Una coalición de organismos encargados de hacer cumplir la ley en Europa y Estados Unidos, anunció el desmantelamiento de ChipMixer, un mezclador de criptomonedas sin licencia que comenzó a operar en agosto de 2017.

> *«El software ChipMixer bloqueó el rastro de blockchain de los fondos, haciéndolo atractivo para los ciberdelincuentes que buscan lavar ganancias ilegales de actividades delictivas como el tráfico de drogas, tráfico de armas, los ataques de ransomware y el fraude con tarjetas de pago»,* dijo Europol en un comunicado.

El ejercicio coordinado, además de desmantelar los sitios web clearnet y dark web asociados con ChipMixer, también resultó en la incautación de 47.5 millones de dólares en Bitcoin y 7 TB de datos.

Los mezcladores, también llamados tumblers, ofrecen anonimato completo por una tarifa al mezclar criptomonedas de distintos usuarios, tanto fondos legítimos como derivados de delitos, de una forma que dificulta rastrear los orígenes.

Esto se logra canalizando distintos pagos en un solo fondo antes de dividir cada monto y transmitirlos a los destinatarios designados, convirtiéndolo así en una opción atractiva para los delincuentes que buscan cobrar e intercambiar el dinero contaminado por moneda fiduciaria.

Según un informe de Chainalysis de enero de 2023, *«los mezcladores procesaron un total de 7800 millones de dólares en 2022, el 24% de los cuales provino de direcciones ilícitas y la gran mayoría del valor ilícito procesado por los mezcladores se compone de fondos robados, la mayoría de los cuales fueron robados por hackers vinculados a Corea del Norte».*

Se estima que ChipMixer, el servicio de mezclador de criptografía centralizado más grande del mundo, blanqueó archivos digitales por valor de no menos de 3750 millones de dólares (152,000 BTC) para impulsar una amplia gama de esquemas delictivos.

La compañía de análisis de blockchain Elliptic, dijo que ChipMixer se ha utilizado para lavar más de 844 millones de dólares en bitcoin que pueden vincularse directamente con actividades delictivas.

> *«ChipMixer fue uno de una variedad de mezcladores usados para lavar las ganancias de los hackeos realizados por Lazarus Group de Corea del Norte»,* dijo el cofundador y científico jefe de Elliptic, Tom Robinson.

Esto comprende el robo de KuCoin en septiembre de 2020, así como los hackeos de Axie Infinity Ronin Bridge y Harmony Horizon Bridge que tuvieron lugar el año pasado.

Group Lazarus está lejos de ser el único cliente malicioso que utilizó el servicio para ofuscar las pistas financieras. Los otros hackers consisten en equipos de ransomware como LockBit, Sodinokibi (también conocido como REvil), Zeppelin, Mamba, Dharma y SunCrypt.

Además, se dice que ChipMixer atrajo más de 200 millones de dólares en Bitcoin vinculados a compras originadas en los mercados de la red oscura, incluyendo 60 millones de dólares de clientes de la ya desparecida Hydra.

La plataforma mezcladora, según el Departamento de Justicia de Estados Unidos (DoJ), también procesó la criptomoneda usada por el grupo de hacking APT28 vinculado a Rusia (también conocido como Fancy Bear o Strontium) para adquirir la infraestructura empleada en relación con un malware llamado Drovorub.

Coincidiendo con la represión, el Departamento de Justicia acusó además a un ciudadano vietnamita de 49 años, Minh Quốc Nguyễn, por su papel en la creación y el funcionamiento de la infraestructura en línea ChipMixer y la publicidad de sus servicios.

> *«ChipMixer facilitó el lavado de criptomonedas, específicamente Bitcoin, a gran escala internacional, instigando a actores nefastos y delincuentes de todo tipo para*

> *evadir la detección»,* dijo la fiscal federal Jacqueline C. Romero.

> *«Plataformas como ChipMixer, que están diseñadas para ocultar las fuentes y destinos de cantidades asombrosas de ganancias criminales, socavan la confianza del público en las criptomonedas y la tecnología blockchain».*

El desarrollo es el último de una serie de acciones de cumplimiento de la ley emprendidas por los gobiernos de todo el mundo para abordar el delito cibernético, y se produce semanas después de que se iniciaran los *«procedimientos penales»* contra los presuntos miembros principales de la banda de ransomware DoppelPaymer.

ChipMixer es también el cuarto servicio mezclador en ser prohibido en los últimos años después de la interrupción de Bestmixer, Blender y Tornado Cash, los dos últimos de los cuales fueron sancionados por el Departamento del Tesoro de Estados Unidos el año pasado por instigar a Lazarus Group y otros hackers en el lavado de dinero mal habido.