Los servidores Linux SSH mal administrados están siendo el objetivo de una nueva campaña que implementa distintas variantes de un malware llamado ShellBot.

> *«ShellBot, también conocido como PerlBot, es un malware DDoS Bot desarrollado en Perl, y de forma característica, utiliza el protocolo IRC para comunicarse con el servidor C&C»*, dijo AhnLab Security Emergency Response Center (ASEC).

ShellBot se instala en servidores que tienen credenciales débiles, pero solo después de que los atacantes utilicen el malware del escáner para identificar los sistemas que tienen el puerto SSH 22 abierto.

Se usa una lista de credenciales SSH conocidas para iniciar un ataque de diccionario para violar el servidor e implementar la carga útil, después de lo cual aprovecha el protocolo Internet Relay Chat (IRC) para comunicarse con un servidor remoto.

Esto abarca la capacidad de recibir comandos que permiten a ShellBot llevar a cabo ataques DDoS y filtrar información recopilada.

ASEC dijo que identificó tres versiones distintas de ShellBot: Modded perlbot v2 de LiGhT, DDoS PBot v2.0 y PowerBots (C) GohacK, las dos primeras ofrecen una variedad de comandos de ataque DDoS utilizando los protocolos HTTP, TCP y UDP.

PowerBots, por otro lado, cuenta con más capacidades de backdoor para otorgar acceso de shell inverso y cargar archivos arbitrarios desde el host comprometido.

Los hallazgos llegan casi tres meses después de que ShellBot fuera empleado en ataques dirigidos a servidores Linux que también distribuían mineros de criptomonedas por medio de un compilador de scripts de shell.

> *«Si se instala ShellBot, los servidores Linux se pueden usar como bots DDoS para*

> *ataques DDoS contra objetivos específicos después de recibir un comando del atacante. Además, el actor de amenazas podría usar varias otras funciones de backdoor para instalar malware adicional o lanzar diferentes tipos de ataques desde el servidor comprometido»,* dijo ASEC.

El desarrollo también se produce cuando Microsoft reveló un aumento gradual en la cantidad de ataques DDoS dirigidos a organizaciones de atención médica alojadas en Azure, pasando de 10 a 20 ataques en noviembre de 2022 a 40-60 ataques diarios en febrero de 2023.