Una campaña de malware activa está haciendo uso de dos vulnerabilidades de día cero con funcionalidad de ejecución remota de código (RCE) para incorporar routers y grabadoras de video en un botnet de denegación de servicio distribuido (DDoS) basado en Mirai.

> *«La carga útil se dirige a routers y dispositivos grabadores de video en red (NVR) mediante credenciales de administrador predeterminadas e instala variantes de Mirai cuando tiene éxito»*, indicó Akamai en un comunicado publicado esta semana.

La información detallada sobre las fallas se mantiene confidencial por el momento para permitir que los dos proveedores publiquen soluciones y evitar que otros actores de amenazas las exploten. Se espera que las correcciones para una de las vulnerabilidades se implementen el próximo mes.

Los ataques fueron detectados inicialmente por la empresa de seguridad y de infraestructura web en sus honeypots a finales de octubre de 2023. Hasta el momento, no se ha identificado a los perpetradores de estos ataques.

El botnet, que ha sido llamado InfectedSlurs debido al uso de lenguaje racial y ofensivo en los servidores de control (C2) y cadenas codificadas, es una variante del malware JenX Mirai que salió a la luz en enero de 2018.

Akamai también identificó otras muestras de malware que parecen estar relacionadas con la variante hailBot Mirai, que emergió en septiembre de 2023, según un análisis reciente de NSFOCUS.

> *«HailBot se desarrolla sobre la base del código fuente de Mirai, y su nombre proviene de la información de cadena 'hail china mainland' que se genera después de ejecutarse»,* detalló la firma de ciberseguridad con sede en Pekín, describiendo su capacidad para propagarse mediante la explotación de vulnerabilidades y contraseñas débiles.

Este desarrollo se presenta mientras Akamai revela la existencia de un web shell denominado wso-ng, una versión avanzada de WSO (acrónimo de «web shell by oRb») que se integra con herramientas legítimas como VirusTotal y SecurityTrails, al mismo tiempo que oculta su interfaz de inicio de sesión detrás de una página de error 404 al intentar acceder.

Una de las capacidades de reconocimiento notables del web shell involucra la obtención de metadatos de AWS para un movimiento lateral posterior, así como la búsqueda de posibles conexiones de base de datos Redis para obtener acceso no autorizado a datos de aplicaciones sensibles.

> *«Los web shells permiten a los atacantes ejecutar comandos en servidores para robar datos o utilizar el servidor como punto de partida para otras actividades, como robo de credenciales, movimiento lateral, despliegue de cargas útiles adicionales o actividad práctica con teclado, mientras permiten a los atacantes persistir en una organización afectada»,* señaló Microsoft en 2021.

El uso de web shells listos para usar también se interpreta como un intento de los actores de amenazas de desafiar los esfuerzos de atribución y pasar desapercibidos, una característica clave de los grupos de ciberespionaje especializados en recopilación de inteligencia.

Otra táctica común adoptada por los atacantes es el empleo de dominios comprometidos pero legítimos con fines de C2 y distribución de malware.

En agosto de 2023, Infoblox reveló un ataque generalizado que involucraba sitios web de WordPress comprometidos que redirigen selectivamente a visitantes a dominios de C2 intermedios y dominios de generación de algoritmos de diccionario (DDGA). La actividad fue atribuida a un actor de amenazas conocido como VexTrio.