Estados Unidos recupera 2.3 mdd de rescate pagado a hackers de Colonial Pipeline

Autor: I. Stepanenko

Fecha: Tuesday 15th of June 2021 07:51:17 PM

El Departamento de Justicia de Estados Unidos dijo este lunes que recuperó 63.7 Bitcoins (valorados actualmente en unos 2.3 millones de dólares), pagados por Colonial Pipeline a los extorsionadores del ransomware DarkSide el pasado 8 de mayo, de conformidad con una orden de incautación autorizada por el Distrito Norte de California.

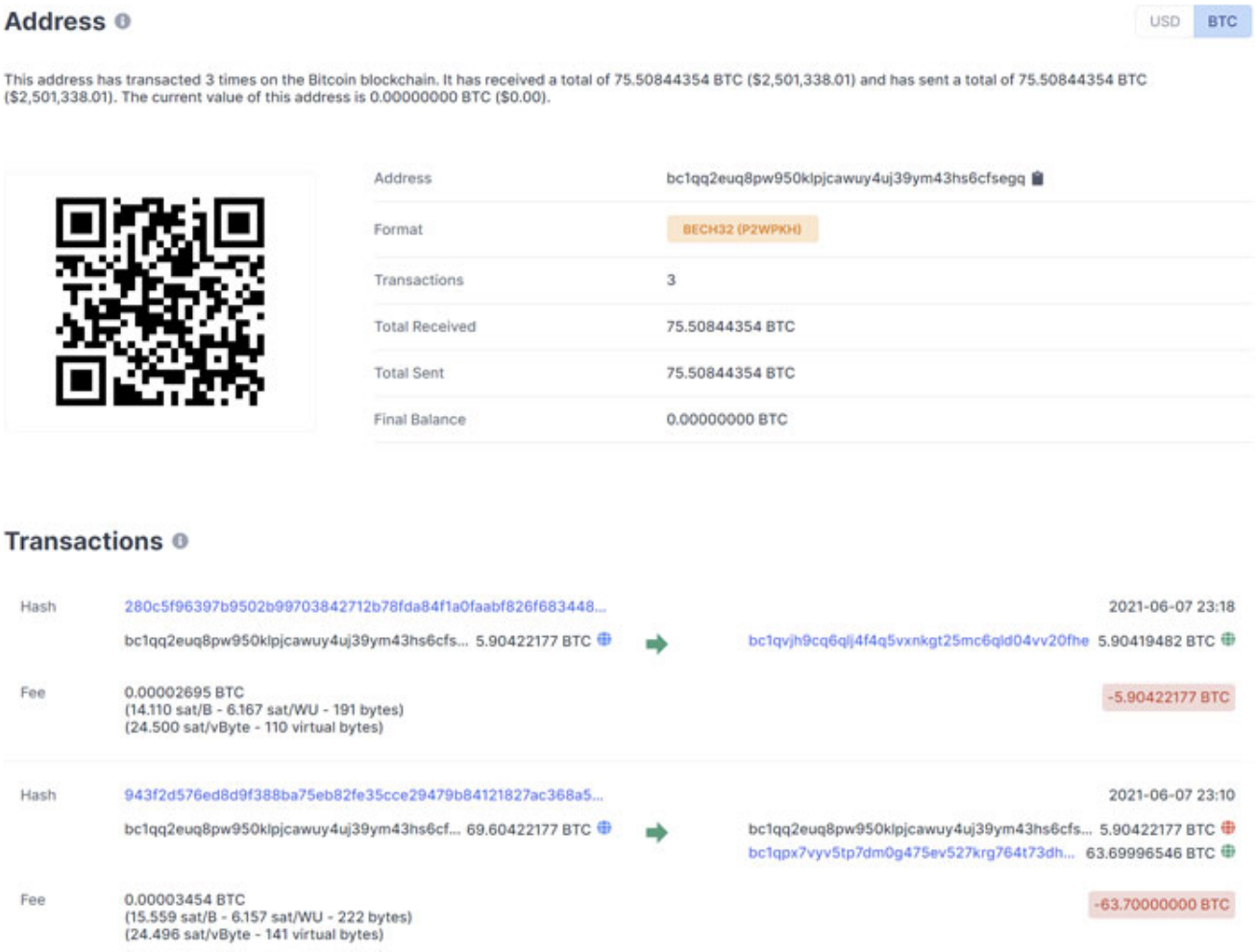
El ataque de ransomware también obstaculizó el suministro de combustible de la compañía del gasoducto, lo que llevó al gobierno a emitir una declaración de emergencia, incluso cuando la compañía desembolsó la cantidad de rescate de aproximadamente 75 bitcoins, equivalentes a aproximadamente 4.4 millones de dólares, para recuperar el acceso a sus sistemas.

Una semana después del incidente que fue duramente publicitado, el sindicato de ransomware como servicio se disolvió con un mensaje de despedida el 14 de mayo a los afiliados, afirmando que sus servidores de Internet y la billetera de criptomonedas fueron confiscados por entidades policiales desconocidas.

Aunque el anuncio de DarkSide se percibió como una estafa de salida, el último movimiento del Departamento de Justicia confirma las especulaciones sobre la participación de las

fuerzas del orden.

Al asegurar que *«los pagos de rescate son el combustible que impulsa el motor de extorsión digital»*, el Departamento de Justicia dijo que siguió los rastros del dinero dejados por el grupo DarkSide hasta una dirección específica de bitcoin al revisar el libro de contabilidad público de Bitcoin, al que se destinaron las ganancias del pago del rescate utilizando la «clave privada» que el FBI tenía en su poder para acceder a los activos criptográficos almacenados en la billetera.



«No hay lugar más allá del alcance del FBI para ocultar fondos ilícitos que nos

> impedirán imponer riesgos y consecuencias a los ciber actores maliciosos. Continuaremos utilizando todos nuestros recursos disponibles y aprovecharemos nuestras asociaciones nacionales e internacionales para interrumpir los ataques de ransomware y proteger a nuestros socios del sector privado y al público estadounidense», dijo el subdirector del FBI, Paul Abbate.

Aún no está claro cómo la agencia de inteligencia llegó a tener en su poder la clave privada, pero DarkSide había informado antes que perdió el acceso a uno de sus servidores de pago.

La compañía de análisis blockchain Elliptic, que identificó la transacción de bitcoin que representa el pago de rescate de Colonial Pipeline, dijo que los bitcoins incautados representan el 85% del monto total del rescate, que generalmente se reserva para los afiliados, y el resto se destina a los desarrolladores de DarkSide. La dirección de Bitcoin se vació alrededor de la 1:40 pm ET del lunes, dijo el Dr. Tom Robinson, cofundador de Elliptic.

> «Hacer responsables a los ciberdelincuentes y alterar el ecosistema que les permite operar es la mejor forma de disuadir y defenderse de futuros ataques de esta naturaleza. El sector privado también tiene un papel igualmente importante que desempeñar y debemos seguir tomando en serio las amenazas cibernéticas e invertir en consecuencia para fortalecer nuestras defensas», dijo el director ejecutivo de Colonial Pipeline, Joseph Blount.