Un grupo de piratas informáticos con presuntos vínculos con China, han estado detrás de una amplia campaña de espionaje cibernético dirigida a organizaciones militares en el sudeste asiático durante casi dos años, según una nueva investigación.

Al atribuir los ataques a un actor de amenazas apodado como Naikon APT, la compañía de seguridad cibernética Bitdefender expuso las tácticas, técnicas y procedimientos en constante cambio adoptados por el grupo, incluida la incorporación de nuevas puertas traseras llamadas Nebulae y RainyDay en sus misiones de robo de datos. Se cree que la actividad maliciosa se llevó a cabo entre junio de 2019 y marzo de 2021.

> *«Al comienzo de la operación, los actores de la amenaza utilizaron el cargador Aria-Body y Nebulae como la primera etapa del ataque. A partir de septiembre de 2020, los actores de amenazas incluyeron la puerta trasera RainyDay en su kit de herramientas. El propósito de esta operación era el ciberespionaje y el robo de datos»,* dijeron los investigadores.

Naikon, también conocido como Override Panda, Lotus Panda o Hellsing, tiene un historial de ataques cibernéticos a entidades gubernamentales en la región de Asia-Pacífico (APAC) en busca de inteligencia geopolítica.

Aunque inicialmente se asumió que había desaparecido del radar desde que se expuso por primera vez en 2015, la evidencia surgió en el pasado mes de mayo, cuando el adversario fue visto usando una nueva puerta trasera llamada Aria-Body para irrumpir sigilosamente en las redes y aprovechar la infraestructura comprometida como un comando y control (C2) para lanzar ataques adicionales contra otras organizaciones.

La nueva ola de ataques identificada por Bitdefender empleó RainyDay como la puerta trasera principal, y los actores lo utilizaron para realizar reconocimientos, entregar cargas

útiles adicionales, realizar movimientos laterales a través de la red y exfiltrar información confidencial.

La puerta trasera se ejecutó mediante una técnica conocida como carga lateral de DLL, que se refiere al método probado y comprobado de cargar DLL maliciosas en un intento por secuestrar el flujo de ejecución de un programa legítimo como Outlook Item Finder.

Como estrategia de respaldo, el malware también instaló un segundo implante llamado Nebulae para acumular información del sistema, realizar operaciones de archivos y descargar y cargar archivos arbitrarios desde y hacia el servidor C2.

> *«La segunda puerta trasera supuestamente se utiliza como medida de precaución para no perder la persistencia en caso de que se detecten signos de infección»,* dijeron los investigadores.

Otras herramientas implementadas por la puerta trasera de RainyDay incluyen un recopilador de archivos que recoge archivos modificados recientemente con extensiones específicas y los carga en Dropbox, un recolector de credenciales y varias utilidades de red como escáneres NetBIOS y proxies.

Además, Bitdefender dijo que RainyDay es probablemente el mismo malware que Kaspersky reveló a inicios del mes, citando similitudes en la funcionalidad y el uso de la carga lateral de DLL para lograr la ejecución.

Llamada FoundCore, la puerta trasera se atribuyó a un actor de habla china llamado Cycldek como parte de una campaña de ciberespionaje dirigida contra el gobierno y las organizaciones militares en Vietnam.