Una red de bots anteriormente considerada inactiva ha sido detectada controlando routers de hogar/oficina pequeña (SOHO) y dispositivos IoT al final de su vida útil (EoL) para impulsar un servicio proxy delictivo denominado Faceless.

> *«TheMoon, que surgió en 2014, ha estado operando en silencio mientras crecía hasta alcanzar más de 40,000 bots provenientes de 88 países en enero y febrero de 2024″,* informó el equipo de Black Lotus Labs en Lumen Technologies.

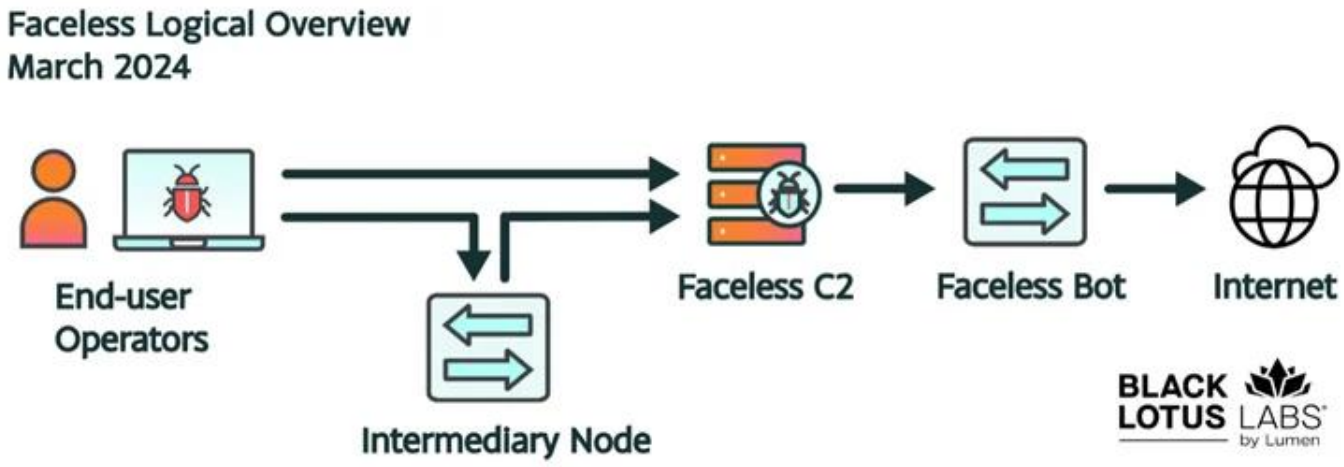
Faceless, descrito por el periodista de seguridad Brian Krebs en abril de 2023, es un servicio proxy residencial malicioso que ofrece servicios de anonimato a otros actores de amenazas por una tarifa insignificante, que cuesta menos de un dólar al día.

Al hacerlo, permite a los clientes enmascarar su tráfico malicioso a través de decenas de miles de sistemas comprometidos anunciados en el servicio, ocultando eficazmente sus verdaderos orígenes.

Se ha determinado que la infraestructura respaldada por Faceless es utilizada por operadores de malware como SolarMarker e IcedID para conectarse a sus servidores de comando y control (C2) y así ocultar sus direcciones IP.

No obstante, la mayoría de los bots se utilizan para realizar ataques de rociado de contraseñas y/o exfiltración de datos, dirigidos principalmente al sector financiero, con más del 80% de los hosts infectados ubicados en los EE. UU.

Lumen señaló que observó por primera vez la actividad maliciosa a finales de 2023, con el objetivo de comprometer routers SOHO y dispositivos IoT al final de su vida útil (EoL) y desplegar una versión actualizada de TheMoon, y finalmente incorporar la botnet a Faceless.



Los ataques implican dejar un cargador que se encarga de descargar un archivo ejecutable ELF desde un servidor C2. Esto incluye un módulo gusano que se propaga a otros servidores vulnerables y otro archivo llamado «.sox» que se utiliza para enrutar el tráfico desde el bot hacia Internet en nombre de un usuario.

Además, el malware configura reglas iptables para bloquear el tráfico TCP entrante en los puertos 8080 y 80, permitiendo únicamente el tráfico de tres rangos de IP específicos. También intenta contactar con un servidor NTP de una lista de servidores NTP legítimos, probablemente para determinar si el dispositivo infectado tiene conectividad a Internet y no se está ejecutando en un entorno controlado.

El ataque a dispositivos al final de su vida útil para formar la botnet no es una coincidencia, ya que estos dispositivos ya no reciben soporte del fabricante y se vuelven vulnerables a las amenazas de seguridad con el tiempo. Además, es posible que los dispositivos sean infiltrados mediante ataques de fuerza bruta.

Un análisis adicional de la red proxy ha revelado que más del 30% de las infecciones duraron más de 50 días, mientras que alrededor del 15% de los dispositivos formaron parte de la red durante 48 horas o menos.

> *«Faceless se ha convertido en un servicio proxy formidable que surgió del desaparecido servicio de anonimato 'iSocks' y se ha convertido en una herramienta integral para los ciberdelincuentes en la ocultación de su actividad. TheMoon es el principal, si no el único, proveedor de bots para el servicio proxy Faceless»*, afirmó la empresa.