Los operadores del troyano TrickBot están colaborando con el grupo de amenazas Shathak para distribuir sus productos, lo que finalmente lleva al despliegue del ransomware Conti en las máquinas infectadas.

> *«La implementación de TrickBot ha evolucionado a lo largo de los años, con las últimas versiones de software malicioso TrickBot que implementa capacidades de carga. TrickBot ha jugado un papel importante en muchas campañas de ataque realizadas por diferentes actores de amenazas, desde ciberdelincuentes comunes hasta actores del estado-nación»,* dijeron los analistas de seguridad de Cybereason Aleksandar Milenkoski y Eli Salem.

El último informe se basa en un documento de IBM X-Force del mes pasado, que reveló las asociaciones de TrickBot con otras bandas de delitos cibernéticos, incluyendo Shathak, para entregar malware patentado.

Shathak, que también se encuentra bajo el nombre de TA551, es un sofisticado actor de ciberdelincuencia dirigido a usuarios finales a escala global, que actúa como distribuidor de malware aprovechando los archivos ZIP protegidos con contraseña que contienen documentos de Office habilitados para macros.

La banda TrickBot, conocida como ITG23 o Wizard Spider, también es responsable de desarrollar y mantener el ransomware Conti, además de arrendar el acceso al software malicioso a los afiliados a través de un modelo de ransomware como servicio (RaaS).

Las cadenas de infección que involucran a Shathak generalmente implican el envío de correos electrónicos de phishing que vienen incrustados con documentos de Word con malware que, en última instancia, conducen a la implementación del malware TrickBot o BazarBackdoor, que luego se usa como un conducto para implementar balizas Cobalt Strike,

así como el ransomware, pero no antes de realizar actividades de reconocimiento, movimiento lateral, robo de credenciales y exfiltración de datos.

Los investigadores de Cybereason dijeron que observaron un tiempo promedio de rescate (TTR) de dos días después de los compromisos, lo que indica la cantidad de tiempo desde que el actor de la amenaza obtiene acceso inicial a una red hasta el momento en que el actor de la amenaza realmente implementa el ransomware.

Los hallazgos también se producen cuando la Agencia de Seguridad de Infraestructura y Ciberseguridad de Estados Unidos (CISA) y la Oficina Federal de Investigaciones (FBI) informaron que se habían producido no menos de 400 ataques de ransomware Conti dirigidos a organizaciones estadounidenses e internacionales a partir de septiembre de 2021.

Para proteger los sistemas contra el ransomware Conti, las agencias recomiendan aplicar una variedad de medidas de mitigación, que incluyen *«requerir autenticación multifactor (MFA), implementar la segmentación de red y mantener actualizados los sistemas operativos y el software».*