Sophos lanza su Informe Anual de Amenazas, el cual detalla los principales ataques cibernéticos

El Informe de Amenazas 2020 de Sophos muestra cómo los ciberataques han aumentado su actividad en ransomware, incrementado el sigilo en aplicaciones maliciosas de Android, aprovechado la configuración incorrecta en la nube y engañado al Machine Learning

Ciudad de México a 6 de noviembre de 2019. – **Sophos** (LSE: SOPH), líder mundial en seguridad cibernética de última generación habilitada para la nube, lanzó su **Informe de Amenazas 2020**, el cual proporciona información detallada sobre el panorama de amenazas cibernéticas en el mundo. El informe, realizado por investigadores de SophosLabs, explora los cambios en el mundo de las amenazas cibernéticas en los últimos 12 meses, descubriendo tendencias que probablemente impactarán en la ciberseguridad durante 2020.

"*El panorama de las amenazas continúa evolucionando, y la velocidad y el alcance de dicha evolución es tan acelerada como impredecible. La única certeza que tenemos es lo que está sucediendo en este momento. Por eso, en nuestro* ***Informe de Amenazas 2020*** *observamos cómo las tendencias actuales podrían afectar al mundo durante el próximo año. Además, detallamos cómo los adversarios son cada vez más sigilosos, y mejores aprovechando errores, ocultando sus actividades y evadiendo tecnologías de detección a través de aplicaciones móviles y redes internas. El* ***Informe de Amenazas 2020*** *no solo es un mapa para los expertos, sino que contiene una guía para ayudar a los defensores a comprender mejor lo que podrían enfrentar en los próximos meses y cómo prepararse*", dijo John Shier, asesor Sr. de Seguridad de Sophos.

Por otra parte, el **Informe de Amenazas 2020** de SophosLabs -el cual se encuentra resumido en este artículo de SophosLabs Uncut- se enfoca en seis áreas donde los investigadores notaron desarrollos peculiares durante el año pasado. Se espera que tengan un impacto significativo en el panorama de amenazas cibernéticas en 2020, y posteriormente, las siguientes tendencias:

Los atacantes de ransomware continúan apostando por hacer ataques activos y automatizados que ponen las herramientas de administración de las organizaciones en su contra, evaden los controles de seguridad y desactivan las copias de seguridad para causar el máximo impacto en el menor tiempo posible.

Las aplicaciones no deseadas se están acercando al malware. En un año que trajo las aplicaciones Android Fleeceware que abusan de las suscripciones, y adware cada vez más sigiloso y agresivo, el **Informe de Amenazas 2020** destaca cómo estas y otras aplicaciones potencialmente no deseadas (PUA por su nombre en inglés), como los complementos del navegador, se están convirtiendo en agentes para entregar y ejecutar malware y ataques sin archivos.

La mayor vulnerabilidad para el *cloud computing* es la configuración incorrecta por parte de los operadores. A medida que los sistemas en la nube se vuelven más complejos y flexibles, el error del operador es un riesgo en potencia. Combinado con una falta general de visibilidad, esto hace que los entornos de computación en la nube sean un objetivo ideal para los ciberatacantes.

El *Machine Learning* diseñado para eliminar *malware* se encuentra bajo ataque. El año 2019 destacó el potencial de los ataques contra los sistemas de seguridad de aprendizaje automático (*Machine Learning*). La investigación mostró cómo los modelos de detección de ML podrían ser engañados, y cómo el aprendizaje automático podría aplicarse a la actividad ofensiva para generar contenido falso muy convincente para la ingeniería social. A la par, los defensores están aplicando el ML al lenguaje como una forma de detectar correos electrónicos y URL maliciosos. Se espera que este juego avanzado de "al gato y al ratón" sea más frecuente en el futuro.

Otras áreas cubiertas en el **Informe de Amenazas 2020** incluyen el peligro de no detectar el reconocimiento cibercriminal oculto en el ruido más amplio del escaneo de Internet, la superficie de ataque continuo del Protocolo de Escritorio Remoto (RDP por su término en inglés) y el mayor avance de los ataques activos automatizados (AAA).

Para obtener información adicional y detallada sobre las tendencias del panorama de amenazas y los cambios en los comportamientos cibercriminales, consulte el Informe de Amenazas 2020 de SophosLabs completo en https://www.sophos.com/threatreport2020.

# # #

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/

Another Company

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

Fernanda Cornejo
fernando.cornejo@another.co

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