Organizaciones en Taiwán y una ONG estadounidense con sede en China han sido blanco de un grupo de hackers patrocinado por el estado chino llamado Daggerfly, que ha utilizado un conjunto de herramientas de malware mejoradas.

La campaña indica que el grupo *«también participa en espionaje interno»*, según informó el equipo de Threat Hunter de Symantec, parte de Broadcom, en un nuevo informe publicado hoy. *«En el ataque a esta organización, los atacantes aprovecharon una vulnerabilidad en un servidor HTTP Apache para instalar su malware MgBot.»*

Daggerfly, también conocido como Bronze Highland y Evasive Panda, había sido previamente observado utilizando el marco de malware modular MgBot en una misión de recolección de inteligencia dirigida a proveedores de telecomunicaciones en África. Se sabe que ha estado operando desde 2012.

> *«Daggerfly parece capaz de adaptarse rápidamente a la exposición actualizando su conjunto de herramientas para continuar sus actividades de espionaje con mínima interrupción»,* señaló la compañía.

El último conjunto de ataques se caracteriza por el uso de una nueva familia de malware basada en MgBot, así como una versión mejorada de un malware conocido para macOS llamado MACMA, que fue revelado por primera vez por el Grupo de Análisis de Amenazas (TAG) de Google en noviembre de 2021. Este malware se distribuía a través de ataques de watering hole dirigidos a usuarios de Internet en Hong Kong, explotando fallos de seguridad en el navegador Safari.

Este desarrollo marca la primera vez que esta cepa de malware, capaz de recolectar información sensible y ejecutar comandos arbitrarios, ha sido explícitamente vinculada a un grupo de hackers específico.

> *«Los actores detrás de macOS.MACMA al menos estaban reutilizando código de*

> *desarrolladores de ELF/Android y posiblemente también podrían haber estado apuntando a teléfonos Android con malware,»* mencionó SentinelOne en un análisis posterior.

Las conexiones de MACMA con Daggerfly también se derivan de superposiciones de código fuente entre el malware y MgBot, y del hecho de que se conecta a un servidor de comando y control (C2) (103.243.212[.]98) que también ha sido utilizado por un dropper de MgBot.

Otro nuevo malware en su arsenal es Nightdoor (también conocido como NetMM y Suzafk), un implante que utiliza la API de Google Drive para C2 y ha sido utilizado en ataques de watering hole dirigidos a usuarios tibetanos desde al menos septiembre de 2023. Los detalles de esta actividad fueron documentados por primera vez por ESET en marzo de este año.

> *«El grupo puede crear versiones de sus herramientas dirigidas a la mayoría de las plataformas de sistemas operativos principales»,* dijo Symantec, agregando que ha *«visto evidencia de la capacidad de troyanizar APKs de Android, herramientas de interceptación de SMS, herramientas de interceptación de solicitudes DNS e incluso familias de malware dirigidas al sistema operativo Solaris.»*

Este desarrollo se produce cuando el Centro Nacional de Respuesta a Emergencias de Virus Informáticos de China (CVERC) afirmó que Volt Typhoon –atribuido por las naciones de Five Eyes como un grupo de espionaje vinculado a China– es una invención de las agencias de inteligencia de EE. UU., describiéndolo como una campaña de desinformación.

> *«Aunque sus principales objetivos son el Congreso de EE. UU. y el pueblo estadounidense, también intenta difamar a China, sembrar discordia entre China y otros países, contener el desarrollo de China y robar a las empresas chinas»*, afirmó el CVERC en un informe reciente.