Chapter 19
Advanced Network Data Analytics for Large-Scale DDoS Attack Detection

Konstantinos F. Xylogiannopoulos
University of Calgary, Calgary, Canada

Panagiotis Karampelas
Hellenic Air Force Academy, Dekelia, Greece

Reda Alhajj
University of Calgary, Calgary, Canada

ABSTRACT

Internet-enabled devices or Internet of Things as it has been prevailed are increasing exponentially every day. The lack of security standards in the manufacturing of these devices along with the haste of the manufacturers to increase their market share in this area has created a very large network of vulnerable devices that can be easily recruited as bot members and used to initiate very large volumetric Distributed Denial of Service (DDoS) attacks. The significance of the problem can be easily acknowledged due to the large number of cases regarding attacks on institutions, enterprises and even countries which have been recently revealed. In the current paper a novel method is introduced, which is based on a data mining technique that can analyze incoming IP traffic details and early warn the network administrator about a potentially developing DDoS attack. The method can scale depending on the availability of the infrastructure from a conventional laptop computer to a complex cloud infrastructure. Based on the hardware configuration as it is proved with the experiments the method can easily monitor and detect abnormal network traffic of several Gbps in real time using the minimum hardware equipment.

DOI: 10.4018/978-1-7998-5348-0.ch019

INTRODUCTION

In recent years, the number of Internet enabled devices is increasing everyday exponentially. According to Ericsson Mobility Report (Ericsson, 2016) in the third quarter of 2016 there are more than 7.5 billion mobile subscriptions worldwide and most of the half of them are broadband. In most of the countries the penetration rate is over 100% which means that there are more mobile devices than the population. In UK in the first quarter of 2016 the percentage of mobile users between the adult population was 93% while more than 71% of the adult population use smart phones and 66% of the mobile users use their smart phone to access the Internet as reported by OfCom (OfCom, 2017). Apart from smart phones, other internet-enabled devices have appeared such as smart TVs, watches, security cameras, printers, washing machines, etc. which are connected to the Internet either directly or through pairing with a smart phone. All these devices are potential victims of the malevolent hackers who wish to exploit security weaknesses of the new devices and the privacy insensitivity or even ignorance of the users. As the number of the devices is increasing and as more and more types of devices are Internet-connected, the possibility of a device high jacking is also increasing. The most apparent reason for this is stealing private information such as financial information, personal emails and photos, etc. which can be used by the attacker for personal gain. However, someone would wonder why someone would like to take control of a smart washing machine apart from playing a trick on the device owner? A smart device, part of the Internet of Things (IoT), since it is connected to Internet is a valuable resource of the network and can be used in the service of, for example, a bot network to attack other legitimate users of the network. This type of attacks has already been reported (Kührer et al., 2014) especially using devices such as routers, VoIP gateways, network printers and surveillance cameras. Latest reports from various security firms have disclosed several serious attempts for distributed denial-of-service volumetric attacks attributed to IoT botnets. An example of such a DDoS attack was reported on September 2016 against the Brian Krebs's security blog. An attack that created traffic of over 600 Gbps and was attributed to an IoT botnet created by Mirai malware (Bertino & Islam, 2017). The same month another attack was reported against the OVH French webhost at 1.1 or more Tbps (US CERT, 2017). On October 21st, 2016, Dyn Service Provider in the US experienced the largest so far reported DDoS attack of more than 1 Tbps which again is attributed to the infected from Mirai malware IoT devices (Arbor Networks, 2016).

In addition to the proliferation of internet-enabled devices and the corresponding security issues that have raised, there is also a proliferation of electronic services that are available through the cloud infrastructure that have also become the main target of several DDoS attacks. The consequences of such attacks in the cloud infrastructure are not only catastrophic to the attacked services but they may also affect other services that are not in the spot due to the possible migrations of the virtual machines of these other services during the attack (Somani, Gaur & Sanghi, 2015). In other cases, some services may depend or may serve other websites and as a result when an attack disrupts the operation of the former, the latter also experience problems. As an example of how a DDoS attack in a Service Provider can affect other services is the aforementioned case of Dyn which is a dynamic DNS service provider offering services to several other companies such as Etsy, PayPal, Microsoft, GitHub, Reddit, Twitter, etc. As a result of the 21st of October attack to Dyn, several services of the other companies were not accessible at least to the East coast of United States (Arbor Networks, 2016). Other services, that are directly targeted, are usually those of commercial companies such as Yahoo, Dell, eBay, Amazon, ZDNet, British Telecom and in 2015 Blizzard WoW, GitHub, New York Magazine, Dreamhost and several other services which may experience downtime from few minutes to several hours due to DDoS