TrickBot, la solución Crimeware-as-a-Service (CaaS) de windows, que es utilizada por una variedad de grupos de hackers para entregar cargas útiles de próxima etapa como ransomware, parece estar experimentando una especie de transición, sin que se registre ninguna actividad nueva desde el principio del año.

La pausa en las campañas de malware se debe *«parcialmente a un gran cambio de los operadores de TrickBot, incluido el trabajo con los operadores de Emotet»,* dijeron investigadores de Intel 471 en un informe.

El último conjunto de ataques que involucró a TrickBot se registró el 28 de diciembre de 2021, incluso cuando la infraestructura de comando y control (C2) asociada con el malware siguió brindando complementos adicionales e inyecciones web a los nodos infectados en la red de bots.

La disminución en el volumen de las campañas también estuvo acompañada por la estrecha colaboración de TrickBot con los operadores de Emotet, que experimentó un resurgimiento a fines del año pasado luego de una pausa de 10 meses después de los esfuerzos de las fuerzas del orden para abordar el malware.

Los ataques, que se observaron por primera vez en noviembre de 2021, presentaban una secuencia de infección que usaba TrickBot como conducto para descargar y ejecutar binarios de Emotet, cuando antes del desmantelamiento, Emotet se usaba generalmente para lanzar muestras de TrickBot.

> *«Es probable que los operadores de TrickBot hayan eliminado gradualmente el malware TrickBot de sus operaciones a favor de otras plataformas, como Emotet. TrickBot, después de todo, es un malware relativamente antiguo que no se ha actualizado de forma importante»,* dijeron los investigadores.

Además, Intel 471 dijo que observó casos en los que TrikBot envió instalaciones de Qbot a los sistemas comprometidos poco después del regreso de Emotet en noviembre de 2021, lo que

una vez más planteó la posibilidad de una reorganización detrás de escena para migrar a otras plataformas.

Con TrickBot cada vez más bajo la lente de las fuerzas del orden en 2021, quizás no sea demasiado sorprendente que el atacante detrás de él esté intentando activamente cambiar de táctica y actualizar sus medidas defensivas.

Según un informe separado publicado por Advanced Intelligence (AdvIntel) la semana pasada, se cree que el cártel de ransomware Conti, adquirió a varios desarrolladores de élite de TrickBot para retirar el malware a favor de herramientas mejoradas como BazarBackdoor.

> *«Quizás una combinación de atención no deseada a TrickBot y la disponibilidad de plataformas de malware más nuevas y mejoradas ha convencido a los operadores de TrickBot para que lo abandonen. Sospechamos que la infraestructura de control de malware (C2) se mantiene porque aún hay algo de valor de monetización en los bots restantes»,* dijeron los investigadores.