Sophos lanza solución antimalware que opera sin archivos y mediante agentes remotos

CIUDAD DE MÉXICO. 17 de marzo de 2021.- Sophos, empresa líder en ciberseguridad de última generación, anunció el lanzamiento de Dynamic Shellcode Protection, una solución que protege a las organizaciones contra ciberataques que involucran *malware* y *ransomware* sin archivos y agentes de acceso remoto.

El lanzamiento llega luego de que investigadores de la compañía descubrieron que los ciberdelincuentes habían inyectado código de ataque encubierto en la región dinámica 'Heap' de la memoria de una computadora para intentar obtener almacenamiento adicional con derechos de ejecución de código.

Dynamic Shellcode Protection se puede activar en cualquier momento en el que se detecte un comportamiento sospechoso en la memoria Heap. Al hacerlo, dificulta a los ciberdelincuentes el uso de memoria como parte de sus técnicas de evasión de defensa.

¿Cómo funciona Dynamic Shellcode Protection?
Dynamic Shellcode Protection detecta y bloquea las violaciones de asignación de la memoria Heap. El director de ingeniería de Sophos, Mark Loman, explica que la solución se basa en el hecho de que las aplicaciones, al instalarse en las computadoras, se almacenan en regiones de memoria que tienen derechos de "ejecución" y que permiten que éstas funcionen.

Cuando esas aplicaciones necesitan un espacio adicional de forma temporal, éste es extraído de la memoria Heap para descomprimir o almacenar más datos. En estos casos, las aplicaciones pueden solicitar que su asignación extra de memoria Heap venga con derechos de ejecución.

Durante un ataque de este tipo, la carga útil del *ransomware* se instala mediante acceso remoto en la memoria. Luego, puede solicitar, como si fuera una aplicación legítima, más espacio ejecutable en la memoria para adaptarse a las necesidades del atacante.

El uso de este tipo de tácticas para plantar un ciberataque de forma remota es una tendencia actual y permite a los entes maliciosos instalar virus más robustos. Este tipo de estrategias les son útiles, ya que les permiten emitir comandos y analizar el entorno de la víctima antes de atacar.

Sophos señala que los agentes de acceso remoto se han utilizado recientemente en ataques de alto perfil como SolarWinds y Gootloader, en los que el atacante tomó el control de un proceso que ya se estaba ejecutando y lo controló para sus propios fines.

Dynamic Shellcode Protection evita la asignación de permisos de ejecución de la memoria Heap para interceptar ciberataques que involucran *malware* y *ransomware* sin archivos o de acceso remoto, y está integrada dentro de Intercept X, plataforma de protección de endpoints de Sophos, compatible con otras aplicaciones y que no aprovecha la nube ni el aprendizaje automático.

###

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/