We’ve been monitoring the Coinbase account activity of a target we know to be involved in writing and distributing ransomware throughout the internet.

An internal source has told us that they usually use a ‘bitcoin tumbler’ service to hide their activities however they’ve stopped doing this now, making it much easier for us to connect the illicit transactions to a particular individual.

Our target recently released a new wave of ransomware under an alias we know to be attributed to past attacks.

The analysis team found that the ransomware demands a peculiarly specific sum of 3.581074451254057 bitcoins exactly. We know that the writer of the virus is highly likely to have selected this figure on 1st February 2020.

We have reason to believe that this particular malware writer always uses the Market Open price as their point of reference (i.e. the price of one bitcoin at the very first moment of every day).

We also know that they use Yahoo Finance to lookup price information for bitcoin.

It is not uncommon for cyber criminals to arrive at a specific amount of cryptocurrency from an arbitrary figure from their home currency. E.g. 10,000 British Pounds might get 1.34745439576493 bitcoins.

For instance, if someone based in the UK wanted £5000 worth of bitcoin at a time where 1 bitcoin costs £20,000, then they would end up with 0.25 bitcoins. They didn’t choose 0.25 bitcoins, its just what they got for the £5000 at the time.

Although someone in Sweden may need to spend 61,223 units of their currency, Swedish Kronas, to get the same 0.25 bitcoins at the same time.

... Think, which is easier to write - £10,000 or £9,965.31? It would be easier to say that someone asking for 1.34745439576493 is from the UK if converting this to British Pounds gives exactly £10,000 yet $13,548.78, €11,432 and so on. It just seems too specific, and it probably is.

We feel we know where our target is based, but we need you to confirm this to help us build up evidence to arrest and prosecute.

Based on the 3.581074451254057 BTC figure being obtained on 1st Feb 2020 from the Market Open price alone, which COUNTRY is the ransomware creator most likely to be from?

We’ve attached a link to a HTML document containing links to all of the relevant bitcoin price pair history data-sets on Yahoo Finance.

<https://drive.google.com/file/d/146PaCOYd4Pma1RJqPupmcmZv-SVveEkm/view?usp=drivesdk>