Cisco ha revelado que un grupo de amenazas chino, identificado como Salt Typhoon, logró acceso posiblemente aprovechando una vulnerabilidad de seguridad conocida, catalogada como CVE-2018-0171, y obteniendo credenciales legítimas de usuarios víctimas como parte de una ofensiva dirigida contra grandes empresas de telecomunicaciones en Estados Unidos.

> *«Este actor malicioso demostró su capacidad para mantener su presencia en los entornos comprometidos utilizando equipos de distintos proveedores durante largos periodos de tiempo, logrando persistir en un caso por más de tres años»*, indicó Cisco Talos, describiendo al grupo como altamente avanzado y con un respaldo financiero significativo.
>
> *«La duración de esta operación sugiere un alto nivel de planificación, organización y paciencia, características habituales en amenazas persistentes avanzadas (APT) y en actores respaldados por estados.»*

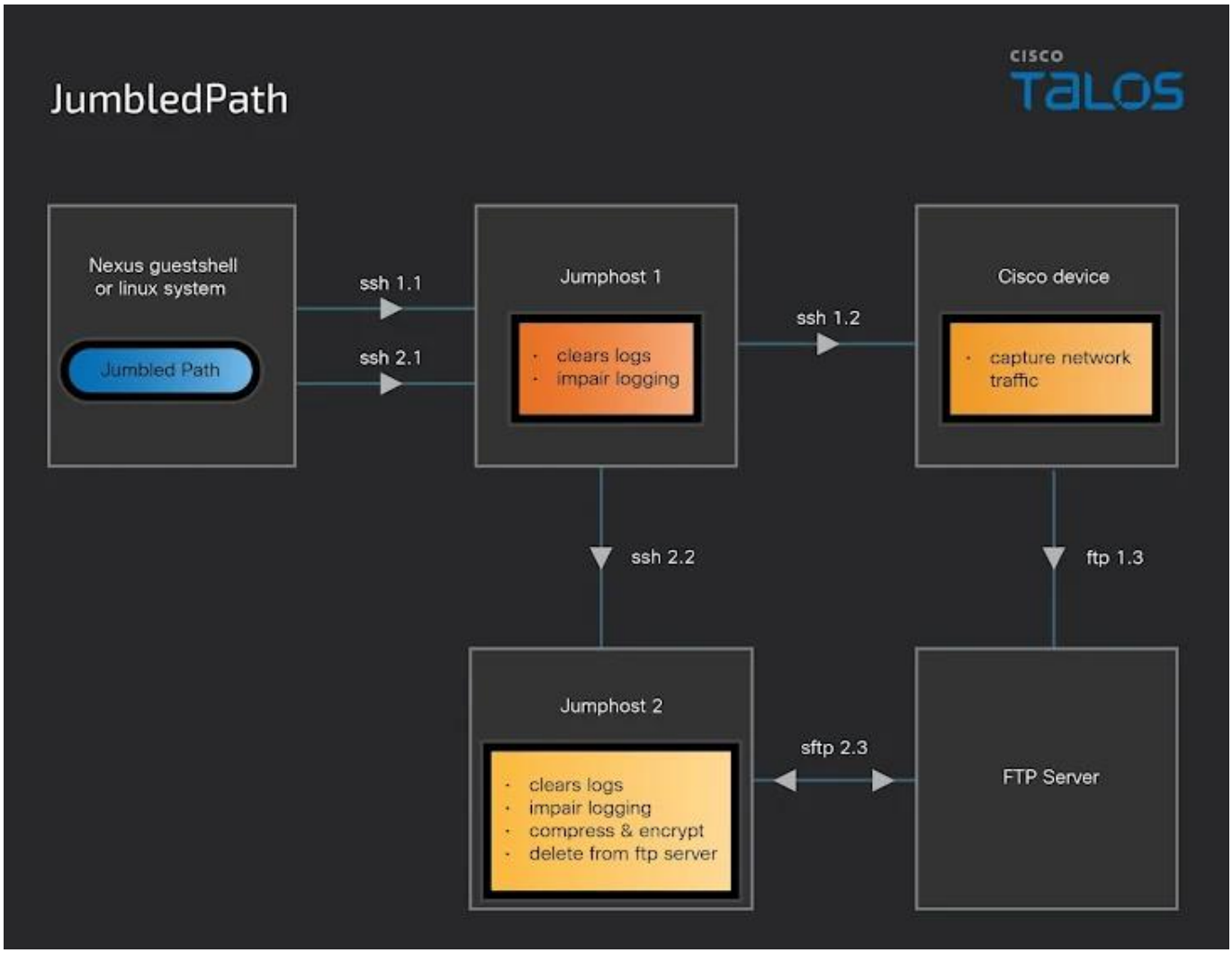
El gigante de redes señaló que no encontró pruebas de que los atacantes hayan explotado otras fallas de seguridad conocidas, en contraste con un informe reciente de Recorded Future que reportó intentos de ataque utilizando vulnerabilidades identificadas como CVE-2023-20198 y CVE-2023-20273 para comprometer redes.

Un elemento clave de esta campaña es el uso de credenciales robadas y válidas para conseguir acceso inicial, aunque el método exacto mediante el cual fueron obtenidas sigue sin esclarecerse. También se ha detectado que los atacantes intentaron recopilar credenciales a través de configuraciones de dispositivos de red y mediante el descifrado de cuentas locales con contraseñas débiles.

> *«Asimismo, hemos observado que el grupo captura tráfico SNMP, TACACS y RADIUS, incluyendo claves secretas utilizadas entre dispositivos de red y servidores TACACS/RADIUS. El objetivo de esta interceptación de tráfico es, con alta*

> *probabilidad, recolectar más credenciales para utilizarlas posteriormente»,* señaló Talos.

Otro comportamiento distintivo de Salt Typhoon es la utilización de técnicas *living-off-the-land* (LOTL) en dispositivos de red, empleando la infraestructura de confianza como un medio para moverse lateralmente entre diferentes empresas de telecomunicaciones.



Se cree que estos dispositivos están siendo aprovechados como puntos intermedios para alcanzar su objetivo final o como un primer paso en la extracción de datos, lo que permite a los atacantes operar sin ser detectados por largos períodos.

Además, se ha identificado que Salt Typhoon altera configuraciones de red para crear nuevas cuentas locales, habilitar acceso a *Guest Shell* y facilitar conexiones remotas mediante SSH. También han implementado una herramienta personalizada llamada *JumbledPath*, diseñada para capturar paquetes en un dispositivo Cisco remoto a través de un servidor intermedio controlado por los atacantes.

El binario ELF basado en Go también es capaz de eliminar registros y desactivar el registro de actividad con el fin de dificultar el rastreo de sus acciones y entorpecer el análisis forense. Esto se complementa con la eliminación periódica de archivos de registro clave, como *.bash_history, auth.log, lastlog, wtmp* y *btmp*, siempre que sea posible.

> *«El uso de esta herramienta permite ocultar el origen y destino real de las conexiones, además de facilitar el movimiento a través de dispositivos o infraestructuras que normalmente no serían accesibles de forma pública o enrutables»*, explicó Cisco.

> *«El actor de amenazas modificó en múltiples ocasiones la dirección de la interfaz de loopback en un switch comprometido y la utilizó como origen de conexiones SSH hacia otros dispositivos dentro del entorno atacado, logrando así evadir las listas de control de acceso (ACL) configuradas en dichos dispositivos.»*

La compañía también detectó *«una actividad generalizada»* dirigida a dispositivos Cisco con la función *Smart Install (SMI)* expuesta, seguida de la explotación de la vulnerabilidad CVE-2018-0171. Sin embargo, Cisco aclaró que esta actividad no está vinculada a Salt Typhoon y no presenta similitudes con ningún grupo de amenazas conocido.