El Departamento de Estado de Estados Unidos anunció el jueves una recompensa de 10 millones de dólares por información relacionada con cinco personas asociadas al grupo de ransomware Conti.

La oferta de recompensa, reportada por primera vez por WIRED, también se destaca por el hecho de que marca la primera vez que se desenmascara el rostro de un asociado de Conti, conocido como *«Target»*. Los otros cuatro asociados fueron referidos como *«Tramp», «Dandis», «Professor» y «Reshaev»*.

El gobierno, además de buscar información sobre los cinco operadores que podrían conducir a su identificación o ubicación, también hace un llamado a las personas para que compartan detalles acerca de Conti y sus grupos afiliados TrickBot y Wizard Spider.

Desde su cambio de marca de Ryuk a Conti, el grupo de ciberdelincuentes transnacional se ha relacionado con cientos de incidentes de ransomware en los últimos dos años.

A partir de enero de 2022, se estima que la operación de ransomware como servicio (RaaS) con sede en Rusia ha afectado a más de 1000 entidades, con pagos a las víctimas que superan los 150 millones de dólares. El Departamento de Estado calificó a Conti como *«la cepa de ransomware más dañina jamás documentada».*

Un análisis de los chats filtrados entre miembros de Conti en marzo de 2022 que surgieron luego de que el sindicato se pusiera del lado de Rusia en el conflicto en curso entre el país y Ucrania, destacó el papel de Target como gerente involucrado en sus operaciones físicas en Rusia.

> *«Las filtraciones so de un nivel sin precedentes y muestran al mundo cómo opera una banda de ransomware multimillonaria respaldada por el gobierno»,* dijeron los investigadores de Trellix en marzo de 2022.

> *«De alguna forma, era casi como un negocio normal; era necesario pagar los salarios, obtener las licencias de software, iniciar el servicio al cliente y formar alianzas estratégicas».*

Aunque la marca Conti fue cancelada, sus miembros aún están activos y siguen su trabajo a través de otras operaciones de extorsión de datos y ransomware bajo distintas ramificaciones, incluyendo Karakurt, Silent Ransom, Quantum y Roy/Zeon.

El desarrollo también se produce poco más de tres meses después de que la agencia dijera que ofrecería una recompensa de hasta 10 millones de dólares por información que conduzca a la identificación y/o ubicación de personas que ocupan puestos clave de liderazgo en el equipo de Conti.