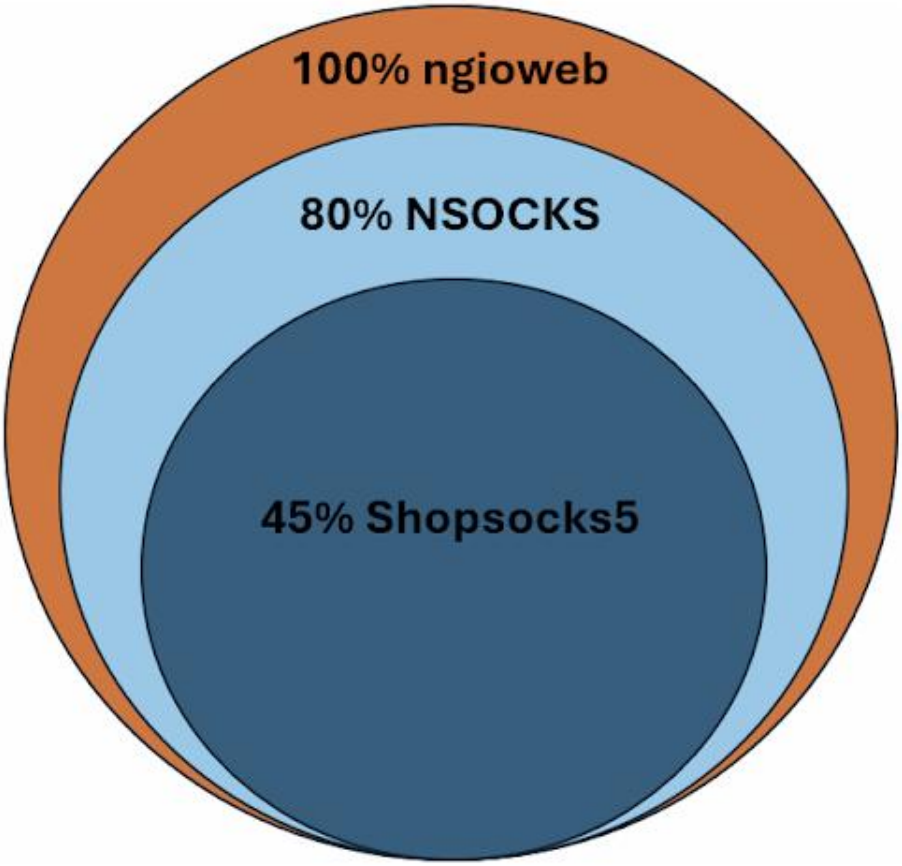
El malware denominado Ngioweb ha sido utilizado para impulsar un servicio de proxy residencial infame llamado NSOCKS, así como otros servicios como VN5Socks y Shopsocks5, según recientes descubrimientos de Lumen Technologies.

> *«Al menos el 80% de los bots de NSOCKS en nuestra telemetría provienen de la botnet Ngioweb, principalmente utilizando enrutadores de oficinas pequeñas/hogar (SOHO) y dispositivos IoT. Dos tercios de estos proxies están ubicados en EE. UU.»*, explicó el equipo de Black Lotus Labs de Lumen Technologies en un informe.
>
> *«La red mantiene un promedio diario de alrededor de 35,000 bots activos, con el 40% permaneciendo operativos durante un mes o más».*

Ngioweb, que fue documentado por primera vez por Check Point en agosto de 2018 en relación con una campaña del troyano Ramnit, ha sido objeto de análisis exhaustivos en las últimas semanas por LevelBlue y Trend Micro. Esta última firma rastrea al actor de amenazas detrás de la operación, con motivaciones económicas, bajo el nombre de Water Barghest.

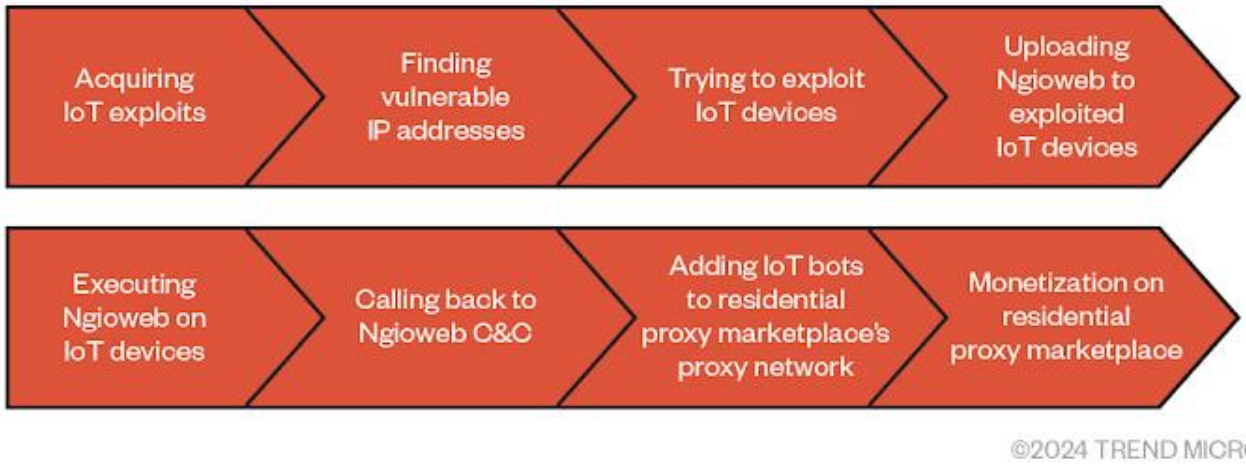
Este malware es capaz de atacar dispositivos que ejecutan tanto Microsoft Windows como Linux, y su nombre proviene del dominio de comando y control (C2) registrado en 2018 bajo el nombre «ngioweb[.]su».

Según Trend Micro, la botnet estaba formada por más de 20,000 dispositivos IoT en octubre de 2024. Water Barghest usa esta red para localizar e infiltrarse en dispositivos IoT vulnerables mediante scripts automatizados, instalar el malware Ngioweb y registrarlos como proxies. Los bots infectados luego se ponen a disposición para su venta en mercados de proxies residenciales.



> *«El proceso de monetización, desde la infección inicial hasta que el dispositivo se convierte en un proxy en un mercado residencial, puede llevar tan solo 10 minutos, lo que indica una operación extremadamente eficiente y automatizada»,* comentaron los investigadores Feike Hacquebord y Fernando Mercês.

Las cadenas de ataque que utilizan este malware explotan una variedad de vulnerabilidades y *zero-days* para penetrar enrutadores y dispositivos IoT domésticos como cámaras, aspiradoras y sistemas de control de acceso, entre otros. La botnet emplea una arquitectura de dos niveles: el primero es una red de cargadores compuesta por 15-20 nodos, que redirige el bot hacia un nodo C2 de carga para descargar y ejecutar el malware Ngioweb.



Un desglose de los proxies de los proveedores residenciales por tipo de dispositivo muestra que los operadores de la botnet han dirigido sus ataques a una amplia variedad de marcas, incluyendo NETGEAR, Uniview, Reolink, Zyxel, Comtrend, SmartRG, Linear Emerge, Hikvision, y NUUO.

Las últimas revelaciones de LevelBlue y Lumen indican que los sistemas infectados con el troyano Ngioweb se están vendiendo como servidores proxy residenciales para NSOCKS, que ya ha sido utilizado por actores maliciosos en ataques de relleno de credenciales (*credential-stuffing*) contra Okta.

> *«NSOCKS ofrece acceso a proxies SOCKS5 en todo el mundo, permitiendo a los compradores elegirlos por ubicación (estado, ciudad o código postal), proveedor de servicios de Internet (ISP), velocidad, tipo de dispositivo infectado y antigüedad. Los precios varían entre $0.20 y $1.50 por 24 horas de acceso, dependiendo del tipo de dispositivo y del tiempo transcurrido desde la infección»*, afirmó LevelBlue.

Los dispositivos afectados también se han encontrado estableciendo conexiones duraderas

con una segunda fase de dominios C2, los cuales son generados por un algoritmo de generación de dominios (DGA). Estos dominios, que pueden llegar a ser unos 15 en cualquier momento, funcionan como el «filtro», evaluando si los bots son aptos para ser incluidos en la red de proxies.

Si los dispositivos cumplen con los requisitos establecidos, los nodos C2 DGA los redirigen hacia un nodo C2 backconnect, que luego los pone a disposición a través del servicio de proxy NSOCKS.

> *«Los usuarios de NSOCKS dirigen su tráfico a través de más de 180 nodos C2 'backconnect' que actúan como puntos de entrada y salida, utilizados para ocultar o hacer de proxy su verdadera identidad. Los responsables de este servicio no solo han proporcionado una vía para que sus clientes encubran el tráfico malicioso, sino que también han diseñado la infraestructura de forma que permita a diversos actores de amenazas crear sus propios servicios»,* explicó Lumen Technologies.

Para complicar aún más la situación, los proxies abiertos respaldados por NSOCKS también han sido aprovechados como una vía para que distintos actores lancen potentes ataques distribuidos de denegación de servicio (DDoS) a gran escala.

Se prevé que tanto el mercado comercial de servicios de proxies residenciales como el mercado clandestino de proxies crezcan en los próximos años, impulsados en parte por la demanda de grupos de amenazas persistentes avanzadas (APT) y grupos de ciberdelincuentes.

> *«Estas redes son frecuentemente utilizadas por delincuentes que descubren vulnerabilidades o roban credenciales, brindándoles una forma eficaz de desplegar herramientas maliciosas sin revelar su ubicación o identidad»*, afirmó Lumen.

> *«Lo que resulta especialmente preocupante es la manera en que un servicio como NSOCKS puede ser utilizado. Con NSOCKS, los usuarios tienen la opción de elegir entre 180 países diferentes para su punto de conexión. Esta capacidad no solo facilita a los actores maliciosos extender sus actividades por todo el mundo, sino que también les permite orientar sus ataques a entidades específicas por dominio, como .gov o .edu, lo cual podría dar lugar a ataques más dirigidos y potencialmente más destructivos».*