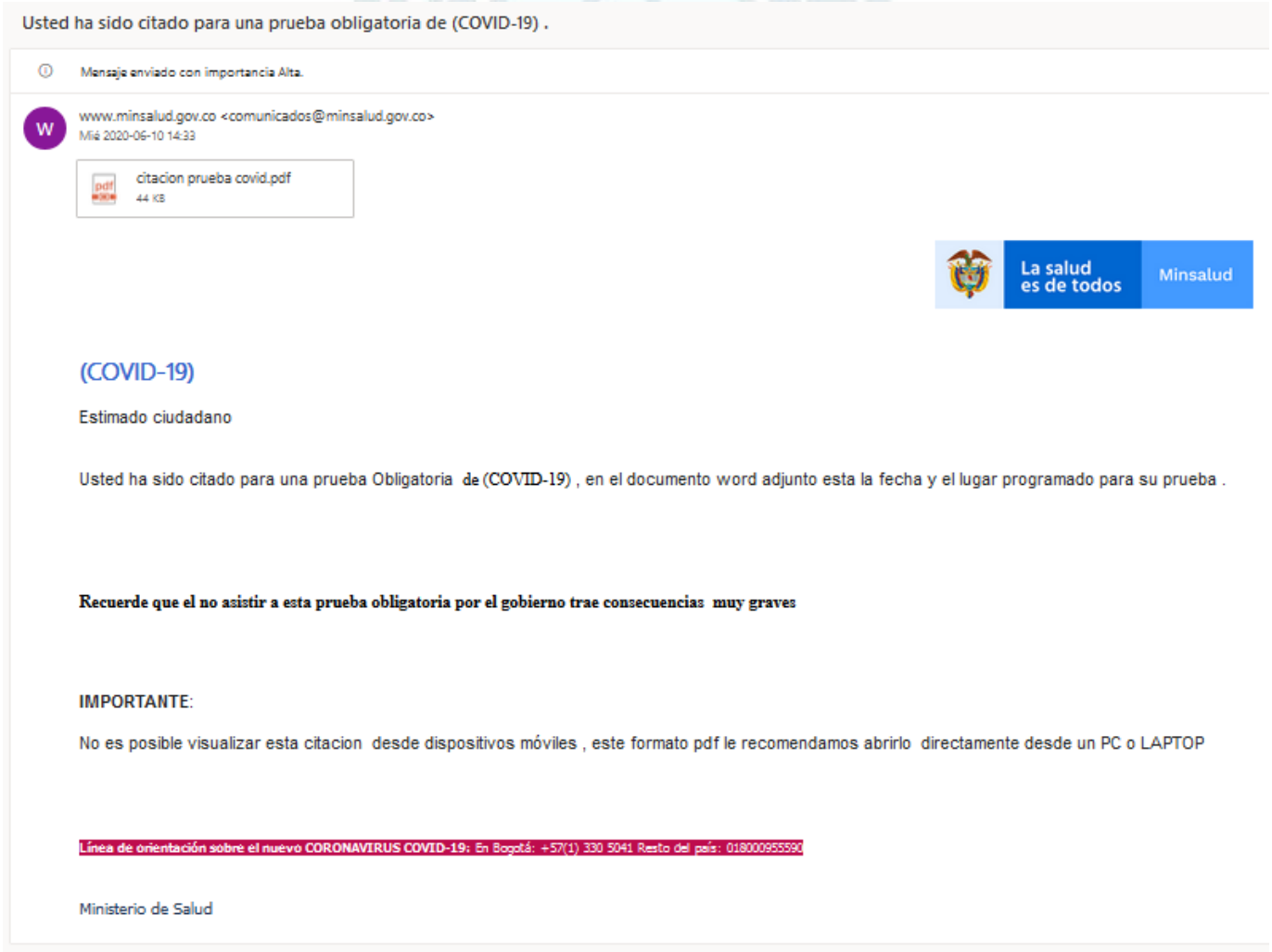
16/06/2020

Alerta - Correo malicioso

Correo Malicioso
Suplantación MinSalud

Dada la declaración de emergencia sanitaria en Colombia a raíz de la pandemia por el COVID-19, varias entidades han reportado en repetidas oportunidades un correo sospechoso proveniente de la cuenta de correo ***comunicados@minsalud.gov.co*** con el siguiente asunto, que simula urgencia: **"Usted ha sido citado para una prueba obligatoria de (COVID-19");** en el cuerpo de dicho mensaje, se indica que *supuestamente* tienen una información relevante para el interés del usuario y adjuntan un archivo PDF donde según se indica en el correo, se amplía la información correspondiente.

Al realizar una revisión de los múltiples correos reportados, inicialmente se identifica que se realizó una suplantación del dominio de la entidad, dado que al revisar los encabezados se encuentran diferentes direcciones IP de origen las cuales **no pertenecen** a MinSalud.



Usted ha sido citado para una prueba obligatoria de (COVID-19) .

Mensaje enviado con importancia Alta.

www.minsalud.gov.co <comunicados@minsalud.gov.co>
Mié 2020-06-10 14:33

citacion prueba covid.pdf
44 KB

La salud es de todos Minsalud

(COVID-19)

Estimado ciudadano

Usted ha sido citado para una prueba Obligatoria de (COVID-19) , en el documento word adjunto esta la fecha y el lugar programado para su prueba .

Recuerde que el no asistir a esta prueba obligatoria por el gobierno trae consecuencias muy graves

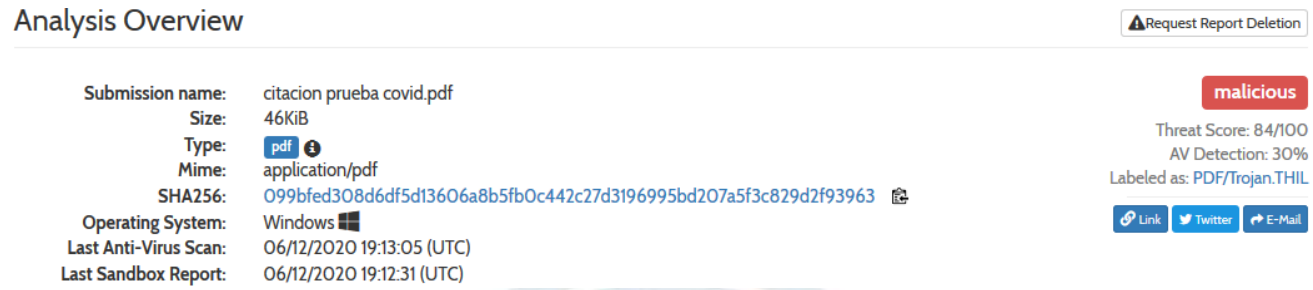
IMPORTANTE:

No es posible visualizar esta citacion desde dispositivos móviles , este formato pdf le recomendamos abrirlo directamente desde un PC o LAPTOP

Línea de orientación sobre el nuevo CORONAVIRUS COVID-19: En Bogotá: +57(1) 330 5041 Resto del país: 018000955590

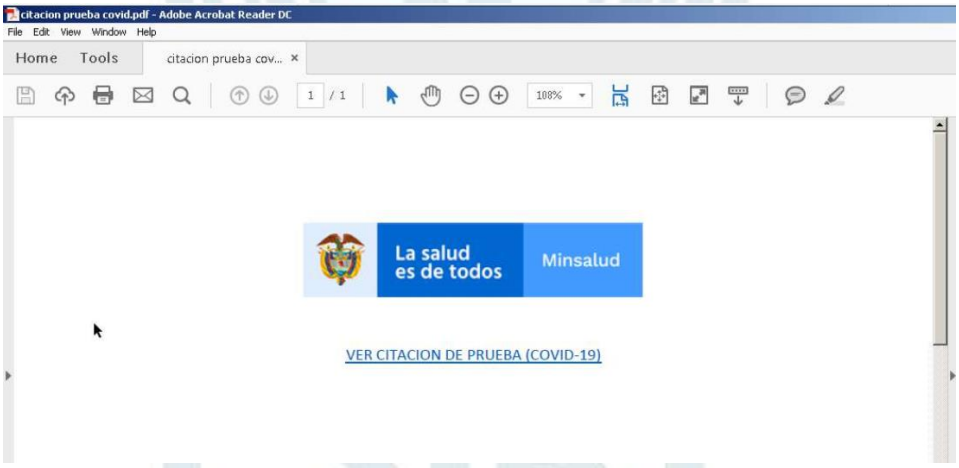
Ministerio de Salud

Por otra parte, se realiza el análisis de los archivos remitidos y su contenido se encuentra catalogado como malicioso.



Ver reporte completo: https://bit.ly/3fjJYfm

Al hacer un análisis detallado del mismo, el PDF contiene solo un enlace con el nombre "*ver citación prueba (COVID-19)*", al hacer click en este enlace se abre el navegador y redirecciona a la URL hxxps://acorturl[.]com/SWVnX y en segundo plano se inicia la conexión a diferentes servidores DNS e intenta conectarse a diferentes direcciones IP, de las cuales varias están catalogadas como sospechosas.



Main object- "citacion prueba covid.pdf"

sha256 099bfed308d6df5d13606a8b5fb0c442c27d3196995bd207a5f3c829d2f93963
sha1 7895c483a5fbb1bc445a93cb017deedd6bff9927
md5 825c1800c6fadab4e71a4dee0980b6e6

DNS requests

domain d1l6p2sc9645hc[.]cloudfront[.]net
domain t[.]co
domain data2[.]gosquared[.]com

Connections

ip 2[.]21[.]36[.]203
ip 2[.]16[.]107[.]73
ip 2[.]16[.]107[.]114
ip 104[.]24[.]114[.]152

ip	151[.]101[.]1[.]44
ip	151[.]101[.]2[.]202
ip	104[.]19[.]148[.]8
ip	23[.]202[.]52[.]174
ip	151[.]101[.]12[.]157
ip	173[.]212[.]234[.]128

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 esté atento a la intencionalidad de los correos electrónicos, ya que los atacantes siempre buscan simular urgencia para que accedan a sus peticiones
- Verificar las URLs y archivos adjuntos antes de descargarlos en páginas como Virus total y/o hybrid analysis
- Si no está seguro de la procedencia del correo o los archivos no los abra y repórtelos
- Toda la información relacionada con la emergencia se encuentra publicada en el sitio oficial: https://coronaviruscolombia.gov.co/Covid19/index.html

Contáctenos

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

Csirtgob@mintic.gov.co

01 8000 910742 Opción 3.