Comparison of DDOS detection methods in real world scenario

Vladislav Bidikov and Igor Mishkovski
Faculty of Computer Science and Engineering
Ss. Cyril and Methodius University
Skopje, North Macedonia

vladislav.bidikov@finki.ukim.mk
igor.miskovski@finki.ukim.mk

***Abstract*—In this paper we will see the current and new developed methods for distributed denial of service attack (DDOS) detection. We will also see some of the possibility for mitigation of attacks in scenarios where they are detected sooner. We will use data from the DDOS attack in June/August/September 2022 on the Faculty and learn valuable lessons from there.**

***Index Terms*—DDOS attacks, networks, protection, netflow, sflow, bgp;**

I. Introduction

DDOS attacks are trending in the last years. And general movement of services to the Cloud create challenges in the ecosystem with trends evolving.[6]. Even in 2023 most of DDOS attacks are volumetric and using amplification methods in order to achieve the goals. DDOS attacks are prevalent but hard to defend against, due to the volatility of the attacking methods and patterns used by attackers, so understanding the DDoS attacks can provide new insights for effective defense since usually existing understandings are based on indirect traffic measures or traffic seen locally.[8] In this paper we will analyse the trends of amplification and also compare detection methods in a real world scenario of a DDOS attack which we saw at the Faculty of Computer Science and Engineering. Possible methods of defence will not be analysed in details.

II. Anatomy of DDOS attacks

A. Size, Methods and Impact

If the past DDOS attacks where generated using hosts (servers) which where the source of unwanted traffic. With the evolution of Internet of Things (IoT) devices and their limited security posture, these devices where usually seen as good source of traffic and this created a new ecosystem of botnets based on IoT devices. One of the biggest botnet is still the Mirai variants which still evolves and try to source as many devices as possible. Even after years of existence and efforts to st it's spread the Mirai-botnet is the biggest enrolled botnet that utilizing IoT devices.[7] One of the other techniques for more efficient DDOS attacks is finding amplification devices which can further increase the volume of the attack. At the current time, this is limited to number of unsafe and well known and used protocols which are described in Table I.

TABLE I
UDP-based amplification attacks

Protocol	Amplification factor
Mitel MiCollab	2200000000
Memcached	50000
NTP	557
CHARGEN	359

If we see the whole picture and combine these facts we can have a ideal botnet which can use the IoT spreading concept and then attack targets by using these amplification protocols crafting a powerful volumetric attack. In the last months, we also see a new breed of botnets which combine both IoT devices and virtual private servers (VPS) in cloud infrastructure providers which even more increased the capability and volume of these volumetric attacks.[1]

B. Detection methods

For years monitoring network devices was the main tool for detection of problems as well as possible DOS attacks. The usual sign of a attack is when a link reaches full capacity. Other measurements where usually connected to the resources of routing hardware where CPU and memory exhaustion was also seen as sighs of attack. This landscape dramatically changed when network equipment became capable of using sapling protocols from the Netflow family which opened a new model of network monitoring and analysis.[5] Based on Netflow (with several extensions to the protocol version) and later IPFIX we see a whole market of software tools both open source and commercial. They share a common detection concept based on the flow data they receive and then try to enrich this data with additional correlation algorithms. The end result is mainly getting the source ip address or maybe the whole network with multiple attackers ready to be added to a mitigation process. We have also seen concepts which leverage modern techniques for detection based on the context of Software Defined Networking (SDN), based on P4 as it recently emerged as a platform-agnostic language for programming the data plane and in turn allowing for customized protocols and packet processing.[2] We also see some combined methods where network taping is used to feed the detection software in order to be able to get more details from the incoming network traffic but these solutions generally use specialized network cards which make them both difficult to deploy and also quite expensive in case we need to monitor larger networks. This is why, Netflow and IPFIX are seen as the industry standard especially when routing platforms have started implementing specialised ASIC chips in order to increase sampling capabilities.[3]

C. Software solutions

Network monitoring solutions with DDOS detection capabilities are usually implemented after we already see some attacks so one major question always presents itself - Which open-source or commercial software suite is the best. There is no direct answer to this question and the best way to approach this is to see what is the best tool combination which will get the job done. In order to see viable options we first must have a good understanding of the network we need to cover. This includes both knowing our routing hardware capabilities but also how we are connected to he internet and our upstream provider connectivity and hardware capabilities. In Table II we have several software solutions which are recognised by the industry.

TABLE II
DDOS DETECTION PLATFORMS

Product	URL	Licence	Protocol
FastNetMon	fastnetmon.com	OSS / Commercial	Netflow, IPFIX, Others;
NtopNG	www.ntop.org	OSS / Commercial	Netflow, IPFIX;
NFA	app.noction.com/nfa	Commercial	NetFlow, IPFIX, Others;
Flowmon	www.flowmon.com	Commercial	Netflow, IPFIX;
NeMo	security.geant.org	OSS	Netflow, IPFIX;
sFlow-RT	sflow-rt.com	OSS	sFlow;

Although most of these tools are based on Netflow, IPFIX and Sflow and of course their commercial protocol counterparts (marked as Other), making them usefull for your network is a process which needs to be done based on some principles:

- Connectivity of your network - number of upstream providers and technology user for making these connections. Having a dynamic routing protocol can increase the hardware resources in place and can limit the capacity of flow data which is available to the software.
- Monitoring right places in your network - monitoring on the entry/exit side is the right place for flow data collection. Generally inbound traffic is sufficient to be able to use these software tools. Some of the tools require both s of the flow data to be able to properly detect anomalies and this sometime is overseen in the implementation phase.
- How much data is enough - since all of the flow protocols are based on sampling of packets in predefined intervals, we sometime have too little or to much data which the software needs to process and this later creates a lot of false positive and false negative results.
- Monitoring is implemented when not under attack - all known detection algorithms and software tools use some kind of baseline calculations which need to determine which i the normal flow and how these flows react based on the normal network activity. Adding network monitoring software when the network is already full of traffic which is part of the attack sets this baseline too high and with traffic patterns which will not detect future attacks as they will be seen as normal network activities.

III. The attacks on FCSE in 2022

A. Network status and tools

The Faculty of Computer Science and Engineering (FCSE) network is considered a small size network - mainly since it's main use is providing services for FCSE and some external clients. The network is based on hybrid OSPF / BGP model - where one AS number is the University AS number, from where network prefixes FCSE uses shared over OSPF, and the second AS number is the Faculty (FCSE) AS number which is statically routed for end users of those network prefixes. Both AS numbers are connected to the IXP.mk fabric, while the two AS numbers have the following upstream connections/capacity:

- University AS (AS5379) - Upstream 10G via Marnet/GEANT;
- FCSE AS (AS52188) - Upstream 10G for BGP via University AS, 1G via commercial ISP, 1G for OSPF connectivity;

Network monitoring was done with NtopNG based on flow data exported from the Cisco core router of the University AS. We also have some DDOS mitigation capabilities coming from the GEANT network based on A10 DDOS scrubbers.

B. Attacks May/June 2022

This started while finishing the semester while classes where still online because of Covid19. The attacks where targeting the FCSE Moodle based LMS. Attacks where volumetric and mainly based on UDP. Attacks last less than 15 minutes so little impact for the users. Existing monitoring and mitigation ”just works”

C. Attacks June/July 2022

With the start of the online exam sessions in June, we start to see real pressure on the network infrastructure. Attack are expanded to both LMS systems (one for classes the other for exams) as well as the Faculty main website. Volume starts to pile up and we now see linger attacks lasting 30-59 minutes. We decide to upgrade connectivity between FCSE and University to 10G for OSPF. We also limit some of the services to be available only in Macedonia via the IXP.mk platform. The exams end without significant problems.

D. Attacks August/September 2022

With the start of the exams for the September session, we again see several targets under volumetric attacks: both LMS, Faculty website, other services, we also start to see random attack targets as well as targeting of core router interface IP addresses. Attacks are still volumetric based on UDP but now last 30-120 minutes. The computer center at FCSE based on the view getting from NtopNG decided to declare a emergency situation since service outages are impacted and exams cannot continue. Further analysis of the situation requires that we install additional software platform like FastNetMON and we also activate the GEANT A10 anti-DDOS tool to ”always online mode”. Even with this grater visibility and additional protection on the network attacks continue and we see attack going above 50 Gbit/second threshold as shown on Figure 1

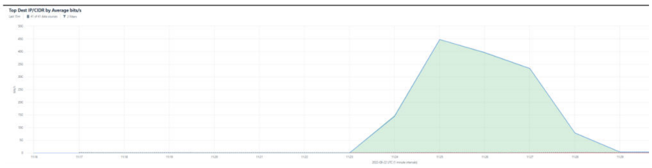


Fig. 1. DDOS attacks peak above the 50 Gbit threshold

Based on the new analysis of both software platforms (NtonNG and FastnetMon) we start to deploy countermeasures on the outside boundary of our network - our connection with GEANT. We also saw that some of the attacks are not also including other protocol type which further stresses the routing hardware based on protocol not being UDP. We also saw a lot of amplification protocols like NTP, DNS, MEMCACHE which top the 70 Gbit / second mark. Filtering rules also showed large packet rates which we successfully dropped on the router edge on the GEANT routers in Sofia (SOF) and Vienna (VIE). Number of dropped packets can be seen on Figure 2.

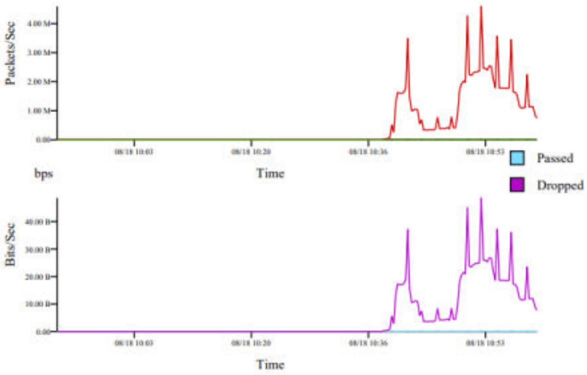
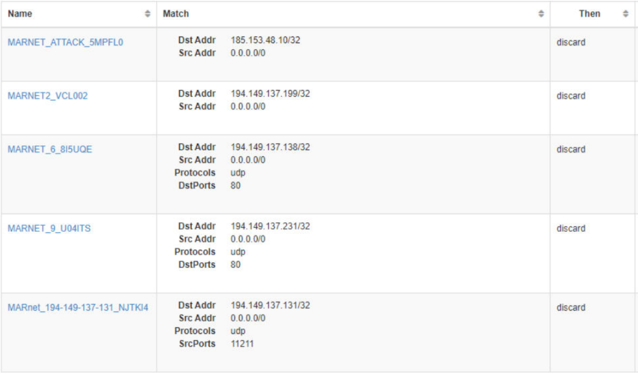


Fig. 2. Packet flow and dropped packets at SOF router

We also, decided to have some of the filter rules permanently in place since we do not use those services on our part of the network in order to reduce future attack surface - we created permanent rules on the GEANT Firewall on Demand (FOD) platform as shown on Figure 3



Name	Match	Then
MARNET_ATTACK_5MPFL0	Dst Addr 185.153.48.10/32 Src Addr 0.0.0.0/0	discard
MARNET2_VCL002	Dst Addr 194.149.137.199/32 Src Addr 0.0.0.0/0	discard
MARNET_6_8I5UQE	Dst Addr 194.149.137.138/32 Src Addr 0.0.0.0/0 Protocols udp DstPorts 80	discard
MARNET_9_U04ITS	Dst Addr 194.149.137.231/32 Src Addr 0.0.0.0/0 Protocols udp DstPorts 80	discard
MARnet_194-149-137-131_NJTKI4	Dst Addr 194.149.137.131/32 Src Addr 0.0.0.0/0 Protocols udp SrcPorts 11211	discard

Fig. 3. Permanent rules for services on FOD

In parallel with these activities on the network, the management of the Faculty decided to return the exams back to psychical form in order to enable better availability to the students. While the attacks, after some time eventually stopped with the final set of measures in place - we continued to analyse the amount of data we have collected in order to disseminate and have eve better lessons learned.

IV. Next steps on the network

The Faculty Computer center will do detailed analysis of the stats and other attack data collected in the specifies time period. Based on the initial information we can see that the size both volumetric and in packets per second classifies this attack as big. Some of the measured which will be put in place to enable more agile reaction to similar situations in the future are mainly in the network upgrade category and can be based on these activities:

- More powerful routers for FCSE - Current routing hardware cannot withstand the traffic levels we saw while being under attack. The Faculty must invest in better hardware which can scale with the need of the network. Equipment based on 1/10 Gbit is not sufficient and future platforms must have 40/100 Gbit cards.
- GEANT Network upgrade to 2 x 100Gb - this will provide better filtering connectivity on our outside edge. Still this required better communication with the GEANT NOC as well development of tools for better communication.
- Total visibility of the network - we plan to install more flow collection tools on more points in the network in order to be able to better see attacks and try to correlate attacks with possible targets.
- BGP black holing and DDOS scrubbing - Having some capability for this will allow the network to be more resilient and volumetric attacks can be stopped more easy. Implementation of platform like this also require better network connectivity in some fragments of the path of packets, which require network upgrades and special

hardware which can allow this to be running as designed. The end goal is that both of these techniques allow almost instant protection of DDOS attacks. Still there is no silver bullet for this so future work on this area is possible.[4]

V. Future work

As presented in the previous part, BGP black holing and DDOS scrubbing combines with flow tools is the future technique for better protection from DDOS attacks, most of the future work will be in that direction. Flow data correlation between platforms and future enrichment of this data can be combined with machine learning and AI algorithms to allow better and more efficient detection and remediation of DDOS attacks. Some initial research in this area actually show that data from Internet Exchange points (IXP) on different geographical locations is usable in detection of DDOS attacks as it utilizes BGP signals to drop traffic for certain routes (blackholing) to sample DDoS and can thus learn new attack vectors without the operator's intervention.[9] Additional area of future work is the analysis of collected data about the DDOS attacks itself. These valuable data can show the vectors which where used as well as if there is any IT systems which can be seen as compromised and used as sources of the attacks. Based on the initial size of the attacks we are confident that there are more than just IoT infected devices and that there is possibility of infected servers which need to have their owners notified in order to stop being used for future attacks.

References

[1] Clodflare. DDoS threat report for 2023 Q1. https://blog.cloudflare.com/ddos-threat-report-2023-q1/, 2023. [Online; accessed 15-April-2023].

[2] K. Friday, E. Kfoury, E. Bou-Harb, and J. Crichigno. Towards a unified in-network ddos detection and mitigation strategy. In *2020 6th IEEE Conference on Network Softwarization (NetSoft)*, pages 218–226, 2020.

[3] A. Herbert, B. Irwin, D. Otten, and M. Balmahoon. Fpga based implementation of a high performance scalable netflow filter. In *Southern Africa Telecommunication Networks and Applications Conference, DF Otten and MR Balmahoon, Eds*, pages 177–182, 2015.

[4] N. Hinze, M. Nawrocki, M. Jonker, A. Dainotti, T. C. Schmidt, and M. Wählisch. On the potential of bgp flowspec for ddos mitigation at two sources: Isp and ixp. In *Proceedings of the ACM SIGCOMM 2018 Conference on Posters and Demos*, pages 57–59, 2018.

[5] R. Hofstede, V. Bartoš, A. Sperotto, and A. Pras. Towards real-time intrusion detection for netflow and ipfix. In *Proceedings of the 9th International Conference on Network and Service Management (CNSM 2013)*, pages 227–234. IEEE, 2013.

[6] N. Hoque, D. K. Bhattacharyya, and J. K. Kalita. Botnet in ddos attacks: trends and challenges. *IEEE Communications Surveys & Tutorials*, 17(4):2242–2270, 2015.

[7] K. Vengatesan, A. Kumar, M. Parthibhan, A. Singhal, and R. Rajesh. Analysis of mirai botnet malware issues and its prediction methods in internet of things. In *Proceeding of the International Conference on Computer Networks, Big Data and IoT (ICCBI-2018)*, pages 120–126. Springer, 2020.

[8] A. Wang, W. Chang, S. Chen, and A. Mohaisen. Delving into internet ddos attacks by botnets: characterization and analysis. *IEEE/ACM Transactions on Networking*, 26(6):2843–2855, 2018.

[9] M. Wichtlhuber, E. Strehle, D. Kopp, L. Prepens, S. Stegmueller, A. Rubina, C. Dietzel, and O. Hohlfeld. Ixp scrubber: learning from blackholing traffic for ml-driven ddos detection at scale. In *Proceedings of the ACM SIGCOMM 2022 Conference*, pages 707–722, 2022.