

Conclusiones principales

Mapa de sitios web maliciosos

Los dominios más peligrosos del mundo



Los lugares de la Web más peligrosos

He aquí una situación real. Tu nuevo amigo de Facebook te envía un enlace o bien realizas una búsqueda en la red que te lleva a una fotografía graciosa de Cameron Diaz. ¿Deberías abrir el enlace o cerrarlo?

Hacer clic en resultados de búsqueda al azar es como jugar a la ruleta rusa con tu ordenador, tu privacidad y tu identidad. Teniendo en cuenta los resultados de este año, sería el equivalente a tener una de 16 recámaras cargadas.

En algún lugar de tu mente, recuerdas ese consejo: "Piensa antes de hacer clic". Este "amigo" podría ser un estafador cibernético, y ese enlace podría llevarte a un sitio que instalará un pequeño programa malicioso llamado Koobface (anagrama de Facebook). ¿Cuál es la decisión segura? ¿Cómo elegir?

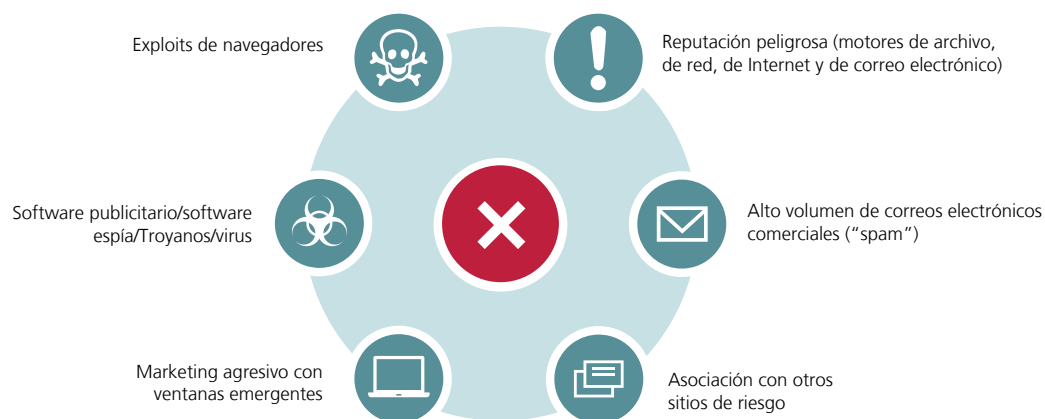
¿Qué dirías si te dijéramos que las letras al final de la URL son de *gran* ayuda para tomar la decisión correcta? ¿Qué dirías si te dijéramos que entre estos cuatro sitios...

- Yourfavoritestore.jp
- Yourfavoritestore.info
- Yourfavoritestore.fr
- Yourfavoritestore.hk

... uno de ellos es 100 veces más probable que contenga software malicioso que puede enviar correo no deseado, vulnerar la seguridad de tu navegador, o algo peor?

Esas letras .JP para Japón, .INFO para los dominios de información genérica, .FR para Francia, .HK para Hong Kong, y más de 200 otros, incluidos .COM y .EDU se denominan dominios de nivel superior (TLD por sus siglas en inglés). Estas letras son una porción de información vital que la red utiliza para organizar sus direcciones y que proporciona indicios esenciales acerca de dónde es conveniente hacer clic.

Amenazas a la seguridad evaluadas por McAfee® Global Threat Intelligence™



El nivel de riesgo se calcula teniendo en cuenta múltiples características de cada sitio web, incluida su reputación por buen comportamiento y actitudes transparentes: asociaciones correctas o nocivas con otros sitios y servicios de Internet.



Por cuarto año consecutivo, McAfee ha estudiado millones de sitios web (¡27 millones este año!) para crear el “Mapa de sitios web maliciosos”. Este año, el riesgo alcanzó los niveles más altos: un 6,2% de los sitios web evaluados presentaron signos de riesgo (comparado con un 5,8% en 2009 y un 4,1% en los dos años anteriores).

Lo que no sabes es que los estafadores, los jefes de la ciberdelincuencia, los hackers y otros de estos personajes malintencionados son selectivos. Prefieren algunos TLD (dominios de nivel superior) a otros. Y McAfee ha descubierto cuáles.

Resulta ser que los estafadores y los hackers registran sus operaciones en los lugares donde es más sencillo hacer negocios o donde advierten posibilidades ventajosas debido a errores de escritura o a asociaciones lógicas. Por ejemplo, dado que es fácil omitir la “O” en una dirección .COM, un jugador inescrupuloso podría registrar la dirección www.mcafee.cm en Camerún (.CM) esperando obtener tráfico de cualquiera que se preocupe por la seguridad.

¿Por qué debería interesarme?

El sólo hecho de ver una página web puede ejecutar códigos maliciosos que roban tu contraseña y tu información de identificación, se aprovechan de las brechas de seguridad que pueda haber en tu ordenador, o directamente toman posesión del mismo. Y puede resultar costoso, avergonzante y realmente difícil recuperar tu ordenador (o tu identidad).

Creemos que, si sabes con anterioridad que tres de cada cinco sitios en un TLD son peligrosos, puedes elegir otro lugar desde donde descargar esa fotografía que estás buscando. Por ejemplo, a pesar del creciente atractivo de Vietnam como destino de vacaciones, quienes visiten sitios registrados en Vietnam (.VN) deberían considerarlo una zona para no visitar. Este año, .VN apareció en nuestra lista de los cinco TLD más peligrosos de Internet, después de que registráramos que un 58% de los sitios que rastreamos incluían contenidos y actividades dañinos, tanto real como potencialmente.



Este año, Vietnam (.VN) apareció en nuestra lista de los cinco TLD más peligrosos, después de que registráramos que un 58% de los sitios que rastreamos incluían contenidos y actividades dañinos, tanto real como potencialmente.



Resultados del año 2010

En general, las amenazas de Internet van en aumento. Los delincuentes trabajan para lograr que sus actividades se vuelvan más difíciles de detectar... y de vigilar.

- **El riesgo va en aumento.** La media total ponderada de sitios web peligrosos aumentó de 5,8% (2009) a 6,2% (2010). Navegar por la red en modo seguro se está volviendo cada vez más difícil, incluso para los usuarios más experimentados.
- **Tráfico intenso = riesgo alto en .COM.** Con una probabilidad de 3 sobre 10 de llegar a un sitio peligroso, .COM (Comercial, el TLD con mayor tráfico) era el TLD más peligroso este año (de acuerdo con nuestro sistema de riesgo ponderado).¹ El software malicioso Koobface, un código peligroso que se difunde a través de los sitios de redes sociales como Facebook y Twitter, se asociaba más a los .COM que a cualquier otro TLD.
- **.INFO registra información peligrosa.** .INFO (Información) escaló hasta el segundo lugar desde el quinto que ocupaba el año pasado. Quienes envían correos no deseados continúan plagando este TLD. Muchos sitios peligrosos .INFO contribuyen

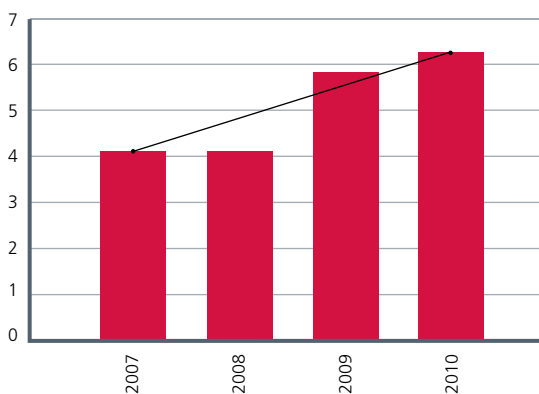
a aumentar el riesgo hospedando contenido que luego se utiliza para campañas de correos no deseados que publicitan desde productos farmacéuticos y relojes hasta software malicioso y antivirus falsos.

- **Los peores agresores.** En total, los cinco TLD con mayor porcentaje de registros peligrosos fueron:

o .COM (Comercial)	31,3%
o .INFO (Información)	30,7%
o .VN (Vietnam)	29,4%
o .CM (Camerún)	22,2%
o .AM (Armenia)	12,1%
- **Un mundo de riesgos.** Nuestros TLD con mayor riesgo incluyen TLD de tres continentes, desde Asia hasta Europa y África, y dos TLD genéricos, ambos operados desde América. La región de Europa, Oriente Medio y África (EMEA por sus siglas en inglés) se ha ganado nuevamente la distinción de tener los TLD más peligrosos entre los top 20, con siete participantes, incluyendo los nuevos miembros en la top 20, Armenia (.AM) y Polonia (.PL).
- **Algunas mejoras importantes:** Singapur (.SG) se merece un reconocimiento por haber disminuido el nivel de peligro y haber pasado así del puesto número 10 el año pasado al puesto número 81 este año; Venezuela (.VE) pasó del puesto 21 al 88 este año; y Filipinas (.PH), del número 6 en 2009 al 25 este año.
- **Perfectamente limpios.** Los cinco TLD que registraron la menor cantidad de dominios peligrosos fueron:

o .TRAVEL (Sector de viajes y turismo)	.02%
o .EDU (Educativo)	.05%
o .JP (Japón)	.08%
o .CAT (Catalanes)	.09%
o .GG (Guemesey)	.10%

Porcentaje de sitios peligrosos en la red



¹Lee acerca de cómo calculamos el riesgo en el informe completo, *Mapa de sitios web maliciosos*.

Lecciones que aprender

Si bien los riesgos son altos, si tomas algunas precauciones, podrás navegar y hacer búsquedas en Internet sin preocuparte.

Este año, el 6,2% de los sitios que monitoreamos presentaba contenidos o actividades maliciosas o potencialmente peligrosas, tales como:

- **Software malicioso (malware).** Código que puede dañar tu sistema, robar información, o permitir que tu ordenador sea controlado por un tercero.
- **Exploits de navegadores.** Ataques y malware que se aprovechan del software vulnerable que pueda tener tu ordenador.
- **Phishing** (robo de identidad). Proveniente de la palabra inglesa "fish" (pescar), son sitios falsos diseñados para "pescar" información o instalar códigos maliciosos.
- **Grado de spam.** Formularios de registro que luego generan enormes cantidades de correos electrónicos comerciales, o correo no deseado.
- **Asociaciones de riesgo.** Sitios con enlaces que te llevan a sitios maliciosos, y sitios que tienen relaciones sospechosas, tales como servicios de hosting poco confiables.

- **Presta atención a los TLD.** Fíjate en las credenciales del TLD que encuentres mientras navegues en Internet. Utiliza las tablas a continuación para conducirte en modo seguro y evitar los riesgos.
- **No pienses que los sitios "más populares" son seguros.** Es de esperar que las zonas de mucho tráfico —tales como .COM (el TLD más peligroso) y sitios web que se encuentran en los rankings de popularidad, como *Alexa*— presenten riesgos. Algunos sitios infectados con malware utilizan técnicas de optimización de motores de búsqueda para infiltrarse en los puestos más altos de las clasificaciones en Internet.
- **Desconfía: algunas amenazas son silenciosas.** Introducir contenido invisible en una página web de apariencia inofensiva es muy sencillo y, cuando la visitas, se descargan malware sin que debas hacer clic para aceptar la descarga. Lo mejor es utilizar un software de búsqueda segura, como *McAfee SiteAdvisor*® antes de visitar un sitio nuevo. No hagas clic si el sitio aparece en rojo o en amarillo.
- **Ten cuidado con las páginas peligrosas dentro de dominios seguros.** Las mediciones de nuestros sitios se basan sobre evaluaciones del sitio en su conjunto, y no sobre las mediciones de las páginas por separado. Debes saber que existen riesgos dentro de las URL individuales que se encuentran en dominios que son generalmente seguros. Encontramos, por ejemplo, muchas URL peligrosas a nivel de página en los sitios .EDU (Educativo).
- **Busca amenazas encubiertas.** La URL que ves es sólo la puerta de entrada. Un servicio de abreviación de URL (como *TinyURL* o *biy.ly*) podría ocultar la verdadera ubicación del contenido. Podría estar en cualquier lugar, incluido en un sitio de software para compartir (shareware), como *RapidShare*. Si bien las actualizaciones de antivirus ayudan a combatir algunas clases de contenido malicioso, también necesitas un software de seguridad integral que analice en forma constante los archivos que descargas y que detecte hasta el contenido malicioso más actual. Un ejemplo de esta clase de software es *McAfee Total Protection*™, que analiza cada archivo en búsqueda de las últimas versiones de spyware de carga libre, registradores de pulsaciones, y Troyanos.
- **Elige a tus "amigos" con cuidado.** Muchos usuarios de Facebook aceptan "solicitudes de amistad" de extraños o de amigos de amigos desconocidos. Esta actitud despreocupada hace que el trabajo delictivo se vuelva fácil, ya que los enlaces maliciosos o encubiertos pueden incluirse en publicaciones y mensajes de amigos que gozan de la "confianza transitiva". Confío en ti, por lo que puedo confiar en tus recomendaciones, ¿no es así? Desde el año 2008, el código malicioso *Koobface* se ha aprovechado de estas redes de confianza para encontrar nuevas víctimas.² No aceptes como "amigo" a personas que no conoces.



²Craig Schmutz, "Koobface remains active on Facebook," [Koobface se mantiene activo en Facebook] McAfee Labs blog. www.avertlabs.com/research/blog/index.php/2008/12/03/koobface-remains-active-on-facebook/

Procede con cuidado

Internet se ha convertido en el centro neurálgico de las redes sociales, del entretenimiento y de la información, así como también de la actividad delictiva. El peligro está ampliamente distribuido por toda la red. Los riesgos aumentan, cambian rápidamente y se vuelven así más difíciles de detectar. No obstante, la comunidad de seguridad y la comunidad de entidades de registro TLD sigue combatiendo, y ganando. Algunos de los peores agresores que se incluyeron en el informe del año pasado fueron algunos de los que más mejoraron este año.

Puedes navegar con cuidado —incluso con confianza— si te mantienes atento a las actividades que entrañan riesgos. Y considera adoptar alguna guía en tiempo real. Hoy en día, incluso los usuarios más experimentados se apoyan en la asistencia de un software de seguridad integral y actualizado con función de búsqueda segura.

Para leer el informe *Mapa de sitios web maliciosos* completo y saber más acerca de las amenazas y de cómo combatirlas, visita [McAfee Security Advice Center](#).



Clasificaciones

Los 10 TLD más peligrosos

ALTO RIESGO ■■■■■■ BAJO RIESGO

País o Nombre	Región	TLD	Clasificación de riesgo en el mundo (2010)	Índice de riesgo ponderado (2010)	2010 Índice de riesgo no ponderado (2010)	Clasificación de riesgo en el mundo (2009)	Índice de riesgo ponderado (2009)	Cambios por año en el riesgo ponderado	Total de dominios evaluados	Total de dominios peligrosos
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 (Pacífico Asiático)	VN	3	29.4%	58.0%	39	0.9%	3,107.9% ↑	24,988	14,492
Camerún	EMEA (Europa, Oriente medio y África)	CM	4	22.2%	44.2%	1	36.7%	-39.5% ↓	3,947	1,746
Armenia	EMEA (Europa, Oriente medio y África)	AM	5	12.1%	24.2%	23	2.0%	512.9% ↑	3,145	760
Islas Cocos (Keeling)	APAC (Pacífico Asiático)	CC	6	10.5%	20.2%	14	3.3%	215.4% ↑	58,713	11,869
Pacífico Asiático	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 (Europa, Oriente medio y África)	RU	9	10.1%	16.8%	9	4.6%	116.7% ↑	329,136	55,373
Samoa Occidental	APAC (Pacífico Asiático)	WS	10	8.6%	16.9%	4	17.8%	-51.8% ↓	22,070	3,734

Los 10 TLD más peligrosos

ALTO RIESGO ■■■■■■ BAJO RIESGO

País o Nombre	Región	TLD	Clasificación de riesgo en el mundo (2010)	Índice de riesgo ponderado (2010)	2010 Índice de riesgo no ponderado (2010)	Clasificación de riesgo en el mundo (2009)	Índice de riesgo ponderado (2009)	Cambios por año en el riesgo ponderado	Total de dominios evaluados	Total de dominios peligrosos
Sector de viajes y turismo	Genérico	TRAVEL	106	0.0%	0.0%	92	0.2%	-88.6% ↓	2,013	1
Educativo	Genérico	EDU	105	0.1%	0.1%	102	0.1%	-48.6% ↓	14,002	15
Japón	APAC (Pacífico Asiático)	JP	104	0.1%	0.1%	103	0.1%	6.6% ↑	464,408	547
Catalán	Patrocinado	CAT	103	0.1%	0.2%	99	0.1%	-31.6% ↓	3,936	7
Guemesey	EMEA (Europa, Oriente medio y África)	GG	102	0.1%	0.2%	57	0.6%	-81.1% ↓	12,092	25
Croacia	EMEA (Europa, Oriente medio y África)	HR	101	0.1%	0.2%	100	0.1%	-11.1% ↓	22,511	50
Irlanda	EMEA (Europa, Oriente medio y África)	IE	100	0.1%	0.2%	101	0.1%	-5.7% ↓	32,120	71
Suiza	EMEA (Europa, Oriente medio y África)	CH	99	0.1%	0.3%	95	0.2%	-13.3% ↓	217,863	572
Australia	APAC (Pacífico Asiático)	AU	98	0.2%	0.3%	93	0.2%	-4.3% ↓	256,103	871
Eslovenia	EMEA (Europa, Oriente medio y África)	SI	97	0.2%	0.4%	79	0.3%	-36.6% ↓	11,339	48

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. McAfee proporciona 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 incomparable McAfee Global Threat Intelligence, McAfee crea productos innovadores que ayudan a los usuarios, las empresas, el sector público y los proveedores de servicios, permitiéndoles cumplir con las normativas, proteger datos, prevenir interrupciones, identificar vulnerabilidades, así como controlar y mejorar continuamente la seguridad. McAfee asegura tu mundo digital.

www.mcafee.com



McAfee, Inc.
2821 Mission College Blvd
Santa Clara, CA 95054
1.866.622.3911
www.mcafee.com

McAfee, Inc. La información incluida en este documento se proporciona sólo con fines educativos y para la conveniencia de los clientes de McAfee. La información aquí contenida está sujeta a cambios sin previo aviso y se proporciona "TAL COMO ESTÁ", sin garantía ni aval en cuanto a la precisión o la aplicabilidad de la información relacionada con 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 subsidiarias en los Estados Unidos y en otros países. Otras marcas pueden reclamarse como propiedad de otros. Los planes, especificaciones y descripciones de los productos aquí mencionados se ofrecen sólo con fines informativos, están sujetos a cambio sin previo aviso y se proporcionan sin garantía de ningún tipo, ya sea expresa o implícita. Copyright © 2010 McAfee, Inc.

14602rpt_mtmw-key-takeaways_0910