



## El ransomware Sodinokibi cambió el Bitcoin por Monero para el pago de los rescates

Una pieza de ransomware que cifra los datos de la víctima y solicita un rescate para restaurar el acceso a ellos, cambió de Bitcoin a Monero como criptomoneda de pago para el rescate, con el fin de proteger mejor la identidad de los hackers.

Según un informe del 11 de abril de [BleepingComputer](#), utilizar Monero hará que sea más difícil para las fuerzas del orden rastrear los pagos de rescate a los piratas informáticos detrás de Sodinokibi. Como menciona el artículo, el analista de estrategia de Europol, Jerek Jakubcek, explicó durante un seminario web de febrero cómo los anoncoins influyen en las investigaciones legales:

*«Debido a que el sospechoso utilizó una combinación de TOR y monedas de privacidad, no pudimos rastrear los fondos. No pudimos rastrear las direcciones IP. Lo que significa que llegamos al final del cambio. Lo que sucedió en la cadena de bloques de Bitcoin fue visible y es por eso que pudimos llegar razonablemente lejos. Pero con la cadena de bloques de Monero, ese fue el punto donde terminó la investigación. Así que este es un ejemplo clásico de uno de varios casos que tuvimos donde el sospechoso decidió mover fondos de Bitcoin o Ethereum a Monero».*

Según el informe, los hackers detrás del ransomware Sodinokibi publicaron en un foro de hackers y malware un post anunciando su cambio a Monero. En la publicación, los piratas informáticos declararon explícitamente que el cambio estaba destinado a dificultar que la policía rastreara el dinero.

*«En este sentido, le informamos que después de un tiempo se eliminará el BTC como método de pago. Las víctimas deben comenzar a comprender la nueva criptomoneda, así como a otras partes interesadas que trabajan con nosotros», dice el anuncio.*



## El ransomware Sodinokibi cambió el Bitcoin por Monero para el pago de los rescates

El sitio web de pago de Sodinokibi ya pide a las personas dejar de pagar con Bitcoin al aumentar el precio de la criptomoneda en un 10% con en comparación con el precio de Monero. De forma curiosa, el grupo también busca socios que puedan recuperar el acceso a los datos para los usuarios con un descuento para que puedan agregarle un recargo.

El analista de amenazas de la firma de seguridad cibernética Emsisoft, Brett Callow, dijo a Cointelegraph que el uso de anoncoin para el pago de rescate de ransomware es menos común de lo que muchos esperarían. También dijo que no se sorprendería si otros grupos de ransomware siguieran su ejemplo.

*«Si bien hay algunos casos de demandas en monedas alternativas, esa será la primera vez que un grupo importante de ransomware se haya asentado en una moneda que no sea Bitcoin. Al igual que otras empresas, las empresas criminales adoptan estrategias que han demostrado que funcionan y, en consecuencia, si este cambio resulta exitoso para REvil, esperaríamos ver a otros grupos comenzar a experimentar con demandas en monedas distintas a Bitcoin».*