

Botnet Detection in Anonymous Networks

Katharina Kuhnert^{*}, Jessica Steinberger^{*,†} and Harald Baier^{*}

^{*} da/sec - Biometrics and Internet Security Research Group,
Hochschule Darmstadt, Darmstadt, Germany
`{Katharina.Kuhnert}@crisp-da.de`
`{Jessica.Steinberger,Harald.Baier}@h-da.de`

[†] Design and Analysis of Communication Systems (DACS)
University of Twente, Enschede, The Netherlands
`{J.Steinberger}@utwente.nl`

Abstract. Botnets are a major threat to the Internet landscape and have been responsible for large scale distributed attacks on online services. To make take down measures more difficult, Botnet operators started to incorporate anonymous networks into their software to protect their users and their Botnets. Although privacy and anonymity is an important goal of such services, cyber criminals also benefit from these properties, hiding their identity and location in the shadow of anonymity. This work investigates Botnets in anonymous networks and proposes mitigation strategies against such threat. This research is still in its initial state and is planned to result in a Ph.D. thesis.

Keywords: Botnet, detection, anonymous networks, Tor, I2P.

1 Introduction

In recent years, research of anonymous networks gained increasing interest as more and more people, businesses and governmental agencies worldwide make use of them to protect their identity and communication. Online censorship prohibits users from accessing services and information on the Internet [1], and projects like Tor and I2P are vital contributions to allow individuals to communicate without risking their privacy [2].

However, the use of such anonymization networks by cyber criminals also became more popular and their malicious activities within these networks affect service operators and legitimate users. One approach to mitigate the effects of malicious activities within anonymous networks currently relies on an entire block of the use of anonymous networks and thus any hidden service [3,4].

Moreover, Botnets have evolved to a major threat to the Internet landscape causing damage by cyber criminals launching Distributed Denial of Service (DDoS) attacks, stealing data or distributing spam [5]. Within the shadow of anonymity and confidentiality, Botnet operators have started to move their communication and recruitment of Botnet-zombies to anonymous networks and thus make it difficult to take down [6,7]. Blocking specific malicious services such as

Botnet controllers hosted on hidden services in the dark web, is difficult to perform and the identification of a Botnet target still remains a challenge [5,8,9,10].

By using anonymous and encrypted communication channels, detecting and blocking Botnet activity within anonymous networks is still in its initial phase [8]. Existing take down measures rely on identifying the Command & Control (C&C) servers to block Botnet traffic. With the increase of Botnet activity within anonymous networks, detection methods are required to perform mitigation [4].

The aim of this work is to provide an extensive characterization of Botnet activities within anonymous networks and to propose mitigation solutions against Botnets using these networks. In addition, this research will contribute to the understanding of what anonymous network services are used by Botnets and if a single Botnet uses multiple anonymous networks to obfuscate its communication.

2 Research Goal and Questions

The overall research goal of this work is to propose methods against the rising threat of Botnets within anonymous networks. To achieve this goal, we split up the overall research goal and investigate four research questions as depicted in Figure 1.

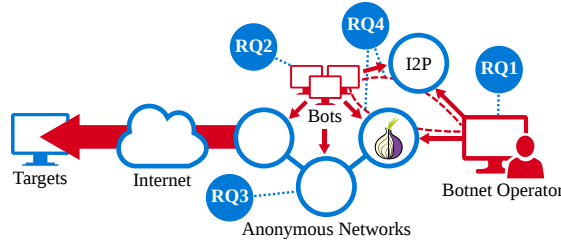


Fig. 1. Research questions overview.

Traditionally, Botnets have been controlled via protocols like Internet Relay Chat (IRC) [11]. These protocols are used by Botnet operators to hide their communication, avoid take down measures and obfuscate their identity [10]. We investigate the use cases of Botnet operators using anonymous networks and its services. We also analyze how Botnet operators integrate such networks into their applications. Thus, the first research question is as follows:

RQ1: Do Botnet operators use anonymous services and if yes, how?

Communication in anonymous networks is routed in such way which makes it difficult to identify the end-to-end communication partners [12,10]. Due to the encryption of all network traffic within an anonymous network, it is not easily possible to gain insight into transmitted data [10]. To gain an understanding of Botnet communication, we will characterize Botnet traffic within anonymous

networks and services. As a result of the characterization, we will derive features that serve as input parameters to build automatic classifiers. Thus, the second research question is as follows:

RQ2: What are the characteristics of Botnet traffic using anonymous networks?

Besides the development of a classification model, the detection of Botnet activities within anonymous networks is required to propose mitigation strategies. Traditional Botnet C&C traffic detection methods are using honeypots, active and passive traffic analysis techniques [10] and are based on the use of state of the art algorithms [13,14,15,16]. Although network traffic within anonymous networks is encrypted, behavior of Botnets can be detected with the aforementioned approaches by using their characteristics [14]. Thus, the third research question is as follows:

RQ3: How can Botnet traffic in anonymous networks be detected?

To make detection and take down measures more difficult, we assume that Botnet operators make use of multiple anonymous networks and services for a particular Botnet. Therefore, we investigate if Botnet operators distribute their anonymous communication over several anonymous networks. In case distributed anonymous Botnet communication is used, we analyze its benefits and how the Botnet traffic is distributed. Thus, the fourth research question is as follows:

RQ4: Does a Botnet use multiple anonymous networks and if yes, how?

3 Proposed methodology

In this Section, we present the approach of this work to answer the research questions.

3.1 Analysis of Botnets in anonymous networks

To answer RQ1, we perform a systematic literature review according to the well-established review methodology described by the Cochrane Community [17]. This systematic review results in an overview presenting Botnets that make use of well-known anonymous networks and its service. In particular, we focus on the most famous anonymous networks Tor and I2P. Furthermore, the systematic review results in an overview presenting the current state of the art Botnet detection methods in context of anonymous networks.

In addition to the systematic literature review, we find evidence of how Botnets use anonymous networks by studying source code of Botnets. Source code of Botnets have become available on the Internet and can be studied by researchers [18,19]. Such implementation details will give insight if and how Botnet communication is actually made by using anonymous networks. The contribution of the results of RQ1 will be an extensive insight of Botnets in anonymous networks and how they communicate.

3.2 Collect traffic data and characterize anonymous Botnet traffic

An important part of this work are measurements of real-world traffic within anonymous networks. Therefore, we deploy measurement nodes within the anonymous networks to collect traffic using OnionScan [20]. In addition, we will create a testbed for anonymous networks using the available Botnet software to create fingerprints of anonymous Botnet traffic. The recorded data allows the classification and detection of Botnet traffic to answer RQ2.

3.3 Create a model to detect Botnet traffic in anonymous networks

The results of the Botnet traffic characteristics serve as input parameters to design a model that distinct between Botnet traffic and non-Botnet traffic in anonymous networks. We create a method for Botnet detection based on state of the art algorithms [13,14,15,16]. To evaluate and optimize our approach, we first test our classifier within our test environment and second, deploy our detection algorithms on real-world anonymous networks. The results of this approach will answer RQ3.

3.4 Investigate in multiple anonymous networks

In this work, we have presented the use case of Botnets hiding their presence in anonymous networks. Using the results of RQ1 to RQ3, we investigate if a single Botnet uses multiple anonymous networks to hide their communication. We attempt to find correlations of Botnet traffic within multiple anonymous networks to answer RQ4.

4 Early results and Final Considerations

Early results of our research revealed that Botnets are using anonymous networks to hide their communication [18,19]. In addition, an initial web search identified the availability of Botnet source code to study Botnet communication and evaluate our detection model. This research is still in its initial phase and the main goal of this work, as described previously, must be achieved within a period of four years, as part of a Ph.D thesis.

Acknowledgment. This work was partly supported by the German Federal Ministry of Education and Research (BMBF), the Hessen State Ministry for Higher Education, Research and the Arts (HMWK) within the Center for Research in Security and Privacy (CRISP) and by the Netherlands Organisation for Scientific Research (NWO) Distributed Denial-of-Service Defense: Protecting Schools and other public organizations (D3) Project.

References

1. Aceto, G., et al.: Analyzing internet censorship in pakistan. In: IEEE 2nd International Forum on Research and Technologies for Society and Industry Leveraging a better tomorrow. (Sept 2016)
2. Cuthbertson, A.: Iran internet censorship forces protesters to turn to dark web. <http://www.newsweek.com/iran-internet-censorship-sees-protesters-turn-dark-web-772182> Accessed: 3. April 2018.
3. Prince, M.: The trouble with tor. <https://blog.cloudflare.com/the-trouble-with-tor> (2016) Accessed: 31. March 2018.
4. Hopper, N.: Challenges in protecting tor hidden services from botnet abuse. In: Financial Cryptography and Data Security, Springer Berlin Heidelberg (2014)
5. Spamhaus Malware Labs: Spamhaus botnet summary 2016. <https://www.spamhaus.org/news/article/733/spamhaus-botnet-summary-2016> (2017) Accessed: 8. April 2018.
6. Blog, G.D.S.: Botnet command server hidden in tor. <https://www.gdatasoftware.com/blog/2012/09/24033-botnet-command-server-hidden-in-tor> Accessed: 30. March 2018.
7. Paganini, P.: Botnet, pro & cons of using tor networks. <http://securityaffairs.co/wordpress/8678/cyber-crime/botnet-pro-cons-of-using-tor-networks.html> Accessed: 30. March 2018.
8. Spamhaus Malware Labs: Spamhaus botnet threat report 2017. <https://www.spamhaus.org/news/article/772/spamhaus-botnet-threat-report-2017> (2018) Accessed: 8. April 2018.
9. Yang, Y., Leung, C.: Botnets drilling away privacy infrastructure. CoRR **abs/1512.06447** (2015)
10. Dharna, P.S.: Analysis and detection of botnets and encrypted tunnels. International Journal of Computer Science Trends and Technology (2017)
11. Sanatinia, A., Noubir, G.: Onionbots: Subverting privacy infrastructure for cyber attacks. In: 45th Annual IEEE/IFIP International Conference on Dependable Systems and Networks. (June 2015)
12. Koch, R., et al.: How anonymous is the tor network? a long-term black-box investigation. Computer (Mar 2016)
13. Asha, S., et al.: Analysis on botnet detection techniques. In: International Conference on Research Advances in Integrated Navigation Systems. (May 2016)
14. Miller, S., Busby-Earle, C.: The role of machine learning in botnet detection. In: 11th International Conference for Internet Technology and Secured Transactions. (Dec 2016)
15. Su, Y.H., et al.: The forward-backward string: A new robust feature for botnet detection. In: IEEE Conference on Dependable and Secure Computing. (Aug 2017)
16. Kapre, A., Padmavathi, B.: Adaptive behaviour pattern based botnet detection using traffic analysis and flow intervals. In: International conference of Electronics, Communication and Aerospace Technology. (April 2017)
17. Higgins, J.P., Greens, S.: Cochrane handbook for systematic reviews of interventions. <http://handbook-5-1.cochrane.org/> Accessed: 08. April 2018.
18. WhitePacket: The open tor botnet (zib). <https://github.com/whitepacket/ZIB-Trojan> Accessed: 6. April 2018.
19. touyachrist: Zeus evolution. <https://github.com/touyachrist/evo-zeus> Accessed: 6. April 2018.
20. OnionScan: Onionscan: Investigating the dark web. <https://onionscan.org> (2018) Accessed: 16. May 2018.