SCAM, estafas en la gestión de los dominios

Cardenal Gardoki, 1
48008 BILBAO (Vizcaya)
Teléfono: 902 012 199
www.hostalia.com

Internet es una fabulosa herramienta que nos permite poder hacer prácticamente de todo sin necesidad de tener que desplazarnos. Realizar compras en comercios online, contratar nuestras próximas vacaciones, o trabajar como si estuviéramos en la oficina es posible gracias a la red. El aumento del uso de este sistema también ha hecho que aumente el número de amenazas que nos podemos encontrar en la red, timos de todos tipos que pueden hacer que perdamos grandes puñados de euros. Entre los más utilizados y que afecta a muchos dueños de dominios está el "Domain Name SCAM", más conocido como SCAM y que será el que tratemos este mes en nuestro WhitePaper.

¿Qué es SCAM?

De forma resumida, podemos definir SCAM como una estafa que puede afectar a cualquier usuario propietario de un dominio. Mediante este mecanismo lo que se intenta es que la víctima contrate a la empresa estafadora servicios de protección de dominios o bien que haga el pago de un elevado importe para realizar la renovación de su dominio y que de esta forma el usuario no lo pierda.

Dear CEO,

Are you the owner of "[DOMINIO]", please?

We have something important to confirm with your company. On the [FECHA], we received an application formally from one company named "During Investment LTD" who applied for the Network Trademark"[DOMINIO]" and some domain names relevant to this trademark from our organization.

After our initial examination, we found that the Network Trademark and domain names applied for registration are as same as your company's name and trademark.

These days we are dealing with it,so we hope to get assistant from your company.

Considering this issue will relate to your intellectual property, now we have not finished the registration of During Investment LTD yet,in order to deal with this issue better, Please forward this email to the person who can be in charge and contact us by telephone or email as soon as possible. Thank you!

Best Regards!

El SCAM no se trata de una técnica nueva, sino que es algo que viene sucediendo desde hace años y que puede afectar a usuarios de cualquier extensión de dominio. Es muy probable que muchos de los que están leyendo este libro blanco hayan recibido en su correo electrónico alguno de estos mensajes informando de esta situación, correos que suelen estar en inglés y que tienen una forma similar a la que podéis ver en la imagen anterior.

Muchas personas, ante el temor de perder su dominio o simplemente por desconocimiento, realizan el pago del importe solicitado y después se dan cuenta de que esa inversión no ha valido para nada. Ante este tipo de correos, desde Hostalia os recomendamos que los ignoréis directamente sin pulsar en ninguno de sus enlaces, o ante cualquier duda, os pongáis en contacto con el servicio de atención al cliente para que os aclaren cualquier tipo de duda.

Modus operandi

Como muchos timos que se dan hoy en día en Internet, el medio utilizado para llevar a cabo estas acciones es el correo electrónico. Los atacantes lo que hacen es buscar dominios al azar a los que enviar estos correos, informando de la necesidad de realizar el pago de una importante suma de dinero para proteger su nombre, o bien para realizar la renovación del dominio.

Para conseguir la dirección de email de la víctima, lo que realizan son consultas al WHOIS del dominio. Si la información que apareciese en él estuviera protegida, entonces prueban suerte en el sitio web con la esperanza de encontrar una dirección de correo electrónica. Conseguido su objetivo, envían el correo electrónico a la víctima presentándose como una compañía de nombres de dominios.

Domain Name:	Registration SEO Period:	Price:	Term:
[illegible]com	03/05/2015 to 03/04/2016	$64.00	1 Year

SECURE ONLINE PAYMENT

Domain Name: [illegible]com
Attn: [illegible]

This important expiration notification notifies you about the expiration offer notice of your domain registration for [illegible]com search engine submission. The information in this expiration notification may contain confidential and/or legally privileged information from the notification processing department of the Domain SEO Service Registration to purchase our SEO Traffic Generator. This information is intended only for the use of the individual(s) named above.
If you fail to complete your domain name registration [illegible]com search engine service by the expiration date, may result in the cancellation of this SEO domain name notification offer notice.

Ejemplo de texto recibido para la renovación de un dominio.

El cuerpo de los mensajes suelen estar en inglés, aunque la mayoría procede de países asiáticos como China o Hong Kong. El mensaje suele informar de que su nombre de dominio está a punto de expirar o bien que alguna otra compañía ha presentado una solicitud para registrar algún nombre de dominio que lleven la palabra del nombre del dominio de la víctima y con el fin de proteger la marca de la víctima, le ofrece la posibilidad de proteger esos nombres bajo el pago de una determinada cantidad de euros.

Para que el mensaje parezca totalmente auténtico, suele terminar con el nombre de la persona, puesto, teléfonos de contacto, sitio web y correo electrónico en su firma.

Tipos de SCAM que nos podemos encontrar

Caso 1

En este caso, el titular o contacto administrativo de un dominio recibe un correo de una empresa distinta a Hostalia que informa sobre la inminente caducidad de un dominio que tiene registrado. En el mensaje se informa de que si no lo renueva con ellos lo perderá. Además suele indicar la fecha de expiración del mismo, fecha que no suele coincidir con la fecha de vencimiento del registro.

Ante cualquier correo de este tipo que no provenga de Hostalia o de la empresa donde tiene registrado sus dominios, actúe eliminándolo directamente para evitar cualquier tipo de problema.

Caso 2

Al igual que en el primer caso, el titular o contacto administrativo recibe un corre informándole de ciertas extensiones de dominios que no tiene registradas. En este caso se puede dar dos variantes:

a) El atacante contacta con la víctima para informarle de que alguien pretende usurpar su marca para extensiones como por ejemplo .cn (China), y se ponen en contacto con nosotros para ofrecernos la posibilidad de registrarlos antes que la otra persona.

b) En la segunda variante, el SCAM informa a la víctima de que un mismo nombre de dominio pero con distinta extensión va a quedar libre, ofreciéndole la posibilidad de registrarlo antes de que se adelante alguien. Esta información puede ser cierta, pero el precio que suelen pedir por el registro suele ser muy elevado. Si de verdad estás interesado en registrar ese dominio, lo mejor es ponerse en contacto con la empresa que te ofrece este tipo de servicio de forma habitual.

Caso 3

Un tipo de scam muy frecuente en territorio hispano es el traslado de dominios .es. Como no tienen auth-code ni bloqueo, cualquiera puede pedir el traslado a su cuenta de un dominio como 'miempresaweb.es'. Por ello el contacto administrativo del dominio nunca debe dar a 'Aceptar' si le llega un email de este tipo, a no ser que el propietario del dominio le haya comunicado previamente su intención de trasladarlo.

Prevenciones

Como suele ocurrir en cualquier ataque que se produce por Internet, el mejor antídoto de todos es hacer caso de nuestra intuición y si vemos que algo no nos cuadra, mejor ignorarlo o informarnos con alguien de confianza para que nos aclare cualquier tipo de duda.

Además de la intuición, podemos tomar una serie de medidas para reducir en todo lo posible que seamos elegidos para sufrir este tipo de estafa.

1.- No pongas tu dirección de correo electrónico visible en tu portal web. Apuesta por los formularios de contacto si quieres permitir que los visitantes se pongan en contacto contigo

2.- Hay que prevenir el envío de formularios de forma automática mediante el uso de sistemas de Captcha

3.- Desconfía de los remitentes desconocidos

En este WhitePaper hemos visto en qué consiste el SCAM de dominios y su forma de actuar, un tipo de amenaza que no puede ser tan peligrosa como otras que circulan por la red, pero que pueden hacernos perder importantes cantidades de dinero.