

Mapping the Mal Web

Los dominios de mayor riesgo del mundo





Mapping the Mal Web

Los dominios de mayor riesgo del mundo

Por:
Barbara Kay, CISSP, asegurado por Design Group
Paula Greve, Directora de investigación de McAfee Labs™

ÍNDICE

Introducción	3
Resultados clave: <i>Mapping the Mal Web IV</i>	4
¿Por qué es importante el Mapping?	6
¿Cómo se abusan los delincuentes de los dominios de mayor nivel?	7
Metodología	9
Algunas advertencias sobre las clasificaciones	11
Desglose de las calificaciones	12
El panorama de amenazas cambiante	21
Comentarios de los operadores y encargados de registrar los dominios de más alto nivel	23
Conclusión	26

Introducción

¿Bonanza o red de bots? La próxima vez que busque la foto de una celebridad o una pista sobre cómo hacer algo, preste atención a los dominios de mayor nivel (en inglés, Top-level domains, TLD), que son los últimos caracteres del final de la URL, en los resultados de la búsqueda. En el estudio Mapping the Mal Web de este año, McAfee descubrió que el riesgo de la Web alcanzó un récord de 6.2% de más de 27 millones de dominios en tiempo real evaluados para este informe. Si el usuario no hace clic con cuidado, el simple hecho de ver una página puede devolverle mucho más de lo esperado. Este año, más sitios web contienen códigos maliciosos que roban contraseñas e información de identidad, se aprovechan de los baches de seguridad en los navegadores o instalan de forma secreta los ingredientes que hacen que los equipos se conviertan en zombies.

Pensamos que si sabe de antemano que tres de cada cinco sitios en un TLD presentan riesgos, podrá elegir un lugar diferente para descargar esa fotografía que está buscando. Por ejemplo, a pesar del crecimiento de la popularidad de Vietnam como destino de vacaciones, los visitantes de los sitios registrados en

Vietnam (.VN) deben considerarlos como una zona “restringida para la navegación”. Este año, .VN se agregó a la lista dentro del grupo de los cinco TLD principales de más riesgos en Internet, puesto que el 58% de los sitios que rastreamos contenía actividades y contenido potencialmente peligroso o malicioso, entre otras cosas:

- **Malware:** código que puede dañar su sistema, robar datos o realizar actividades maliciosas en otros equipos (incluye registradores de pulsaciones, ladrones de contraseña y equipos zombies).
- **Aprovechamiento de los puntos débiles del navegador:** ataques y malware que se aprovechan del software vulnerable de su equipo.
- **Phishing:** sitios falsos que parecen ser legítimos, pero que están diseñados para la obtención fraudulenta de información (“phish”, en inglés) o para instalar códigos maliciosos.
- **Grado de spam:** formularios de inscripción que harán que una persona reciba grandes cantidades de correos electrónicos comerciales o spam.
- **Asociaciones riesgosas:** sitios con enlaces que llevan al usuario a sitios maliciosos y sitios con asociaciones sospechosas, como su sitio de propiedad, registro o servicio de host.

Amenazas de seguridad evaluadas por McAfee® Global Threat Intelligence™



Calculamos el nivel de riesgo según las formas en que se relacionan las distintas características con cada sitio web.

Los TLD .INFO y .CM tienen casi la misma cantidad de sitios riesgosos y seguros, mientras que los .VN tienen más sitios riesgosos que seguros.



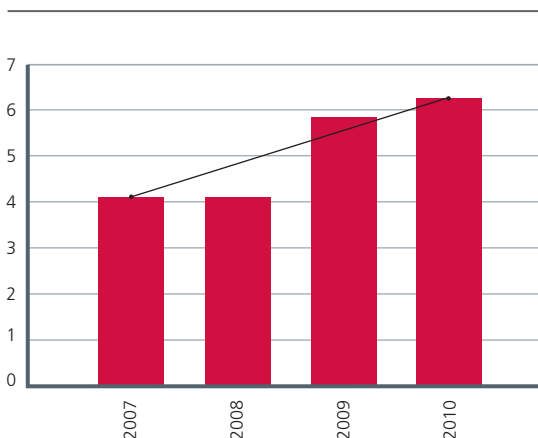
Resultados claves: *Mapping the Mal Web IV*

En este cuarto análisis anual de los riesgos relativos de los TLD, McAfee ha descubierto que el riesgo general de la Web es superior al del año pasado. Vimos mayores riesgos en algunas porciones de la Web que ya eran riesgosas, como .INFO; algunas reducciones de riesgo significativas dentro de los TLD más riesgosos del año pasado, especialmente Singapur (.SG) y Venezuela (.VE); y nuevas áreas de interés, como Vietnam (.VN), Armenia (.AM) y Polonia (.PL).

Nota: todas las estadísticas de riesgo se refieren a riesgos ponderados, a menos que se indique lo contrario.

- **Riesgo mayor:** el promedio general ponderado de sitios riesgosos aumentó de 5.8% (2009) a 6.2% (2010). En 2007 y 2008, encontramos un 4.1% de sitios web clasificados en rojo (evitar) o amarillo (usar con precaución). Aunque usamos una metodología diferente los dos primeros años, la línea de tendencia (hacia arriba y a la derecha) parece mantenerse. Navegar de forma segura por la Web es cada vez más dificultoso.

Porcentaje de sitios de riesgo en la Web



- **Los cinco TLD más riesgosos:** con un riesgo ponderado de 31.3%, el TLD .COM (Comercial; el TLD con mayor tráfico) fue el más riesgoso. Le quitó el título a .CM (Camerún), que cayó al cuarto lugar este año, mientras que .INFO se colocó en una posición más riesgosa: avanzó al segundo lugar desde el quinto lugar que ocupaba el año pasado. Los cinco TLD con mayor porcentaje de registros de riesgo fueron los siguientes:

- .COM (Comercial)	31.3%
- .INFO (Información)	30.7%
- .VN (Vietnam)	29.4%
- .CM (Camerún)	22.2%
- .AM (Armenia)	12.1%

- **Distribución mundial:** las regiones de Europa, Oriente Medio y África (EMEA) volvieron a ganar la dudosa distinción de tener los TLD más riesgosos entre los 20 principales, con siete entradas; Armenia (.AM) y Polonia (.PL) se incluyeron dentro de los 20 nuevos integrantes. Las siguió la región de Asia y el Pacífico (APAC) con seis TLD, mientras que los dominios genéricos, como Red (.NET), ocuparon cinco puestos entre los 20 más riesgosos. El único ingreso del Continente Americano fue Estados Unidos (.US), en el puesto 14.
- **Liderazgo genérico:** al comparar los riesgos por región, los TLD genéricos y patrocinados tuvieron el mayor riesgo promedio. Con 7.9%, estos TLD excedieron el promedio general, mientras que los tres grupos regionales cayeron por debajo del promedio de 6.2%. APAC cayó del promedio del año pasado de 13% a 4.9%, el Continente Americano tuvo un promedio de 2.7%, EMEA sólo 1.9%.

- **Algunas de las mejoras más importantes:** Singapur (.SG) merece un reconocimiento por caer del puesto 10 dentro de los más riesgosos, obtenido el año pasado, al puesto 81 este año; Venezuela (.VE) descendió del puesto 21 al 88 este año y las Filipinas (.PH) del puesto 6 en 2009 al puesto 25 este año.
- **Algunos para observar:** evaluamos únicamente los TLD con resultados de 2,000 o más sitios en tiempo real. Sin embargo, dos TLD de bajo volumen se habrían ubicado entre los cinco primeros puestos si hubiésemos incluido todos los TLD.
 - Senegal (.SN), con 33% de riesgo, habría liderado en el puesto uno, tal vez debido a que no tiene restricciones de registro (<http://en.wikipedia.org/wiki/sn>).
 - El Territorio Británico del Océano Índico (.IO) hubiese estado en el quinto lugar (con un riesgo del 11.5%). Es posible que sea un TLD popular debido a que no tiene restricciones de registro de segundo nivel que limiten los nombres que pueden aparecer detrás del TLD, por eso ofrece posibilidades de reutilización ingeniosas: “.IO se usa en ataques de dominio como eugen.io, moustach.io o pistacch.io, al igual que con el archivo de servicio de host drop.io” (<http://en.wikipedia.org/wiki/io>).

- **Bien limpios:** los cinco TLD con los menores dominios de riesgo, cada uno con 0.1% o menos dominios con riesgos clasificados, fueron los siguientes:

- .TRAVEL (Industria de viajes y turismo)	.02%
- .EDU (Educativo)	.05%
- .JP (Japón)	.08%
- .CAT (Catalán)	.09%
- .GG (Guernesey)	.10%

Nota: las clasificaciones se basan en evaluaciones generales de los sitios, no en clasificaciones de páginas individuales. Los usuarios deben ser conscientes de que aún existen riesgos en URL individuales que pertenecen a dominios que generalmente son seguros. Por ejemplo, encontramos algunas URL riesgosas de páginas individuales con dominio .EDU.

- **El gobierno pierde su liderazgo:** el TLD más seguro en 2009, Gobierno (.GOV), descendió veintitrés puestos este año, si bien permanece en el mismo grado de riesgos, con sólo 0.3%. Todos los sitios de riesgo que encontramos allí se clasificaron en rojo.





¿Por qué es importante el *Mapping*?

McAfee publica el informe *Mapping the Mal Web* para tres comunidades diferentes, con tres objetivos diferentes:

- Para la comunidad de registros y de encargados de registrar dominios, esperamos que este informe reconozca a los que trabajan para reducir los registros de estafadores y para cerrar sitios maliciosos, y que estimule a otros a ponerse en contacto con los líderes para adaptar las mejores prácticas a sus desafíos únicos. Un incentivo es la reducción de riesgos. Anteriormente, hemos trabajado para ayudar con los registros de la lista de los "más agresivos", para lo cual brindamos nuestra investigación sobre los datos de riesgos. Consecuentemente, hemos visto reducciones drásticas en la cantidad de sitios de riesgo en sus TLD.
- Para los propietarios de sitios, esperamos que el informe pueda ser una guía útil al momento de decidir sobre la "ubicación" pública de sus registros.
- Para los clientes y administradores de empresas de TI, esperamos que el informe funcione como una verificación de la realidad, una advertencia de que el riesgo está muy distribuido por la Web, de que los riesgos están aumentando y son más imperceptibles, y de que incluso el usuario más experimentado necesita la ayuda de un software de seguridad integral y actualizado con funciones de búsqueda seguras.



¿Cómo abusan los delincuentes de los dominios de mayor nivel?

Un TLD es uno de los organizadores de la Web, el código de letras al final del sitio web que nos indica dónde está registrado el sitio. Si bien es probable que todos reconozcamos los dominios .COM y .GOV, muchos otros TLD son más difíciles de interpretar, como .AM para Armenia o .CM para Camerún. Los estafadores se aprovechan de esa falta de conocimiento, al igual que la realidad de que muchos consumidores simplemente no prestan atención al sufijo del TLD cuando realizan búsquedas. Muchos consumidores hacen clic en el primer resultado que parece interesante y terminan siendo víctimas de los delincuentes que se toman el tiempo para optimizar sus sitios para los motores de búsqueda.

Algunos TLD son más riesgosos que otros. Los estafadores y piratas cibernéticos registran sus operaciones en lugares donde es más sencillo hacer su trabajo o donde ven una oportunidad financiera mediante errores ortográficos o asociaciones lógicas. Debido a que es fácil omitir la "O" en una dirección .COM, un jugador inescrupuloso puede registrar la dirección www.mcafee.cm en Camerún con la

intención de conseguir tráfico de consumidores y usuarios comerciales preocupados por la seguridad. Por ejemplo, éste sería un sitio posible donde colocar un programa antivirus falso, con la expectativa de que el consumidor sea susceptible a un mensaje de alerta que indique: "tiene un virus, instale este software".

Los responsables de la registración trabajan con diligencia para controlar esta actividad conocida como *typosquatting*, o errores tipográficos deliberados. Los errores tipográficos deliberados cubren todo el espectro de sitios, desde los que generan ingresos por la publicidad a partir de su tipografía, pasando por sitios aparcados que desearían venderle esa dirección, hasta sitios completos de phishing que obtienen información personal o instalan software malicioso.

Los software más peligrosos (algunas veces llamados "inadvertidos") son invisibles para los usuarios: los usuarios no necesitan hacer clic ni aceptar de forma consciente una descarga para infectarse o ser atacados. La mayoría de los *malware* y ataques hacen lo posible para permanecer indetectables. Los consumidores tal vez no noten durante días o semanas que existe un problema y mientras tanto, los delincuentes vacían sus cuentas bancarias, acceden a cuentas de juego online, infectan "amigos" de redes sociales o examinan los ciclos de la CPU en su red de *bots*.

De la misma manera, el usuario promedio no sabe si un sitio .COM está hospedado en EE. UU. o China. A menos que usen una herramienta clasificatoria para asesorarse, los visitantes necesitan hacer una búsqueda más profunda para determinar si pueden confiar en la ubicación que visitan. ¿.VN se refiere a Vietnam o a Venezuela? La respuesta puede crear una gran diferencia con respecto a los riesgos.



Mientras que los buenos trabajan para mejorar la supervisión¹ de las regulaciones y los registros, los delincuentes invierten en software ágil e infraestructuras resistentes (ver la barra lateral de zombis). Cuando el ambiente se caldea en uno de los TLD, mueven rápidamente sus entradas principales de Internet a sitios más flexibles y menos exigentes, sin la necesidad de reubicar los servidores físicos ni modificar los contenidos.

Tenga cuidado con los zombis

Los zombis son equipos corruptos ubicados en hogares y negocios. Los delincuentes los conectan para lanzar diferentes ataques: *spam*, *phishing* y robo de datos. Las redes de *bots* son grupos de zombis que distribuyen la actividad y así ayudan a los propietarios de bots a permanecer "bajo el radar", para poder evitar la detección y regulación, como las bajas en las instalaciones de ISP. Obtienen una infraestructura de nivel comercial para cometer ciberdelitos a un costo insignificante.

Además de ser baratos para operar, los zombis ayudan a los expertos de bots a conservar su anonimato. El éxito de esta estrategia puede explicar los distintos impactos de la baja de McColo, que rebajó los volúmenes globales de spam en 2008,² y la baja de la red de bots de Zeus en marzo de 2010, que duró sólo unas pocas horas.³

El TLD nos dice únicamente dónde está registrado un sitio. El sitio web, incluyendo su contenido, los servidores y propietarios, se puede encontrar en cualquier otra parte. Una tendencia de los criminales consiste en colocar contenido dentro de servicios de archivos compartidos gratuitos para el consumidor y luego sacar el contenido a los TLD según sea necesario. Debido a que los archivos almacenados en servicios como BitTorrent, YouTube y RapidShare cambian constantemente, se ha probado que es muy difícil regular dicho contenido.

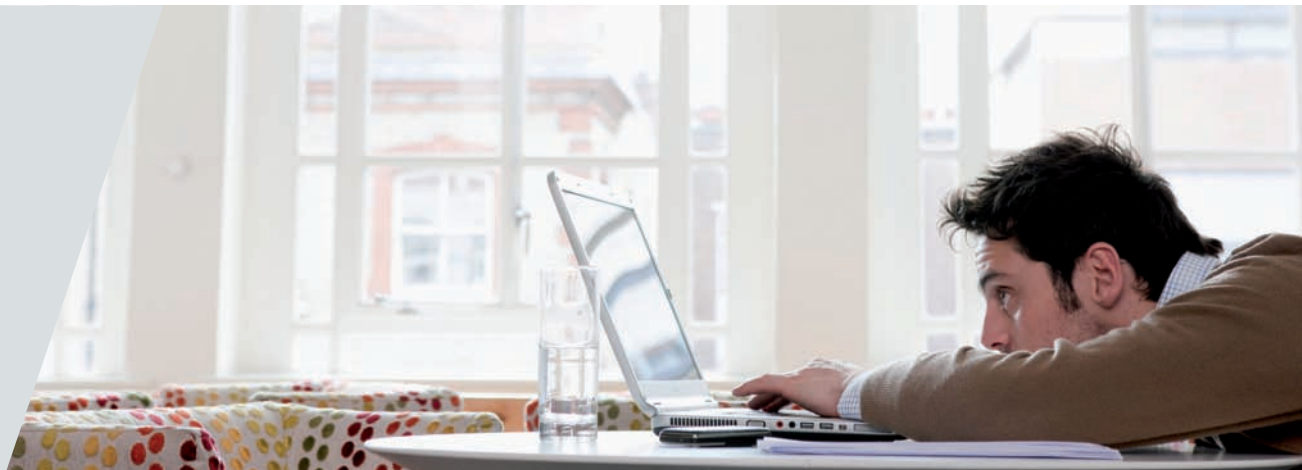
Diversos factores afectan el modo de selección de TLD de los delincuentes:

- **Precios más bajos:** siendo todo igual, los estafadores prefieren a los responsables de registros con registraciones baratas, descuentos por compras en cantidad y políticas de reembolso generosas.
- **Falta de regulación:** siendo todo igual, los estafadores prefieren a los responsables de registros que "no preguntan" en la registración. Cuanta menos información tenga que dar un estafador, mejor. De la misma manera, los estafadores prefieren a los responsables de registros que actúan lentamente, si es que siquiera lo hacen, cuando se notifican dominios maliciosos.
- **Facilidad para registrarse:** siendo todo igual, los estafadores prefieren a los responsables de registros que les permiten registrar grandes cantidades. Esto ocurre aún más en el caso de *phishers* y estafadores que necesitan grandes volúmenes de sitios para compensar el alto nivel de bajas realizadas por los administradores de TLD.

¹ McAfee 2010 Threat Predictions, pág. 9, se puede descargar en varios idiomas desde http://www.mcafee.com/us/threat_center/white_paper.html

² <http://arstechnica.com/security/news/2009/01/two-months-after-mccolo-takedown-spam-levels-yet-to-recover.asp>

³ <http://www.thetechherald.com/article.php/2010105363ISP-takedown-dials-smashes-Zeus-botnet-%E2%80%93-for-a-few-hours>





Metodología

Este año no hubo cambios en la metodología. Al igual que el informe del año pasado, este informe usa la base de datos McAfee Global Threat Intelligence, que refleja los datos de más de 150 millones de sensores ubicados en más de 120 países. Estos sensores (equipos individuales, dispositivos de entrada a redes, software con puntos terminales, servicios hospedados en la nube) provienen de consumidores, pequeñas y medianas empresas, clientes corporativos, instituciones educativas y agencias gubernamentales.

Nuestro enfoque consiste en identificar los riesgos por medio del análisis de patrones de tráfico en la Web, comportamientos de la Web, contenidos hospedados y enlaces. Accedemos a sitios individuales para analizar los comportamientos y contenidos riesgosos o maliciosos, y también analizamos lo que se puede llamar "contexto del sitio": cómo se registra, se consulta y se usa el sitio, y cómo se accede a él.

- Los **sitios** web se evalúan en busca de: el aprovechamiento de los puntos débiles del navegador, phishing y ventanas emergentes excesivas. El aprovechamiento de las vulnerabilidades del navegador (que a menudo se identifican también como descargas inadvertidas), permite que se instalen virus, capturadores de pulsaciones del teclado (*keyloggers*) o spyware en el equipo de un usuario sin su consentimiento y, a menudo, sin que lo sepa. También examinamos los enlaces salientes para ver si dirigen a los visitantes a otros sitios clasificados como riesgosos según McAfee.

- Las **descargas** se analizan instalando software en los equipos de ensayo para comprobar si hay virus o cualquier *adware* en paquetes, *spyware* o cualquier otro programa potencialmente no deseado. McAfee no evalúa archivos individuales ofrecidos punto a punto (en inglés, *peer-to-peer* o P2P) ni programas de archivos compartidos como BitTorrent o plataformas de contenidos como iTunes o Rhapsody. Sí evaluamos archivos encontrados en cualquier sitio de distribución libre (*freeware*) o compartida (*shareware*), como RapidShare, y software de clientes P2P y BitTorrent. La misma clase de servicios que se usan para los archivos compartidos funcionan muy bien para la distribución de *malware*.
- Los **formularios** de inscripción se completan con una dirección de correo electrónico de un solo uso para poder realizar un seguimiento del volumen y el "grado de *spam*" de posteriores mensajes de correo electrónico. El grado de *spam* (correo no deseado) se refiere a las características del contenido comercial del correo electrónico, así como al uso de tácticas para engañar a los programas que actúan como filtro del correo electrónico no deseado.

Además, McAfee Global Threat Intelligence se correlaciona con la información disponible de otros vectores amenazantes, incluidos el tráfico de correo electrónico, el tráfico de intrusiones en la red y el análisis de malware para determinar una clasificación integral de la reputación de un sitio web.

Clasificamos en rojo a los sitios web que contienen códigos maliciosos (como troyanos, virus y *spyware*) o que se aprovechan de los puntos débiles del navegador, que hayan ganado una reputación peligrosa debido a las reputaciones correlativas de sus archivos, correo electrónico, Web y redes. Los sitios en amarillo merecen precaución antes de usarlos, con frecuencia debido al grado de *spam*, las ventanas emergentes excesivas o los enlaces a sitios riesgosos. Casi todos los TLD tienen una mezcla de sitios en rojo y en amarillo.

Delincuentes más creativos, tácticas defensivas más sofisticadas

Todos los años, los delincuentes desarrollan técnicas más intrincadas e innovadoras para ocultar sus actividades. Este año, por ejemplo, las redes de *bots* tuvieron gran influencia en las nuevas categorías de sitios maliciosos, una de nuestras clasificaciones de análisis que incluye virus, troyanos y redes de *bots*.

Debido a que los delincuentes son más hábiles, nosotros también mejoramos. McAfee tiene más de 400 investigadores dedicados al análisis de amenazas. Este equipo global crea herramientas para detectar cambios en la Web, analiza datos de los sensores e identifica el comportamiento y las huellas que indican riesgo. Cada conocimiento nuevo se acopla a nuestra red de inteligencia global para amenazas con el fin de realizar un análisis aún más profundo. Por eso, si bien nuestra metodología sigue siendo la misma, incorporamos cambios constantes dentro de nuestra tecnología para garantizar que realizamos una evaluación precisa de los verdaderos riesgos a los que se enfrentan los usuarios en la actualidad.

	Método no ponderado		Método ponderado	
	TLD N.º 1	TLD N.º 2	TLD N.º 1	TLD N.º 2
Sitios de riesgo	10	100	10	100
Sitios totales	100	10,000	100	10,000
Todos los sitios de riesgo	Irrelevante	Irrelevante	200	200
Clasificación de riesgos	10.0%	1.0%	7.5%	25.5%

Las clasificaciones

Como mencionamos anteriormente, restringimos nuestro análisis a los TLD para los cuales rastreamos al menos 2,000 sitios. Para este informe, incluimos 106 TLD de los 271 que rastreamos, lo que representa dos dominios más que en el año 2009.

Todos los dominios frente a los dominios en tiempo real

Incluimos únicamente los dominios en tiempo real, aquellos que estaban activos en el momento en que se realizó el estudio: 27,304,797 dominios. Los datos en tiempo real representan una instantánea neutral que captura el estado del sistema TLD el día en que recopilamos los datos. Existe una variación de riesgo que es natural, a tal punto que un estudio realizado una semana más tarde podría mostrar resultados diferentes.

Ni programado ni anunciado

No cronometramos el estudio ni promediamos los resultados con muestras múltiples. Además, tampoco anunciamos la fecha. Tomando muestras al azar y sin programarlo podemos asegurarnos de que no haya engaños en el proceso.

Riesgo ponderado

Al igual que en el informe del año anterior, la clasificación de riesgos es ponderada: un 50% de las clasificaciones surgen a partir de la relación de los sitios en riesgo de un TLD con los sitios totales y el restante 50%, de la relación de los sitios en riesgo de un TLD con todos los sitios en riesgo. Creemos que esta metodología de clasificación refleja el nivel de riesgo al que se enfrenta un usuario típico al navegar por la Web. En otras palabras, creemos que un usuario de la Web se resistiría más a visitar un TLD sabiendo que contiene 50% de los sitios en riesgo de toda la Web, incluso si esos sitios en riesgo representan sólo el 1% de los dominios totales del TLD.

Ejemplo: un TLD con 100 sitios en riesgo de 10,000, en tanto que los 100 sitios de riesgo formaron parte de un total de 200 sitios de riesgo en todos los TLD [(50% * 100/10,000) + (50% * 100/200) = 25.5%], se podría clasificar como más riesgoso que el TLD con 10 sitios de riesgo de 100 [(50% * (10/100) + (50% * (10/200)) = 7.5%].

Esta metodología significa que, sólo en algunos casos, un TLD con varios sitios de riesgo pero con una clasificación de riesgos generales más baja, se puede clasificar en puestos más altos (más riesgoso) que un TLD inferior con una porción relativamente superior de sitios de riesgo.

Ejemplo: 6.1% de los 15.5 millones de sitios .COM (Comercial) que analizamos fueron clasificados como riesgosos, un poco menos que nuestro promedio general de 6.2%. Sin embargo, cuando ponderamos el riesgo de los .COM por la cantidad total de sitios de riesgo de todo el mundo, la relación aumentó al 31.3% y se convirtió en el TLD más riesgoso. Por el contrario, 58% de los 24,988 sitios web .VN (Vietnam) que evaluamos fueron riesgosos, pero cuando ponderamos ese riesgo por la cantidad total de sitios de riesgo de todo el mundo, la relación descendió al 29.4% y determinó que los .VN son menos riesgosos que los .COM.

Algunas advertencias sobre las clasificaciones

No ponderado por el tráfico

Nuestras clasificaciones no son ponderadas por el tráfico que recibe un TLD. No distinguimos entre un TLD muy popular que recibe un gran cantidad de tráfico en sus sitios de riesgo y los menos populares que reciben poco tráfico. Este enfoque coincide con la realidad de que los sitios maliciosos con frecuencia ascienden rápidamente a la cima de un millón en Internet (según lo medido por el tráfico) y permanecen allí durante unas semanas mientras los usuarios se infectan. Un usuario que no hace más que quedarse con los sitios populares, o los resultados de búsqueda principales, aún se encuentra en peligro.

No ponderado por el tipo de riesgo

Nuestro análisis no distingue entre amenaza menor, moderada y trivial. En otras palabras, un dominio clasificado en color amarillo por una descarga poco riesgosa es tan considerable como uno clasificado con color rojo por hospedar un código de ataque con descargas inadvertidas. La registración a un sitio que resulta en correo electrónico spam se pondera igual que un sitio con una descarga infectada con virus.

No ponderado por el tamaño del TLD

McAfee no tiene acceso a todos los “archivos de zona” del encargado de registros o a la lista de todos los dominios públicos registrados. Por lo tanto, en ciertos casos, no podemos acceder al porcentaje de los sitios web públicos de un TLD del cual tenemos clasificaciones. Sin embargo, si nos limitamos a clasificar únicamente los TLD de los cuales tenemos grandes muestras, creemos que nuestras evaluaciones generales de riesgos y, consecuentemente, nuestras clasificaciones tendrán gran importancia estadística.

Ejemplo: consideramos 297,946 dominios de .PL (Polonia). De ellos, encontramos que 17,398, o 5.8% del total, eran riesgosos. Suponiendo que el total de la población de dominios .PL es de 2,970,000, nuestro tamaño de muestras es aproximadamente del 10.0%. Con un nivel de confianza del 95%, nuestro intervalo de confianza es +/- 0.08%. En otras palabras, podemos estar un 95% seguros de que el porcentaje actual de sitios de riesgo se encuentra entre 5.72% y 5.88%.

Dominios que no son URL

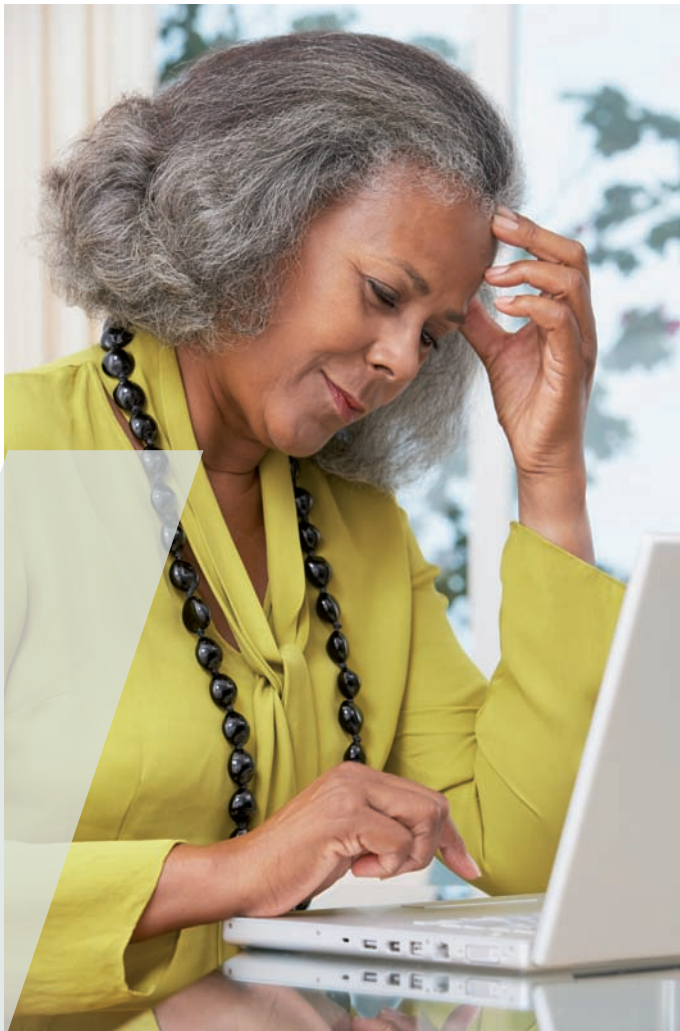
Este estudio incorpora únicamente clasificaciones en el nivel de los dominios, no URL individuales dentro de un dominio. Esto es importante porque McAfee ha encontrado numerosos ejemplos de URL *individuales* maliciosas dentro de *dominios* que de otra manera serían seguros, como .HR (Croacia) y .EDU (Educativo).

Sin modificaciones para eliminar sitios de riesgo

Sabemos que, en algunos casos, los operadores de TLD se encuentran bajo obligaciones contractuales que no les permiten eliminar ciertos tipos de dominios que McAfee considera de riesgo. Además, el comportamiento del sitio web que lleva a la eliminación por un registro puede no considerarse inapropiado en otro. McAfee no distingue entre estas reglas diferentes.

Otros

Por último, nuestras clasificaciones no consideran los dominios que no rastreamos.



Desglose de las clasificaciones

Clasificaciones generales

RIESGO ALTO ■ ■ ■ ■ ■ RIESGO BAJO

Pais o nombre	Región	TLD	Clasificación mundial de riesgos 2010	Relación de riesgos ponderados 2010	Relación de riesgos no ponderados 2010	Clasificación mundial de riesgos 2009	Relación de riesgos ponderados 2009	Cambio año a año en el riesgo ponderado	Dominios totales rastreados	Dominios totales de riesgo
Comercial	Genérico	COM	1	31.3%	6.1%	2	32.2%	-2.8% ↓	15,530,183	948,995
Información	Genérico	INFO	2	30.7%	46.6%	5	15.8%	94.5% ↑	533,711	248,806
Vietnam	APAC	VN	3	29.4%	58.0%	39	0.9%	3,107.9% ↑	24,988	14,492
Camerún	EMEA	CM	4	22.2%	44.2%	1	36.7%	-39.5% ↓	3,947	1,746
Armenia	EMEA	AM	5	12.1%	24.2%	23	2.0%	512.9% ↑	3,145	760
Islas Cocos (Keeling)	APAC	CC	6	10.5%	20.2%	14	3.3%	215.4% ↑	58,713	11,869
Asia y el Pacífico	Genérico	ASIA	7	10.3%	20.6%	N/A	N/A	N/A	3,122	642
Red	Genérico	NET	8	10.1%	10.5%	7	5.8%	73.7% ↑	1,556,813	163,466
Rusia	EMEA	RU	9	10.1%	16.8%	9	4.6%	116.7% ↑	329,136	55,373
Samoa Occidental	APAC	WS	10	8.6%	16.9%	4	17.8%	-51.8% ↓	22,070	3,734
Tokelau	APAC	TK	11	8.4%	15.9%	19	2.3%	262.0% ↑	91,876	14,630
Organización	Genérico	ORG	12	6.4%	7.4%	11	4.2%	50.3% ↑	1,224,870	90,290
Negocio	Genérico	BIZ	13	6.3%	11.8%	13	3.6%	74.3% ↑	121,622	14,350
Estados Unidos	Continente Americano	US	14	6.0%	11.2%	17	3.1%	95.7% ↑	119,861	13,365
República Popular China	APAC	CN	15	4.8%	8.3%	3	23.4%	-79.5% ↓	261,298	21,711
Ex Unión Soviética	EMEA	SU	16	4.6%	9.2%	8	5.2%	-9.8% ↓	8,478	784
Santo Tomé y Príncipe	EMEA	ST	17	3.7%	7.3%	12	3.8%	-1.6% ↓	11,997	880
Rumania	EMEA	RO	18	3.7%	7.1%	20	2.2%	63.5% ↑	56,312	3,982
Georgia	EMEA	GE	19	3.5%	7.0%	N/A	N/A	N/A	2,311	162
Polonia	EMEA	PL	20	3.4%	5.8%	60	0.5%	574.2% ↑	297,946	17,398
India	APAC	IN	21	3.4%	6.5%	22	2.0%	67.8% ↑	49,368	3,218
Montserrat	EMEA	MS	22	3.2%	6.3%	N/A	N/A	N/A	3,382	213
Pakistán	APAC	PK	23	2.8%	5.5%	18	2.8%	0.5% ↑	4,947	273
Niue	APAC	NU	24	2.5%	5.0%	24	1.9%	32.3% ↑	27,420	1,362
Filipinas	APAC	PH	25	2.2%	4.3%	6	13.1%	-83.4% ↓	9,625	418
Montenegro	EMEA	me	26	2.1%	4.3%	N/A	N/A	N/A	5,465	233
Tonga	APAC	TO	27	2.1%	4.2%	33	1.1%	94.5% ↑	13,150	550
Trinidad y Tobago	Continente Americano	TT	28	1.9%	3.8%	51	0.6%	217.6% ↑	4,287	165
Familias e individuos	Genérico	NAME	29	1.7%	3.3%	16	3.1%	-45.9% ↓	6,726	223
Tuvalu	APAC	TV	30	1.7%	3.2%	38	0.9%	80.1% ↑	40,770	1,316
Kazajstán	EMEA	KZ	31	1.5%	3.1%	15	3.1%	-50.2% ↓	4,708	144
Islas Turcas y Caicos	Continente Americano	TC	32	1.5%	3.0%	40	0.9%	74.8% ↑	11,187	338
Dispositivos móviles	Genérico	MOBI	33	1.5%	3.0%	25	1.7%	-14.4% ↓	6,861	204
Marruecos	EMEA	MA	34	1.5%	3.0%	N/A	N/A	N/A	2,024	60
Laos	APAC	LA	35	1.5%	2.9%	26	1.6%	-8.7% ↓	4,143	122
Colombia	Continente Americano	CO	36	1.5%	2.9%	68	0.4%	249.0% ↑	3,618	106
Belice	Continente Americano	BZ	37	1.3%	2.5%	30	1.2%	2.2% ↑	3,472	88

Clasificaciones generales (continuación)

RIESGO ALTO  RIESGO BAJO

País o nombre	Región	TLD	Clasificación mundial de riesgos 2010	Relación de riesgos ponderados 2010	Relación de riesgos no ponderados 2010	Clasificación mundial de riesgos 2009	Relación de riesgos ponderados 2009	Cambio año a año en el riesgo ponderado	Dominios totales rastreados	Dominios totales de riesgo
Corea del Sur	APAC	KR	38	1.1%	2.2%	28	1.5%	-26.7% ↓	70,261	1,530
Isla de Navidad	APAC	CX	39	1.1%	2.2%	74	0.4%	195.6% ↑	6,084	136
Letonia	EMEA	LV	40	1.1%	2.1%	71	0.4%	163.1% ↑	10,015	210
Canadá	Continente Americano	CA	41	0.9%	1.6%	64	0.5%	90.5% ↑	169,543	2,777
Eslovaquia	EMEA	SK	42	0.9%	1.7%	45	0.8%	11.4% ↑	37,643	649
Serbia	EMEA	RS	43	0.9%	1.7%	N/A	N/A	N/A	2,031	35
Unión Europea	EMEA	EU	44	0.8%	1.6%	59	0.5%	60.3% ↑	80,278	1,288
Ucrania	EMEA	UA	45	0.8%	1.6%	36	1.0%	-19.7% ↓	38,619	615
Estados Federados de Micronesia	APAC	FM	46	0.7%	1.5%	66	0.4%	69.7% ↑	4,075	60
Malasia	APAC	MY	47	0.7%	1.5%	80	0.3%	122.1% ↑	15,200	221
Tailandia	APAC	TH	48	0.7%	1.5%	32	1.1%	-34.8% ↓	8,912	130
Reino Unido	EMEA	UK	49	0.7%	0.9%	55	0.6%	30.3% ↑	898,229	8,503
Moldavia	EMEA	MD	50	0.7%	1.4%	N/A	N/A	N/A	2,644	38
Belarús	EMEA	BY	51	0.7%	1.4%	29	1.3%	-44.8% ↓	4,372	62
Georgia del Sur e Islas Sándwich del Sur	EMEA	GS	52	0.6%	1.2%	48	0.6%	-7.1% ↓	4,578	55
Perú	Continente Americano	PE	53	0.6%	1.2%	41	0.9%	-32.9% ↓	5,176	60
República Checa	EMEA	CZ	54	0.6%	1.0%	54	0.6%	-4.7% ↓	101,781	1,068
Irán	EMEA	IR	55	0.5%	1.1%	37	0.9%	-42.5% ↓	17,874	191
Lituania	EMEA	LT	56	0.5%	1.1%	44	0.8%	-36.9% ↓	11,517	121
Ecuador	Continente Americano	EC	57	0.5%	1.0%	49	0.6%	-18.8% ↓	2,496	26
Emiratos Árabes Unidos	EMEA	AE	58	0.5%	1.0%	65	0.5%	7.9% ↑	4,123	42
Uruguay	Continente Americano	UY	59	0.5%	1.0%	75	0.4%	35.0% ↑	3,277	33
Hong Kong	APAC	HK	60	0.5%	1.0%	34	1.1%	-53.8% ↓	17,960	176
República de China (Taiwán)	APAC	TW	61	0.5%	1.0%	52	0.6%	-16.3% ↓	56,000	534
Bélgica	EMEA	BE	62	0.5%	0.9%	81	0.3%	49.2% ↑	123,606	1,124
Liechtenstein	EMEA	LI	63	0.5%	1.0%	90	0.2%	110.3% ↑	3,000	29
Timor Oriental	APAC	TL	64	0.5%	1.0%	58	0.5%	-11.6% ↓	5,309	51
Hungría	EMEA	HU	65	0.4%	0.9%	53	0.6%	-23.9% ↓	71,650	614
Alemania	EMEA	DE	66	0.4%	0.5%	83	0.3%	43.8% ↑	1,504,163	7,052
Arabia Saudita	EMEA	SA	67	0.4%	0.9%	42	0.9%	-48.7% ↓	2,630	23
Bosnia	EMEA	BA	68	0.4%	0.9%	46	0.8%	-43.9% ↓	2,671	23
Indonesia	APAC	ID	69	0.4%	0.8%	56	0.6%	-23.7% ↓	6,138	52
Brasil	Continente Americano	BR	70	0.4%	0.7%	70	0.4%	5.0% ↑	290,350	2,084
Finlandia	EMEA	FI	71	0.4%	0.8%	85	0.3%	41.5% ↑	35,046	283
Argentina	Continente Americano	AR	72	0.4%	0.8%	50	0.6%	-36.7% ↓	80,324	603
España	EMEA	ES	73	0.4%	0.7%	27	1.6%	-75.6% ↓	103,555	749
Nueva Zelanda	APAC	NZ	74	0.4%	0.7%	94	0.2%	86.8% ↑	56,240	416
Francia	EMEA	FR	75	0.4%	0.7%	61	0.5%	-24.8% ↓	244,237	1,626
Austria	EMEA	AT	76	0.4%	0.7%	89	0.2%	58.4% ↑	139,244	966
Israel	EMEA	IL	77	0.4%	0.7%	31	1.2%	-70.4% ↓	29,113	209

Clasificaciones generales (continuación)

RIESGO ALTO ■ ■ ■ ■ ■ RIESGO BAJO

Pais o nombre	Región	TLD	Clasificación mundial de riesgos 2010	Relación de riesgos ponderados 2010	Relación de riesgos no ponderados 2010	Clasificación mundial de riesgos 2009	Relación de riesgos ponderados 2009	Cambio año a año en el riesgo ponderado	Dominios totales rastreados	Dominios totales de riesgo
Nauru	APAC	NR	78	0.4%	0.7%	62	0.5%	-29.9% ↓	8,199	58
Turquía	EMEA	TR	79	0.4%	0.7%	47	0.7%	-46.6% ↓	36,466	252
Suecia	EMEA	SE	80	0.4%	0.7%	88	0.3%	35.8% ↑	102,870	684
Singapur	APAC	SG	81	0.3%	0.7%	10	4.6%	-92.6% ↓	15,632	105
Noruega	EMEA	NO	82	0.3%	0.6%	77	0.4%	-8.5% ↓	50,089	317
Grecia	EMEA	GR	83	0.3%	0.6%	73	0.4%	-22.7% ↓	41,357	243
Gobierno	Genérico	GOV	84	0.3%	0.6%	104	0.0%	1,188.3% ↑	6,415	38
México	Continente Americano	MX	85	0.3%	0.6%	69	0.4%	-26.7% ↓	49,601	284
Luxemburgo	EMEA	LU	86	0.3%	0.6%	98	0.1%	102.4% ↑	6,750	38
Italia	EMEA	IT	87	0.3%	0.5%	78	0.3%	-17.6% ↓	314,171	1,495
Venezuela	Continente Americano	VE	88	0.3%	0.5%	21	2.1%	-86.7% ↓	5,842	32
Estonia	EMEA	EE	89	0.3%	0.5%	76	0.4%	-30.1% ↓	11,302	58
Sudáfrica	EMEA	ZA	90	0.3%	0.5%	96	0.2%	50.6% ↑	72,629	357
Portugal	EMEA	PT	91	0.2%	0.5%	86	0.3%	-13.2% ↓	38,869	189
Vanuatu	APAC	VU	92	0.2%	0.5%	97	0.2%	49.1% ↑	15,211	70
Países Bajos	EMEA	NL	93	0.2%	0.3%	84	0.3%	-24.4% ↓	583,943	1,980
Bulgaria	EMEA	BG	94	0.2%	0.5%	43	0.8%	-73.1% ↓	17,974	81
Dinamarca	EMEA	DK	95	0.2%	0.4%	91	0.2%	0.7% ↑	151,472	627
Islandia	EMEA	IS	96	0.2%	0.4%	87	0.3%	-19.8% ↓	6,102	26
Eslovenia	EMEA	SI	97	0.2%	0.4%	79	0.3%	-36.6% ↓	11,339	48
Australia	APAC	AU	98	0.2%	0.3%	93	0.2%	-4.3% ↓	256,103	871
Suiza	EMEA	CH	99	0.1%	0.3%	95	0.2%	-13.3% ↓	217,863	572
Irlanda	EMEA	IE	100	0.1%	0.2%	101	0.1%	-5.7% ↓	32,120	71
Croacia	EMEA	HR	101	0.1%	0.2%	100	0.1%	-11.1% ↓	22,511	50
Guernesey	EMEA	GG	102	0.1%	0.2%	57	0.6%	-81.1% ↓	12,092	25
Catalán	Patrocinado	CAT	103	0.1%	0.2%	99	0.1%	-31.6% ↓	3,936	7
Japón	APAC	JP	104	0.1%	0.1%	103	0.1%	6.6% ↑	464,408	547
Educativo	Genérico	EDU	105	0.1%	0.1%	102	0.1%	-48.6% ↓	14,002	15
Industria de viajes y turismo	Generic	TRAVEL	106	0.0%	0.0%	92	0.2%	-88.6% ↓	2,013	1

Nota: las entradas con "N/A" fueron TLD nuevos en el informe de este año, por eso no hay cambios año a año.

Región del Continente Americano

RIESGO ALTO ■ ■ ■ ■ ■ RIESGO BAJO

País o nombre	TLD	Clasificación mundial de riesgos 2010	Relación de riesgos ponderados 2010	Relación de riesgos no ponderados 2010	Clasificación mundial de riesgos 2009	Relación de riesgos ponderados 2009	Cambio año a año en los riesgos ponderados	Dominios totales rastreados 2010	Dominios de riesgo totales 2010
Estados Unidos	US	14	6.0%	11.2%	17	3.1%	95.7% ↑	119,861	13,365
Trinidad y Tobago	TT	28	1.9%	3.8%	51	0.6%	217.6% ↑	4,287	165
Islas Turcas y Caicos	TC	32	1.5%	3.0%	40	0.9%	74.8% ↑	11,187	338
Colombia	CO	36	1.5%	2.9%	68	0.4%	249.0% ↑	3,618	106
Belice	BZ	37	1.3%	2.5%	30	1.2%	2.2% ↑	3,472	88
Canadá	CA	41	0.9%	1.6%	64	0.5%	90.5% ↑	169,543	2,777
Perú	PE	53	0.6%	1.2%	41	0.9%	-32.9% ↓	5,176	60
Ecuador	EC	57	0.5%	1.0%	49	0.6%	-18.8% ↓	2,496	26
Uruguay	UY	59	0.5%	1.0%	75	0.4%	35.0% ↑	3,277	33
Brasil	BR	70	0.4%	0.7%	70	0.4%	5.0% ↑	290,350	2,084
Argentina	AR	72	0.4%	0.8%	50	0.6%	-36.7% ↓	80,324	603
México	MX	85	0.3%	0.6%	69	0.4%	-26.7% ↓	49,601	284
Venezuela	VE	88	0.3%	0.5%	21	2.1%	-86.7% ↓	5,842	32

- .CO (Colombia) mostró uno de los aumentos de riesgo más importantes y pasó del puesto 68 al 36 este año. Hallamos que los riesgos principales asociados con .CO se relacionan con actividades maliciosas, URL que funcionan como intermediarios para otros hosts maliciosos, como las redes de bots de sistemas comprometidos y los centros de comando y control que los manipulan.
- .VE (Venezuela) fue uno de los TLD que más mejoró este año y pasó del puesto 21 en 2009 al puesto 88.

Región de Asia y el Pacífico (APAC)

RIESGO ALTO ■ ■ ■ ■ ■ RIESGO BAJO

País o nombre	TLD	Clasificación mundial de riesgos 2010	Relación de riesgos ponderados 2010	Relación de riesgos no ponderados 2010	Clasificación mundial de riesgos 2009	Relación de riesgos ponderados 2009	Cambio año a año en los riesgos ponderados	Dominios totales rastreados 2010	Dominios de riesgo totales 2010
Vietnam	VN	3	29.4%	58.0%	39	0.9%	3,107.9% ↑	24,988	14,492
Islas Cocos (Keeling)	CC	6	10.5%	20.2%	14	3.3%	215.4% ↑	58,713	11,869
Samoa Occidental	WS	10	8.6%	16.9%	4	17.8%	-51.8% ↓	22,070	3,734
Tokelau	TK	11	8.4%	15.9%	19	2.3%	262.0% ↑	91,876	14,630
República Popular de China	CN	15	4.8%	8.3%	3	23.4%	-79.5% ↓	261,298	21,711
India	IN	21	3.4%	6.5%	22	2.0%	67.8% ↑	49,368	3,218
Pakistán	PK	23	2.8%	5.5%	18	2.8%	0.5% ↑	4,947	273
Niue	NU	24	2.5%	5.0%	24	1.9%	32.3% ↑	27,420	1,362
Filipinas	PH	25	2.2%	4.3%	6	13.1%	-83.4% ↓	9,625	418
Tonga	TO	27	2.1%	4.2%	33	1.1%	94.5% ↑	13,150	550
Tuvalu	TV	30	1.7%	3.2%	38	0.9%	80.1% ↑	40,770	1,316
Laos	LA	35	1.5%	2.9%	26	1.6%	-8.7% ↓	4,143	122
Corea del Sur	KR	38	1.1%	2.2%	28	1.5%	-26.7% ↓	70,261	1,530
Isla de Navidad	CX	39	1.1%	2.2%	74	0.4%	195.6% ↑	6,084	136
Estados Federados de Micronesia	FM	46	0.7%	1.5%	66	0.4%	69.7% ↑	4,075	60
Malasia	MY	47	0.7%	1.5%	80	0.3%	122.1% ↑	15,200	221
Tailandia	TH	48	0.7%	1.5%	32	1.1%	-34.8% ↓	8,912	130
Hong Kong	HK	60	0.5%	1.0%	34	1.1%	-53.8% ↓	17,960	176
República de China (Taiwán)	TW	61	0.5%	1.0%	52	0.6%	-16.3% ↓	56,000	534
Timor Oriental	TL	64	0.5%	1.0%	58	0.5%	-11.6% ↓	5,309	51
Indonesia	ID	69	0.4%	0.8%	56	0.6%	-23.7% ↓	6,138	52
Nueva Zelanda	NZ	74	0.4%	0.7%	94	0.2%	86.8% ↑	56,240	416
Nauru	NR	78	0.4%	0.7%	62	0.5%	-29.9% ↓	8,199	58
Singapur	SG	81	0.3%	0.7%	10	4.6%	-92.6% ↓	15,632	105
Vanuatu	VU	92	0.2%	0.5%	97	0.2%	49.1% ↑	15,211	70
Australia	AU	98	0.2%	0.3%	93	0.2%	-4.3% ↓	256,103	871
Japón	JP	104	0.1%	0.1%	103	0.1%	6.6% ↑	464,408	547

Nota: las entradas con "N/A" fueron TLD nuevos en el informe de este año, por eso no hay cambios año a año.

- En general, la región de Asia y el Pacífico dominó la categoría "que más mejoró" y llegó a ocupar cuatro de las cinco posiciones más altas, liderada por Singapur (.SG) en el número uno y luego la República Popular China (.CN), las Filipinas (.PH) y Samoa Occidental (.WS). Este logro es muy impresionante debido a que estos cuatro TLD estuvieron el año pasado dentro de la lista de los diez TLD más riesgosos.
- Sin embargo, Vietnam (.VN) pasó del puesto 39 de los más riesgosos en 2009, al tercero más riesgoso en 2010. Al igual que Colombia (.CO), los riesgos predominantes asociados con .VN se relacionan con actividades maliciosas, sitios usados para enmascarar a otros hosts maliciosos, al igual que actividades de comando y control.
- Japón resultó ser uno de los TLD menos riesgosos del mundo y volvió a ser el menos riesgoso de APAC.

Europe, Middle East, and Africa (EMEA) region

RIESGO ALTO  RIESGO BAJO

País o nombre	TLD	Clasificación mundial de riesgos 2010	Relación de riesgos ponderados 2010	Relación de riesgos no ponderados 2010	Clasificación mundial de riesgos 2009	Relación de riesgos ponderados 2009	Cambio año a año en los riesgos ponderados	Dominios totales rastreados 2010	Dominios de riesgo totales 2010
Camerún	CM	4	22.2%	44.2%	1	36.7%	-39.5% ↓	3,947	1,746
Armenia	AM	5	12.1%	24.2%	23	2.0%	512.9% ↑	3,145	760
Rusia	RU	9	10.1%	16.8%	9	4.6%	116.7% ↑	329,136	55,373
Ex Unión Soviética	SU	16	4.6%	9.2%	8	5.2%	-9.8% ↓	8,478	784
Santo Tomé y Príncipe	ST	17	3.7%	7.3%	12	3.8%	-1.6% ↓	11,997	880
Rumania	RO	18	3.7%	7.1%	20	2.2%	63.5% ↑	56,312	3,982
Georgia	GE	19	3.5%	7.0%	N/A	N/A	N/A	2,311	162
Polonia	PL	20	3.4%	5.8%	60	0.5%	574.2% ↑	297,946	17,398
Montserrat	MS	22	3.2%	6.3%	N/A	N/A	N/A	3,382	213
Montenegro	ME	26	2.1%	4.3%	N/A	N/A	N/A	5,465	233
Kazajstán	KZ	31	1.5%	3.1%	15	3.1%	-50.2% ↓	4,708	144
Marruecos	MA	34	1.5%	3.0%	N/A	N/A	N/A	2,024	60
Letonia	LV	40	1.1%	2.1%	71	0.4%	163.1% ↑	10,015	210
Eslovaquia	SK	42	0.9%	1.7%	45	0.8%	11.4% ↑	37,643	649
Serbia	RS	43	0.9%	1.7%	N/A	N/A	N/A	2,031	35
Unión Europea	EU	44	0.8%	1.6%	59	0.5%	60.3% ↑	80,278	1,288
Ucrania	UA	45	0.8%	1.6%	36	1.0%	-19.7% ↓	38,619	615
Reino Unido	UK	49	0.7%	0.9%	55	0.6%	30.3% ↑	898,229	8,503
Moldavia	MD	50	0.7%	1.4%	N/A	N/A	N/A	2,644	38
Belarús	BY	51	0.7%	1.4%	29	1.3%	-44.8% ↓	4,372	62
Georgia del Sur e Islas Sándwich del Sur	GS	52	0.6%	1.2%	48	0.6%	-7.1% ↓	4,578	55
República Checa	CZ	54	0.6%	1.0%	54	0.6%	-4.7% ↓	101,781	1,068
Irán	IR	55	0.5%	1.1%	37	0.9%	-42.5% ↓	17,874	191
Lituania	LT	56	0.5%	1.1%	44	0.8%	-36.9% ↓	11,517	121
Emiratos Árabes Unidos	AE	58	0.5%	1.0%	65	0.5%	7.9% ↑	4,123	42
Bélgica	BE	62	0.5%	0.9%	81	0.3%	49.2% ↑	123,606	1,124
Liechtenstein	LI	63	0.5%	1.0%	90	0.2%	110.3% ↑	3,000	29
Hungría	HU	65	0.4%	0.9%	53	0.6%	-23.9% ↓	71,650	614
Alemania	DE	66	0.4%	0.5%	83	0.3%	43.8% ↑	1,504,163	7,052
Arabia Saudita	SA	67	0.4%	0.9%	42	0.9%	-48.7% ↓	2,630	23
Bosnia	BA	68	0.4%	0.9%	46	0.8%	-43.9% ↓	2,671	23
Finlandia	FI	71	0.4%	0.8%	85	0.3%	41.5% ↑	35,046	283
España	ES	73	0.4%	0.7%	27	1.6%	-75.6% ↓	103,555	749
Francia	FR	75	0.4%	0.7%	61	0.5%	-24.8% ↓	244,237	1,626
Austria	AT	76	0.4%	0.7%	89	0.2%	58.4% ↑	139,244	966
Israel	IL	77	0.4%	0.7%	31	1.2%	-70.4% ↓	29,113	209
Turquía	TR	79	0.4%	0.7%	47	0.7%	-46.6% ↓	36,466	252
Suecia	SE	80	0.4%	0.7%	88	0.3%	35.8% ↑	102,870	684
Noruega	NO	82	0.3%	0.6%	77	0.4%	-8.5% ↓	50,089	317
Grecia	GR	83	0.3%	0.6%	73	0.4%	-22.7% ↓	41,357	243
Luxemburgo	LU	86	0.3%	0.6%	98	0.1%	102.4% ↑	6,750	38
Italia	IT	87	0.3%	0.5%	78	0.3%	-17.6% ↓	314,171	1,495
Estonia	EE	89	0.3%	0.5%	76	0.4%	-30.1% ↓	11,302	58
Sudáfrica	ZA	90	0.3%	0.5%	96	0.2%	50.6% ↑	72,629	357
Portugal	PT	91	0.2%	0.5%	86	0.3%	-13.2% ↓	38,869	189

RIESGO ALTO  RIESGO BAJO

País o nombre	TLD	Clasificación mundial de riesgos 2010	Relación de riesgos ponderados 2010	Relación de riesgos no ponderados 2010	Clasificación mundial de riesgos 2009	Relación de riesgos ponderados 2009	Cambio año a año en los riesgos ponderados	Dominios totales rastreados 2010	Dominios de riesgo totales 2010
Países Bajos	NL	93	0.2%	0.3%	84	0.3%	-24.4% ↓	583,943	1,980
Bulgaria	BG	94	0.2%	0.5%	43	0.8%	-73.1% ↓	17,974	81
Dinamarca	DK	95	0.2%	0.4%	91	0.2%	0.7% ↑	151,472	627
Islandia	IS	96	0.2%	0.4%	87	0.3%	-19.8% ↓	6,102	26
Eslovenia	SI	97	0.2%	0.4%	79	0.3%	-36.6% ↓	11,339	48
Suiza	CH	99	0.1%	0.3%	95	0.2%	-13.3% ↓	217,863	572
Irlanda	IE	100	0.1%	0.2%	101	0.1%	-5.7% ↓	32,120	71
Croacia	HR	101	0.1%	0.2%	100	0.1%	-11.1% ↓	22,511	50
Guernesey	GG	102	0.1%	0.2%	57	0.6%	-81.1% ↓	12,092	25

Nota: las entradas con "N/A" fueron TLD nuevos en el informe de este año, por eso no hay cambios año a año.

- Dos TLD de EMEA aumentaron su riesgo de forma significativa este año comparado con 2009. .PL (Polonia) pasó del puesto 60 al 20 este año y .AM (Armenia) del puesto 23 al 5 en términos de riesgo.
- .PL tiene dominios asociados con todos los riesgos, incluso actividades y descargas maliciosas, y URL de host asociadas con ataques y campañas de *spam*.
- Los riesgos asociados con .AM están más centralizados y se concentran en las actividades maliciosas, como servicios de comando y control y otros servicios relacionados.

TLD genéricos y patrocinados

RIESGO ALTO  RIESGO BAJO

Nombre	Región	TLD	Clasificación mundial de riesgos 2010	Relación de riesgos ponderados 2010	Relación de riesgos no ponderados 2010	Clasificación mundial de riesgos 2009	Relación de riesgos ponderados 2009	Cambio año a año en los riesgos ponderados	Dominios totales rastreados 2010	Dominios de riesgo totales 2010
Comercial	Genérico	COM	1	31.3%	6.1%	2	32.2%	-2.8% ↓	15,530,183	948,995
Información	Genérico	INFO	2	30.7%	46.6%	5	15.8%	94.5% ↑	533,711	248,806
Asia y el Pacífico	Genérico	ASIA	7	10.3%	20.6%	N/A	N/A	N/A	3,122	642
Red	Genérico	NET	8	10.1%	10.5%	7	5.8%	73.7% ↑	1,556,813	163,466
Organización	Genérico	ORG	12	6.4%	7.4%	11	4.2%	50.3% ↑	1,224,870	90,290
Negocio	Genérico	BIZ	13	6.3%	11.8%	13	3.6%	74.3% ↑	121,622	14,350
Familias e individuos	Genérico	NAME	29	1.7%	3.3%	16	3.1%	-45.9% ↓	6,726	223
Dispositivos móviles	Genérico	MOBI	33	1.5%	3.0%	25	1.7%	-14.4% ↓	6,861	204
Gobierno	Genérico	GOV	84	0.3%	0.6%	104	0.0%	1,188.3% ↑	6,415	38
Catalán	Patrocinado	CAT	103	0.1%	0.2%	99	0.1%	-31.6% ↓	3,936	7
Educativo	Genérico	EDU	105	0.1%	0.1%	102	0.1%	-48.6% ↓	14,002	15
Industria de viajes y turismo	Genérico	TRAVEL	106	0.0%	0.0%	92	0.2%	-88.6% ↓	2,013	1

- Casi la mitad (47%) de los sitios de Información (.INFO) evaluados fueron rojos o amarillos; la mayoría de ellos (43%), rojos. Muchos de los riesgos identificados dentro del TLD .INFO están asociados con el host de contenido usado para las campañas de *spam*. Este contenido puede ser sobre artículos, *malware* o antivirus falsos. Además, hubo muchos sitios dentro del TLD .INFO que estuvieron asociados con otros dominios y servidores maliciosos. Muchos de esos sitios luego se hicieron evidentes en campañas de antivirus falsos y actividades de la red de *bots* de Zeus.
- Más del 14% de las URL de Koobface (45,213) estaban dentro de Comercial (.COM), sin presencia significativa dentro de otros TLD.

Tendencias de riesgo de color rojo frente al amarillo

Las clasificaciones en rojo se emplean en los sitios que contienen códigos maliciosos (como troyanos, virus y spyware), que se aprovechan de los puntos débiles del navegador o que hayan ganado una reputación peligrosa como resultado de las reputaciones correlativas de sus archivos, correo electrónico, Web y redes. Los sitios en amarillo merecen precaución antes de usarlos, con frecuencia debido al grado de spam, las ventanas emergentes excesivas o los enlaces a sitios riesgosos.

La mayoría de los TLD tiene una mezcla de sitios en rojo y en amarillo. Algunos, sin embargo, tienen tendencias fuertes hacia el amarillo o el rojo. Por ejemplo, de los 642 dominios de la región de Asia y el Pacífico (.ASIA), 619 fueron amarillos. Por el contrario, 100% de los dominios de riesgo en Gobierno (.GOV), Islandia (.IS), Educativo (.EDU) e Industria de viajes y turismo (.TRAVEL) fueron rojos. Como ocurre, no nos preocupamos demasiado por estos cuatro TLD. Ninguno de los cuatro TLD tiene más de 40 sitios de riesgo en total y todos en general son seguros. Sin embargo, Vietnam (.VT) tiene 14,492 sitios en rojo, lo que representa un 99.89% de sus sitios de riesgo y ayuda a justificar la tercera posición como uno de los TLD más riesgosos.

Con tendencia hacia el amarillo

País o nombre	TLD	Sitios de riesgo en total	Porcentaje en amarillo	Porcentaje en rojo
Asia y el Pacífico	ASIA	642	96.4%	3.6%
Armenia	AM	760	94.2%	5.8%
Finlandia	FI	283	89.1%	11.0%
Tokelau	TK	14,630	86.3%	13.7%
Islas Cocos (Keeling)	CC	11,869	85.5%	14.5%
Canadá	CA	2,777	82.0%	18.0%
Reino Unido	UK	8,503	77.8%	22.2%
Tuvalu	TV	1,316	77.7%	22.3%
Dispositivos móviles	MOBI	204	76.0%	24.0%
Malasia	MY	221	74.7%	25.3%
Niue	NU	1,362	73.3%	26.7%
Suecia	SE	684	65.2%	34.8%
Estados Federados de Micronesia	FM	60	65.0%	35.0%
Nueva Zelanda	NZ	416	61.8%	38.2%
Colombia	CO	106	56.6%	43.4%
Samoa Occidental	WS	3,734	55.8%	44.2%
China	CN	21,711	55.5%	44.5%
Rusia	RU	55,373	55.4%	44.6%
Perú	PE	60	51.7%	48.3%
Australia	AU	871	51.7%	48.3%

Con tendencia hacia el rojo

País o nombre	TLD	Sitios de riesgo en total	Porcentaje en amarillo	Porcentaje en rojo
Gobierno	GOV	38	0.0%	100.0%
Islandia	IS	26	0.0%	100.0%
Educativo	EDU	15	0.0%	100.0%
Industria de viajes y turismo	TRAVEL	1	0.0%	100.0%
Vietnam	VN	14,492	0.1%	99.9%
Islas Turcas y Caicos	TC	338	3.3%	96.8%
Polonia	PL	17,398	3.5%	96.5%
Trinidad y Tobago	TT	165	4.2%	95.8%
Timor Oriental	TL	51	5.9%	94.1%
Croacia	HR	50	8.0%	92.0%
Serbia	RS	35	8.6%	91.4%
Información	INFO	248,806	8.6%	91.4%
Nauru	NR	58	8.6%	91.4%
Arabia Saudita	SA	23	8.7%	91.3%
Hungría	HU	614	9.1%	90.9%
Emiratos Árabes Unidos	AE	42	9.5%	90.5%
Negocio	BIZ	14,350	9.8%	90.2%
Santo Tomé y Príncipe	ST	880	10.3%	89.7%
Tailandia	TH	130	10.8%	89.2%
Georgia	GE	162	11.1%	88.9%
Turquía	TR	252	11.5%	88.5%
Isla de Navidad	CX	136	11.8%	88.2%
Guernesey	GG	25	12.0%	88.0%
Uruguay	UY	33	12.1%	87.9%
Laos	LA	122	12.3%	87.7%
Montserrat	MS	213	13.6%	86.4%

El panorama de amenazas cambiante

Los volúmenes de *malware* continúan aumentando en 2010, cuyos primeros seis meses fueron la mitad de año más activa de todos los tiempos con respecto a la producción de *malware*.⁴ Las clases de *malware* están evolucionando y hay más software de ejecución automática (desde los dispositivos de USB), más antivirus falsos (software de alertas falsas), más *malware* de redes sociales y mucho más *spam* creíble y personalizado. Las amenazas avanzadas persistentes (en inglés, *Advanced persistent threats*, APT) pueden combinar diferentes técnicas para hacer funcionar o ejecutar sus ataques, por lo tanto, un sitio web no es más que una parte del rompecabezas de amenazas.

Un tipo de zombi diferente: *malware* que nunca muere

Una de las noticias más importantes de principios de junio fue un ataque masivo de inyección SQL. Un “salpicón” de ataques desde miles de sitios web insertó un iFrame que redirigía a los usuarios a una página maliciosa que luego descargaba y ejecutaba un archivo. Dichos ataques ocurren periódicamente, al menos una vez cada tres meses.

Una vez que el dominio malicioso es derribado, las noticias y las preocupaciones sobre ese ataque en particular pasan a segundo plano. Pero lo que no sabemos es la cantidad de sitios que no se pudieron limpiar luego del ataque. Un mes después del ataque de junio, conocido como www.robint.us, contamos 51,900 sitios que aún estaban infectados con la inyección SQL.

Esta falta de limpieza no es exclusiva. El ataque 2677.in aún redirige a los usuarios en 26,800 páginas web, yahoosite.ru aún tiene efecto en 1,380 sitios, el ataque de killpp.cn de 2008 aún se encuentra presente en 680 páginas y k.18xn.com acosa otros 538 sitios. Es probable que estos problemas empeoren ya que la naturaleza dinámica y fluida de la Web hace que sea sencillo inyectar y ocultar ataques.

—Informe de amenazas de McAfee:
segundo trimestre de 2010

Los sitios de redes sociales facilitan el trabajo del delincuente debido a que los enlaces maliciosos o encubiertos se pueden incluir en las publicaciones y mensajes de los amigos que disfrutan de la “confianza transitiva”. Confío en usted, entonces puedo confiar en sus “recomendaciones”, ¿no es así? Desde 2008, el gusano Koobface ha estado atacando estas redes de confianza para encontrar nuevas víctimas para sus códigos maliciosos y nuevos bots de zombis para sus redes de bots.⁵ Hubo una gran actividad del gusano Koobface en 2010. Clasificamos 315,415 URL como maliciosas en relación a Koobface. Más del 14% de estas URL (45,213) estuvieron dentro de nuestro TLD más riesgoso, .COM, sin concentración significativa dentro de otros TLD.

El segundo TLD más riesgoso del año fue un microcosmos de este torbellino de *malware*: .INFO. Hacer clic en un enlace con este dominio arrojó una probabilidad del 47% de llevarnos a una página de riesgo. Cuando investigamos las clases de amenazas para .INFO, la gran mayoría se marcó como riesgosa debido a cómo se registraron y a las reputaciones de su dominio, derivadas de nuestra base de datos de actividades sospechosas observadas a lo largo del tiempo.

El siguiente factor de riesgo de .INFO fueron los sitios maliciosos. Algunos de estos sitios funcionan como *malware*, ataques o una combinación de ambos. Algunos funcionan como servidor de comando y control, servidor comprometido o dominio sobre un servidor apropiado por el *bot*. Muchos sitios contienen descargas de antivirus falsos (también conocidos como *scareware* y software de alerta falsa) y el *malware* de la red de bots de Zeus, que refleja las actividades dominantes en el panorama general de las amenazas.

Las redes de *bots* de Zeus usan técnicas especiales y sofisticadas para esquivar los fuertes sistemas de autenticación usados en las operaciones bancarias online, que incluyen contraseñas de un solo uso, y así suponen una amenaza grave y peliaguda para los consumidores y las empresas. Por último,

los sitios de *phishing* representan un porcentaje significativo de los sitios en rojo de .INFO.

Cuanto más trabajamos, más trabajo tenemos

Debido a que los responsables de los registros de TLD ajustan las restricciones para el uso de sus dominios, los delincuentes buscan otras formas de atacar la Web. Los conjuntos de herramientas de *malware* fácilmente disponibles se conectan con tecnologías de la Web 2.0 inseguras, tales como AJAX, XML, Flash, iFrames y JavaScript, y con los sitios web, equipos y navegadores con poco mantenimiento o poco configurados. Las combinaciones infinitas de herramientas y vulnerabilidades de software facilitan la incorporación de contenidos de riesgo dentro de dominios que de otra manera serían legítimos. Estos contenidos invisibles no exigen que el usuario “haga clic para descargar” para atacar las vulnerabilidades en el navegador.

Por ejemplo, un pirata cibernético puede usar un ataque especial llamado inyección SQL para implantar un tipo específico de código invisible llamado iFrame. El iFrame, que puede ser más pequeño que un píxel y esconderse detrás de otras imágenes o ventanas emergentes, incluye una URL que de forma silenciosa redirige al usuario a un sitio donde puede recibir contenidos maliciosos.

En un intento por desbaratar las detecciones del navegador de URL falsas, el iFrame incorporado puede usar servicios de URL de restricción tales como bit.ly o Tinyurl para encubrir la URL.

Los servicios de URL de restricción intentan hacer un mejor trabajo para reconocer este abuso, pero sus esfuerzos se han eludido fácilmente. Por ejemplo, los delincuentes pueden detectar un lugar de origen de los visitantes y seleccionar únicamente el tráfico que quieren conectar con su sitio.

⁴ Informe de amenazas de McAfee: segundo trimestre de 2010, se puede descargar en varios idiomas desde http://www.mcafee.com/us/threat_center/white_paper.html

⁵ Craig Schmagar, “Koobface remains active on Facebook” (Koobface permanece activo en Facebook), McAfee Labs Blog, www.avertlabs.com/research/blog/index.php/2008/12/03/koobface-remains-active-on-facebook/

Por medio del redireccionamiento de sitios, el atacante separa el contenido de la línea inicial de ataque. Por lo tanto, se puede volver a utilizar el contenido en esfuerzos en serie y también se pueden realizar pequeñas modificaciones en las versiones o cambios para evitar las herramientas de detección basadas en la frecuencia. ¿El sabor de Koobface o Zeus se está tornando demasiado conocido? Pruebe esto para cambiar un poco.

Movimientos rápidos, objetivos específicos

Es posible introducir material malicioso en sitios poco protegidos, así como cualquier contenido generado por usuarios, ya sea un archivo JPEG, un blog o un foro. Si bien los sitios con poco mantenimiento suelen hospedar *malware* conocido durante meses o años (consulte el recuadro de la página 21), algunos de los actores de amenazas más astutos aparecen y desaparecen en pocas horas. Un centro de red de *bots* de comando y control puede estar “despierto” solamente cinco minutos por día.

Para protegerse de estas actividades fugaces, pero lucrativas, se deben actualizar con frecuencia las evaluaciones en el nivel de las URL y de las rutas. Por eso, los usuarios de la Web se ven beneficiados por las inspecciones de contenido (análisis de los últimos *malware*) realizadas en tiempo real.

Tras introducir *malware* en un sitio, los términos de búsqueda infectados continúan siendo la forma más popular, y sutil, para los delincuentes a la hora de dirigir el tráfico a sus sitios. Los delincuentes prestan especial atención a los desastres, las aventuras de los famosos, los eventos deportivos y otros temas de

actualidad. Crean publicidades y fabrican sitios web con términos populares, hacen que aparezcan en los índices de los motores de búsqueda, luego usan redes de *bots* y hacen clic en motores para llevar su contenido a la primera página en los resultados de búsqueda. Cuando los usuarios hacen clic en esos elementos en los resultados de la búsqueda, viajan a sitios donde obtienen descargas maliciosas. Un sitio malicioso puede ser nuevo, estar creado con un propósito y tener contenidos actuales, o puede ser un sitio inocente que ha sido pirateado.

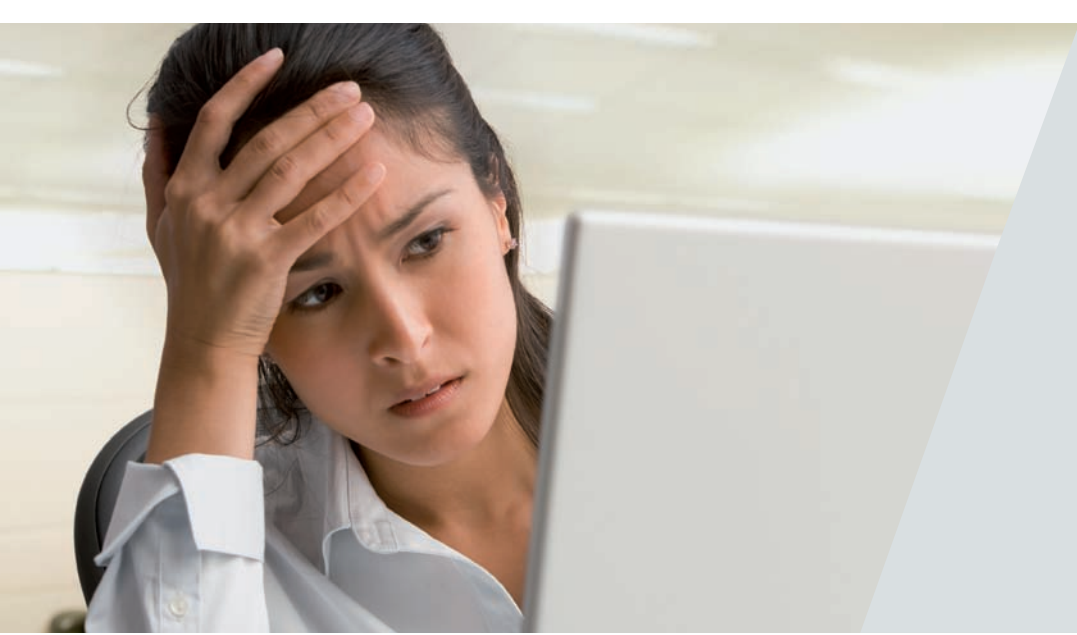
Cualquiera de estos enfoques y todos ellos logran su objetivo con información personal, inicios de sesión en cuentas, datos de cuentas sobre amigos, contraseñas y zombis de la red de *bots*.

Ya son móviles

Clasificado en el puesto 33 de riesgos, el TLD de dispositivos móviles (.MOBI) fue uno de los más seguros en la Web este año, pero lo estamos siguiendo de cerca tanto a él como al uso general de la Web móvil. Por ejemplo, en la actualidad los ataques incorporan cada vez más dispositivos móviles. La red de *bots* de Zeus puede solicitar a los usuarios su número de teléfono móvil y un número de autorización y luego usar esa información en una transacción financiera. Si un mensaje *spam* o un formulario de la Web obtiene un número móvil, ese número puede usarse en ocasiones subsecuentes, enviar más *spam*, engaños de *phishing* o enlaces a sitios con *malware*. Los millones de teléfonos inteligentes con acceso a Internet desperdigados por el mundo simplemente aumentan las oportunidades para los estafadores.

“En 2009, 6% de las URL maliciosas identificadas por McAfee para proteger a los usuarios estaban en el nivel de las rutas. Ya en 2010, el porcentaje ha aumentado al 16%”.

—Informe de amenazas de McAfee:
segundo trimestre de 2010



Comentarios de los operadores y encargados de registrar los dominios de más alto nivel

Además de nuestras ideas, queremos ofrecerle algunas perspectivas de la comunidad de TLD de la primera línea de administración de riesgos. Solicitamos comentarios de algunos de los TLD que mencionamos en este informe e incorporamos experiencias, color y contexto a nuestro análisis.

.INFO (Información)

“Como administrador del registro .INFO, Afiliados se compromete a detener la actividad abusiva en el dominio .INFO. Por ese motivo, en el año 2008, establecimos nuestras políticas antiabuso líderes en la industria y hemos estado trabajando con dinamismo junto con nuestros responsables de registros (que venden directamente a los responsables de registros finales) para derrotar el “phishing” y otros abusos.

Desafortunadamente, el aumento en la popularidad de .INFO ha llamado la atención de los creadores de spam y, por consiguiente, hemos comenzado a desplegar algunas tácticas nuevas. Hay mucho por hacer. El desafío es difícil porque como operador de registro de gTLD, Afiliados no puede decidir quién vende los nombres de dominio de .INFO o a quiénes se los venden.

.INFO es el hogar de millones de sitios útiles y legítimos. Por eso, no se aconseja simplemente bloquear correo electrónico según la dirección de TLD, ya que se pueden perjudicar más víctimas inocentes. Por el contrario, los

métodos más sofisticados para filtrar correo electrónico pueden disminuir el daño sin causar efectos secundarios no deseados”.

—Roland LaPlante,
vicepresidente sénior y
gerente de marketing
de Afiliados

.JP (Japón)

“Creo que nuestros esfuerzos continuos para mejorar la seguridad de los nombres del dominio JP han aumentado la confianza de los encargados de registros y los usuarios en dicho dominio.

Para registrar un nombre de dominio JP, debe cumplir ciertos requisitos. Especialmente, el registro de un nombre de dominio JP de tipo organizativo (p. ej.: EJEMPLO.CO.JP) tiene requisitos diferentes según el tipo de dominio (p. ej.: únicamente las empresas que son sociedades anónimas en Japón pueden registrar EJEMPLO.CO.JP).

Si se descubre que un nombre de dominio JP registrado no cumple con estos requisitos, se invalida el registro por medio de los procedimientos adecuados.

En este caso, en el pasado, JPRS como registro verificaba el estado y tomaba medidas para invalidar el nombre, si correspondía, por medio de los responsables de registros JP. En junio de 2008, JPRS reforzó la regla de registro de nombre de dominio JP para CO.JP y permitió que el registro cancele los registros falsos si la cancelación realizada por los responsables de registros no funcionaba. Además, en noviembre de 2009, ampliamos la extensión de la regla a todos los nombres con dominio JP de tipo organizativo y geográfico.

Al reforzar estas reglas, y mediante la cooperación continua con los responsables de los registros JP, JPRS abordó de forma rigurosa y rápida el asunto de los registros falsos.



También tomamos medidas para enfrentar el problema de los nombres de dominio registrados y usados en actividades fraudulentas como el phishing. Con la colaboración de JPCERT/CC y otras organizaciones relacionadas, JPRS examina el grado de malevolencia de los nombres de dominio supuestamente abusados. Si se confirma el abuso del nombre, JPRS le solicita al responsable de registros de JP que invalide el nombre.

Además, JPRS ha implementado continuamente, desde 2006, la eliminación de registros de servidores DNS en los casos en que el nombre de host contenga un nombre de dominio JP inexistente.

Con respecto a las extensiones de seguridad del sistema de nombre de dominio (en inglés, Domain Name System Security Extensions, DNSSEC), planeamos comenzar a firmar la zona JP en octubre de 2010 e introducir DNSSEC en los servicios de nombre de dominio JP en enero de 2011. Además, con el objetivo de promocionar una instrucción para la comunidad y esparcir DNSSEC, en noviembre de 2009 se estableció un foro llamado "DNSSEC de Japón". Uno de los miembros del personal de JPRS trabaja como vicepresidente del foro.

Estos esfuerzos persistentes han dado buenos resultados; por ejemplo, la cantidad de reclamos por phishing que recibe JPRS se ha reducido bastante, aproximadamente a un reclamo por mes".

—Yumi Ohashi
Gerente de relaciones
internacionales y gubernamentales
JPRS

.SG (Singapur)

"El Centro de información de red de Singapur (en inglés, Singapore Network Information Centre, SGNIC) estimula a las empresas y a los individuos a adoptar y usar nombres de dominio .SG. De esta forma, además de identificarse mejor con los usuarios y consumidores de Singapur, podrían ampliar su presencia en el mercado global.

Quienes visitan un sitio .SG pueden estar seguros de que está regulado por los requisitos de registro de SGNIC para garantizar la responsabilidad. Eso se debe a que quien solicita un nombre de dominio .SG debe presentar la documentación adecuada cuando quiera registrar un nombre de dominio bajo las diferentes categorías de nombres .sg, que reflejan su estado como entidad. Por ejemplo, un responsable de registros ".com.sg" podría necesitar proporcionar pruebas de que es una entidad comercial registrada con la Autoridad Reguladora Contable de Singapur (ACRA) o cualquier organismo profesional, mientras que un responsable de registros ".EDU.SG" debe registrarse en el Ministerio de Educación o ser reconocido por otras agencias relevantes. En el caso de los registros de corporaciones extranjeras, las solicitudes deben estar respaldadas por una dirección de contacto en Singapur.

Cuando SGNIC reciba críticas adversas sobre el uso de un nombre de dominio ".SG", investigará inmediatamente, trabajará con sus responsables de registros y, cuando sea adecuado, consultará a las agencias relevantes para garantizar el cumplimiento de sus reglas de registro. Cualquier nombre involucrado en casos de malas interpretaciones o fraude, o que se use para hospedar material que infrinja las leyes o normas de las autoridades reguladoras rectificadas por los responsables de los registros, en caso de incumplimiento, será suspendido o eliminado por SGNIC. Debido a que el contenido de Internet puede hospedarse en cualquier parte, incluso luego de que se haya registrado un nombre en Singapur, SGNIC trabaja de forma activa con la comunidad internacional de Internet, incluidos los grupos especializados en estabilidad y seguridad de Internet, para supervisar y prevenir el posible abuso de nombres de dominio ".SG".

SGNIC cree que estas medidas han ayudado a asegurar que los nombres de dominio ".SG" continúen siendo seguros y que se usen con propósitos legales".

—Mr. Lim Choon Sai
Gerente general
Singapore Network Information Centre
Pte Ltd.



.WS (Samoa Occidental)

“En el transcurso del último año, nos hemos centrado en reducir la cantidad de dominios de riesgo bajo nuestro TLD .WS mediante la aplicación de verificaciones adicionales y módulos de seguridad en nuestra infraestructura de registros. La supervisión proactiva de los responsables de registros de dominio nos permite evitar que el contenido malicioso se vuelva público.

También nos hemos asociado con empresas de seguridad online establecidas para implementar un sistema mejorado de críticas que nos notificará rápidamente acerca de dominios posiblemente maliciosos que luego podrán detectar quienes ingresen al sitio web. A medida que sabemos más acerca de cómo se crean y se activan las amenazas online, somos capaces de identificar y neutralizar posibles problemas antes de que causen daños. Junto con esta información y fortaleciendo los lazos con nuestros responsables de registros .WS acreditados, hemos logrado desarrollar un sistema de notificación para informar a los responsables de registros acerca de posibles registros de nombres de dominio maliciosos. De la misma manera, también se encuentra activo un servicio para notificar a los hosts de la Web que brindan servicios de host para dominios .WS. Para combatir el correo electrónico spam, la supervisión avanzada de la actividad del correo electrónico de nuestros servidores permite reconocer rápidamente a los remitentes de correo no deseados y evitar que logren su objetivo.

Como Registro oficial para el dominio de nivel superior .WS, siempre hemos valorado nuestra reputación en toda la comunidad online desde que lanzamos la zona hace más de una década. Global Domains International fue una de las primeras empresas que formó parte del grupo de trabajo de Conficker en el nivel de Registro. Trabajamos con ellos ayudándolos en sus esfuerzos para identificar el gusano y mitigar su daño, y lo seguimos haciendo para asegurarnos de que nuestro TLD .WS no se use para proliferar la amenaza de Conficker.

Las modificaciones de nuestro sistema de registro se transforman continuamente para ser congruentes con las tácticas de abuso, que cambian continuamente. Al familiarizarnos con los métodos populares usados por quienes intentan participar en actividades maliciosas online, podemos garantizar integridad y seguridad dentro de la zona de .WS”.

—Alan Ezeir
Presidente
Global Domains International

Conclusión

El nivel de riesgo aumenta mientras los tipos de riesgo en la Web cambian cada vez más rápido. Debido a que los delincuentes encuentran maneras de sepultar y encubrir sus actividades, los usuarios de la Web deben encontrar nuevas formas de mantenerse al margen de estas amenazas y a la vez conservar la alegría y el valor de navegar en la Web.

Los consumidores tal vez no recuerden todos los lugares de riesgo mencionados en este informe. Incluso si pudieran, hemos demostrado que el TLD más riesgoso de un año puede ser mejorado al año siguiente. Los consumidores pueden evitar los lugares peligrosos de la Web si usan software de seguridad de confianza y actualizados en los equipos con funciones de búsqueda seguras, como McAfee Total Protection™. En este caso, es muy buena idea permitir la colaboración de la tecnología.

Las empresas saben que actualmente la Web es fundamental para sus operaciones y que muchos empleados sienten que tienen derecho de acceder a la Web mientras trabajan. Esta expectativa aumentará a medida que el trabajo y el hogar se entremezclen con un personal más móvil y remoto, un mayor uso de dispositivos personales y un cambio implacable hacia la conexión continua. La forma más simple de ayudar a los usuarios a manejar los riesgos de la Web consiste en agregar la funcionalidad de la reputación de la Web a sus otras defensas. Las indicaciones visuales actualizadas en tiempo real pueden ayudar a educarlos sobre los riesgos y, a la vez, protegerlos de ellos.

Los operadores de TLD de riesgo deben encontrar esperanza en este informe. Es muy posible revertir una reputación riesgosa o mantener una buena reputación. Las empresas dedicadas a la seguridad como McAfee se comprometen a ayudarlo. Con la red de inteligencia global contra amenazas más amplia del mundo, le podemos ofrecer datos actualizados sobre lo que ocurre e ideas inteligentes acerca de lo que puede hacer para reducir su exposición.

El próximo año, quizá nos encontremos con que las redes de bots de zombis se sustituyeron por una táctica nueva que dependa de cientos de millones de dispositivos móviles con capacidad de datos en todo el mundo. El año que viene, esperamos informar el progreso y las medidas para contrarrestarlo creadas por los responsables de registros de TLD y la comunidad de seguridad.

Acerca de McAfee, Inc.

McAfee, Inc., con sede en Santa Clara, California, es la empresa dedicada a la tecnología de seguridad más importante del mundo. La empresa brinda servicios y soluciones proactivas y comprobadas que ayudan a hacer más seguros los sistemas, las redes y los dispositivos móviles en todo el mundo, y permiten a los usuarios conectarse, navegar y comprar en Internet con mayor seguridad. Respaldada por el inigualable McAfee Global Threat Intelligence, McAfee crea productos innovadores que ayudan a los usuarios, las empresas, el sector público y los proveedores de servicios al permitirles cumplir con las regulaciones, proteger datos, prevenir interrupciones, identificar vulnerabilidades y controlar y mejorar continuamente la seguridad. McAfee asegura su mundo digital.

<http://www.mcafee.com>



La información incluida en este documento se proporciona sólo con fines educativos y para la conveniencia de los clientes de McAfee. La información incluida en este documento está sujeta a cambios sin aviso previo, y se proporciona "EN ESTAS CONDICIONES" sin garantía con respecto a la exactitud o utilidad de la información de cualquier situación o circunstancia específica.

McAfee, el logotipo de McAfee, McAfee Global Threat Intelligence, McAfee Labs y McAfee Total Protection son marcas registradas o marcas comerciales de McAfee, Inc. o sus filiales en los Estados Unidos y en otros países. Otras marcas pueden reclamarse como propiedad de otros. Los planes, las especificaciones y las descripciones del producto en este documento han sido proporcionados sólo con fin informativo y están sujetos a cambios sin previo aviso, y se proporcionan sin ningún tipo de garantía, expresa o implícita. Copyright © 2010 McAfee, Inc.

10902rpt_mapping-mal-web_0910