Sophos acelera la detección y respuesta contra ataques a Linux

CIUDAD DE MÉXICO. 19 de abril de 2022.- Sophos, líder mundial de ciberseguridad de última generación dio a conocer los avances de su tecnología Sophos Cloud Workload Protection, incluidas nuevas capacidades de seguridad para host de sistemas operativos Linux.

Estas mejoras aceleran la capacidad de detección y respuesta contra ataques en curso dentro de dichos sistemas operativos, además de que mejoran las operaciones y refuerzan el rendimiento de las aplicaciones.

Según una nueva investigación de SophosLabs, las herramientas distribuidas de denegación de servicio (DDoS), los mineros de criptomonedas y varios tipos de puertas traseras fueron los tres principales tipos de amenazas contra Linux entre enero y marzo de 2022.

Las herramientas DDoS representaron casi la mitad de todas las detecciones de malware de Linux durante ese periodo de tiempo, probablemente debido a la incidencia de ataques automatizados que intentan infectar a los servidores debidamente actualizados. SophosLabs también detectó un aumento reciente en las estrategias de ataque basadas en utilizar herramientas dirigidas a hipervisores, es decir una capa de software que permite utilizar, dentro del mismo monitor, diversas máquinas de sistemas operativos diferentes.

“Los entornos Linux continúan creciendo a medida que las organizaciones de todo el mundo migran cada vez más las cargas de trabajo a la nube. Aunque se considera que Linux es uno de los sistemas operativos más seguros, aún alberga riesgos inherentes y basados en aplicaciones y no es inmune a los ataques cibernéticos”, dijo Joe Levy, director de tecnología y productos de Sophos.

"Los atacantes se dirigen a los hosts y contenedores de Linux porque son de gran valor y, a menudo, están desprotegidos. Sophos Cloud Workload Protection ya automatiza y simplifica la prevención y detección de estos ataques en sistemas Windows, y ahora proporciona las mismas capacidades a los sistemas operativos Linux”, añade.

Protección de la infraestructura de Linux

A través de la integración de la tecnología Capsule8, que Sophos adquirió en julio de 2021, Sophos Cloud Workload Protection brinda una visibilidad potente de los hosts y contenedores de Linux, protegiéndolos de ciberamenazas avanzadas. Aprovecha el análisis en torno a las tácticas, técnicas y procedimientos (TTP) de los atacantes para proporcionar detecciones de amenazas nativas de la nube, que incluyen:

- Escapes de contenedores: esta herramienta identifica a los atacantes que aumentan los privilegios de acceso a los hosts.

- Cryptomineros: detecta comportamientos comúnmente asociados con los mineros de criptomonedas.
- Destrucción de datos: alertas de que un atacante puede estar intentando eliminar indicadores de compromiso que forman parte de una investigación en curso.
- Exploits del kernel: detecta cuando las funciones internas del kernel, es decir el núcleo del sistema operativo, están siendo manipuladas en un host.

Una vez que se detectan las amenazas, Sophos XDR asigna puntuaciones de riesgo a los incidentes y proporciona datos contextuales que permiten a los analistas de seguridad, así como al equipo de respuesta gestionada frente a amenazas de Sophos, agilizar las investigaciones y centrarse en los incidentes de mayor prioridad.

Sophos Cloud Workload Protection se integra a la perfección con el ecosistema de ciberseguridad adaptable de Sophos, que sustenta toda la cartera de soluciones de la compañía. El ecosistema inteligente unifica la gama de capacidades de la plataforma de seguridad nativa de la nube, que incluye Sophos Cloud Workload Protection, Sophos Cloud Security Posture Management, escaneo de infraestructura como código, administración de derechos de infraestructura en la nube y supervisión de gastos, para garantizar la visibilidad, la seguridad y el cumplimiento.

Disponibilidad

Sophos Cloud Workload Protection ahora está disponible con Sophos Intercept X Advanced for Server con XDR y Sophos Managed Threat Response, y se administra dentro de la plataforma nativa de la nube Sophos Central. Se puede implementar como una solución de un solo agente que es ideal para los equipos de operaciones de seguridad, ya que brinda protección flexible con límites de recursos optimizados, sin implementar un módulo de kernel.

Sophos Cloud Workload Protection también estará disponible pronto como sensor de Linux, lo cual es ideal para DevSecOps y equipos de centros de operaciones de seguridad (SOC) que requieren una visión profunda de las cargas de trabajo con un impacto mínimo en el rendimiento. Dicho sensor proporcionará integración API en las soluciones existentes de automatización, orquestación, gestión de registros y respuesta a incidentes.

###

Sobre Sophos

Sophos es un líder mundial en ciberseguridad de próxima generación y 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 de inteligencia 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, las redes y los puntos finales contra ransomware, malware, exploits, phishing y una amplia gama de otros ciberataques. Sophos proporciona una única consola de gestión integrada basada en la nube, Sophos Central, la pieza central 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 revendedores y proveedores de servicios administrados (MSP) en todo el mundo. Sophos tiene su sede en Oxford, Reino Unido. Hay 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/