



Pruebas de COVID-19, máscaras y medicamentos encuentran un ‘hogar’ en la Dark Web

Por John Shier, Experto Senior de Seguridad en Sophos

Los ciberdelincuentes han encontrado, en los últimos meses, distintas formas de aprovecharse de la pandemia del coronavirus. Diversas investigaciones de Sophos han mostrado cómo han utilizado al COVID-19 para propagar ataques y se ha advertido sobre estafas y prácticas como el phishing relacionadas con el coronavirus.

Lo anterior ha permeado en la escena del comercio ilegal en línea, conocida como ‘mercado negro’ o ‘Dark Web’. En ella, fueron encontrados diversos sitios de venta de productos ilegales, como Empire Market, que comercializan más de 1,000,000 de dólares por semana y en los que se ofrecen productos como medicamentos antivirales, pruebas para detectar el COVID-19, y kits de sustancias desinfectantes que no se encuentran de forma comercial. A continuación algunos de los hallazgos más relevantes de esta investigación:

Medicamentos

Empire Market tiene más de 52 mil productos listados en 11 categorías, pero al ingresar a la pestaña ‘Drogas y Fármacos’ se encuentra una mayor variedad que en cualquier otra. En ella se ofrecen 49 variedades distintas de sustancias como cloroquina o hidroxiclороquina, activos que se utilizan para producir medicamentos contra la inflamación y los efectos de la artritis, por mencionar ejemplos de su uso. El sitio vendedor afirma tener un suministro ilimitado y ofrece 9,000 píldoras por \$1,194 dólares.

También se encontró un lote de favipiravir, sustancia que se encuentra en etapa experimental contra los virus, por parte de un vendedor que también ofrecía un kit de desinfectante para manos contra el COVID-19. Destacaba un listado de productos de lopinavir y ritonavir, una combinación antiviral comúnmente utilizada para el tratamiento y prevención del VIH, que actualmente está en proceso de investigación como un posible tratamiento para COVID-19.

Drogas recreativas

El 30 de mayo de 2019, había un listado de 24,569 drogas recreativas en Empire Market. Un año después, hay más de 34,000. Eso equivale a un incremento interanual de 42%, de los cuales Empire obtiene el 4% de los ingresos que generan.

SOPHOS

Con un crecimiento como ese, el tráfico ilícito de drogas en el mercado 'negro' parece no haber sufrido ningún efecto negativo durante la pandemia. Sin embargo, sí parecía que la temática 'pandemia' se había convertido en un motivo para su comercialización. Empire contaba con algunos descuentos significativos en esta categoría derivado del coronavirus, aunque no está claro si dichas ofertas se lanzaron porque los vendedores anticipaban una caída drástica en las ventas por el virus.

Pruebas caseras de COVID-19

Después, realizamos una búsqueda de artículos que solo están en el mercado como resultado directo de la pandemia, comenzando con los kits de pruebas rápidas de COVID-19 en el hogar.

Ahí hallamos nueve ejemplos de kits caseros para COVID-19, de los cuales seis se están fabricando de manera legítima. Una de las opciones presentaba un logotipo y un nombre de dominio, pero al sitio al que vincula parece haber existido con al menos tres nombres de dominio diferentes desde el 9 de marzo de 2020. Al visitar el sitio, se encuentra un portal que también ofrece a la venta los kits de prueba. Nos pusimos en contacto con el sitio para obtener detalles sobre las pruebas, como su certificación y origen, pero no recibimos respuesta.

Esos sitios utilizaban en sus ligas de acceso las palabras 'corona' y 'safe' (seguro) como ganchos para atraer tráfico. Lo anterior, desde luego, no tiene nada de malo, pero ha habido un 'boom' en los registros de nombres de dominio con temas de coronavirus desde el comienzo de la pandemia, muchos de los cuales se están utilizando con fines maliciosos. Para la última semana de mayo, los sitios dejaron de ofrecer kits de pruebas en el hogar para la venta, pero sus páginas de Facebook, Instagram y Twitter todavía los están promocionando.

Máscaras y protección personal

Se ofrece una gran cantidad de productos de protección personal (PPE), desde máscaras quirúrgicas hasta cubrebocas tipo N99, aquellos con una efectividad de 99%. Los precios van desde decenas de dólares por una máscara hasta miles por cajas de ellas.

También fueron hallados algunos lotes de desinfectante para manos comercial, pero no hay disponibilidad de guantes ni botas de protección. Si bien algunas de estas ofertas pueden ser estafas, la mayoría de los que hallamos eran reales. Algunos de ellos, de acuerdo con las investigaciones, podrían ser productos robados de los almacenes o desviados durante el envío.

Cursos sobre 'Aprenda a hacer Fraudes'

Las ventas con motivo de la pandemia no solo se aplican a bienes físicos como medicamentos, kits de prueba o EPP. Los vendedores de productos digitales también han tomado como motivo al coronavirus y ofrecen guías o cursos para cometer fraudes en línea desde el hogar. ¿Por

SOPHOS

qué? Esto debido a que saben que derivado de la pandemia hay más gente en casa, sin pasar por alto que muchas personas han perdido sus empleos y requieren una forma de generar ingresos.

Conclusión

El impacto de COVID-19 en Empire Market ha sido limitado en términos de la cantidad de productos que se ofrecen. Sin embargo, es uno de los pocos mercados prominentes que no ha prohibido la venta de productos relacionados con la pandemia y parece estar feliz de beneficiarse del coronavirus. Otros mercados están estableciendo restricciones en la venta de muchos de los productos presentados anteriormente, mientras que para Empire Market, el negocio continúa marchando de manera normal.

####

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 evolucionando, 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/>