Un grupo de hackers aprovechó una vulnerabilidad de día cero en los dispositivos VPN de SonicWall para implementar una variedad de ransomware llamada FIVEHANDS antes de que la compañía lanzara los parches correspondientes.

El grupo, rastreado por la compañía de seguridad cibernética Mandiant como UNC2447, se aprovechó de una vulnerabilidad de *«neutralización de comandos SQL inadecuada»* en el producto SSL-VPN-SMA100 (CVE-2021-20016, con puntuación CVSS de 9.8) que permite a un atacante no autenticado lograr un control remoto para ejecutar código.

> *«UNC2447 monetiza las intrusiones extorsionando a sus víctimas primero con el ransomware FIVEHANDS y luego aplicando agresivamente la presión a través de amenazas de atención de los medios y ofreciendo datos de las víctimas a la venta en foros de hackers. Se ha observado que UNC2447 apunta a organizaciones en Europa y América del Norte, y ha mostrado constantemente capacidades avanzadas para evadir la detección y minimizar el análisis forense posterior a la intrusión»,* dijeron los investigadores de Mandiant.

CVE-2021-20016 es el mismo día cero que la compañía con sede en San José dijo que fue explotado por *«actores de amenazas sofisticados» para organizar un «ataque coordinado a sus sistemas internos»* a inicios de este año. El 22 de enero, Masterhacks informó que SonicWall había sido vulnerada al explotar *«probables vulnerabilidades de día cero»* en sus dispositivos de acceso remoto de la serie SMA 100.

La explotación exitosa de la falla otorgaría al atacante la capacidad de acceder a las credenciales de inicio de sesión, así como a la información de la sesión, que después podría usarse para iniciar sesión en un dispositivo vulnerable de la serie SMA 100 sin parches.

Según la subsidiaria propiedad de FireEye, las intrusiones ocurrieron entre enero y febrero de 2021, y el actor de amenazas utilizó el malware SombRAT para implementar el ransomware FIVEHANDS. Cabe mencionar que SombRAT fue descubierto en noviembre de 2020 por investigadores de BlackBerry junto con una campaña llamada CostaRicto.

Los ataques de UNC2447 involucran infecciones de ransomware que se observaron por primera vez en la naturaleza en octubre de 2020, comprometiendo inicialmente los objetivos con el ransomware HelloKitty, antes de cambiarlo por FIVEHANDS en enero de 2021.

> *«Según las observaciones técnicas y temporales de las implementaciones de HelloKitty y FIVEHANDS, es posible que HelloKitty haya sido utilizado por un programa de afiliados general desde mayo de 2020 hasta diciembre de 2020, y FIVEHANDS desde aproximadamente enero de 2021»,* dijeron los investigadores.

FIVEHANDS también se diferencia de DeathRansom y HelloKitty en el uso de cuentagotas de solo memoria y características adicionales que le permiten aceptar argumentos de línea de comandos y utilizar el Administrador de Reinicio de Windows para cerrar un archivo actualmente en uso antes del cifrado.

La divulgación se produce menos de dos semanas después de que FireEye divulgara tres vulnerabilidades previamente desconocidas en el software de seguridad de correo electrónico de SonicWall que fueron explotadas activamente para implementar un shell web para el acceso de puerta trasera a la víctima. FireEye rastrea esta actividad maliciosa bajo el nombre de UNC2682.