Sophos Threat Report 2022: el ‘agujero negro’ del ransomware masivo e interconectado

- ***Este informe identifica las tendencias en servicios de ransomware, malware, herramientas de ataque, criptomineros y más, que están afectando la seguridad a nivel global de cara al año próximo.***

CIUDAD DE MÉXICO. 09 de noviembre de 2021.- Sophos, líder mundial en ciberseguridad de última generación, publicó el **Sophos Threat Report 2022** (reporte de amenazas de Sophos), que muestra cómo la fuerza gravitacional del ransomware está formando un ‘agujero negro’ que atrae a otras ciberamenazas para formar un sistema malicioso masivo e interconectado, con implicaciones significativas para la seguridad de TI.

El informe, escrito por investigadores de SophosLabs Security, cazadores de amenazas y miembros del equipo de respuesta de Sophos Managed Threat Response, proporciona una perspectiva multidimensional y única sobre las amenazas y tendencias de seguridad que enfrentan las organizaciones en 2022.

El informe de amenazas de Sophos 2022 analiza las siguientes tendencias clave:

1.- Durante el próximo año, el panorama del ransomware se volverá más uniforme, con "especialistas" de ataque que ofrecerán diferentes elementos de un ‘ataque como servicio’, además de que proporcionarán ‘manuales’ con herramientas y técnicas que permitirán a otros grupos de adversarios implementar ataques muy similares.

Según los investigadores de Sophos, actualmente existen más ofertas de **ransomware como servicio (RaaS)**, por lo que los desarrolladores de amenazas se centraron en alquilar código e infraestructura maliciosa a terceros. Algunos de los ataques de ransomware de más alto perfil del año 2021 involucraron a RaaS, incluyendo un ataque contra Colonial Pipeline por parte de una filial de DarkSide.

Además, un afiliado de Conti ransomware filtró la guía de implementación proporcionada por los operadores de dicho ataque, revelando el paso a paso a paso que los atacantes podrían utilizar para implementar ese ransomware posteriormente.

Una vez que tienen el malware que necesitan, los afiliados de RaaS pueden recurrir a los agentes de acceso inicial y las plataformas de distribución de malware para encontrar y apuntar a posibles víctimas.

2.- Las ciberamenazas seguirán adaptándose para distribuir y entregar ransomware, todo mediante tácticas como cargadores de data, ‘goteros’ y otros programas maliciosos básicos; cada vez más avanzado y operados por humanos. Entre las tácticas que se seguirán utilizando figuran los corredores de acceso inicial comprometidos; correo ‘no deseado’; y adware.

3. El uso de múltiples formas de extorsión por parte de atacantes de ransomware para presionar a las víctimas. Se espera que el pago del rescate continúe además de que los montos pagados se incrementen. En 2021, Sophos catalogó 10 tipos diferentes de tácticas de presión, desde el robo de datos y exposición, hasta las llamadas telefónicas amenazantes, ataques distribuidos de denegación de servicio (DDoS) y más.

4. Las criptomonedas seguirán alimentando delitos cibernéticos como ransomware. Sophos espera que la tendencia continúe hasta que las criptomonedas globales se encuentren mejor reguladas. Durante 2021, los investigadores de Sophos descubrieron criptomineros como Lemon Duck y el menos común, MrbMiner.

"El ransomware prospera gracias a su capacidad para adaptarse e innovar", dijo Chester Wisniewski, científico investigador principal de Sophos. *"Por ejemplo, aunque las ofertas de RaaS no son nuevas, en anteriores años, su principal contribución fue poner al ransomware al alcance de los atacantes menos calificados o menos capacitados, así como aquellos con menor poder financiero"*, indica.

"Esto ha cambiado y, en 2021, los desarrolladores de RaaS están creando un código sofisticado para determinar la mejor manera de extraer cantidades de dinero aún mayores, destinando a otros las tareas de encontrar víctimas, instalar y ejecutar el malware, así como lavar las criptomonedas robadas. Esto está distorsionando el panorama de ciberamenazas, mientras que las herramientas comunes como los cargadores, 'goteros' y agentes de acceso inicial están siendo absorbidos por el 'agujero negro', aparentemente devorador, en el que se ha convertido el ransomware", añade.

"Ya no es suficiente que las organizaciones asuman que están seguras simplemente monitoreando las herramientas de seguridad y asegurándose de que estén detectando códigos maliciosos. Ciertas combinaciones de detección son el equivalente a un ladrón rompiendo un jarrón de flores mientras trepa por la ventana trasera. Los defensores deben investigar las alertas, incluso aquellas que en el pasado pueden haber sido insignificantes, ya que estas intrusiones comunes han florecido al punto de tener la capacidad de tomar control de redes enteras", concluye el especialista.

###

Sobre Sophos

Sophos es la empresa líder mundial en ciberseguridad de última generación, que protege a más de 500.000 organizaciones y millones de consumidores en más de 150 países de las ciberamenazas más avanzadas de la actualidad. Con tecnología para la detección de amenazas, inteligencia artificial y aprendizaje automático de SophosLabs y SophosAI, Sophos ofrece una amplia cartera de productos y servicios avanzados para proteger a los usuarios, redes y endpoints contra ransomware, malware, exploits, phishing y una amplia gama de ciberataques. Sophos proporciona una plataforma única de gestión integral basada en la nube llamada Sophos Central, el eje de un

ecosistema de ciberseguridad adaptable que cuenta con un 'lago de datos' centralizado que aprovecha un amplio conjunto de API abiertas disponibles para clientes, socios, desarrolladores y otros proveedores de ciberseguridad. Sophos vende sus productos y servicios a través de socios distribuidores y proveedores de servicios administrados (MSP) en todo el mundo. Sophos tiene su sede en Oxford, Reino Unido. Para más información, ingresa a www.sophos.com.