Chapter 25
Prediction, Detection, and Mitigation of DDoS Attacks Using HPCs:
Design for a Safer Adaptive Infrastructure

Pablo Pessoa Do Nascimento
Universidade Federal de Pernambuco, Brazil

Isac F. A. F. Colares
Universidade Federal de Pernambuco, Brazil

Ronierison Maciel
Universidade Federal de Pernambuco, Brazil

Humberto Caetano Da Silva
Universidade Federal de Pernambuco, Brazil

Paulo Maciel
Universidade Federal de Pernambuco, Brazil

ABSTRACT

Web service interruptions caused by DDoS (distributed denial of service) attacks have increased considerably over the years, and intrusion detection systems (IDS) are not enough to detect threats on the network, even when used together with intrusion prevention systems (IPS), taking into account the increase of assets in the traffic path, where it creates unique points of failure in the system, and also taking into account the use of data that contains information about normal traffic situations and attacks, where this comparison and analysis can cost a significant amount of host resources, to try to guarantee the prediction, detection, and mitigation of attacks in real-time or in time between detection and mitigation, being crucial in harm reduction. This chapter presents an adaptive architecture that combines techniques, methods, and tools from different segments to improve detection accuracy as well as the prediction and mitigation of these threats and to show that it is capable of implementing a powerful architecture against this type of threat, DDoS attacks.

DOI: 10.4018/978-1-7998-5728-0.ch025

INTRODUCTION

Having in mind that computer system disruptions caused by a distributed denial of service (DDoS) attacks are now more prevalent than ever and the trend is growing. And only Intrusion Detection Systems (IDS) are not enough to detect threats on the network, even when used in conjunction with Intrusion Prevention Systems (IPS), as these devices work directly with signatures and their effectiveness is vulnerable to unknown attacks, where these attacks can successfully simulate legitimate traffic without being detected, as there are no records or signatures of these attacks; therefore, malicious traffic can be identified as legitimate traffic without being detected by IDS/IPS systems, producing False Positives (FP), which is a complex network topology may come to harm legitimate users of the web service or making it unavailable for legitimate users (Ndibawela, Govardhan, Okada, & Kadobayashi, 2015).

Also take into account that the use of data sets containing information about attack situations and normal traffic, for validation of detection techniques and tools, is a very challenging approach, as many of these data sets do not portray the current reality, they are incomplete or they cannot be shared, as they contain confidential confidential information (Sharafaldin, Lashkari & Ghorbani, 2018; Pelloso, Vergu, Santos & Nogueira, 2018). Techniques using data sets require a relevant amount of resources and an active comparison of traffic with the data set can generate a significant load on the asset, which depending on where this analysis and comparison is made, the specific asset can be overloaded, when they are the target of attacks, which can cause the service to suffer instability or even become unavailable (Sengupta, Chowdhary, Sabur, Huang, Alshamrani, & Kambhampati, 2019).

The combination of several classifiers can improve detection accuracy, together with techniques and tools from different procedures, can provide action plans capable of minimizing damage, thus being a powerful defense against this type of threat, which are DDoS attacks (Righi, 2017). Thus, providing an adaptable model that identifies malicious agents and provides decision-making (such as reducing the baud rate), to ensure the availability of the Web service in future threat systems (Addepalli, Karri, & Jyothi, 2017). The information in the application access log can be used, for example, in crime situations where the web service was; or, in cases of confirmed attacks, users can be notified, considering that their machines are often used in a botnet network without their knowledge (Maciel, Araujo, Dantas, Melo, Guedes, & Maciel, 2018).

It is possible to develop a defense mechanism, analyzing the host's behavior and using the performance counters present in the processors, the Hardware Performance Counters (HPCs), where the occurrences of low-level hardware events are monitored, correlating the events with the network. statistics, such as the number of requests in the application and the number of users connected, it is possible to create a filter at the application level, using a performance model that predicts the impact of requests, being able to make decisions when suspicious traffic is identified, sending it for later analysis, which may result in the removal of the filter or the presentation of a CAPTCHA to the user, to verify legitimate access (Singh, & De, 2015).

Techniques and tools that have fixed limits for detection and alerts are vulnerable to limits of learning limits, where once the malicious agent knows how far he can consume the bandwidth of the network, it sends attacks below this limit, consuming the bandwidth of the network. service, without being detected by the security systems the limit, having this mentality the implementation of techniques and mechanisms of dynamic variation of the detection limit, is a viable strategy in situations like these to avoid attacks of this nature (Compton, 2019).