BOTNETS AND CRYPTO CURRENCY
EFFECTS OF BOTNETS ON THE BITCOIN ECOSYSTEM

by

Hitesh Dharmdasani
A Thesis
Submitted to the
Graduate Faculty
of
George Mason University
In Partial fulfillment of
The Requirements for the Degree
of
Master of Science
Information Security and Assurance

Committee:

	Dr. Damon McCoy, Thesis Director
	Dr. Angelos Stavrou, Committee Member
	Dr. Brent ByungHoon Kang, Committee Member
	Dr. Sanjeev Setia, Chairman, Department of Computer Science
	Dr. Kenneth S. Ball, Dean Volgenau School of Engineering
Date: May 3, 2013	Spring Semester 2013 George Mason University Fairfax, VA

Botnets and Crypto Currency - Effects of Botnets on the Bitcoin ecosystem

A thesis submitted in partial fulfillment of the requirements for the degree of Master of Science at George Mason University

By

Hitesh Dharmdasani
Bachelor of Engineering
KLS Gogte Institute of Technology, 2011

Director: Dr. Damon McCoy, Professor
Department of Computer Science

Spring Semester 2013
George Mason University
Fairfax, VA

Acknowledgments

I would like to express my sincere gratitude to my advisor Dr. Damon McCoy for his immense support during the course of my study, for his patience, motivation and immense knowledge. He has been a constant support in all my efforts. I would also like to thank Dr. Angelos Stavrou and Dr. Brent ByungHoon Kang for their insightful comments and suggestions

This project saw great collaboration with amazing researchers and I am thankful for their help and effort towards this project Dr. Kirill Levchenko, Dr. Alex C. Snoeren, Dr. Stefan Savage, Dr. Nicholas Weaver, Dr. Chris Grier, Mr. Brian Krebs, Mr. Danny Yuxing Huang and Ms. Sarah Meiklejohn. Thank you very much.

I would also like to thank my father Mr. Naresh Dharmdasani, my mother Mrs. Rekha Dharmdasani and my sister Ms. Heena Dharmdasani for supporting me and my interests. Thank you to Ms. Pooja Srikant, Ms. Smita Srikant, Mr. Prateek Pawar, Mr. Brian D'Souza, Mr. Praveen, Ms. Sonia Malani, Ms. Sneha Malani and all my other friends who always saw the best of me.

Table of Contents

List of Tables

List of Figures

Abstract

BOTNETS AND CRYPTO CURRENCY - EFFECTS OF BOTNETS ON THE BITCOIN ECOSYSTEM

Hitesh Dharmdasani

George Mason University, 2013

Thesis Director: Dr. Damon McCoy

Nearly every aspect of a hacked computer and a users online life can be and has been commoditized. Recent trends into crypto currencies have made the former even more true as cyber criminals are now commiting crime for monetary benefit and not just to out smart each other. In this study, I look more closely at Bitcoin, a de-centralized crypto currency which has become increasingly popular in the last six months. This study focuses on the analysis of the bitcoin economy, the involvement of malware and botnets and its effect to the currency.

Chapter 1: Introduction

1.1 Motivation

Since its birth, Bitcoin has seen tremendous growth and has been much talked about. As of this writing, there are more than 11 million bitcoins in circulation, with an exchange rate of $236 per bitcoin making the bitcoin economy worth approximately 2.5 billion dollars. With more than thirty-six exchanges operating worldwide that offer exchange services to many of the worlds currencies. Bitcoin has gained immense popularity and also the attention of policy makers. This growth in popularity has also grabbed the attention of cyber criminals who want to make quick money. Also, with bitcoin not being controlled by any central organization and free from government regulation, it is perfect for money laundering and for use of payment in obtaining illegal goods. Which makes it a favorite with the underground world.

This is the first instance where resources (i.e. CPU cycles) are stolen, abused and monetized at a large scale. Assuming a mediocre botnet with 10,000 compromised hosts, each capable of producing hashes at the modest rate of 5 mega-hashes per second, we estimate that the botnet all together can produce at least 3.3 bitcoins per day. At the current exchange rate, the daily profit is close to US $600; this number will be significantly higher if some of the compromised hosts have GPUs, whose parallelism can be further exploited for mining.

It is intriguing to note that cyber crime is not just limited to stealing credit card information or any of the previously seen methods. It has made its way to producing real money at the expense of someone elses resources: turning it into a lucrative business

Our results have shown that bitcoin is indeed being abused by botnet owners. There is conclusive evidence of malware that is known to contact domains that act as proxies to

known public pools so that their identity is hidden and estimates of some portion of the malware in our dataset has given first hand indications of the revenue generated by such malware.

I hereby present my work with the goals of understanding the bitcoin economy from a botnets perspective, to reveal the information of such botnet owners and the accounts that they use and to determine the footprint left by botnets in value of bitcoins to the bitcoin economy.

1.2 Background

1.2.1 About Bitcoin

Bitcoin is a decentralized digital currency based on an open-source, peer-to-peer Internet protocol. It was first documented by a pseudonymous developer named Satoshi Nakamoto(w hose name is conjectured to be fake by some, and who has not been heard from since April 2011). Further an open source project on sourceforge saw the birth of the first bitcoin client. The initialization of the currency with a genesis block happened on 3rd January 2009. Followed by an announcement on the cryptography mailing list at metzdowd.com. Every bitcoin can be divided into 100 million smaller units that are called satoshis, defined to exactness by eight decimal points. Unlike traditional currencies, Bitcoin does not have a central issuing authority, hence making its way across international borders. Bitcoin borrows heavily on the fact that like many real world currencies, that a currency is any object, or any sort of record, accepted as payment for goods and services and repayment of debts in a given country or socio-economic context; hence validating the currency

Even though generation of bitcoins is not an illegal activity, as all other forms of money making, bitcoin is not spared to the shadows of cyber crime and malware, The very nature of bitcoin not being limited by international borders creates an opportunity for members of the underground economy to exploit this privilege and offer goods and services in exchange for bitcoin which can later be exchanged for in any currency desired. Although anonymity

was not a part of the bitcoin protocol specification, the use of public key infrastructure makes all transactions anonymous even though the value transferred is public; their sender and recipients remain anonymous.

Peers in the bitcoin network can transfer bitcoins to each other by issuing a transaction. A transaction consists of a hash of the last transactions corresponding to the coin being spent also indicating what was the previous transaction for this bitcoin along with the public key of the recipient of the exchange and his own signature. Any node in the network can verify the authenticity of a bitcoin by checking the chain of signatures

Table 1.1: Structure of a block in bitcoin

Field	Value
hash	000000000000061b55e0c9db394fae7d067746451a3f7e3857cd842b9a083d4
version	2
$hash_{previous}$	00000000000000ef82578761f0e5aa4f02e4f90bbbb9e350820a038a091bbf74
merkelroot	6200ea79cf4031a0a3b18c869c7dc832998c28310ed4553ab1656fab3b969161
epoch time	1365627045
target bits	436350910
nonce	50368043
no of transactions	267
size in bytes	150956

All transactions in bitcoin are put into blocks that together form a block-chain. The block-chain is always available to all the nodes in the network. This method ensures that all nodes in the network know about all the transactions that have happened previously, which is necessary when a new transaction from a sender to a receiver has to be validated. The problem of double spending in bitcoin has been looked at as the process by which a peer would change a transaction in a block that indicated that the BTC was spent. This also means that if a peer inside the network would wish to double spend. It would hence have to re do all the work that was required to establish that block and all the following blocks in the block chain. Also, for the nodes in the network to accept such tainted blocks the speed of a tainted block generation will have to out beat that of the honest nodes for

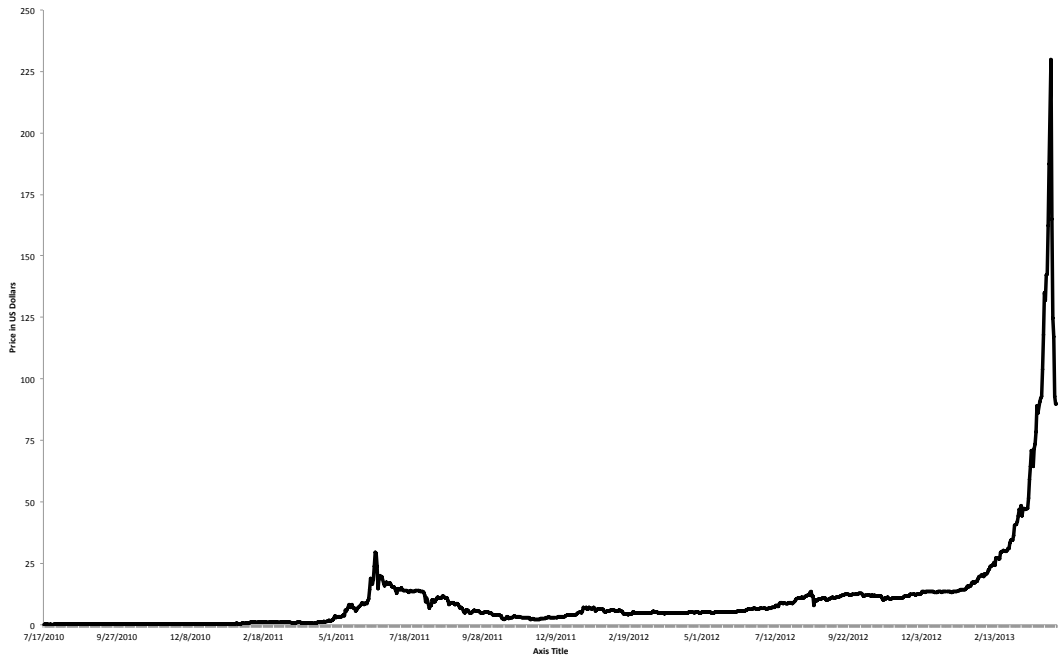

Figure 1.1: Growth of Bitcoin.

which the probability drops as the number of blocks in the block chain increase

To understand how bitcoin works it is necessary for us to know some aspects about the bitcoin protocol. These are explained below in brief.

1.2.2 Mining

Bitcoins are generated through the process of mining, They are awarded to "miners" that solve increasingly complex proof-of-work problems and hence are rewarded for the same by being credited with bitcoins. This methodology induces new bitcoins into the system and helps grow the currency. According to the protocol, the growth of bitcoins follows a geometric progression that is hard coded into the network. IT is also dependent upon the degree of mining activity happening in the network; The greater the speed of mining, The more difficult it gets to generate bitcoins. Bitcoin miners are also rewarded for confirming transactions that happen on the bitcoin network and such fees are termed as transaction fees. Also, there are rewards for confirming an entire block in which case the miner node

is rewarded with the transaction fees as well as a fixed reward that drops as the currency grows, as of this writing the reward for mining a block is 25 BTC.

Table shows the comparison of different mining hardware. Since the rise of difficulty in bitcoin. It has become impossible for miners to use a CPU and gain substantial rewards in bitcoin. ASICs dominate the generation of bitcoin with respect to their hash rate. Although using multiple CPUs in parallel and using pooled mining approaches, it is possible to generate substantial earnings as we shall see in Section 1.2.4.

Table 1.2: Comparison of Mining Powers

Type	Specification	Hash Rate	Time to mine one block
CPU	Core i5-650	5.1 MHash/s	205 years 24 weeks
GPU	ATI Radeon 7970	555 MHash/s	1 years 46 weeks
FPGA	BitForce SHA256 Single	832 MHash/s	1 years 13 weeks
ASIC	Avalon ASIC	66300 MHash/s	5 days 18 hours

1.2.3 Proof-of-work

Proof-of-work refers to data that is produced to meet certain requirements. The gist of the process is in the fact that the probability of meeting the said requirements through random processes is low, Thus proving to be computationally time consuming. Proof-of-work can also be thought as a mechanism that ensures faith by proving that enough time and resources are spent in establishing the validity of the subject than an attacker normally would.

The proof-of-work in bitcoin involves generating a hash from a pre known piece of data such that the hash produced is followed by a certain number of zeros. It is also to be known that such a problem increases in complexity exponentially as the number of zeros. A getwork RPC call built into the bitcoin protocol provides all mining clients with data to work on. The return value of getwork consists of H which is a SHA-256 hash of S; the internal state (i.e. Merkle tree) and the internal nonce N (i.e. coinbase, a 32-bit (4-byte) field) . the

merkel tree is a data structure formed by repeated hashing of the hash of each block in the block chain, the merkel tree establishes the authenticity of every block and hence every transaction in the bitcoin network. The value of N changes for every invocation of getwork as the nonce returned is the last nonce tried by the pool. The return value also contains the challenge, Indicating the number of leading zeros required when $hash(S, N')$ is performed where N' is the nonce that has to be found by the mining client. Since the enumeration of a 32 bit field would require 2^{32} permutations in the worst case. Such brute force approaches consume resources on the part of the miner.

1.2.4 Pooled Mining

Due to the nature of bitcoin mining. GPUs and distributed systems have been thought of for mining in pools. With the difficulty d at the time of writing to be 7673000 and assuming an average hashing power h of a CPU to be 5 MHash/s

$$t = d * 2^{32}/h \tag{1.1}$$

it would take a single CPU 208 years to generate a block. In pooled mining. A set of nodes by using miner software sign up on a pool and hence associate their wallet address with their account on the pool and then work on smaller chunks of the larger problem to establish the proof-of-work or simultaneously on the same problem in a race to finish it. Some pools provide a miner with a daily payout of the profits made by that pool, others calculate participation of every node in the network and calculate payouts accordingly. A share is awarded to the node in the pool that display a proof-of-work that is similar to the original proof-of-work.

As seen above, the creation of bitcoins is computationally expensive. Even in the case of pooled mining, it is seen that a single node cannot earn a lot of bitcoins quickly as he is only paid according to his contribution to the total computational effort. Learning from Charlton [1], Kirk [2] and Dima [3], It is possible that cyber attacks be launched to steal

bitcoins from wallets. as the wallet can be a local file on disk when stored on a desktop computer it makes it easy for any Trojan to spread and exfiltrate such files out of a victims computer. Further more, bitcoins contained in such wallets can be transferred to wallets owned by perpetrators and due to the nature of bitcoin, remain untraceable in the future. Unless mining pool owners identify wallets and corresponding account holders.

1.3 Malware Mining

Malware mining typically happens through mining pools as solo mining is a losing game. There are three primary ways by which a malware can mine bitcoins. These are shown in Figure 1.2

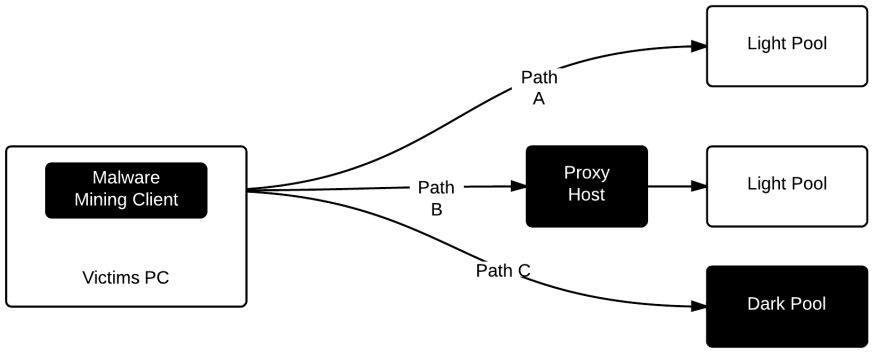

Figure 1.2: Malware Mining approaches.

Malware miners that use path A have accounts setup on the light pools. This method reveals the identity of the malware owners once the malware is blacklisted and any complaints to the pool owners can cause the malware authors to lose their accounts on the pool. This saves a lot infrastructure setup on the part of the botnet owner. However it is more prone to be blacklisted once such malware is detected.

Miners that adopt path B have higher degree of anonymity in their operations. In the

case of path B the getwork request from the mining client on the miners PC goes to the proxy server which can in turn contact a light pool on which the botnet has an account to perform the getwork RPC call and hence proxy the requests of getwork.

In the case of path C the botnet sets up its own mining pool and directly connects to the bitcoin network. Such infrastructure requires that the mining pool run a server to provide getwork responses to its clients. This method provides greater anonymity as the pool is closed to the botnet masters workers and hides the amount of mining being done which makes it difficult to calculate the profits made by such pools

Chapter 2: Literature review

Crypto currencies have been talked about in the past, But no other has had widespread adoption as bitcoin, Several currencies have adopted the bitcoin method of peer-to-peer ledger keeping such as Litecoin,BBQCoin, and Terracoin. Risks associated with such currencies have been documented in Brezo and Bringas [4].

There have been many efforts to understand the properties of the bitcoin network, In particularly the problem of double spending of bitcoins has been looked into depth in Ghassan O. Karame and Capkun [5]. Ghassan O. Karame and Capkun [5] suggests that it is indeed possible to double spend a bitcoin provided some necessary conditions are met. It has also to be noted that double spending in bitcoin is only possible when the sender(attacker) is not made to wait for the verification of the transaction thus carried out.

Martins and Yang [6] gives an elaborate overview of the bitcoin system. Also mentioning the fact that bitcoin has close encounter with malware attacks by which it is found that Trojans extradite files containing bitcoins for which real world instances have been seen in Bestuzhev [7] Charlton [1], Kirk [2] and Dima [3]

Even though bitcoin is said to provide pseudonymity through public key infrastructure Reid F. [8] has suggested that such anonymity is limited. It is possible to pair public keys of peers to their IPs and hence obtaining some information about the location of the peers.

Anti-virus vendors such as Kaspersky and Sophos have been detecting and deactivating botnets that were known to perform bitcoin mining. In the case of Ortloff [9] it is seen that the Hlux or Kelihos botnet specialized in stealing bitcoin wallets. This botnet was also known for contacting its command and control for bitcoin features during the time of takedown. Plohmann and Gerhards-Padilla [10] also shows us that it is indeed possible to build a bot network for mining and such activities have been documented in the wild.

Although this case study forms a base case for our analysis. There have been no investigations regarding the actual owners of such bot networks and the accounts they operate on. Further FBI [11] also states that bitcoin mining through bot networks is seen as an active threat. Which, as we see now, has come to be true.

Bestuzhev [12] documents the most recent outbreak of Bitcoin mining malware. It was shown to spread using Social Engineering attack vectors over Skype Instant Messaging. Showing us the active nature of malware mining.

Chapter 3: Goals

3.1 Categorizing Malware Miners

Once a host is infected by a malicious program(i.e. Malware). The malware includes a generic version of a bitcoin client and then invokes the miner client without the user's knowledge. Such malware is also known to inject entries into the registry of a windows based machine such that it is invoked on system startup. In the case that the malware is a dropper, It contacts the Command-and-Control of the botmaster to download settings associated with the mining client.

Primary analysis by querying public sources of information such as threatexpert.com has shown us that the mining client is invoked directly with the credentials in clear text. This has also helped us in understanding which mining pools are used by malware and what accounts are used to perform the mining. We have also collected more than 2000 distinct samples of malware, which indicates that 74% of the samples use well-known public pools(hereafter referred to as light pools) and unknown private pools(hereafter referred to as dark pools). With this knowledge we are now able to categorize malware according to its behavior with respect to the type of mining pool being joined.

3.2 Determining Extent of Botnet miners

Figure 3.1 shows the chart of distribution of the blocks that were mined by various pools that have claimed the block to be mined by them. It has to be noted that the unknown section of the chart which mentions that 23% of the blocks are mined by unknown pools says that those blocks are not claimed by any pool and not that those blocks are mined by dark pools. Unknown pools may also consist of solo miners who mine without the

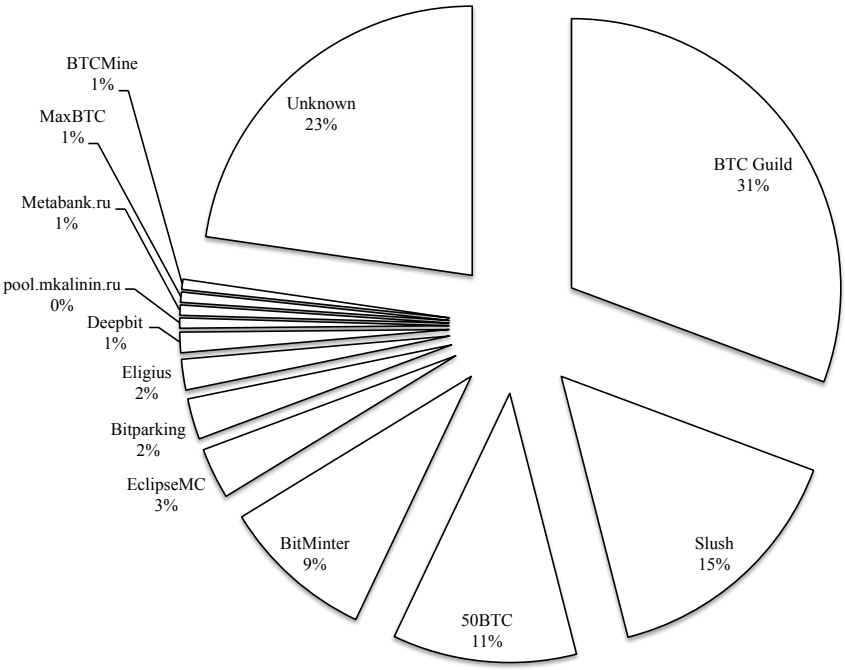

Figure 3.1: Mining Block distribution.

assistance of the network. But it is safe to say that some portion of those unknown pools could be dark pools. In our primary analysis we show that some dark pools use proxying mechanisms to mine. The dark pool domain responds to getwork requests by proxying to a light pool. Hence some blocks that might be mined by malware will reflect as being mined by light pools, even though the payouts of such mining activity have been paid to the wallet associated with the credentials used by the malware.

3.3 Determining Payouts to Botnets

Determining the payouts to individual wallets also remains a crucial part of the study. Every pool maintains a private record of account name to wallet address mappings. These mappings are used to credit an individual when the node associated with the said credentials

mines a block or verifies a transaction. Thus one method would be to act as malware and focus resources into mining a block. Once a block is mined, Its payout will be a part of the new block that shall be created. And hence wallets that receive payouts for that account can be identified. It is possible that the botnet master uses a public key for receiving each bitcoin from mining rewards. In this case we shall be able to find the wallet address only for that one reward. This shall foil our attempts to know about all the earnings for the dark pool.

Chapter 4: Analysis Techniques

4.1 Linking Light pools and Dark pools

From the analysis of our malware dataset. We were able to retrieve 255 distinct username, password and mining pool domain pairs. 81% of those logins belong to light pools and 19% belong to dark pools. Table 4.1. shows the frequency of malware trying to contact each domain for mining.

Table 4.1: Frequency of Pool occurrence

Pool Domain Name	No. of samples	No. of distinct logins	Type of Pool
pool.50btc.com	899	47	Light
mining.eligius.st	513	44	Light
xd.x3x9.asia	320	2	Dark
us2.eclipsemc.com	127	51	Light
pool.bitclockers.com	114	30	Light
xxa.m94vo3.com	85	2	Dark
mine2.btcguild.com	56	12	Light
dns.domain-crawlers.com	51	4	Dark
paljacinke.aquarium-stakany.org	40	3	Dark
keep.hustling4life.biz	36	3	Dark
abcpool.dload.asia	27	2	Dark
api.bitcoin.cz	25	7	Light
pool.dload.asia	23	5	Dark
google-updaete.com	9	9	Dark
eu.triplemining.com	7	7	Light
b.mobinil.biz	5	3	Dark

We can see that majority of malware use direct mining to light pools by choosing path A. From our analysis we have seen that there are some malware credentials are shared between pool.50btc.com and mining.eligius.st. Some malware logins use the wallet addresses

associated with those accounts as usernames. Using public information we have come to the conclusion that malware belonging to our dataset has mined a total of 1917.835345 BTC. The payout to these wallets also indicate that the bitcoins have been transferred to bitcoin24.com which an exchange that might be used to cash out the bitcoins into real world currency. It is not possible to know if the bitcoins have been cashed out as the bitcoins are moved around in internal wallets within bitcoin24 and it is hard to estimate if the bitcoins were cashed out or stored in safe haven.

Regarding bitcoin mining by dark pools it is to our knowledge that the domains: xd.x3x9.asia, xxa.m94vo3.com, abcpool.dload.asia, pool.dload.asia are all the same as they all resolve to the same IP address, and hence are the same mining pool. Determining the earnings of such pools cannot be done via public data, as the wallet addresses are not known. Thus we shall employ another technique.

Since the bitcoin protocol necessitates that all nodes that solve getwork responses be connected directly to the bitcoin network through miner client. The block that is mined is relayed by the pool and not by an individual. Hence a dark pool can leverage on this by obtaining getwork request from a light pool by performing getwork through a login associated with the malware author and in turn broadcasting that getwork response to all nodes the malware author controls. This gives rise to an interesting scenario in which blocks that are announced by light pools might actually be mined by nodes in the network that are under control of the malware author.

As we know that the login credentials are sent in clear text. By cross checking all logins against other light pools and dark pools we have examined that there exists an intersection between accounts on dark pools and light pools. The intersection is shown in Table 4.2. This intersection tells us that either the dark pools use their corresponding light pools as proxy accounts and in the case where two dark pools intersect, It may indicate the possibility of mergers of cyber criminals in the hope of more mining power. Our effort to investigate such intersecting logins has helped us in the case of 50BTC where we were able to find wallet address information and also know that a Web Money account was used with one of

Table 4.2: Intersection of login credentials

Original Pool	Association with	No of logins
mining.eligius.st	pool.50btc.com	19
dns.domain-crawlers.com	pool.50btc.com	4
b.mobinil.biz	*.asia	2
mine2.btcguild.com	*.asia	1
www.btcminers.biz	*.asia	1
pool.bitclockers.com	deepbit.net	1
keep.hustling4life.biz	pool.50btc.com and suppp.cantvenlinea.biz	1
thehood.k4912m.com	*.asia	1

$*.asia$ *compromises of* $pool.dload.asia$, $abcpool.dload.asia$, $abc.dload.asia$, $xxa.m94vo3.com$, $xxyz.l0za.su$ *and* $xd.x3x9.asia$

them. In some cases, pool owners have thwarted our requests to divulge information about accounts that are known to be connected to malware.

Further, Examining the response to getwork sent back by all the pools gives us a clear indication of the nature of their mining operations. It has been confirmed that the keep.hustling4life.biz known to be an active mining pool during July 2012 was a proxy to pool.50btc.com. Malware reports also indicate that this domain was known to be associated with the ngr-bot and was spreading bitcoin mining malware through its dropper services. Since then keep.hustlin4life.biz has re surfaced with its new incarnation being supp.cantvenlinea.biz, which had a major breakout using Skype Instant Messaging as a vector, and further using a dropper service similar to the ngr-bot. Due to public attention these domains are now offline. We are able to conclude on the above after observing getwork responses that indicate proxying headers and the equal nature of mining pool communications and the fact that they share the same login credentials when proxying to pool.50btc.com

Lastly, It is also known from the analysis of Wyke [13] that the domain name www.google-updaete.com is known to be associated with the popular Zero Access botnet. Looking at passive DNS data between May and October 2012 provided by the Security Information

Exchange(SIE), we can have a clear indication of the extent of the botnet in the past.

Table 4.3: Passive DNS analysis for mining pools

Domain Name	No. of DNS queries
*.asia	926
google.updaete.com	99
domain-crawlers.com	128
mobinil.biz	176

The data also shows us that google-updaete.com which indicates having a TTL of 600 is also an indication of a domain name changing its IP often due to obvious reasons for bot networks. Whereas dns.domain-crawlers.com and pool.dload.asia show stronger values of TTL and are also still having prevailing mining operations, cemented by the fact that there is new malware found everyday known to contact these pools.

The logins from malware that use wallet addresses to mine can be directly queried for in public sources. For the Eligius mining pool. Such information is made public by Eligius [14]. Thus by querying these services we have the data show in Figure 4.1

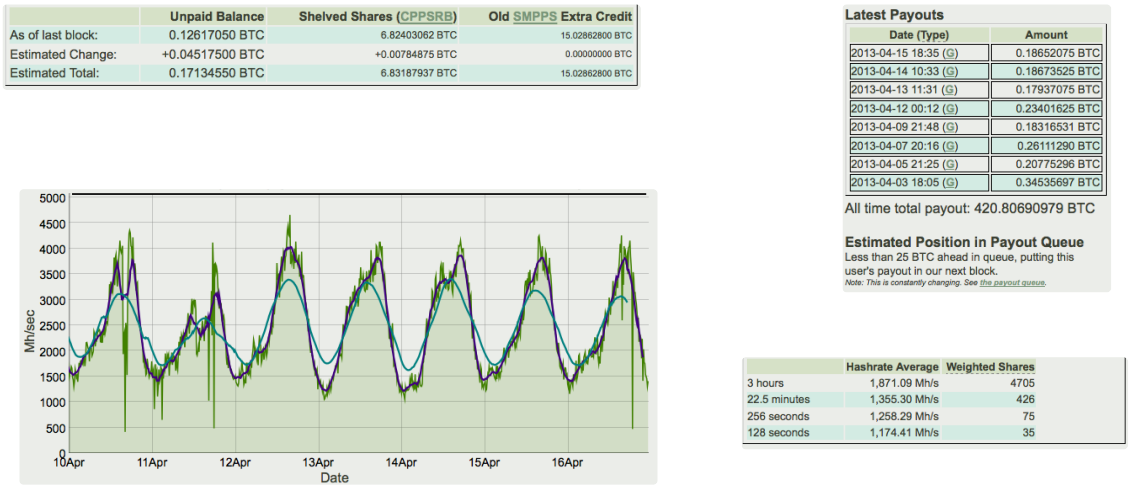

Figure 4.1: Mining Statistics Published by Eligius.

Consolidating such wallets by using the API services we can find the total earnings of all malware that use Eligius accounts for mining.

Wallet Address	Total Bitcoin Earnings
Eligius	
*13VdYJzQCGH7cMr9uWJKTZzDdn4cfDnWNn	155.4716365
*1C8qRSmrzdy6rYFTxJnmgSoQJfFUADCZd8	94.11867676
*1zPRh4V76nJG7gKSRFbgXkwQNAEaLg3Jt	29.6862976
1FiPR4mrXRHaioi2cV8J5VEnrvEha3enHL	25.24513006
*15EeddVj5rr6zmLfH1M26KvFX5KKJh3xgt	73.48552516
13j4XQEnXzgTi3ihJLLi3DctDZbU26KJ16	0
1NnKm4PxyU2VT4HYv4xhcdB8SN7FgxJvWb	0.17465576
1526rgSwoZHvbSpTSU4tFoCsb9btB4JNFk	2.02817743
*1Azge5CfpHQP6keWgkHPvTcZzjHamuFRba	30.8329784
1a3dpd9zAbitPRHxKBEk5FSmNfWGRyTwS	8.30711285
1ByFLx1JhEj2T1sEADy93C8KHTqjukyqYc	18.79870933
1P3NJr5aoDWTniA6MUHBobuTWZSC1sA19R	0.04210666
*169TpR47JVcLaQXdGYE6Lv4Ps9DbVqHhSi	0
*1JBv6w4ANiXmKAVLEppmRzbMAPb8J8hJXU	0
*17Cui3EPPfDDtzero3psqEjFQBbBcCuCh2	64.09157134
1DVRw3s4dXhYRqrex3Jo4LjatrXdzLErWX	0.90595414
*1LbvWiHtmdB4YCx9joaAG3q7VwLzoZbxrL	113.3983645
1Q9FTdf2pCEpMWMfS63G42aEWpTaCJWgUc	0.05944538
1EvbCsEzYZruqXEGEgM17TwVmGnFFmjfFU	0.00004774
*12eLiAEAqM6ME9MXA8B8iH7Re6CZ666q7s	158.3191376
*1G2Hvt8U2iSehUo7xeYhi5UEMYZH4kHV87	43.88168442
*1AfBS5JktqkEStGxsQBxCuw27M8VXLcegn	16.09563828
*128hGH8iEffuEmAEikvez1qneeqnqvZhWg	158.3191376

Table 4.4: Payouts for Malware Wallets linked to Eligius

*1E3zYD19djF4q99hVcTCNkUMrS7CBSzweV	139.3389039
*1JxZ1ZFRotC2c3RKiRP8FUavgivZjofdCr	26.97299129
*18MyygdhxCHa8yyMvNM9eVSUSSCnJenMQc	5.14275827
1PbPiV1X9x8MGPw2jdoZdypZ3wYAuZmL7h	28.2658766
*1K35n15e4pfMKaf3nt22pQg8RhXkrcef6m	61.91122602
*16PBTCQdPGdNAsz11GHK4X2Dic4AzpT3kr	16.77956342
*19zKypkzMmTF8UdXPZXgJPbHS2KAvb6XCE	0
1CzDdv9SSYmDqdhRqtEv8vYixnD22Z2qMT	0.07402819
*1G28x32bCqyevHRYcHP6gnSTpnqk5rLmfy	102.1192588
1ES11Ke5mxgz9MYiJ2Pb1MgY2FFYnfs5fA	52.33521919
17VJ4nebUbfBoydRC7vLynQruXyqMCDY1W	0.28116362
1PyoNmwdNP7PQWQwjCLiK8Av5V9eAGhKcL	0.54878984
*1ASNjJjUou6RPkmP81nJUuhbZDkxAaHQhX	420.0202668
15gXtYvFZaeZxz8aqfwHPhq6RBycoUxBoF	0
*1KkdapEbgWsuFsnfZz8ywu81T1aUpHfpbD	1.15421631
1NL9copk9NGwfA9k6z1gB7qLqzTmYDXofn	2.02461013
*1tKiADSZFTtdnrQagrharb1QRBZevhAJY	0
*12J2hosbVqDm1QBGTStqRTb3spdkJpHtiR	52.46483898
1AFVcMGK9dTRUAMD6YFPgqSU7whV99KpK7	14.95154188
50BTC	
139HogxWskiV8qmAmpMjwJC5tV8ZpZBgP6	0.1881046
1EytsdkqjFgoJRZpBGoXRgWq246mFDK6dp	0
Total Bitcoin from Malware	1917.835345 BTC

Further invetigations into these wallets by observing the block chain has shown us that bitcoins deposited into these wallets have been transferred into another set of wallets. Navigating further down the linked list of the block chain. It is observed that all the bitcoins

are eventually transferred to wallets that belong to bitcoin24, which is a bitcoin exchange. On 12th April 2013, bitcoin24 suffered an attack and has since suspended all operations. The fate of accounts created on bitcoin24, which also provided services for bitcoin storage, is unknown. An example of such transfers has been shown in Figure 4.2

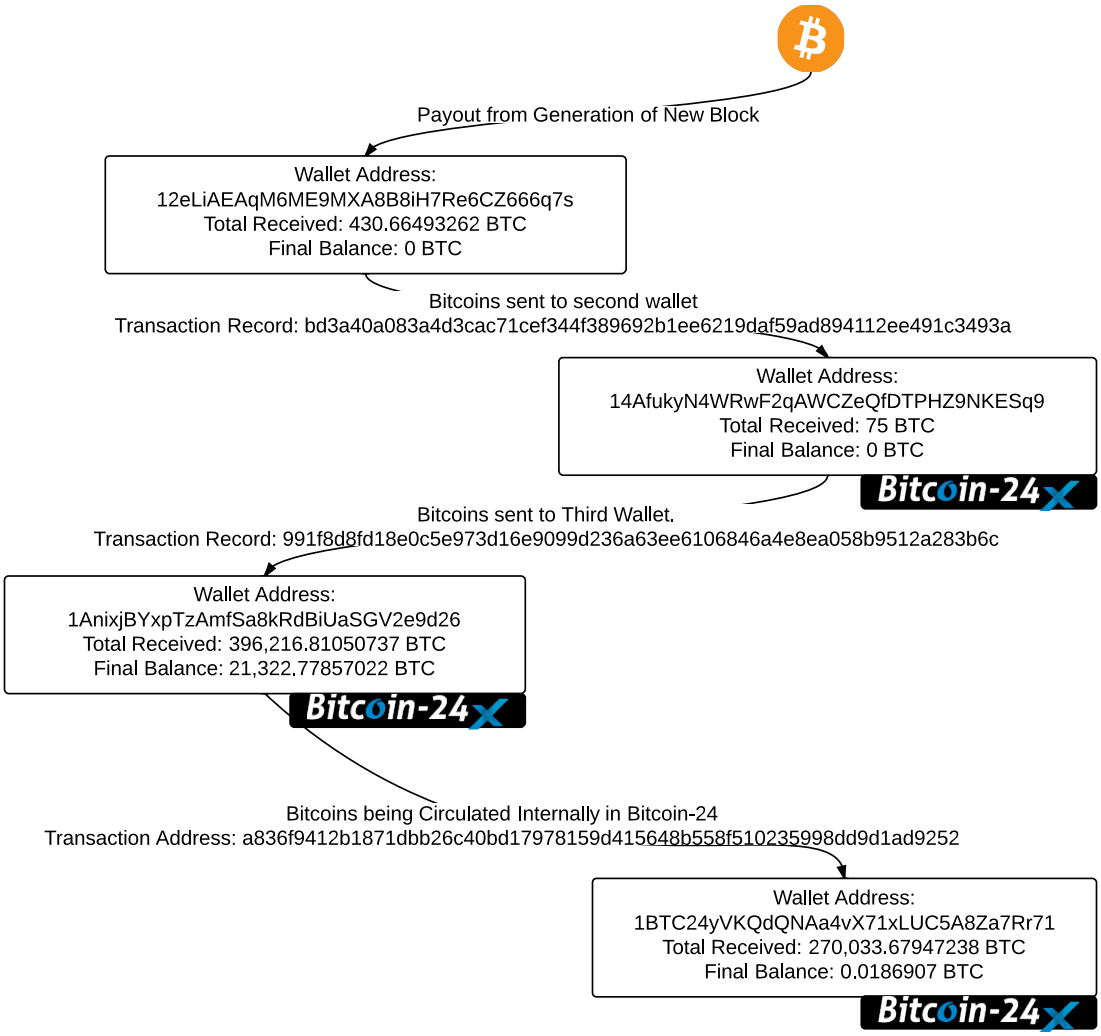

Figure 4.2: Cashing out of Bitcoins.

Wallet addresses with a tag of bitcoin24 indicate wallets that belong to bitcoin24. Since

bitcoin24 is an exchange, it provides services for cold storage of wallet such that they cannot be compromised. Hence in such a setup, it is familiar to find bitcoins being internally circulated within the wallets owned by the exchange. These transfers can also mean that the bitcoins have been cashed out into real world currency. However it is not possible to determine the transactions happening within the exchange without the help of the exchange operators.

50BTC also provides services for querying wallet information. The information provided by 50BTC is not as descriptive as the one provided by Eligius. But, nonetheless it gives us an insight into the amount of activity in malware-affiliated wallets.


```
{
   "user":
   {
      "confirmed_rewards":1.1055248600001
      "payouts":19.7416197
      "hash_rate":"4928.47"
      "active_workers":1
   }
   "workers":
   {
      "1":
      {
         "worker_name":"1KkdapEbgWsuFsnfZz8ywu81T1aUpHfpbD"
         "hash_rate":"4928.47"
         "shares":1780
         "stales":13
         "invalid":403
         "checkpoint_shares":0
         "checkpoint_stales":0
         "checkpoint_invalid":0
         "total_shares":6589107
         "total_stales":61372
         "total_invalid":312710
         "last_share":1366228301
         "blocks_found":3
         "alive":true
      }
   }
}
```


Figure 4.3: Results from 50BTC.

Wallet Address	No of Blocks Found	Total Earnings
13VdYJzQCGH7cMr9uWJKTZzDdn4cfDnWNn	0	20.74534453
1C8qRSmrzdy6rYFTxJnmgSoQJfFUADCZd8	7	240.96123811
1zPRh4V76nJG7gKSRFbgXkwQNAEaLg3Jt	10	276.88567775
15EeddVj5rr6zmLfH1M26KvFX5KKJh3xgt	2	26.710484
1NnKm4PxyU2VT4HYv4xhcdB8SN7FgxJvWb	0	4.31767762
1Azge5CfpHQP6keWgkHPvTcZzjHamuFRba	1	87.62399745
169TpR47JVcLaQXdGYE6Lv4Ps9DbVqHhSi	3	91.39938806
1JBv6w4ANiXmKAVLEppmRzbMAPb8J8hJXU	0	3.57991109
17Cui3EPPfDDtzero3psqEjFQBbBcCuCh2	2	56.45460725
1LbvWiHtmdB4YCx9joaAG3q7VwLzoZbxrL	3	82.40201278
12eLiAEAqM6ME9MXA8B8iH7Re6CZ666q7s	6	269.94341268
1G2Hvt8U2iSehUo7xeYhi5UEMYZH4kHV87	2	111.88501908
1AfBS5JktqkEStGxsQBxCuw27M8VXLcegn	0	9.50278382
128hGH8iEffuEmAEikvez1qneeqnqvZhWg	0	0.107744
1E3zYD19djF4q99hVcTCNkUMrS7CBSzweV	5	79.86288764
1JxZ1ZFRotC2c3RKiRP8FUavgivZjofdCr	5	156.1476703
18MyygdhxCHa8yyMvNM9eVSUSSCnJenMQc	6	59.71066072
1K35n15e4pfMKaf3nt22pQg8RhXkrcef6m	0	56.09093378
16PBTCQdPGdNAsz11GHK4X2Dic4AzpT3kr	1	48.0960167
19zKypkzMmTF8UdXPZXgJPbHS2KAvb6XCE	1	38.86354649
1G28x32bCqyevHRYcHP6gnSTpnqk5rLmfy	6	203.0483816
1KkdapEbgWsuFsnfZz8ywu81T1aUpHfpbD	3	19.7416197
1tKiADSZFTtdnrQagrharb1QRBZevhAJY	2	37.27761926
12J2hosbVqDm1QBGTStqRTb3spdkJpHtiR	8	201.10247129
13VdYJzQCGH7cMr9uWJKTZzDdn4cfDnWNn	0	20.74534453

Table 4.5: Payouts for Malware Wallets linked to 50BTC

1C8qRSmrzdy6rYFTxJnmgSoQJfFUADCZd8	7	240.96123811
1zPRh4V76nJG7gKSRFbgXkwQNAEaLg3Jt	10	276.88567775
15EeddVj5rr6zmLfH1M26KvFX5KKJh3xgt	2	26.710484
1NnKm4PxyU2VT4HYv4xhcdB8SN7FgxJvWb	0	4.31767762
1Azge5CfpHQP6keWgkHPvTcZzjHamuFRba	1	87.62399745
169TpR47JVcLaQXdGYE6Lv4Ps9DbVqHhSi	3	91.39938806
1JBv6w4ANiXmKAVLEppmRzbMAPb8J8hJXU	0	3.57991109
17Cui3EPPfDDtzero3psqEjFQBbBcCuCh2	2	56.45460725
1LbvWiHtmdB4YCx9joaAG3q7VwLzoZbxrL	3	82.40201278
12eLiAEAqM6ME9MXA8B8iH7Re6CZ666q7s	6	269.94341268
1G2Hvt8U2iSehUo7xeYhi5UEMYZH4kHV87	2	111.88501908
1AfBS5JktqkEStGxsQBxCuw27M8VXLcegn	0	9.50278382
128hGH8iEffuEmAEikvez1qneeqnqvZhWg	0	0.107744
1E3zYD19djF4q99hVcTCNkUMrS7CBSzweV	5	79.86288764
1JxZ1ZFRotC2c3RKiRP8FUavgivZjofdCr	5	156.1476703
18MyygdhxCHa8yyMvNM9eVSUSSCnJenMQc	6	59.71066072
1K35n15e4pfMKaf3nt22pQg8RhXkrcef6m	0	56.09093378
16PBTCQdPGdNAsz11GHK4X2Dic4AzpT3kr	1	48.0960167
19zKypkzMmTF8UdXPZXgJPbHS2KAvb6XCE	1	38.86354649
1G28x32bCqyevHRYcHP6gnSTpnqk5rLmfy	6	203.0483816
1KkdapEbgWsuFsnfZz8ywu81T1aUpHfpbD	3	19.7416197
1tKiADSZFTtdnrQagrharb1QRBZevhAJY	2	37.27761926
12J2hosbVqDm1QBGTStqRTb3spdkJpHtiR	8	201.10247129
Total Earnings		4364.9222114

The wallet shown in Figure 4.3. is known to be associated with two mining pools. 50BTC and Eligius. The different pool statistics show that this wallet is being used with

both pools, as the statistics differ, we can clearly see that this wallet is being primarily being used with Eligius. Statistics on eligius show us that this worker has been mining at the rate of 3.4 MHash/s, which is relatively low. It is also seen that this wallet has been used very recently and Eligius does not show payouts for this wallet before April 2013. This helps us observe a trend where in wallets that have been used for a while can be discarded by malware authors in order to maintain anonymity. Changing wallets frequently provides some degree of anonymity but as seen in Figure 4.2 when such infrequently used wallets combine all their bitcoins into a exchange wallet. It becomes easier to identify payouts as we know that all payouts shall be directed to an exchange wallet by observing the block chain.

Although the information provided by 50BTC is limited in nature as compared to eligius. It gives us ground truth about the number of blocks mined by wallet addresses. 50BTC also reports the state of the malware wallets as being active or inactive. It has been seen that some wallets marked as inactive still maintain active working state with the Eligius mining pool. We have confirmed that the aforementioned wallets have mined a total of 146 blocks with 50BTC and have earned a total of 4364.9222114 BTC as payouts. The collective hashing power for currently active logins is known to be 9642.2 MHash/s.

4.2 Reversing Merkel Roots

A single block can be found by only one pool. As per the bitcoin protocol. Once a block is found, the network moves on to find the next block. Due to the race of solving a block, all the nodes in the network are working on the same block until it is found. Once a block is found it is announced to the network and a verification of the proof-of-work accepts that block and a reward of 25 BTC forms the first transaction of the next block. Unless pools themselves announce the result of mining blocks. There is no public record for pool-block associations. We have developed a method to determine such associations.

We take advantage of the fact that when a miner client calls getwork. As we know that the response of getwork contains a H which is a SHA-256 hash of S; the internal state (i.e.

Merkle tree) and the internal nonce N (i.e. coinbase). The value of N changes for every invocation of getwork. Thus by invocating getwork at a regular interval of 1 second, we accumulate all values of H for different values of N since we know that the merkel tree hash will change only when the block corresponding to the getwork is solved. This method also leverages on the fact that the response to getwork remains consistent in the sense that all nodes in the pool are solving the same block and hence by definition working on close versions of the getwork response value. This provides us with a table for every pool with its corresponding H; giving us a history of getwork responses and their changes per second. Repeating this over a large period of time gives us data for the next step.

As we know the blocks that are already mined from the bitcoin public record. These records provide us with the accepted values for the nonce N_{mined}, the new internal state S_{mined} and thus the hash $H_{mined} = hash(n_{mined}, S_{mined})$ for that block. If we can find the value of H_{mined} in our table of getwork responses, we can determine the pool. That said, It is possible that due to the narrow range of collected values vs. the actual enumeration of all values of H that were possible, It would be more often than not required to recomputed the values of H for different values of n that were calculated prior to obtaining n_{mined}. It is observed that the change in the value of n follows a predictable pattern. By permuting over all possible values at the altered bit positions we are able to construct all possible ns . Thus by performing the hash H' for every value of n' over the same S_{mined} as $H' = hash(S_{mined}, n')$. If we arrive at a collision of H' with any value in our table, we have mimicked mining process backwards to identify the pool.

As the bit positions have to be flipped once for every altered bit in n hence this method has a running time of $O(2^n)$. Even with this efficiency we are able to prove that dns.domain-crawlers.com claims to have solved the same block as pool.50btc.com. Indicating that the former is a proxy to the latter. It is also to be noted that domain-crawlers.com and pool.50btc.com have 3 login credentials that work interchangeably. This was possible due to the low entropy in the amount of needed bit flips. The search space for the (2^n) blowout can be decreased by performing a computation that shall give us the coin base transaction

closest to the coinbase in the block transaction reward. Thus by concentrating our reverse mining process on the closest coinbase, it is possible to reduce our search space.

With the current method we are able to establish that dns.domain-crawlers.com has been proxying to pool.50btc.com and pool-de.50btc.com (50BTC domain specific to Germany). We are able to conclude on the above on the grounds that the login credentials that are created by any user on 50BTC can also be used to login into dns.domain-crawlers.com, credentials from other pools and random usernames and passwords are not accepted hence confirming that credentials are indeed being checked. Also, our reverse mining has shown that block number 225570 was mined by domain-crawlers, pool.50btc and pool-de.50btc whereas the blockchain information show us that the block was claimed by 50BTC; 50BTC also claims that they mined the block as shown in Figure 4.4. The payout addresses for the mined block point to a wallet address belonging to 50BTC hence telling us that dns.domain-crawlers.com is indeed a proxy to 50BTC.

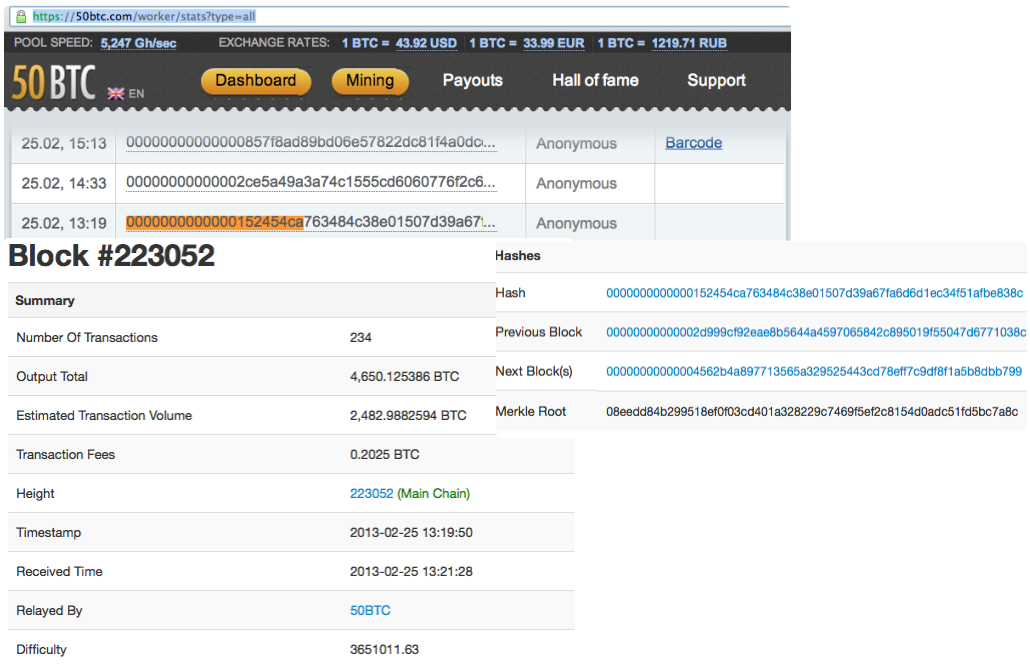

Figure 4.4: Domain Crawlers block claimed by 50BTC.

4.3 Inducing Signals in Malware wallets

As we have seen in the previously, in the case where a botnet owner is using the proxy method for mining, it is hard to determine the payouts for the botnet miner as there will be a condition where the proxy and the actual light pool being proxied will announce the same block. It is up to the network to determine which block gets accepted. The block whose proof-of-work gets verified first shall be the one to win the reward.

As of this writing it is known that the there is a block confirmed in the network roughly every 10 minutes. With our goal to determine the payouts and the addresses of the wallets to which these payouts are directed to, It is required to monitor all the payments in the bitcoin network per block. Such reward transactions are very common, hence it is very difficult to point to a single transaction in the network. We have developed a technique by which pointing out to rouge transactions would be possible. We try and introduce a rise in the amount of payments received by wallets that appear in blocks on a daily basis. This requires us to perform mining on the part of the malware. Continuous mining for a 24-hour period with two Radeon graphics cards that are capable of computing more than 1.1 GHash/s together shall cause an increase in the payouts to the wallets being monitored. Currently we are able to produce The increase in the payouts to the wallets following the days of our mining is a strong indicator of the wallet being associated with a botnet owner.

It is also to our disadvantage that the induced signal can be confused in the deluge of noise. Especially with the growth of bitcoin, more peers have joined the network increasing the total hashing rate of the network, increasing speed of block generation, increasing the amount of transactions and hence the noise. The strongest signal indicator can be induced if an Application Specific Instruction Circuit system would be used for performing mining operations as ASICs are capable of computing more than 65 GHash/s.

Our approach assumes that payouts that occur from one login are sent to one wallet address hence having only one output wallet as a transaction in the coinbase. When the payout of mined coins is sent to multiple addresses, the effort of our mined signal will be reduced by the number of entities in the output of the new coinbase. This signal shall be

impossible to find since we will never see an increase in one wallet and rather there will be a marginal increase in many wallets.

Chapter 5: Future Work

By identifying proxy-mining pools, it has been possible to enumerate the accounts and hence co-operation with pool operators shall help curb theft of CPU cycles on victim computers. Our goal is to completely understand the adversaries in the bitcoin malware ecosystem and determine their mining operations. We are confident in finding more wallet addresses and malware usernames to build and more distinctly correlate the different adversaries in the ecosystem. More broadly, it would be interesting to find the usage of malware-mined bitcoins in the real world. Questions regarding the usage of bitcoins in conjunction with Silk Road have been brought up and we believe that future work shall give us more insight into the nature of such activities.

Improving our methods of analysis also remains a challenging problem. Reducing the search space intelligently shall help us in finding malware wallets in reasonable time. Since the problem currently revolves around enumerating the hashing address space it is computationally intensive. The results from analysis has shown us that the search space can be limited to getwork requests that are retreived sixty seconds before the block has been solved. Thus by reducing our target area, We hope to be able to confirm proxying instances of other dark pools beside domain-crawlers.com

It is also in our interest to use statistics offered by pools such as Eligius to statistically determine the nature, size and location of bots in the botnet. A more irregular hash rate might indicate that the bots being used belong to Asian countries as they are known not to be online for extended periods of time and also that the bots belonging to those countries have a lower price per infection on the underground market. However proving such assumptions is considered future work.

With our eventual goal being to find mechanisms to blacklist and intervene on such mining operations. We also focus on finding effective methods of interventions. Interventions

to mining are possible at the domain level by which domains belonging to dark pools can be shut down at the registrar level. However this does not botnet owners to use public pools or proxying mechanisms to perform mining, For the cases above, It would be more effective to blacklist usernames and wallet addresses shall stop mining at the public pools. Since usernames from blacklisted malware are sent in clear text, collaboration among pool operators shall make sure that wallet addresses associated with tainted workers are not processed for payouts hence thwarting attempts made by botnet owners to use public pools.

A cost benefit analysis would be a primary way to determine the depth of malware in bitcoin, Calculating the cost of infections and corelating it against the amount of time a compromised machine is online before it is cleaned of infections indicates if mining through compromised machines remains profitables. Such end-to-end analysis shall also help us in understanding how bitcoin is traded as a commodity in the underground market rather than a currency.

Lastly, It is also in our interest to examine how much bitcoin mining was done by previously known botnets such as Zero Access. Although the domain name google-updaete.com was known to be used with Zero Access bots, there is no evidence of actual bitcoin mining being performed by using this domain except for SIE data indicating DNS lookups, which is limited to only one Internet Service Provider. Investigations into such areas shall reveal more about the underlying bitcoin economy and probably also reveal the hidden owners of the newly found crypto currency

We are also actively looking to investigate mechanisms of interventions at the pool level such as blocking IPs that perform bitcoin mining from registering to the pools, This shall stop proxying bots. A large section of botnet miners can be stopped by blocking workers from pools since it is seen that malware uses one worker in multiple infections. Disallowing suspicious IPs from anncouncing and claiming blocks can also be analyzed for intervention into such crimes.

Chapter 6: Anecdote

This study has revealed interesting properties in the bitcoin system, and how cyber criminals are leveraging on it. Firstly, with the ability to buy compromised machines it is easier than can be thought of to create ones own mining pool. Umawing [15] reported spread of Win32/Fareit; Malware known to spread through rouge websites that leverages on the victim through the Blackhole exploit kit to drop a mining bot.

Secondly, It is seen that malware distribution is being done with login information that is crated by the cyber criminals on public pools such as 50BTC showing that malware mining is happening in the open and there are currently no methods of reporting and stopping such mining activities. A good starting point would be to blacklist pool accounts that are derived from malware.

Tracking botnet behaviour is a race, As more and more malware is being released everyday, the starting point would be to find malware samples and categorize pools that it belongs to and identify wallet addresses to which profits are being paid. Intervening on such levels makes it harder for the botnet masters to create new wallets rapidly as the cash out will require them to send bitcoins to wallets that belong to an exchange.

Chapter 7: Conclusion

Our results are favorable in establishing our premise that mining by malware is very much active. They offer conclusive glimpses into the mining and distribution of such malware. Our results have also shown us that there is a new dimension to monetization due to malware. Also, results as seen by in Grier et al. [16] makes us believe that the possibility of such an attack is very much within the reach of cyber criminals. We have also established the connections between dark pools and light pools. With help in kind from pool operators it has also been possible to find the behavior of mining operations. This has shown us that malware authors could send different payouts to a unique address and hence distribute their earnings at the payout level. We have also found success in tracing wallets being sent to exchanges where they could be stored or cashed out. We have also determined collective earnings from all malware to be approximately 6282 BTC($640,764). Although these earnings correspond to less than 20% of the login information we have collected which tells us that we have just scraped the surface. Additionally, These logins are known to be associated with malware and not with bot networks. So it would be possible to see higher payout information when wallet addresses of bot owners are revealed due to our reverse mining technique.

Secondly, It is also to be noted that 50BTC allows direct deposits of bitcoins to WebMoney accounts. With the help from the pool operators of 50BTC it was possible to relate logins and wallet addresses. It is found that username *dragonson@list.ru_gunshop* is associated with wallet address 1JB6ssTD2dxHF4JdworNRKNwmUmn6A2GVX which is also linked to a WebMoney account with reference number R469779967727. This also makes us believe that apart from malware authors using exchanges such as bitcoin24. WebMoney can be used to cash out bitcoins. Figure shows one example of malware miners using WebMoney. In this case wallet address mentioned above(i.e. 1JB6ssTD2dxHF4JdworNRKNwmUmn6A2

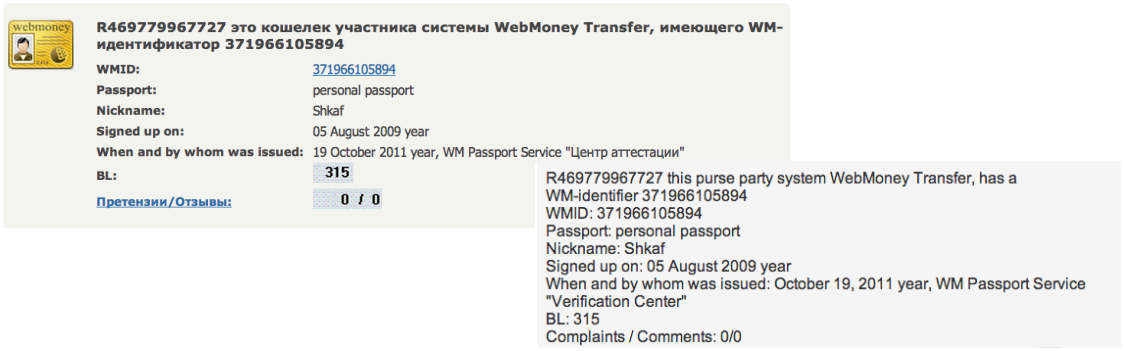

Figure 7.1: 50BTC Malware wallet using Webmoney.

GVX) is associated with WebMoney account R469779967727; having a reputation of good reputation of 315. Hence it is not possible to intervene in the case of such mining operations unless pool operators are willing to act on malware logins by providing inside information.

Thirdly, Matching domain name records of dload.asia domains. It is seen that the dark pool compromises of a group of people. It is possible to say that because it has been observed that until February 2011. Pools dload.asia, m94vo3.com and xD.x3x9.asia had different operations. Regular monitoring shows us that from March 2013 to April 2013. All these domains resolved to the same IP address. This meant that all login credentials could be used interchangeably and hence showed us that dload.asia was a conglomerate of mining pools. However as of this writing it is seen that the domain name records have changed and these pools now mine independently. The TTL for the domain name record of xd.x3x9.asia is 300, which indicates a fast flux situation. We have also observed frequent changes in IPs belonging to the domain. As a part of further domain name investigations we also know that the email address that was used to register the domain name of dload.asia was also used to register the domains x1x2.in and mobinil.biz all belong to an alias of *redem*.

As the landscape of bitcoin continually changes, we have also observed new logins and malware being introduced daily. This makes us fairly condident about the existence of such illegal activites. We are positive of our results as they offer glimpses into the distribution

and mechanisms of mining malware, and into the relationships between various pools.

Bibliography

[1] Alistair Charlton. Bitcoin traders robbed as mt. gox exchange attacks continue. *International Business Times UK*, 2013. URL `http://www.ibtimes.co.uk/articles/456466/20130412/bitcoin-exchange-ddos-attacks-continue-traders-robbed.htm`.

[2] Jeremy Kirk. Bitcoin storage service, instawallet, suffers database attack. *IDG News Service*, 2013. URL `http://www.techhive.com/article/2033044/bitcoin-storage-service-instawallet-suffers-database-attack.html`.

[3] Bianca Dima. Exchange site bitcoinica hacked, usd 90,000 stolen. *HOTforSecurity*, 2012. URL `http://www.hotforsecurity.com/blog/exchange-site-bitcoinica-hacked-us90000-stolen-1719.html`.

[4] Félix Brezo and Pablo G. Bringas. Issues and risks associated with cryptocurrencies such as bitcoin. In *Proceedings of The Second International Conference on Social Eco-Informatics*. Think Mind, IARIA, 2012.

[5] Elli Androulaki Ghassan O. Karame and Srdjan Capkun. Double-spending fast payments in bitcoin. In *Proceedings of the 2012 ACM conference on Computer and communications security*. ACM Press, 2012.

[6] Sergio Martins and Yang Yang. Introduction to bitcoins: a pseudo-anonymous electronic currency system. In *Proceedings of the 2011 Conference of the Center for Advanced Studies on Collaborative Research*, pages 349–350. ACM, 2011.

[7] Dmitry Bestuzhev. An avalanche in skype. *Securelist - Information about Viruses,*

Hackers and Spam, 2012. URL http://www.securelist.com/en/blog/208194206/An_avalanche_in_Skype.

[8] Harrigan M. Reid F. An analysis of anonymity in the bitcoin system. In *IEEE Third International Conference on Privacy, Security, Risk and Trust*, pages 1318 – 1326, 2011.

[9] Stefan Ortloff. Botnet shutdown success story - again: Disabling the new hlux/kelihos botnet. Technical report, Kaspersky Labs, 2013. URL http://www.securelist.com/en/blog/208193431/.

[10] Daniel Plohmann and Elmar Gerhards-Padilla. Case study of the miner botnet. In *Proceedings of the 4th International Conference on Cyber Conflict*, pages 1 – 16. NATO CCD COE Publications, 2012.

[11] FBI. Bitcoin virtual currency: Unique features present distinct challenges for deterring illicit activity. Technical report, Directorate of Intelligence, Fedral Bureau of Investigation, 2012. URL http://cryptome.org/2012/05/fbi-bitcoin.pdf.

[12] Dmitry Bestuzhev. Skypemageddon by bitcoining. *Securelist - Information about Viruses, Hackers and Spam*, 2013. URL http://www.securelist.com/en/blog/208194210/Skypemageddon_by_bitcoining.

[13] James Wyke. The zeroaccess botnet - mining and fraud for massive financial gain. Technical report, SophosLabs, 2012. URL http://www.sophos.com/en-us/why-sophos/our-people/technical-papers/zeroaccess-botnet.aspx.

[14] Eligius. Eligius pool mining statistics, 04 2013. URL http://www.eligius.st/~wizkid057/newstats/userstats.php/.

[15] Jovi Umawing. Fareit goes bitcoin mining. *ThreatTrack Security Labs IT Blog*, 2013. URL http://www.threattracksecurity.com/it-blog/fareit-goes-bitcoin-mining/.

[16] Chris Grier, Kurt Thomas, Lucas Ballard, Juan Caballero, Neha Chachra, Christian J. Dietrich, Kirill Levchenko, Panayiotis Mavrommatis, Damon McCoy, Antonio Nappa, Andreas Pitsillidis, Niels Provos, Zubair Rafique, Moheeb Abu Rajab, Christian Rossow, Vern Paxson, and Stefan Savage. Manufacturing compromise: The emergence of exploit-as-a-service. In *Proceedings of the 2012 ACM conference on Computer and communications security*, 2012.

[17] Bitcoin charts, April 2013. URL `http://bitcoincharts.com/`.

[18] Bitcoin wiki, April 2013. URL `https://en.bitcoin.it/wiki/Main_Page`.

[19] Simon Barber, Xavier Boyen, Elaine Shi, and Ersin Uzun. Bitter to better - how to make bitcoin a better currency. In *Financial Cryptography and Data Security*, 16th International Conference, FC 2012, pages 399–414. Springer Berlin Heidelberg, 2012.

[20] Satoshi Nakamoto. Bitcoin: A peer-to-peer electronic cash system. 2009. URL `http://bitcoin.org/bitcoin.pdf`.

[21] Peck M.E. The cryptoanarchists' answer to cash. In *IEEE Spectrum*, volume 49, pages 50 – 56. IEEE, 2012.

[22] Moshe Babaioff, Shahar Dobzinski, Sigal Oren, and Aviv Zohar. On bitcoin and red balloons. In *Proceedings of the 13th ACM Conference on Electronic Commerce*, pages 56–73. ACM, 2011.

Hitesh Dharmdasani

http://mason.gmu.edu/ hdharmda/

hdharmda@gmu.edu

(703) 409 - 9135

Education

M.S. Information Security and Assurance — GPA 3.76/4.00 *May 2013*
George Mason University, Fairfax, VA

B.E. Computer Science and Engineering — GPA 3.83/4.00 *June 2011*
KLS Gogte Institute of Technology, Belgaum, Karnataka, India

Career History

Graduate Research Assistant under Professor Damon McCoy, *George Mason University Spring 2012 - Present*

- Actively researching Malware, Botnets and Cybercrime.
- Working with contained malware analysis, Using PostgreSQL for data analysis, Clustering Malware according to behaviour, Data gathering using web crawlers and analysing the underground economy

Developer Intern, *eth1 network solutions* *Fall 2010*

- Designed a web service for the real estate market. Implemented in Python using Django.
- My responsibilities were to develop core funtionality, Integrate google maps API and deploying the web application

Selected Publications

Damon McCoy, Hitesh Dharmdasani, Christian Kreibich, Geoffrey M. Voelker and Stefan Savage. "**Priceless: The role of payments in abuse advertised goods**," in *Proceedings of the ACM Conference on Computer Communications Security.* 2012.

Skills

Programming: Python, HTML/CSS, bash, PHP, SQL, C, Assembly, Java, C#

Operating Systems: Windows, Mac OS X, Linux

Other VMware ESXi, Bro IDS, Selenium, Mechanize, BeautifulSoup, Metasploit, Wireshark

Projects

Masters Thesis, *Malware Botnets and Crypto currency* *Spring 2012 - Present*

- An analysis of bitcoin, the de-centralized crypto currency and the effect of malware and botnets on its economy
- Analysis of web page redirection w.r.t the ZeroAccess Botnet
- The effect of interventions into the sale of abuse advertised goods

Android Rootkit *Spring 2013*

- Developed a rootkit in C for the android kernel. Capable of hiding files, processes, open ports and providing a reverse shell

Service Specific Intrusion Detection, *Fall 2012*

- Developed in Python. The aim of the project was to provide intrusion detection capabilities in a non-memory intensive manner.

Malware Identification Crawler, *Fall 2012*

- Developed a web crawler in Python that makes use of the Google search API to find MD5's malware by giving keywords. Malware corresponding to the keyword can be later obtained for analysis

Buffer Fixed Length Obfuscation in OpenSSH, *Spring 2012*

- Made OpenSSH secure against side channel attacks when used in tunnel mode using C. Changed the implememtion of packet exchange between a client and tunnel endpoint to send packets at fixed intervals and improvised on uniform packet size distribution