Un grupo de hackers de ransomware ruso apuntó a una entidad no identificada en el sector del juego en Europa y América Central, al reutilizar herramientas personalizadas desarrolladas por otros grupos APT como MuddyWater de Irán, según una nueva investigación.

Esta inusual cadena de ataque involucró el abuso de credenciales robadas para obtener acceso no autorizado a la red de la víctima, lo que finalmente condujo al despliegue de cargas útiles de Cobalt Strike en activos comprometidos, dijeron Felipe Duarte e Ido Naor, investigadores de la compañía israelí de respuesta a incidentes Security Joes, en un informe publicado la semana pasada.

Aunque la infección se contuvo en esta etapa, los investigadores caracterizaron el compromiso como un caso de sospecha de ataque de ransomware.

Se cree que la intrusión tuvo lugar en febrero de 2022, y los atacantes utilizaron herramientas posteriores a la explotación como ADFind, NetScan, SoftPerfect y LaZagne. También se utilizó un ejecutable AccountResource para obtener credenciales de administrador por fuerza bruta y una versión bifurcada de una herramienta de tunelización inversa llamada Ligolo.

Llamada Sockbot, la variante modificada es un binario de Golang que está diseñado para exponer los activos internos de una red comprometida a Internet de forma sigilosa y segura. Los cambios realizados en el malware eliminan la necesidad de utilizar parámetros de línea de comandos e incluyen varias comprobaciones de ejecución para evitar la ejecución de varias instancias.

Debido a que Ligolo es una herramienta principal elegida por el grupo de estado-nación iraní MuddyWater, el uso de una bifurcación de Ligolo ha planteado la posibilidad de que los atacantes estén tomando herramientas utilizadas por otros grupos e incorporando sus propias firmas en un probable intento de confundir la atribución.

Los enlaces a un grupo de ransomware de habla rusa provienen de superposiciones de

artefactos con kits de herramientas de ransomware comunes. Además, uno de los archivos binarios implementados (AccountResource) contiene referencias codificadas en ruso.

> *«La estrategia utilizada por los actores de amenazas para acceder y pivotar sobre la infraestructura de la víctima nos permite ver un enemigo persistente y sofisticado con algunas habilidades de programación, experiencia en equipos rojos y un objetivo claro en mente, que está lejos del perfil habitual de script kiddie»,* dijeron los investigadores.

> *«El hecho de que el punto de entrada de esta intrusión fuera un conjunto de credenciales comprometidas reafirma la importancia de aplicar controles de acceso adicionales para todos los diferentes activos de cualquier organización»,* agregaron.