Unsubscribeservices

Uri Mtz

<2022-05-31 mar>

Contents

1	Anzuelo	1
2	Información remitente y título	2
3	Contenido 3.1 Contenido del enlace	3
1	Anzuelo	
	← Tu nuevo MG MG5 está cerca de ti Da click y cotiza de inmediato	

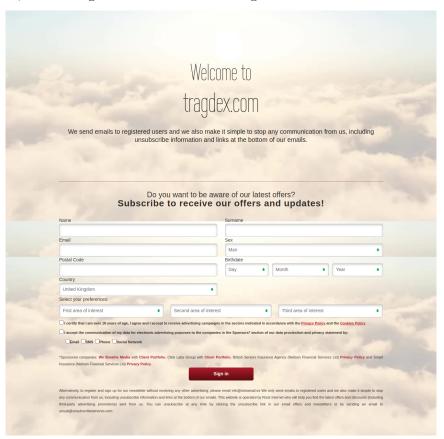


2 Información remitente y título

El remitente, identificado por Outlook como MG5 2022, bajo el correo info@news.tragdex.com envía un correo titulado Tu nuevo MG MG5 está cerca de ti Da click y cotiza de inmediato

https://tragdex.com es el dominio del correo remitente, si se entra a su página, lleva a una página estática que muestra un texto en inglés, mencionando que sólo son una página que envía mails a sus usuarios registrados, más adelante muestra una forma que invita al usuario a registrarse, esta forma acepta cualquier dato sin verificar si tiene un sentido alguna información, únicamente el nombre y apellido deben contener más de 3 caracteres y el correo debe tener un dominio válido, si se registra un correo cualquiera, inmediatamente no llega ningún tipo de correo de confirmación.

Al pie de la forma contiene una nota que menciona algunas supuestas empresas que patrocina este dominio, estas páginas y empresas parecen ser reales, sin embargo se necesita más investigación.



Este dominio fue registrado con "Don Dominio", una web europea (española al parecer), que te permite comprar dominios.

3 Contenido

El correo en si mismo no es peligroso, ya que no contiene ningún archivo adjunto, sin embargo intenta mostrarse como un anuncio acerca de una cotización.

Los elementos nombrados:

- en línea
- darme de baja
- MG
- Conócelo
- siga este enlace

Contienen un enlace que lleva a la dirección: https://mailing.monskuar.com/

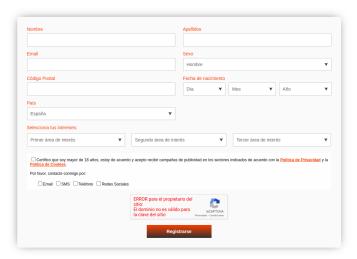
3.1 Contenido del enlace

El enlace lleva a una página que solicita dar clic en un botón para comprobar que no eres un robot, este botón está hecho con un elemento div dentro del código html, el cual no ejecuta ningún script malicioso, sin embargo la página posee un código que funciona como redireccionamiento en cuanto el usuario hace clic en el botón, el script es el siguiente:

El dominio https://monskuar.com, es un dominio registrado con "Don Dominio", la página es una página estática similar a la que es dominio del correo remitente, a diferencia de la primera, esta se muestra en español, sin embargo esto es debido a la detección del país, las características son similares, sin embargo esta página no te permite registrarte debido a que no está configurado de manera correcta su captcha.



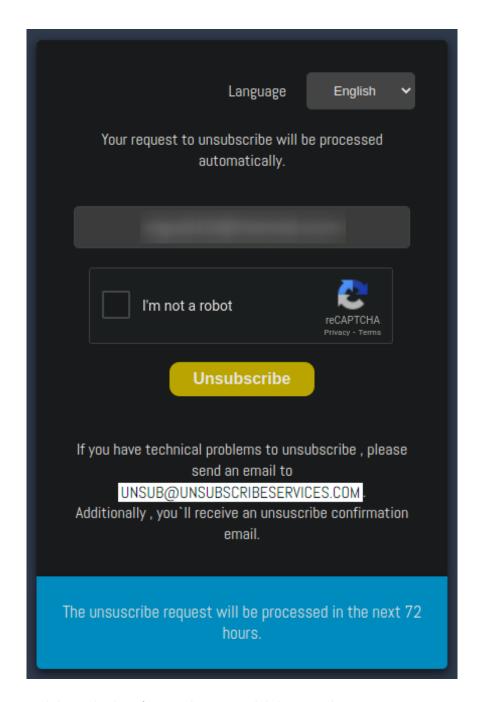
¡Suscríbete a nuestro boletín de noticias!





Al finalizar el redireccionamiento desde https://monskuar.com, lleva hacia https://unsubscribeservices.com, página que supuestamente te permite eliminar tu supuesta suscripción a su lista de suscripción. Promete que la solicitud será procesada en las próximas 48 horas.

Por tratarse de un redireccionamiento, los enlaces acarrean el correo, por lo que será mostrado automáticamente en la forma, únicamente solicita comprobar que no eres un robot usando un captcha.



La búsqueda de información acerca del dominio únicamente muestra que fue registrado con "OVH", mientras el resto de la información se mantiene privada.

Una breve búsqueda en internet muestra https://www.mywot.com/scorecard/unsubscribeservices.com como uno de los primeros resultados, el cual muestra 3 reseñas, las cuales describen que el sitio únicamente es usado para suscribirte a una lista de correo de spam y que la supuesta desuscripción nunca sucede.

Este dominio y todo lo que conllevó anteriormente está ligado a algún usuario o empresa española, por lo tanto, gran parte de sus objetivos son de habla hispana.

3.2 Tomando medidas de seguridad

Para evitar caer en este tipo de estafas se recomienda lo siguiente:

- Estos correos entran normalmente a la carpeta de *correo no deseado* o *spam*, por lo que pueden ser ignorados sin ningún riesgo.
- Si el correo llega a la bandeja principal, la manera de identificar esta estafa es el sentido común, en este caso, si no ordenaste una cotización del producto mencionado, es muy probable que sea una estafa.
- Si cualquiera de los enlaces llevan al mismo destino a pesar de que sea contradictorio, por ejemplo, conócelo y darme de baja son frases contradictorias, sin embargo ambas llevan a la misma dirección, por lo tanto es altamente probable que se trate de una estafa.
- Bloquear al remitente usando su cliente de correo o su proveedor,
 Gmail provee funciones de filtro para que automáticamente se eliminen
 o rechacen los correos de ese remitente
- Tomando medidas de seguridad Para evitar caer en este tipo de estafas se recomienda lo siguiente:
 - Estos correos entran normalmente a la carpeta de correo no deseado o spam, por lo que pueden ser ignorados sin ningún riesgo.
 - Si el correo llega a la bandeja principal, la manera de identificar esta estafa es el sentido común, en este caso, si no ordenaste una cotización del producto mencionado, es muy probable que sea una estafa.
 - Si cualquiera de los enlaces llevan al mismo destino a pesar de que sea contradictorio, por ejemplo, conócelo y darme de baja son frases contradictorias, sin embargo ambas llevan a la misma

- dirección, por lo tanto es altamente probable que se trate de una estafa.
- Bloquear al remitente usando su cliente de correo o su proveedor,
 Gmail provee funciones de filtro para que automáticamente se eliminen o rechacen los correos de ese remitente.