Computer Communications 62 (2015) 59–71

Contents lists available at ScienceDirect

Computer Communications

journal homepage: www.elsevier.com/locate/comcom

Inferring distributed reflection denial of service attacks from darknet

Claude Fachkha *, Elias Bou-Harb, Mourad Debbabi

Computer Security Laboratory, Concordia University, Canada
National Cyber-Forensics and Training Alliance, Canada

ARTICLE INFO

Article history:
Received 24 April 2014
Received in revised form 13 November 2014
Accepted 26 January 2015
Available online 3 February 2015

Keywords:
DDoS
DRDoS
DNS
Darknet
Cyber threats

ABSTRACT

This work proposes a novel approach to infer and characterize Internet-scale DNS Distributed Reflection Denial of Service (DRDoS) attacks by leveraging the darknet space. Complementary to the pioneer work on inferring Distributed Denial of Service (DDoS) activities using darknet, this work shows that we can extract DDoS activities without relying on backscattered analysis. The aim of this work is to extract cyber security intelligence related to DRDoS activities such as intensity, rate and geo-location in addition to various network-layer and flow-based insights. To achieve this task, the proposed approach exploits certain DDoS parameters to detect the attacks and the expectation maximization and *k*-means clustering techniques in an attempt to identify campaigns of DRDoS Attacks. We empirically evaluate the proposed approach using 1.44 TB of real darknet data collected from a/13 address space during a recent several months period. Our analysis reveals that the approach was successful in inferring significant DNS amplification DRDoS activities including the recent prominent attack that targeted one of the largest anti-spam organizations. Moreover, the analysis disclosed the mechanism of such DNS amplification attacks. Further, the results uncover high-speed and stealthy attempts that were never previously documented. The extracted insights from various validated DNS DRDoS case studies lead to a better understanding of the nature and scale of this threat and can generate inferences that could contribute in detecting, preventing, assessing, mitigating and even attributing of DRDoS activities.

1. Introduction

Cyber attacks continue to threaten today's information technology. These threats are growing dramatically in terms of size and impact targeting large organizations, Internet service providers and governments. A DDoS attack is one of the major cyber attacks that attempts to make a computer or network resources unavailable. DDoS activities, indeed, dominate today's attack landscape. In a recent report by Arbor Networks [1], it was concluded that 48% of all cyber threats are DDoS. Further, it was stated that the top 4 perceived threats for the next 12 months will be DDoS related, targeting customers, network and service infrastructure. Governmental organizations, corporations as well as critical infrastructure were also recently deemed as DDoS victims [2–4].

A DNS-based DRDoS attack is a form of DDoS that relies on the use of publicly accessible open recursive DNS servers to overwhelm a victim system with DNS response traffic [5]. A recent event demonstrated that even a cyber security organization became a victim of the largest (i.e., 300 Gbps) DNS amplification DDoS attack in history [6]. The above facts concur that DDoS attacks in general, and DRDoS in particular, are and will continue to be a significant cyber security issue, causing momentous damage to a targeted victim as well as negatively affecting, by means of collateral damage, the network infrastructure (i.e., routers, links, etc.), the finance, the trust in, and the reputation of the organization under attack.

In this work, we tackle the following questions:

1. How to infer large-scale DNS-based DRDoS activities?
2. What are the characteristics of DNS amplification DRDoS attacks?
3. What inferences can we extract from analyzing DNS DRDoS traces?

Answering those questions would aid computer security response teams, law enforcement agencies and governments to build a darknet-based central infrastructure to scrutinize DNS-based amplification traffic in order to contribute in understanding, detecting, preventing, assessing, mitigating and even attributing of DRDoS attacks.

* Corresponding author at: Computer Security Laboratory, Concordia University, Canada. Tel.: +1 514 848 2424x3166.
E-mail address: c_fachkh@encs.concordia.ca (C. Fachkha).

http://dx.doi.org/10.1016/j.comcom.2015.01.016
0140-3664/

In this context, we frame this paper's contributions as follows:

- Proposing a systematic flow-based approach for inferring DNS amplification DDoS activities by leveraging DNS queries to darknets.
- Characterizing the inferred DDoS threats during several months period.
- Applying clustering and similarity algorithms in an attempt to identify campaigns of DNS amplified DDoS attacks.

The remainder of this paper is organized as follows: In Section 2, we provide an overview and background information on DNS amplification attacks and the darknet space. In Section 3, we present the proposed approach and elaborate on various aspects of its components. In Section 4, we empirically evaluate the approach and disclose several DNS amplified DDoS case studies. In Section 5, we survey the related work. Finally, Section 6 summarizes the paper, pinpoints some lessons learned and discusses the future work.

2. Background

In this section, we provide some background information related to the mechanism of DNS amplified DDoS attacks, the darknet space and DNS queries targeting the darknet.

2.1. DNS-based DRDoS attacks

A DNS amplification attack is a well known practice of a DDoS, in which malicious users abuse open DNS servers to bombard a victim with DNS reply traffic [5]. The technique consists of an invader directing a DNS name lookup query to an open DNS server having the source IP spoofed to be the victim's address. Subsequently, all DNS server responses will be sent to the targeted victim. In general, malicious users will request domains that cover a large zone to increase the amplification factor. In order to have a high impact on the victim, the attackers use DNS requests of type **ANY** to returns all possible known information to the victim, and hence increase the amplification of the attack. Moreover, in order to increase the size of the attack with little effort, attackers use botnets (i.e., campaigns) [7] to synchronize an army of bots and order them to send the DNS requests. Based on such concepts, Fig. 1 depicts a basic DNS amplification attack with recursive DNS. In the first two steps, the attacker uses a botnet to generate spoofed DNS lookup requests to the Internet. In step 3–7, the internal and external DNS servers collaborate in order to provide an answer to the requester. Finally, in step 8 and 9, the amplified replies congest the victim's computer and network resources with a large flood of traffic.

2.2. Darknet space

In a nutshell, darknet traffic is Internet traffic destined to unused Internet addresses (i.e., dark sensors). Since these addresses are unallocated, any traffic targeting such space is suspicious. Darknet analysis has shown to be an effective method to generate cyber threat intelligence [8,9]. Darknet traffic is typically composed of three types of traffic, namely, scanning, backscattered and misconfiguration [10]. Scanning arises from bots and worms while backscattered traffic commonly refers to unsolicited traffic that is the result of responses to DDoS attacks with spoofed source IP addresses. On the other hand, misconfiguration traffic is due to network/routing or hardware/software faults causing such traffic to be sent to the darknet sensors.

2.3. DNS queries on darknet

On the darknet space, one can also observe a significant number of DNS queries that could be sent by the following sources:

- Attacker spoofing the victim's IP: This scenario is depicted in Fig. 2a. In this case, the attacker sends spoofed DNS queries on the Internet address space using the victim's IP address. All replies from the open DNS resolvers (i.e., hosts X and Z) will bounce back towards the victim.
- Compromised victim: This scenario is depicted in Fig. 2b. In this case, the attacker uses the victim's machine to send DNS queries. The attacker might use several techniques to control the victim's machine, including malware infection and/or vulnerability exploitation. This scenario does not involve spoofed DNS queries.
- Scanner: In this scenario, the attacker scans the Internet to infer the locations of open DNS resolvers. This task requires collecting information from the reply packets and hence, a non-spoofed address is used by the scanners.
- Others: Other hosts may include firewalls to reduce the impact of the attack or misconfigured devices, etc.

In our work, we assert that high speed **ANY** DNS queries [5] will be sent from an attacker spoofing the victim's IP and/or compromised victim but not from a scanner. In other words, scanners might send **ANY** DNS queries to the Internet but with low-speed rate to avoid receiving the amplified flood of replies.

3. Proposed approach

This section presents and elaborates on our proposed approach that aims at generating darknet flows and inferring DNS-based DRDoS activities by leveraging darknet data. *The approach exploits the idea of analyzing DNS queries that target the darknet space that were originally intended by the attacker to reach Internet open DNS resolvers* [11]. Please note that our work leverages the dark space to infer and characterize amplification attacks. Intuitively, such an approach will not be able to pinpoint attacks that do not target such space; this limitation, however, is a generic drawback with any work that employs darknet to infer malicious activity [12]. In this case, our approach could be used in conjunction with other approaches that infer amplification attacks using operational non-dark spaces to provide a more comprehensive view of such attacks. Indeed, the approach takes as input darknet traffic and outputs inferred DNS amplification DRDoS insights. It is based on several components, namely, the flows generation, the detection, the rate classification and the clustering components. We discuss these components in what follows.

3.1. Flow generation

The flow generation component takes an input darknet traffic to produce flows of traffic on a daily basis. A flow is defined as a series of consecutive packets sharing the same source IP address targeting darknet addresses. In order to generate such flow, (1) we collect network traces that consist of a unique source and destination IP pair, and (2) merge all flows that belong to the same source IP.

3.2. Detection component

The detection component takes as input darknet traffic and outputs DNS-based DRDoS flows. To achieve the detection task, we base our detection component on analyzing DNS queries targeting darknet addresses. These DNS queries are attempts towards port 53. In order to detect DNS amplification DDoS, we built our