Log4Shell: la amenaza que no ha estallado masivamente, pero que no dará respiro

CIUDAD DE MÉXICO. 27 de enero de 2022.- En ocasiones, cuando una amenaza cibernética no genera un impacto devastador, puede creerse que en realidad no se trata de una verdadera amenaza.

Pero ese es un error grave que sucede con Log4Sell, encontrado en el software Apache Log4J ampliamente utilizado a principios de diciembre de 2021. Aunque el mundo no ha visto una afectación masiva de esa vulnerabilidad, ésta se ha inmiscuido ya en muchas aplicaciones y productos digitales, y probablemente será explotada severamente en el futuro.

- **Explotación masiva limitada**

Sophos cree que el uso masivo de Log4Shell se evitó porque la gravedad del error unió a la comunidad digital y de seguridad para actuar de inmediato. Tan pronto como los detalles del error quedaron al descubierto, los servicios en la nube, los paquetes de software y las empresas más grandes del mundo tomaron medidas.

Además, la empresa ha encontrado un patrón típico para una vulnerabilidad. En los primeros días, el volumen de escaneos del sistema con fines de vulneración fue moderado, pero una semana después hubo un crecimiento exponencial que alcanzó su máximo nivel entre el 20 y el 23 de diciembre de 2021.

Sin embargo, desde finales de diciembre hasta enero de 2022, la curva de intentos de ataque se estabilizó y disminuyó. Esto no significa que el nivel de amenaza también haya disminuido, ya que en este momento, un porcentaje cada vez mayor de detecciones probablemente serán ataques reales, y cada vez menos aquellos que provengan de investigadores que monitoreen el estado de los parches.

- **La geografía de los intentos de ataque**

Existen variaciones interesantes en ubicaciones de los intentos de ataque y escaneos. En diciembre, Estados Unidos, Rusia y China, así como los países de Europa Occidental, fueron los principales focos. Esto cambió drásticamente a principios de 2022, en donde China y Rusia no aparecen más como objetivos frecuentes.

Y si bien EE.UU. sigue siendo uno de los principales focos, es importante decir que India ascendió a la posición número uno, destacándose también Turquía, Brasil e incluso Australia.

Es difícil especular por qué estas regiones son los principales destinos para los intentos actuales. Una razón podría ser que estos países tienen muchos participantes activos en programas de recompensas por errores, con la esperanza de ganar dinero siendo los primeros en alertar a las organizaciones de que están expuestos.

- **La amenaza permanece**

Nadie está libre de riesgo, Sophos señala que incluso existen atacantes que aseguraran el acceso a un objetivo vulnerable, pero que pudieron aún no abusar de ese acceso para lanzar malware, por lo que la violación exitosa permanece sin ser detectada.

Con el tiempo, es probable que las aplicaciones orientadas a un exploit de Log4Shell se identifiquen parcheadas o eliminadas. Sin embargo, Sophos muestra que existe una gran cantidad de archivos Java Archive (JAR) vulnerables en los puntos finales protegidos que no han cambiado, los cuales podrían convertirse en una herramienta ideal para el movimiento lateral malicioso en el futuro.

La compañía considera que el intento de explotación de la vulnerabilidad de Log4Shell probablemente continuará durante años y se convertirá en el objetivo favorito de los probadores de vulneración. La urgencia de identificar dónde se usa y actualizar el software con el parche sigue siendo tan crítica como siempre.

####

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/