BOLETÍN INSTITUCIONAL
INSTITUTO NACIONAL DE SALUD

SEGURIDAD DE LA INFORMACIÓN: PHISHING Y CORONAVIRUS

Sonia Gutiérrez-García[1], Jaime Barrantes-Centurion[1], Jenny Sánchez-Silva[1]

Resumen

Los investigadores de seguridad de la información han identificado múltiples estafas de phishing que tienen como objetivo capitalizar el miedo de las personas con coronavirus, para ellos los estafadores se hacen pasar por autoridades Sanitarias como el CDC o la OMS con el fin de engañar a las personas para que entreguen su información personal. Mediante esta forma los usuarios pueden ser víctimas de los ciberdelincuentes. Este artículo presenta una breve información de las formas de ataques informáticos aprovechándose de los temas coyunturales que se están presentando a nivel mundial y las medidas que se deben tomar para no caer en estafas.

Palabras claves: Phishing (/fishing/), malware, ciberdelincuentes, seguridad de la información.

Introducción

A principios de febrero, se registraron las primeras infecciones del virus COVID-19, después de que se propagó por todo el mundo desde un epicentro en Wuhan, China.

Esta situación permite que los atacantes cibernéticos se aprovechen de los temores colectivos y coyunturales para hacerse pasar por funcionarios de salud, engañar a las personas y así obtener información personal. Los expertos en seguridad de la información advierten sobre la existencia de nuevas campañas de phishing diseñadas para aumentar los temores globales que existen en la actualidad.

El Phishing hace referencia a una de las tantas modalidades de estafa que utilizan los ciberdelicuentes con la finalidad de obtener información personal y de importancia, como las contraseñas, información de bancos u otra información personal que sirva al atacante para realizar actos delictivos.

[1] Oficina General de Información y Sistemas, Instituto Nacional de Salud (INS). Lima, Perú

Citar como: Gutiérrez-García S, Barrantes-Centurion J, Sánchez-Silva J. Seguridad de la información: phishing y coronavirus. Bol Inst Nac Salud. 2020;26 (1-2):17-21.

Existe una amplia variedad de técnicas que los phishers utilizan para lograr la obtención de información de sus víctimas. Aunque siempre hay indicadores y formas de identificar los casos de phishing, muchas veces no es fácil discernir cuándo un mensaje es legítimo y cuándo se trata de un phishing.

Phishing en correos sobre el coronavirus para el robo de credenciales

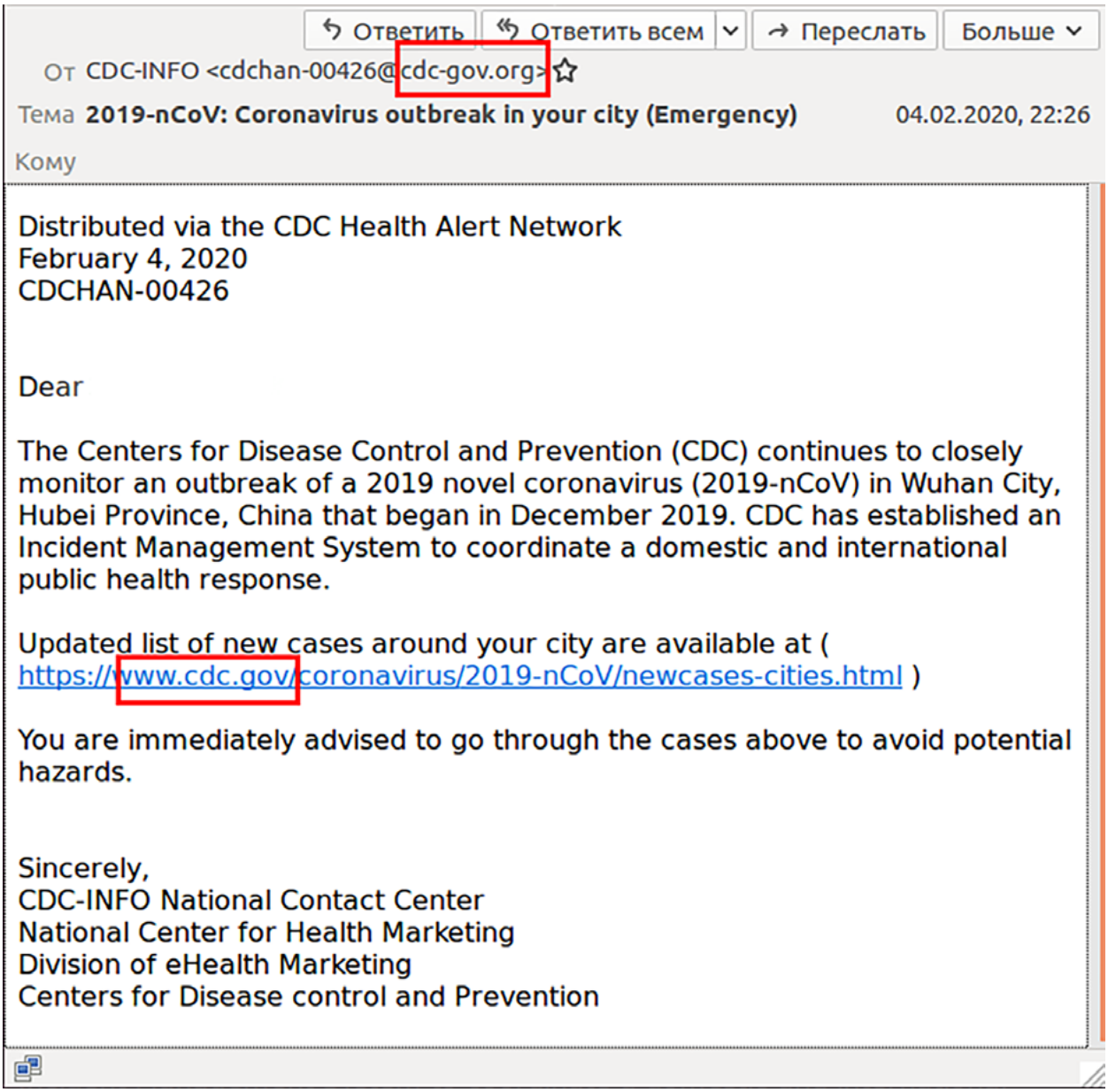
Los ciberdelincuentes buscan explotar la necesidad generalizada de noticias sobre el brote para usarlo como un señuelo. MIMECAST, es una compañía internacional especializada en la administración de correo electrónico basado en la nube, que ha detectado una de esas campañas, con correos electrónicos titulados ***"Especialista de Singapur: Medidas de seguridad del Coronavirus"*** en donde, al hacer clic en el enlace agregado dentro del correo electrónico conducirá a una descarga encubierta de malware.

Fuente: BlogBankia

"La única intención de estos actores de amenazas es jugar con el temor genuino del público para aumentar la probabilidad de que los usuarios hagan clic en un archivo adjunto o enlace entregado en una comunicación maliciosa, para causar infección o para obtener ganancias monetarias. Esta es una elección racional por parte de los delincuentes, ya que la investigación ha demostrado que más del 90% de los compromisos se producen por correo electrónico, y que más del 90% de esas infracciones son atribuibles principalmente a errores del usuario.", explicó el director de inteligencia de amenazas de MIMECAST, Francis Gaffney.

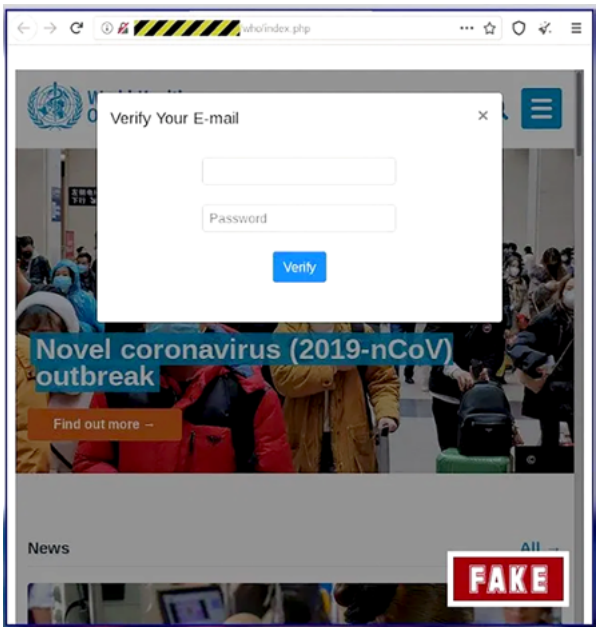
Kaspersky y Sophos; empresas antimalware; también han dado la voz de alarma sobre los ataques de phishing con temas de coronavirus, donde detectaron múltiples archivos pdf (acrobat), mp4 (videos) y docx (documentos de Word) maliciosos que afirmaban contener actualizaciones e información sobre cómo mantenerse a salvo del virus.

Ejemplo de mensaje de correo con temas de Coronavirus



En el supuesto mensaje enviado por el CDC indica que se ha creado un sistema para controlar y coordinar acciones referidas al tema de la Salud Pública y el Coronavirus tanto en el interior del país como fuera del mismo y exhorta a los destinatarios a que ingresen a una página adicional que les brindará información actualizada sobre casos nuevos de infección en su ciudad. Es importante notar que la interfaz del sitio web es idéntica a Microsoft Outlook, a pesar que el sitio no guarda ninguna relación con esta empresa. De manera intencionada solicita credenciales de inicio de sesión y una contraseña de manera que los delincuentes puedan robar credenciales de un email enviándoles los datos del usuario y contraseña para posteriormente acceder a la cuenta original de correo del usuario y pesquisar información de utilidad para cometer sus crímenes.

Otro ejemplo de estos correos son los siguientes:



> “La coyuntura de salud actual, en la que el coronavirus ha derivado en más de mil muertes alrededor del mundo según datos de la Organización Mundial de la Salud (OMS), ha llamado la atención de ciberdelincuentes que buscan aprovechar el brote para robar la información de los usuarios alrededor del mundo”.

El correo versa lo siguiente:

> “Acceda al documento adjunto para conocer las medidas de seguridad contra la propagación del coronavirus. Da clic en el botón debajo para descargar. Los síntomas comunes incluyen fiebre, tos, y problemas al respirar”.

Es importante tener en cuenta que la lectura atenta del email es lo más sencillo para detectar su falsedad. Se puede notar que el sitio del enlace contenido en el correo electrónico es HTTP y no HTTPS lo que indica que el sitio no cuenta con un certificado de seguridad. Este sitio fraudulento es una copia idéntica del sitio oficial de la OMS, y puede ser diferenciado de éste porque al abrirlo inmediatamente aparece una ventana emergente solicitando nuevamente datos de interés como el email y la contraseña del usuario, para luego supuestamente descargar el contenido.

Conclusiones

Lo peligroso de esta modalidad de ataque cibernético es que aprovecha la actual coyuntura del Coronavirus, sacando ventaja del miedo y la preocupación de los usuarios por tener cuanto antes información sobre la enfermedad al cliquear un enlace. Al hacerlo, el delincuente estará accediendo a datos de su correo electrónico y contraseña.

En la actualidad se dispone de herramientas que pueden ayudar a evitar ser víctimas de estas estafas, la mayor protección contra el phishing depende del mismo usuario. Es preciso que se conozcan los peligros y las técnicas empleadas en los phishing para que se puedan identificar de forma eficaz estos casos.

Para evitar este tipo de fraudes se recomienda:

- Mantenga el software de su equipo (PC o laptop) actualizada.
- No te dejes llevar por la presión.
- No abra correos de usuarios desconocidos o que no haya solicitado.
- No descargue ni abra archivos de fuentes no fiables ni responda a los correos sospechosos.
- No responda a solicitudes de información personal y financiera a través de correo electrónico. Las entidades financieras nunca lo hacen.
- Verifica la URL antes de dar clic. Comprobar que la página es segura, para ello la dirección de la página deberá comenzar con HTTPS://.
- Nunca envíes información personal que sea solicitada a través de correo de sitios no confiables o desconocidos. En caso de que ya lo hayas hecho, cambia tu contraseña de inmediato.
- No uses la misma contraseña para los diversos sistemas de información a los cuales tienes acceso. Proteja sus contraseñas.

Referencias

1. Coronavirus Attacks Aim to Spread Malware Infection [Internet]. 2020 [citado 10 marzo 2020]. Disponible en: https://www.infosecurity-magazine.com/news/coronavirus-attacks-malware
2. Mensajes de phishing sobre el coronavirus [Internet]. 2020 [citado 10 marzo 2020]. Disponible en: https://www.infosecurity-magazine.com/news/coronavirus-attacks-malware
3. Mimecast [Internet]. 2020 [citado 10 marzo 2020]. Disponible en: https://en.wikipedia.org/wiki/Mimecast
4. Detectan campaña de phishing en alerta sobre coronavirus [Internet]. 2020 [citado 10 marzo 2020]. Disponible en: https://codigoespagueti.com/noticias/internet/detectan-campana-de-phishing-en-alerta-sobre-coronavirus/
5. Email scammers are taking advantage of coronavirus fears to impersonate health officials and trick people into giving up personal information [Internet]. 2020 [citado 10 marzo 2020]. Disponible en: https://www.businessinsider.com/coronavirus-email-scam-covid-19-phishing-false-information-who-cdc-2020-2
6. Informe de divulgación Phishing [Internet]. 2020 [citado 10 marzo 2020]. Disponible en: https://www.seguridad.andaluciaesdigital.es/documents/410971/1437699/phising+2017/01950ce7-731f-48a6-821a-79388e571bff