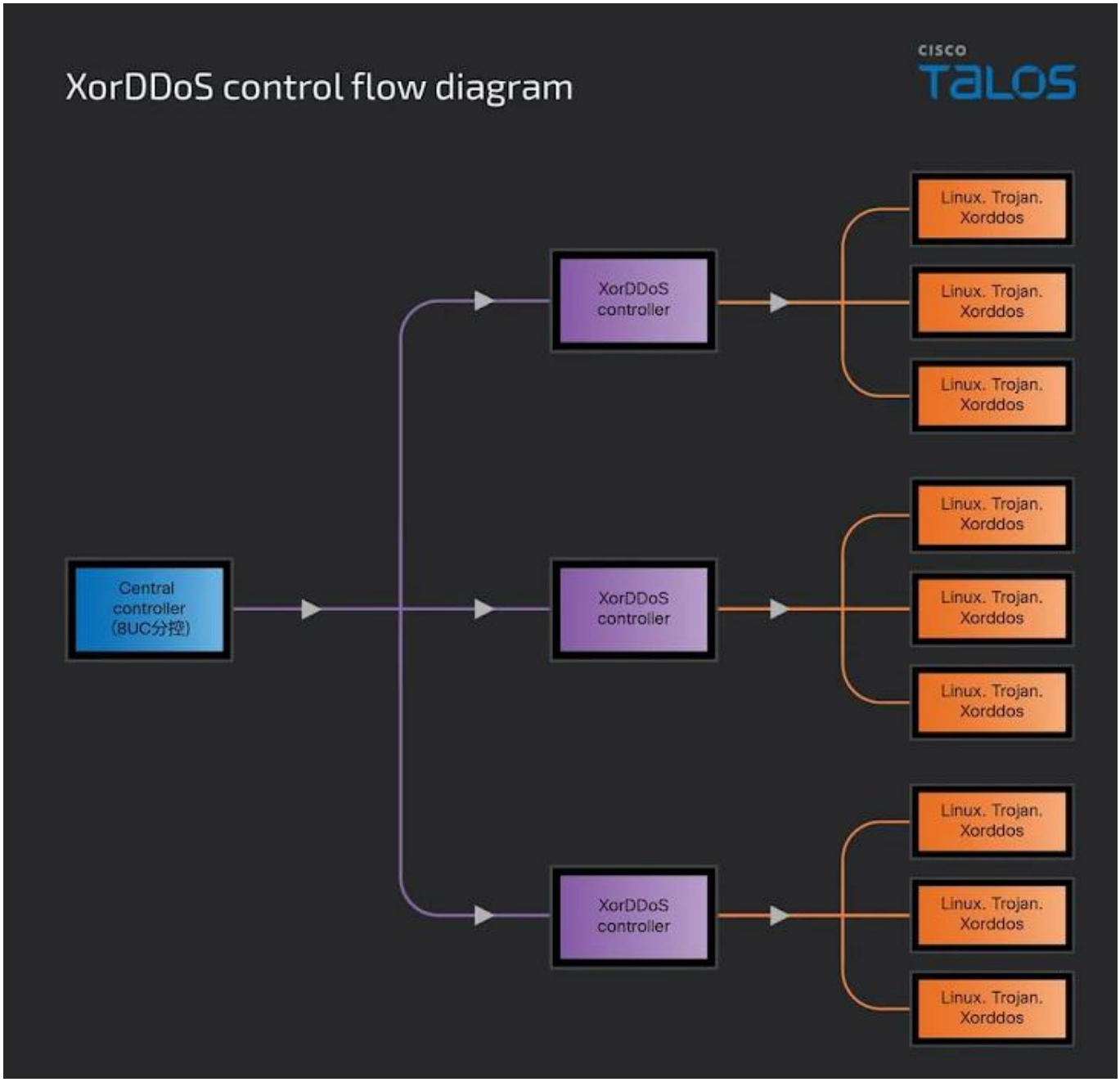
Investigadores en ciberseguridad han alertado sobre los riesgos continuos que representa un malware de denegación de servicio distribuido (DDoS) conocido como XorDDoS, el cual ha tenido como objetivo a Estados Unidos en el 71.3 % de los ataques entre noviembre de 2023 y febrero de 2025.

Según un análisis publicado el jueves por Joey Chen, investigador de Cisco Talos, *"desde 2020 hasta 2023, el troyano XorDDoS ha aumentado considerablemente en su presencia"*.

Este crecimiento se debe no solo a su amplia distribución a nivel mundial, sino también al incremento de solicitudes DNS maliciosas asociadas con su infraestructura de comando y control (C2). Además de atacar máquinas Linux expuestas, el troyano ha ampliado su alcance a servidores Docker, convirtiendo los dispositivos infectados en parte de una red de bots.

Casi el 42 % de los dispositivos comprometidos están en Estados Unidos, seguidos por Japón, Canadá, Dinamarca, Italia, Marruecos y China.



XorDDoS es un malware conocido desde hace más de una década por atacar sistemas Linux. En mayo de 2022, Microsoft informó un aumento importante en su actividad, destacando que estas infecciones también abrían la puerta a otros programas maliciosos como Tsunami,

dedicado a la minería de criptomonedas.

El principal método de acceso inicial consiste en ataques de fuerza bruta a Secure Shell (SSH) para obtener credenciales válidas, lo que permite luego descargar e instalar el malware en dispositivos IoT y otros equipos conectados a Internet que sean vulnerables.

Una vez logra acceso, el malware establece persistencia mediante un script de inicialización y una tarea programada (cron job), de forma que se ejecute automáticamente al iniciar el sistema. También utiliza una clave XOR («BB2FA36AAA9541F0») para descifrar su configuración interna y obtener las direcciones IP necesarias para comunicarse con su servidor de control.

En 2024, Talos detectó una nueva variante del subcontrolador XorDDoS, denominada versión VIP, junto con su controlador central y una herramienta de creación de malware, lo que sugiere que este conjunto podría estar siendo comercializado como un producto.

El controlador central se encarga de gestionar múltiples subcontroladores XorDDoS y de enviar comandos de ataque DDoS de manera simultánea. A su vez, cada subcontrolador coordina una botnet formada por dispositivos comprometidos.

Joey Chen también señaló que la configuración de idioma de los distintos componentes del malware sugiere fuertemente que sus operadores hablan chino.