CSIRT GOBIERNO DE COLOMBIA

El futuro digital es de todos | Gobierno de Colombia MinTIC

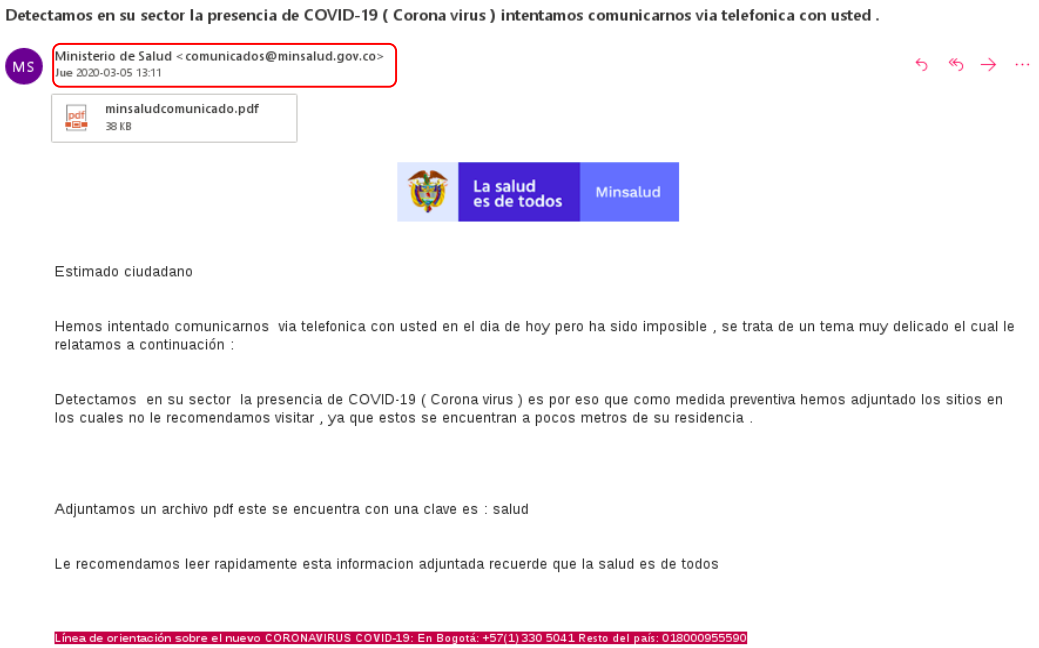
06/03/2020

Alerta - Correo malicioso

Correo Malicioso
Suplantación MinSalud

El día 06 de marzo varias entidades han reportado un correo sospechoso proveniente de la cuenta de correo ***comunicados@minsalud.gov.co*** con el asunto **"Detectamos en su sector la presencia de COVID-19 (Corona virus) intentamos comunicarnos via telefonica con usted",** donde se indica que se ha detectado la presencia del virus COVID-19 en el sector de residencia y adjuntan un archivo PDF donde según el cuerpo de correo, se encuentra la información ampliada de dicha alarma.

Al realizar una revisión del contenido del correo, inicialmente se identifica que se realizó una suplantación del dominio, dado que al revisar los encabezados se encuentra que la IP de origen (128.90.112.209) del correo **no pertenece** a MinSalud.



Detectamos en su sector la presencia de COVID-19 (Corona virus) intentamos comunicarnos via telefonica con usted .

MS Ministerio de Salud <comunicados@minsalud.gov.co>
lue 2020-03-05 13:11

minsaludcomunicado.pdf
38 KB

La salud es de todos | Minsalud

Estimado ciudadano

Hemos intentado comunicarnos via telefonica con usted en el dia de hoy pero ha sido imposible , se trata de un tema muy delicado el cual le relatamos a continuación :

Detectamos en su sector la presencia de COVID-19 (Corona virus) es por eso que como medida preventiva hemos adjuntado los sitios en los cuales no le recomendamos visitar , ya que estos se encuentran a pocos metros de su residencia .

Adjuntamos un archivo pdf este se encuentra con una clave es : salud

Le recomendamos leer rapidamente esta informacion adjuntada recuerde que la salud es de todos

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

Por otra parte, se realiza el análisis del archivo adjunto y su contenido se encuentra catalogado como malicioso.

Submission name:	minsaludcomunicado.pdf
Size:	40KiB
Type:	pdf
Mime:	application/pdf
SHA256:	df6a1c0438e73f8ef748fd436b4199cf79d76f92e493e02e1d0fa36152697c4a
Operating System:	Windows
Last Anti-Virus Scan:	03/06/2020 14:04:07 (UTC)
Last Sandbox Report:	03/05/2020 21:52:35 (UTC)

malicious

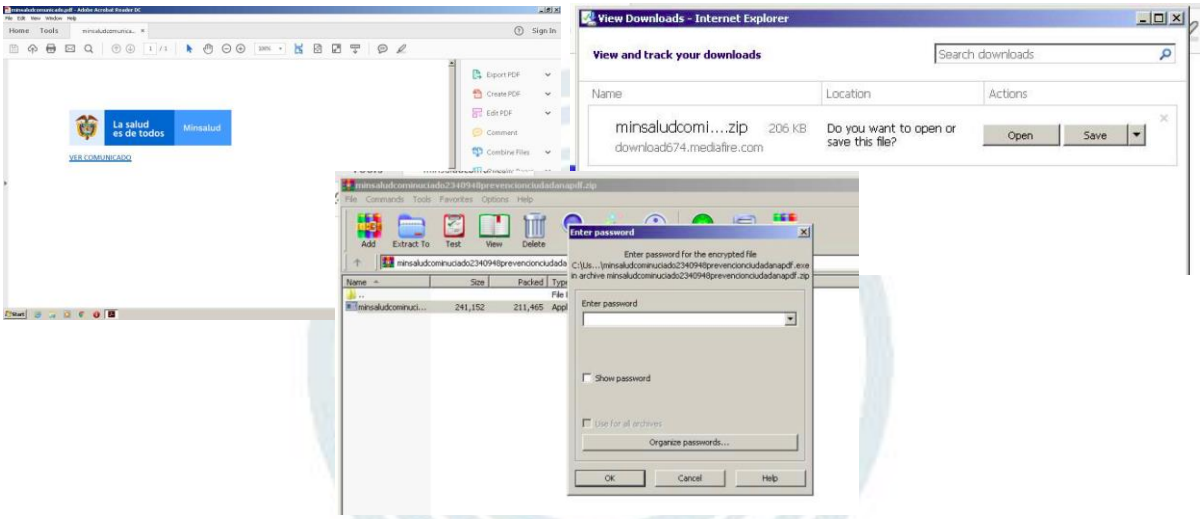
Threat Score: 78/100
AV Detection: 31%
Labeled as:
TROJ_FRS.VSNW.BdId5C2.BdId

Link | Twitter | E-Mail

Ver reporte completo: https://bit.ly/38E4JyS

#MásTICMejorPaís

Al hacer un análisis detallado del mismo, el PDF contiene solo un enlace con el nombre "*ver mi comunicado*", este link redirecciona al usuario a una página 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, se descraga un .exe que 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:

Minsaludcomunicado.pdf
- sha256 df6a1c0438e73f8ef748fd436b4199cf79d76f92e493e02e1d0fa36152697c4a
- sha1 ee0a4642f174c38824c4728d5f8045398543536e
- md5 290e9f0d52265eff7f79e94d1fcb00c3

Executable file
- sha256 19e3d412c8c76d11d1b54ccc97e187c3576c886f3abc59e22faf3e98f563c9be

DNS requests
- domain acortaurl[.]com
- domain download674[.]mediafire[.]com
- domain mediafire[.]com

Connections
- ip 104[.]24[.]115[.]152
- ip 104[.]16[.]202[.]237
- ip 205[.]196[.]120[.]122
- ip 92[.]122[.]255[.]51

HTTP/HTTPS requests
- hxxp://www.mediafire.com/file/f3zewybq24cu5o9/minsaludcominuciado2340948prevencionciudadanapdf[.]zip
- hxxp://www.bing.com/favicon[.]ico
- hxxp://download674.mediafire.com/vqlcx7eurv9g/f3zewybq24cu5o9/minsaludcominuciado2340948prevencionciudadanapdf[.]zip

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 generar miedo para que accedan a sus peticiones.
- Si no está seguro de la procedencia del correo o los archivos no los abra y repórtelos.

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.