Informe de seguridad

BLUE COAT®

La seguridad fortalece el negocio

NO PASAR

Una investigación de Blue Coat traza un mapa de las zonas más turbias de la Web

Septiembre de 2015

HALLAZGOS CLAVE

- En los últimos dos años hubo una explosión de dominios de nivel superior nuevos.
- Las políticas poco estrictas de algunas de las organizaciones que los administran generan zonas peligrosas.
- La actividad maliciosa sigue aumentando.
- Los chicos malos siempre necesitan un nuevo suministro de dominios para hacer de las suyas.

Introducción

Es posible que muchos usuarios, cuando hacen clic en un enlace, no presten atención a las letras que están después del "." en la dirección de un sitio web. Es posibe que no sepan que esas simples letras representan un dominio de nivel superior (TLD) (básicamente una "zona" de direcciones) que mantiene un grupo o una empresa específicos. Tal como sucede en el mundo físico, el riesgo relativo de visitar un sitio web de una de estas zonas puede variar notablemente según quién administra a los "residentes" de ese lugar.

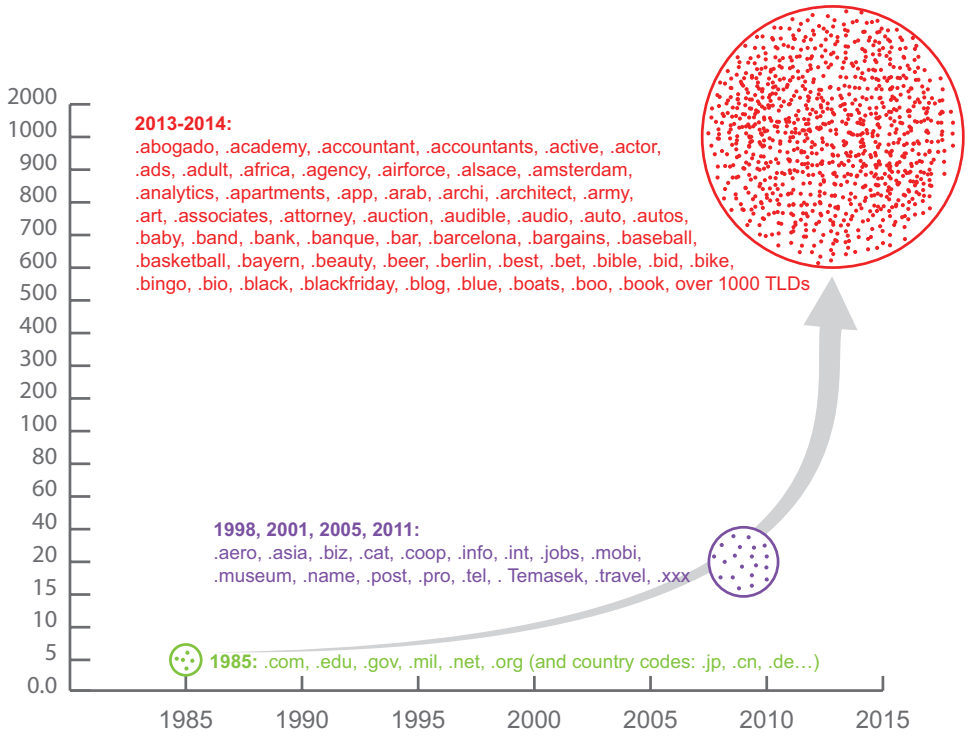
Durante los últimos dos años, hubo una explosión de zonas nuevas en la Web, muchas de las cuales no son ni seguras ni amigables. Muchas cosas cambiaron desde los primeros días de Internet, cuando la Web tenía solo seis dominios de nivel superior (TLD) comunes. En ese entonces, la mayoría de los consumidores y las empresas encontraban solo unos pocos TLD estándares, como .com, .net, .org, .edu,.gov, y algunos dominios de "código de país", como .fr (Francia) y .jp

No obstante, desde el año 2013, el total de TLD creció desmesuradamente. Hasta mediados de agosto de 2015, el conteo de TLD válidos emitidos era de más de mil. A medida que creció la cantidad de TLD también aumentaron las oportunidades para los atacantes.

Las empresas y los consumidores necesitan mayor orientación para comprender qué tan seguros o qué tan peligrosos son estos nuevos TLD, en lo que respecta a seguridad Web. En un mundo ideal, los TLD serían ejecutados por operadores que tienen en cuenta la seguridad, revisan diligentemente las nuevas aplicaciones de nombres de dominio y rechazan las que no cumplen con un conjunto de criterios estrictos. La realidad, en muchas de estas zonas, es que esto no está sucediendo.

Sobre la base de un análisis de solicitudes web de más de 15 000 empresas y 75 millones de usuarios, los investigadores de Blue Coat crearon una lista de las zonas más peligrosas y más seguras de la Web.

La gran explosión de TLD



En sus inicios, la Web estaba limitada a seis TLD normales y aproximadamente 100 TLD de “código de país”. La situación continuó así durante una década, período en el cual se agregaron unos pocos TLD adicionales en 1998, 2001, 2005; algunos de estos probablemente sean conocidos para muchos usuarios (.info, .biz, .mobi, .name, .pro) y otros no tanto (.aero, .asia, .cat, .coop, .int, .jobs, .museum, .tel, .travel, .post). El infame “.xxx” se agregó en 2011.

Luego se produjo una explosión: en 2013 y 2014 se aprobaron más de 600 TLD nuevos y la tendencia continuó en 2015. A principios de 2015, el conteo de TLD válidos era de 795 (incluidos los códigos de país) y para mediados de agosto, el conteo era de más de mil.

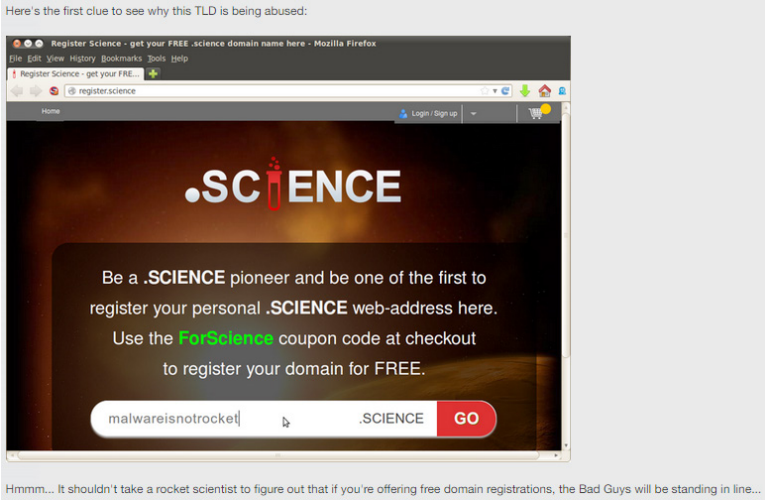
Las políticas poco estrictas para comprar TLD constituyen un peligro

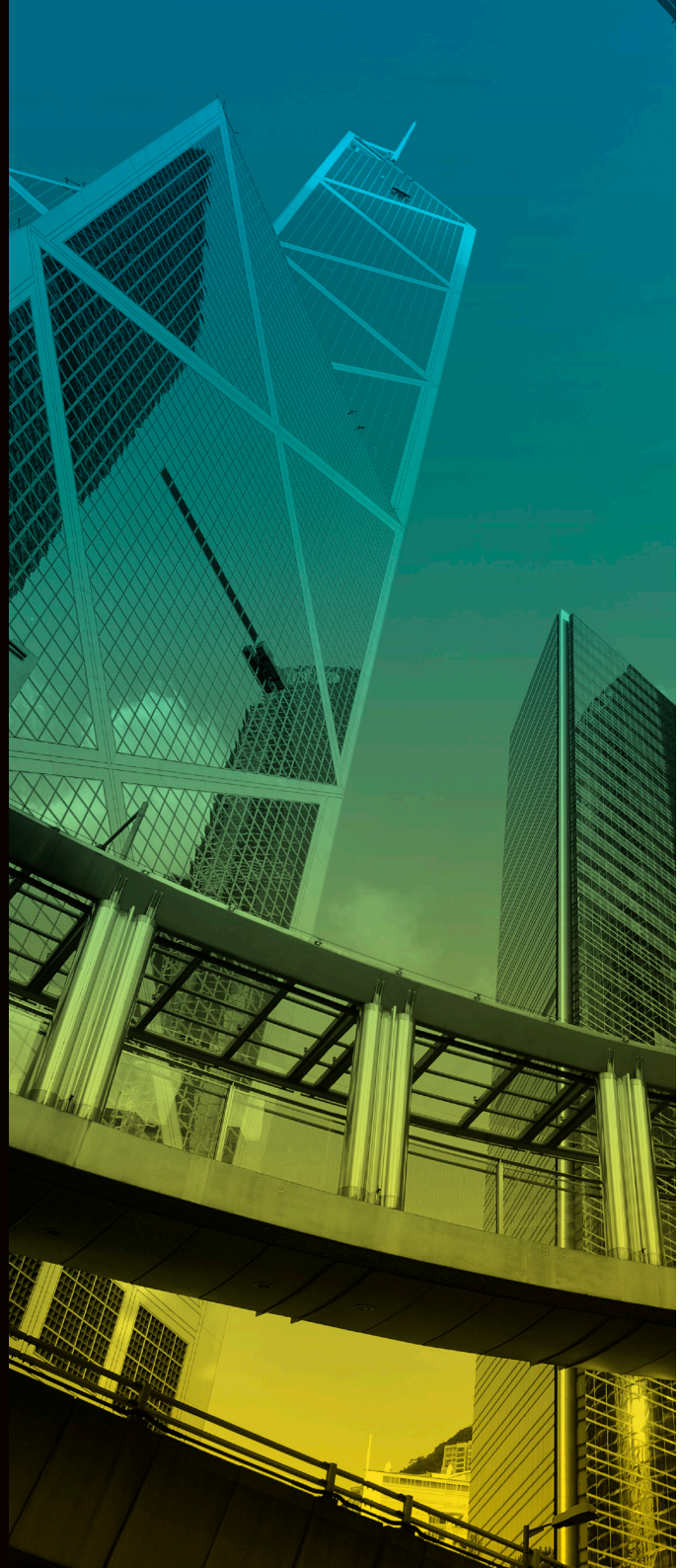
El aumento dramático de TLD nuevos puede atribuirse a una nueva iniciativa de dominios de nivel superior genéricos (gTLD) lanzada por la Corporación de Internet para la Asignación de Nombres y Números (ICANN) en el año 2012. El documento de la ICANN con Preguntas frecuentes sobre los gTLD describe la meta original de la iniciativa:

> *“Uno de los propósitos clave de la ICANN es promover la competencia en el mercado de nombres de dominios y, al mismo tiempo, garantizar la seguridad y la estabilidad de Internet. Los nuevos dominios de nivel superior genéricos (gTLD) ayudan a alcanzar ese propósito; posibilitan que haya mayores opciones para el consumidor, facilitando la competencia entre proveedores de servicio de registro. En poco tiempo, emprendedores, empresas, gobiernos y comunidades de todo el mundo podrán presentar una solicitud para operar un registro de dominio de nivel superior de su elección”.*

Cada TLD nuevo se encuentra bajo el control de una organización que debe pagar una cuota de evaluación inicial de USD 185 000 a ICANN y que además debe probar que cuenta con la infraestructura y la pericia para ejecutar un nuevo registro de TLD.

Lo ideal sería que todos estos nuevos registros (y todos los registros de código de país) apliquen el mismo nivel de precaución a la hora de permitir que alguien compre dominios en su nuevo espacio, pero muchos no lo hacen, y los “chicos malos” saben dónde comprar.





A los fines de esta investigación, consideramos que un dominio es “turbio” si está clasificado en nuestra base de datos como:

Más común	Menos común
Correo no deseado	Malware
Estafa	Botnet
Sospechoso	Phishing (suplantación de identidad)
Software posiblemente no deseado (PUS)	

Cualquier dominio de la base de datos que no tenga alguna de estas categorías se consideró “no turbio”. Nuestro deseo es que los TLD calificados como turbios sigan el ejemplo de los TLD más seguros; con un poco de esfuerzo es posible que los impostores queden fuera de juego.

Los 10 principales“TLD con sitios turbios*” de la Web

Puesto	Nombre de dominio de nivel superior	Porcentaje de sitios turbios
1	.zip	100,00 %
2	.review	100,00 %
3	.country	99,97 %
4	.kim	99,74 %
5	.cricket	99,57 %
6	.science	99,35 %
7	.work	98,20 %
8	.party	98,07 %
9	.gq (Guinea Ecuatorial)	97,68 %
10	.link	96,98 %

** Hasta el 15 de agosto de 2015 – Los porcentajes se basan en categorizaciones de sitios web efectivamente visitados por nuestros 75 millones de usuarios. Un TLD con un porcentaje de 100 por ciento de sitios turbios se correlaciona con los sitios categorizados por Blue Coat.*

Los investigadores de Blue Coat analizaron decenas de millones de sitios web solicitados por 75 millones de usuarios de todo el mundo para clasificar los TLD que presentan mayor riesgo de amenaza a los visitantes. Todos los TLD mencionados arriba tienen más del 95 % de sus sitios con calificaciones turbias en nuestra base de datos principal. Es decir, la mayoría de los sitios que utilizan estos TLD que obtuvieron una calificación en la base de datos se clasificaron como turbios (por ejemplo, malware, correo no deseado, estafa, phishing, sospechoso, etc.). Cada uno de estos TLD tiene cientos, miles o decenas de miles de sitios web calificados y menos del 5 % de estos se clasificaron como normales.

Ejemplos de actividad de riesgo

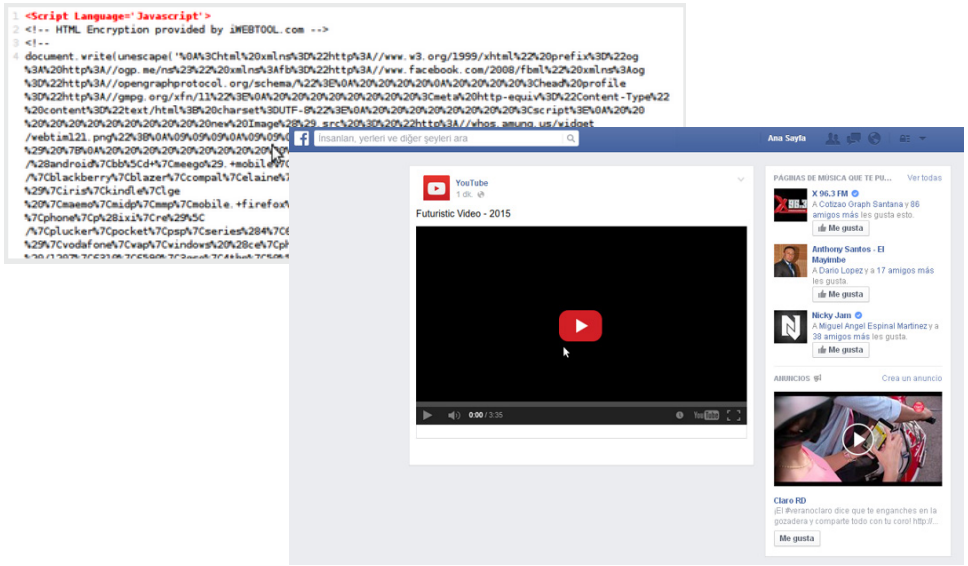
Los TLD turbios son suelo fértil para la actividad maliciosa. La mayoría de estos sitios web están siendo aprovechados por atacantes en correo no deseado y estafas y para distribuir software posiblemente no deseado. Otros están relacionados con la optimización o el posicionamiento de los motores de búsqueda, u otros "sitios basura" que se clasificarían como sospechosos.

Los chicos malos siempre necesitan un nuevo suministro de dominios para hacer de las suyas. La investigación anterior de Blue Coat "Estrellas por un día: cómo se oculta el malware entre sitios web fugaces de Internet", analizó en profundidad la manera en que la mayoría de los sitios de la Web existen menos de 24 horas.

Los enlaces a estas ubicaciones se incluyen en las campañas de correo no deseado y cambian rápidamente para aumentar las posibilidades de evadir las defensas de seguridad antes de que se actualicen. La explosión de TLD nuevos proporcionó un suministro casi ilimitado de sitios "estrella por un día" para el ataque.

Una campaña reciente contra el malware muestra de qué manera se utiliza el TLD .kim para actividad corrupta:

Se determinó recientemente que sitios como buu.kim y newido.kim son utilizados por páginas con un Javascript oculto que produjo páginas como la siguiente:



La mayor parte del contenido de estas páginas consiste en realidad en archivos de imagen alojados en un sitio malicioso denominado fourapp.info. Las personas que visitan estas páginas y no cuentan con protección reciben una solicitud para descargar el malware.

En una falsificación diferente con un ataque mediante un video falso, el sitio ".country" (que según las investigaciones de Blue Coat es el de mayor tráfico) un día de mediados de junio formó parte de una red de estafa de un "video asombroso":

Esta estafa cada vez más común guiaba a los visitantes hasta una "página atractiva" generalmente diseñada para que el usuario crea que está visitando YouTube cuando, en realidad, se encuentra en un sitio falso que no tiene enlace legítimo con YouTube. Inmediatamente debajo del video que no funciona aparecen comentarios falsos de alguien que quiere saber cómo reproducir el video y de otra persona que explica que primero debe "compartir" o "dar me gusta" en el video, o bien, responder una encuesta en línea. Cuando los visitantes siguen estas instrucciones, divulgan datos personales en la encuesta, o bien, los estafadores envían correo no deseado a sus amigos de Facebook.

En la imagen n.º 1 se muestra un ejemplo de lo que los usuarios creían que era un "asombroso" video pornográfico. La imagen utilizada a modo de atracción se cubrió de negro.

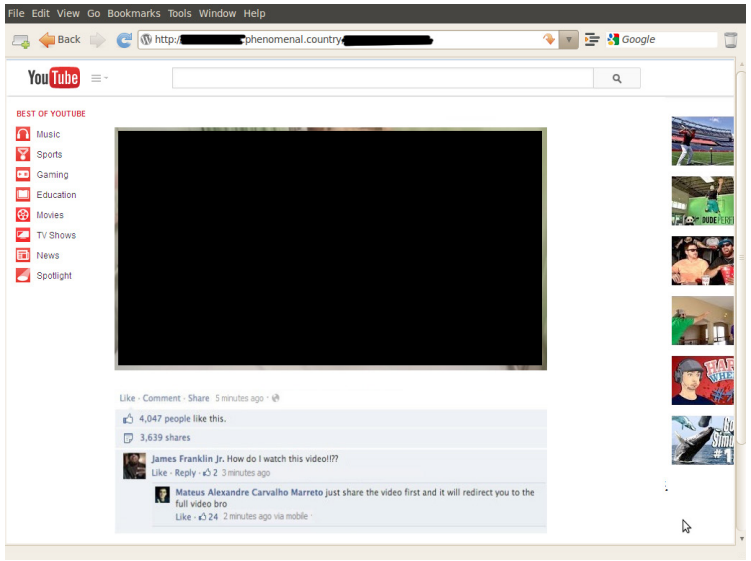
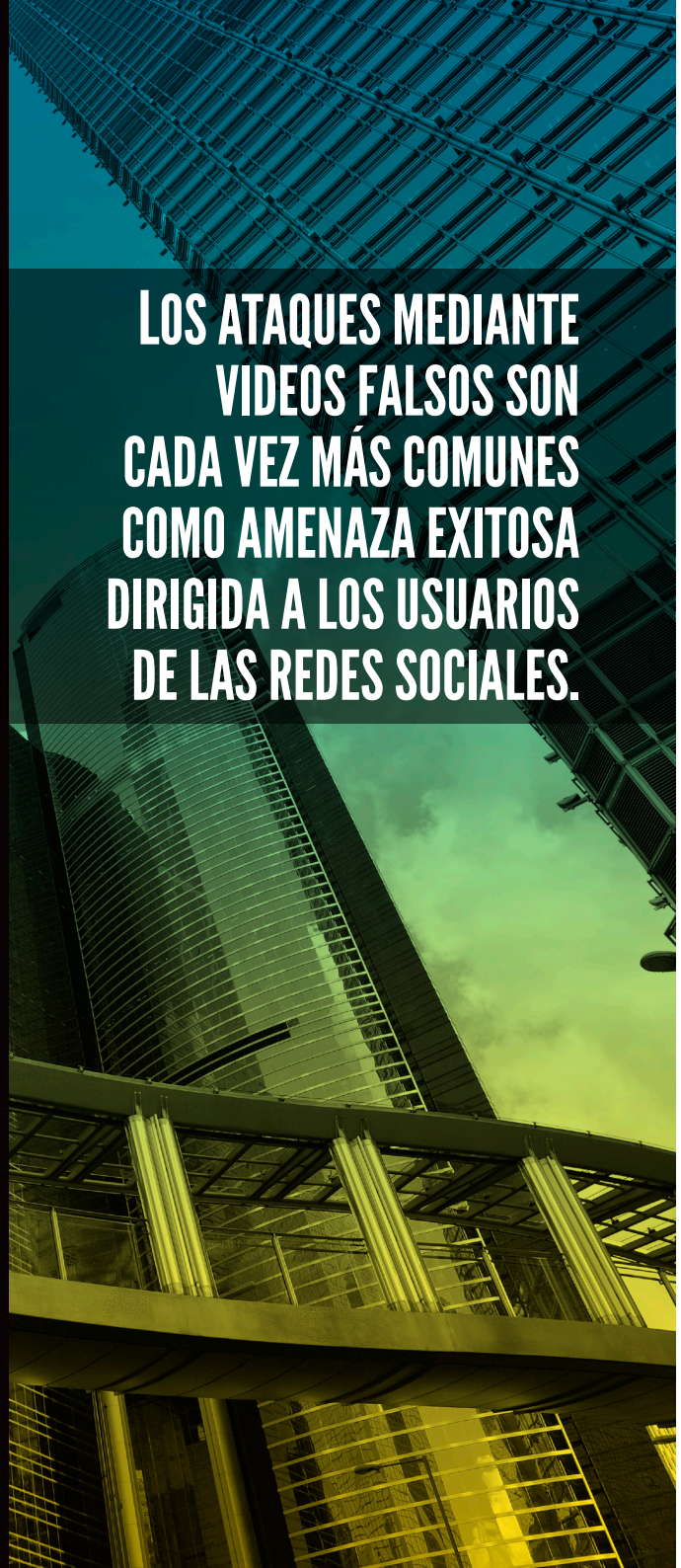


Imagen n.º 1



LOS ATAQUES MEDIANTE VIDEOS FALSOS SON CADA VEZ MÁS COMUNES COMO AMENAZA EXITOSA DIRIGIDA A LOS USUARIOS DE LAS REDES SOCIALES.

Muchos sitios de los TLD turbios se utilizan exclusivamente para estafas y correo no deseado. En la imagen n.º 2 se muestra lo que los visitantes veían si ingresaban a la página principal del sitio web que aloja esta estafa.

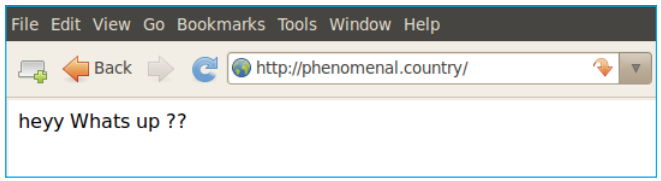


Imagen n.º 2

Las imágenes n.º 3, 4 y 5 son ejemplos representativos de las encuestas falsas a las que se direcciona a los usuarios desde la página del video que no funciona, de acuerdo con el tráfico asociado.

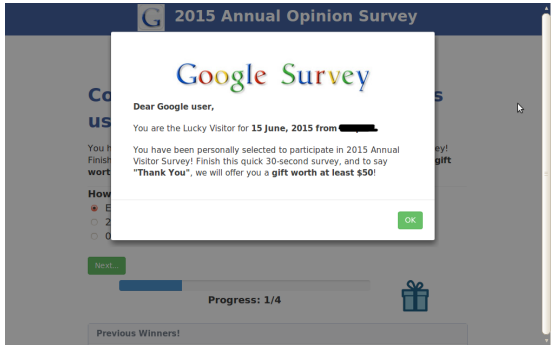


Imagen n.º 3

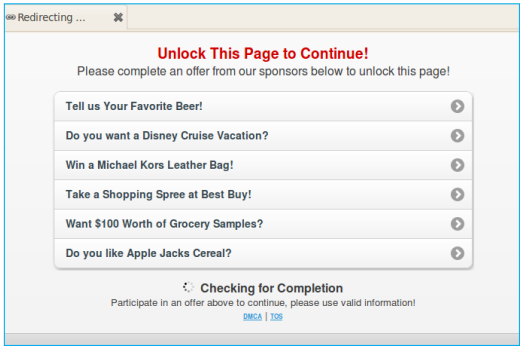


Imagen n.º 4

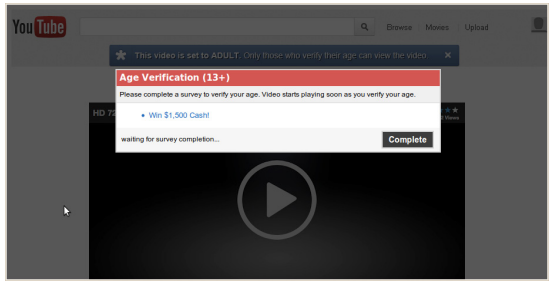


Imagen n.º 5

Vemos esta campaña con mucha frecuencia, generalmente con sitios que reciben cientos de intentos de visitas por día; esto quiere decir que la gente está haciendo clic en ese enlace. Prácticamente todo ese tráfico proviene de Facebook; es decir que el esquema de los estafadores funciona.

Las zonas "más seguras" de la Web

Puesto	Nombre de dominio de nivel superior	Porcentaje de sitios turbios
10	.jp (Japón)	1,95 %
9	.london	1,85 %
8	.kw (Kuwait)	1,61 %
7	.tel	1,60 %
6	.gi (Gibraltar)	1,26 %
5	.gov	0,96 %
4	.church	0,84 %
3	.ck (Islas Cook)	0,52 %
2	.jobs	0,36 %
1	.mil	0,24 %

En comparación, la siguiente lista muestra los diez TLD turbios con menor clasificación, es decir los TLD históricamente "más seguros". Todos estos TLD tienen menos del dos por ciento de sus sitios calificados con clasificaciones turbias hasta la fecha.

No obstante, debemos tener cuidado de leer bastante en esta sección.

Solo algunos de estos (.jp, .gov y .mil) tienen una gran cantidad de sitios en la base de datos de Blue Coat. Por ejemplo, .London tiene más de 100 sitios hasta ahora. Tampoco hay garantía de que los TLD que actualmente tienen menores niveles de riesgo los mantengan. En el pasado observamos que se hackearon muchos sitios web de iglesias pequeñas, así que con el tiempo el dominio .church es posible que no siga siendo un santuario.

Al ser buenos TLD de propósito general, los dominios .tel y .jobs parecen ser objetivos claros de los atacantes en el futuro. Además, .ck es un punto a tener en cuenta ahora que lo identificamos públicamente como un lugar bastante seguro, dado que quienquiera que esté ejecutando este registro probablemente no tenga recursos para alejar a los chicos malos.

Mientras tanto, el nuevo registro .sucks podría unirse a la lista de los "más seguros". Si bien recientemente hubo bastante controversia en torno a este TLD que le cobraba a las marcas USD 2000 o más al año a modo de registro previo, el costo también ayudará a reducir la cantidad de dominios registrados por atacantes.

Aún así, esta lista demuestra que si un registro se esfuerza por mantener la zona limpia realmente puede marcar una diferencia en la Web.

Cómo minimizar el riesgo para empresas y consumidores

En resumen, todos, sean usuarios de empresa o consumidores, deben estar atentos y cautelosos sobre las zonas de Internet que visitan. Ni siquiera los TLD "más seguros" están exentos del riesgo de las amenazas de corruptos y sigue siendo tan crítico como siempre aplicar políticas y protección de seguridad digital estrictas.

- Las empresas deben analizar la posibilidad de bloquear el tráfico que lleva a los TLD de mayor riesgo. Por ejemplo, Blue Coat recomendó anteriormente que las empresas consideren el bloqueo del tráfico hacia los dominios .work, .gq, .science, .kim y .country. Los otros cinco TLD de la lista de los 10 más turbios merecen igual consideración.
- Los usuarios deben estar muy atentos al hacer clic en los enlaces que incluyen estos TLD si los encuentran en resultados de búsqueda, correos electrónicos o entornos de redes sociales.
- Si no está seguro de la fuente, pase el mouse sobre un enlace para verificar si lo lleva hasta la dirección que aparece en el texto del enlace.
- Recuerde que puede "mantener presionado" un enlace en un dispositivo móvil (no solo hacer clic) para verificar que lo lleve donde afirma.

v.BC-WEBS-SHADIEST-NEIGHBORHOODS-A4-EN-v1I-0815

BLUE COAT®

La seguridad fortalece el negocio

Sede Corporativa
Sunnyvale, CA USA
+1.408.220.2200

Blue Coat Brasil
São Paulo
+55 11 3443 6879

Blue Coat México
México D.F.
+52 55 3300 5825

Blue Coat Argentina
Buenos Aires
+54 (11) 4850 1215