Un análisis de más de 70 mil millones de registros DNS llevó al descubrimiento de un nuevo y sofisticado conjunto de herramientas de malware denominado Decoy Dog, dirigido a redes empresariales.

Decoy Dog es evasivo y emplea técnicas como el envejecimiento estratégico del dominio y el goteo de consultas de DNS, en el que se transmite una serie de consultas a los dominios de comando y control (C2) para no despertar sospechas.

> *«Decoy Dog es un conjunto de herramientas cohesivo con una serie de características muy inusuales que lo hacen identificable de forma única, particularmente cuando se examinan sus dominios a nivel de DNS»,* dijo Infoblox en un aviso.

La compañía de ciberseguridad, que identificó el malware a inicios de abril de 2023 después de una actividad anómala de señalización de DNS, dijo que sus características atípicas le permitieron mapear dominios adicionales que son parte de la infraestructura de ataque.

El uso de Decoy Dog en la naturaleza es «*muy raro*», con la firma DNS que coincide con menos del 0.0000027% de los 370 millones de dominios activos en Internet, según la empresa con sede en California.

Uno de los componentes principales del kit de herramientas es Pupy RAT, un troyano de código abierto que se entrega mediante un método llamado tunelización de DNS, en el que las consultas y respuestas de DNS se usan como un C2 para lanzar cargas útiles de forma sigilosa.

Cabe mencionar que el uso de Pupy RAT multiplataforma se ha relacionado con hackers de estados nacionales de China, como Earth Berberoka (también conocido como

GamblingPuppet) en el pasado, aunque no existe evidencia que sugiera la participación del atacante en la campaña.

La investigación adicional sobre Decoy Dog sugiere que la operación se había establecido al menos un año antes de su descubrimiento, con tres configuraciones de infraestructura distintas detectadas hasta la fecha.

Otro aspecto crucial es el comportamiento inusual de señalización de DNS asociado con los dominios de Decoy Dog, de modo que se adhieren a un patrón de solicitudes de DNS periódicas, pero poco frecuentes para pasar desapercibidos.

> *«Los dominios de Decoy Dog se pueden agrupar en función de sus registradores compartidos, servidores de nombres, direcciones IP y proveedores de DNS dinámicos»*, dijo Infoblox.

> *«Dadas las otras similitudes entre los dominios de Decoy Dog, esto es indicativo de que un hacker está evolucionando gradualmente en sus tácticas o que varios hackers implementan el mismo conjunto de herramientas en distintas infraestructuras».*