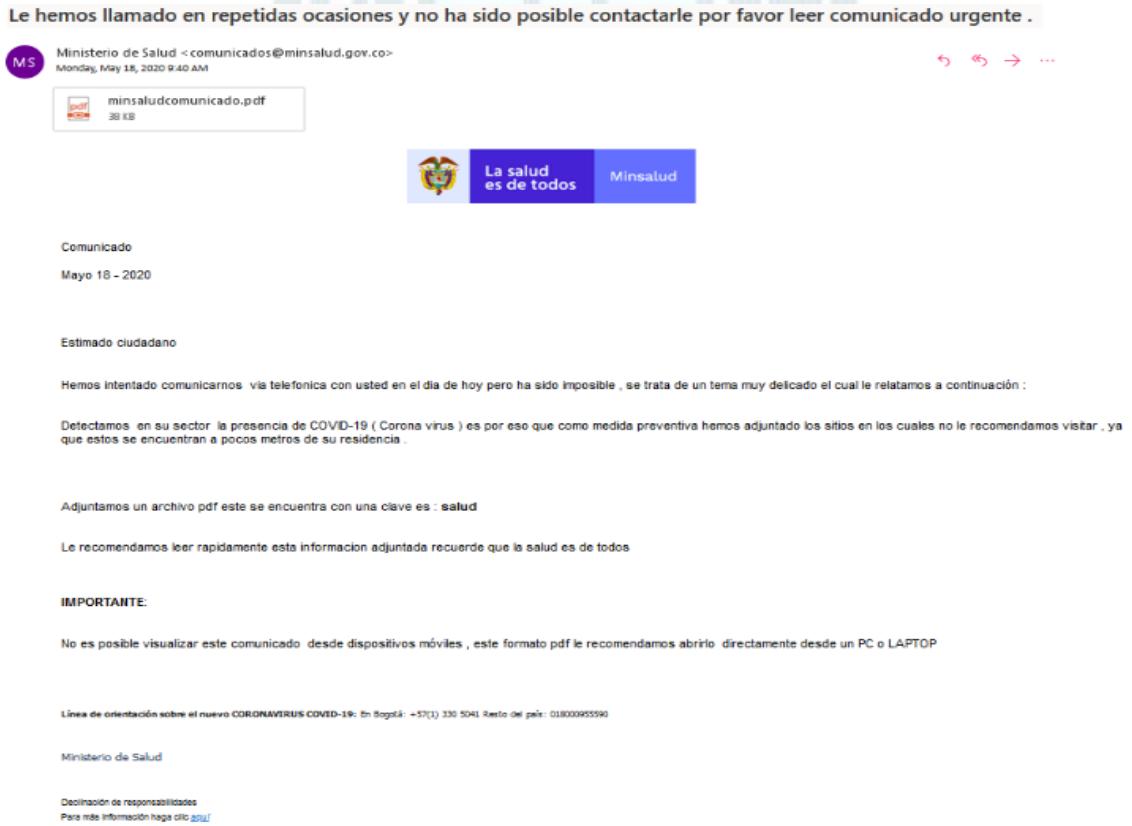
28/05/2020

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: **"Le hemos llamado en repetidas ocasiones y no ha sido posible contactarle por favor leer comunicado urgente";** 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.



Le hemos llamado en repetidas ocasiones y no ha sido posible contactarle por favor leer comunicado urgente .

Ministerio de Salud <comunicados@minsalud.gov.co>
Monday, May 18, 2020 9:40 AM

minsaludcomunicado.pdf
38 KB

La salud es de todos | Minsalud

Comunicado

Mayo 18 - 2020

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

IMPORTANTE:

No es posible visualizar este comunicado 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

Declinación de responsabilidades
Para más información haga clic aquí

Por otra parte, se realiza el análisis de los archivos remitidos 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)

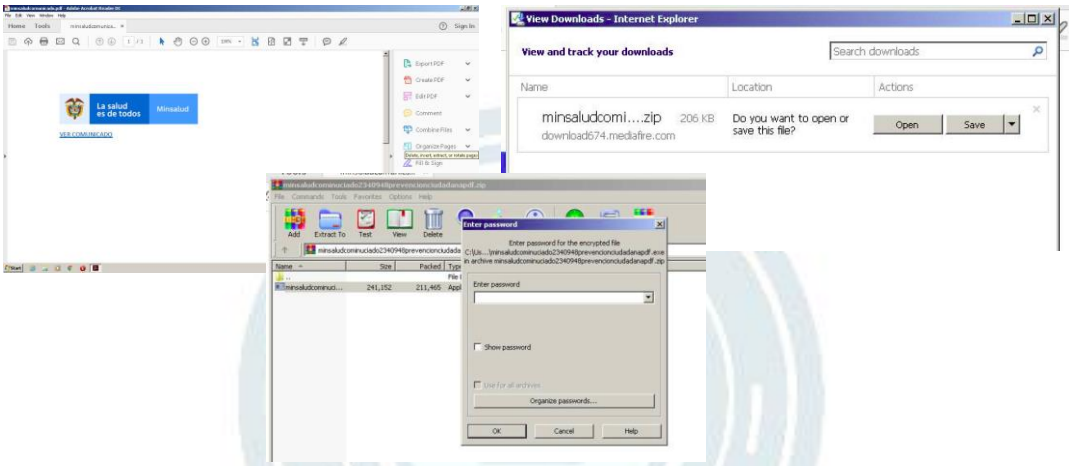
malicious

Threat Score: 78/100
AV Detection: 31%
Labeled as:
TROJ_FRS.VSNW.Bdld5C2.Bdld

Link | Twitter | E-Mail

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

Al hacer un análisis detallado del mismo, el PDF contiene solo un enlace con el nombre "*ver 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 descarga un .exe que se ejecuta automáticamente 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.

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.
- 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.