Google ha logrado debilitar de forma considerable a NetNut, una de las mayores redes dedicadas a convertir dispositivos domésticos en nodos de retransmisión alquilados para canalizar el tráfico de terceros.

En colaboración con el FBI, Lumen y otras organizaciones, el Grupo de Inteligencia sobre Amenazas de Google (GTIG) informó esta semana que consiguió reducir en millones la cantidad de dispositivos funcionales que integraban esta infraestructura.

Según Google, NetNut —también identificada como Popa— opera como una extensa red distribuida entre dispositivos domésticos de todo el mundo, incluidos televisores inteligentes y equipos de streaming. GTIG estima que la red está conformada por al menos dos millones de dispositivos.

Si alguno de estos equipos se encuentra en un hogar, terceros pueden utilizar la conexión a Internet de esa vivienda para enrutar su propio tráfico, haciendo que la dirección IP del propietario aparezca asociada a cualquier actividad realizada.

Cómo funciona

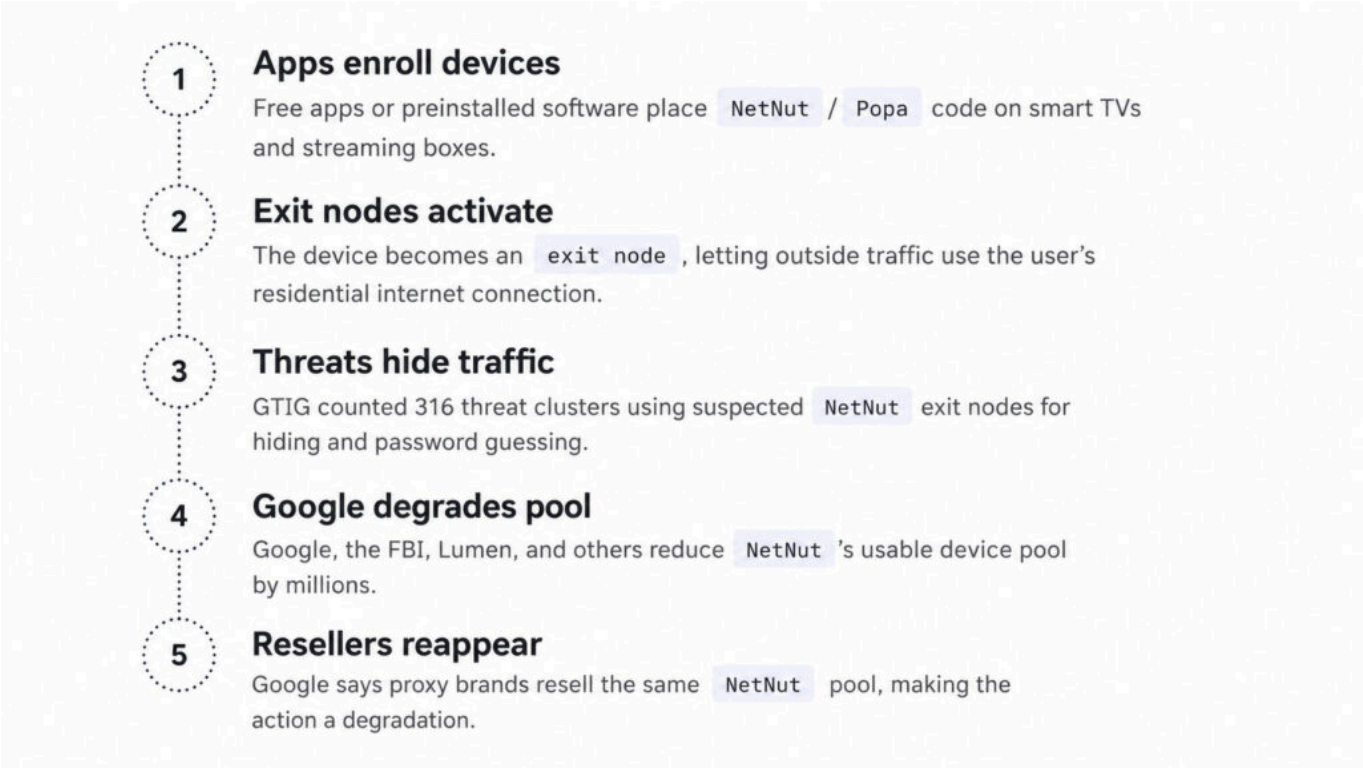
Las redes de proxies residenciales comercializan acceso a direcciones IP pertenecientes a hogares reales. Los ciberdelincuentes pagan por utilizar estas conexiones con el fin de que su tráfico parezca provenir de usuarios comunes, en lugar de centros de datos, cuyos accesos suelen ser detectados y bloqueados por herramientas de seguridad.

Para conformar este tipo de infraestructura, los operadores necesitan ejecutar su software en dispositivos domésticos. En algunos casos, el código viene instalado de fábrica en equipos económicos de fabricantes poco conocidos; en otros, se incorpora cuando el usuario instala una aplicación gratuita que oculta esta funcionalidad. Una vez activo, el dispositivo se convierte en un *«nodo de salida»*, es decir, un punto desde el cual circula el tráfico de otros usuarios.

Google advierte que un nodo de salida introduce tráfico externo dentro de la red doméstica,

proporcionando a los atacantes una posible vía de acceso hacia otros dispositivos conectados. Además, algunos de estos equipos también han sido incorporados a botnets de gran escala como Mirai y Badbox 2.0.

Durante una sola semana de junio, GTIG identificó 316 grupos de amenazas distintos que utilizaron presuntos nodos de salida de NetNut. Entre ellos figuraban tanto organizaciones de ciberdelincuencia como actores dedicados al espionaje, quienes aprovecharon la infraestructura para ocultar su ubicación real y ejecutar ataques de fuerza bruta contra credenciales.

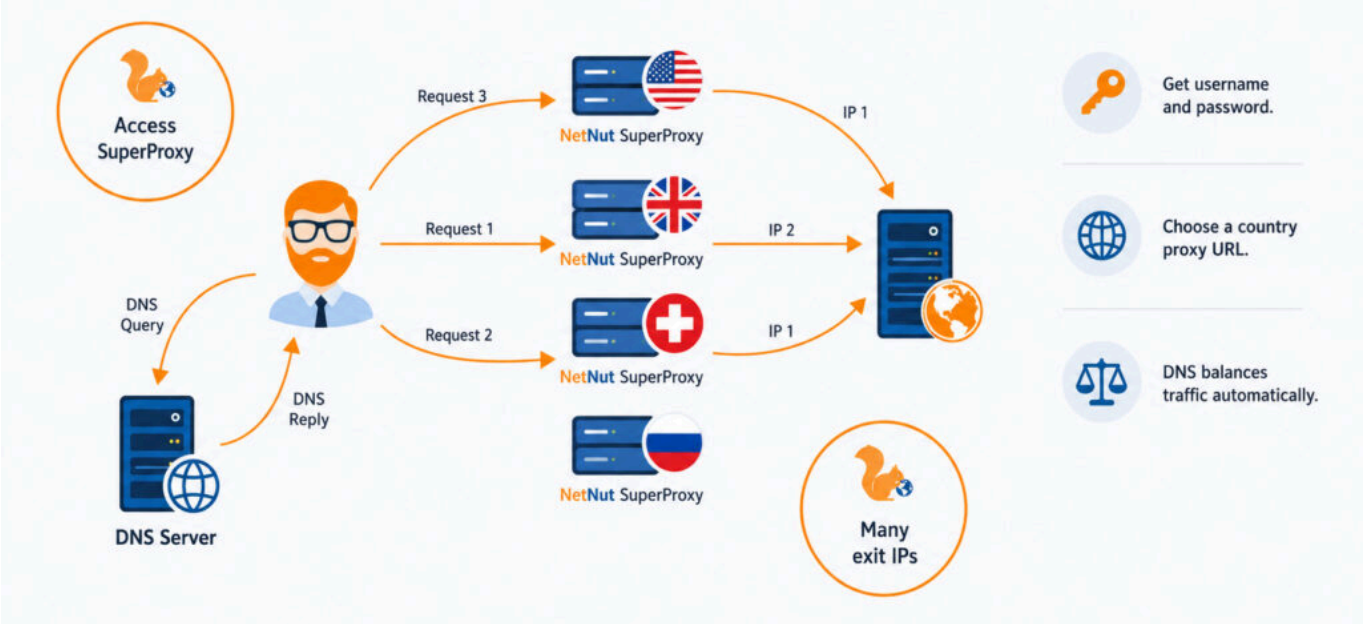


La empresa detrás de la red

A diferencia de la mayoría de las botnets de proxies, NetNut puede vincularse con una

empresa pública. En junio, investigadores de Qurium, Synthient, Nokia Deepfield y Spur relacionaron a Popa con NetNut.

NetNut es un proveedor de servicios de proxy perteneciente a la empresa israelí Alarum Technologies (NASDAQ: ALAR), que cotiza en bolsa. Durante una prueba controlada, Synthient comprobó que el tráfico enviado a través de la pasarela comercial de NetNut terminaba saliendo por un dispositivo previamente incorporado a Popa.

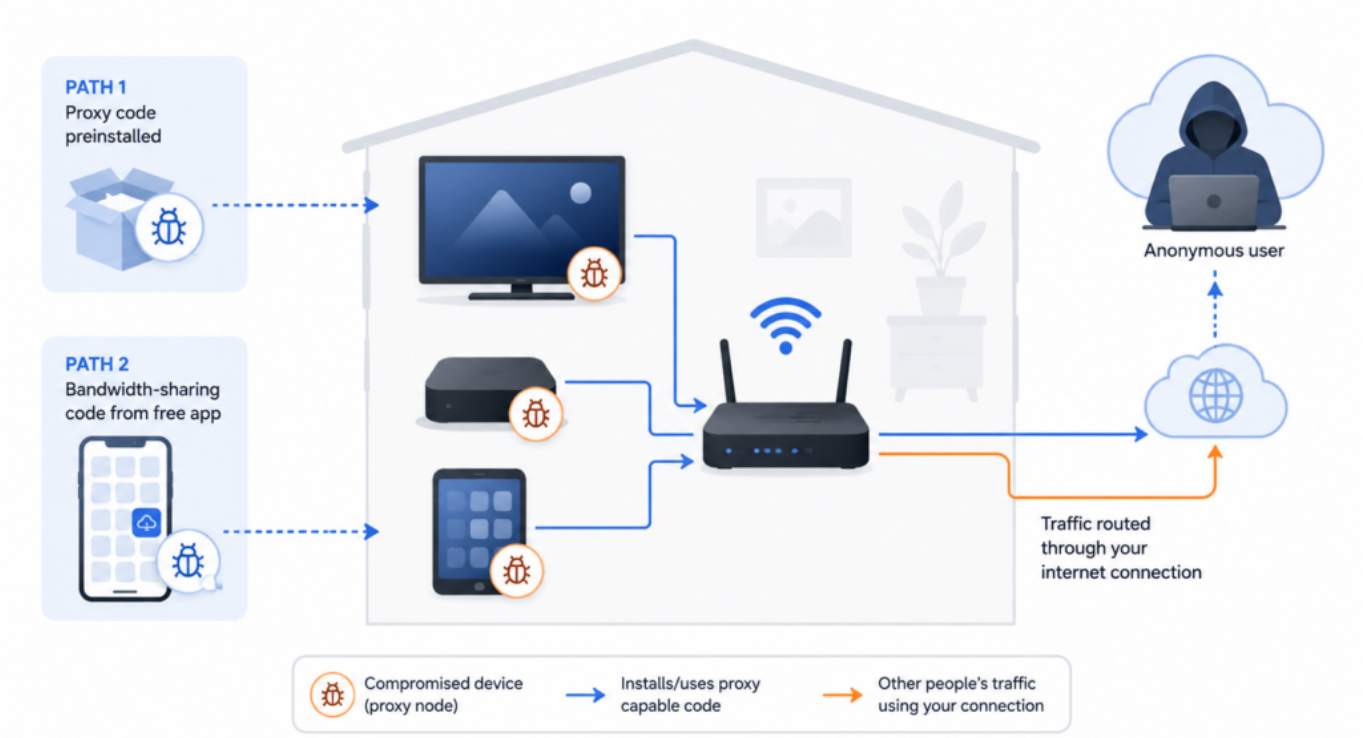


Los investigadores señalaron que este experimento demuestra la ruta seguida por el tráfico, aunque no constituye una prueba de lo que NetNut conocía o pretendía hacer. La evaluación de Google coincide con estas conclusiones: considera que NetNut y Popa forman parte de una misma infraestructura y sostiene que los hallazgos públicos concuerdan con su análisis sobre el funcionamiento de esta botnet.

Por su parte, Alarum rechaza que NetNut pueda calificarse como una «*botnet*». La compañía afirma que el estudio contiene «*afirmaciones demostrablemente inexactas y deducciones erróneas en lugar de hechos verificados*», y sostiene que su software está diseñado para

compartir ancho de banda únicamente con el consentimiento de los usuarios y sin comprometer la seguridad de los dispositivos.

Sin embargo, las pruebas realizadas por los investigadores ponen en duda esa explicación. Synthient informó que ninguna de las más de veinte aplicaciones analizadas mostraba a los usuarios un aviso solicitando consentimiento para participar en este tipo de red.



Por qué una sola intervención no basta

Desmantelar NetNut resulta especialmente complejo debido a la forma en que está estructurada. La empresa mantiene un programa de revendedores que permite a otras compañías comercializar el acceso a su red utilizando marcas diferentes. Google afirma tener un alto grado de confianza en que numerosos servicios de proxy aparentemente

independientes revenden, en realidad, la misma infraestructura de NetNut.

Como consecuencia, una única operación de interrupción afecta simultáneamente a múltiples proveedores que aparentan ser independientes, aunque comparten la misma red subyacente.

Esta es también la razón por la que Google describe la operación como una degradación y no como una eliminación definitiva. La compañía recuerda que, tras una acción previa contra la red IPIDEA, quedó demostrado que este tipo de infraestructuras suelen recuperarse rápidamente, ya que sus operadores comienzan a adquirir capacidad de otras redes competidoras, convirtiéndose incluso en revendedores de estas. Según Google, generar un impacto duradero requiere actuar de manera coordinada contra varios proveedores relacionados al mismo tiempo.

En enero, Google y sus socios lograron interrumpir las operaciones de IPIDEA, una red con sede en China que llegó a ser una de las mayores de su categoría. Posteriormente, en julio de 2025, Google inició acciones legales contra los responsables de Badbox 2.0, la botnet compuesta por dispositivos Android TV comprometidos que comparte componentes con Popa. En ambos casos, las redes demostraron una notable capacidad para recuperarse.

Qué deben hacer los consumidores

La señal de alerta más evidente es la aparición de aplicaciones que prometen recompensas económicas por el *«ancho de banda no utilizado»* o por *«compartir su conexión a Internet»*. Este es uno de los principales mecanismos mediante los cuales estas redes consiguen incorporar nuevos dispositivos.

Además, se recomienda:

- Descargar aplicaciones únicamente desde tiendas oficiales y revisar cuidadosamente los permisos solicitados por aplicaciones VPN o de proxy.
- Mantener habilitadas las funciones de protección integradas, como Google Play

Protect.
- Adquirir televisores inteligentes y dispositivos de streaming de fabricantes reconocidos, evitando equipos de marcas desconocidas.

La demanda de direcciones IP residenciales no desaparece cuando una de estas redes es desarticulada; simplemente se desplaza hacia otros proveedores. Para los equipos de seguridad y las plataformas tecnológicas, el siguiente indicador clave será determinar si el tráfico asociado con NetNut reaparece a través de marcas operadas por sus revendedores.