Una variante de Linux de una backdoor conocida como SideWalk, se utilizó para apuntar a una universidad de Hong Kong en febrero de 2021, lo que subraya las capacidades multiplataforma del implante.

La empresa eslovaca de seguridad cibernética ESET, que detectó el malware en la red de la universidad, atribuyó la puerta trasera a un actor de estado-nación denominado SparklingGoblin. Se dice que la universidad no identificada ya fue atacada por el grupo en mayo de 2020 durante las protestas estudiantiles.

> *«El grupo apuntó continuamente a esta organización durante un largo período de tiempo, comprometiendo con éxito múltiples servidores clave, incluido un servidor de impresión, un servidor de correo electrónico y un servidor usado para administrar los horarios de los estudiantes y las inscripciones en los cursos»*, dijo ESET.

SparklingGoblin es el nombre que se le dio a un grupo chino de amenazas persistentes avanzadas (APT) con conexiones al paraguas Winnti (también conocido como APT41, Bario, Earth Baku o Wicked Panda). Es conocido principalmente por sus ataques dirigidos a varias entidades del este y sudeste de Asia al menos desde 2019, con un enfoque específico en el sector académico.

En agosto de 2021, ESET descubrió una nueva pieza de malware de Windows personalizado con nombre en código SideWalk (también conocido como ScrambleCross), que fue aprovechado exclusivamente por el actor para atacar una empresa minorista de computadoras sin nombre con sede en Estados Unidos.

Hallazgos posteriores de Symantec, por parte del software de Broadcom, vincularon el uso de SideWalk con un grupo de ataque de espionaje que se rastrea bajo el nombre de Grayfly, al mismo tiempo que señalan las similitudes del malware con las de CrossWalk.

> *«Las tácticas, técnicas y procedimientos (TTP) de SparklingGoblin se superponen parcialmente con los TTP de APT41. La definición de Grayfly dada por Symantec parece (al menos parcialmente)superponerse con SparklingGoblin»,* dijo Mathieu Tartare, investigador de malware de ESET.

La última investigación de ESET se sumerge en la contraparte de Linux de SideWalk (originalmente llamada StageClient en julio de 2021), y el análisis también revela que Spectre RAT, una botnet de Linux que salió a la luz en septiembre de 2020, es de hecho una variante temprana de SideWalk para Linux.

Además de las múltiples similitudes de código entre SideWalk Linux y varias herramientas de SparklingGoblin, se encontró una de las muestras de Linux usando una dirección de comando y control (66.42.103[.]222) que SparklingGoblin usó anteriormente.

Otros puntos en común incluyen el uso de la misma implementación de ChaCha20 a medida, múltiples subprocesos para ejecutar una tarea en particular, el algoritmo ChaCha20 para descifrar su configuración y una carga útil de resolución de caída muerta idéntica.

A pesar de estas superposiciones, hay algunos cambios significativos, el más notable es el cambio de C a C++, la adición de nuevos módulos integrados para ejecutar tareas programadas y recopilar información del sistema, y cambios en cuatro comandos que no se manejan en la versión de Linux.

> *«Debido a que hemos visto la varianle de Linux solo una vez en nuestra telemetría (implementada en una universidad de Hong Kong en febrero de 2021), se puede considerar que la variante de Linux es menos frecuente, pero también tenemos menos visibilidad en los sistemas Linux, lo que podría explicar esto»,* dijo Tartar.

> *«Por otro lado, la variante Spectre Linux se usa contra cámaras IP y dispositivos NVR y DVR (en los que no tenemos visibilidad) y se propaga masivamente al explotar una vulnerabilidad en dichos dispositivos».*