2º Correo falso de Hacienda

19/05/2023

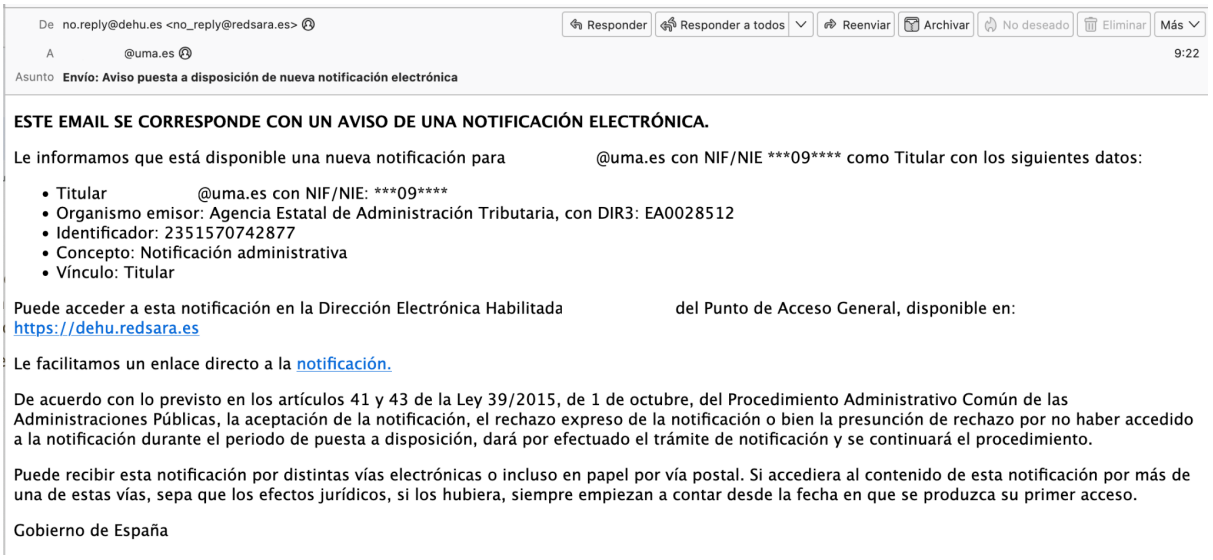
Vicerrectorado de empresa, territorio y transformación digital
Servicio Central de Informática
Unidad de Seguridad
seguridadsci@uma.es

Visión general

Como comentamos en el caso del correo del mes de marzo, es muy habitual que en ciertos momentos, como ahora con la campaña de hacienda, entren muchos correos simulando ser ellos. Un caso típico de phishing.

Aspecto

El aspecto del correo-e, que está entrando estos días, es el siguiente:



De no.reply@dehu.es <no_reply@redsara.es>
Responder | Responder a todos | Reenviar | Archivar | No deseado | Eliminar | Más
A @uma.es 9:22
Asunto **Envío: Aviso puesta a disposición de nueva notificación electrónica**

ESTE EMAIL SE CORRESPONDE CON UN AVISO DE UNA NOTIFICACIÓN ELECTRÓNICA.

Le informamos que está disponible una nueva notificación para @uma.es con NIF/NIE ***09**** como Titular con los siguientes datos:

- Titular @uma.es con NIF/NIE: ***09****
- Organismo emisor: Agencia Estatal de Administración Tributaria, con DIR3: EA0028512
- Identificador: 2351570742877
- Concepto: Notificación administrativa
- Vínculo: Titular

Puede acceder a esta notificación en la Dirección Electrónica Habilitada del Punto de Acceso General, disponible en: https://dehu.redsara.es

Le facilitamos un enlace directo a la notificación.

De acuerdo con lo previsto en los artículos 41 y 43 de la Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas, la aceptación de la notificación, el rechazo expreso de la notificación o bien la presunción de rechazo por no haber accedido a la notificación durante el periodo de puesta a disposición, dará por efectuado el trámite de notificación y se continuará el procedimiento.

Puede recibir esta notificación por distintas vías electrónicas o incluso en papel por vía postal. Si accediera al contenido de esta notificación por más de una de estas vías, sepa que los efectos jurídicos, si los hubiera, siempre empiezan a contar desde la fecha en que se produzca su primer acceso.

Gobierno de España

A simple vista vemos ya que la dirección no tiene mucho que ver con la agencia y está dirigido a alguien de la UMA.

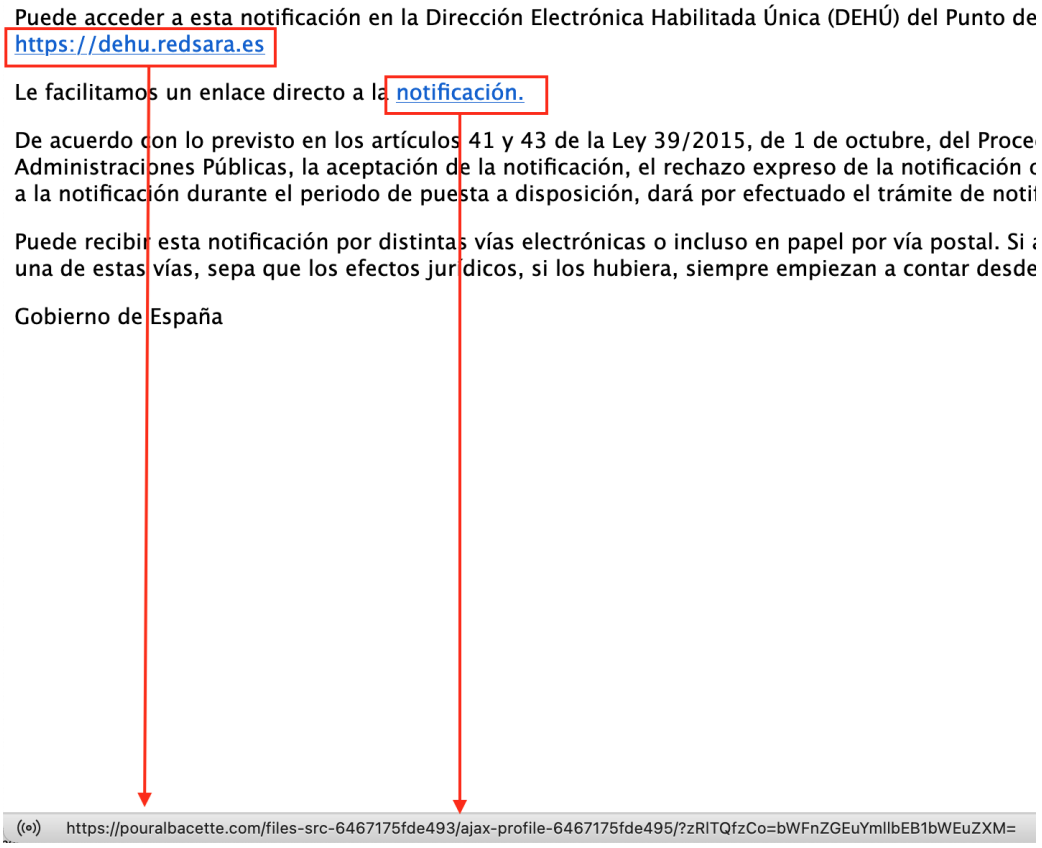
Los datos del titular son los de la persona a quien va destinado el correo.

Supuestamente lo mandan desde no.reply@dehu.es<no_reply@redsara.es>, pero esto como vimos en el curso, es la parte más fácil de falsificar. Es en lo primero que debemos desconfiar.

Dehu, dentro de la red sara, es un portal de notificaciones para las administraciones públicas, su web real es:

https://dehu.redsara.es/

Vamos a revisar los enlaces, pasamos el ratón sobre los enlaces pero **sin hacer click** para comprobar a dónde nos llevan.



Vemos que la dirección ya no es la del portal de notificaciones. Ahí está el phishing.

Vamos ahora a analizar la cabecera.

Análisis de la cabera

Como hemos visto en el taller, me fijo en el **to**, el **from** y el primer servidor que recepciona el correo **Received**.

```
Received: from arsalan by server.morosoftsites.com with local
(Exim 4.96)
      (envelope-from <arsalan@server.morosoftsites.com>)
      id 1pzuRl-00045h-01
      for pepelopezlopez@uma.es;
      Fri, 19 May 2023 15:22:41 +0800
To: pepelopezlopez@uma.es
Subject:
=?UTF-8?B?RW52w61vOiBBdmlzbyBwdWVzdGEgYSBkaXNwb3NpY2nDs24gZGUgWZpY
2FjacOzbiBlbGVjdHLDs25pY2E=?=
X-PHP-Script:
firashaidar.arsalan.morosoftsites.com/wp-content/plugins/woocommer
ce/src/Admin/API/Reports/Stock/Stats/Stats.php for 185.121.137.203
X-PHP-Originating-Script: 1004:Stats.php
From: =?UTF-8?B?bm8ucmVwbHlAZGVodS5lcw==?= <no_reply@redsara.es>
Reply-To: no_reply@redsara.es
```

El **to** y el **from**, como hemos dicho anteriormente, es la parte más fácil de falsear. Ahí está relacionado con la Red Sara y nos podría confundir, aunque no le deberíamos hacer caso.

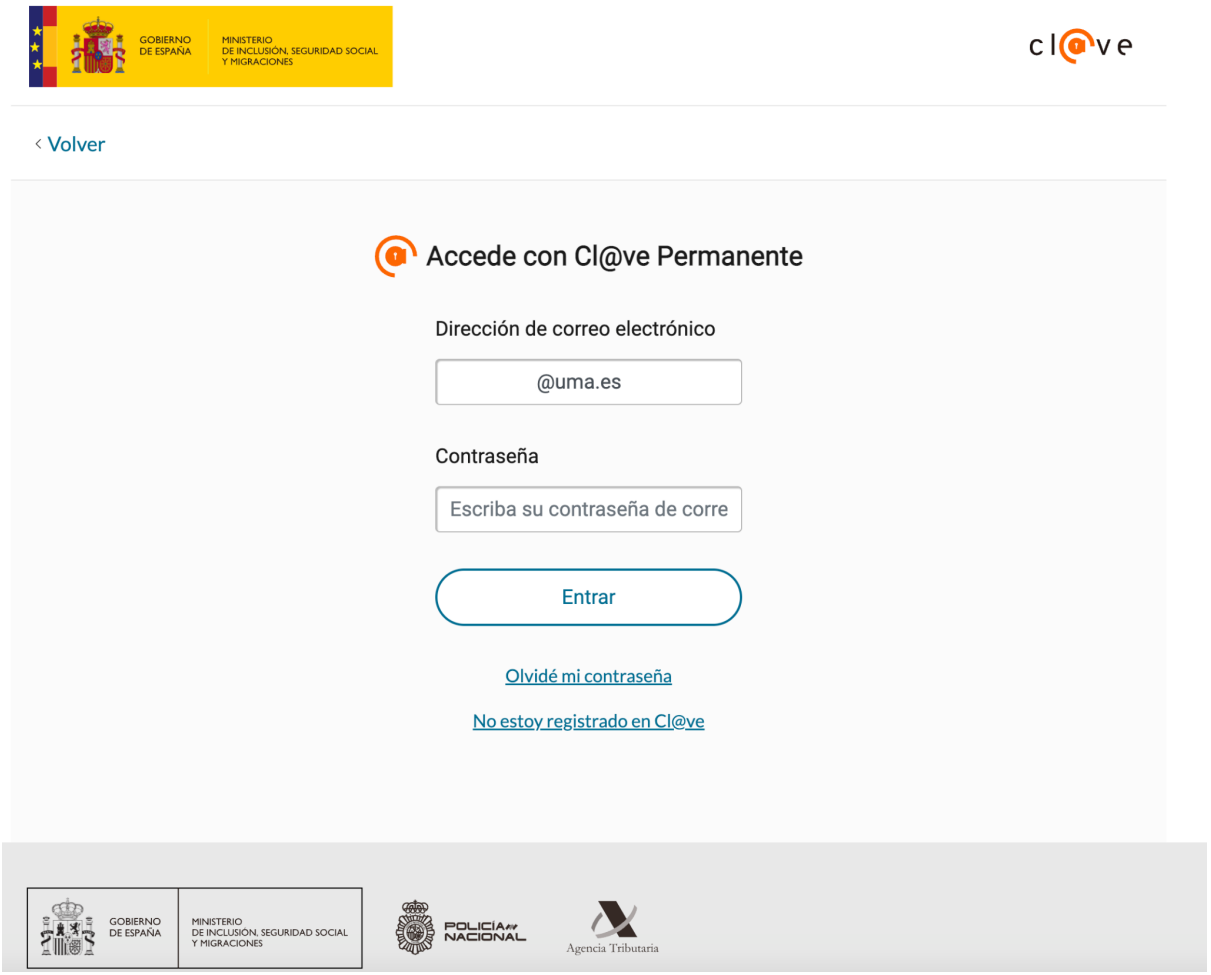
Veamos el **received**, ahí si que vemos un servidor desde el que se ha mandado el correo, que nada tiene que ver con la **aeat**:

```
Received: from arsalan by server.morosoftsites.com with local
```

Es un sitio que probablemente han vulnerado y desde allí están mandando el phishing.

He hecho click en el enlace !!

Si hacemos click en el enlace, nos llevará a la siguiente página web



Es una página de phishing, similar a la que hemos visto en el curso de este año. Ponen tu dirección de correo electrónico y piden la contraseña.

Si no has puesto la contraseña y ahí te has dado cuenta del **phishing**, no pasa nada. Asegúrate que tienes el antivirus actualizado y escanea el disco.

Si quieres, cambia la contraseña tras pasar el antivirus si no ha detectado nada.

Yo si he puesto mis credenciales

```
Deberías repasar los apuntes del curso
```

Tienes que cambiar la contraseña lo antes posible, pero cuidado, no lo hagas desde el ordenador comprometido.

Puedes hacerlo desde el móvil o desde el ordenador de un compañero.

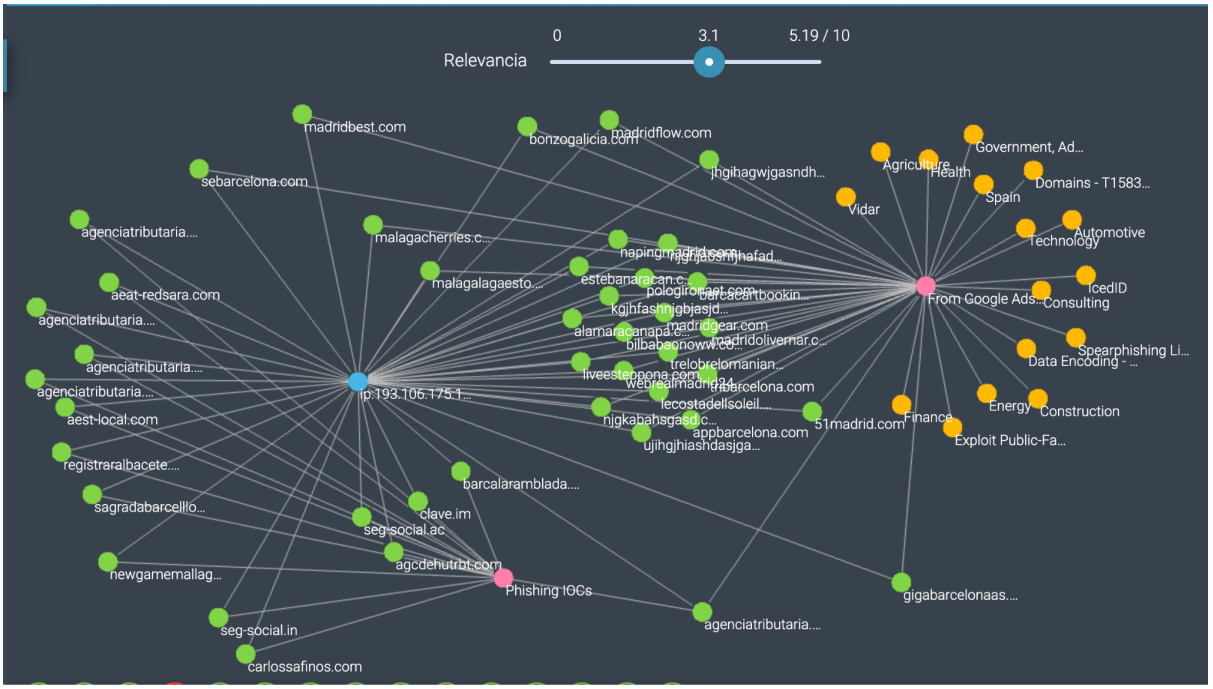
Luego, asegúrate si tienes el antivirus instalado y actualizado. Lanza un escaneo a todo el disco.

One more thing

Desde el SCI, hemos cortado el acceso a esos dominios y páginas webs, pero mañana puede aparecer otro parecida. Es realmente complicado, sin vuestra ayuda y conocimiento, acabar con estos ataques de ingeniería social por phishing.

En este caso, una de las direcciones IP implicadas en esta incidencia es de origen ruso y ha registrado numerosos dominios relacionados con la AEAT e incluso con Málaga.

Os lo muestro aquí:



Como siempre os digo, tenéis las direcciones seguridadsci@uma.es e incidentes@uma.es a vuestra disposición.

Espero que os sirva de ayuda!