Distributed Threat Analytics System for Denial-Of-Service Attacks

Prabhakar Krishnan, Vinay Gurram

Abstract*:*In recent years, we have seen the rise of application specific attacks that exploit the vulnerabilities in the network protocols (HTTP, DNS, SMTP, other) and try to overwhelm the server application, not just the connectivity pipe. In this paper, we propose an advanced DoS Threat Analytics System (DTAS) to mitigate the full range of DoS network attacks – not just volumetric, based on comprehensive collaborative detection algorithms, implemented in the Elasticsearch Big Data platform. DTAS security solution is driven by powerful threat detection algorithms that: a) dissects all attack probabilities in the network traffic, b) Uses behavioural analytics to correlate multiple parameters and generate multi-vector representations, c) Employs dynamic challenges to verify normal versus attack traffic. The DTAS analytics engine analyses multiple IP attributes within TCP and UDP flows, ICMP, HTTP and DNS traffic, count, frequency, headers, payloads, detecting covert traffic, amplification attacks trying to target the services on the network. By measuring all these attributes, our system creates a multi-vector heuristic representation of the normal or baseline traffic flows. We have used datasets from UCLA, downloaded traces from real world incidents and tested the efficacy of the system with various large-scale simulated DoS attacks in the test network. Our experiments show that the DTAS framework can detect DoS attacks in real time, without impacting the latency to benign traffic in the network and with accuracy up to 95% detection rate for attacks.

Index Terms*: *Botnet,Distributed Denial of Service (DDoS) attack, Network Security, Threat Analytics

I. INT RODUCTION

DDoS/Botnet attacks are on the rise as the network is growing at rapid pace due to the digital transformation of human lives and operations. Hence, they pose complex, tough challenges to enterprises, data center administrators, security agencies and solution vendors and research communities, security solution vendors, researchers, enterprises, Internet access and Cloud services providers. A malicious node or a group of nodes, aiming to deny access to resources on computer networks, causes these DoS attacks and they are also called availability-based attacks.Detection and defense mechanisms are just evolving to keep up with such attacks. Such DoS attacks have been there over decades, but the recent phenomenon and scale and sophistication of this 'denial of service have evolved dramatically due to commercial gain & criminal motives of local adversaries and also other state agencies. Such attacks include distributed (DDoS) using a network of victim machines harvested from the public cloud called 'botnet attacks, data amplification attacks using vulnerable network protocols (such as DNS, HTTP,TCP) Distributed reflector (DRDoS) attacks. Given this trend, these attacks and threat cannot be mitigated by legacy approaches and on-the-premise defense solutions. With the rise of “Internet-of-Everything”(IoE/T) comes the need for higher security. According to research firm Gartner, 63% of in use IoT devices in 2017 are consumer products. Some of the hardest problems in security have been the “Distributed Denial of Service (DDoS)” [1] and reports of DDoS attacks have also been on the increase. According to *Corero* Network’s DDoS Trends and Analysis report [2] “The reason for rapid surge in DDoS attacks is attributed to increase in frequency to the growing availability of DDoS-for-hire services, and the proliferation of unsecured Internet of Things (IoT) devices”. In 2016, “Mirai botnet” [3] was the first reported massive DDoS-attack, as the Internet services in eastern-coast of US became offline caused by this attack, using an army of hacked surveillance cameras that attacked the largest managed DNS infrastructure at Dyn. These series of attacks sparked attention and serious consideration for the security of “IoT or smart” devices and the trustworthiness of the data from the associated applications. Kaspersky Research Lab [4] reported botnet consisting of five million devices such as routers, switches and modems. Botnets have been the primary means causing application layer DDoS flooding attacks, growing to 1Tbps rate, it seems the real challenges of botnets have just started. The use of AI has also become more widespread with hackers utilizing AI-based botnets, launching noise generation attacks to weaken the automated defense systems. We had seen the recently Black Nurse DDoS attack targets firewall vulnerable to ping flood, which is vulnerable of ICMP protocol: type 3, code3 destination port unreachable. This attack exploited the vulnerabilities of firewall rules. This attack leverages ICMP packets against the clients primarily based on news and by simply disabling the ICMP type 3.One of the large DDoS attacks on Dyn DNS in October 2016.It had taken down twitter, Spotify, Netflix, GitHub, amazon and Reddit and other websites throughout the attack. The crimes were committed by Mirai botnet a group of anonymous attackers announced by cyber security news.

Manuscript published on 30 March 2019.
*****Correspondence Author(s)

Prabhakar Krishnan Amrita Center for Cybersecurity Systems and Networks, Amrita School of Engineering,Amrita Vishwa Vidyapeetham, Amrita University, Amritapuri, India.
Vinay Gurram, Amrita Center for Cybersecurity Systems and Networks, Amrita School of Engineering,Amrita Vishwa Vidyapeetham, Amrita University, Amritapuri, India.

Attack was committed due to vulnerabilities in IoT devices, home routers, printers etc. Mirai botnet requested to launch to all vulnerable devices on Dyn DNS servers.

The network-based malware campaign attacks the transport protocol standard layers “(i.e. IP, UDP, ICMP,TCP) and also target network services such as DNS,HTTP. Attacks aimed at networking stack layers 3/4 are flooding type, so as to saturate the network and make it unresponsive to legitimate services traffic”. The attacks in the layers above the IP, for e.g. TCP,DNS, HTTP are tough to detect and mitigate with a traditional standalone firewall solution.

Very large-scale attacks from layers 3 and above always originate from distributed sources and such distributed attacks are targeted to one victim network or service. such attack traffic can saturate the victim network and also overwhelm the firewall or gateway on the edge. There is trend of botnet driven attacks, in which a fleet of benign machines are recruited through some dropper malware and control/command adversary can orchestrate a massive distributed attack campaign, targeting a network or enterprise or region or DNS zone. As the attack is meant to affect the availability, the attack packets are just one-way with spoofed IP/MAC addresses and with automated spoofing tools available to the attackers the packet stream content and headers arerandomized, beating the filtering mechanisms at the firewall or IDS.Conventional DDoS detection systems were originally designed to stop volumetric attacks, the most rudimentary of DDoS assaults. The key objective our work is to develop an advanced DDoS protection system, with distributed implementation and deployed in collaborative way with end-points and firewall or IDS devices in the large network. Our next-generation DoS detection system called DTAS, can be deployed in the enterprise network at the network gateway level or as a network service similar to Network Function Virtualization (NFV) and as an security application in the modern Software Defined Networks (SDN). This paper is organized as : Section I provides an introduction to SDN threat landscape and sets the context, Section II presentsthe taxonomy of DDoS Attack Vectors, Section III discusses the prior research work in the related area, Section IV presents our proposed methodology and architecture, Section V describes the implementation, Section VI presents the evaluation and experience with an early prototype DDoS threat analytics system and conclusion.

II. Security threats, risks and attack vectors

In this section, we will categorize the DDoS threat and attack vectors in an enterprise network. DDoS attacks are quite wide and have broad attack vectors. We first present a taxonomy of the common DDoS attack methods in Fig. 1.

Our system classifies the DDoS attacks into 2 main classes:

1. Bandwidth depletion: This attack floods the victim network with malign traffic and garbled packets, hence denying the legitimate service packets from reaching the servers in that network. This type of attack can further be characterized as flooding (just indiscriminate traffic generation) or amplification (in which a particular protocol packets are replicated multiple times) attacks.
2. Resource depletion: This attack is designed to steal or consume or exhaust the resources of a target service or a victim system. Thus, the victim system or service will be unable to process legitimate requests from its clients or users. Such attack is commonly executed by sending malformed packets to misuse the network communication protocols.

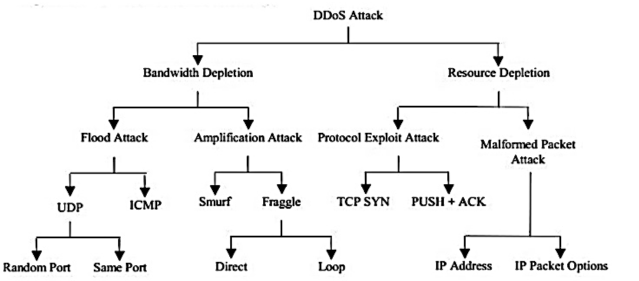

Fig 1. DDoS Attack Taxonomy

III. Related works

DDoS attacks show traffic pattern different from genuine traffic and the main goal of a DoS detection system is to detect these attack patterns based on packet capture and traffic analysis. The authors of research work [5] presented existing DDoS mitigation strategies in the cloud network. They have also shown how some of the behavioral characteristics of the DDoS attacks can bring new approaches to cloud security.Kubra[6] presented a systematic review of entropy-based detection mechanisms for DDoS attacks. They have studied state-of-the-art filtering techniques and documented the advantages and shortcomings. The authors in the research work [7] had proposed a novel filtering mechanism based on client based on client query network entropy, classification of client addresses and recursive characteristics in DNS protocol/server hierarchy. They created a whitelist by selecting legitimate clients with query times high or long tailed, high rank FRS and so on. So, this classification technique results into DNS servers that support recursive name lookups, web crawlers, spiders and any other legitimate bots running from well-known domains.

In the research work by Chang et.al [8], authors have proposed an attack classification scheme with machine learning approach. They implemented ANN for attack detection and used the Apache Spark streaming analytics system. The methodology of their work runs into five phases namely: “(1) Packet Collector, (2) Hadoop HDFS, (3) Format Converter, (4) Data Processor, (5) Neural Network detection. Their classification algorithm used network attributes from IP headers and the main features used by their ANN(Artificial neural networks) to detect the DDoS attacks are:1) Number of packets,2) Average of packet size,3) Time interval variance,4)Packet size-variance,5)Number of bytes,6) packet rate,7) bit-rate”. Authors claim that the main feature of their work is the implementation with Apache Spark, which does in-memory computing that makes their analytics program to run 100x faster than in traditional computing architecture.

Our work combines the key features of the above-mentioned research [8] and advance in multiple axes, construct an analytics framework that process huge amount of network traffic data and to achieve accuracy we have distributed collaborative behavior engine to detect the temporal and spatial correlations in the traffic pattern. And the responsiveness of this system is fast due to our implementation in Elasticsearch (ELK) framework and further acceleration using GPGPU machines.

IV. DoS Threat Analytics System (DTAS)

To address the key shortcomings and limitations of the existing solutions, we propose our future work a novel framework to effectively detect and mitigate DDoS attacks. Our proposed frameworkcalled *DTAS*, the system architecture is shown in Fig.2.

The major components of the DTAS are described here:

ELK stands for *Elasticsearch Logstash and Kibana* which are technologies for big data analytics. We can import network traffic data into elastic search database, indexed and do behavioral , statistical analytics with data and visualize it in *Kibana* and trigger alarms using Watcher.

Elastic search: It is used for indexing every attack dataset in JSON format applying index name, type, id and mapping data with respect to every attack, characteristics applying characteristics on the indexed data set. It is one of the fastest searchable data-store for big data analysis.

Logstash: This is used for parsing, filtering the required information from the input network or log data and transport to the index of the elastic search. It can collect the information from many fields like MySQL table, MongoDB or *csv*. And adaptable to funnel data from any type of sources, mainly parsing and pushing into elastic search data-store.

Kibana: It is used for building dashboard , running analytic algorithms on the Elasticsearch data-store and visualize. The best advantage is that we can create dynamic dashboards, slice and dice, gain insights into the data in charts, data table, line chart, markdown widget, tile maps, pie charts, vertical bar chart, time series, etc.

Packetbeats: The near real time data can be collected by Packetbeats module. It is a lightweight network data shipper.

Watcher: It is an API for creating, managing and testing watches. A watch describes a single alert and can contain multiple notification actions.

Based on the system architecture our DTAS work-flowmethodology runs into five phases.

1. Packets/data collection using packet beats or file beat or elastic search,
2. Logstash using for collecting, parsing and transporting the data into elastic search,
3. Saving, indexing, searching data with elastic search,
4. Visualization of data and analytics in kibana.
5. Detection and alarming or alerting using watcher.

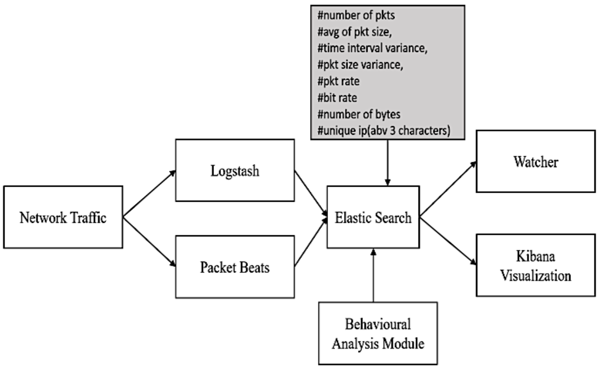

Fig 2 DTAS Framework

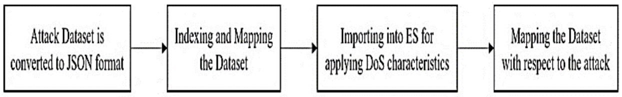
Attack Dataset is converted to JSON format
Indexing and Mapping the Dataset
Importing into ES for applying DoS characteristics
Mapping the Dataset with respect to the attack

Fig 3. Workflow of Elasticsearch

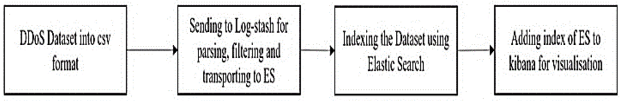
DDoS Dataset into csv format
Sending to Log-stash for parsing, filtering and transporting to ES
Indexing the Dataset using Elastic Search
Adding index of ES to kibana for visualisation

Fig 4. Workflow of Logstash

V. IMPLEMENTATION

DoS detection phase: we will be taking characteristics to detect DoS attack from a hybrid approach Fig.2. We have started with existing scripts, data samples on ELK stack with respect to all attacks which represented in kibana dashboard visualization. We have tried with snort IDS, but it could not capture each and every packet of incoming traffic with large number of responses. So, we have included packet beats for tapping network data along with snort rules which is WL, BL & RL. Whatever DoS attack, it would have to pass through this detection phase as its connected in-line or passive tap at the network gateway.

PCAP replay attack: Taking *pcap* file and replaying the attack scenario in some closed and restricted surroundings with a similar situation.

Analysis: Based on the characteristics of information in kibana, we can do post analysis of the attack, target of the attack, sources and destination addresses, port numbers etc.
Attack detection: Based on the frequency of traffic and average packet size with reference to the time, If the attacker had set up the botmaster with a similar number of packets per second or minute, remaining all bots will do attack with the same amount which was such by the bot master.

VI. Evaluation and Analysis

The DTAS is deployed in the test network(Fig.5) that emulated real life enterprise network and simulated attacks. The live network data tapped and captured by packetbeats and the output is pushed by Logstash into indexing of elastic search. DTAS triggers actionable detection alerts and rules that is fed into the enterprise network Firewall/IDS and the attacks are prevented from further crossing the gateway.We have taken DDOS data set from Laboratory for Advanced Systems Research (LASR) at the University of California, Los Angeles (UCLA) and also the captured attack traffic and fed into the DTAS system.

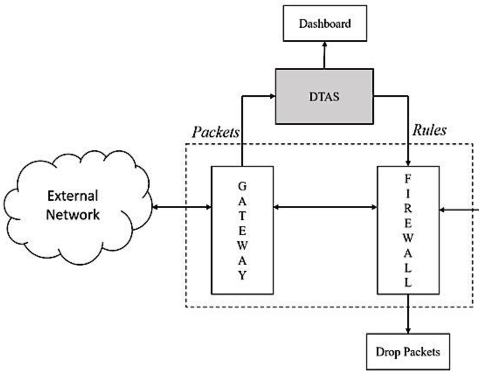

Fig 5 DTAS Deployment

Attributes that are used for our behavioral analysis include volume of traffic (Layer 3-7 protocols such as TCP, ICMP,UDP, DNS, HTTP), number of hostnames per domain, geographic location and domain history.

Other attributes include: 1) total packet count, 2) Ave. packets size, 3) inter-packet gap, 4) velocity of the packet stream5)total bytes,6) standard deviation, 7) entropy and variance.

We have taken four different attack scenarios (Fig.6-9):

1. Constant rate attack
2. Pulsing attack
3. Increasing rate attack
4. Gradual pulse attack

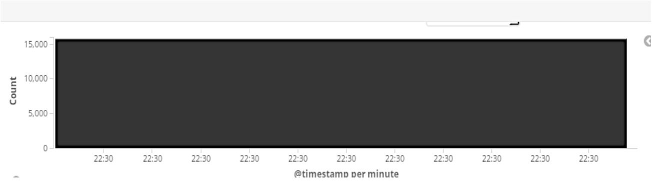

Fig 6 Constant Rate Attack

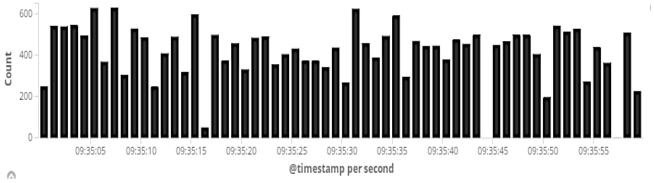

Fig 7. Pulsating Attack

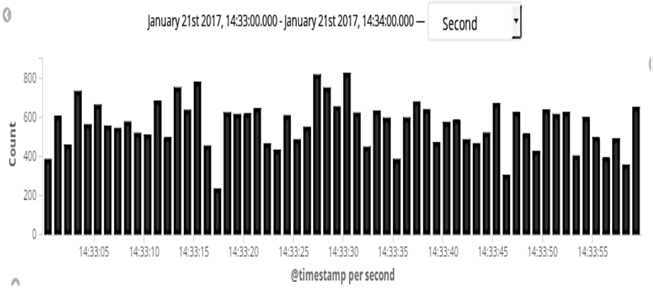
January 21st 2017, 14:33:00.000 - January 21st 2017, 14:34:00.000 — Second

Fig 8. Increasing Rate Attack

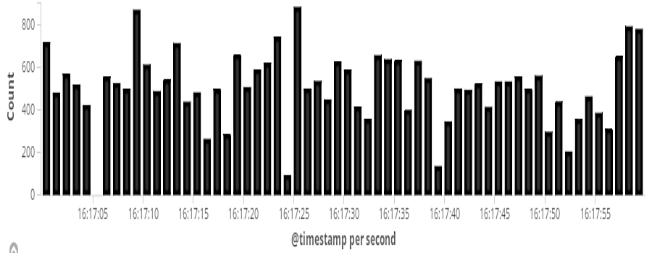

Fig 9. Gradual Pulse Attack

We evaluated the effectiveness of our prototype DTAS in how quickly it can restore the throughput of legitimate traffic in the presence of given DDoS attacks. The results are shown in Fig. 10, it took less than 10 seconds for the legitimate traffic to recover its throughput after the mitigation started. Thus, we can conclude that DTAS generally provides rapid mitigation response in restoring the performance of the legitimate traffic.

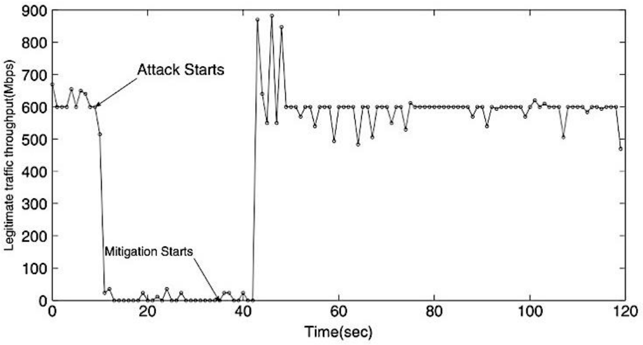

Fig 10. Response of DTAS under Attack

VII. CONCLUSION

In this paper, we presented an advanced distributed detection system for DoS attacks, leveraging big data platform. Our proposed solution consists of open source framework ELK stack, *packetbeats* and SNORT/IDS, that are proven technologies and readily available for implementation. The observations in our experiments proved that the DTAS framework has the capabilities to investigate the DDoS attacks with varying intensities and voluminous , asymmetric flow patterns as well.

Even though some of those DDoS attacks that happened recently, involve public IoT devices such as cameras, there's no reason to think that they are likely the only source of future DDoS attacks. As more and more devices (fridges, fitness trackers, sleep monitors etc.) are added to the Internet they'll likely be unwilling participants in future attacks.

We plan to advance our research and build a cooperative multi-domain DDoS framework with multiple parties, researchers and also crowd source malware samples from DoS attack victims to train the ML-based threat analytics and early warning system.

REFERENCES

1. Shameli-Sendi et al. "Taxonomy of distributed denial of service mitigation approaches for cloud computing." Journal of Network and Computer Applications 58 (2015): 165-179.
2. Corero DDoS Trends Report,2017 http://info.corero.com/DDoS-Trends-Report.html
3. “Source code for IoT botnet Mirai released”, https://krebsonsecurity. com/2016/10/source- code- for- iot- botnet- mirai- released/
4. Vladimir Kuskov et al. “Honeypots and the Internet of Things”, Kaspersky Research - https://securelist.com/honeypots-and-the-internet-of-things/78751/
5. Krishnan, Prabhakar, Jisha S. Najeem, and Krishnashree Achuthan. "SDN Framework for Securing IoT Networks." In International Conference on Ubiquitous Communications and Network Computing, pp. 116-129. Springer, Cham, 2017
6. Kalkan, Kübra et al. "Filtering-Based Defense Mechanisms Against DDoS Attacks: A Survey." IEEE Systems Journal (2016).

*Published By:
Blue Eyes Intelligence Engineering
and Sciences Publication (BEIESP)
© Copyright: All rights reserved.*

7. Pan, Lanlan, Xuebiao Yuchi, and Yong Chen. "Mitigating DDoS attacks towards Top Level Domain name service." Network Operations and Management Symposium (APNOMS)18th Asia-Pacific. IEEE, 2016.
8. Hsieh, Chang-Jung, and Ting-Yuan Chan. "Detection DDoS attacks based on neural-network using Apache Spark." Applied System Innovation (ICASI), 2016 International Conference on. IEEE, 2016.
9. Fachkha, Claude, Elias Bou-Harb, and Mourad Debbabi. "Fingerprinting internet DNS amplification DDoS activities." New Technologies, Mobility and Security (NTMS), 2014 6th IntlIEEE Conference.
10. Acarali, Dilara, et al. "Survey of approaches and features for the identification of HTTP-based botnet traffic." Journal of Network and Computer Applications 76 (2016): 1-15.
11. Holl,Patrick."ExploringDDoSDefenseMechanisms."Network25(2015).
12. Zargar et al. "A survey of defense mechanisms against distributed denial of service (DDoS) flooding attacks." IEEE communications surveys & tutorials 15.4 (2013): 2046-2069.
13. Mekhitarian, Araxi, and Amir Rabiee. "A simulation study of an application layer DDoS detection mechanism." (2016).
14. B. Pa Poornachandran, Premjith and K. P. Soman, “A distributed approach for predicting malicious activities in a network from a streaming data with support vector machine and explicit random feature mapping,” in IIOAB Journal, 2016, pp. 24–29.