COVID-19: el disfraz de ‘moda’ entre ciberatacantes

- *Los ataques que usan el COVID-19 como pretexto para atraer a las víctimas se triplicaron en una semana*
- *Se estima que el 3% del volumen de spam actual tiene al coronavirus como palabra clave para su propagación*

Ciudad de México. 1 de abril de 2020.- SophosLabs ha detectado que durante las últimas semanas las palabras ‘COVID-19’ y ‘Coronavirus’ se están utilizando cada vez con mayor frecuencia en nombres de dominio apócrifos, spam, phishing y malware a nivel mundial.

En el informe ‘Enfrentando las innumerables amenazas vinculadas al COVID-19’, publicado en el blog de SophosLabs, la empresa líder en ciberseguridad de última generación muestra el volumen en el que se han incrementado las estafas de correo electrónico bajo estas palabras claves para enganchar la atención de los usuarios.

El documento indica que en de una semana a otra, los ataques con esa etiqueta se han triplicado. SophosLabs actualizará los datos publicados en dicho informe durante los siguientes días, conforme se desarrollen nuevos resultados.

También se ha demostrado que los ciberatacantes se hacen pasar por la organización Mundial de la Salud (OMS), los Centros para el Control y la Prevención de Enfermedades de América del Norte(CDC), así como de la Organización de las naciones Unidas (ONU) para sus estafas.

“Los ciberatacantes no pierden el tiempo y crean campañas ventajosas que se aprovechan de los crecientes temores por el virus. Por ese motivo no generan campañas complejas, y es fácil ver, por ejemplo, que los atacantes detrás de una nueva estafa son los mismos que propagaron ataques anteriores, utilizando otras palabras clave”, explica Chester Wisniewski, jefe de investigación en SophosLabs.

El especialista estima que alrededor del 3% del volumen de spam actual, que es de cientos de miles de millones de ataques, utiliza al COVID-19 como pretexto.

Indica también que existen similitudes en el cuerpo de los emails de ataques anteriores con los propagados de manera reciente. El vocero señala que fue detectado un correo electrónico apócrifo proveniente de la dirección erecruit@who.int bajo el asunto “Advertencia de salud”. “*Pero cuando revisamos cuidadosamente el texto del correo electrónico vimos muchas similitudes con spam previo”,* señala.

Wisniewski prevé que, conforme avance el tiempo, más y más cibercriminales utilizarán al COVID-19 para atraer a sus víctimas y robar información, o dinero.

Otro factor que influye son las opiniones o declaraciones emitidas por figuras públicas de alta credibilidad, desde celebridades hasta políticos y mandatarios. En semanas anteriores, el presidente de Estados Unidos, Donald Trump, indicó que un medicamento llamado cloroquina podría ser eficaz contra el coronavirus. De inmediato los spammers comenzaron a utilizar el nombre de dicho fármaco para propagar contenido.

Cabe recordar también el caso de ciberdelincuentes que solicitaron fondos en Bitcoin a nombre del Fondo de Respuesta Solidario de la OMS, una iniciativa que solicita donaciones únicamente en dólares.

Sophos recomienda, finalmente, verificar que la información que se consulte con respecto al COVID-19 en línea provenga de fuentes oficiales, como el sitio de la OMS y las plataformas de los ministerios de salud locales.

###

Sobre Sophos

Como líder mundial en seguridad cibernética de última generación, Sophos protege de las amenazas cibernéticas más avanzadas de la actualidad a más de 400,000 organizaciones de todos los tamaños en más de 150 países. Desarrolladas por SophosLabs -un equipo global de inteligencia de amenazas y ciencia de datos-, las soluciones basadas en la nube y en IA de Sophos aseguran endpoints (computadoras portátiles, servidores y dispositivos móviles) y redes contra las técnicas de ciberataque que están evolución, incluyendo ransomware, malware, exploits, extracción de datos, violaciones de adversarios activos, phishing, entre otras. Sophos Central, plataforma de administración nativa de la nube, integra la cartera completa de productos de última generación de Sophos, incluida la solución de endpoint Intercept X y el firewall de próxima generación XG, en un único sistema de "seguridad sincronizada" accesible a través de un conjunto de APIs.

Sophos ha impulsado la transición hacia la ciberseguridad de próxima generación, aprovechando las capacidades avanzadas en la nube, el aprendizaje automático, las API, la automatización, la respuesta ante amenazas administradas y más, para brindar protección de nivel empresarial a organizaciones de cualquier tamaño. Sophos vende sus productos y servicios exclusivamente a través de un canal global de más de 47,000 socios y proveedores de servicios administrados (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 con el símbolo "SOPH". Más información disponible en www.sophos.com

Síguenos en:
Facebook: https://www.facebook.com/SophosLatam/
Twitter: https://twitter.com/SophosLatAm
LinkedIn: https://www.linkedin.com/company/sophos/


SOPHOS


SOPHOS