Log4Shell: la 'llave de acceso' mediante puertas traseras a servidores Horizon

CIUDAD DE MÉXICO. 29 de marzo de 2022.- Sophos, líder mundial en ciberseguridad de última generación, publicó nuevas investigaciones sobre cómo los atacantes utilizan la vulnerabilidad Log4Shell para proporcionar puertas traseras y scripts de creación de perfiles a servidores VMware Horizon sin parches.

El nuevo informe revela que con el uso de esta vulnerabilidad los atacantes crearon tres puertas traseras diferentes y cuatro criptomineros, que posteriormente son ofrecidas a ciberdelincuentes para su acceso a los servidores.

Log4Shell es una vulnerabilidad de ejecución remota de código en Apache Log4J, uno de los componentes de registro de Java. Este componente está integrado en cientos de productos de software. Su último parche de seguridad se realizó en diciembre de 2021.

"*Las aplicaciones ampliamente utilizadas, como VMware Horizon, que están expuestas a Internet y deben actualizarse manualmente, son particularmente vulnerables a los ataques a gran escala*", dijo Sean Gallagher, investigador principal de seguridad de Sophos. "*Las detecciones de Sophos revelan oleadas de ataques dirigidos a servidores Horizon, a partir de enero, y entregan una variedad de puertas traseras y criptomineros a servidores sin parches, así como scripts para recopilar información del dispositivo".*

"*Sophos cree que algunas de las puertas traseras pueden ser proporcionadas por agentes maliciosos que buscan asegurar el acceso remoto a un objetivo de alto valor para luego venderlo a otros atacantes, como los operadores de ransomware*", añade.

Las múltiples cargas útiles de ataque que Sophos detectó usando Log4Shell para apuntar a servidores Horizon vulnerables incluyen:

- Dos herramientas legítimas de administración y monitoreo remoto: Atera agent y Splashtop Streamer, probablemente destinadas para uso malicioso como creación de puertas traseras
- La puerta trasera maliciosa Sliver
- Los criptomineros z0Miner, JavaX miner, Jin y Mimu
- Varios shells inversos basados en PowerShell que recopilan información de dispositivos y copias de seguridad

Según Sophos, los atacantes están utilizando varios enfoques diferentes para infectar objetivos. Si bien algunos de los ataques anteriores utilizaron Cobalt Strike para organizar y ejecutar las cargas útiles del criptominero, la mayor ola de ataques que comenzó a mediados de enero de 2022 ejecutó esta herramienta directamente desde el componente Apache Tomcat del servidor VMware Horizon. Esta ola de ataques continúa.

“Los hallazgos de Sophos sugieren que múltiples adversarios están implementando estos ataques, por lo que el paso de protección más importante es actualizar todos los dispositivos y aplicaciones que incluyen Log4J con la versión parcheada del software”, dijo Gallagher.

“Log4J está instalado en cientos de productos de software y es posible que muchas organizaciones desconocen la vulnerabilidad que acecha dentro de su infraestructura, particularmente en software comercial, de código abierto o personalizado que no cuenta con soporte de seguridad regular. Y aunque la aplicación de parches es vital, no será suficiente si los atacantes ya han podido instalar una puerta trasera en la red”, concluye.

###

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/