01/07/2020

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 ***pruebascuidadania@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) .

www.minsalud.gov.co <pruebascuidadania@minsalud.gov.co>
Mié 2020-07-01 10:27

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

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

Analysis Overview

Request Report Deletion

Submission name:	citacion prueba covid.pdf
Size:	46KiB
Type:	pdf
Mime:	application/pdf
SHA256:	50fc85479949ac0449f3f66d97837a93a000d60dbaa3c8c80bfb7cb0a51105cf
Operating System:	Windows
Last Anti-Virus Scan:	07/01/2020 20:48:24 (UTC)
Last Sandbox Report:	07/01/2020 20:48:22 (UTC)

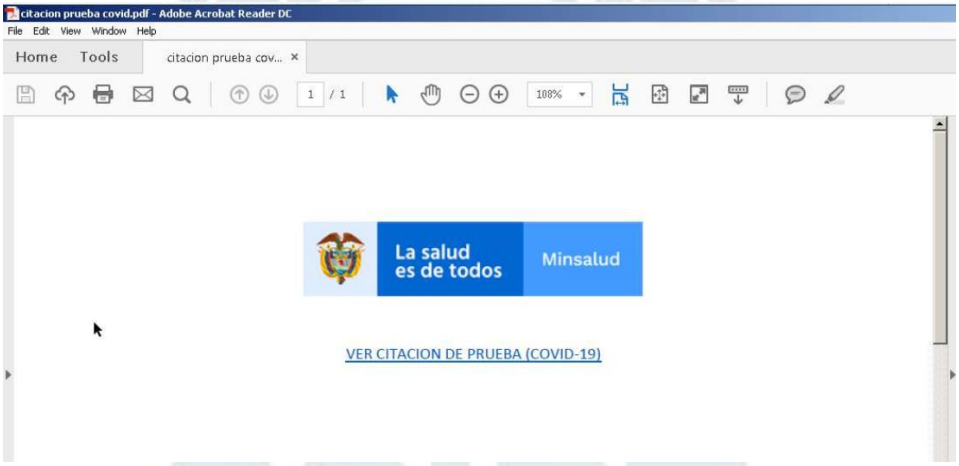
malicious

Threat Score: 85/100
AV Detection: 26%
Labeled as: PDF.Phishing

Link Twitter E-Mail

Ver reporte completo: https://bit.ly/2VzLsKY

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://acortaurl[.]com/mimnsaludpp 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	50fc85479949ac0449f3f66d97837a93a000d60dbaa3c8c80bfb7cb0a51105cf
sha1	e0b0882d9db9683b06eb44bdc576c95fd51972e6
md5	cb227298bca6149e194339adde4124f5

Connections

ip	184[.]173[.]200[.]12
ip	172[.]67[.]187[.]194
ip	192[.]35[.]177[.]64
ip	2[.]16[.]107[.]73
ip	2[.]16[.]107[.]114
ip	104[.]108[.]58[.]248
ip	99[.]86[.]7[.]229
ip	184[.]173[.]200[.]13
ip	50[.]97[.]172[.]202
ip	54[.]197[.]13[.]220
ip	151[.]101[.]1[.]44

ip	104[.]121[.]152[.]36
ip	143[.]204[.]208[.]165
ip	172[.]217[.]23[.]98
ip	52[.]222[.]147[.]46
ip	54[.]173[.]29[.]20
ip	2[.]16[.]107[.]24
ip	104[.]19[.]147[.]8
ip	147[.]75[.]33[.]233
ip	2[.]16[.]107[.]8
ip	147[.]75[.]85[.]120
ip	54[.]210[.]109[.]30
ip	147[.]75[.]102[.]197
ip	151[.]101[.]2[.]202
ip	23[.]42[.]18[.]223
ip	104[.]18[.]21[.]226

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.