Bitcoin Mining based Botnet Analysis

Pallaw Singh Aswal
Department of Computer Science and Engineering,
Uttaranchal University,
Dehradun, India

Anchit Bijalwan
Department of Computer Science and Engineering,
Uttaranchal University,
Dehradun, India

ABSTRACT
Bitcoin, a decentralized P2P currency in recent years has gained a tremendous attention due to its ability to create anonymous financial transactions. This leads to bitcoins being the choice of currency for users having privacy as a important issue. Bitcoin mining, a process resulting in the generation of new bitcoins, is performed by miner operators for reception of incentives in the form of Bitcoins. To increase the profit this has given rise to bitcoin mining through botnet also known as miner botnet. In this paper we discuss how bitcoin are generated and how botnet generate bitcoing.We further analyze the network flow of two botnets namely Neris and ZeroAccess and provide a DNS relation in identifying the botnet. We further propose a framework and a security algorithm to protect our system from being a part of botnet thus protecting our system form attacks such as spamming , non- availability, DDoS etc.

Keywords
Botnet, Botmaster, Bitcoin, SHA-256, bitcoin mining, mining pool

1. INTRODUCTION
Bitcoin is an electronic form of currency which is not supported by any form of real asset. Bitcoins are not under control of any form of organization or by any form of governmental authority. Bitcoins transactions are based on an algorithm whole structure is a decentralized P2Psystem [1].Bitcoin was originally formed to eradicate the transaction costs which are created when intermediate parties have to resolve disputes and validate transactions. Bitcoin overcame this by using a system where validation of transactions is done by all of the other bitcoin users who work together, thus creating a public chain of record of custody for each bitcoin [2].The users can use their bitcoin currency through wallets which are electronic in form , which they can keep on their computers to reduce the risk of theft or they can also store bitcoins in wallet through an online wallet [3].Key-pairs set of private and public keys are the base of Bitcoin Wallets. The private keys are used to authorize transactions while the public keys generate an address, essentially a string of letters and numbers approximately twenty seven to thirty four characters long. No information is stored in addresses about the user; on the other hand public keys can be used
to track the transactions that happened [4].The identity of the bitcoin user always remains anonymous but the bitcoin itself can be traced through the chain of every addresses that hold it. Every bitcoin contains a history of time-stamped of transactions where it moved from one address to another [5]. A transaction is time-stamped when it commits and protecting it from any changed later. This notarizes the transaction and thus preventing the bitcoins from being duplicated or spent twice. Currently there are more than 10.7 million bitcoins in exist and is gradually increasing day by day [6]. Bitcoin took a peak in September of 2012, reaching more than 60,000 users. But this amount got constant to 20,000 user later on [7].The Demise of Bitcoin due to system vulnerabilities has been predicted by some people but they are mistaken [8].Instead Bitcoin is feasible for those who seek unlawful acts such as purchase of guns or drugs illegally online, international terrorist agendas or sponsor domestic, or even hire a hit man in anonymously.
Nowadays, main threats that the Internet users face are botnets [9]. Botnets are used for all sorts of unlawful activities e.g. personal data theft, spam, bitcoin, DDoS, cyber, bitcoin mining etc. [10]. In recent years we have seen a constant growth of botnets [11].

Botnets are networks of centralized Command-and-Control (C&C) servers which act as the singular point of control for its network. Botnets having a centralized type of structure are easily to control and maintain. The Botmaster uses its C&C server to communicate with its network of bots. This type of architecture, however has an important drawback that the centralized C&C servers have a single point of failure. This means whole botnet is defeated if we are able to taking down the C&C servers. To overcome this problem, bot masters have moved to a more advanced network structure that is a P2P network. The P2P botnets remove the single point of failure due to its distributed network thus making the disruption of the botnet much harder. In this type of network structure, the bots of the botnet network exchange commands among themselves.

Some of the bot master still use a centralized form of network but side by side implement techniques to reduce the chances of detection. One of the ways to achieve this is through the use of a Tor-network (Onion routing protocol). Using the Tor-network, the bot-master are able to locate their C&C servers anonymously. The tor network provides anonymity to its users by creating an encrypted routing system to allows publishing of services and avoid traffic analysis without revealing their locations. To do so, Tor networks provide services known as hidden services. Hidden services are characterized by services like shell providing services, web servers and others which can be accessed using the Tor-network [12]. Due to this the clients using the service do not require the actual address that is actual location of the service thus ensuring service anonymity. Bot-masters can set the C&C servers as hidden services making it impossible to detect the C&C locations thus the take down the botnet becoming more difficult. While the bot master tries to hide its network, it also exposes the same due to peculiar properties of the Tor network. Such technique are still not being actively deployed for P2P botnets, but it is fully applicable and could in fact, provide further resistance in take down attempts. It has been noted for a few time that a botnet's combined computing power can be used for variety of villainous functions. we are able to currently add bitcoin mining to it list [13]. Through the use of pooled bitcoin mining, a botnet master might covertly mine Bitcoins using the processing power of a victim's system. Miner Botnet does this by installing bitcoin Mining software of to the victims System such as CGMiner etc. Once its installed on victims system it is

made to run in background using the processing speed of CPU and GPU of its host to mine bitcoin. The Mining software installed is made to join a pool which can be either public pool or dark pool. In public pool the Botnet has a chance to get detected and banned. In Dark pool there is no threat as seen in public pool but the Botmaster has to take the added construction and maintenance of the dark pool on him [14]. Once the pool has been joined all the bots under the control of the Bot master start mining bitcoin using the bot masters bitcoin wallet to save the mined bitcoin. Another point of the bitcoin currency is its apparent anonymity, beside decentralized authority spread across a peer-to-peer network; this makes the currency even more appealing to cybercriminals. Using an average pc and solely were ready to compute roughly one mega-hashes/second. In this paper section 1 deals with introduction, section 2 comprises of literature survey, section 3 with methodology, traffic analysis is discussed in section 4, our proposed idea and result are shown section 5 and lastly section 6 contains the conclusion.

2. LITERATURE SURVEY

Reid et al. [15] carried out an important analysis of anonymity in bitcoin, advocating the creation of appropriate tools to associate many public-keys with each other, and with external identifying information. Every activity of known users can be observed in detail only by using passive analysis, but the authors take into consideration active analysis also, where an interested party can deploy a Bitcoins and with other users to discover even more information.

Moser et al. [16] focused on analyzing mixing services, such as Bitcoin Fog, that claim to kill the details related to origin of transactions, thus increasing the anonymity of its users. Stock et al. [17] analyzed the topology and dynamics of the Bitcoin transaction graph, detecting structural patterns that have implications for the anonymity of users in.

Meenakshi et al. [18] paper outlines the technique of Botnet forensic analysis and its implementation. The specific research gaps present in his implementation are presented as challenges later on in this paper. Based on previous digital forensics models a generic process for botnet forensics is proposed. The work done by the author is presents as an overview on implementation and botnet forensics analysis which will be more important for security.

Anchit et al. [19] has discussed about Random-UDP flooding attack being a different type of attack in which the attacker sends multiple UDP datagram of different sizes at a time caused a DDoS attack and thus further proposed a technique for the forensics of Random-UDP flooding attack. His tried to get close to the source of such attacks. The proposed technique is capable to knowing the source of Random-UDP flooding by a bot attack.

Christin et al. [20] collected precious information about the Silk Road State of the art, goals and challenges For the seizure by the FBI.

Meiklejohn et al. [21], stressed the investigating on use of Bitcoin for criminal purposes at scale. This is done by using a small number of manually labeled transactions and thus the authors were able to identify interactions and the institutions between them and thereby demonstrated that this approach is able to have considerable insight on the structure of the Bitcoin economy and how Bitcoin are used.

Reid et al. [22] downloaded the public transaction block chain and used this method to cluster Bitcoin addresses into users. To prove this they created two networks and analyzed its topologies by modeling the flow of bitcoins among users and transactions. Thus showing how these graphs, along with external data from form posts, can be used to track a target (a thief).

Ron et al. [23] mirrored Reid and Harrigan's two-graph solution when analyzing typical behavior of entities on a Bitcoin network, which includes how these entities acquire and spend bitcoins and also how they move their funds found to protect their privacy.

Androulaki et al. [24] approach was using data collected in a university setting from a simulation of bitcoin usage .The authors used Hierarchical Agglomerate Clustering and K-means to tie together behavioral similarities. Clustering is also done to inputs with outputs based on their own heuristic.

Guofei et al. [25] also used input and output clustering to create a list of known Bitcoin addresses for each party, which actively interacted with other parties on the Bitcoin network, using this data to assign identities to their clusters. At the end it uses the flow analysis to study interactions among users.

3. METHODOLOGY

For proper results the process need to work in a systematic way as following. The methodology section having five steps as shown in Fig 1.

1. Setting up the Environment: This step is about creating a virtual operating system (VMware) so we can capture the functioning of the malware without damaging our true OS.
2. Running Malware: This step deals with running the malware on the virtual OS and capturing its activity using different tools such as Advance task manager & wireshark.
3. Analyzing the Data: This step deals with Analysis of the data captured in step second. The captured data is seen for abnormal traffic, packets sent to unknown ip addresses, data in packets etc.
4. Result: The result is generated by the analysis of the data. The different findings we find are posted as the result of the experiment.
5. Conclusion: Finally, the research got a conclusion which is based on all the above steps and what we have figured out from it.

It is accompanied with documentation briefing about every step and parameters we took.

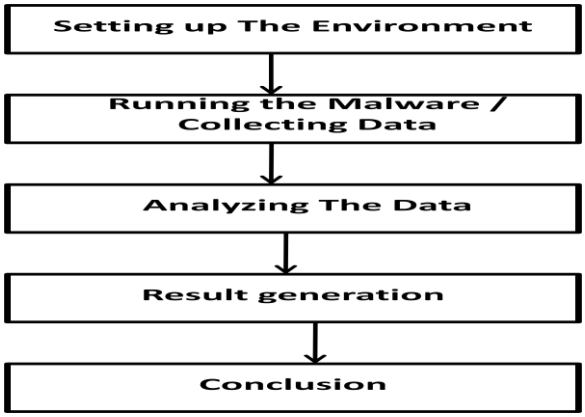

Fig 1 : Research Methodology

4. BITCOIN BOTNET TRAFFIC ANALYSIS

In this section we have analyzed the Pcap files of a Botnet known as Neris and ZeroAccess. On analysis of general traffic we see there are DNS queries generated to request for the IP address of some site. We then get a reply to the DNS query as a DNS answer packet sent by the DNS server with the answer field containing the

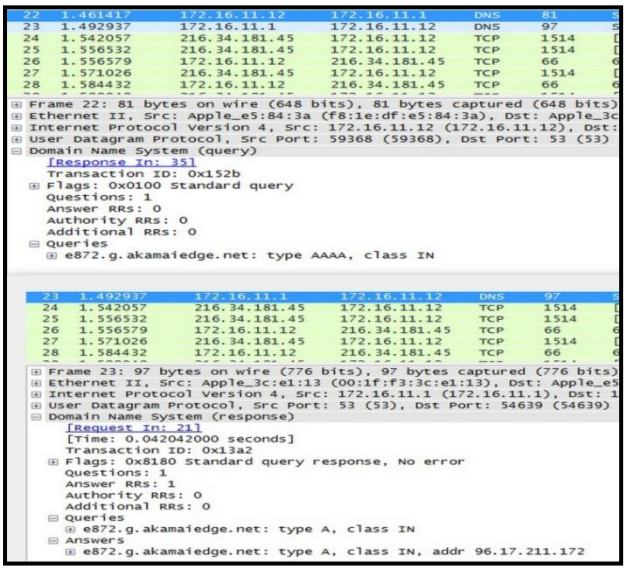

Fig 2: A normal DNS Request and reply

Answer to the query (IP address of the websites). Figure 2 describes a normal DNS request and reply and Figure 3 and Figure 4 describe a DNS request and reply generated from a compromised system, part of the Bitcoin.

4.1 Normal Traffic

In normal traffic the DNS reply contains one to three IP addresses as the reply of the DNS query. As seen in Figure 2 where the DNS query from IP address 172.16.11.1 was satisfied with the DNS reply with a single entity in answer field of the reply.After Receiving the DNS reply we now know the IP address associated with the website and now we can start connecting using this IP address.

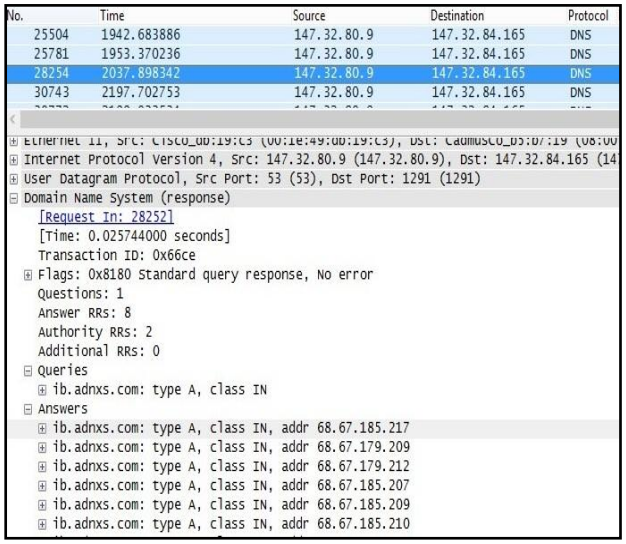

Fig 3: DNS request and reply generated from a Compromised system by a Neris botnet.

4.2 Anomaly Traffic

In case of botnet there are a number of servers from which the bot can communicate as not to have a single point of breakdown and thus not be destroyed easily incase authorities take down one or more of its servers. For this reason the botmaster establishes many C&C server's whose addresses are relayed to the bot as an reply for its DNS query. When a DNS reply has more than seven to eight answer in the answer field it can be possibly be a botnet related DNS query generated by our compromised system (bot) as seen in Figure 3 of Neris Botnet (IRC Type).

It downloads a Trojan file Trojan.Obvod from the compromised website. This Trojan has the ability to change url and redirect to its choice of sites as well as download and install software.

The Software downloaded is a bot program responsible for redirectional spamming and Bitcoin Mining. Further communication is done after bot program installation which needs data (configuration file) from the C&C server and thus knows the details of the attack that needs to be carried out.

Once the DNS query is satisfied the bot program starts to connect to the C&C server, as explained earlier that is third phase of botnet life cycle. Once connected the bot program awaits for the botmaster command. This may in time lead to a downloading of some modules to update the bot program or downloading of a configuration file which gives the details of an attack to the bot program on how where and when the attack shall commence.

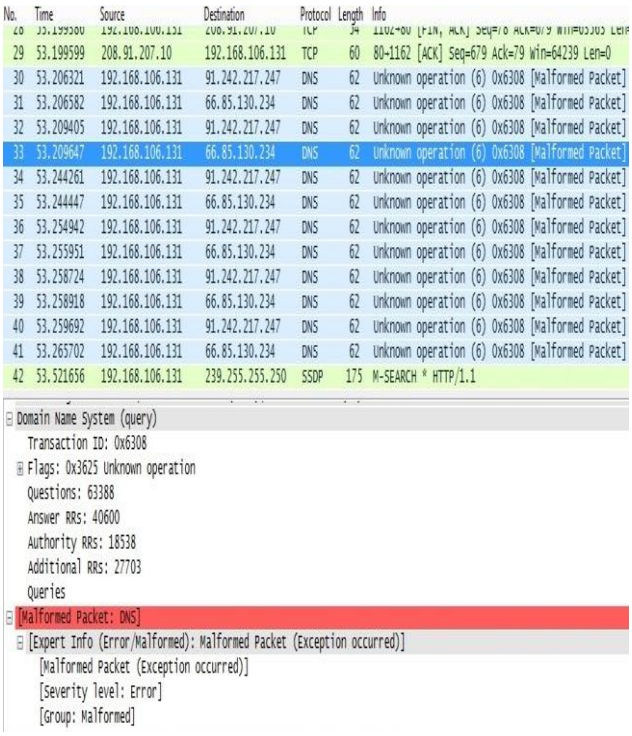

Fig 4: DNS Malformed packet generated from a Compromised system by a ZeroAccess botnet.

The Figure 3 is the net flow generated by running the Neris botnet. This botnet is mainly famous for bitcoin Mining. It uses packets send out on port 53 which belongs to DNS traffic. The packets are not actually DNS request/response packets but actually a way to communicate with the C&C server to carry out its attack (Bitcoin Mining). As seen in the Figure 4 the packets are recognized as DNS packet but are shown as

Malformed Packet. These malformed DNS packets have a answer field value of more than 3000 in average.

5. PROPOSED IDEA AND EXPERIMENT

As we analyze botnet effected system we see that there is a similarities in the packets they request, the replies that come and also the data of the configuration file downloaded by the bot program used to launch the attacks. In the above example for botnet the DNS reply to a DNS query contained more than a threshold limit that we can set accordingly (best case more than 7) of answers in the answer field as seen in Fig 2.Thus we need to stop our system from becoming a bot in a botnet. So we propose a framework as seen in Fig 5. The framework starts with packet capturing from the TCP/IP stack. After this white paper and Black paper filtering is applied. The white paper filtering contains all the port and IP address that are genuine that is belongs to OS traffic or verified applications while the Black paper filtering contains the IP addresses of the already know malware and attackers.

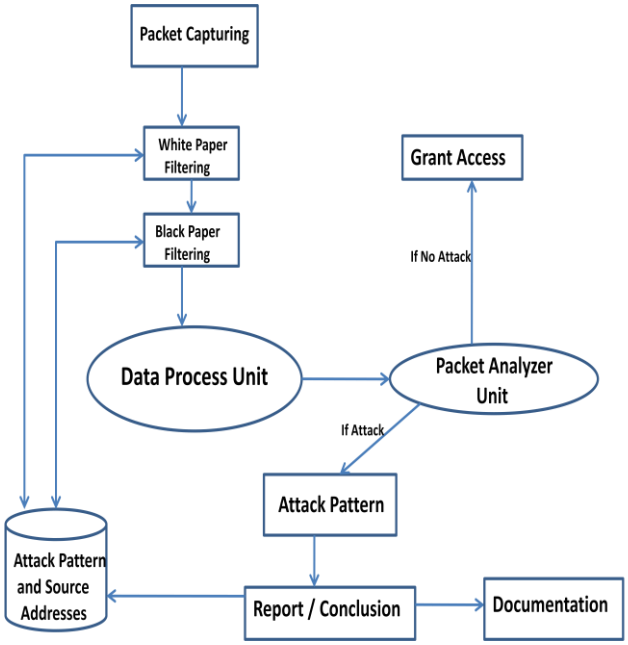

Fig 5 : Proposed Framework

The use of such filters helps us to reduce the load on the overall security framework. After this we forward the packet to Data processing unit where only revealing data is extracted and rest of the data is dropped and sends it to packet analyzer module. The packet analyzer module is responsible for the attack detection and mitigation. IS does this by analyzing different fields of the packet and trying to correlate if it is harmful or not in nature. One of the algorithm we propose is the DNS threshold algorithm as seen is Fig6.This is done by seeing the DNS replies and if the answer field Has more than few entities then we can just quarantine such packet till the user or system administrator looks into the contents of the DNS request and reply and decide if they are genuine or generated by the malicious program (botnet) that might have infiltrated our system. Discarding such packets will stop the bot program running on our computer from communicating with the C&C server making it unable to download the configuration file and thus stop the bot from performing the attack in the case of the two malware we studied the attack that uses our processor/GPU to mine Bitcoin and spam in some cases. As we will implement the proposed Algorithm we shall be able to stop the botnet from using our system for its purposes. Our algorithm wipes of the Bot program that has entered our system but stop its functioning by stopping its communication with its C&C server. This will leave the bot program into a Zombie state not being able to execute its attack as seen in case of Zero-

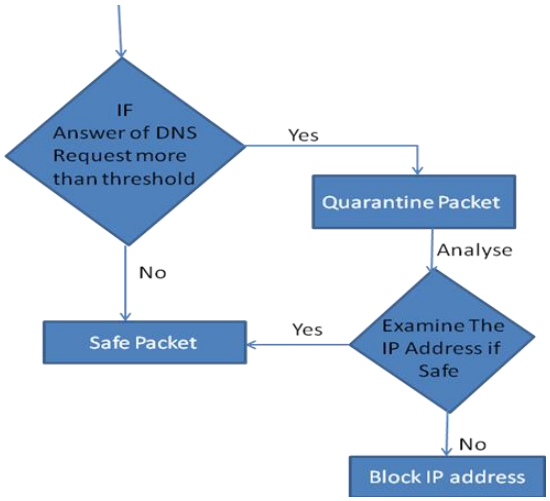

Fig 6: DNS Threshold Algorithm

Access to mine Bitcoins. Our algorithm may hamper the normal browsing of the Internet but after few iteration of updating by System Admin it will work in a optimized way only blocked the malware and having no hindrance to the normal traffic and operations on our system.

6. CONCLUSION AND FUTURE SCOPE

Botnet are able to do perform many types of attack such as DDoS, Bitcoin mining spam, identity theft, etc. The general population is prone to attacks such as identity theft, spamming etc while DDoS attacks are mostly targeted towards big organizations to disrupt their functioning and thus leading to financial losses. Therefore, there is a need to stop these type of the attacks, affecting our system. In this paper presented a Algorithm doesn't totally eliminate the threat of a attack from a botnet attack but at least reduce the threat to a certain level.

There is still a lot of work that needs to be done to mitigate the risk of attacks by Botnet as much as possible. We are able to secure the system and help it protect from Trojans/Botnets using means like Anti viruses, strong firewall etc but still a lot of works needs to be done on C&C level disruption in P2P & hybrids type botnets. Botnets exist due to the hidden malware on our system which is another topic of future research that to build a reliable information system to notify the infected user. Our proposed idea helps in mitigating the risk till some level but still a large number of users remain unnoticed, not knowing the risk of the attacks like spam and DDoS.

7. REFERENCES

[1] Sandeep Yadav, Ashwath Kumar Krishna Reddy, A.L. Narasimha Reddy, Supranamaya Ranjan, "Detecting Algorithmically Generated Domain-Flux Attacks with DNS Traffic Analysis", 2012.

[2] Satoshi Nakamoto, Bitcoin: A Peer-to-Peer Electronic Cash System 8 (2008)

[3] Joshua Davis, The Crypto-Currency, NEW YORKER, Oct. 10, 2011, at 62

[4] Dion, D. A. "I'll Gladly Trade You Two Bits on Tuesday for a Byte Today: Bitcoin, Regulating Fraud in the E-Conomy of Hacker-Cash." U. Ill. JL Tech. & Pol'y: 165.

[5] Peng, T., C. Leckie, and K. Ramamohanarao, Survey of network-based defense mechanisms countering the DoS and DDoS problems. ACM Computing Surveys (CSUR), 2007. 39(1): p. 3.

[6] Meiklejohn, S., Pomarole, M., Jordan, G., Levchenko, K., McCoy, D., Voelker, G. M., and Savage, S. (2013, October), "A fistful of bitcoins: characterizing payments among men with no names," In Proceedings of the 2013 conference on Internet measurement conference, ACM, pp. 127-140.

[7] Moser. Anonymity of Bitcoin transactions: an analysis is of mixing services. In Proceedings of Münster Bitcoin Conference,2013

[8] Reid, F. and M. Harrigan An analysis of anonymity in the bitcoin system, Springer.

[9] NicolasC hristin. Traveling the Silk Road: a measurement analysis of a large anonymous online market place .In Proc .of the 22nd int. l conf. on World Wide Web, WWW'13, pages213–224,2013

[10] H. Choi, H. Lee and H. Kim, "Botnet Detection By Monitoring Group Activities in DNS Traffic", in Proc. 7th IEEE International Conference on Computer and Information Technology (CIT 2007), 2007, pp.715-720.

[11] Alomari, E., et al., Botnet based distributed denial of service (DDoS) attacks on web servers: classification and art. arXiv preprint arXiv:1208.0403, 2012.

[12] Passerini, E., et al., Fluxor: Detecting and monitoring fast-flux service networks, in Detection of intrusions and malware, and vulnerability assessment. 2008, Springer. p. 186-206.

[13] Daan, A.F. Shosha, and P. Gladyshev, BREDOLAB: shopping in the cybercrime underworld, in Digital Forensics and Cyber Crime. 2013, Springer. p. 302-313.

[14] Mohammad M. Masud, Tahseen Al-khateeb, Latifur Khan, Bhavani Thuraisingham, Kevin W. Hamlen, Flow Based Identification of Botnets Traffic by Mining Multiple Log Files, In Distributed Framework and Applications, 2008. DFmA 2008.

[15] Fergal Reid and Martin Harrigan. An analysis of anonymity in thebitcoinsystem.SecurityandPrivacyinSocialNetworks,pages97–223,2013

[16] Moser. Anonymity of Bitcoin transactions: an analys is of mixing services. In Proceedings of Münster Bitcoin Conference,2013.

[17] Stock, B., et al. Walowdac-analysis of a peer-to-peer botnet. in Computer Network Defense (EC2ND), 2009 European Conference on. 2009: IEEE.

[18] Thapliyal, M., A. Bijalwan, et al. A Generic Process Model for Botnet Forensic Analysis. Conference on Advances in Communication and Control Systems.

[19] Bijalwan, A., M. Wazid, et al. "Forensics of Random-UDP Flooding Attacks." ISSN 1796-2056 Volume 10, Number 5, May 2015 **10**(5): 287.

[20] Micha Ober, Stefan Katzenbeisser, and Kay Hamacher. Structure and anonymity of the Bitcoin transaction graph. Future Internet, 5(2):237–250, 2013

[21] Meiklejohn, S., Pomarole, M., Jordan, G., Levchenko, K., McCoy, D., Voelker, G. M., and Savage, S. (2013, October), "A fistful of bitcoins: characterizing payments among men with no names," In Proceedings of the 2013 conference on Internet measurement conference, ACM, pp. 127-140.

[22] Reid, F. and M. Harrigan (2013) "An analysis of anonymity in the bitcoin system," in Security and Privacy in Social Networks, Springer, pp. 197-223.

[23] Ron, D. and A. Shamir (2012) "Quantitative Analysis of the Full Bitcoin Transaction Graph," IACR Cryptology ePrint Archive, 2012, p. 584.

[24] Androulaki, E., G. Karame, M. Roeschlin, T. Scherer, and S. Capkun (2012) "Eval- uating User Privacy in Bitcoin," IACR Cryptology ePrint Archive, 2012, p. 596.

[25] Guofei Gu, Roberto Perdisci, Junjie Zhang and Wenke Lee, "BotMiner: Clustering Analysis of Network Traffic for Protocol and Structure-Independent Botnet Detection ", In 17th USENIX Security Symposium, 2008.