An Advanced Hyper-Efficient Design to Detect Random Peer-to-Peer Botnets

Isma Farah Siddiqui[1,2(✉)], Nawab Muhammad Faseeh[3], Scott UK-Jin Lee[4], and Mukhtiar Ali Unar[5]

[1] Department of Software Engineering, Mehran UET, Jamshoro, Pakistan
[2] Software Engg Lab, Hanyang University, ERICA Campus, Hanyang, South Korea
isma.farah@faculty.muet.edu.pk, isma2012@hanyang.ac.kr
[3] Sungkyunkwan University, Seoul, South Korea
faseeh@skku.edu
[4] Department of Computer Science and Engineering, Hanyang University, Hanyang, South Korea
scottlee@hanyang.ac.kr
[5] Department of Computer Systems Engineering, Mehran UET, Jamshoro, Pakistan
mukhtiar.unar@faculty.muet.edu.pk

Abstract. Botnets have become one of the most solemn threats to Internet security. Botnets comprises over a network of infected nodes known as 'bot'. Bots are controlled by human operators (botmasters). Random nature of Peer-to-Peer botnets has influenced sinkhole researchers to compromise over occupation of hunted command and control in a complex manner and due to variable nature of action, they are often good deserters. In this paper, we present a design of an advanced hyper-efficient mechanism which has the ability to pursue Peer-to-Peer randomized botnets. It provides capacity to detain targeted sinkholes and identify arbitrary execution of contagion in infected nodes. In the end, method acquires the composition of different cubic formations for proper lookup of random natured Peer-to-Peer botnets.

Keywords: Botnets · Bot · Botmasters · Sinkhole

1 Introduction

Botnets are malicious programmed nodes, which are remotely controlled by botmasters. A botnet consists of bots and botmasters, postures a severe threat to internet security. The botmaster launch attacks such as Distributed Denial of Service (DDOS) and perform scam tasks such as phishing and spamming [1].

It is a matter of deep concern that the number of bot variants and the number of new bots are increasing every day. The huge propagation of botnets can be largely indorsed with the massive collection of computer nodes with 'always on' broadband connectivity that is tranquil to infect. The point of focus for a botmaster is to target home computers as well as the educational institutes computers because they are less

F.K. Shaikh et al. (Eds.): IMTIC 2013, CCIS 414, pp. 251–258, 2014.
DOI: 10.1007/978-3-319-10987-9_23

protected and have a huge storage with fast connectivity, and frequently direct connectivity with the backbone.

A command and control (C&C) system is a bridge through which bots connect to receive commands from botmaster. To this point, Internet Relay Chat (IRC) [1] protocol has been used by botnets to deploy C&C channels, so detecting patterns are customized to this protocol.

The botnets are programmed to achieve a target and are efficient enough to keep dispersing instructions, but they need to be familiar to get an interruption as the servers are recognized. In this way, it becomes rough for servers to distract all the information which becomes result of reducing the efficiency of botnets. In order to explain the scenario, it would be a disastrous for a botnet to shut down the C&C because it would lose all the effort done for the collection of bots and would result the termination of contact with botmaster. It is the reason for the propagation of peer-to-peer (P2P) botnets. P2P botnet does not hold any C&C server and the hierarchy of all nodes connected becomes complex in such a way that no any node recognize the C&C residing among one of them. The random natured P2P botnets have not only a decentralized C&C but it divide the central system in more than one location. In this paper, we present a design to identify such random P2P botnets.

The rest of the paper is drafted as follows. In Sect. 2, we briefly review the related work. In Sect. 3, we describe random P2P identification. In Sect. 4, we describe performance evaluation about the identification of random Peer-to-Peer botnets and discuss experimental results. Finally, in Sect. 5 we draw out conclusions and future work.

2 Related Work

Botnets have become a dynamics research area in recent years. An overview of bots and botnets was presented by Puri [2]. Botnets were monitored using honeynet by McCarty [3]. First built of P2P botnet named Slapper worm was analyzed by Arce and Levy [4]. The systematic dissection of botnets in details appeared in the past were given by Zhou and Xuxian [5]. Zeng et al. [6] presented a monitoring system to redirect DNS mapping of a C&C Server. Another researcher named Rafael [7] presented a passive detection of botnets by lookups of spam queries.

Botnets have an origin of using IRC for their C&C servers, most of the researchers detected and monitored network traffic to identify them. Abnormal IRC traffic detection modules were designed by Narang and Jagan [8]. P2P botnets have changed their straight intrusion in the shape of random attitude [9]. By random nature author describes the botnet attitude of changing C&C to random nodes so sinkholes could not be identified by security researchers as seen in Fig. 1.

3 Random P2P

To detect randomness in such an efficient system includes few components which are integrated with each other as follows:

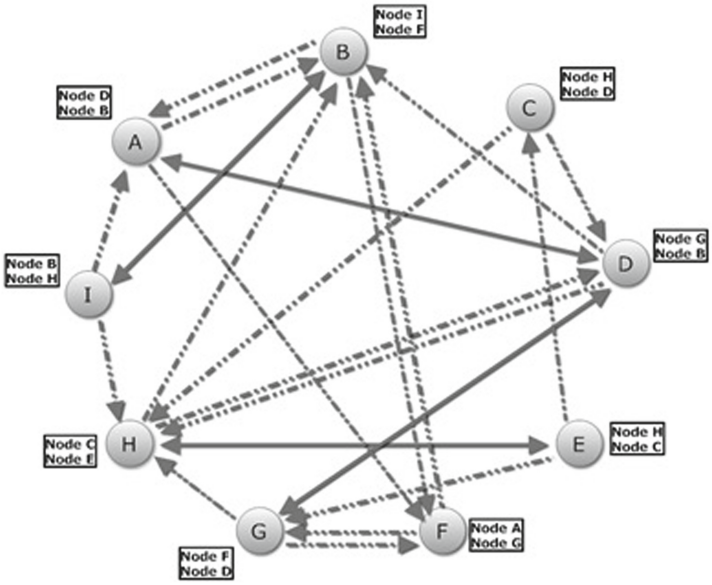

Fig. 1. Random P2P Botnet

3.1 Random P2P C&C Identification

Random P2P botnets apply botmaster-defined hierarchy to keep C&C among servant bots. Figure 2 illustrates the basic functionality of communicating infected client bots with medium layer servant bots. They are interlinked with each other in such a manner that acknowledgement mentioning infected bot and C&C can only be distinguished through detection between packet sampling among them.

Furthermore, paroxysm [10] is the only identification procedure through which information can be figured out over the network as illustrated from Fig. 2. Moreover, due to P2P decentralized nodes, all nodes are linked to networks and their subnets to attain the last node.

In order to identify malicious commands sent through a random C&C among bots, a paroxysm packet must be observed. It must have a sampling of destination with some defined attributes and randomization columns which are to be analysed for identification of temporary C&C node.

In the text below, D_a is used to identify nature of node paroxysm and D_s to recognize dispersed feature in the nodes. For ΔM time, t period samples are kept in considerations. Every node D network, links is structured in such a way that connectivity at each sample time forms a group $\{P_{d1}, P_{d2},\ldots.., P_{dq}\}$. W_{dr} is related with links of D node at the rate of R.

In a ΔM period, get the random average of the connections

$$P_s = \frac{1}{q}\sum_{a=1}^{q} P_{sq}$$

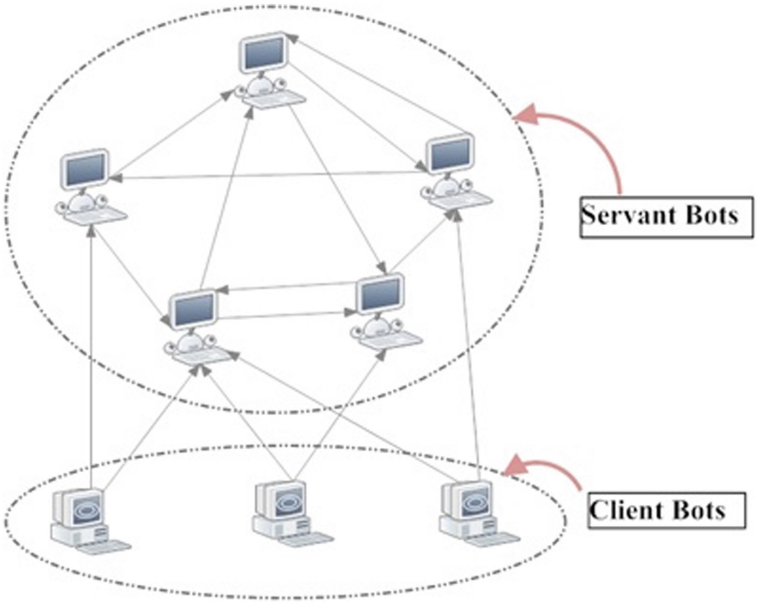

Fig. 2. Random P2P internal structure

At r, node D_{ar} is obtained with unit of paroxysm as:

$$D_{ar} = \frac{P_{dr}}{P_d}$$

Lets D_{amax} = Max (D_{a1},D_{a2},.....,D_{am}),

$D^{x}_{amax} = D_{amax} \times (1 - z\ \%)$, $D^{y}_{amin} = D_{amax} \times c\%$; [here z and c will remain fix.]

Furthermore, T_w is the number of sets to identify the criteria $\{D_{ai} \mid D_{ai} < D^{x}_{amin}\}$ and O_{Tw} has the collection of sets related to $T_{w.}$ Furthermore, Q_z is the number of sets to identify the criteria $\{D_{ai} \mid D_{ai} < D^{y}_{amin}\}$ and O_{Qz} has the collection of sets related to Q_z.

D_a unit can be defined as:

$$D_a = \frac{O_{Qz}}{O_{Tw}}$$

$D_f = \frac{K_e}{K_u}$ is the dispersed node of D. T_w has a container which includes the set of nodes linked with it as $K_{u;}$ T_w has a container which holds the set of subnets Q_z. As per the defined phrase, random P2P detection can be identified through Algorithm 1.

Alg. 1. P2P Detection of node

1. Calculate D_a and D_f of the node D;
2. If $D_a > D_{ca}$ and $D_f > D_{cf}$, wind up P2P node in the node D.

Samples of P2P nodes has delivered the paroxysm and dispersed values which are the properties related to D_{ca} and $D_{cf.}$

3.2 Random P2P Botnet Identification

Botnet which is of random P2P nature, bots have many similarities in action and reaction. The behaviour of such bots can include following properties [11]:

1. Scan Mode
2. DDoS Attack
3. Spam Sender
4. Binary Downloading
5. Exploits

Figure 4 illustrates different activities of random P2P botnet in a network. In Fig. 4 individual behaviour of botnets are identified with different nature of attacks like port scanners, spam senders with same SMTP destination locations, the behaviour of acquiring same files for a unethical activity, DDoS attack with lots of connections at the same time while engaging with exploits.

In order to extract bots attitude from defined method, given procedure can have some detections of bots. If we compare our method with other mechanisms, it is autonomous and does not relate with any given protocol.

In order to resolve different behaviours of botnets, let's assume set $D_p = \{D_1, D_2, D_i \ldots\}$ is the set of collection nodes in a P2P network. Assuming a sample of D_p as the collection of β_N. Let $N_{c\text{-}}$ as scanning behaviour, behaviour related to exploits is named as N_e and DDoS behaviour attack is related to N_o. In order to identify the individual action, evaluate the similarity of nodes in $\beta_{N.}$

As per the evaluation of the suspect attitude five groups $\{N'_c\ N'_s\ N'_d\ N'_e\ N_o\}$, we define their similarity as $\{T'_c T'_s T'_d\ T'_e T_o\}$ where $N_{\beta N}$ is the set of nodes into β_N.

$T_o = \frac{O_{\beta N}}{N_{\beta N}}$. $O_{\beta N}$ is set of nodes whose has the same DDoS parameters.

$T_e = \frac{E_{\beta N}}{N_{\beta N}}$. $E_{\beta N}$ is set of nodes whose has the same exploit parameters.

$T_s = \frac{S_{\beta N}}{N_{\beta N}}$. $S_{\beta N}$ is set of nodes whose has the same spam parameters.

$T_d = \frac{D_{\beta N}}{N_{\beta N}}$. $D_{\beta N}$ is set of nodes whose has the same downloading parameters.

$T_c = \frac{C_{\beta N}}{N_{\beta N}}$. $C_{\beta N}$ is set of nodes whose has the same scan parameters.

The similarity behaviour of β_N is $T = T_c + T_s + T_d + T_e + T_o$

As per the explained phrase, the random P2P Botnet detection algorithm is defined in Algorithm 2.

Alg. 2. P2P Botnet detection

1. Calculate the similarity of T of Ω_N
2. Determine set D_p as a Botnet if T >M_N.

Computation of M_N can be evaluated from the identified P2P botnets statistics.

4 Performance Evaluation

4.1 Random P2P Nodes Detection

To get results, we have taken into consideration three P2P protocol applications such as uTorrent, FrostWire and Transmission in a wired personal network to identify our required results based on specified criteria.

In order to get results, our simulation includes 100 nodes and the number related to P2P application user's nodes is 30. The mean time for the simulation is 3600 s, having x-axis as 1and y-axis as 10 illustrated in Fig. 3.

As shown in Fig. 3 common nodes are clearly separated from P2P nodes in the ratio of D_a & D_p. The threshold for this simulation holds the equity of: C_{Da} = 10, C_{Dp} = 1.

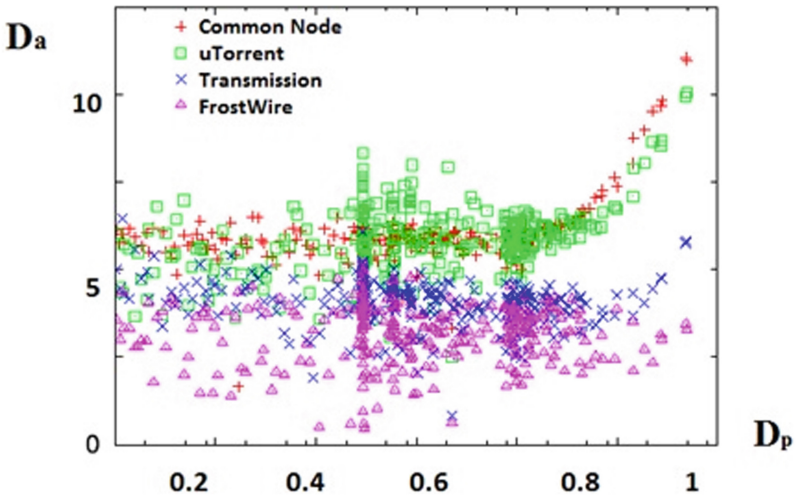

Fig. 3. Performance evaluation of random P2P Botnets

4.2 Random P2P Botnet Detection

Bots can perform their malicious activity many times in a single day. Zeus [12], Kelihos.B [13], ZeroAccess [14] and Sality [15] are the four types of botnets which are set for the simulation results. It can be clearly observed that our method identifies and differentiate the nodes of not having any botnets and the ones with the flavour of botnets through mentioned algorithm as declared in Table 1.

Table 1. Random P2P Botnet Detection result

Samples	T_c	T_s	T_d	T_e	T_o	T
No Bots	0	0	0.07	0	0	0.07
Zeus(silver)	0.1	0.8	0.4	0	0.9	2.2
Kelihos.B(Green)	0.9	0	0.9	0	0.8	2.6
ZeroAccess(Blue)	0.9	0.5	0.8	0.7	0.7	3.6
Sality(Gray)	0.3	0	0.3	0	0.5	1.1

The results of random P2P botnet detection algorithm are categorized and shown in Fig. 4 where we have mentioned four types of botnets in their prescribed categories.

After having results, main feature of Zeus is identified as sending spam, Kelihos.B and Sality depicts lots of scanning behaviour whereas ZeroAccess shows doing DDOS. By using detection algorithm, infected bots can be detected in a P2P network.

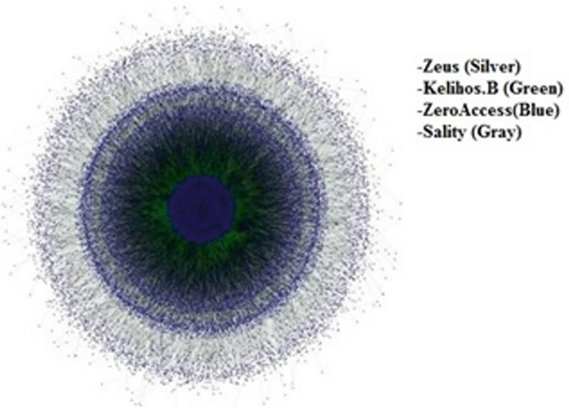

Fig. 4. Random P2P Botnet Detection

5 Conclusion and Future Work

A naïve user perform any activity on system related to IRC usage, lottery web sites, free advertisers and money web sites, anonymous conversations, encoded water mark pictures and free full version software. Such systems are easy resource to be

contaminated to the network of botnets and enlist for the botnets into a ready position for unethical act.

In this paper, we have presented a mechanism for detecting random P2P botnets. It describes how unidentified C&C can be identified in a random P2P botnet network and the way it can be captured for extending to a sinkhole. The mechanism is based on an idea to shrink the strength of random P2P botnets.

In future work, we will focus on secure sinkholes and P2P botnets activities in captured sinkholes.

References

1. Grizzard, J.B., et al.: Peer-to-peer botnets: overview and case study. In: Proceedings of the First Conference on First Workshop on Hot Topics in Understanding Botnets (2007)
2. Puri, R.: Bots & botnet: an overview. SANS Institute 2003 (2003)
3. McCarty, B.: Botnets: big and bigger. IEEE Secur. Priv. **1**(4), 87–90 (2003)
4. Arce, I., Levy, E.: An analysis of the slapper worm. IEEE Secur. Priv. Mag. **1**, 82–87 (2003)
5. Zhou, Y., Xuxian J.: Dissecting android malware: characterization and evolution. In: IEEE Symposium on Security and Privacy (SP). IEEE (2012)
6. Zeng, J., Tang, W., Liu, C., Hu, J., Peng, L.: Efficient detect scheme of botnet command and control communication. In: Liu, C., Wang, L., Yang, A. (eds.) ICICA 2012, Part I. CCIS, vol. 307, pp. 576–581. Springer, Heidelberg (2012)
7. Rodríguez-Gómez, R.A., Maciá-Fernández, G., GarcíaTeodoro, P.: Survey and taxonomy of botnet research through lifecycle. ACM Comput. Surv. (CSUR) **45**, 45 (2013)
8. Narang, P., Reddy, J.M., Hota, C.: Feature selection for detection of peer-to-peer botnet traffic. In: Proceedings of the 6th ACM India Computing Convention. ACM (2013)
9. Li, H., et al.: Modeling to understand P2P botnets. In: IEEE Second International Conference on Instrumentation, Measurement, Computer, Communication and Control (IMCCC) (2012)
10. Han, K.-S., Im, E.G.: A Survey on P2P Botnet Detection. In: Kim, K.J., Ahn, S.J. (eds.) Proceedings of the International Conference on IT Convergence and Security 2011. LNEE, vol. 120, pp. 589–593. Springer, Heidelberg (2012)
11. Xu, Z., et al.: Utilizing enemies' P2P strength against them. In: Proceedings of the 2012 ACM Conference on Computer and Communications Security (2012)
12. Lu, C., Brooks, R.R.: P2P hierarchical botnet traffic detection using hidden markov models. In: Proceedings of the 2012 Workshop on Learning from Authoritative Security Experiment Results. ACM (2012)
13. Greengard, S.: The war against botnets. Commun. ACM **55**, 16–18 (2012)
14. Dave, V., Guha, S., Zhang, Y.: ViceROI: catching click-spam in search ad networks. In: Proceedings of the 2013 ACM SIGSAC Conference on Computer & Communications Security. ACM (2013)
15. Wichmann, A., Gerhards-Padilla, E.: Using infection markers as a vaccine against malware attacks. In: IEEE International Conference on Green Computing and Communications (GreenCom), pp. 737–742, 20–23 November 2012