Estas son las principales amenazas en el panorama de ciberseguridad hacia 2021

CIUDAD DE MÉXICO. 18 de noviembre de 2020.- Sophos, líder mundial en ciberseguridad de última generación, publicó su Informe de Amenazas 2021 de Sophos (Sophos 2021 Threat Report), en el que se explica cómo **la propagación de *ransomware*** y el cambiante comportamiento de los atacantes formará el panorama de amenazas y ciberseguridad hacia 2021. El informe, escrito por los investigadores de seguridad de SophosLabs, entre otros expertos de la firma, proporciona una perspectiva integral sobre las **amenazas y tendencias** desde su inicio hasta el impacto que generan.

El reporte señala principalmente tres tendencias clave en cuestión de ciberseguridad hacia 2021:

1. Se incrementará la brecha entre los operadores de *ransomware*

Las familias de *ransomware* más sofisticadas continuarán perfeccionando y cambiando sus técnicas, tácticas y procedimientos (TTP) para volverse más evasivas y de sofisticación similar a la de un estado-nación, dirigidas a organizaciones más grandes con demandas de rescate multimillonarias. En 2020, estas familias incluyen a Ryuk y RagnarLocker. En el otro extremo del espectro, el de nivel más bajo, Sophos anticipa un aumento en el número de atacantes principiantes, que buscarán *ransomware* más simple, como Dharma, que les permite apuntar a presas más pequeñas pero en grandes volúmenes.

Otra tendencia será la "extorsión secundaria", en la que, junto al cifrado de datos, los atacantes roban y amenazan con publicar información sensible o confidencial si no se cumplen sus demandas. En 2020, Sophos informó sobre Maze, RagnarLocker, Netwalker, REvil y otras familias de ransomware que están utilizando esta táctica.

"*El modelo de negocio de ransomware es dinámico y complejo. Durante 2020, Sophos vio una clara tendencia hacia la diferenciación de los adversarios en términos de sus habilidades y objetivos. Sin embargo, también hemos visto familias de ransomware que comparten las mejores herramientas y forman 'cárteles' de colaboración con estilo propio"*, dijo **Chester Wisniewski, científico investigador principal de Sophos**. "*Algunos, como Maze parecían estar cerca de desaparecer, pero algunas de sus herramientas y técnicas resurgieron bajo la apariencia de un recién llegado ransomware llamado Egregor. El panorama de los ciberataques aborrece el vacío, por lo que si una amenaza desaparece, otra rápidamente ocupará su lugar. Es casi imposible predecir a dónde irá el ransomware el año próximo, pero es probable que las tendencias de ataque discutidas en el informe de amenazas de Sophos de este año continúen en 2021*".

2. Amenazas como el *malware* básico requerirán de una atención más seria

Estas amenazas pueden parecer de bajo nivel, pero los Access Brokers o agentes de acceso inicial a los sistemas están diseñados para asegurar un punto de apoyo en un objetivo, recopilar datos esenciales y compartirlos con una red de comando y control que proporcionará más instrucciones para continuar con un ataque de mayor sofisticación. Si los operadores humanos están detrás de este tipo de amenazas, revisarán cada máquina comprometida en busca de su geolocalización y otros signos de alto valor, y luego venderán el acceso a esos equipos al mejor postor, como una operación de ransomware importante. Por ejemplo, en 2020, Ryuk utilizó Buer Loader, un programa utilizado para la descarga de archivos, para propagar su *ransomware*.

"*El malware propagado mediante productos básicos puede parecer una tormenta de arena para obstruir el sistema de alerta. De lo que analizó Sophos, está claro que los defensores deben tomar estos ataques que lucen menores muy en serio, debido al lugar al que podrían conducir. Cualquier infección puede dar pie a otro tipo de ciberataques de mayor tamaño. Muchos equipos de seguridad sentirán que una vez que se ha bloqueado o eliminado el malware y se ha limpiado la máquina comprometida se ha evitado el incidente*", dijo **Wisniewski**. "*Es posible que no se den cuenta de que el ataque fue en más de una máquina y que el malware, propagado mediante Emotet y Buer Loader, puede conducir a Ryuk, Netwalker y otros tipos de ransomware avanzados, y es posible que TI no note la presencia del ataque hasta que se implemente el ransomware, posiblemente en medio de la noche o el fin de semana. Subestimar las infecciones 'menores' podría resultar muy costoso*".

3. Herramientas legítimas, servicios y destinos de red comunes, el modo de evadir a los servicios de ciberseguridad

Sophos detectó que los ciberdelincuentes continuarán aprovechándose del abuso de herramientas legítimas, lo que les permite permanecer fuera del radar mientras se mueven por la red hasta que están listos para lanzar la parte principal del ataque, como el *ransomware*. Para los atacantes existe el beneficio de que el uso de herramientas comunes y legítimas dificulta la atribución del ciberataque. En 2020, Sophos informó sobre la amplia gama de herramientas de ataque estándar que ahora son ampliamente utilizadas.

"*El abuso de herramientas comunes y legítimas para disfrazar un ataque activo ocupó un lugar destacado en los hallazgos de Sophos durante 2020. Esta técnica desafía los enfoques de seguridad tradicionales porque la aparición de herramientas comúnmente utilizadas al interior de una empresa no activa automáticamente una señal de alerta. Aquí es donde la caza de amenazas liderada por un equipo humano y la respuesta administrada a ataques realmente entra en juego",* dijo **Wisniewski.** "*Los expertos conocen las anomalías sutiles y saben detectar aquellos rastros que los criminales suelen dejar, como el uso de una herramienta legítima en el momento o el lugar equivocados. Para los cazadores de amenazas capacitados o los administradores de TI que utilizan las funciones de detección y respuesta de endpoints (EDR),*

estas señales son valiosos signos que pueden alertar a los equipos de seguridad sobre un posible intruso y un ataque en curso".

El Informe de Amenazas 2021 de Sophos también incluye las siguientes tendencias:

- **Ataques a servidores:** los atacantes se dirigen a servidores que ejecutan tanto Windows como Linux, y aprovechan estas plataformas para atacar organizaciones desde dentro.

- **El impacto de la pandemia de COVID 19 en la seguridad de TI:** existen desafíos de seguridad derivados de trabajar desde casa utilizando redes personales protegidas por niveles de seguridad muy variables.

- **Los desafíos de seguridad que enfrentan los entornos en la nube:** la computación en la nube ha soportado con éxito muchas de las necesidades empresariales actuales de los entornos informáticos, pero se enfrenta a desafíos diferentes a los de una red empresarial tradicional.

- **Servicios comunes como RDP y VPN:** estos siguen siendo un foco de ataques muy común en el perímetro de la red. Los atacantes también usan RDP para moverse lateralmente dentro de las redes violadas sin que los equipos de seguridad lo noten.

- **Aplicaciones de *software* tradicionalmente marcadas como "potencialmente no deseadas":** existen aplicaciones que pueden convertirse en un foco de propagación ya que entregan una gran cantidad de anuncios, mismos que son cada vez más indistinguibles del malware manifiesto.

- **La sorprendente reaparición de un error antiguo, VelvetSweatshop:** se trata de una función de contraseñas predeterminada para versiones anteriores de Microsoft Excel, que se utiliza para ocultar contenido malicioso en documentos y evadir la detección avanzada de amenazas.

- **La necesidad de aplicar algunos enfoques de la epidemiología:** esto con el fin de cuantificar las ciberamenazas invisibles, no detectadas y desconocidas, todo para cerrar las brechas en la detección, evaluar de mejor manera el riesgo y definir prioridades.

Si quieres saber más sobre el estudio mira este video en el que **Chester Wisnieski, científico investigador principal de Sophos**, explica a detalle algunos de los hallazgos más importantes del reporte. También te comparto dos artículos adicionales sobre el *Informe de Amenazas de Sophos 2021:*

- El Informe de Amenazas 2021 de Sophos destaca un camino a seguir de SophosLabs Uncut

- Informe de amenazas 2021 de Sophos de Naked Security

El informe completo de amenazas de Sophos 2021 está disponible en www.sophos.com/threatreport.

###

Sobre Sophos

Como líder mundial en seguridad cibernética de última generación, Sophos protege a más de 400,000 organizaciones en más de 150 países de las amenazas cibernéticas más avanzadas de la actualidad. Desarrolladas por SophosLabs, un equipo global de inteligencia contra amenazas cibernética y ciencia de datos, las soluciones basadas en inteligencia artificial y nativas de la nube de Sophos ofrecen seguridad a endpoints (computadoras portátiles, servidores y dispositivos móviles) y redes contra las diversas técnicas de ciberdelincuencia que están en constante evolución, incluidos ransomware, malware, exploits, extracción de datos, incumplimientos de adversarios activos, phishing y más. Sophos Central, una plataforma de administración nativa de la nube, integra toda la cartera de productos de próxima generación de Sophos, incluida la solución de endpoint Intercept X y el Firewall XG, en un único sistema de "seguridad sincronizada" accesible a través de un conjunto de APIs.

Sophos ha impulsado la transición a la ciberseguridad de última generación, aprovechando las capacidades avanzadas en la nube, el aprendizaje automático, las API, la automatización, la respuesta ante amenazas 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 53,000 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. Para obtener más información visita www.sophos.com.

Síguenos en:

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