



**SEGURIDAD DEL EXPLORADOR WEB
PROTECCIÓN CONTRA MALWARE DE INGENIERÍA SOCIALMENTE
RESULTADOS DE LAS PRUEBAS COMPARATIVAS
2ª EDICIÓN**



**APPLE SAFARI 4
GOOGLE CHROME 2
MICROSOFT WINDOWS INTERNET EXPLORER 8
MOZILLA FIREFOX 3
OPERA 10 BETA**

**VERSIÓN DE LA METODOLOGÍA: 1.2
JULIO 20, 2009**

Publicado por NSS

Labs. © 2009 NSS Labs

CONTACTO:

P.O. Box 130573
Carlsbad, CA 92013

Tel. +1.512.961.5300
Correo electrónico: info@nsslabs.com
Internet: <http://www.nsslabs.com>

Todos los derechos reservados. Ninguna parte de esta publicación se puede reproducir, fotocopiar, almacenar en un sistema de recuperación o transmitir sin el consentimiento expreso por escrito de los autores.

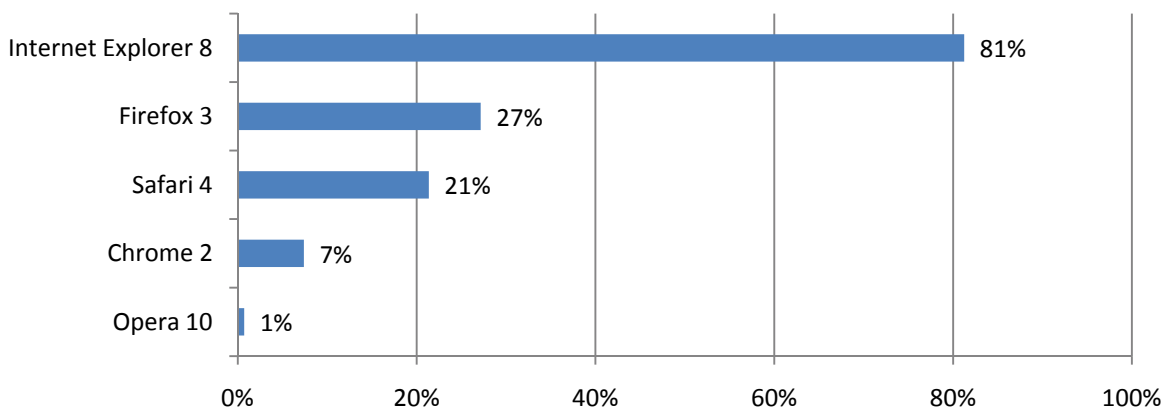
Por favor observe que el acceso o uso a este Informe está condicionado a lo siguiente:

1. La información en este Informe está sujeta a cambio por parte de NSS Labs sin previo aviso.
2. NSS Labs considera que la información en este informe es precisa y confiable, pero esto no se garantiza. Todo uso y dependencia de este Informe son bajo su exclusivo riesgo. NSS Labs no está obligada ni es responsable por cualquier daño, pérdida o gasto que surja por cualquier error u omisión en este informe.
3. NO SE OTORGAN GARANTÍAS, EXPRESAS O IMPLÍCITAS, POR NSS LABS. NSS LABS POR ESTE ACTO RENUNCIA Y EXCLUYE TODAS LAS GARANTÍAS IMPLÍCITAS, INCLUYENDO GARANTÍAS IMPLÍCITAS DE COMERCIALIZACIÓN, ADECUACIÓN PARA UN PROPÓSITO PARTICULAR Y NO INFRACCIÓN. EN NINGÚN CASO NSS LABS SERÁ RESPONSABLE POR CUALQUIER DAÑO CONSECUENCIA, INCIDENTAL O INDIRECTO, NI POR CUALQUIER PÉRDIDA DE INGRESOS, GANANCIAS, DATOS, PROGRAMAS DE CÓMPUTO U OTROS ACTIVOS, INCLUSO SI SE LES ADVIERTE LA POSIBILIDAD DE ELLO.
4. Este Informe no constituye un respaldo, recomendación o garantía de cualquiera de los productos (hardware o software) probados, ni del hardware y software utilizado en las pruebas de los productos. Las pruebas no garantizan que no existan errores o defectos en los productos, o que los productos cubrirán sus expectativas, requerimientos, necesidades o especificaciones, ni que funcionarán sin interrupción.
6. Todas las marcas registradas, marcas de servicio y nombres comerciales utilizados en este Informe son marcas registradas, marcas de servicio y nombres comerciales de sus respectivos propietarios y no se realiza respaldo, patrocinio, afiliación o implicación alguna en alguna de las pruebas en las que este Informe o NSS Labs esté implicado, ni esto se debe inferir.

RESUMEN EJECUTIVO

Durante julio de 2009 NSS Labs realizó la segunda prueba de la protección del explorador Web contra el malware de ingeniería social, la amenaza de seguridad más común e impactante que afrontan los usuarios de Internet actualmente.¹ Este informe siguió la misma metodología de Pruebas en Vivo que la prueba realizada en el primer trimestre de 2009, (consulte: www.nsslabs.com/browser-security). Ésta se basa en evidencia validada empíricamente recopilada durante 12 días de pruebas 24x7, realizadas cada 4 horas, sobre 69 corridas de prueba separadas, cada una agregando nuevos URLs de malware nuevos. Cada producto se actualizó con la versión más reciente disponible al momento de iniciar las pruebas y se permitió acceso a Internet en vivo.

Media del Índice de bloqueo para malware de ingeniería social



Internet Explorer 8 capturó 81% de las amenazas en vivo, un registro excepcional que sobrepasó el siguiente mejor explorador (Firefox 3) por un margen de 54%. Windows Internet Explorer 8 mejoró 12% entre las pruebas del primer trimestre y segundo trimestre, lo cual es evidencia de los esfuerzos concentrados que Microsoft está realizando en la tecnología SmartScreen.

Firefox 3 capturó 27% de las amenazas en vivo, bastante más bajo que Internet Explorer 8. Sin embargo, éste fue el mejor entre los productos que utilizan la API SafeBrowsing de Google. (Nota: Firefox 3.5 no era lo suficientemente estable para ser probado durante el curso de esta prueba. Posteriormente estuvo disponible una revisión para resolver el problema de estabilidad. Pudimos verificar manualmente que la protección era idéntica entre las versiones 3.0.11 y 3.5).

Safari 4 capturó 21% de las amenazas en vivo. La protección general varió enormemente, con dos cortos periodos de caídas severas.

Chrome 2 capturó apenas 7% de las amenazas en vivo, un descenso de 8% desde la prueba anterior.

Opera 10 Beta capturó solamente 1% de las amenazas en vivo y prácticamente no aporta protección contra el malware de ingeniería social. En nuestra validación de cama de prueba, verificamos que efectivamente no hay diferencia entre Opera 9 y Opera 10 Beta.

¹ Nota: Este estudio no compara la seguridad del explorador relacionada con vulnerabilidades en complementos o en los exploradores mismos.

CONTENIDO

1	<i>Introducción</i>	1
1.1	La amenaza de malware de ingeniería social	1
1.2	Seguridad del explorador Web	1
2	<i>Resultados sobre la efectividad</i>	2
2.1	Composición de la prueba – URLs maliciosos	2
2.2	Bloqueo de URLs con malware de ingeniería social	3
2.3	Bloqueo de URLs con malware de ingeniería social Over Time	4
2.4	Productos de SAFEBROWSING	5
2.5	Cambios inter pruebas	6
3	<i>Conclusiones</i>	7
4	<i>Apéndice A: Ambiente de las pruebas</i>	8
4.1	Descripción del Host cliente	8
4.2	Descripción de la operación en red	9
5	<i>Apéndice B: Procedimientos de las pruebas</i>	10
5.1	Duración de las pruebas	10
5.2	Conjuntos de muestra para URLs de malware	11
5.3	URLs de catálogos	11
5.4	Confirmar la presencia de muestras de URLs	11
5.5	Ejecutar dinámicamente cada URL	12
5.6	Reducción	12
5.7	Validación posterior a las pruebas	12
6	<i>Apéndice C: Infraestructura de las pruebas</i>	13

1 INTRODUCCIÓN

1.1 LA AMENAZA DE MALWARE DE INGENIERÍA SOCIAL

Los ataques del malware de ingeniería social plantean un riesgo significativo para los individuos y organizaciones por igual pues amenazan con comprometer, dañar o adquirir información confidencial, personal y corporativa. Las estadísticas de 2008 y 2009 muestran una aceleración de la tendencia. Detectar y evitar estas amenazas continúa siendo un desafío a medida que los delincuentes siguen siendo muy agresivos. Los investigadores de antivirus informan que han detectado entre 15,000 y 50,000 programas maliciosos nuevos por día, e incluso mencionan una cifra tan alta como “millones por mes”, conforme a Kaspersky.²

Aunque no todos estos programas maliciosos se utilizan en ataques de ingeniería social, esta técnica se está aplicando crecientemente al Web para distribuir rápidamente el malware y evadir los programas de seguridad tradicionales. Actualmente, el 53% del malware se suministra a través de descargas de Internet versus apenas 12% a través de correo electrónico, mientras IFrame explota y otras vulnerabilidades comprenden 7% y 5%, respectivamente, de los vectores de infección de malware globales, conforme a las estadísticas de Trend Micro.³ Además, una cifra cercana a 0.5% de las solicitudes de descarga realizadas a través de Internet Explorer 8 son maliciosas, conforme a Microsoft.⁴

Los delincuentes están aprovechando las relaciones de confianza implícita inherentes en los sitios de redes sociales (por ejemplo, Facebook, MySpace, LinkedIn, etc.) y el contenido aportado por los usuarios (por ejemplo, blogs, Twitter, etc.) que permiten la rápida publicación y anonimato. Del mismo modo, la velocidad a la cual estas amenazas ‘giran’ a nuevas ubicaciones, es asombrosa y plantea un importante desafío para los proveedores de seguridad.

Para más claridad, la siguiente definición se utiliza para un URL de malware de ingeniería social: **un vínculo de página Web que dirige directamente a una ‘descarga’ que suministra una carga útil maliciosa cuyo tipo de contenido podría causar su ejecución.** Éstos son vínculos que parecen seguros, como una aplicación de protector de pantalla, una actualización codec de video, etc., pero se han diseñado para engañar al usuario y lograr que los descargue. Los profesionales de seguridad también se refieren a estas amenazas usando distintos términos, tales como descargas concensuales o peligrosas.

1.2 SEGURIDAD DEL EXPLORADOR WEB

Los modernos exploradores Web ofrecen una capa de protección adicional contra estas amenazas al aprovechar los mecanismos en la nube, basados en reputación, para advertir a los usuarios. Este informe examina la capacidad de cinco diferentes exploradores Web para proteger a los usuarios contra el malware de ingeniería social.⁵ Cada uno de los cinco exploradores Web tiene tecnologías de seguridad agregadas para combatir las amenazas basadas en el Web. Sin embargo, no todos ellos tienen el mismo enfoque ni reivindicar detener la misma profundidad de ataques.⁶

² Kaspersky, Eugene en <http://www.examiner.com/x-11905-SF-Cybercrime-Examiner~y2009m7d17-Antimalware-expert-and-CEO-Eugene-Kaspersky-talks-about-cybercrime>

³ Cruz, Macky “Most Abused Infection Vector”. *Trend Labs Malware Blog*, 7 Dic 2008. <http://blog.trendmicro.com/most-abused-infection-vector/>

⁴ <http://blogs.msdn.com/ie/archive/2009/03/25/ie8-security-part-ix-anti-malware-protection-with-ie8-s-smartscreen-filter.aspx>

⁵ Explosiones que instalan malware sin que el usuario esté consciente (también conocidos como “clickjacking” y “descargas drive-by”) y no se incluyen en este estudio en particular.

La protección del explorador contiene dos componentes funcionales básicos. El fundamento es un sistema en la nube basado en la reputación que registra en Internet en busca de sitios Web maliciosos y clasifica el contenido de manera acorde; ya sea que los agregue a una lista negra o blanca, o les asigne una calificación (dependiendo del enfoque del proveedor). Esto se puede realizar de forma manual, automática, o alguna combinación de ambas. El segundo componente funcional reside dentro del explorador Web y solicita información sobre la reputación por parte de los sistemas en la nube acerca de URLs específicos y después refuerza las funciones de advertencia y bloqueo.

Cuando los resultados informan que un sitio es “malo”, el explorador Web redirecciona al usuario a un mensaje/página de advertencia para indicar que el URL es malicioso. En el caso de que el URL sea una descarga, el explorador Web indica al usuario que el contenido que está a punto de descargar (o está descargando) es malicioso y que la descarga se debe abortar/cancelar. Por el contrario, cuando un sitio Web se determina como “bueno”, el explorador Web no realiza acción alguna y el usuario no tiene conocimiento que se realizó una verificación de seguridad por parte del explorador.

2 RESULTADOS SOBRE LA EFECTIVIDAD

2.1 COMPOSICIÓN DE LA PRUEBA – URLs MALICIOSOS

Los datos en este informe abarcan un periodo de pruebas de 12 días, desde el 7 de julio hasta el 18 de julio de 2009. Todas las pruebas se realizaron en nuestro laboratorio en Austin, TX. Durante el curso de las pruebas monitoreamos rutinariamente la conectividad para confirmar que los exploradores pudieran acceder a los sitios de Internet en vivo que estaban bajo prueba, así como a sus servicios de reputación en la nube. Durante el curso de este estudio, se realizaron 69 pruebas separadas (cada 4 horas) sin interrupción para cada uno de los 5 exploradores.

El énfasis se colocó sobre la novedad, por lo tanto, se evaluó un número de sitios más grande de la cifra que se conservó finalmente como parte del conjunto de resultados. Consulte la metodología para obtener más detalles.

2.1.1 NÚMERO TOTAL DE URLs MALICIOSOS EN LA PRUEBA

A partir de una lista inicial de 12,000 nuevos sitios sospechosos, 2,171 URLs potencialmente maliciosos se pre-investigaron para su inclusión en la prueba y estuvieron disponibles al momento de ingresar a la prueba. Los exploradores pudieron acceder exitosamente a éstos al menos en una ejecución. Retiramos las muestras que no pasaron nuestros criterios de validación, incluyendo aquellos contaminados por explosiones o que contenían muestras inválidas. De los 2,171 URLs iniciales, finalmente 608 URLs pasaron nuestro proceso de post-validación y se incluyeron en los resultados finales, aportando un margen de error de 3.91% con un intervalo de confianza de 95%.

2.1.2 NÚMERO PROMEDIO DE URLs MALICIOSOS AÑADIDOS POR DÍA

Un promedio de 197 nuevos URLs validados se añadieron al conjunto de pruebas por día. Aunque ciertos días se añadieron más o menos a medida que fluctuaban los niveles de actividad delictiva.

⁶ La protección contra la suplantación de identidad se probó separadamente por razones técnicas y está disponible en un informe acompañante.

2.1.3 MEZCLA DE URLs

La mezcla de URLs usada para las pruebas fue representativa de las amenazas en el Internet. Se tuvo cuidado de no sobrecargar ningún dominio para que no representara más del 10% del conjunto de la prueba. Así, un número de sitios fue retirado después de alcanzar su límite.

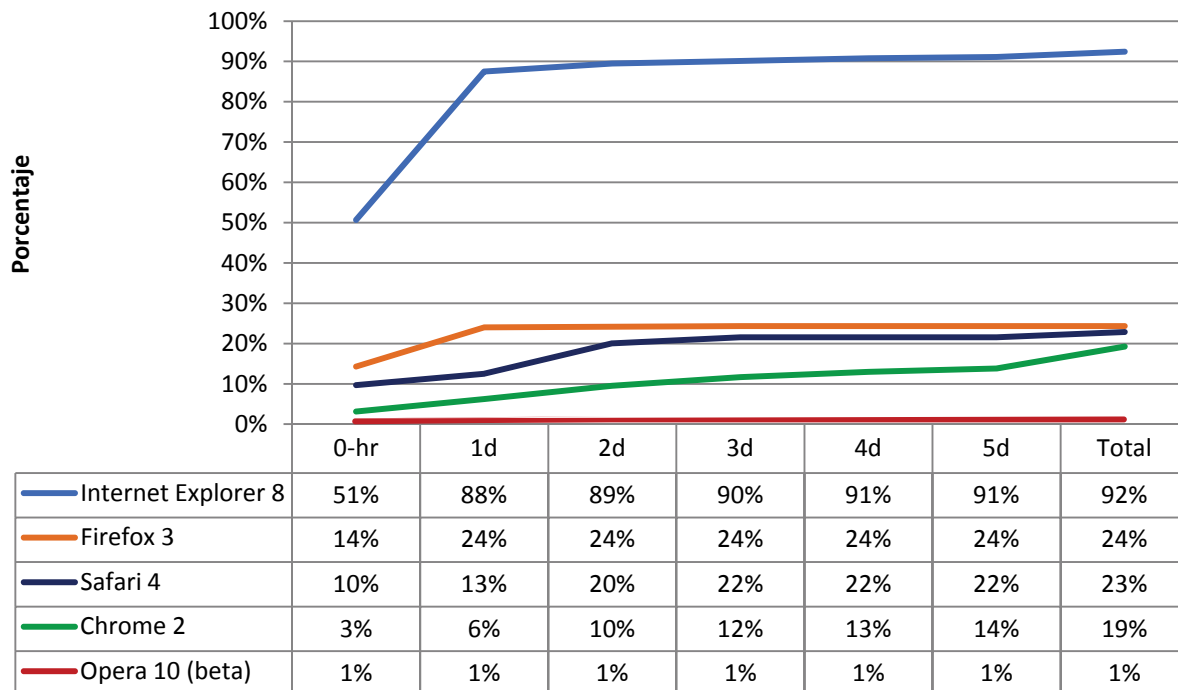
2.2 BLOQUEO DE URLs CON MALWARE DE INGENIERÍA SOCIAL

NSS Labs evaluó la capacidad de los exploradores para bloquear URLs maliciosos tan rápidamente como los encontraban en el Internet. Continuamos probándolos cada cuatro horas para determinar cuánto tiempo requería un proveedor para agregar protección, en caso de que lo hicieran.

2.2.1 TIEMPO PROMEDIO PARA BLOQUEAR SITIOS MALICIOSOS

La siguiente gráfica del tiempo de respuesta muestra cuánto tiempo requirieron los exploradores bajo prueba para bloquear la amenaza una vez que ésta se introdujo dentro del ciclo de prueba. Los índices de protección acumulados se enumeran para la 'hora cero', y después en los primeros 5 días. Las calificaciones de protección final para la duración de la prueba del URL se resumen bajo la columna "Total". En general, al menos la mitad de la protección total de un explorador se logró en la hora cero. Sin embargo, Internet Explorer 8 continuó agregando tanto como 41% de protección adicional durante el curso de la prueba. Otros exploradores agregaron apenas entre 0% y 16% durante el curso de la prueba.

Histograma de respuesta al URL de malware



Finalmente, los resultados revelan grandes variaciones en las capacidades de los exploradores para proteger contra el malware de ingeniería social, con Internet Explorer 8 que protege a los usuarios contra 68% más URLs maliciosos únicos que su competidor más cercano, Firefox 3. Las tendencias muestran que Chrome 2,

Safari 4 y Firefox 3 convergen todos en un índice de protección apenas por debajo de 25%, indicador de que no obstante que comparten la misma fuente de SafeBrowser de Google, existe una diferencia operativa en su implementación.

2.2.2 PROMEDIO DEL TIEMPO DE RESPUESTA PARA BLOQUEAR MALWARE

Con objeto de proteger a la mayoría de la gente, un sistema de reputación de un explorador debe ser tanto rápido como preciso. Esta tabla responde la pregunta: ¿cuánto tiempo en promedio debe esperar un usuario antes de visitar un sitio malicioso si éste se agregó a la lista de bloqueo? La tabla muestra el tiempo promedio para bloquear un sitio de malware una vez que éste se introdujo en el conjunto de prueba, pero *únicamente si éste fue bloqueado durante el curso de la prueba*. Los sitios no bloqueados no se incluyeron, debido a que no hay una forma matemáticamente empírica de clasificar “nunca”. Por lo tanto, aunque Opera 10 Beta registró el tiempo de bloqueo más rápido, no se puede suponer por ello que bloqueó más malware. De hecho, bloqueó la menor cantidad de todos los exploradores.

El valor de esta tabla consiste en proporcionar un contexto para el *índice de bloqueo general*, de tal forma que si un explorador bloqueó 100% del malware, pero requirió 240 horas (10 días) para hacerlo, éste realmente proporciona menos protección que un explorador con un índice de bloqueo general de 70% pero un promedio de tiempo de respuesta de 10 horas.

Explorador:	Promedio de tiempo agregado
Opera 10 Beta	5.5
Firefox 3	6.7
Internet Explorer 8	9.2
Safari 4	31.5
Chrome 2	76.8
<i>media</i>	25.9

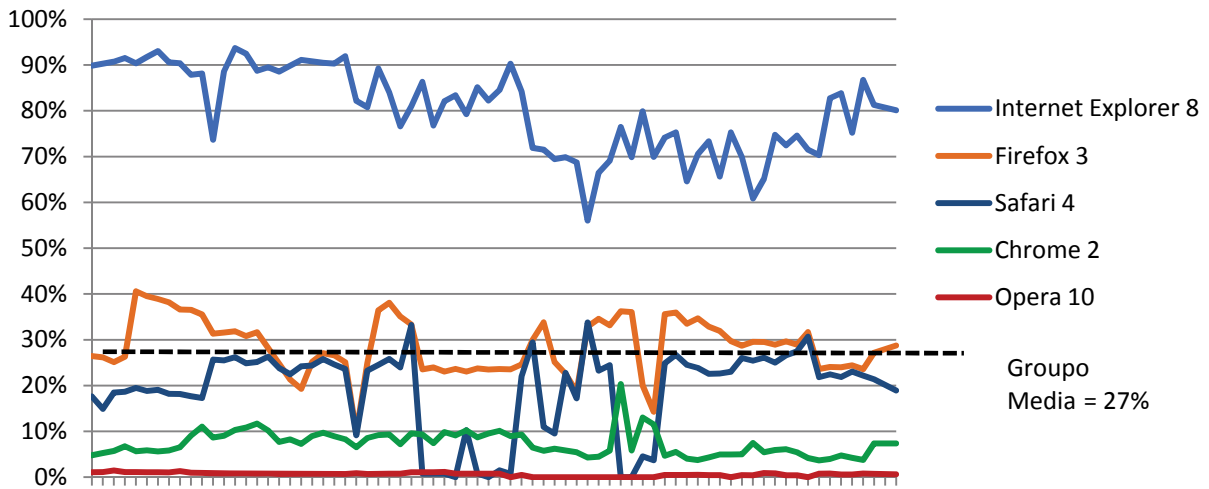
La media de tiempo para bloquear un sitio (si éste está bloqueado del todo) es de 25.9 horas. Por lo tanto, Opera, Firefox e Internet Explorer se encuentran por encima del promedio al agregar nuevos bloqueos.

2.3 BLOQUEO DE URLS CON MALWARE DE INGENIERÍA SOCIAL CON EL TIEMPO

Las métricas para bloquear URLs individuales representan sólo una perspectiva. Cuando se trata de los escenarios de uso diario, los usuarios están visitando una gran variedad de sitios que pueden cambiar rápidamente. Por lo tanto, en un periodo determinado, el conjunto disponible de URLs maliciosos es revolvente y continuar el bloqueo de estos sitios es un criterio esencial para la efectividad. Así pues, NSS Labs probaron un conjunto de URLs en vivo cada cuatro horas. Las siguientes tablas y gráficas muestran las evaluaciones repetidas del bloqueo durante el curso de 12 días, 69 ciclos de prueba para cada uno de los cinco exploradores. Cada clasificación representa la protección en un punto de tiempo determinado.

Como se muestra en la gráfica, Internet Explorer 8 demostró un nivel de protección muy alto, pero cayó en la segunda mitad de la prueba y después mostró signos de recuperación cerca del final. Safari fue muy inconsistente, con dos cortos periodos de graves caídas en la protección. Firefox tuvo un rango entre 20% y 40%.

Protección contra malware de ingeniería social durante el tiempo

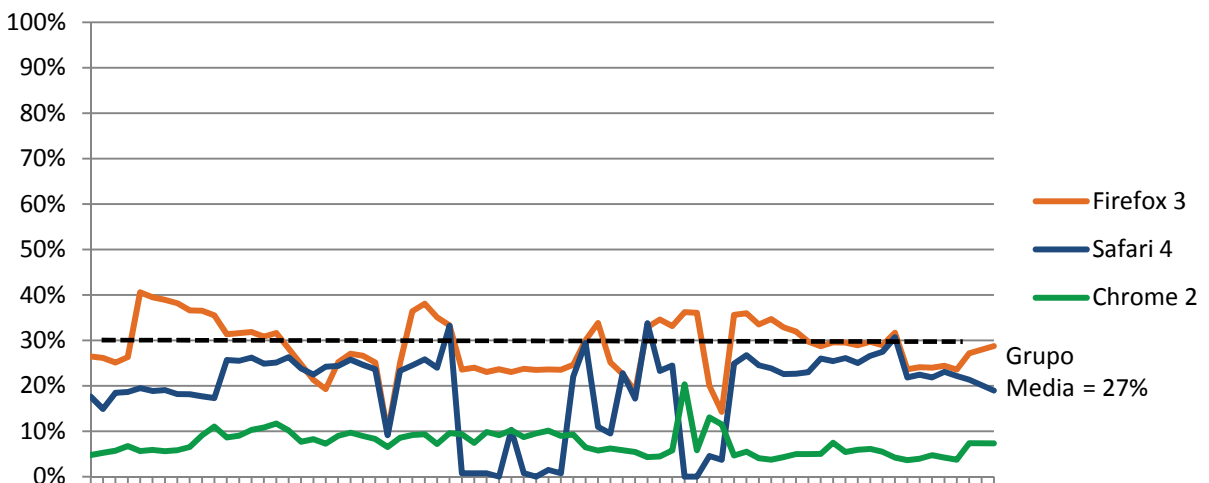


Observe que el porcentaje de protección promedio se desvía de los resultados de URL únicos por diversas razones. Primero, estos datos incluyen diversas pruebas de un URL. Así pues, si éste se bloqueó temprano, esto mejorará la clasificación. Si éste continúa siendo omitido, esto deteriorará la clasificación. Así pues, los resultados de las pruebas de URL individuales se conformaron con el tiempo.

2.4 PRODUCTOS DE SAFE BROWSING

No obstante que Chrome, Firefox y Safari utilizan todos la alimentación de datos Safe Browsing de Google , nuestras pruebas detectaron resultados muy distintos en términos de efectividad para bloquear los URLs de malware de ingeniería social.

Protección contra malware de ingeniería social durante el tiempo - Productos de SafeBrowsing



Pueden existir diversas explicaciones para esta variación, pero los desarrolladores no proporcionaron explicación alguna. Sin embargo, sabemos que cada explorador tiene contacto directamente con el sitio del desarrollador respectivo y éste es el único punto en el canal de comunicación en donde se pueden tomar decisiones adicionales.

Fundamentalmente, cada explorador o servidor intermediario puede implementar la API de forma distinta; lo puede invocar en distintos momentos con diferentes parámetros y determinar los bloqueos de manera distinta. Además, como un proyecto de fuente abierta, la implementación de Mozilla utiliza una estructura de base de datos y un método de acceso diferentes a los otros dos exploradores propietarios. Por último, como se mencionó en la Sección 2.2.1 y se indicó en el Histograma de respuesta al URL de malware, los índices de protección de los Productos de SafeBrowsing demostraron signos de converger justo debajo de 25%. Esto respalda la noción de que existen diferencias operativas entre las implementaciones de la API, pero que las listas de bloqueo son las mismas (o muy similares).

2.5 CAMBIOS INTER PRUEBAS

Debido a que utilizamos la misma metodología de pruebas tanto en las pruebas de febrero como de julio de 2009, esto nos permite una fácil comparación de manzanas con manzanas sobre los cambios de rendimiento con el tiempo. Como se demuestra en la siguiente tabla, Internet Explorer 8 aumentó su protección en 12%, una ganancia considerable sobre un 69% que ya era fuerte en la prueba anterior.

	febrero 09	julio 09	Cambio	Internet Explorer Comparado	Firefox Comparado
Internet Explorer 8	69%	81%	12%		-54%
Firefox 3	30%	27%	-3%	54%	
Safari 4	24%	21%	-3%	60%	6%
Chrome 2	16%	8%	-8%	74%	20%
Opera 10 Beta	5%	1%	-4%	80%	27%

Todos los otros exploradores disminuyeron su protección entre 3% y 8%, dentro del margen de error. Las columnas de la extrema izquierda indican cuánto mejor (o peor) se compararon Internet Explorer 8 y Firefox 3 contra las clasificaciones de los otros exploradores.

Entre la prueba anterior y ésta, todas las versiones de explorador se actualizaron al código más reciente disponible. Internet Explorer 8 se actualizó desde un código Release Candidate (RC) a Generally Available (GA). Firefox 3.07 se actualizó a 3.0.11. Safari se actualizó de v3 a v4. Chrome se actualizó de v1.0.154 a v2.0.172.39 Opera se actualizó de v9.64 a v10 beta.

3 CONCLUSIONES

El uso de sistemas de reputación para ayudar a los exploradores en su lucha contra el malware de ingeniería social es un sólido uso de las tecnologías de nube. Sin embargo, no todas las implementaciones de proveedores ni las operaciones diarias rinden los mismos resultados.

A partir de esta prueba y las comparaciones con pruebas anteriores, fue evidente que Microsoft continúa haciendo considerables mejoras para añadir protección contra el malware de ingeniería social en **Internet Explorer 8** (tecnología de filtro SmartScreen). Con una clasificación de bloqueo URL única de 92% y una clasificación de protección con el tiempo de 81%, Internet Explorer 8 fue ampliamente el mejor en la protección contra el malware de ingeniería social. El aumento de 41% desde la hora cero hasta los 5 días de bloqueo sugiere un mecanismo de retroalimentación muy superior.

En un distante segundo lugar, **Firefox 3** logró una clasificación de 27% de protección contra malware, 54% menos protección que Internet Explorer 8. La clasificación de URL única de Firefox fue también significativamente más baja, en 24%.

Safari 4 capturó 23% de los URLs únicos y sólo 21% de los sitios de malware disponibles durante nuestra prueba con el tiempo. Esto representó una reducción de 3% comparada con la prueba del trimestre anterior. Además, la protección varió enormemente, con dos cortos periodos de graves caídas.

A diferencia de la prueba anterior en la cual se observaron problemas operativos, **Chrome 2** se ejecutó muy consistentemente, aunque de forma deficiente. Chrome 2 perdió la mayoría del terreno comparado con Internet Explorer 8 durante las dos pruebas, al declinar 8% y bloquear 74% menos sitios maliciosos que el líder.

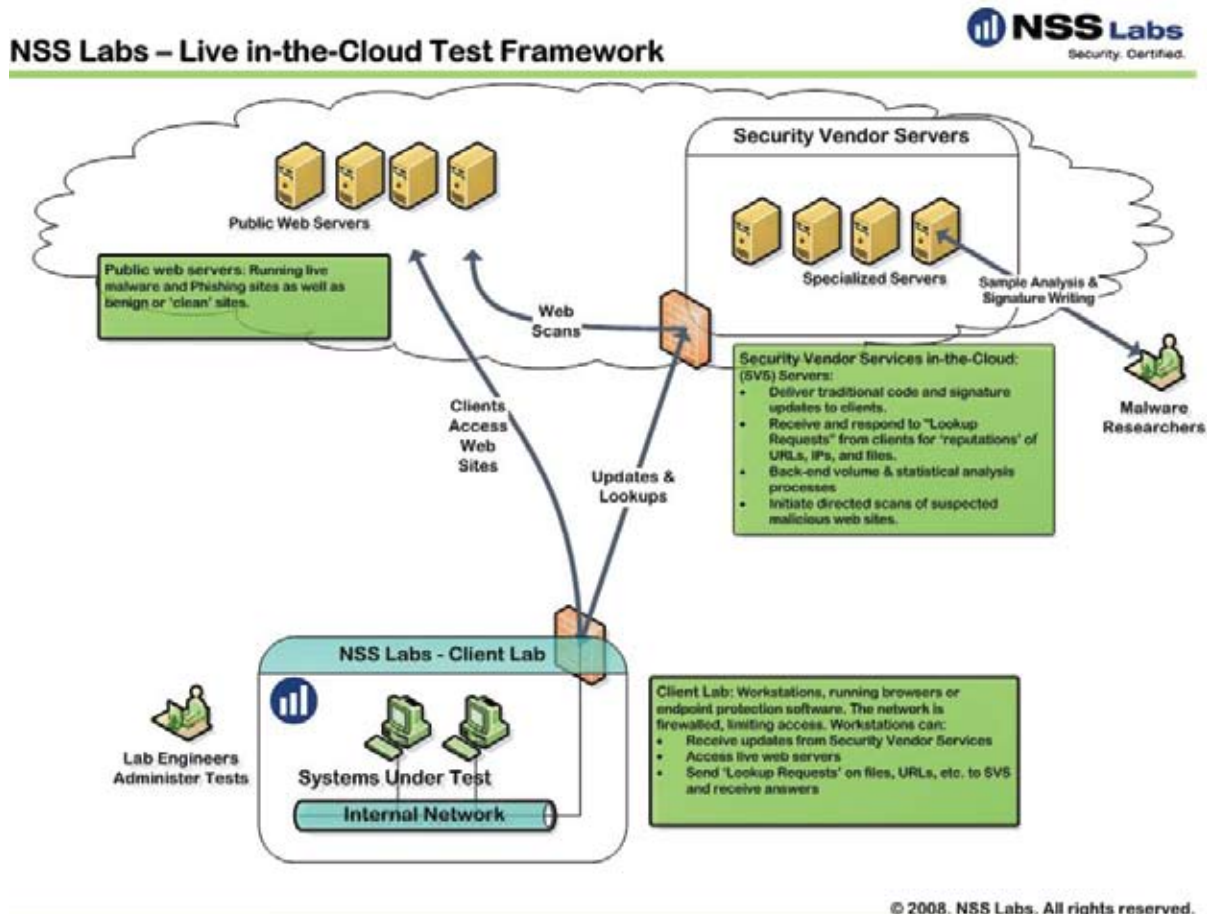
El índice de bloqueo general de **Opera 10** fue de 1% muy por debajo del margen de error. Para estar seguros, verificamos dos veces la configuración y verificamos manualmente una porción de URLs significativa, con el mismo resultado. Los usuarios no deben esperar protección alguna contra el malware de ingeniería social por parte de Opera 10 Beta.

Los exploradores proporcionan a los usuarios otra capa de protección gratuita contra el malware de ingeniería social, adicional a los productos de protección de punto final y esto no se debe considerar como un reemplazo para los programas antivirus. Espere las próximas pruebas de producción anti-malware por parte de NSS Labs en el tercer trimestre de 2009.

4 APÉNDICE A: AMBIENTE DE LAS PRUEBAS

NSS Labs creó un complejo ambiente de las pruebas y metodología para evaluar las capacidades protectoras de los exploradores de Internet bajo las condiciones más cercanas posibles al mundo real, al tiempo que mantenía el control y la verificación de los procedimientos.

Para esta prueba de seguridad del explorador, NSS Labs creó un ambiente de laboratorio de pruebas “en vivo” con objeto de duplicar las experiencias del usuario bajo condiciones del mundo real.



4.1 DESCRIPCIÓN DEL HOST CLIENTE

Todo el software de explorador probado se instaló en máquinas virtuales idénticas con las siguientes especificaciones:

- Microsoft Windows 7 RC (build 7100)
- 1 GB de RAM
- 8 GB HD

Las máquinas de explorador se probaron antes y durante las pruebas para asegurar su funcionamiento apropiado. Los exploradores tuvieron acceso completo a Internet de forma que podrían visitar los sitios reales en vivo.

4.2 LOS EXPLORADORES PROBADOS

Los exploradores, o productos bajo prueba, fueron obtenidos independientemente por NSS Labs. En todos los casos se utilizaron las versiones de software generalmente disponibles, excepto para Opera 10. Cada producto se actualizó a la versión más reciente disponible en el momento de iniciar las pruebas. La siguiente es una lista real de los exploradores Web que se probaron:

- Microsoft Windows Internet Explorer 8 (build 8.0.7100.0)
- Google Chrome v2.0.172.33
- Apple Safari v4.0.2 (530.19.1)
- Mozilla Firefox v3.0.11
- Opera 10 Beta – v10.00b1 (build 1551)

Una vez que empezaron las pruebas, se congeló la versión del producto con objeto de preservar la integridad de las pruebas. Estas pruebas dependieron del acceso a Internet para los sistemas de reputación y acceso al contenido en vivo. Generalmente, existe una separación configurable entre las actualizaciones de software y las actualizaciones de base de datos o firma, con objeto de extraer analogías por parte de los antivirus, IPS y prácticas de software generales.

4.3 DESCRIPCIÓN DE LA OPERACIÓN EN RED

Los exploradores se probaron en cuanto a su capacidad para proteger al cliente en casos de uso “conectado”. Por lo tanto, nuestras pruebas consideraron y analizar la efectividad de la Protección del explorador en un arnés de pruebas de Internet en vivo en el mundo real.

El sistema host tiene una tarjeta de interfaz de red (NIC) y se conectó a la red a través de un puerto conector de 1 GB. La operación en red de las pruebas de NSS Labs es una infraestructura de multi-Gigabit basada en torno a los conectores Cisco Catalyst Serie 6500 (con interfaces de Gigabit tanto de fibra como de cobre).

Para los propósitos de estas pruebas, NSS Labs utilizó hasta 84 sistemas de escritorio cada uno ejecutando un explorador Web, seis (14) por cada explorador Web (6 tipos de explorador). Los resultados se registraron en una base de datos MySQL DB.

5 APÉNDICE B: PROCEDIMIENTOS DE LAS PRUEBAS

El propósito de las pruebas fue determinar qué tan bien los exploradores Web probados protegen a los usuarios contra la mayoría de las amenazas de malware más importantes en el Internet actual. Un aspecto clave fue el tiempo. Debido a la rápida velocidad y agresividad con la cual los delincuentes propagan y manipulan los sitios Web maliciosos, un objetivo fundamental fue asegurar que los sitios “más frescos” posibles se incluyeran en las pruebas.

NSS Labs desarrolló un arnés de “Pruebas en vivo” y metodologías propietarios únicos. De manera continua, NSS Labs recopiló las amenazas basadas en Web desde diversas fuentes, incluyendo socios y nuestros propios servidores. Las amenazas potenciales se examinaron algorítmicamente antes de ser insertadas en nuestra cola de pruebas. Las amenazas se insertaron y se examinaron continuamente 24x7. Una observación exclusiva en este procedimiento, es que NSS Labs valida las muestras antes y después de las pruebas. Las pruebas reales de las amenazas se ejecutaron cada cuatro horas e iniciaron con la validación de la existencia del sitio y su conformidad con la definición de la prueba.

Todas las pruebas se ejecutaron de una manera altamente controlada y los resultados se registraron y archivaron meticulosamente en cada intervalo de las pruebas.

5.1 DURACIÓN DE LAS PRUEBAS

La prueba del Explorador de NSS Labs se realizó continuamente (24x7) durante 12 días. A lo largo de la duración de las pruebas, se agregaron nuevos URLs a medida que se descubrieron.

5.1.1 FRECUENCIA DE LAS PRUEBAS

Durante el curso de las pruebas, cada URL se ejecutó a través del arnés de pruebas cada cuatro horas, independientemente del éxito o falla y NSS Labs continuó intentando descargar una muestra de malware con el Explorador Web a lo largo de la duración de las pruebas.



5.2 CONJUNTOS DE MUESTRA PARA URLS DE MALWARE

La frescura de los sitios de malware es un atributo clave para este tipo de pruebas. Con objeto de utilizar la frescura de los URLs más representativos, NSS Labs recibe un amplio rango de muestras provenientes de diversas fuentes.

5.2.1 FUENTES

Primero, NSS Labs opera su propia red de trampas de spam y vasijas de miel. Estas cuentas de correo electrónico con tráfico de alto volumen, producen miles de correos electrónicos únicos y varios cientos de URLs únicos por día. El archivo de NSS Labs crece continuamente con Malware y virus que contienen Gigabytes de muestras confirmadas. Además, NSS Labs mantiene relaciones con otros investigadores de seguridad independientes, redes y compañías de seguridad que le proporcionan acceso a URLs y contenido malicioso. Los conjuntos de muestra contienen URLs maliciosos distribuidos a través de: SPAM, redes sociales y sitios Web maliciosos. Las explosiones que contienen cargas útiles de malware (explosiones + malware) es decir, “clickjacking” o “impulsado por descargas” se excluyeron de las pruebas. Se realizaron todos los esfuerzos para considerar envíos que reflejaran una distribución de malware como en el mundo real, categóricamente, geográficamente y por plataforma.

Además, NSS mantiene una colección de ‘URLs limpios’ que incluye sitios tales como Yahoo, Amazon, Microsoft, Google, NSS Labs, principales bancos, etc. Periódicamente se ejecutan los URLs limpios a través del sistema para verificar que los exploradores no estén sobrebloqueados.

5.3 URLS DE CATÁLOGOS

Los nuevos sitios se agregan al Conjunto de consideración de URL tan pronto como es posible. Se anota la fecha y hora en que cada muestra se introdujo. La mayoría de las fuentes se insertaron automática e inmediatamente, mientras que algunos métodos requieren un manejo manual y se pueden procesar en 30 minutos. Todos los artículos en el conjunto de consideración se catalogaron con un ID de NSS Labs único, independientemente de su validez. Esto nos permitió rastrear la efectividad de las fuentes de muestras.

5.4 CONFIRMAR LA PRESENCIA DE MUESTRAS DE URLS

El tiempo es fundamental debido a que el objetivo de las pruebas es examinar la efectividad contra los sitios de malware ‘más frescos’ posibles. Debido a la naturaleza de las alimentaciones y la velocidad del cambio, no es posible validar cada sitio a profundidad antes de las pruebas debido a que los sitios podrían desaparecer rápidamente. Por ello, a cada uno de los artículos bajo prueba se les da una revisión superficial para verificar que esté presente y accesible en Internet en vivo.

Con objeto de ser incluido en el Conjunto de ejecución, los URLs deben estar vivos durante la iteración de las pruebas. Al comenzar cada ciclo de prueba, se confirma la disponibilidad del URL asegurando que cada sitio se pueda alcanzar y esté activo (por ejemplo, una página Web distinta a 404 se devuelve).

La validación ocurre dentro de unos minutos después de recibir las muestras de nuestras fuentes. Nota: Estas clasificaciones se validan adicionalmente después de la prueba y los URLs se reclasifican y/o se eliminan acordemente.

5.4.1 ARCHIVAR EL CONTENIDO DEL URL ACTIVO

El contenido del URL activo se descarga y se guarda en un servidor de archivo con un número de ID NSS único. Esto permite que NSS Labs preserve el contenido del URL para propósitos de control y validación.

5.5 EJECUTAR DINÁMICAMENTE CADA URL

Una utilidad de automatización cliente solicita que cada uno de los URLs se considere ‘presente’ basado en los resultados de la prueba 5.4 a través de cada uno de los exploradores Web en la prueba. NSS registra si se permitió o no que el malware se descargara, y si la descarga intentó disparar una advertencia desde la protección contra malware del explorador.

5.5.1 CLASIFICAR Y REGISTRAR LOS RESULTADOS

La respuesta resultante se registra ya sea como “Permitida” o “Bloqueada y Advertida”.

- Pasó: NSS Labs define “pasó” con base en que un explorador Web evitó exitosamente que se descargara el malware y emitió correctamente una advertencia.
- Falló: NSS Labs define “falla” basado en que un explorador Web falló en evitar que el malware fuera descargado y falló en emitir una advertencia.

5.6 REDUCCIÓN

A lo largo de las pruebas, los ingenieros de laboratorio revisan y reducen los URLs y el contenido fuera de conformidad del conjunto de ejecución de las pruebas, por ejemplo, un URL que se clasificó como malware pero fue reemplazado por un host Web con una página splash genérica, es eliminado de las pruebas.

Si una muestra de URL deja de estar disponible para su descarga durante el curso de las pruebas, la muestra se elimina del conjunto de pruebas para dicha iteración. NSS Labs verifica continuamente la presencia de cada muestra (disponibilidad para descarga) y añade - elimina cada muestra del conjunto de pruebas acordemente. En caso de que una muestra de malware deje de estar disponible para la iteración de las pruebas y después vuelve a estar disponible para una iteración posterior, ésta se agregará de regreso a la colección de pruebas. Las muestras que no estén disponibles no se incluyen en los cálculos de éxito o fracaso de un explorador Web.

5.7 VALIDACIÓN POSTERIOR A LAS PRUEBAS

La validación posterior a las pruebas permite que NSS Labs reclasifique e incluso elimine muestras que o no eran maliciosas o no estaban disponibles antes de que las pruebas se iniciaran. NSS Labs utilizaron dos diferentes filtros de arena para reducir y validar el malware (CW Sandbox de Sunbelt y Norman Analyzer), además de validar después las muestras sospechosas utilizando diversos escáneres antivirus en caso necesario.

6 APÉNDICE C: INFRAESTRUCTURA DE LAS PRUEBAS

Nuestro agradecimiento especial para nuestros socios de la infraestructura de las pruebas que nos proporcionaron gran parte del equipo, software y soporte para hacer posibles estas pruebas:

