Un recién creado conjunto de dispositivos de seguridad, incluyendo firewalls y routers de marcas como Cisco, DrayTek, Fortinet y NETGEAR, está siendo aprovechado como una red encubierta para la transferencia de datos por actores de amenazas persistentes avanzadas, entre ellos el grupo de amenazas asociado a China conocido como Volt Typhoon.

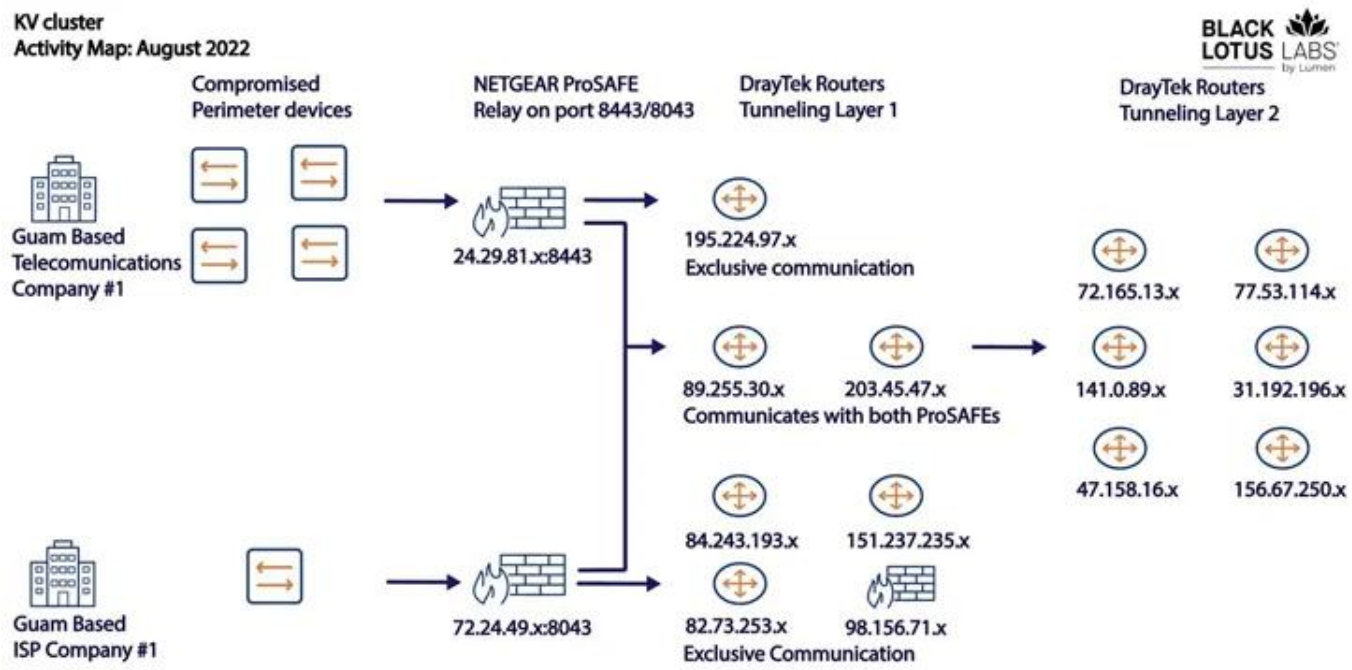
Identificado como KV-botnet por el equipo de Black Lotus Labs en Lumen Technologies, esta red maliciosa representa una fusión de dos grupos de actividad complementarios que han estado operando desde al menos febrero de 2022.

> *«La campaña en cuestión se centra en infectar dispositivos en el borde de las redes, un sector que ha mostrado vulnerabilidades en las defensas de muchas empresas, especialmente con el cambio hacia el trabajo remoto en los últimos años»,* según señala la compañía.

Los dos grupos, denominados KV y JDY, se consideran distintos pero trabajan en conjunto para posibilitar el acceso a objetivos de alto perfil y establecer infraestructura encubierta. Los datos de telemetría indican que el botnet está siendo controlado desde direcciones IP ubicadas en China.

Mientras que los bots del grupo JDY se enfocan en exploraciones más amplias utilizando técnicas menos sofisticadas, el componente KY, que utiliza principalmente productos obsoletos y fuera de servicio, se reserva para operaciones manuales dirigidas a objetivos de alto perfil seleccionados por el primero.

Se sospecha que Volt Typhoon es al menos uno de los usuarios del KV-botnet, representando un subconjunto de su infraestructura operativa. Esto se evidencia por la marcada disminución en las operaciones durante junio y principios de julio de 2023, coincidiendo con la divulgación pública del enfoque de este colectivo adversario en la infraestructura crítica en los Estados Unidos.



Microsoft, el primero en exponer las tácticas del actor de amenazas, indicó que este *«busca integrarse en la actividad normal de la red al dirigir el tráfico a través de equipos de pequeñas oficinas y oficinas domésticas (SOHO) comprometidos, incluyendo routers, firewalls y hardware de VPN».*

La metodología exacta del proceso inicial de infección utilizada para vulnerar los dispositivos es actualmente desconocida. Esto es seguido por el malware de primera fase que toma medidas para eliminar programas de seguridad y otras cepas de malware, asegurándose de ser la *«única presencia»* en estas máquinas.

Asimismo, está diseñado para recuperar la carga principal desde un servidor remoto, el cual, además de enviar señales de vuelta a dicho servidor, también es capaz de cargar y descargar archivos, ejecutar comandos y activar módulos adicionales.

Durante el último mes, la infraestructura del botnet ha experimentado una transformación, enfocándose en cámaras IP de Axis, lo que sugiere que los operadores podrían estar

preparándose para una nueva serie de ataques.

> *«Un aspecto particularmente interesante de esta campaña es que todas las herramientas parecen residir completamente en la memoria. Esto complica enormemente la detección, a costa de la persistencia a largo plazo»,* destacaron los investigadores.

> *«Dado que el malware reside totalmente en la memoria, simplemente apagando y encendiendo el dispositivo, el usuario final puede detener la infección. Aunque esto elimina la amenaza inminente, la reinfección ocurre de forma regular».*

Estos descubrimientos coinciden con el informe de The Washington Post que señaló que alrededor de dos docenas de entidades críticas en Estados Unidos han sido infiltradas por Volt Typhoon en el último año, incluyendo servicios públicos de energía y agua, así como sistemas de comunicación y transporte.

> *«Los piratas informáticos a menudo buscaron ocultar sus rastros al encauzar sus ataques a través de dispositivos inocentes como routers domésticos u oficinistas antes de llegar a sus víctimas»*, agregó el informe.