Correo falso de Hacienda

06/03/2023

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

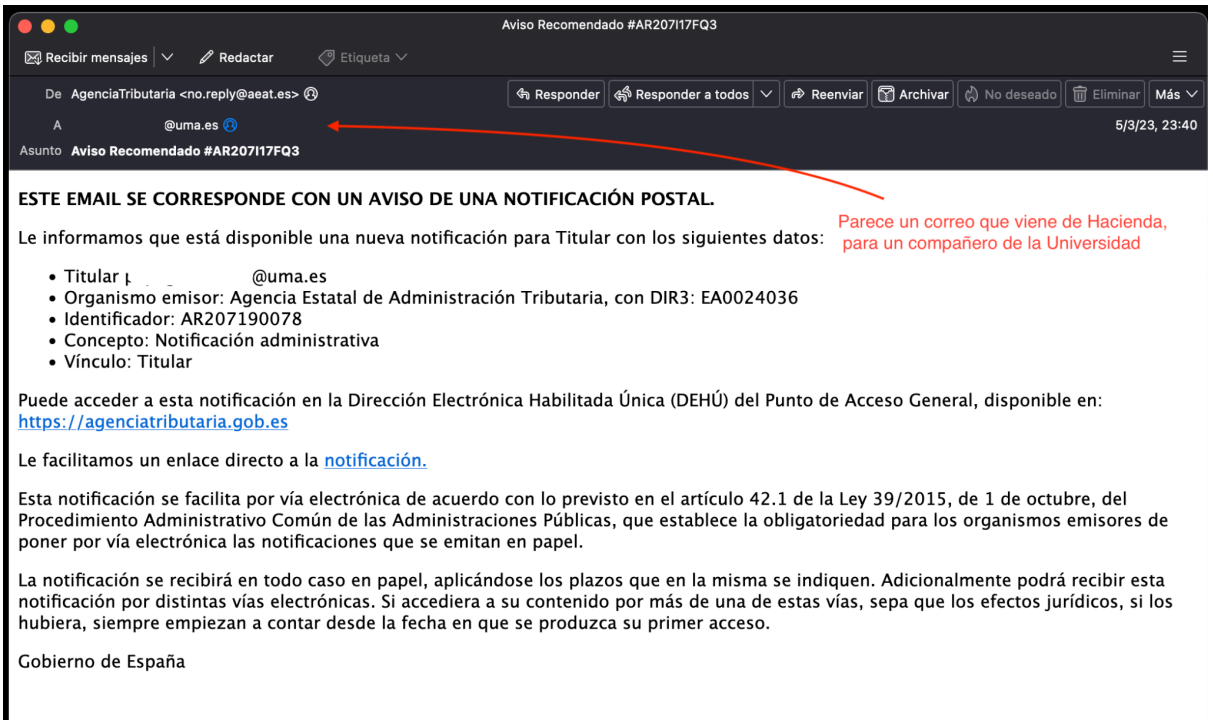
Visión general

Es muy común entre los atacantes que cuando existen grandes campañas, como por ejemplo la de la Renta, nos inunden con correos relacionados para intentar engañarnos.

Cuidado con esto. Esta vez os traigo un correo que me ha reportado un compañero y entró ayer domingo día 5 de marzo.

Aspecto

El aspecto del correo-e es el siguiente:

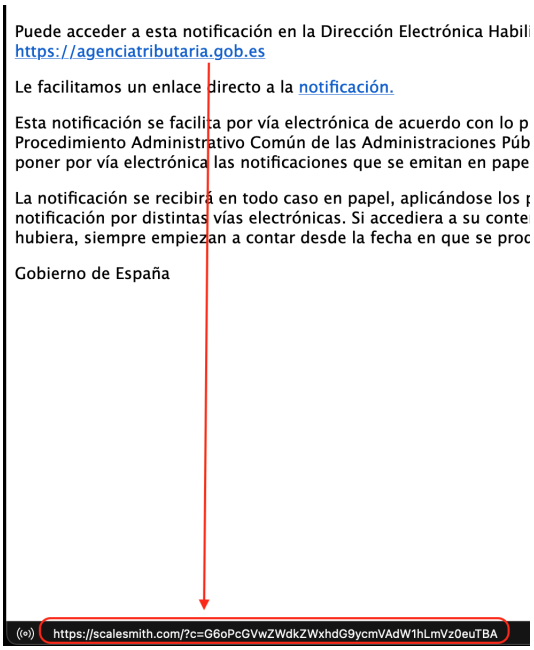


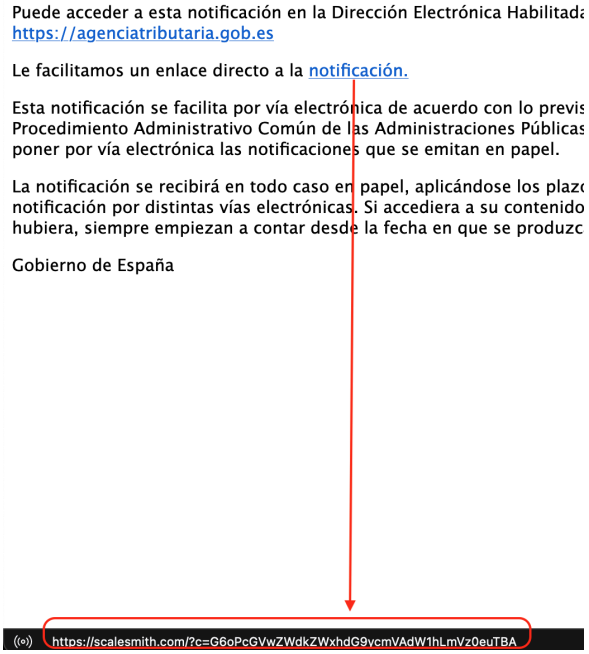
A simple vista puede parecer un correo de la Agencia Tributaria, proviene de una dirección no.reply@aeat.es a un correo de la UMA.

Las direcciones **noreply@** se suelen utilizar en los servidores de correo para correos que se envíen y no necesiten respuesta. Pero fijaros, aquí viene el primer engaño; normalmente las direcciones son **noreply@** y en este caso nos encontramos **no.reply@**

Esta dirección con ese punto no es normal, aquí podríamos empezar a sospechar.

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





Ambos enlaces llevan a un sitio web ***scalesmith.com*** que tampoco tiene nada que ver con la Agencia Tributaria. Además llevan un parámetro codificado, *G6oPcGVwZWdkZWxhdG9ycmVAdW1hLmVz0euTBA*, que es la dirección de correo electrónico de la persona que ha recibido el correo. Esto se llama ofuscación de datos.

Observad que en el primer enlace parece que me iba a llevar a https://agenciatributaria.gob.es, pero realmente me llevará a otro sitio. Esto es muy importante, una cosa es cómo lo ponen con el editor de texto y otra, dónde está programado el enlace.

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 host81-155-234-82.range81-155.btcentralplus.com
([81.155.234.82]:54778 helo=zed-international.com)
     by bella.ndx8.com with esmtpsa  (TLS1.2) tls
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256
     (Exim 4.95)
     (envelope-from <no.reply@aeat.es>)
     id 1pYx1m-0001fE-1y
     for xxxxxxxxxx@uma.es;
     Sun, 05 Mar 2023 15:40:26 -0700
Content-Type: multipart/related;
boundary="------------060703000607030201040404"
MIME-Version: 1.0
Date: Sun, 05 Mar 2023 23:40:22 +0100
Subject: Aviso Recomendado #AR207I17FQ3
From: AgenciaTributaria <no.reply@aeat.es>
To: xxxxxxxxxx@uma.es
```

En el **From** podemos ver lo que antes hemos comentado. En el campo nombre, **AgenciaTributaria** y como dirección de envío **<no.reply@aeat.es>**

Esta parte, como hemos comentado en el taller, en la más fácil de falsificar, es la del lado del cliente que compone el mensaje.

El **to** es la dirección a la que se envía y es una dirección de la UMA

En el primer **received**, que es el primer servidor que recepciona el mensaje vemos que su nombre es **host81-155-234-82.range81-155.btcentralplus.com** y su dirección IP es **81.155.234.82**

No es normal que la Agencia Tributaria utilice un servidor sin su nombre de dominio, **aeat** y además que sea **.com**

Mirad este fragmento de cabecera de un correo que si lo ha mandado la agencia:

```
Received: from domprodd.aeat ([10.30.200.4])
          by 10.30.169.2
          with ESMTP id 20140723092909 63-863968 ;
          Wed, 23 Jul 2014 09:29:09 +0200
```

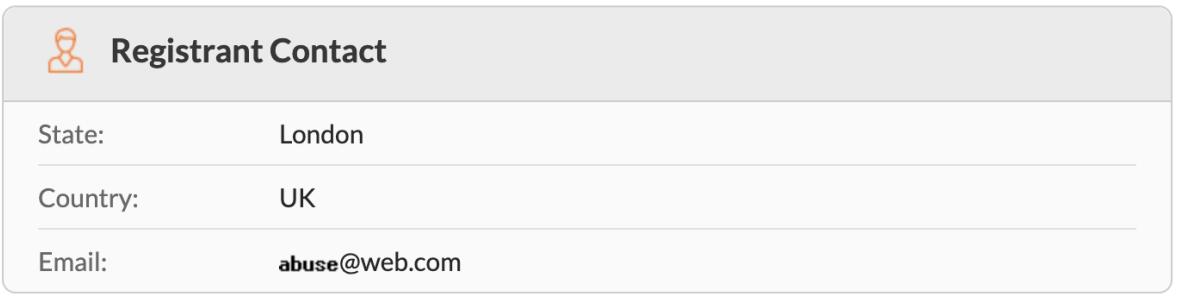
Aquí si tenemos un dominio de un servidor de correo con dominio aeat, **domprodd.aeat.** Su IP es 10.30.200.4

Análisis del servidor desde el que se ha mandado el mail

Disponemos de muchas herramientas on-line para averiguar más datos sobre los servidores de Internet. Estas herramientas se llaman **whois**, también es un comando de sistema operativo Linux o Mac.

Desde esta url podemos hacer averiguaciones sobre el dominio o la IP que aparece en el mensaje, https://www.whois.com/whois/

El dominio según miramos en la cabecera es la parte final del nombre DNS, **btcentralplus.com,** lo consultamos en Whois y entre la información nos encontramos que es un servidor de Londres, no parece que tenga mucho que ver con la AEAT.



Análisis del contenido (one more thing)

Si analizamos en el código del correo su contenido veremos lo siguiente:

```
--------------060703000607030201040404
Content-Transfer-Encoding: base64
Content-Type: text/html; charset=utf-8

PCFkb2N0eXBlIGh0bWw+DQo8aHRtbD4NCiAgPGhlYWQ+DQogICAgPG1ldGEgY2hhcn
NldD0iVVRG
LTgiPg0KICA8L2hlYWQ+DQogIDxib2R5Pg0KICAgIDxkaXY+PC9kaXY+DQogICAgPH
A+PHN0cm9u
Zz4gRVNURSBFTUFJPHNwYW4gc3R5bGU9ImJvcmRlcjowcHggZG90dGVkIGNvbG9yOi
MyMDA5Mjsi
Pkw8L3NwYW4+IFNFIENPUlJFPHNwYW4gc3R5bGU9ImJvcmRlcjowcHggOSBjb2xvcj
ojMjY5OyI+
Uzwvc3Bhbj5QT05ERSBDT04gVU4gQVZJUzxzcGFuIHN0eWxlPSJib3JkZXI6MHB4IG
dyb292ZSBj
b2xvcjojMTM5NjsiPk88L3NwYW4+IERFIFVOQSBOT1RJRjxzcGFuIHN0eWxlPSJib3
JkZXI6MHB4
IDkgY29sb3I6IzIzNDg3OyI+STwvc3Bhbj5DQUNJw5NOIFBPU1RBTDxzcGFuIHN0eW
xlPSJib3Jk
ZXI6MHB4IGRhc2hlZCBjb2xvcjojNDE5OyI+Ljwvc3Bhbj48L3N0cm9uZz48L3A+DQ
ogICAgPHA+

..... y sigue
```

Todo eso que estamos viendo es código ofuscado en base-64, si lo decodificamos podremos ver el contenido en texto descifrado:

```
<!doctype html>
<html>
  <head>
    <meta charset="UTF-8">
  </head>
  <body>
    <div></div>
```

```
    <p><strong> ESTE EMAI<span style="border:0px dotted
color:#20092;">L</span> SE CORRE<span style="border:0px 9
color:#269;">S</span>PONDE CON UN AVIS<span style="border:0px
groove color:#1396;">O</span> DE UNA NOTIF<span style="border:0px
9 color:#23487;">I</span>CACIÓN POSTAL<span style="border:0px
dashed color:#419;">.</span></strong></p>
    <p> Le info<span style="border:0px groove
color:#81536;">r</span>mamos que está disponible una nueva
notific<span style="border:0px dashed color:#125329;">a</span>ción
para Titular con los sigui<span style="border:0px outset
color:#888645;">e</span>ntes datos:</p>
    <ul>
      <li> T<span style="border:0px dotted
color:#7711;">i</span>tular xxxxxxx@uma.es</li>
      <li> Organis<span style="border:0px double
color:#73652;">m</span>o emiso<span style="border:0px outset
color:#6977;">r</span>: Age<span style="border:0px solid
color:#3759;">n</span>cia Esta<span style="border:0px ridge
color:#513;">t</span>al de Administ<span style="border:0px ridge
color:#2838;">r</span>ación Trib<span style="border:0px outset
color:#6558;">u</span>taria, con DIR3: EA00<span style="border:0px
inset color:#38294;">2</span>4036</li>
      <li> I<span style="border:0px double
color:#4509;">d</span>entificador: AR20<span style="border:0px
inset color:#236;">7</span>190078</li>
      <li> Co<span style="border:0px outset
color:#54744;">n</span>cepto: No<span style="border:0px 9
color:#24878;">t</span>ificación ad<span style="border:0px inset
color:#742831;">m</span>inistrativa</li>
      <li> V<span style="border:0px 8 color:#1108;">í</span>nculo:
T<span style="border:0px 8 color:#492677;">i</span>tular</li>
    </ul>
    <p> Puede acceder a esta notifica<span style="border:0px 8
color:#0002;">c</span>ión e<span style="border:0px double
color:#656661;">n</span> la Dirección Electró<span
style="border:0px 8 color:#299951;">n</span>ica Habilitada
Únic<span style="border:0px groove color:#28964;">a</span> (DEHÚ)
del Punto de Acces<span style="border:0px dashed
color:#23977;">o</span> General, disponible en: <a
href="https://scalesmith.com/?c=G6oPcGVwZWdkZWxhdG9ycmVAdW1hLmVz0e
uTBA">https://agen<span style="border:0px 8
```

```
color:#514;">ci</span>atri<span style="border:0px dashed
color:#431;">bu</span>taria.gob.es</a></p>
    <p> Le faci<span style="border:0px 8
color:#51196;">l</span>itamos un en<span style="border:0px ridge
color:#549;">l</span>ace di<span style="border:0px dashed
color:#23647;">r</span>ecto a la <a
href="https://scalesmith.com/?c=G6oPcGVwZWdkZWxhdG9ycmVAdW1hLmVz0e
uTBA">notificación.</a></p>
    <p> Esta notificación se facilita por vía electrónica de
acuerdo con lo previsto en el ar<span style="border:0px ridge
color:#2157;">t</span>ículo 42.1 de la Ley 39/2015, de 1 de
octubre, del Procedimiento Adminis<span style="border:0px dashed
color:#3491;">t</span>rativo Común de las Administraciones
Públicas, que establece la obligatoriedad para los organismos
emisores de poner por vía electrónica las notificaciones que se
emitan en papel.</p>
    <p> La notificación se recibirá en todo caso en papel,
aplicándose los plazos que en la misma se indiquen. Adicionalmente
podrá recibir esta notificación por distintas vías elect<span
style="border:0px double color:#296;">r</span>ónicas. Si accediera
a su conten<span style="border:0px dashed
color:#05520;">i</span>do por m<span style="border:0px groove
color:#014241;">á</span>s de una de estas ví<span
style="border:0px 9 color:#59421;">a</span>s, sepa que los efectos
jurídicos, si los h<span style="border:0px double
color:#6565;">u</span>biera, siempre empiezan a contar desde la
fecha en que se produzca su primer acceso.</p>
    <p> Go<span style="border:0px ridge
color:#45539;">b</span>ierno de Es<span style="border:0px dashed
color:#91177;">p</span>aña</p>
    </div>
  </body>
</html>
```

Y de ese código en html podemos sacar lo que antes pudimos ver pasando el ratón por el enlace:

```
<a
href="https://scalesmith.com/?c=G6oPcGVwZWdkZWxhdG9ycmVAdW1hLmVz0e
uTBA">
```