Se ha observado una sospechosa campaña de hacking vinculada a China, dirigida a dispositivos SonicWall Secure Mobile Access (SMA) 100 sin parches, con el fin de colocar malware y establecer una persistencia a largo plazo.

> *«El malware tiene la funcionalidad de robar las credenciales de los usuarios, proporcionar acceso de shell y persistir por medio de las actualizaciones de firmware»*, dijo la compañía de seguridad cibernética Mandiant.

La compañía de inteligencia de amenazas y respuesta a incidentes, propiedad de Google, está rastreando la actividad bajo su nombre no categorizado UNC4540.

El malware, una colección de scripts y bash y un solo binario ELF identificado como una backdoor TinyShell, está diseñado para otorgar al atacante acceso privilegiado a los dispositivos SonicWall.

El objetivo general detrás del conjunto de herramientas de personalizado parece ser el robo de credenciales, con el malware que permite al adversario desviar las credenciales cifradas criptográficamente de todos los usuarios registrados. Además, proporciona acceso de shell al dispositivo comprometido.

Mandiant también mencionó la comprensión profunda del atacante del software del dispositivo, así como su capacidad para desarrollar malware personalizado que puede lograr la persistencia en las actualizaciones de firmware y mantener un punto de apoyo en la red.

Se desconoce el vector de intrusión inicial exacto utilizado en el ataque, y se sospecha que el malware probablemente se implementó en los dispositivos, en algunos casos ya en 2021, al aprovechar fallas de seguridad conocidas.

Coincidiendo con la divulgación, SonicWall ha lanzado actualizaciones (versión 10.2.1.7) que vienen con nuevas mejoras de seguridad como el Monitoreo de Integridad de Archivos (FIM) y la identificación de procesos anómalos.

El desarrollo se produce casi dos meses después de que se descubriera que otro atacante de China explotaba una vulnerabilidad ya parcheada en Fortinet FortiOS SSL-VPN como un ataque de día cero contra una entidad gubernamental europea y un proveedor de servicios gestionados (MSP) ubicado en África.

> *«En los últimos años, los atacantes chinos han implementado múltiples exploits de día cero y malware para una variedad de dispositivos de red orientados a Internet como una ruta hacia la intrusión empresarial completa»,* dijo Mandiant.