Sophos adquiere Capsule8 para expandir su protección a servidores Linux

- **La empresa añade así la tecnología líder en detección y respuesta de amenazas para dichos sistemas a su ecosistema de ciberseguridad adaptable (ACE).**

CIUDAD DE MÉXICO. 07 de julio de 2021.- Sophos, líder mundial en ciberseguridad de última generación, anunció hoy que ha adquirido a Capsule8, un pionero y líder del mercado en visibilidad, detección y respuesta en tiempo real para servidores de Linux que cubren las instalaciones y cargas de trabajo en la nube. Fundada en 2016, Capsule8 es una empresa privada que tiene su sede en Nueva York.

"*Sophos ya protege a más de dos millones de servidores para más de 85,000 clientes en todo el mundo, y el negocio de seguridad de servidores de Sophos está creciendo a más del 20% anual"*, dijo Dan Schiappa, Chief Product Officer (CPO) de Sophos. "*La protección integral del servidor es un componente crucial de cualquier estrategia de ciberseguridad eficaz en la que las organizaciones de todos los tamaños se centran cada vez más, especialmente a medida que más cargas de trabajo se trasladan a la nube. Con Capsule8, Sophos ofrece soluciones avanzadas para proteger los entornos de servidor y amplía su posición como proveedor líder de ciberseguridad a nivel mundial*".

Capsule8 se dedica exclusivamente al desarrollo de ciberseguridad de Linux y se ha establecido como un líder tecnológico con grandes ganancias de clientes y un crecimiento de facturación del 77% al término del último año fiscal, que concluyó el 31 de marzo de 2021. Impulsado por el dramático crecimiento de las plataformas en la nube, Linux se ha convertido en el sistema operativo dominante para cargas de trabajo de servidor. El diseño de alto rendimiento y bajo impacto de la empresa es ideal para servidores Linux, especialmente aquellos que se utilizan para cargas de trabajo a gran escala, infraestructura de producción y almacenamiento de datos comerciales críticos.

"*La idea principal detrás de Capsule8 radica en que proporcionar seguridad de nivel empresarial para sistemas Linux requiere la implementación de componentes diseñados específicamente para ese entorno"*, dijo Fernando Montenegro, analista principal de investigación de 451 Research. "*A medida que las organizaciones adoptan modelos cada vez más basados en la nube, los entornos informáticos están migrando hacia Linux para su ejecución. Para los equipos de seguridad, a menudo más familiarizados con los conceptos centrados en Windows, esto representa un desafío potencial. Este es el espacio que se pretende abordar, combinando una arquitectura optimizada para Linux con más funciones destinadas a la seguridad empresarial y los equipos de operaciones de TI".*

Sophos está integrando la tecnología de Capsule8 en su Ecosistema de Ciberseguridad Adaptable (ACE) recientemente lanzado, lo que proporciona una seguridad potente y liviana para servidores Linux y contenedores en la nube dentro de esta plataforma abierta. Sophos

también incluirá dicha tecnología en sus soluciones Extended Detection and Response (XDR); los productos de protección de servidor Intercept X; los servicios de Sophos Managed Threat Response (MTR) y Rapid Response. Esto ampliará aún más el lago de datos de Sophos, ofreciendo así inteligencia continua para la búsqueda de amenazas avanzadas, las operaciones de seguridad y las prácticas de protección del cliente.

"*Capsule8 es la principal plataforma de respuesta y detección especialmente diseñada para Linux. Brindamos a los equipos de seguridad la visibilidad que necesitan para proteger la infraestructura de producción de Linux contra comportamientos no deseados, mientras que al mismo tiempo abordamos los problemas de costo, rendimiento y confiabilidad*", dijo John Viega, CEO de Capsule8. "*Con esta tecnología las organizaciones ya no están obligadas a elegir entre la estabilidad del sistema y el nivel de seguridad apropiado. Dado el crecimiento y la naturaleza de misión crítica de los entornos Linux, y el panorama de amenazas dirigidas que cambia rápidamente, las organizaciones deben estar seguras de que sus entornos Linux son eficaces y seguros".*

La inteligencia de amenazas de Sophos Labs revela que los adversarios están diseñando tácticas, técnicas y procedimientos (TTP) dirigidos específicamente a los sistemas Linux, a menudo explotando el software del servidor como un punto de entrada inicial. Después de hacerse un hueco, los atacantes suelen desplegar scripts para realizar más acciones automatizadas como:

- Descartar las claves del protocolo Secure Shell (SSH) para obtener acceso directo
- Intentar eliminar los servicios de seguridad existentes
- Deshabilitar marcos de control de acceso obligatorio (MAC), como AppArmor y SELinux
- Ajustar o deshabilitar las reglas de firewall del servidor
- Instalación de archivos de configuración y malware posterior al exploit
- Moverse lateralmente a través de la infraestructura existente con herramientas como SSH, Chef, Ansible, Salt y Puppet

Los cibercriminales utilizan servidores Linux comprometidos como *botnets* de criptominería o como una infraestructura de alto nivel para lanzar ataques hacia otras plataformas, alojar sitios web maliciosos o enviar correos electrónicos apócrifos. Dado que los servidores Linux a menudo contienen datos valiosos, los atacantes también los atacan para el robo de información y ransomware.

"*Los atacantes de hoy son increíblemente agresivos y ágiles, ya que adaptan sus TTP para centrarse en las oportunidades más fáciles, más grandes o de más rápido crecimiento. A medida que más organizaciones cambian a servidores Linux, los adversarios están adaptando sus enfoques para atacar estos sistemas. Para mantenerse protegidas, las organizaciones deben tener en cuenta una capa sólida pero liviana de seguridad de Linux que se integra automáticamente y comparte inteligencia con terminales, redes y otras capas y plataformas de seguridad*", dijo Schiappa. *""Proporcionaremos esta capacidad líder en la industria, además de una visibilidad y detección estratégica mediante la combinación de Capsule8 con nuestros productos y servicios del ecosistema de ciberseguridad adaptable, mejorando en gran medida*

la capacidad de encontrar y eliminar actividades sospechosas antes de que se vuelvan maliciosas".

Sophos espera comenzar con los programas de acceso a sus productos y servicios aprovechando la tecnología Capsule8 a finales de este año fiscal.

####

Sobre Capsule8
Capsule8 es el pionero detrás de la seguridad integrada a sistemas Linux. Su tecnología está diseñada para evitar costosos tiempos de inactividad, hosts sobrecargados o problemas de estabilidad causados por las herramientas de seguridad tradicionales. Fundada en 2016 y con sede en Nueva York, Capsule8 hace posible que las organizaciones con tecnología Linux protejan los sistemas de producción y aseguren el crecimiento. Obtenga más información en www.Capsule8.com.

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.

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