CSIRT
GOBIERNO DE COLOMBIA

El futuro digital es de todos
Gobierno de Colombia
MinTIC

12/03/2020

Boletín – Campañas (COVID-19)

Con la aparición del COVID-19 o corona virus, el CSIRT de Gobierno identificó eventos de seguridad digital como:

1. Noticias falsas:

Desde la aparición del (COVID-19) o Coronavirus, se han generado diversas narrativas maliciosas (noticias falsas, medias verdades y/o hechos descontextualizados) por parte de páginas y medios potencialmente desinformativos que posteriormente han sido distribuidos y compartidos a través de varios portales web y redes sociales, entre las que se argumentan teorías como: **"el coronavirus es un arma de guerra creada en un laboratorio"** o **"Coronavirus, ¿la excusa para la vacuna que alterará nuestro ADN para siempre?**.

ALERTANACIONAL

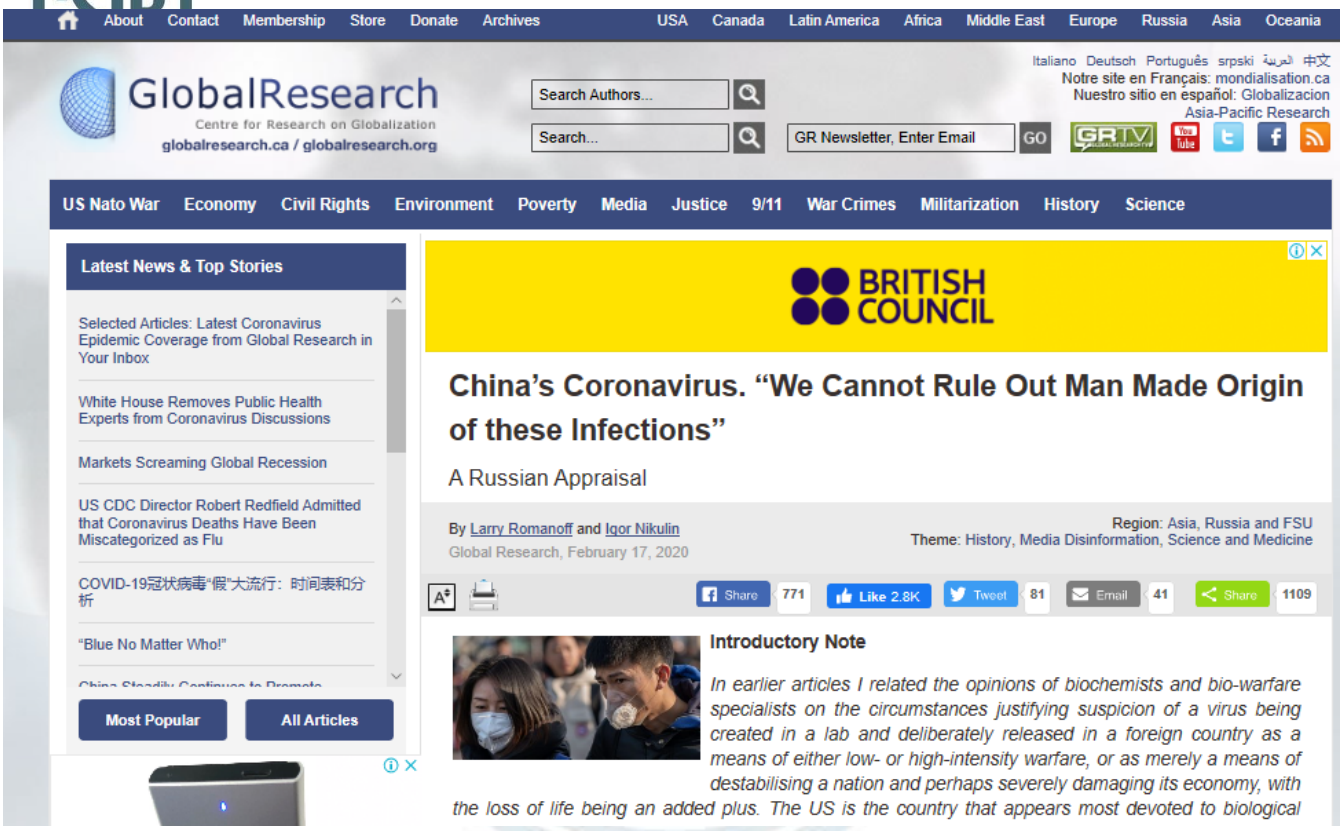
ESPAÑA REGIONES DE ESPAÑA INTERNACIONAL SOCIEDAD ECONOMÍA DEPORTES SUCESOS OPINIÓN CINE Y TELEVISIÓN REDES SOC

CIENCIA Y TECNOLOGÍA

Coronavirus, ¿la excusa para la vacuna que alterará nuestro ADN para siempre?

Published 1 semana agoon 03/03/2020
By REDACCION

#MásTIC MejorPaís

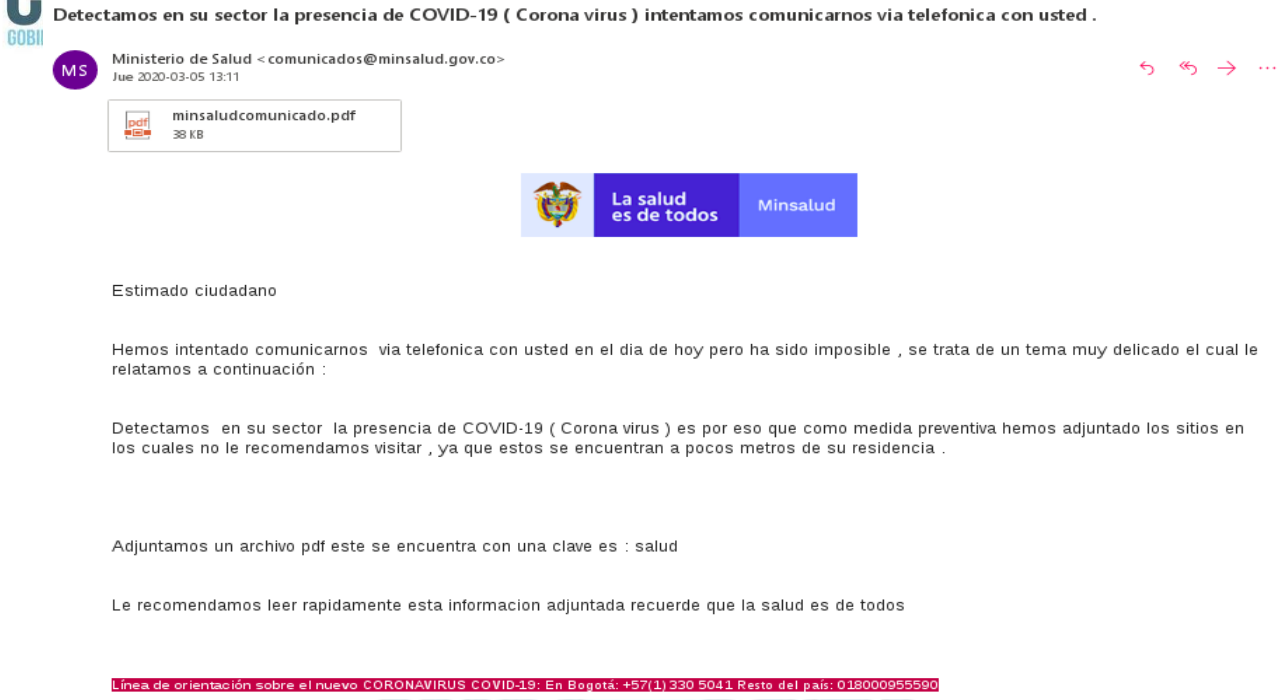


1.1. Recomendaciones

- Remitirse a los medios oficiales, para ello el gobierno nacional a dispuesto el siguiente portal, en donde se publica toda la información relevante referente al (COVID-19) o coronavirus https://go.gov.co/Covid-19
- Verificar y contrastar la información en medios oficiales y paginas confiables.
- **No** compartir información de la que no se esté seguro y no hayamos podido verificar.
- A pesar de que la información este publicada en una página que cuente con certificado HTTPS https:// y este en otro idioma como Ingles, **No** significa que la información sea confiable.

2. Campañas de phishing

A través de correo electrónico, se envían correos suplantando al Ministerio de Salud con asuntos como: **"Detectamos en su sector la presencia de COVID-19 (Corona virus) intentamos comunicarnos vía telefónica con usted",** donde se indica que se ha detectado la presencia del virus COVID-19 en el sector de residencia y adjuntan archivos que contienen códigos maliciosos.



2.1. Indicadores de compromiso (IoC) del archivo:

A continuación, se incluyen los indicadores de compromiso con el fin de que se puedan identificar otros equipos de cómputo afectados o prevenir su afectación.

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

2.2. Recomendaciones

- Siempre verificar la legitimidad de la cuenta de donde proviene el correo electrónico.
- No hacer clic en enlaces que vengan en los correos electrónicos, siempre ingresar directamente a la dirección oficial del sitio.
- Siempre estar 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.

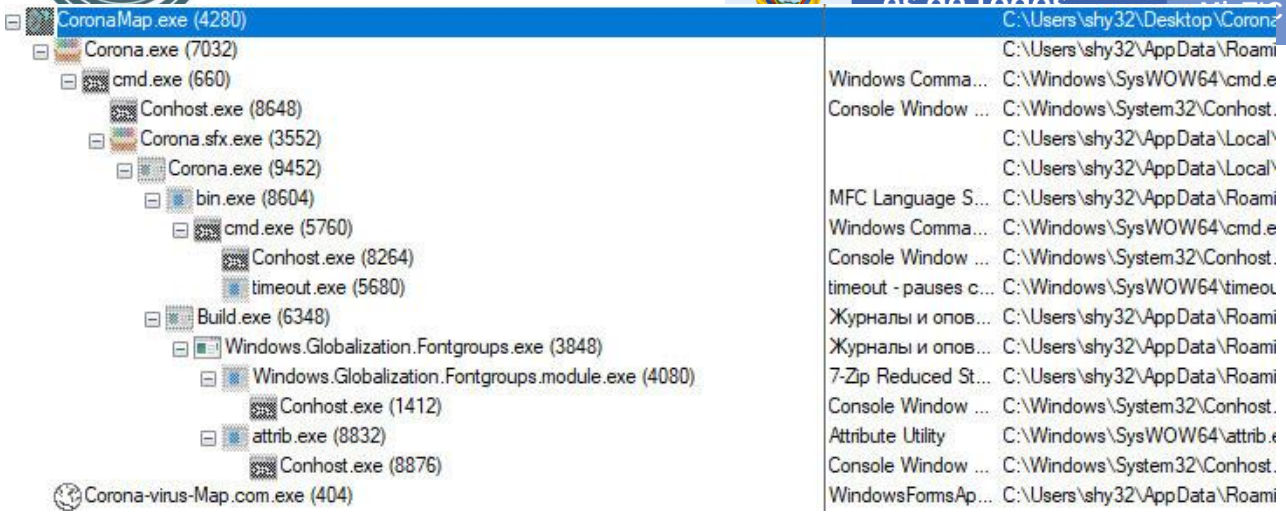
3. Difusión de malware en aplicaciones relacionadas con información del coronavirus

Los cibercriminales han utilizado algunas aplicaciones de 'Mapas de Coronavirus' para infectar los equipos de cómputo con malware con el fin de robar contraseñas e información.

El ataque de malware apunta específicamente a las personas que buscan presentaciones cartográficas de la propagación de COVID-19 en Internet, y los engaña para que descarguen y ejecuten una aplicación maliciosa que, en su interfaz, muestra un mapa cargado desde un archivo legítimo de una fuente en línea, pero en el fondo compromete el equipo de cómputo.

La ejecución de Corona-virus-Map.com.exe da como resultado la creación de duplicados del archivo Corona-virus-Map.com.exe y múltiples Corona.exe, Bin.exe, Build.exe y

Windows.Globalization.Fontgroups. archivos exe.



Además, el malware modifica un puñado de registros en ZoneMap y LanguageList. También se crean varios mutexes. La ejecución del malware activa los siguientes procesos: Bin.exe, Windows.Globalization.Fontgroups.exe y Corona-virus-Map.com.exe. Estos intentan conectarse a varias URL.

3.1. Indicadores de compromiso (IoC) del archivo:

A continuación, se incluyen los indicadores de compromiso con el fin de que se puedan identificar otros equipos de cómputo afectados o prevenir su afectación. Todos los indicadores de compromiso pueden ser consultados en: https://blog.reasonsecurity.com/2020/03/09/covid-19-info-stealer-the-map-of-threats-threat-analysis-report/

Muestra analizada:
https://www.virustotal.com/gui/file/2b35aa9c70ef66197abfb9bc409952897f9f70818633ab43da85b3825b256307/detection
Nombre de archivo Corona-virus-Map.com.exe
MD5 73da2c02c6f8bfd4662dc84820dcd983
SHA-1 949b69bf87515ad8945ce9a79f68f8b788c0ae39
SHA-256 2b35aa9c70ef66197abfb9bc409952897f9f70818633ab43da85b3825b256307
Tamaño de archivo 3,26 MB (3421696 bytes)
Tipo de archivo Win32 EXE
Primera presentación 2020-03-02 16:50:25

3.2. Recomendaciones

- Mantener instalado y actualizado un antivirus en todos sus dispositivos.
- **No** descargar software y aplicaciones de páginas no oficiales.
- Mantener todos sus dispositivos actualizados y aplicar los últimos parches de seguridad, liberados por los fabricantes.

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.