TARJETA INFORMATIVA 018/2020

Washington, D.C., a 25 de marzo de 2020

2020 "Año de Leona Vicario, Benemérita Madre de la Patria"

Modos de operación relacionados con ciberdelitos motivados por la alerta sanitaria del Covid2019

Antecedentes

En días pasados el *Federal Bureau of Investigation* (FBI) publicó que ***los usuarios de Internet podrían ser víctimas de robo de su dinero, información personal o cualquier otro fraude, ya que los estafadores cibernéticos están aprovechando la pandemia de COVID-19***.

Introducción

La situación actual de alerta sanitaria con motivo del COVID-2019 está propiciando que los delincuentes se aprovechen de ésta. Los cibercriminales son conscientes de la incertidumbre y la sensibilidad que la enfermedad está provocando en la sociedad para aprovechar el empleo de tecnologías de la información y de la comunicación (TIC).

De este modo, independientemente de conductas identificadas para ofertas de bienes y servicios a precios superiores a su valor en el mercado o por parte de operadores no autorizados, el fraude en Internet ha encontrado una nueva ventana de oportunidad para la comisión de estafas online, empleando diferentes plataformas para conducir al engaño de ciudadanos. También se están detectando campañas de difusión de malware aprovechando la necesidad de información que el COVID-2019 despierta en el ciudadano.

Derivado de información recibida por diferentes agencias policiales, se conoce de la existencia de los siguientes modos de operación.

Tendencias Criminales Identificadas (Modos de Operación)

- Se ha detectado una proliferación de páginas web falsas creadas para vender productos sanitarios. Normalmente son sitios web donde se venden geles desinfectantes, guantes o mascarillas asegurando la entrega en poco tiempo. Permiten el abono del producto mediante tarjeta de crédito/débito, pero suelen ofrecen descuentos si se paga mediante trasferencia bancaria. Una vez realizado el pedido, no llega nada y es imposible contactar con el vendedor
- Además, han aparecido individuos y empresas que explotando la situación del Coronavirus ofrecen curas falsas que se venden en línea

- También, se conoce del envío de correos electrónicos masivos (*spam*) que contienen mensajes donde se suplantan sitios web oficiales (*phising*) como Cruz Roja, la Organización Mundial de la Salud, hospitales y otros similares, solicitando contribuir económicamente a campañas solidarias. Se han observado campañas similares que se trasmiten aprovechando el alcance de redes sociales como *Twitter, Instagram* o *Facebook* o aplicaciones de mensajería tipo *Whatsapp* o *Telegram*
- Asimismo, se ha detectado el envío de correos electrónicos masivos (*spam),* con contenidos relacionados con el COVID-19 y que llevan adjuntos archivos que, al descargarlos, ejecutan malware tipo ransomware o troyanos bancarios. **Imagen 1.-** Se simula un correo de la Organización Mundial de la Salud (OMS) donde se adjunta un archivo .ZIP o .RAR con un supuesto libro, el cual una vez descargado, ejecuta el troyano *GuLoader* que roba todo tipo de información personal.

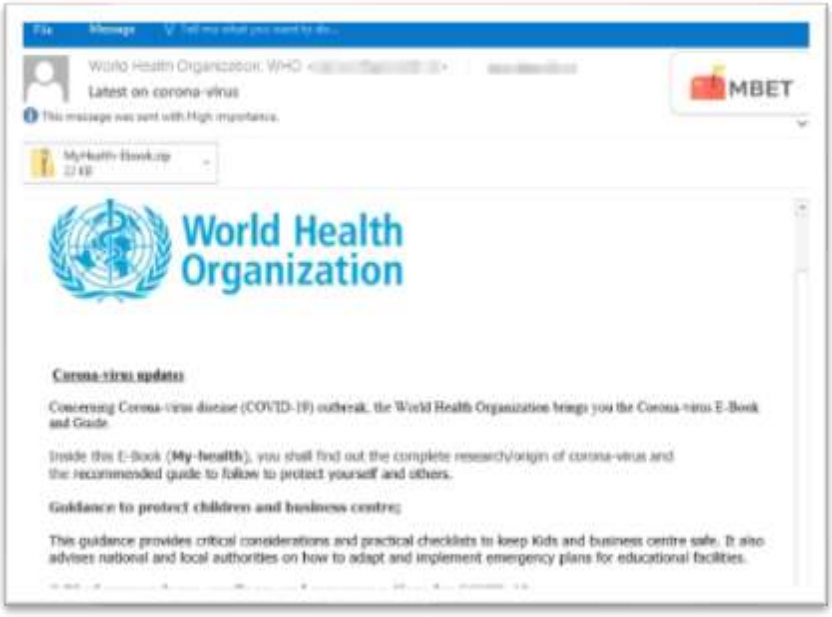


Imagen 1, fuente https://blog.malwarebytes.com/social-engineering/2020/03/cybercriminals-impersonate-world-health-organization-to-distribute-fake-coronavirus-e-book/

- Otra manera de dispersar malware viene vinculada a los distintos mapas interactivos o infografías interactivas. En este caso se invita acceder a determinados apartados de estos sitios web, procediéndose a la descarga automática del malware. **Imagen 2.-** Distribución del malware AZORult[1] contenido en un mapa sobre incidencia del coronavirus.

[1] Malware que roba información personal tipo *cookies*, historial de navegación o contraseñas

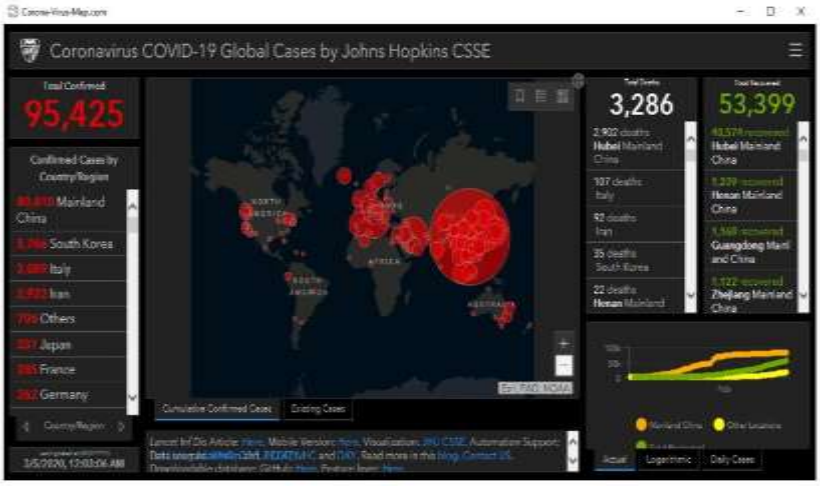
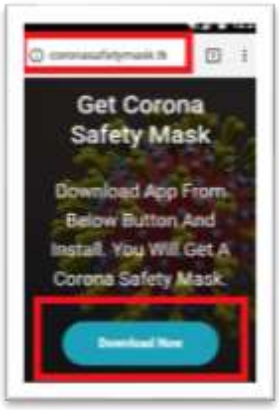


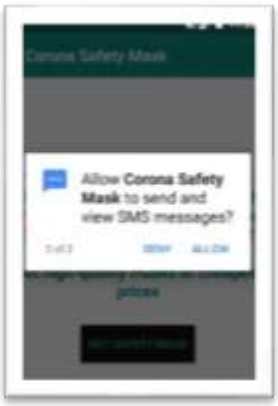
Imagen 2, fuente https://www.cybereason.com/blog/just-because-youre-home-doesnt-mean-youre-safe

- También, campañas de distribución de malware para dispositivos móviles mediante la descarga de aplicaciones. El usuario cree que instala una aplicación oficial, pero realmente se ejecuta un malware que roba los datos bancarios. **Imagen 3.-** La aplicación "*Ways to Get Rid of Coronavirus*" supuestamente creada por la **Organización Mundial de la Salud.** El usuario descarga el troyano bancario *Cerberus* que extrae las claves de la banca online.

Imagen 3, fuente https://www.cybereason.com/blog/just-because-youre-home-doesnt-mean-youre-safe

- Finalmente, se ha detectado una aplicación que facilita al usuario la adquisición de mascarillas. **Imagen 4a.-** El usuario realmente instala un ransomware que inutiliza el dispositivo. Además, como se le da el permiso de acceso a la agenda y enviar mensajes (**Imagen 4b**), envía un SMS a todos nuestros contactos (**Imagen 4c**) para que se descarguen la misma aplicación y así extender la "infección".





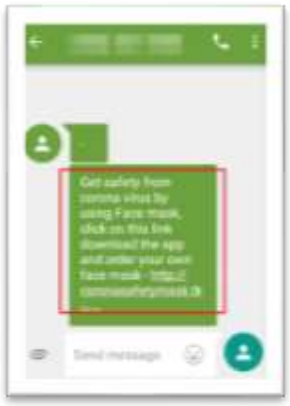


Imagen 4a **Imagen 4b** **Imagen 4c**

Fuente https://www.zscaler.com/blogs/research/new-android-app-offers-coronavirus-safety-mask-delivers-sms-trojan

Recomendaciones

- ✓ Se sugiere no hacer clic en enlaces, ni abrir archivos adjuntos que no reconozca o que no sean de confianza.
- ✓ Tener cuidado con los sitios web y las aplicaciones que dicen rastrear los casos de COVID-19 en todo el mundo. Recuerde que los delincuentes utilizan sitios web maliciosos para infectar y bloquear dispositivos hasta que se reciba el pago.
- ✓ Tener cuidado con cualquiera que venda productos que pretendan prevenir, tratar, diagnosticar o curar COVID-19, así como tratamientos o equipos falsificados.

Lo último que necesita la población en medio de esta pandemia, son los delincuentes que intentan sacar provecho de la ciudadanía y de sus preocupaciones.

Tarjeta Informativa elaborada por la Agregaduría de Guardia Nacional en la Embajada de México en los EUA, Washington, D.C., a partir de información proporcionada por la Policía Judicial de la Guardia Civil en España, Interpol y el Federal Bureau of Investigation (FBI).