# Review of “Know your Enemy: Tracking Botnet”

ITC6080 Network Security Concepts

Siyang Feng

# CONTENTS

# 1 REVIEW AND SUMMARIZE

The botnet is still one of the hot topics in the modern network community because it's hard to prevent and analysis before. The most famous attack relying on botnets is the DDoS attack. February 28th, 2018, the biggest code hosting platform, GitHub, was out of service from 17:21 to 17:26 UTC and intermittently out of service in the following four minutes due to the DDoS attack. It's the biggest DDoS attack which GitHub has ever suffered. The peak of this attack is at 1.35Tbps as the figure showing below [1].

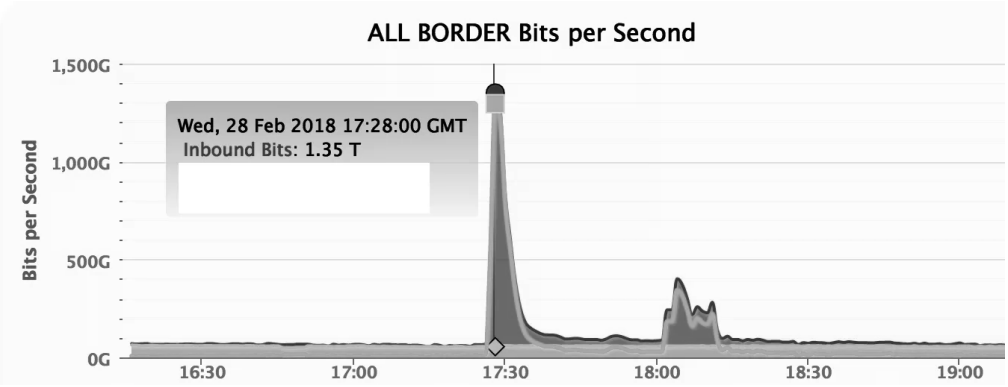


*Figure 1 GitHub DDoS Attack in 2018*

The DDoS attack is one of the significant attacks which is very hard to prevent and replies on the Botnets. This paper introduces one of the most popular cyber threats, botnets, and the method (honeynet) of tracking botnets. This paper describes the botnets as the enemy of our modern cyber community because it achieves some kind of attacks which cannot work with other methods, like Distributed denial-of-service (DDoS) attack. This paper starts with the introduction to botnets and its working principles and the types and usage of the botnets. Then this paper provides the tracking tool (mwcollect2) which is used to provide experiment result to exam the botnets.

## 1.1 BOTNETS

As the paper concludes, the botnet is a special network which consists of tens of thousands of compromised machines remotely controlled by the attacker. Not only the home PCs but also the development of IoT, the botnet become more popular than ever before because of the lower security of IoT technology. Attackers even with low-level hacking technic can still

have the ability to remotely control the IoT system to achieve the DDoS attack such as GitHub suffered in 2018.

The majority of Botnets rely on the Internet Relay Chat (IRC), the form of internet real-time communication. It's designed for the group (1-to-many) and P2P communication in the channel in original purpose. The advantages of IRC server are easily set up, available without payment and many crackers have rich experience on IRC communication. The advantages of IRC lead to its popularity in Botnet generating and remotely controlling.

Another reason for the popularity of botnets is that it's easy in use. As the paper said, the botnet is nothing but a tool which is one of the malwares. To spread, the malware scans the large network and figure out the known vulnerable computers and then, infect them into a bot. Then, the bots join a specific IRC channel and wait for the further commands from the attacker. This principle allows the attacker to the remote controlling. The structure of the botnets attack is showed in the below figure [2].

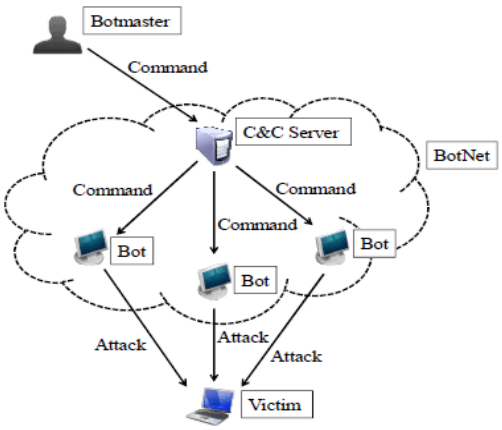


*Figure 2 Structure of the Botnet*

There are a lot of different types of bots. Except for the Agobot and its similar types, other bots are all based on IRC. Agobot is special which utilizes the control protocol. Botnets are wildly used in large range attack which is its feature. The well-known one is DDoS. Besides DDoS, other usages, for instance, spamming, keylogging, sniffing traffic, manipulating online games and polls, and mass identity theft, are also popular botnet attack.

## 1.2 HONEYNETS

The honeypot is a very popular technique to discover the tools, motives, and tactics of attackers. The aim of the honeypot is to build a trap to appeal cracker and attacker. And the log is used to record the activities. With the analyzing of the attack, security managers can have a deeper understanding of the attack. Basically, the honeypot is the system with loopholes to appeal cracker to attack.

Comparing with the honeypot, honeynet is a new concept developing from the honeypot. The honeynet is a high interaction honeypot technology which uses the real system and applications to interact with attackers. In the honeynet, there are one to multiple honeypots included and also the firewall and IDS. The benefit of the honeynet is that it provides a real network environment. And it reduces the risk of honeynet exposure.

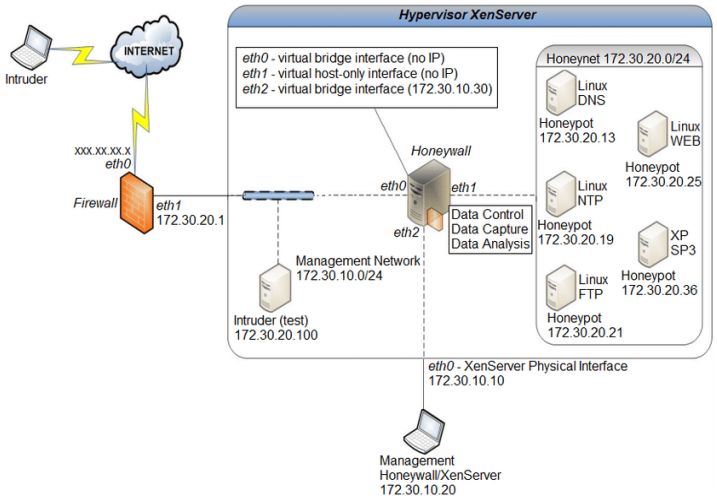


*Figure 3 Structure of the Honeynet*

The figure above displays the normal structure of honeynet [3]. The structure and feature of honeynet make it very suitable to track botnets. This paper uses a GenII Honeynet with some windows honeypots and snorts inline to collect attacker information.

With the tracking of botnets using honeynets, they found more than 100 botnets in the last four months. Also, there were 226,585 unique IP joining one or more monitored channels. Moreover, 226 DDoS attacks against 99 unique targets were observed.

# 2 PAPER CRITIQUE

## 2.1 OTHER USAGE OF BOTNETS - MINING

The botnets paper summarizes ten usages of the botnets, such as DDoS and mass identity theft. All of those ten usages are very traditional and easy to imagine. With the decentration concept, blockchain, and digital currency development, the technology of botnet mining is in progress. In recent few years, especially after the incident of WannaCry, digital currencies, especially Bitcoin, increase their value. And the Internet currency generates a great market recent few years. Thus, some of the attackers start to try mining.

The creator of cryptocurrency mining botnets earns about millions of money through secretly infecting the various of compromised machines crossing the world [4]. The botnet mining collects tens of thousands of machines and connects them together within the network. The attackers use the computing ability of bots and their electricity to mining the currency without notification to the machine owners. With the value increasement of the digital currency, attackers can bear less stress to gain more money than traditional cybercriminals. An incident happened in February 2018. There are more than half a million machines which are infected by the cryptocurrency mining botnet, Smominru. And those bots mine about 9000 Monero crypto coins in total. There are already different kinds of mining botnets in the market. And the top 3 are [5]:

- Smominru which is the biggest mining botnet recently;
- DDG botnets targeting servers which have mined about $1.5 million;
- ADB Miner which infects Android devices.

The paper said botnets don't require creators having a high technology of security and knowledge of the network. The only thing required is botnets tools. Most of the botnet's creators don't have the good skill of coding. However, the botnet mining requires the knowledge of coding and mining. With the social development, the new cybercriminal may require higher knowledge than ever before especially considering the botnets in the future.

## 2.2 BOTNETS IN THE FUTURE

The mining botnets are already in progress which requires higher technology than before. But what about the future? One thing is sure that the botnets in the future would become more complex than before for higher abilities and maybe more features.

The significant features of botnets are that one botnet consist of a large number of bots and each bot will run the exact command the controller sends and if there is no new command, the bots will wait for the new one and no other actions. Thus, in this way, the bots in the same channel will only perform the same actions and there is no self-action. When honeynets are used to track the botnets, the only thing to do is to analyze intention and command from the creators. To know the attacking method from creators is the aim is the key of the botnets. The other bots are just like the real zombies with following the instructions. The attack within this kind of feature is simplified. The strength of this attack is a great number of bots. The large size will generate a strong power to attack one target. That is the key to DDoS attack.

However, the report about the preview of cybersecurity in 2018 from Fortinet FortiGuard Labs mentioned a new word, Hivenet [6]. Hivenet consists of tens of thousands of swarmbots. In the basic structure, Hivenet is very similar to the Botnet. The preview report described that the botnets are dangerous and it's responsible for the billions of unauthorized cyber communications in each quarter. However, it described Hivenet as much more frightening of its unit, swarmbot.

The significant difference between Botnets and Hivenets is artificial intelligence. In recent years, artificial intelligence has become a huge role to play in cybersecurity. The artificial intelligence can perform more quickly and efficiently in cyber protection but as well as cyber-attack. Moreover, security within AI can also learn newer and better security practices with the training. The technologies of AI of security make the defense more active and flexible. The problem is that the technology of AI not only do significant progress in protection but also attack as well. The botnets have provided strong and stable basic to Hivenet. The unit of the Hivenet, swarmbot, is powered by AI. Then, the swarmbot can be able to make a lot of autonomous decisions relying on the situation it facing without the

instructions from the controller. The swarmbot with AI can learn by itself and cooperative combat and it achieves the auto-infect and auto-attack like the real virus in nature. Comparing botnets, Hivenets are more like the army and each swarmbot has its own role. It's closer to the word of the paper title, the enemy. The significant feature of Hivenets can be summarized into four aspects:

1. Consist of a large number of items (swarmbot) which is similar to botnets, but each swarmbot has the ability of self-learning.
2. Decentration. It means the leaving of any swarmbot will not influence the whole works of Hivenets. It's different from botnets. Actually, the botnet contains the center which is the person or device who create and send the instructions. The generator is the center of the botnet. However, Hivenets might be different. There is no real leader and each item do its own work regarding the environment ideally.
3. Intelligential. Each swarmbot has its own ability to control itself. Intelligence makes the swarmbot identifying environment, self-learning, and self-decision. There isn't exactly any instruction to decide the activity of the swarmbot.
4. Cooperating. When the swarmbot has its own intelligence, they can cooperate as a real army. If the cooperating attack achieved, the DDoS attack will be more threatening than ever before. The whole DDoS attack will be harder to control and unpredictable.

The good news is that the Hivenets are still not ever appear in the real cyber-attacks. It still exists in the concept only. But it will one of the directions of the future Botnets. One of the biggest issues about Hivenets which attackers may also consider is that if the Hivenets will be under control by the creator. If not, Hivenets will become a disaster than any other attack on the network and society.

## 2.3 CONSIDERATION OF KEYLOGGING

Keylogging is an interesting topic in the botnets. The paper said bots are spread through malware. In my understanding, the malware is Trojan in most of the Botnets. There are different kinds of Trojan on the internet. What the keylogging used is the keylogger Trojan.

Besides, there are multiple types of Trojan can be used in Botnets. Besides keylogger Trojan, there are Trojan-Backdoor, Trojan-Downloader, Ransomware and others. Within this concept, one botnet is spread through a type of malware. And each kind of malware should have one feature. It means even though the paper has listed ten usages of the botnets. There are only one or two usages can be applied to one botnet depending on the spreading malware. Thus, with the analysis of the spreading type, the security worker can guess the usage of the botnets.

The botnets working on the keylogging is spread through keylogger. It's really a very smart method for stealing the password and other sensitive information. Normally, cybersecurity workers are more interested in information protection when the information is in the transfer. It does important because, with the wireless transfer, the information becomes easier stolen when it on the way than wired network. That is the reason why cryptography is very popular nowadays. There are three popular methods to crack sensitive information, especially password: brute force, directory, and rainbow table attack. All of them relies on great computing abilities and powerful table or dictionary. Also, the technology of cryptography development, the algorithm of encoding will be more and more complex. In this way, it will take a lot of time to crack one password. However, keylogging is totally different. The reason I evaluate keylogger smart is that this way can steal every typing information and avoid the large computing about cracking the cryptography. What the attacker should do is just spreading their keylogger Trojans.

As the paper said, it's very easy for attackers to retrieve sensitive information. It's generally impossible to encrypt the typing. Typing has become the most straight-forward way to sensitive information. To retrieve the information wanted, a filter mechanism is implemented to filter the keywords. The example of PayPal is suited. The password of PayPal is definitely encrypted when it transfers. However, with the help of keylogger, the filter runs and selects all the data related to "PayPal". It's hard to imagine how quick the attacker will steal sensitive information.

Considering the keylogger, I find it's necessary about using the one-time password and biometric password. I think there are three methods can reduce the risk of the keylogger:

- Increase the security level of the system. It's very important. Trojan aurally hijacks the system with the known weakness. Update the security level will reduce the possibility of hijacked.
- Use the virtual keyboard. Avoid using the physical keyboard can reduce the risk of sensitive information stolen. However, most of the people feel uncomfortable one virtual keyboard using.
- Improve the authentication method. The keylogger is useful on stealing the password and other sensitive information on the keyboard. Thus, if the password can only be used in one time, there is no risk after stolen.

# 3 CONCLUSION

The reason I choose this paper is that botnets is a very interesting topic and I really want to know the detail. This paper teaches me a lot. With the review of the paper, I have the deeper understanding of the botnets and the tracking method, honeynets. In the class, I only studied honeypot. Thus, the difference between honeynets and honeypots interested me. This paper provides me the instance of the botnets tracking. I think the reason why the author chooses honeynets instead of honeypots is the more realistic simulation of the cyber environment. Also, honeynets can include multiple different OS, for instants, combining Windows, Linux, and MacOS together. In this way, the researcher can compare the result of the different system which may help the deeper analysis. As I mentioned above, botnets in the future might be smarter with AI technology. It could be easier to distinguish the fake network without any application inside. The more real the fake network is, the more effective the log system recorded will be.

# 4 REFERENCE

[1] Kottler, S. (2018, March 01). February 28th DDoS Incident Report. Retrieved from https://github.blog/2018-03-01-ddos-incident-report/

[2] Hsiao, H., Tung, S., Shih, M., & Sung, W. (2017). Using Botnet structure to construct the communication system of a real-time monitoring platform: Botnet structure for real-time monitoring platform. 2017 13th International Conference on Natural Computation, Fuzzy Systems and Knowledge Discovery (ICNC-FSKD). doi:10.1109/fskd.2017.8393235

[3] Rodrigues, G. P., Albuquerque, R. D., Deus, F. G., Jr., R. D., Júnior, G. D., Villalba, L. G., & Kim, T. (2017). Cybersecurity and Network Forensics: Analysis of Malicious Traffic towards a Honeynet with Deep Packet Inspection. Applied Sciences, 7(10), 1082. doi:10.3390/app7101082

[4] Seth, S. (2019, March 12). What is Botnet Mining? Retrieved from https://www.investopedia.com/tech/what-botnet-mining/

[5] Balaban, D. (2018, May 09). Top 3 Crypto Mining Botnets: Smominru, DDG, and ADB.Miner. Retrieved from https://www.itspmagazine.com/from-the-newsroom/top-3-crypto-mining-botnets-smominru-ddg-and-adbminer

[6] Manky, D. (n.d.). Cybersecurity 2018 – The Year in Preview: Federal Enforcement Trends. Retrieved from https://www.jdsupra.com/legalnews/cybersecurity-2018-the-year-in-preview-38452/