


Chapter 5

Detecting DDoS Attacks on Multiple Network Hosts: Advanced Pattern Detection Method for the Identification of Intelligent Botnet Attacks

Konstantinos F. Xylogiannopoulos

 <https://orcid.org/0000-0003-2376-898X>

University of Calgary, Canada

Panagiotis Karampelas

 <https://orcid.org/0000-0003-1684-7612>

Hellenic Air Force Academy, Greece

Reda Alhaji

University of Calgary, Canada and Global University, Lebanon

ABSTRACT

The proliferation of low security internet of things devices has widened the range of weapons that malevolent users can utilize in order to attack legitimate services in new ways. In the recent years, apart from very large volumetric distributed denial of service attacks, low and slow attacks initiated from intelligent bot networks have been detected to target multiple hosts in a network in a timely fashion. However, even if the attacks seem to be “innocent” at the beginning, they generate huge traffic in the network without practically been detected by the traditional DDoS attack detection methods. In this chapter, an advanced pattern detection method is presented that is able to collect and classify in real time all the incoming traffic and detect a developing slow and low DDoS attack by monitoring the traffic in all the hosts of the network. The experimental analysis on a real dataset provides useful insights about the effectiveness of the method by identifying not only the main source of attack but also secondary sources that produce low traffic, targeting though multiple hosts.

DOI: 10.4018/978-1-7998-5348-0.ch005

INTRODUCTION

Distributed Denial of Service (DDoS) attacks tend to be one of the major security threats against information system infrastructure. In the first half of 2018 according to Netscout took place more than 2.8 billion attacks with escalated metrics such as volume and maximum size (Modi, 2018). This is mainly attributed to the rapid deployment of Internet of Things (IoT) devices in various application fields such as automotive applications, industrial sites, consumer places, smart cities, etc. The latest reports estimate the active IoT devices to 27 billion in 2018 and project them to 125 billion by 2030 (HIS Markit, 2017). These devices can be smart TVs, watches, security cameras, printers, washing machines, smart vehicles, autonomous sensors, etc. which most of the times are connected directly to the Internet. According to security experts (Bhattacharya, 2018 and OWASP, 2016), there is a large number of potential vulnerabilities in IoT devices ranging from insecure or misconfigured web servers, insufficient authentication mechanisms that communicate the user credentials in text to insufficient configuration with default passwords, etc. As a result, while 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. From 2014, there are reports of exploiting vulnerabilities in routers, VoIP gateways, network printers and surveillance cameras in order to realize DDoS attacks against legitimate services (Kührer et al., 2014). The following years, several DDoS attacks were reported to have been initiated by bot networks constituted by IoT devices. On September 2016, an attack that created traffic of over 600 Gbps and was attributed to an IoT botnet created by Mirai malware was unleashed against Brian Krebs's security blog (Bertino and Islam, 2017). At the same time, another attack was reported against a French webhost called OVH at 1.1 or more Tbps (US CERT, 2017). Later in the same year, Dyn Service Provider in the US experienced a very large DDoS attack of more than 1 Tbps which again is attributed to the infected from Mirai malware IoT devices (Arbor Networks, 2016). In 2017, several more DDoS attacks took place in companies from different business domains interrupting their services for several hours. In August 2017, Dreamhost one of the biggest web hosting companies suffered a DDoS attack targeting their DNS servers making the hosted by the company websites inaccessible for four hours (Blake, 2017) while in October 2017 a DDoS attack put offline the UK National Lottery's website during the Saturday's draws when a lot of people were ready to play in the lottery (Cluley, 2017). Another victim, on November 2017, was the US newspaper Boston Globe that suffered from a two-day DDoS attack which made their websites inaccessible for most of the period of both days (Bray, 2017). The DDoS attacks have continued in 2018 culminating with the largest known so far DDoS attack against GitHub with peak at 1.35Tbps which was successfully mitigated after 10 minutes of service unavailability moving the traffic to the infrastructure of an edge computing provider Akamai (Kottler, 2018). 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 and Sanghi, 2015). In GitHub, for example, the intermission of operation affected several other companies that use GitHub as their code repository and thus during the attack they were not able to run their businesses. Apart from individual companies, several governmental services have also been targeted by DDoS attacks. Several such incidents have been reported in the past in several countries such as Georgia, Estonia, Ukraine, Syria, UK, USA, etc. (Loukas and Oke, 2010) where multiple governmental services become unavailable during the DDoS attacks. A more recent attack on November 2016 in Liberia targeted two Internet Service Providers that operate the only fiber Internet cable that connects the country to the Internet (Kolkman, 2016). The specific attack which interrupted

13 more pages are available in the full version of this document, which may be purchased using the "Add to Cart" button on the publisher's webpage:

www.igi-global.com/chapter/detecting-ddos-attacks-on-multiple-network-hosts/261972

Related Content

The Comprehensive Approach as a Strategic Design to Run the Military-Industrial Complex in Operations

Mirva Salminen and Aki-Mauri Huhtinen (2012). *International Journal of Cyber Warfare and Terrorism* (pp. 22-30).

www.irma-international.org/article/the-comprehensive-approach-as-a-strategic-design-to-run-the-military-industrial-complex-in-operations/81251

The States' Reflexes in This War and Struggle of the Middle East Countries Over the COVID-19 Pandemic in the Soft and Hard Wars Started All Over the World

Ouz Keskin, Mortaza Chaychi Semsari, Ahmet Gedik, Gudrat Badalov and Somayyeh Bikari (2023). *Handbook of Research on War Policies, Strategies, and Cyber Wars* (pp. 352-365).

www.irma-international.org/chapter/the-states-reflexes-in-this-war-and-struggle-of-the-middle-east-countries-over-the-covid-19-pandemic-in-the-soft-and-hard-wars-started-all-over-the-world/318513

Convolutional Neural Network-Based Automatic Diagnostic System for AL-DDoS Attacks Detection

Fargana J. Abdullayeva (2022). *International Journal of Cyber Warfare and Terrorism* (pp. 1-15).

www.irma-international.org/article/convolutional-neural-network-based-automatic-diagnostic-system-for-al-ddos-attacks-detection/305242

Cyberpeacekeeping: New Ways to Prevent and Manage Cyberattacks

A. Walter Dorn and Stewart Webb (2019). *International Journal of Cyber Warfare and Terrorism* (pp. 19-30).

www.irma-international.org/article/cyberpeacekeeping/224947

The Need for a National Data Breach Notification Law

Kirk Y. Williams (2016). *National Security and Counterintelligence in the Era of Cyber Espionage* (pp. 190-202).

www.irma-international.org/chapter/the-need-for-a-national-data-breach-notification-law/141046