La automatización y el ransomware: Sophos detecta incidencia en la propagación automática

- *Sophos detectó una incidencia de ataques automatizados que tratan de explotar una vulnerabilidad de los servidores Atlassian*

CIUDAD DE MÉXICO. 22 de junio de 2022.- De manera reciente, Sophos Labs realizó una investigación que reveló una vulnerabilidad grave dentro Confluence, la intranet central de Atlassian. Si bien la cantidad de servidores vulnerables aún es baja, Sophos detectó una incidencia alta de ataques contra este tipo de servidores, que se ejecutan en Windows o Linux. Dos de esos ataques, dieron como resultado el despliegue de cargas útiles del ransomware Cerber.

La vulnerabilidad, CVE-2022-26134, permite que un atacante genere un webshell de acceso remoto, sin escribir ninguna clase de código en el almacenamiento local del servidor. Atlassian ha publicado actualizaciones del producto (que también solucionan otras vulnerabilidades relacionadas con la seguridad) y estrategias de mitigación, que la mayoría de sus clientes parecen estar implementando.

Pero todo esto tiene una particularidad destacable: la mayoría de casos que Sophos detectó parecen estar automatizados, y algunos de los atacantes usan un shell web sin archivos para propagar varias cargas útiles en un solo movimiento, incluidos bots tipo Mirai; un paquete de Linux malicioso llamado pwnkit; un criptominero conocido como z0miner; y shells web basados en archivos, escritos en formatos ASP o PHP.

Esto indica que los atacantes iniciales que aprovecharon este exploit lo hicieron para, posteriormente, difundir una colección más amplia de herramientas de piratería.

- **‘Gusanos’ de ransomware**

En los dos incidentes en los que los atacantes intentaron implementar ransomware, Sophos detectó ejecuciones inesperadas (probablemente maliciosas) de la herramienta ‘curl’ en el servidor antes de la implementación. Mientras la compañía intentaba comunicarse con los clientes afectados, el atacante entregó un comando de PowerShell codificado al servidor de Confluence que controlaba.

El comando codificado era una instrucción para descargar y ejecutar un programa de Windows, guardado en el directorio ‘%temp%’ en una carpeta con el nombre svcPrvinit.exe. Luego, enviaba la instrucción de eliminar el programa toda vez que había sido ejecutado. Es ahí en donde la carga útil se despliega y se multiplica en diversas carpetas dentro del sistema vulnerado.

Sophos explica que si los servidores no hubieran estado protegidos y el ataque hubiera tenido éxito, los operadores habrían descubierto que la mayoría de sus archivos ahora tendrían el sufijo .locked adjunto a sus nombres, y cada carpeta contendrá un archivo llamado __$$RECOVERY_README$$__. html con un enlace a un sitio web del delincuente y una solicitud de pago dentro de los 30 días siguientes. Todo esto, acompañado de la siguiente amenaza: "publicaremos información sobre sus datos privados en sitios web públicos de noticias".

No hubo evidencia de que los atacantes hubieran desencriptado datos privados de los servidores, ni que los atacantes hubieran hecho ningún movimiento lateral para pasar de los servidores a otras máquinas en las redes de los objetivos.

- **Detección y guía**

Como la mayoría de los clientes de Atlassian han sido notificados sobre las instalaciones vulnerables, cada día que pasa hay menos instancias de servidores Confluence públicos vulnerables. Sophos emitió algunas instrucciones para mover los componentes vulnerables a carpetas que no son de acceso público; por su parte, una actualización de parches por parte de Atlassian debería resolver el problema de la vulnerabilidad en el corto o mediano plazo.

Sumado a ello, Sophos considera que si bien el reinicio de un servidor eliminará cualquier código de shell remoto en la memoria de las máquinas infectadas, éste no eliminará los componentes del kit de herramientas de piratas informáticos que algunos atacantes colocan en el directorio %temp% en Windows. En algunos casos, puede justificarse la eliminación manual del contenido de esas carpetas.

###

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/