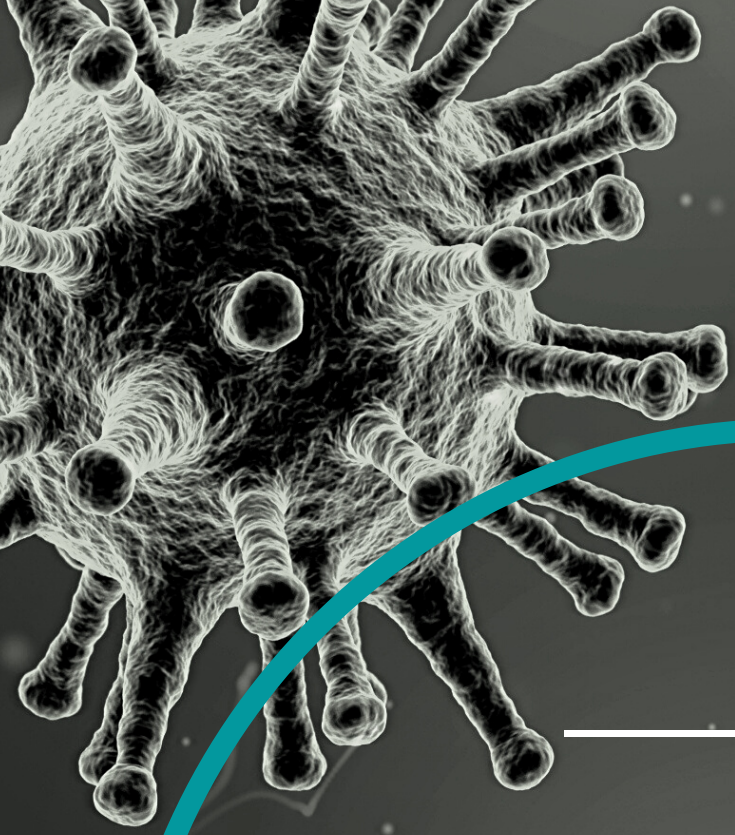

G.E.I.E.S.
GRUPO ESTATAL DE INTERVENCIÓN EN EMERGENCIAS SOCIALES

REPUNTE DE LAS CAMPAÑAS DE PHISHING

RELACIONADAS CON LA PANDEMIA COVID-19

24-03-2020

Consejo General del Trabajo Social

DOCUMENTO ELABORADO POR ticdatum

A los efectos de su máxima divulgación se participa la alerta emitida el 19 de marzo de 2020 por el equipo de Respuesta a Incidentes del Centro Criptológico Nacional, CCN-CERT, por la que se advierte que se está detectando un repunte importante de las campañas de malware que emplean temáticas relacionada con la pandemia del Coronavirus/COVID-19 para infectar a individuos y organizaciones de todo el mundo.

En estos momentos, existen registrados más de 24.000 dominios en Internet que contienen los términos: “coronavirus”, “corona-virus”, “covid19” y “covid-19”. De ellos, más de la mitad, 16.000, han sido creados en este mes de marzo (10.000 en la última semana). Algunos de ellos tienen fines legítimos y otros están dedicados a realizar campañas de spam, spear-phishing o como servidores de mando y control. También se ha detectado que algunos troyanos como Trickbot y Emotet han evolucionado sus TTP para evadir la detección, utilizando las noticias relacionadas con el coronavirus.

Medidas de prevención

Para prevenir la infección durante estas campañas, el CCN-CERT está llevando a cabo diferentes acciones y mantiene las siguientes recomendaciones:

- **Listas negras**
  El CCN-CERT ha recopilado en tres listas negras los indicadores que permiten la detección y bloqueo de muchas de estas campañas: listas de IP, dominios y hashes de las muestras empleadas. Estas listas se irán actualizando periódicamente. Pueden descargar dichas listas en el siguiente enlace: http://ccn-cert.net/cibercovid19
- **Ciberconsejos**
  Se han publicado una serie de ciberconsejos ante las campañas de malware (CiberCOVID19), tanto de phishing, como de desinformación prevención de incidentes y se ha creado un hilo en Twitter bajo los hashtag: #NoTeinfectesConElMail y #CiberCOVID19. Este hilo se actualiza diariamente con nuevas informaciones relacionadas con el coronavirus.
- **Teletrabajo**
  Del mismo modo, y sabedores de la vulnerabilidad que puede llegar a representar la generalización del teletrabajo, se ha publicado el Informe de Buenas Prácticas: CCN-CERT BP/18 Recomendaciones de Seguridad para situaciones de teletrabajo y refuerzo en vigilancia y el Abstract de Medidas de seguridad para acceso remoto.
- **Correo electrónico**
  Dado que el vector principal de infección para estas campañas es el correo electrónico, se recomienda revisar el Informe de Buenas Prácticas CCN-CERT BP/02 de correo electrónico.
- **Otras recomendaciones**
  Por último, es preciso mantener el Sistema Operativo y el antivirus actualizado, así como disponer de copias de seguridad offline (sin conexión con la red).

Dª Ana I. Martín Ramos, Exmagistrada, Abogada especializada en protección de datos
D. Iñaki Pariente de Prada, ExDirector de la Agencia Vasca de Protección de Datos,
abogado especializado en protección de datos