Dark markets‘ survey

Degree programme : BSc in Computer Science | Specialisation : IT Security
Thesis advisor : Prof. Dr. Emmanuel Benoist
Expert : Daniel Voisard (Federal Office of Communication OFCOM)

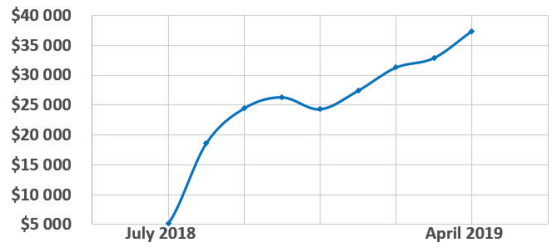
Dark markets are a very big part of the dark net traffic. These markets are of course quite private and do not leak a lot of information. The purpose of this thesis is a deep analysis of these markets with answers to some questions such as: Which offer yields the most? Who are the best sellers? The final objective is the estimation of the income of these sellers as well as the comparison of these estimations with their actual income obtained with their bitcoin address.

Dark markets and multisignature

Dark markets are websites for buying and selling illegal items (drugs, weapons, credit cards, etc.). The big problem for users of this kind of site is the trust placed in other vendors or even the site itself. To address this problem, some markets have incorporated a feature called bitcoin multisignature. Multisignature is a system for sending transactions to a neutral account until the product arrives. This account can only send the money if two out of three users accept the transaction (the users are the market, the seller and the buyer). This function ensures that the market does not steal funds and that the seller / buyer does not steals the other party.

Tools for crawling and analysing

My project has two different parts. The first part represents the creation of a tool for crawling and analyzing data from the three largest existing markets. This system creates threads sending html queries to the site in question. Once the answers have arrived, the document is parsed and the information are stored in a database. The database contains all the offers of a site and their information. One of the most interesting information is the number of reviews for a given offer and the amount spent. Indeed, one some site, when a buyer writes down a review on an offer, the amount spent by this user is shown. This allowed me to estimate the average amount received by a seller. With this estimation for each offer, it’s possible to estimate the income of a seller or even of a category. The estimations are then displayed in the same application allowing the user to crawl and analyses the site with the same tool. The second part of this project represents the automation of a breach discovered during a previous thesis. This flaw uses a multisig function of the Wall street market site allowing to recover some sellers’ bitcoin addresses. Indeed, when creating a multisig transaction, the buyer has 3 days to send the money to an address generated by the market. At the end of those 3 days, the market stops the transaction and returns the multisig addresses of the 3 signers. This allowed me to retrieve the address of the seller and to compare this address to other transactions in the blockchain. Once I found some transaction using this multisig address, the bitcoin addresses of these transactions can be considered the seller’s actual addresses.



Unigarant’s effective monthly income

Uncover some Bitcoin addresses

The recovered results are very interesting. Indeed, it was possible for me to recover the values of the markets which allowed me to compute some estimates of income. It was then possible to recover some bitcoin addresses (the closure of the site prevents me from recovering everything) to be able to compare the actual income and the estimates. Thanks to this, I have been able to show that the estimates are not far from the reality allowing me to increase the credibility of the rest of the data.

These bitcoin addresses also allowed me to retrieve Wall Street Market’s bitcoin address while they were trying to steal all users’ money. This address was appearing multiple time in the transactions of some sellers and looked really suspicious. A huge amount of bitcoin was transferred in a few days and some transaction really looked doubtful. After analyzing the income and done some researches, I found some post mentioning this address as Wall street’s one. This allowed me to trace the amount sent by this address (more than 11M$) and find some transaction to a bitcoin trading platform or even to the account of one of the admin.

Jérémy Valentin Vizzarri