Un malware de botnet de Linux conocido como XorDdos ha sido testigo de un aumento del 254% en la actividad en los últimos seis meses, según las últimas investigaciones de Microsoft.

El troyano, llamado así por llevar a cabo ataques de denegación de servicio en sistemas Linux y su uso de cifrado basado en XOR para las comunicaciones con su servidor de comando y control (C2), ha estado activo desde al menos 2014.

> *«La naturaleza modular de XorDdos proporciona a los atacantes un troyano versátil capaz de infectar una variedad de arquitecturas de sistemas Linux»,* dijeron Ratnesh Pandey, Yevgeny Kulakov y Jonathan Bar Or, del equipo de investigación de Microsoft 365 Defender.

> *«Sus ataques de fuerza bruta SSH son una técnica relativamente simple pero efectiva para obtener acceso a la raíz sobre una serie de objetivos potenciales».*

El control remoto sobre vulnerabilidades IoT vulnerables y otros dispositivos conectados a Internet se obtiene mediante ataques de fuerza bruta de shell seguro (SSH), lo que permite que el malware forme una red de bots capaz de transportar ataques de denegación de servicio distribuido (DDoS).

Además de estar compilado para arquitecturas ARM, x86 y x64, el malware está diseñado para admitir distintas distribuciones de Linux, sin mencionar que cuenta con funciones para desviar información confidencial, instalar un rootkit y actuar como un vector para actividades de seguimiento.

En los últimos años, XorDdos se ha centrado en servidores Docker desprotegidos con puertos expuestos (2375), utilizando sistemas victimizados para abrumar una red o servicio de destino con tráfico falso para volverlo inaccesible.

Desde entonces, XorDdos se ha convertido en la principal amenaza dirigida a Linux en 2021, según un informe de CrowdStrike publicado a inicios de enero.

> *«XorDdos utiliza mecanismos de evasión y persistencia que permiten que sus operaciones sigan siendo robustas y sigilosas»,* dijeron los investigadores.

> *«Sus capacidades de evasión incluyen ofuscar las actividades del malware, evadir los mecanismos de detección basados en reglas y la búsqueda de archivos maliciosos basada en hash, así como el uso de técnicas anti-forenses para romper el análisis en árboles de procesos»,* agregaron.