CSIRT
GOBIERNO DE COLOMBIA

El futuro digital es de todos
Gobierno de Colombia
MinTIC

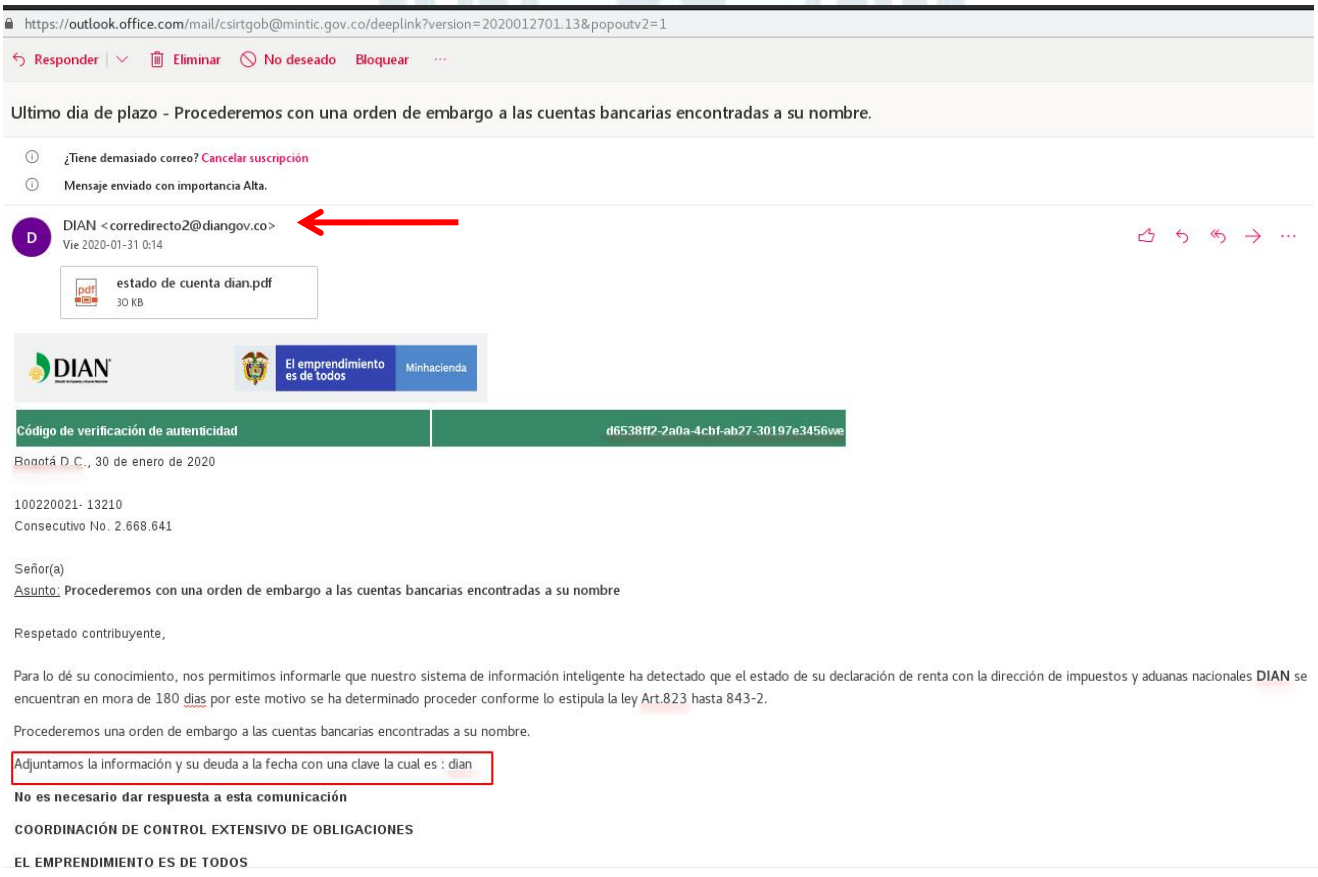
**31/01/2020**

# Alerta - Correo malicioso

## Correo Malicioso
## Suplantación DIAN

Desde el día 30 de enero varias entidades han reportado un correo sospechoso proveniente de la cuenta de correo ***corredirecto2@diangov.co*** con el asunto **"Ultimo dia de plazo - Procederemos con una orden de embargo a las cuentas bancarias encontradas a su nombre.",** donde se indica que la persona que recibe el mismo se encuentra en mora y adjuntan un archivo PDF donde según el cuerpo de correo, se encuentra la información de dicha deuda.

Al realizar una revisión del contenido del correo, inicialmente se identifica que el dominio **no pertenece** a la DIAN y se encuentra registrado en un hosting gratuito.



https://outlook.office.com/mail/csirtgob@mintic.gov.co/deeplink?version=2020012701.13&popoutv2=1

Responder | Eliminar | No deseado | Bloquear | ···

Ultimo dia de plazo - Procederemos con una orden de embargo a las cuentas bancarias encontradas a su nombre.

¿Tiene demasiado correo? Cancelar suscripción

Mensaje enviado con importancia Alta.

D DIAN <corredirecto2@diangov.co>
Vie 2020-01-31 0:14

estado de cuenta dian.pdf
30 KB

DIAN | El emprendimiento es de todos | Minhacienda

| Código de verificación de autenticidad | d6538ff2-2a0a-4cbf-ab27-30197e3456we |
|---|---|

Bogotá D.C., 30 de enero de 2020

100220021- 13210
Consecutivo No. 2.668.641

Señor(a)
Asunto: **Procederemos con una orden de embargo a las cuentas bancarias encontradas a su nombre**

Respetado contribuyente,

Para lo dé su conocimiento, nos permitimos informarle que nuestro sistema de información inteligente ha detectado que el estado de su declaración de renta con la dirección de impuestos y aduanas nacionales **DIAN** se encuentran en mora de 180 dias por este motivo se ha determinado proceder conforme lo estipula la ley Art.823 hasta 843-2.

Procederemos una orden de embargo a las cuentas bancarias encontradas a su nombre.

Adjuntamos la información y su deuda a la fecha con una clave la cual es : dian

**No es necesario dar respuesta a esta comunicación**

**COORDINACIÓN DE CONTROL EXTENSIVO DE OBLIGACIONES**

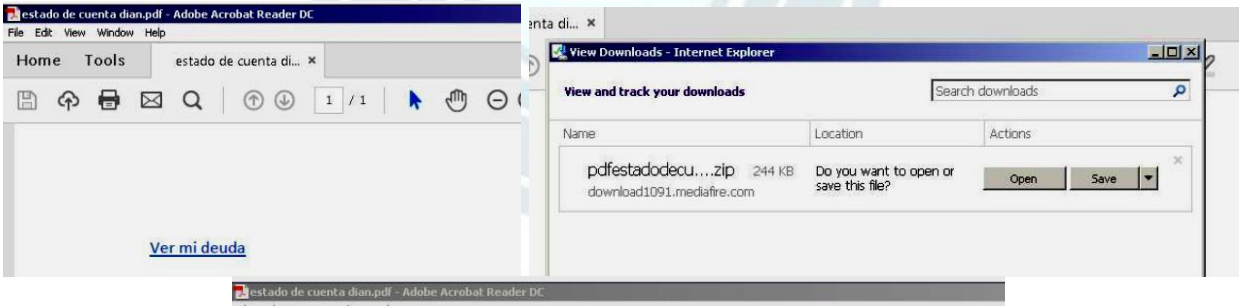
**EL EMPRENDIMIENTO ES DE TODOS**

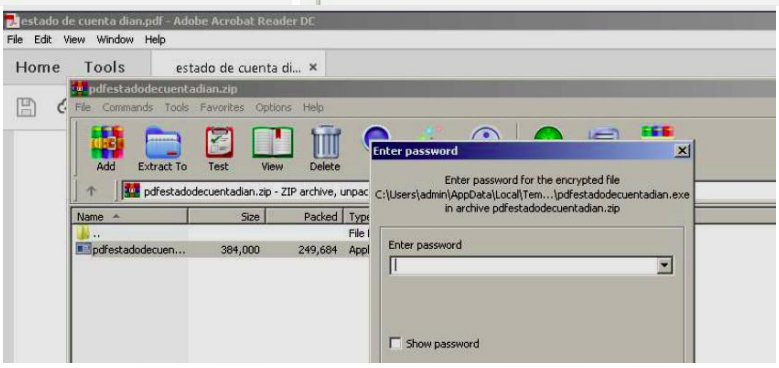
#MásTIC MejorPaís

Por otra parte se descarga el archivo que trae adjunto el correo, este se analiza y el contenido del mismo esta reportado como malicioso.


Ver reporte completo: https://bit.ly/31edpK1

Al hacer un análisis detallado del mismo, el PDF contiene solo un enlace con el nombre "*ver mi deuda*", este link redirecciona al usuario a una pagina de internet en la que se descarga un archivo .zip el cual contiene un archivo ejecutable que se encuentra protegido por contraseña.




Al descomprimir el archivo, este se ejecuta automaticamente en segundo plano e inicia a realizar cambios en las llaves de registro del sistema y a realizar comunicaciones de C&C (comando y control) a IPs externas.

A continuación se relacionan los IoC del archivo:

Main object- "estado de cuenta dian.pdf"
- sha256 7a8dc7adfec488d907201785cc4e9a6519ff955c2e1f66d5a6ad933190a73f18
- sha1 98d267d3531c50c05166da4b9b67628ddda5b550
- md5 3234897985f74322eaef9b4cf6ca9765

Dropped executable file
- sha256 C:\Users\admin\AppData\Local\Temp\Rar$EXb2652.47403\pdfestadodecuentadian.exe
  8d07790c1bca6f041466c8ac759e5784c6566f1d4cae04fe4c47d21f7ae09a43

DNS requests
- domain acortaurl.com
- domain www.mediafire.com
- domain www.bing.com
- domain download1091.mediafire.com

Connections
- ip 104.24.115.152
- ip 205.196.122.32
- ip 104.16.202.237

HTTP/HTTPS requests
- url http://www.bing.com/favicon.ico
- url http://www.mediafire.com/file/gop1d6zqpbo0fqv/pdfestadodecuentadian.zip/file

## Recomendaciones

- Siempre verifique la legitimidad de la cuenta de donde proviene el correo electrónico.
- No haga clic en enlaces que vengan en los correos electrónicos, siempre ingrese directamente a la dirección oficial del sitio.
- Siempre este atento a la intencionalidad de los correos electrónicos, ya que los atacantes siempre buscan generar miedo para que accedan a sus peticiones.
- Si no esta seguro de la procedencia del correo o los archivos no los abra y reportelos.

## Contáctenos

Si tienes alguna consulta técnica comunicarse con CSIRT Gobierno a través de los siguientes canales:

Csirtgob@mintic.gov.co

**01 8000 910742 Opción 4.**