Effect of IoT botnets on Cryptocurrency

Jan-Willem Nijhuis
University of Twente
P.O. Box 217, 7500AE Enschede
The Netherlands
jwj.nijhuis@student.utwente.nl

ABSTRACT
As technology advances, more and more devices have Internet access. This gives rise to the Internet of Things. With all these new devices connected to the Internet, cybercriminals are undoubtedly trying to take advantage of these devices, especially when they have poor protection. These botnets will have a large amount of processing power in the near future. This paper will elaborate on how much processing power these IoT botnets can gain and to what extend cryptocurrencies will be influenced by it. This will be done through a literature study which is validated through an experiment.

Keywords
Cryptocurrency, Mining, Botnets, Botmasters, The Internet of Things

1. INTRODUCTION
"Cryptocurrency is an encrypted decentralized digital currency transferred between peers and confirmed in a public ledger called block-chain via a process known as mining" [9]. The use of such a currency makes it hard for governments to tax, since it is not owned by a central authority. This makes it a great currency for traders who do not want to be dependent on such a central authority. Cryptocurrencies are free floating and therefore their value is not subject to inflation [4].

Making a transaction with a cryptocurrency such as Bitcoin requires the owner of the coins to broadcast a signed receipt to where they are being sent. This transaction will then be added to a pool of unchecked transactions. To validate transactions they will be hashed together on a block which is being added onto the block-chain by miners. This adding onto the block-chain requires constant hashing and therefore a lot of computational power.

This is where the miners come in. They will all try to find the next block for the block-chain which contains all transaction data. The miner finding the next block is rewarded with a few Bitcoin or other form of cryptocurrency depending on what they were mining [25].

Because mining cryptocurrency can be profitable there are lots of companies which set up large cryptocurrency farms to mine these currencies. The potential profit these companies make will be a trade-off off between energy consumption, equipment costs, and the value of the gained currency.

Currency can also be mined by individuals. This is however, depending on the hardware, a lot less energy efficient and therefore most likely not profitable. Cybercriminals try to circumvent these costs by having hijacked computers and devices do the mining [17]. A single computer or device will not generate a lot of processing power, therefore the cybercriminals will cluster computers together in a group which is called a botnet. A cybercriminal running a botnet is called a botmaster [9].

The introduction of all sorts of new Internet connected gadgets in all sectors of modern life has brought life to what is called the Internet of Things (IoT). All sorts of devices are now connected to the Internet. However IoT devices are often designed with poor security or even none at all [18]. This makes IoT devices a prime target to be hacked and added to a botnet. Botmasters now also target IoT with their malware [15].

1.1 Problem Statement
With the upcoming rise of the IoT and the poor securities of lots of devices, cybercriminals will undoubtedly add IoT devices to their botnets. The number of smart devices excluding smartphones, tablets and personal computers was around 9 billion in 2016 and is expected to grow up to 28.1 billion by 2020 [18]. Given that so many smart devices will exist in the near future botnets will grow to immense sizes and have tons of processing power. This paper will analyze to what extend botmasters will use the processing power of these IoT botnets for cryptocurrency mining.

1.2 Research Questions
In order to get a proper vision of how the Internet of Things interacts with botnets and cryptocurrencies the following questions are asked:

1. How can a cryptocurrency be influenced by miners?
2. How do IoT botnets compare to other ways of mining cryptocurrency?
   2.1. How much mining-power does an IoT botnet require to have an impact?
      2.1.1. How good is a smart device at mining cryptocurrency?
3. What tasks can an IoT botnet perform?
4. To what extend will IoT botnets influence cryptocurrencies?

2. METHODOLOGY

Permission to make digital or hard copies of all or part of this work for personal or classroom use is granted without fee provided that copies are not made or distributed for profit or commercial advantage and that copies bear this notice and the full citation on the first page. To copy otherwise, or republish, to post on servers or to redistribute to lists, requires prior specific permission and/or a fee.

27th Twente Student Conference on IT July, 2017, Enschede, The Netherlands
Copyright 2017, University of Twente, Faculty of Electrical Engineering, Mathematics and Computer Science.
The questions have to be answered sequentially in order to get a clear answer on the last question. Getting good answers on all questions requires some amount of background knowledge, which shall be presented before going further in depth.

2.1 Influence
To find out how a cryptocurrency can be influenced it needs to be understood how a cryptocurrency works and how new coins are distributed. Looking at how a cryptocurrency can be abused before it is released might also be of interest, this is called premining. It might also be interesting to look at the currency from an economical perspective, to know what causes influxes in its price. From all of this knowledge a proper answer can be deducted.

2.2 Hashing power
To get a grasp of the mining power an IoT botnet has, a literature study will be done on the sizes of IoT botnets of being caught. Example devices which they are made up of. The most common IoT devices will be compared on their different hashing powers. From this can be derived how much currency the botnets can mine. This will then be analyzed and compared to other methods of mining cryptocurrency.

2.2.1 Device Strength
In order for hardware to be compared several devices will be analyzed to see which can perform the hashing algorithm the fastest. Given that different hardware architectures perform hashing algorithms at different speeds the results should be taken with a grain of salt. A raspberry pi 2 is used as default device. This should give a rough overview of the processing and hashing power an IoT device can deliver.

2.2.2 Network Strength
A study has to be done to determine the strength of a network. Firstly it needs to be clear how a total hashrate can be obtained from multiple devices. Then a study has to be done on the sizes of IoT botnets to find the total amount of hashing power a botnet has.

2.2.3 Legitimate methods
Cryptocurrency farms do not use large botnets of compromised devices to mine their currency. They instead use specialized hardware which is built with its only purpose being hashing. These methods will be compared with botnets to see which would be dominant.

2.3 Botnet use-cases
Botnets provide flexible toolset for various illegal activities, providing remarkable financial gain with a low risk of being caught. Examples include sending SPAM emails, DDoS attacks or the automated extraction of sensible credentials such as account login information or banking details [15].

A botnet might be assigned different tasks depending on the availability of its bots. A botnet designed to mine cryptocurrency fares best when the bots in a network have a high availability or uptime [28].

A literature study will determine which of these use-cases is most viable and profitable for a botmaster.

2.4 Validation of data
An experiment will be done to verify whether the device strengths obtained from the literature are correct. Different settings will be tested to see how the most hashing power can be obtained. It will also be tested to what extend other running applications will have an effect on the hashing power.

2.5 Influence of IoT botnets on cryptocurrencies
Once all relevant literature has been studied and the data validated, a discussion will elaborate on the overall influence of IoT botnets on cryptocurrencies.

3. BACKGROUND

3.1 Using Cryptocurrencies
Different cryptocurrencies have different ways of being obtained. Bitcoins, for example, can be obtained in two ways; one can simply buy them online through vendors. This is the most straightforward way of obtaining them; after paying a seller, the bitcoins will be simply transferred to a personal wallet. The other way of obtaining bitcoins is through mining. The block-chain which is a shared public ledger which contains all information of all previous transactions. To add on to this block-chain cryptography needs to be used. A computer can be used to find the next block on the chain, this requires hashing. Whenever a new block is found some new bitcoins are generated and added on to the finders wallet, as well as all transaction fees made by other users.

3.1.1 Coins
The names for the coins of every cryptocurrency are all different and are usually some sort of modification of the name of the cryptocurrency. For example Bitcoin uses Bitcoins, Litecoin uses Litecoins, Ethereum uses Ethers, and Ripple uses XRP [6] [19] [16] [24].

3.1.2 The wallet
Every cryptocurrency uses some form of a wallet to store their coins. These wallets consist of a public address and a private key. The public address is needed to give someone coins and are visible to anyone. The private key is used to verify a transaction being send from an address. This is done using asymmetric-encryption.

3.1.3 The block-chain
Most cryptocurrencies depend on a mechanism called a block-chain. A block-chain is a public ledger which contains all previous transaction data. Finding the next block of the block chain requires both luck and hashing power. All transaction data has to be combined with a random number in a manner depending on the cryptocurrency, and the outcome has to be fitting. This means that the time required to find the next block is also somewhat random.

3.1.4 Difficulty
The Bitcoin and Litecoin block-chain changes the difficulty of finding the next block. The Bitcoin block-chain does so about every two weeks with the new difficulty depending on the time it took to find the blocks for the chain. The difficulty is set in such a way that it takes about ten minutes to find the next block. A transaction should not be counted as successful until after several new block have been added on the the chain. As coins might be double spend otherwise [20]. This makes trading bitcoins a slow endeavor. Several other cryptocurrencies such as the very similar Litecoin [19] use a shorter timespan to add on to their block-chain. This has faster transactions, however it requires more confirmations to
prevent double-spending and also produces larger quantities of coins. Some cryptocurrencies behave differently, such as for example Ethereum and Ripple. Ethereum also runs on block-chain technology, but is more adaptable and flexible and is used to fuel applications running on it [16]. Ripple was created with a set number of it being created at the start and no more can be created, this also means it cannot be mined [24].

3.1.5 hashing
The method of finding the next block of the block-chain differs per currency. They all make use of some sort of hashing algorithm to find the next block on the block-chain. Bitcoins use the SHA-256 hashing algorithm to add on to the block-chain whereas Litecoin uses scrypt, and Ethereum uses a SHA-3 hashing variant called Keccak. So mining these currencies requires different amounts of processing power and different hardware will perform better on some of them.

3.2 Mining Cryptocurrencies
Mining cryptocurrencies requires hashing power. The more processing power a user has the more it can hash. This means that having a stronger computer, depending on the hardware, will most likely hash more than a weaker or older one. But having more computers will also impact the amount of hashes done per time unit. Therefore it is regularly seen that botnets composed of personal computers will use their processing power to mine cryptocurrencies [5].

Older and more valuable cryptocurrencies might have hardware dedicated to their hashing algorithm. This is already the case for Bitcoin and Litecoin. These dedicated hardware miners can hash a lot more than other devices and are a keystone in cryptocurrency farms [7].

3.3 Pooling
Block-chain technology usually[16] only rewards the individual finder of the next block. Because a lot of machines are usually mining a currency it is very unlikely that a single person or machine ever finds the next block on the chain. This would deter most people from mining a currency, however people started mining in groups, sharing the loot equally over the amount of work done. These are called pools and most miners are part of such pools. Joining a pool has as benefit that the amount of currency gained becomes less luck based and are being distributed more according to workload. Pools give miners a more stable income of the designated currency [6].

Cybercriminals will very often join such a pool or set up their own pools[17] so they can easily add on all of the devices in their botnets. This makes it a lucrative business if their botnets are big enough and have large amounts of power.

4. INFLUENCE ON CRYPTOCURRENCIES BY MINERS
The value of a cryptocurrency can for approximately 84% of its relative value be determined by three variables. The first of these variables is the computational difficulty to mine the coins. If the indirect difficulty is higher the coin will be worth more. The second variable is the amount of coins generated per time unit. The less coins are brought in to a system the more they are worth. And the final variable is the hashing algorithm used by the cryptocurrency. Some algorithms make a currency more valuable than others [1].

This means than the value of a cryptocurrency alternative to bitcoin called an altcoin can be predicted with some accuracy. This gives people a good impression of how valuable a cryptocurrency is and what its growth rate may be [2].

Pre-mining cryptocurrencies is a way in which malicious developers already mine a currency before it goes live, making them already have a large share of the available coins. They hope to then be able to sell the coins later on for a sizable profit. However, because of the nature of the block chain their intents are usually clear from the beginning and a currency will lose interest from the public [3].

4.1 Hashing power
4.1.1 Individual
Different devices have different hashrates and different coins have different corresponding hashrates. Several different hierarchal positions can be taken as examples. A raspberry pi 2 is analyzed as being in line with some of the higher powered chips of smart devices, then it will be compared with other means of hashing. Note that there is no FPGA in the Litecoin chart because they have been largely skipped. Figure 1 has been created from this data, it shows a logarithmic scale with a factor of 100 of hashing power per device for both Bitcoin and Litecoin [10] [8] [29] [30] [31].

4.1.2 network
Miners often collaborate in pools to share rewards claimed from mining. Because mining in pools has no drawback in hashing power [27] most users will prefer to mine in pools. Pools often keep a small percentage of you mined currency for them to keep running and make a profit. Users choose for the pools which keep the least amount of coins so competition is fierce. Some people think such pools are against the spirit of cryptocurrencies and have set up a decentral-
ized mining pool [22] to keep a larger share of the mined block.

IoT botnets can grow up to immense sizes, with mirai growing up 380 000 devices [34] and Hajime having about 300 000 [32]. However not all IoT botnets have this size as the total amount of identified infected IoT devices is around 500 000 [34].

Writing code for IoT appliances is very meticulous and requires different assembly programs for different kernels [33].

5. EXPERIMENTAL VALIDATION

5.1 Setup
A raspberry pi 2 will be used to determine whether the values obtained from other sources are accurate. The pi will run the latest version of raspbian operating system [23]. To find the hashrates a program called cpuminer [11] will be used. This program requires a pool address to work for and store the mined currency. The Minergate [21] pool will be used to mine Litecoin, and Slushpool [26] will be used to mine Bitcoin.

5.2 Results
The results gained from the experiment differ very little from the data from the sources [31] [29]. These differences are less than 20% from what the sources state. Individual microprocessors will have a small deviation in which clock speeds they can run at. These small differences in power may very little difference on a larger scale as their hashing power will regress to the mean. See appendix A for the hashrates resulting from running cpuminer on the raspberry pi.

6. USE CASES

6.1 DDoS
IoT botnets have remarkable power to execute DDoS attacks. Because they consist of lots of different devices and are located throughout legitimate devices, they are hard to deal with. DDoS attacks also require little processing power as they only need to send data over the Internet. IoT devices are inherently capable of sending data over the Internet as that is what makes them a part of the IoT. Running DDoS attacks is also remarkably profitable for a botmaster as they can ask for up to 4 000 dollars per week for a DDoS attack consisting of 50 000 bots [35].

6.2 SPAM
The number of SPAM emails sent is steadily declining. The reason for this is that current SPAM protection is becoming more and more adapt at picking out the SPAM emails [36]. This also means that it is becoming less attractive for botmasters to have their botnets send SPAM emails.

6.3 Credentials
While regular botnets are great for stealing data and credentials. This is not the case for IoT botnets as they are not connected to a users hard-drive. Most IoT devices have nothing of value to compromise. The only exception to this are cameras. But the data they collect is also usually of little value as nothing interesting happens for most of the time. It will take ages for a cybercriminal to try and filter out all the interesting moments. This also makes stealing personal data or credentials a non-appealing business for IoT botmasters.

7. DISCUSSION

Bitcoins and other cryptocurrencies are a large business in which many cybercriminals and other criminals alike are infested. However cybercriminals cannot use all their means to fuel cryptocurrencies. Cybercriminals want to use their precious gained bots to make as much money as they can. Because mining cryptocurrencies is most likely not the most effective use of their IoT botnet cybercriminals will probably use their IoT botnets for other things. IoT botnets are great for DDoS attacks and can to a lesser extend also be used for sending SPAM and stealing credentials or personal data, and a botmaster will try to find whatever is most profitable for him.

Since bitcoins require immense amounts of hashing power to be mined a raspberry pi is really small on this scale. Given the current amount of total hashes and the current difficulty to find the next block the amount of Bitcoin earned can be calculated [12]. Here we can see that a 1 Terahashes per second device gives a profit in Bitcoin of under 2 dollars per day. From this value the electricity costs and pool costs are not yet deducted. This means, given a hashing rate of 160 kilohashes per second for a raspberry pi, that mining bitcoins using raspberry pis is completely unfeasible. Even if someone had a million raspberries in a mining pool they would not even gain 20 cents per day [12].

For Litecoin a raspberry pi can only do about 500 hashes per hour, however, the ASICs for scrypt have not been as far developed as for SHA256. This means that percentage more will be gained. Given a fairly large IoT botnet composed of 50 000 devices with similar processing power to that of raspberry pis will mine less than 2 dollars worth of Litecoin in a day [13]. Which is a lot less than a similar sized botnet would earn a botmaster when used for DDoS attacks.

8. CONCLUSION

The price of cryptocurrencies will increase if more of it is being mined. However older cryptocurrencies such as Bitcoin can be influenced very little as they already use immense amounts of processing power. Younger currencies can be very well influenced by such botnets. However this remains a gamble as the cryptocurrency might be seen as being pre-mined if one user gains too much coins of such a currency and become worthless.

The recent influx of ASICs on the cryptocurrency market has given professional miners quite an advantage in the hashing-power department and makes other means of mining become insignificant. These devices will even outperform absurdly large amounts off small devices mining the same currency and makes IoT botnet mining most likely not worth the effort.

Other tasks botmasters will assign their IoT botnet to do will include DDoSing and to a lesser extend sending SPAM emails and stealing personal data. These offer the botmaster a better source of income and will be a more likely use of these IoT botnets.

With this we can safely conclude that botmasters will rarely use their botnets to mine cryptocurrencies and therefore have little influence on them. However, when a few botmasters decide to create a currency of their own, or fuel a small existing one, they could mine this together to help such a currency to grow and hope on a return of the investment.

9. FUTURE WORK
Since botnets will not go away in the coming few years research needs to be done in order to determine how large the threat of these will be. Botnets, both IoT and regular ones, will both have a lot of power which will be used with malicious intent. Determining the amount of damage these are capable of doing is of great importance in order to prepare for it and eventually counter it.

10. ACKNOWLEDGEMENTS

I would like to thank my supervisor Dr. Ir. Nirvana Meratnia for her guidance and support during the research. I would also like to thank my peer reviewers for their insights and suggestions.

11. REFERENCES

APPENDIX
A. HASHRATES PI

Figure 2. ltc

Figure 3. btc