Un grupo de hackers iraní conocido como Oilrig, se ha convertido en el primer actor de amenazas conocido públicamente en incorporar el protocolo DNS sobre HTTPS (DoH) en sus ataques.

Vicente Díaz, analista de malware para Kaspersky, dijo en un seminario web la semana pasada que el cambio ocurrió en mayo de este año, cuando Oilrig agregó una nueva herramienta a su arsenal de piratería.

Según Díaz, los operadores de Oilrig comenzaron a usar una nueva utilidad llamada DNSExfiltrator como parte de sus intrusiones en las redes pirateadas.

DNSExfiltrator es un proyecto de código abierto disponible en GitHub que crea canales de comunicación encubiertos mediante la canalización de datos y luego ocultarlos dentro de protocolos no estándar.

La herramienta puede transferir datos entre dos puntos usando solicitudes DNS clásicas, pero también puede usar el protocolo DoH más nuevo.

Díaz dijo que Oilrig, también conocido como APT34, ha estado utilizando DNSExfiltrator para mover datos lateralmente a través de redes internas y luego exfiltrarlos a un punto externo.

Es probable que Oilrig utilice DoH como un canal de exfiltración para evitar que sus actividades sean detectadas o monitoreadas mientras mueve datos robados.

Esto se debe a que el protocolo DoH es actualmente un canal de exfiltración ideal por dos principales razones. Una es que se trata de un nuevo protocolo que no todos los productos de seguridad son capaces de monitorear. Luego, está cifrado de forma predeterminada, mientras que DNS es texto sin cifrar.

El hecho de que Oilrig fue una de las primeras APT (Amenazas Persistentes Avanzadas, un término que se usa para describir grupos de piratería respaldados por el gobierno), para desplegar DoH no es realmente una sorpresa.

Durante su historia, el grupo ha incursionado en técnicas de exfiltración basadas en DNS. Antes de adoptar el kit de herramientas DNSExfiltrator de código abierto en mayo, el grupo había estado utilizando una herramienta personalizada llamada DNSpionage desde al menos 2018, según informes de Talos, NSFOCUS y Palo Alto Networks.

En la campaña de mayo, Kaspersky dijo que Oilrig extrajo datos a través de DoH a dominios relacionados con COVID-19.

Durante el mismo mes, Reuters informó independientemente, sobre una campaña de phishing dirigida por piratas informáticos iraníes no identificados, que atacó al gigante farmacéutico Gilead, que en ese momento anunció que comenzó a trabajar en un tratamiento para el virus COVID-19. Sin embargo, no está claro si se trata de los mismos incidentes.