Una investigación más detallada de un software malicioso hallado recientemente llamado Decoy Dog ha mostrado que es una actualización importante sobre el Pupy RAT, un troyano de acceso remoto de fuente abierta del que se inspira.

> *"Decoy Dog cuenta con un paquete completo de habilidades potentes e inéditas hasta el momento, incluyendo la posibilidad de trasladar a los afectados a otro controlador, lo que les facilita mantener el contacto con los equipos vulnerados y quedarse escondidos durante extensos lapsos de tiempo. Algunos afectados han comunicado activamente con un servidor Decoy Dog durante más de un año",* afirmó Infoblox en un reporte del martes.

Otras funciones nuevas le permiten al software malicioso ejecutar código Java cualquiera en el cliente y conectarse a controladores de urgencia usando un mecanismo parecido a un algoritmo convencional de generación de dominios DNS (DGA), con los dominios Decoy Dog creados para responder a las consultas DNS repetidas desde los clientes vulnerados.

El avanzado kit de herramientas fue hallado por primera vez por la firma de seguridad cibernética a inicios de abril de 2023 tras observar una actividad inusual de balizamiento DNS, mostrando sus ataques muy enfocados contra las redes de empresas.

Los orígenes de Decoy Dog continúan sin estar claros, pero se cree que está manejado por un grupo de piratas informáticos respaldados por estados, que usan tácticas diferentes pero atienden a los pedidos entrantes que concuerdan con la estructura de la comunicación del cliente.

Decoy Dog usa el sistema de nombres de dominio (DNS) para realizar el mando y control (C2). Un extremo que está vulnerado por el software malicioso se comunica con, y recibe órdenes de, un controlador (o sea, un servidor) mediante consultas DNS y respuestas de

direcciones IP.

Los actores de la amenaza tras la operación se dice que han hecho cambios rápidos a su infraestructura de ataque en respuesta a las divulgaciones previas, desactivando algunos de los servidores de nombres DNS, así como registrando nuevos dominios de sustitución para establecer la persistencia remota.

> *"En vez de apagar su operación, el actor trasladó a los clientes vulnerados existentes a los nuevos controladores. Esta es una respuesta extraordinaria que muestra que el actor consideró necesario mantener el acceso a sus víctimas actuales",* indicó Infoblox.

La primera instalación conocida de Decoy Dog se remonta a finales de marzo o inicios de abril de 2022, después de lo cual se detectaron otros tres grupos bajo el control de distintos controladores. Hasta ahora se han detectado un total de 21 dominios Decoy Dog.

Además, un conjunto de controladores registrados desde abril de 2023 se ha adaptado incorporando una técnica de geocercado para limitar las respuestas a las direcciones IP del cliente a ciertas ubicaciones, con una actividad observada limitada a Rusia y Europa del Este.

> *"La falta de visión sobre los sistemas y vulnerabilidades subyacentes que se explotan hace que Decoy Dog sea una amenaza constante y grave. La mejor defensa contra este software malicioso es DNS",* dijo la Dra. Renée Burton, jefa de inteligencia de amenazas en Infoblox.