gl/0e1iaf [consulta: 2012, noviembre 01].

BIELOVA, Nataliia (2012). Survey on JavaScript Security Policies and their Enforcement Mechanisms in a Web Browser. (Documento en línea). Disponible: http://goo.gl/GttuIF [consulta: 2012, marzo 03].

CASTILLO, Sergio; MÚRCIA, José; GARCÍA, Joaquin (2010). El Spyware como amenaza contra navegadores Web. (Documento En línea). Disponible: http://goo.gl/YeQ8TR [consulta: 2010, octubre 10].

CHOI, YoungHan; KIM, TaeGhyoon; CHOI, SeokJin (2010). Automatic Detection for Javascript Obfuscation Attacks in Web Pages through String Pattern Analysis. (Documento en línea). Disponible: http://goo.gl/xQdSZP [consulta: 2013, marzo 30].

DEWALD, Andreas; HOLZ, Thorsten; FREILING, Felix (2010). ADSandbox: Sandboxing Javascript to fight Malicious Websites. (Documento en línea). Disponible: http://goo.gl/M9V5wW [consulta: 2012, marzo, 21].

DOUGHERTY, Chad (2012). Practical Identification of SQL Injection Vulnerabilities. (Documento en

línea). Disponible: https://goo.gl/wrleUc [consulta: 2013, febrero 27].

FOREST, Damien; CHOO, Christopher; KNG, Vicent; HO Siang (2010). National University of Singapore. HoneySift: A fast approach for low interaction client based Honeypot. (Documento en línea). Disponible: http://goo.gl/4jfL82 [consulta: 2013, abril 05].

HERNÁNDEZ, Roberto; FERNÁNDEZ, Carlos; BAPTISTA, Pilar (2012). Metodología de la investigación. (Documento en línea). Disponible: http://goo.gl/KIjtz1 [consulta: 2011, marzo 03].

JARAUTA, Javier; SIERRA, José; PALACIOS, Rafael (2006). Análisis de Riesgos. (Documento en línea). Disponible: http://goo.gl/AB3Lok [consulta: 2012, abril 07].

MCAFEE (2010). Mapping the Mal Web. The world's riskiest domains mcafree. (Documento en línea). Disponible: http://goo.gl/XB0lAl [consulta: 2012, febrero 10].

MALWAREDOMAIN (2012). Lista de URLs Asociada a Spyware. (Documento en línea). Disponible: http://goo.gl/lZsuru [consulta: 2012, noviembre 01].

MICROSOFT (2013). Microsoft Security Intelligence Report. Volumen 16 – July throught Decembre, 2013. (Documento en línea). Disponible: http://goo.gl/kBpcPL [consulta: 2014, julio 16].

MICROSOFT (2012). Internet Explorer 6 Service Pack 1 – Español. (Documento en línea). Disponible: http://goo.gl/zE3mQx [consulta: 2012, noviembre 24].

MSDN MICROSOFT (2004). Browser Helper Objects: The Browser the Way You Want It. (Documento en línea). Disponible: http://goo.gl/LkgSHN [consulta: 2012, mayo 17].

NORTON (2010). Malware Removal Guide. (Documento en línea). Disponible: http://goo.gl/mkd9vD [consulta: 2013, mayo 13].

OLDAPPS (2012). Versiones Antiguas de Internet Explorer 6.0 (Full Istaller). (Documento en línea). Disponible: http://goo.gl/9Hy1MF [consulta: 2012, noviembre 24].

PCTOOLS (2012). Software antiSpyware. (Documento en línea). Disponible: http://goo.gl/8h86UY [consulta: 2012, agosto 19].

PONNE, Jhogel (2012). Mecanismo de Seguridad Activo en Navegadores Web para Protección de Ataques tipo Spyware. (Documento en línea). Disponible: http://goo.gl/MWmlhc [consulta: 2013, mayo 15].

PROCESS MONITOR (2012). Herramienta de Monitoreo. (Documento en línea). Disponible: http://goo.gl/hRHc01. [Consulta: 2012, Agosto 14].

PUSHPENDRA, Kumar; SRIJITH, Kumar (2012). Analysis on Man in the Middle Attack on SSL. (Documento en línea). Disponible: http://goo.gl/LCSSjC [consulta: 2013, febrero 05].

STAMMINGER, Andreas; KRUEGEL, Christopher; VIGNA, Giovanni; KIRDA, Engin (2009). Automated Spyware Collection and Analysis. (Documento en línea). Disponible: http://goo.gl/UG4hF7 [consulta: 2012, abril 15].

SENN, James (2001). **Análisis y Diseño de Sistemas de Información**. Segunda Edición. Editorial McGraw-Hill. México.

SEIFERT, Christian; WELCH, Ian; KOMISARCZUK, Peter (2008). Identification of Malicious Web Pages with Static Heuristics. (Documento en línea). Disponible: http://goo.gl/IeHaCM [consulta: 2012, marzo 18].

UPEL (2010). Proyectos Factibles. (Documento en línea). Disponible: http://goo.gl/rTrsTp [consulta: 2012, febrero, 24].

WIRESHARK (2012). Analizador de Protocolos de Red. (Documento en línea). Disponible: http://goo.gl/9NjASA [consulta: 2012, agosto 17].

W3SCHOOLS (2014). Browser Statistics. (Documento en línea). Disponible: http://goo.gl/eWi0Az [consulta: 2014, julio 14].

UNIVERSIDAD
DEL ZULIA

Multiciencias

Vol 15, Nº 3

Edición por el ***Fondo Editorial Serbiluz.***
Publicada en septiembre de 2015.
Universidad del Zulia. Maracaibo-Venezuela

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