Quentin Moore
qrm6ff

Problem Set 3

1a) 1ALXarqN55Fc2g7EcSFPxSc7em72SvFMSJ
1b) This address was used from 4/11/2014 to 5/7/2014
1c) There appear to be 2 victims that paid to this address
1d) 1.47 BTC (~$735) and 2.44 BTC (~$1220) were paid to this address.
1e) Although payouts went to different addresses in each outbound transaction, there seemed to be a 60/40 split each time someone paid to this address.
1f) The addresses that recieved the 60% cut had a total of 2000+ transactions, while the addresses that received the 40% cut had a total of <100 transactions. Perhaps this is one of many ransom ventures by the person who received the 60% cut from this particular ransom venture.
1g) This address received larger payments from fewer people than most of the addresses we are investigating. The 60/40 split is also more even than most splits, implying that there may be "partners" in this venture, rather than one ransomist simply paying a fee to someone else.

2a) Questionable merchants have a big incentive to stay anonymous. Thus since the team was analyzing anonymity with regard to addresses, and how to link multiple addresses to a single user, it is natural to obtain data about these questionable merchants.
2b) By dealing with questionable merchants, one may be assisting in a criminal enterprise or otherwise associating with criminals. Even if the transactions were made in order to conduct research, helping a criminal enterprise can be ethically and/or legally wrong.

3) A transaction can have multiple inputs owned by different entities. The public keys for these inputs are publically available. The proof of ownership of the inputs by each individual entity can be provided without revealing the private key to the other owners of the inputs, and then send them as part of the same transaction.

4) HD wallets link a set of addresses together into clusters since the addresses produced are determinstic, thus, heuristic 2 does not really provide any additional links that are not already obvious by the nature of how HD wallets work.d

5) The output transaction will have a value between 0.0012615 and 0.0014138 BTC
6) Using two forwarding addresses would require someone to look at all sets of two transactions within the block that sum to a total of 0.0012615 to 0.0014138 BTC. This makes the workload to deanonymize the transaction far harder, especially if there are many transactions that total to values smaller than this range in the block.

7) BitPay.com-old Btc-e.com BTC-e.com-old MtGoxAndOthers seem to be the tagged addresses that receive bitcoin from the ransomists. These are the exchanges they are using to cash out.

8 and 9 in code.

10) An automated mixing service takes in the deposits from users and then sends back bitcoin from other users of the service, minus a fee. Since these services usually have a quick turnaround time, you can make a guess at which transaction is the output from the mixer based on the transactions included in the next block. Therefore, these automated services do not offer the highest level of anonymity. There are some mixers that process manually and pay out from a totally separate wallet, but even this does not provide full anonymity since the bitcoin still had to come from somewhere. The presence of a public ledger makes it very difficult to provide full anonymity (although mixing does slow down the process of tracing the flow of money).