Un grupo de hackers chinos fue descubierto en una campaña sostenida de espionaje cibernético dirigida a entidades gubernamentales en Australia, Indonesia, Filipinas, Vietnam, Tailandia, Mynmar y Brunei. Esta campaña ha estado activa y no se detectó durante al menos cinco años.

El grupo, llamado Naikon APT, conocido alguna vez como uno de los APT más activos en Asia hasta 2015, llevó a cabo una serie de ataques cibernéticos en la región Asia-Pacífico (APAC) en busca de inteligencia geopolíticia.

Según el último informe de los investigadores de Check Point, el grupo APT de Naikon estuvo trabajando los últimos 5 años en silencio, utilizando una puerta trasera llamada Aria-body para operar sigilosamente.

> *«Dadas las características de las víctimas y las capacidades presentadas por el grupo, es evidente que el propósito del grupo es reunir inteligencia y espiar a los países a los que se dirige»,* dijeron los investigadores.

En resumen, la backdoor de Aria-body se está utilizando para tomar el control de las redes internas de una organización objetivo, además de los ataques crecientes de una compañía ya violada para infectar a otra.

> *«Esto incluye no solo localizar y recopilar documentos específicos de computadoras y redes infectadas dentro de los departamentos del gobierno, sino también extraer unidades de datos extraíbles, tomar capturas de pantalla y registro de teclas, además de recolectar los datos robados para espionaje».*

Campaña de inteligencia geopolítica

Documentado por primera vez en 2015, el grupo Naikon APT utiliza señuelos de correo electrónico diseñados como un vector de ataque inicial contra agencias gubernamentales de alto nivel y organizaciones civiles y militares, que, al abrirse, instalaron software espía que filtraba documentos confidenciales para servidores de control y mando remotos (C2).

Aunque no se han informado nuevos signos de actividad desde entonces, la última investigación de Check Point proyecta sus operaciones con una nueva perspectiva.

> *«Naikon intentó atacar a uno de nuestros clientes haciéndose pasar por un gobierno extranjero, fue cuando volvieron a nuestro radar luego de una ausencia de cinco años, y decidimos investigar más»,* dijo Lotem Finkelsteen, gerente de inteligencia de amenazas en Check Point.

No solo se emplearon múltiples cadenas de infección para entregar la puerta trasera de Aria-boy, sino que los corres electrónicos maliciosos también contenían un archivo RTF denominado The Indians Way.doc, que estaba infectado con un generador de exploits llamado RoyalBlood, que generó un cargador (intel.wll) en la carpeta de inicio de Microsoft Word del sistema («%APPDATA%\Microsoft\Word\STARTUP»).

RoyalBlood es un armador RTF compartido inicialmente entre los actores de amenazas chinos. Cabe mencionar que se ha detectado una forma de operar similar en una campaña contra las agencias gubernamentales de Mongolia, llamada Vicious Panda, que se descubrió explotando el brote de coronavirus en curso para plantar malware por medio de trucos de ingeniería social.

En un mecanismo de infección separado, los archivos de almacenamiento se empaquetaron con un ejecutable legítimo (como Outlook y Avast Proxy), y una biblioteca maliciosa para

colocar el cargador en el sistema de destino.

Independientemente del método para obtener un punto de apoyo inicial, el cargador estableció una conexión con un servidor C2 para descargar la carga útil de la backdoor Aria-body de la siguiente etapa.

> *«Luego de obtener el dominio C&C, el cargador lo contacta para descargar la siguiente y última etapa de la cadena de infección. Aunque parezca simple, los atacantes operan el servidor de C&C en una ventana diaria limitada, conectándose en línea solo durante unas pocas horas cada día, lo que dificulta el acceso a las partes avanzadas de la cadena de infección»*, agregaron los investigadores.

El RAT Aria-body, llamado así en base al nombre *«aria-body-dllX86.dll»*, dado por los autores del malware, cuenta con todas las características que se esperan de una puerta trasera típica: crear y eliminar archivos y directorios, tomar capturas de pantalla, buscar archivos, recopilar metadatos de archivos, recopilar información del sistema y la ubicación, entre otros.

Algunas variaciones recientes de Aria-body también están equipadas con capacidades para capturar pulsaciones de teclas e incluso cargar otras extensiones, según los investigadores, lo que sugiere que la backdoor está en desarrollo activo.

Además de filtrar los datos recopilados al servidor C2, la puerta trasera escucha cualquier comando adicional que se ejecute. Un análisis posterior de la infraestructura C2 descubrió que se utilizaron varios dominios durante largos períodos de tiempo, con la misma dirección IP reutilizada con más de un dominio.

Con todas estas tácticas avanzadas, los hackers lograron comprometer y utilizar servidores dentro de los ministerios infectados como servidores C2 para lanzar ataques y retransmitir y enrutar los datos robados, en lugar de la detección de riesgos al acceder a los servidores remotos.

Mientras tanto, Check Point atribuyó la campaña a Naikon APT, basándose en similitudes de código en Aria-body y la herramienta de espionaje detallada por Kaspersky *«XSControl»* en 2015, así como el uso de dominios C2 (mopo3[.]net), que se resuelven en la misma dirección IP que los dominios mencionados por este último.

> *«Si bien el grupo Naikon APT se ha mantenido fuera del radar durante los últimos cinco años, parece que no han estado inactivos. De hecho, es todo lo contrario. Al utilizar una nueva infraestructura de servidor, variantes de cargador en constante cambio, carga sin archivos en memoria, así como una nueva puerta trasera, el grupo APT de Naikon pudo evitar que los analistas rastrearan su actividad hacia ellos»,* concluyeron los investigadores.