Measuring Darknet Vendors Revenue Using Bitcoin Multisig Feature

Degree programme: BSc in Computer Science | Specialisation: IT-Security
Thesis advisor: Prof. Dr. Emmanuel Benoist
Expert: Daniel Voisard (BAKOM)

Darknet markets, or darkmarkets, raise many questions around themselves. What products are sold? In what quantity? Who are the vendors? What is their revenue? This last question is still outstanding. Many approximate answers were given but no exact one. The objective of our thesis is to prove the involvement of a vendor or a darkmarket in Bitcoin transactions and thus compute their turnover.

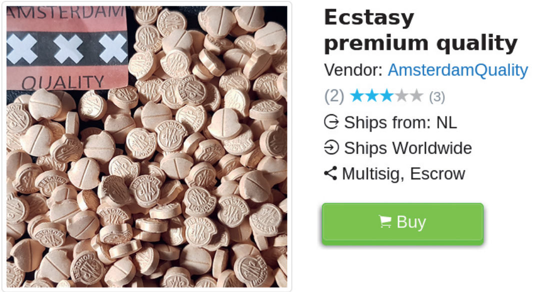
Darknet, Trust And Multisig

A customer buys cocaine on a darkmarket and pays his order in Bitcoins. But the vendor never delivers the product. Due to the illegal aspect of the purchase, he has no legal basis to claim a refund. A strong trust relationship is therefore needed between the buyer and the seller.

A solution used by some darkmarkets for solving this problem is the multisignature feature, or multisig, implemented in the Bitcoin protocol. In this method, the buyer, the seller and the market create a multisig address, where the consumer has to deposit the right amount of Bitcoins. In order to transfer the payment from this address to another address, the release transaction needs to be signed by two out of the three parties, hence the term multisignature. This means, none of them can release the payement without the agreement of another participant. In case of conflict, the client can refund the payment with the approval of the darkmarket.

Multisig Traceability

The underlying principle of Bitcoin multisig is asymmetric cryptography. Indeed, the multisig address is generated with a public key from each of the participants and the release transaction is signed with their respective private keys. Because the Bitcoin blockchain is a public ledger, every public key involved in this scheme is stored on the blockchain and is thus accessible to everyone. In other words, a public key known to belong to a vendor means a transaction involved with this key also involves the vendor himself. Normally, the keys used for multisig should be used only one time. However, we have proven that such keys were used more than once. In addition, we were able to link some of these keys to darkmarket vendors, meaning we can trace their transactions whenever they use their keys.



Ecstasy premium quality

Vendor: AmsterdamQuality

(2) ★★★☆☆ (3)

Ships from: NL

Ships Worldwide

Multisig, Escrow

Buy

Typical order on a darkmarket

Wall Street Market

Wall Street Market, the darkmarket we have chosen to study, is one of the main active market and the largest one supporting multisig transactions, and provides an extraordinary amount of transaction data to study. At first sight, it seems to be a highly secure market, which is true from different points of view. But a negligence in payment methods results in an information leak, allowing most of the darkmarket transactions to be traced. Using this with the multisig traceability, it is possible to have an in-depth analysis of this darkmarket.

During our study, we have initially gathered many vendors public keys and analysed this data, but the payment methods negligence allows us to follow the whole market and not only its vendors. Now we can be sure that, since the start of this year, the average turnover per week of Wall Street Market is at least $477 370, including $24 655 exclusively from multisig transactions. The average number of multisig per week is 90 compared to 3'115 for the overall transactions during the same period. The average amount per multisig transaction is $265 compared to $150 for other ones.

The fact that multisig is not use every time is because Wall Street Market claims higher fees for such transactions. But when the degree of trust is important, such as in expensive transaction, customers prefer to protect themselves with multisig.

Julien Farine

Xavier Hennig