CYBER THREATS BASED ON BOTNET AND ITS DETECTION MECHANISMS

Mohamed Jamaldeen Ahamed Sabani[1], Janarthanan Krishnamoorthy[2]
[1]Depertment of Information & Communication Technology, SEUSL, [2]Virtusa, Sri Lanka
[1]mjasabani@seu.ac.lk, [2]janarthananmoorthy@gmail.com

ABSTRACT

Modern network system facing challenges in securing network infrastructure. Cybercrime has been becoming challenge to the security filed cause of increasing growth of internet usage. One of the most significant threats faced by the network connected system is Botnet. The Botnet is an evolving threat to the cybersecurity, and with the existence of command and control server (C&C server). It makes most malware attack compared to all other attacks. The bots in a network which causes a malicious act is known as the Botnet attack. The main aim of the Bot attack will vary from key-logging attack in a network to severe attack like Distributed Denial of Service (DDoS). An attacker called Bot-master controls this Botnet. This paper discusses different types of architecture in botnets such Centralized botnets with HTTP and IRC protocols, Decentralized botnets with P2P and Hybrid architecture. Meanwhile it discusses various threats and different detection mechanisms based on Signature, Anomaly, DNS, Data mining and Machine learning detection methods which used to detect bots in a network system. However many pieces of research have been done on a botnet to detect and control the botnet activities, but still, it's a challenging topic in cyber security. Botnets are now in raising the edge of attack by an attacker, thus researches on detecting the botnets with higher accuracy, especially on bot cloud, mobile Botnet is timely required.

Keywords: Bot, Botnet, Command and Control Server, DDoS, Centralized Botnet, Decentralized Botnet

Introduction

Nowadays the main concern of the world is protecting security of network from Cyber-attacks. The cyber-attacks which cause damage to the infrastructure and the network system. The most known threat to any network is the Botnet. The term bot came from the word Robot (Saha & Gairola, 2005). The function of the Botnet is automated through programs and scripts. The Bot is a compromised computer which can be located anywhere in the network system such as school, homes, companies, etc. The botnets are controlled over by the attacker who is knowns as the bot-master. These bots act like zombies which allow the attacker to do malicious activities by hiding his/her identity. Botnets are usually used to perform Distributed Denial of Service attack. Botnets are controlled by the bot-master over the command and control server (C&C server) (Rodriguez, 2017). The main reason for using Botnet in cyber-crimes is that the attacker can hide his/her identity, and it is difficult to find/locate the command and control server. It can also hide the malicious traffic within the usual traffic. Some researchers have discovered the botnets which can attack mobile devices and which controlled over by SMS or Bluetooth. Another latest evolution of botnets is Bot cloud, which is used in the cloud services. Cloud bots are very easy to develop as the online services are always connected to the internet and very difficult to detect them (Rodriguez, 2017). This paper will discuss the types of architecture in Botnets and its detecting mechanism that are used to detect the bots attack.

Related Works and Analysis

Many researches have been done on the botnet attack on command and control (C&C) model where the bot-master used IRC (Internet Relay Chat) protocol to communicate to each Bot. In C&C model, a single attacker communicates and controlled all bots in a network. This uses the centralized server which serves as a bridge between the bot-master and the botnets. Then the botnets were improved and developed to P2P (Peer to Peer) model. In P2P model, there is no single point of control over the botnets, and it more difficult to detect as they can regenerate. The previous detection methods are based on the assumption as the earlier bots were focused on performing some limited attacks (Chaware & Bhingarkar, 2016). The researchers have come up with new techniques to detect and control bot attacks. Bot attacks were discovered based on behavioral analysis, machine

learning, signature-based, data mining based, etc. (Rodriguez, 2017) (Tesfahun & Bhaskari, 2013). This paper presents a completed overview on the architecture of botnets, its life cycle and new advanced detecting techniques to identify botnets in a network.

Botnets can be defined as the compromised host that is managed by the remote attacker through simple command and control servers (Saha & Gairola, 2005)**.** Bot-master connected to the bots through the command and control server and sending the commands to the bots. The channel that communicates between the bot-master and the bots called the C&C channel or command and control channel (Chang, Mohaisen, Wang, & Chen, 2015). The malicious machines are infected with the malicious software which is injected to the hosts through the propagation mechanism by the bot-master. Once the host machine gets infected, these hosts become like zombies, and they were used to perform attacks among other hosts or perform Denial of Services attacks (Perdisci, Lee, & Feamster, 2010)**.** Bot-master looks for the hosts with fast transmission rate, availability, low level of security and remote locations (Saha & Gairola, 2005).

2.1 Botnet Life cycle:

The botnet life cycle has been developed with five phases. They are an initial injection, secondary injection, connection phase, C&C server and upgrading and maintenance phase (Rodriguez, 2017)**.**

Initial Injection:

This is the first phase of the botnet attack. In this phase, the bot-master find the vulnerable host for the Botnet. This can be done through several exploitation methods such as phishing, spam email, unwanted downloads of malware from websites, infected files attached to the emails, infected removable disk such as pen-drive, etc. Once the attacker exploits infection to the vulnerable host, it will identify the address of C&C server for the communication with bot-master (Rodriguez, 2017) (Perdisci et al., 2010)**.**

Secondary injection:

Once the first phase is completed successfully, it will be moved to the second phase. In this phase, the infected host will run the program which will search for the malware binaries in the provided network database. Once the malware is entirely installed that host became an active bot (Zombie). This Bot will use HTTP (Hypertext Transfer Protocol), IRC (Internet Relay chat) or P2P (Peer to Peer) protocols for the attack (Rodriguez, 2017) (Perdisci et al., 2010).

Connection:

This is the main phase in the Botnet, where it establishes the connection with the C&C server to receive the commands from the bot-master. In this phase, the Bot receives the commands from the bot-master and Bot will reply to C&C server. Bot-master does restart all the bots to check the activeness of the bots to receive the commands (Rodriguez, 2017).

Command and Control Server (C&C):

This is the real functioning part of the botnet life cycle. It starts working from the C&C server. The bot-master controls all zombies or bots through C&C server by commanding. All infected host needs to know the address of the command and control server (C& C) when downloading the script (Rodriguez, 2017)**.** The C&C server create with different topologies such as centralized, hierarchical and hybrid, which is the combination of HTTP and the IRC protocol (Rodriguez, 2017).

Upgrade and monitoring Phase:

In this phase, it prevents the C&C server from the track by changing its location after a few periods. In this phase, the bot-master work on the active bots to infect new host machines to increase the numbers of bots (Rodriguez, 2017) (Perdisci et al., 2010)**.**

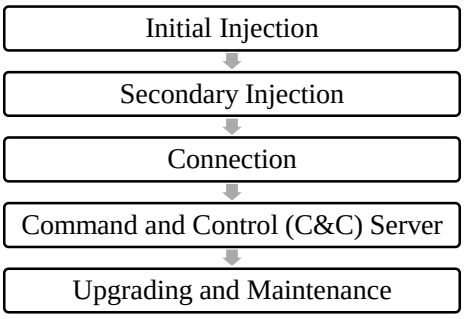

Figure 1: Botnet Life cycle

2.2 Types of Botnets

The common way to classify the botnets is based on the kind of architecture design. Bot-master designs the Botnet into more complex by using different types of protocols and topologies. Most common types are centralized botnets with HTTP and IRC protocols and decentralized botnets with P2P and hybrid architecture (Rodriguez, 2017).

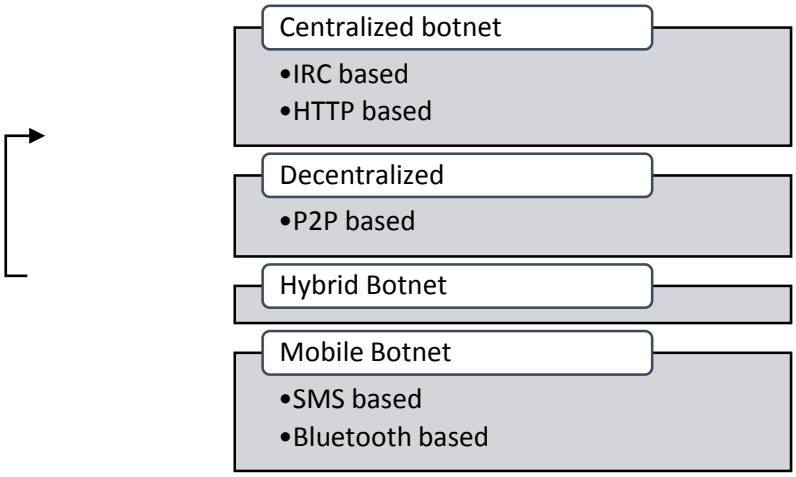

Figure 2: Types of Botnets

Centralized Botnet:
This architecture is a simple design, which has a single central C&C server which is connected to all bots in the network. All infected hosts or bots are directly connected to this central C&C server. This server is used to create bots for botnets and also to communicate with the bots to receives messages from all bots and pass it to bot-master when he requested (Rodriguez, 2017).

This C&C server possess a high bandwidth for communicating with the bots. Ago bots, SD bots, and RBots are some examples of centralized botnet model. This centralized Botnet can be developed by using the IRC and HTTP protocols (Rodriguez, 2017).

The main advantage of the centralized Botnet is fast response reaction and proper coordination with bots over the network. It gives direct feedback to Bot-master from Botnet, which is more comfortable for an attacker to monitor the status, such as the number of active bots and their global distribution. The main disadvantage of centralized architecture is that there are possibilities of a central point of failure at the C&C server (Chen & Lin, 2015). If a single C&C server is detected, then all other bots in a network can be easily detected. This makes the system vulnerable. This made the attackers develop the decentralized architecture of botnets (Bailey, Cooke, Jahanian, Xu, & Karir, 2009).

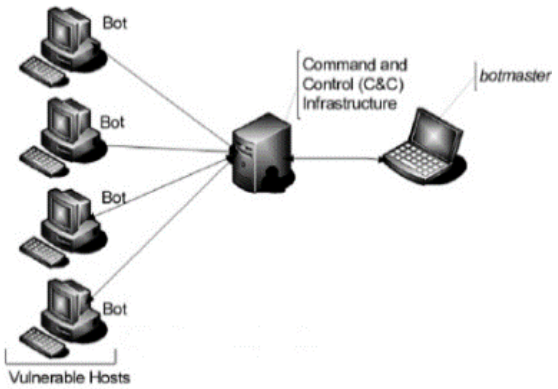

Figure 3: Centralized Botnet model

IRC Based botnet:
IRC the term refers to Internet Relay Chat, which works with real-time internet text messages (Chang et al., 2015). IRC protocol is used by the bot-master to create a channel among the bots and to communicate with them. This is a simple architecture. The limitation of using the IRC is, the communication can be easily detected and traced out by observing the IRC traffic with normal traffic (Bailey et al., 2009). The network admin or the network security officers may detect the IRC traffic and block them using the firewall. This limitations in the IRC made the attacker to develop the HTTP based botnet architecture. (Rodriguez, 2017) (Perdisci et al., 2010).

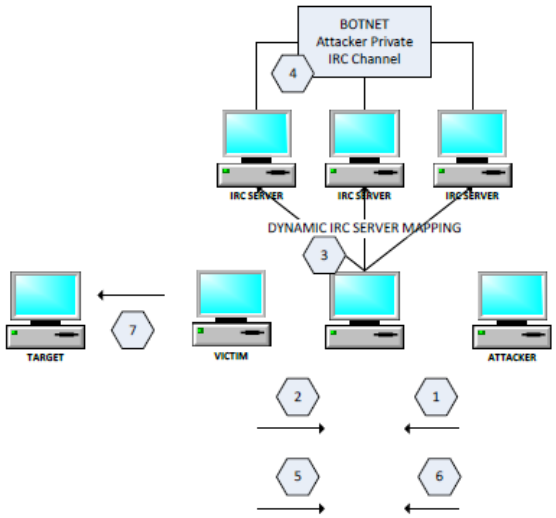

Figure 4: IRC based Botnet model

HTTP Based:
HTTP refers to HyperText Transfer Protocol, which is a popular botnet architectural design. This protocol can hide traffic with regular network traffic. Bobox, click Bot, SD bot, Rustok are some examples of HTTP based bots (Rodriguez, 2017) (Bailey et al., 2009). This type of botnets can bypass the firewall as this is combines with the regular HTTP traffic. It is complicated to detect because HTTP is a standard protocol which is used in network communication (Hadianto & Purboyo, 2018).

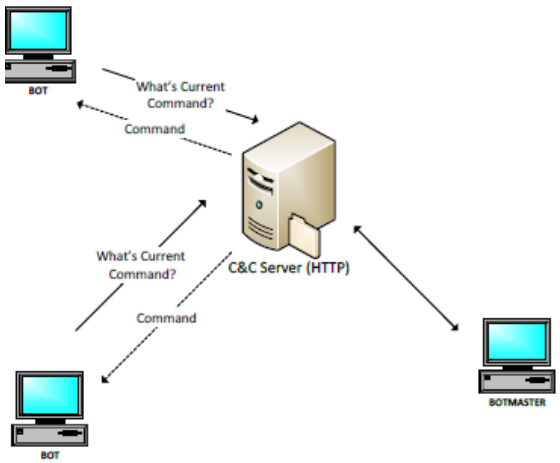

Figure 5: HTTP based Botnet model

Decentralized Botnet:
The weakness of easy detection of having the C&C server made the attackers have decentralized botnets. This provides high flexibility and robustness to handle the number of bots. In this architecture, the botnets are not controlled over by a single server but instead, the bot-master use bot as a server to perform the actions (Rodriguez,

2017). Decentralized botnets use P2P protocols (Perdisci et al., 2010).

Peer to Peer (P2P):

In Peer to Peer (P2P) model, all bots are connected with each other without having a centralized C&C server. The main focus of having the P2P protocol is, it is challenging to detect the C&C server. The bot-master uses different bots to send command each time. The architecture of P2P protocol is much complicated, and thus, it provides hard to detect them. This model acts like a client and server model where all bots can work as a client or server (Rodriguez, 2017) (Bailey et al., 2009).

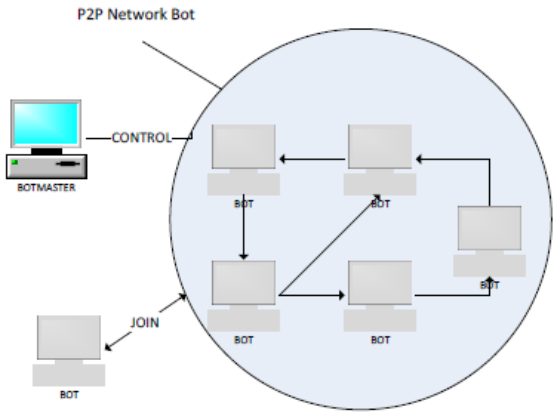

Figure 6: P2P based botnet Model

Hybrid Botnet:

The combination of centralized and the decentralized model is known as the Hybrid model botnet. In this model, an encryption key is used to hide botnet traffic from normal traffic. It uses random vulnerable ports and sends encrypted messages in the Botnet. The hybrid model uses P2P protocols, which are divided into two groups. One is servant bots, and another one is client bots. The servant bots can act as both client and server (Rodriguez, 2017). These servant bots are configured with a static and routable IP address. Meanwhile, client bots are configured with a dynamic and non-routable IP address. These bots work behind the firewall and do not connect to the global network (Bailey et al., 2009).

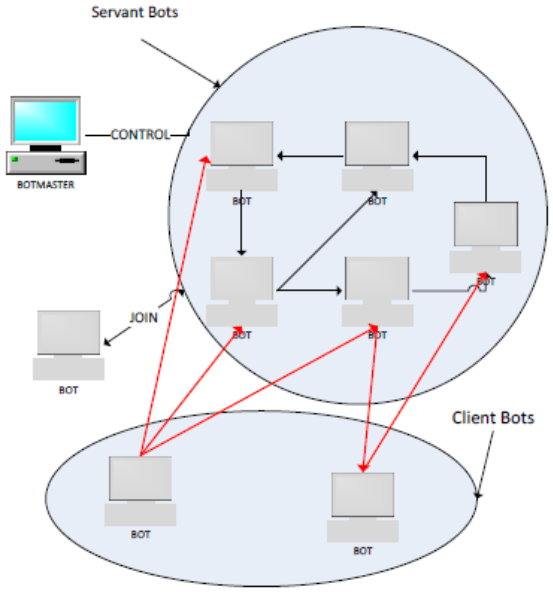

Figure 7: Hybrid type botnet model

2.3 Advanced Botnet Threats

Various types of threats can be created using with botnets by an attacker. Bots can be used for specific type of attacks or for many types of attacks.

Denial of Service attack:

Distributed Denial of service is a common attack performed by the botnets. This attack is sued to send a large number of ICMP packets or SYN packets to a particular network or send a large number of requests to the site from different bots in a botnet (Saha & Gairola, 2005). AgoBot, SDBot, PhatBot are some common bots which are being used for DDoS attack(Chen & Lin, 2015). There was a massive DDoS attack on high profile targets by a botnet call "Mirai", mainly it embedded with IoT devices. (Antonakakis et al., 2017).

Infecting new hosts

Infected bots in Botnet is used to find other vulnerable hosts to infect them. This can be done through social engineering and by through malicious emails (Chen & Lin, 2015).

Spam

Botnets are used to send spam by an attacker's choice with an SMTP engine. The victims cannot trace back the source of spam because Botnet distributes a much larger the volume of spam by its high computing power and availability of bandwidth (Chen & Lin, 2015). Phatbot is one of the common bots used for spamming (Saha & Gairola, 2005).

Device Spoofing

Bots can spoof the IP addresses of the victim host. Attackers can also force new bots with new IP addresses, and by modifying the code or other attributes, the attacker can change the signature of the bots. Device fingerprint access is more reliable as it does not depend on the user agent or IP address. As per research now, the bot-masters are working to defeat the fingerprint protection (Tesfahun & Bhaskari, 2013).

Apart from above mentioned malicious activities of the Botnet, there are some more attacks bots can perform in locally such as stealing information, information modification, key logger, data leakage, unauthorized access, etc. (Bailey et al., 2009) (Saha & Gairola, 2005). Nowadays a group of bots refers as social botnets are raising in attacks on online social networks by mimicking and interacting among normal users using some techniques in a way to reduce their detection (Zhang, Zhang, Zhang, & Yan, 2018).

2.4 Detection Techniques

There are different detecting techniques and mechanisms used to detect bots in a network system to control the threats of botnets.

Signature-based detection

This detecting technique uses an existing signature of a botnet to create a database. Then this uses a pattern based matching method to compare the signature of network traffic with the existing bots. This method is faster due to the database which has stored the existing signature of the botnets. This detection method is not suitable to detect the new botnets as it can detect only the known and already traced botnets (Kaur & Singh, 2016) (Rodriguez, 2017). It is also performing the IP scanning to detect the Bot by scanning the group of IP host which are seen in the IRC channel (Micro & Paper, 2006).

Anomaly-based

A botnet of infected machines acts together to perform a group related to anomalous behaviors (Yadav, Reddy, Reddy, & Ranjan, 2010). Anomaly technique method detects the Botnet by monitoring the network traffic. This method is distinguishing the malicious traffic from the normal network traffic, and thus, it detects the Botnet (Rodriguez, 2017). The anomaly-based technique is further divided into host-based detection and network-based detection. In host-based, the detection system will monitor the internals of the computer such as processing overhead, accessing to suspicious files, etc. In the network-based monitoring, it will monitor the network traffic (Chang et al., 2015)**.**

DNS based

DNS based detection is the combination of anomaly and signature-based detection. This technique also based on the unusual traffic generated by botnets. The bots in the Botnet are connected to communicate with the C&C server. Thus it must use the DNS query. This query information will be collected from the DNS query on this technique (Rodriguez, 2017). The presence of Botnet can be easily detected by monitoring DNS traffic (Thakur et al., 2012). This is also used to find the location of the C&C server and the bot-master. Another advantage of using this technique is if one bot from the Botnet is detected. The whole Botnet can be easily traced because all bots are using the same domain to perform queries. This is also used to detect the C&C server as it uses IP headers (Rodriguez, 2017) (Silva, Silva, Pinto, & Salles, 2013)**.**

Data mining based

Data mining technique is used to detect the high volume of network traffic, and thus, it finds the malicious traffic from it. This detection method is not suitable to detect the encrypted command and control server as it hides within regular traffic. So the data mining technique is used only in the data classification and clustering (Rodriguez, 2017) (Elhadi, Maarof, & Barry, 2013)**.**

Machine learning

Machine learning technique has become more popular in detecting malicious activities in the industry. This

provides an algorithm and mathematical calculation models to compare many factors on performing the behavioral analysis (Tesfahun & Bhaskari, 2013). This mechanism will monitor the complete working of different botnets, and it will generate a list of all bots with its signature. This list is useful to detect the new incoming bots into the botnets (Rodriguez, 2017).

Conclusion

A botnet is considered as the most dangerous malware when compared along with other malware in today's world. Many pieces of research have been done on a botnet to detect and control the botnet activities, but still, it's a challenging topic in internet security. A botnet can also be used for legal purposes when controlling and monitoring the activities of employers in an organization. Instead, most of the time, it has been used for the illegal purpose of controlling and stealing information from an organization by an attacker (Rodriguez, 2017). Honeynet, machine learning and intrusion detection system (IDS) are the most successful detecting technique at present.

Future research will be carried on detecting the botnets with 100% accuracy, especially on bot cloud, mobile Botnet. These botnets are now in raising the edge of attack by an attacker.

References

Antonakakis, M., April, T., Bailey, M., Bernhard, M., Arbor, A., Bursztein, E., … Zhou, Y. (2017). Understanding the Mirai Botnet. USENIX Security, 1093–1110. https://doi.org/10.1016/j.religion.2008.12.001

Bailey, M., Cooke, E., Jahanian, F., Xu, Y., & Karir, M. (2009). Al survey of botnet technology and defenses. In Proceedings - Cybersecurity Applications and Technology Conference for Homeland Security, CATCH 2009. https://doi.org/10.1109/CATCH.2009.40

Chang, W., Mohaisen, A., Wang, A., & Chen, S. (2015). Measuring botnets in the wild: Some new trends. In ASIACCS 2015 - Proceedings of the 10th ACM Symposium on Information, Computer and Communications Security. https://doi.org/10.1145/2714576.2714637

Chaware, S. P., & Bhingarkar, P. S. (2016). A Survey of HTTP Botnet Detection. International Research Journal of Engineering and Technology (IRJET).

Chen, C. M., & Lin, H. C. (2015). Detecting botnet by anomalous traffic. Journal of Information Security and Applications. https://doi.org/10.1016/j.jisa.2014.05.002

Elhadi, A. A. E., Maarof, M. A., & Barry, B. I. A. (2013). Improving the detection of malware behaviour using simplified data dependent API call graph. International Journal of Security and Its Applications. https://doi.org/10.14257/ijsia.2013.7.5.03

Hadianto, R., & Purboyo, T. W. (2018). A Survey Paper on Botnet Attacks and Defenses in Software Defined Networking. International Journal of Applied Engineering Research.

Kaur, N., & Singh, M. (2016). Botnet and botnet detection techniques in cyber realm. In Proceedings of the International Conference on Inventive Computation Technologies, ICICT 2016. https://doi.org/10.1109/INVENTIVE.2016.7830080

Micro, T., & Paper, W. (2006). Taxonomy of Botnet Threats. Micro.

Perdisci, R., Lee, W., & Feamster, N. (2010). Behavioral Clustering of HTTP-based Malware and Signature Generation using Malicious Network Traces. In USENIX Symposium on Networked Systems Design and Implementation.

Rodriguez, C. (2017). Advancing to Bot Management and Security. Stratecast Perspectives & Insight for Executives (SPIE)—Special Publication, 17(7).

Saha, B., & Gairola, A. (2005). Botnet: An Overview.

Silva, S. S. C., Silva, R. M. P., Pinto, R. C. G., & Salles, R. M. (2013). Botnets: A survey. Computer Networks, 57(2), 378–403. https://doi.org/10.1016/j.comnet.2012.07.021

Tesfahun, A., & Bhaskari, D. L. (2013). Botnet Detection and Countermeasures- A Survey. IJETTCS, 2(4), 309–314.

Thakur, M. R., Khilnani, D. R., Gupta, K., Jain, S., Agarwal, V., Sane, S., … Dhekne, P. S. (2012). Detection and prevention of botnets and malware in an enterprise network. International Journal of Wireless and Mobile Computing. https://doi.org/10.1504/IJWMC.2012.046776

Yadav, S., Reddy, A. K. K., Reddy, A. L. N., & Ranjan, S. (2010). Detecting algorithmically generated malicious domain names. In Proceedings of the ACM SIGCOMM Internet Measurement Conference, IMC. https://doi.org/10.1145/1879141.1879148

Zhang, J., Zhang, R., Zhang, Y., & Yan, G. (2018). The rise of social botnets: Attacks and countermeasures. IEEE Transactions on Dependable and Secure Computing, 15(6), 1068–1082.