Los operadores detrás del malware TrickBot han resurgido con nuevos trucos que tienen como objetivo aumentar su presencia mediante la expansión de sus canales de distribución, lo que en última instancia conduce al despliegue de ransomware como Conti.

Se ha descubierto que el actor de amenazas, al que se le asignaron los nombres ITG23 o Wizard Spider, se asocia con otras bandas de ciberdelincuencia conocidas como Hive0105, Hive0106 (también conocido como TA551 o Shathak), y Hive0107, lo que se suma a un número creciente de campañas en las que los atacantes están apostando por entregar malware propietario, según un informe de IBM X-Force.

> *«Estos y otros proveedores de delitos informáticos están infectando a redes corporativas con malware mediante el secuestro de hilos de correo electrónico, utilizando los formularios de respuesta falsa de los clientes y empleados de ingeniería social con un centro de llamada falsa conocida como BazaCall»*, dijeron los investigadores Ole Villadsen y Charlotte Hammond.

Desde que surgió en el panorama de las amenazas en 2016, TrickBot ha evolucionado de un troyano bancario a una solución de crimeware modular basada en Windows, mientras que también se destaca por su capacidad de recuperación, demostrando la capacidad de mantener y actualizar su conjunto de herramientas e infraestructura a pesar de los múltiples esfuerzos de las autoridades y grupos de industria para elimminarlo. Además de TrickBot, al grupo Wizard Spider se le atribuye el desarrollo de BazaLoader y una puerta trasera llamada Anchor.

Aunque los ataques montados a inicios del año se basaron en campañas de correo electrónico que entregaban documentos de Excel y una treta del centro de llamadas denominada *«BazaCall»* para entregar malware a los usuarios corporativos, las intrusiones recientes que comenzaron alrededor de junio de 2021 se caracterizaron por una asociación con dos afiliados de delitos cibernéticos para aumentar su infraestructura de distribución aprovechando los hilos de correo electrónico secuestrados y los formularios de consulta de clientes de sitios web fraudulentos en los sitios web de la organización para implementar

cargas útiles de Cobalt Strike.

> *«Este movimiento no solo aumentó el volumen de sus intentos de entrega, sino que también diversificó los métodos de entrega con el objetivo de infectar a más víctimas potenciales que nunca»,* dijeron los investigadores.

En una cadena de infección observada por IBM a finales de agosto de 2021, se dice que el afiliado de Hive0107 adoptó una nueva técnica que consiste en enviar mensajes de correo electrónico a las empresas objetivo informando que sus sitios web han estado realizando ataques distribuidos de denegación de servicio (DDoS) en sus servidores, instando a los destinatarios a hacer clic en un enlace para obtener pruebas adicionales. Una vez que se hace clic, el enlace descarga un archivo ZIP que contiene un descargador de JavaScript malicioso, que a su vez, se pone en contacto con una URL remota para buscar el malware BazaLoader y soltar Cobalt Strike y TrickBot.

> *«ITG23 también se ha adoptado a la economía del ransomware mediante la creación del ransomware como servicio (RaaS) de Conti y el uso de sus cargas útiles BazaLoader y TrickBot para hacerse un hueco en los ataques de ransomware. Este último desarrollo demuestra la fuerza de sus conexiones dentro del ecosistema ciberdelincuente y s*u capacidad para aprovechar estas relaciones para expandir el número de organizaciones infectadas con su malware», agregaron los investigadores.