Sophos detecta campaña de phishing en alerta sobre coronavirus

- *Según una encuesta de Sophos, el 36% de las 3,100 empresas encuestadas fueron víctimas de phishing*

Los ciberdelincuentes aman las crisis, porque les dan razones creíbles para contactar a potenciales víctimas y atacar mediante campañas de phishing. 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.

Sophos, la empresa líder en ciberseguridad de última generación, detectó una nueva campaña de phishing disfrazada de una alerta de coronavirus COVID-2019. Se trata de un email apócrifo a nombre de la OMS, que utiliza el logo de la organización y que advierte al usuario sobre la gravedad e impacto del coronavirus.

“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”, dicta el correo electrónico.

El primer indicio para detectar la falsedad del correo es sencilla: en el documento hay faltas de ortografía y errores de redacción. Sophos encontró también que el sitio al que redirige el enlace contenido en el correo electrónico es un HTTP y no un HTTPS, es decir, no cuenta con el certificado de seguridad que indica que la comunicación entre usuario y sitio web está encriptada, protocolo muy usual en la actualidad.

Este sitio web es una versión idéntica al sitio oficial de la OMS, con la diferencia de que al abrirlo aparece una ventana emergente que solicita al usuario su correo electrónico y la contraseña del mismo, para supuestamente dejarlo descargar el contenido.

El equipo de ciberseguridad de Sophos indica que los ciberdelincuentes no tardaron más allá de algunos minutos en realizar un *render* idéntico al del sitio oficial de la OMS y colocarlo detrás de la liga falsa.

El peligro de este ataque radica en que la preocupación de los usuarios por conocer información sobre el brote y las medidas para proteger a sus familiares y allegados puede derivar en que se le de clic al enlace. Una vez que esto sucede, tus datos de correo electrónico y contraseña estarán en poder de ciberdelincuentes.

Además, esa información estará abierta para todo aquel que esté conectado a la misma red que tú, por ejemplo, en caso de estar conectado a través del WiFi de un hotel o una cafetería, ya que son datos que enviaste en un sitio sin encriptación.

El usuario afectado no se da cuenta de que acaba de ser víctima de cibercriminales. Luego de escribir sus datos y dar clic en el botón 'Verificar', el sitio redirecciona al portal oficial de la OMS, que se ve idéntico al de la página previa.

¿Qué hacer para prevenirte de este ataque?

·No te dejes llevar por la presión

Es muy importante que ante crisis de este tipo el usuario no se sienta presionado a dar clic o acceder a sitios desconocidos por la preocupación que el propio virus le genera.

·Verifica la URL antes de dar clic

Si el sitio web desplegado no cuenta con el certificado HTTPS, busca de manera manual la página a la que fuiste redireccionado para rectificar que no se trate de un sitio apócrifo.

·Nunca escribas datos que un sitio no debería pedirte

No hay razón para que una advertencia de salud te pida tu correo electrónico y contraseña, por ejemplo.

·Si ya lo hiciste, cambia tu contraseña de inmediato

Si caíste en la trampa, entonces debes apresurarte. Los ciberdelincuentes no tardan demasiado en utilizar la información adquirida de sus víctimas para distintos fines, así que entre más rápido reacciones y cambies tu contraseña, mejor.

·No uses la misma contraseña para distintas plataformas

Cuando un cibercriminal obtenga tu correo y contraseña, es probable que la pruebe en diferentes plataformas o sitios web en los que tengas una cuenta. Utiliza distintas contraseñas, sobre todo en plataformas en las que la información que arrojas sea sensible.

Ante estas campañas que quieren aprovechar el pánico por el coronavirus, así como cualquier otro tipo de ataque, la tecnología de Sophos protege a las organizaciones de las diversas amenazas en materia de ciberseguridad, en donde el phishing figura como una de las prácticas más comunes entre ciberdelincuentes. De hecho, de acuerdo a la encuesta *El rompecabezas imposible de la ciberseguridad* realizada por Sophos, el 36% de las 3,100 empresas encuestadas fueron víctimas de phishing. Además, este tipo de ataque fue el más frecuente en todos los países estudiados estudiados, a excepción de Colombia, en el que fue la segunda amenaza más común.

# # #

Sobre Sophos

Como líder mundial en seguridad cibernética de última generación, **Sophos** protege a casi 400 mil organizaciones de todos los tamaños en más de 150 países de las amenazas cibernéticas más avanzadas de la actualidad. Desarrollado por SophosLabs -un equipo global de *Threat Intelligence* y *Data Science*- las soluciones nativas de la nube y mejoradas por IA de Sophos, aseguran protección en puntos finales (computadoras portátiles, servidores y dispositivos móviles) y redes contra tácticas y técnicas cibercriminales en evolución, incluidas las filtraciones de adversarios activos y automáticos, ransomware, malware, exploits, exfiltración de datos, phishing y más. La galardonada plataforma basada en la nube de Sophos Central integra toda la cartera de productos de **Sophos**, desde la solución de punto final, Intercept X, hasta el Firewall XG, en un único sistema llamado Seguridad Sincronizada. Los productos de **Sophos** están disponibles exclusivamente a través de un canal global de más de 47 mil socios y proveedores de servicios gestionados (MSP).
Sophos también pone a disposición de los consumidores sus innovadoras tecnologías comerciales a través de Sophos Home. La compañía tiene su sede en Oxford, Reino Unido, y cotiza en la Bolsa de Londres bajo el símbolo "SOPH". Más información está disponible en www.sophos.com

Síguenos en:
Facebook: https://www.facebook.com/SophosLatam/
Twitter: https://twitter.com/Sophos
LinkedIn: https://www.linkedin.com/company/sophos/
Instagram: https://www.instagram.com/sophossecurity/?hl=es-la
Youtube: https://www.youtube.com/user/SophosProducts

Contacto
Fernando Cornejo
fernando.cornejo@another.co

Mario García
mario@another.co
M.: 55 3930 2474