



CERT-EU Security Whitepaper 17-003

DDoS Overview and Response Guide

V.Revuelto, S.Meintanis, K.Socha
ver. 1.0
March 10, 2017

TLP: WHITE

1 Introduction

A *distributed denial-of-service* attack (or *DDoS* attack) is a malicious attempt using multiple systems to make computer or network resources unavailable to its intended users, usually by interrupting or suspending services connected to the Internet.[1]

The evolution of DDoS attack techniques and targets has been continuously followed in the past by the specialists ranging from powerful companies, which manage an important part of the global Internet bandwidth and content delivery networks, to security expert blogs. However, recently it has caught general attention due to several incidents that might mean a change of paradigm in the way such attacks have been addressed so far, mainly for two reasons presented below.

First, from a technical perspective, it is remarkable that the bandwidth of some of the latest attacks skyrockets in comparison to what has been seen previously. On October 21, 2016, a series of DDoS attacks against Dyn DNS (a DNS provider used by many important Internet companies) impacted the availability of a number of sites concentrated in the north-east of the United States and, later on, other areas of the USA. Impacted sites included among others: PayPal, Twitter, Reddit, GitHub, Amazon, Netflix, Spotify, and RuneScape. Also, earlier that month, the attacks against the *Krebs on Security* blog and the French Internet service and hosting provider OVH reached 620 Gbps and 1.2 Tbps respectively [2].

The attack against the *Krebs on Security* blog trying to silence it – this blog has been very active explaining the techniques and motivation of the DDoS threat actors [3] – is especially revealing about this change of scale. The blog, which had been targeted by DDoS attacks previously, was protected by the Akamai DDoS mitigation service. Akami was providing protection for free due to the public relevance of this blog in the community. However following the attacks in October 2016, Akami was forced to cancel the service due to the huge resources needed for the mitigation:

Akamai had protected krebsonsecurity.com for four years, but the magnitude of the attacks seen during the final week were significantly larger than the majority of attacks Akamai sees on a regular basis. [4]

Botnets exploiting vulnerabilities in hundred of thousands of Internet connected devices, such as cameras, DVRs, and home DSL routers were behind an important part of these massive attacks. The fact that security was not one of the design targets for these devices was long considered a potential threat by the security community, which was often neglected by the manufacturers. These potential threats have turned into serious incidents with many devices affected. On November 26, 2016, Deutsche Telekom announced an outage affecting over 900 000 customers. The affected customers all had routers that were vulnerable to a specific exploit that was incorporated into an Internet of Things (IoT) worm that was released on the Internet. The aim of this worm was to add these devices under the control of one of the botnet masters. During that week, there was a peak of traffic related to that vulnerability – most prominently in Brazil and the UK [5, 6].

The second factor to be underlined is the fact that in August 2016 the code of one of the IoT botnets was publicly released on Internet, which makes it much more easy for different threat actors to achieve such attacks by exploiting vulnerabilities in the IoT devices. It is difficult to assess at the moment, how this potentially easy proliferation of such botnets will affect the number and power of the attacks in the future.

Strategies to mitigate DDoS need to be adopted. These should focus initially on prevention, but eventually by designing multi-layered defense strategies. Therefore, DDoS threats should

be taken into account as part of Business Continuity Planning, along with issues such as site selection, power outages, and natural disasters.

In this document, CERT-EU has focused on procedures for securing IT infrastructure from threats against **availability**. The white-paper is based on proven DDoS identification and mitigation methods that can effectively and efficiently respond to DDoS attacks.

1.1 Target Audience

This document is aimed at general IT staff that has undertaken the responsibility of being prepared to respond to DDoS incident. This document only provides high-level guidelines. Different approaches are possible and may be valid. This document should rather be seen as a guideline in case of the absence of more specific local policies and procedures related to this topic. It does not supersede any specific applicable policies or procedures, which should be followed if they exist.

In case of doubts or any additional questions about this document, do not hesitate to seek further advice and assistance from your respective authorities or CERT-EU team.

2 DDoS Attack Categories

There are three primary categories of DDoS attacks [1]:

Volumetric Attacks: These include UDP, ICMP, and other (spoofed or not) packet floods. The attack aims to saturate the bandwidth of the targeted resource. Magnitude is measured in bits per second. In this category it is important to underline the amplification attacks – attacks that take advantages of the asymmetry design of some protocols (such as DNS and NTP) to flood the victim with the answers to queries, which multiply many times the number of bits of the query.

Protocol Attacks: These include SYN floods, fragmented packet attacks, Smurf, and more. This type of attack consumes actual server resources or resources on the intermediate equipment, such as firewalls and load balancers. Magnitude is measured in packets per second.

Application Layer Attacks: These include slow POST, HashDos, GET flood, clogging and more. This attack sends data according to specific features of well-known applications such as HTTP, DNS, SMTP, SSL. Comprised of seemingly legitimate packets, the goal of these attacks is the depletion of certain resources in the application. Magnitude is measured in requests per second.

The different layers potentially used by the DDoS attacks are presented in Figure 1.

3 DDoS Threat Landscape

Getting global information concerning the evolution of the DDoS attacks is not an easy task, because the information is spread between the ISPs and the targets of the attacks all around the Internet. For writing this white-paper, CERT-EU has reviewed the latest reports from two of the leading companies offering defense services against DDoS. These reports are based on the data recorded by these defense networks and in one of them also on information from a periodic technical survey sent to its clients [7, 4]. The aim of this white-paper is not to reproduce nor summarize these reports, but to offer some of the conclusions with analysis, but underlining the original sources.

DDoS on OSI

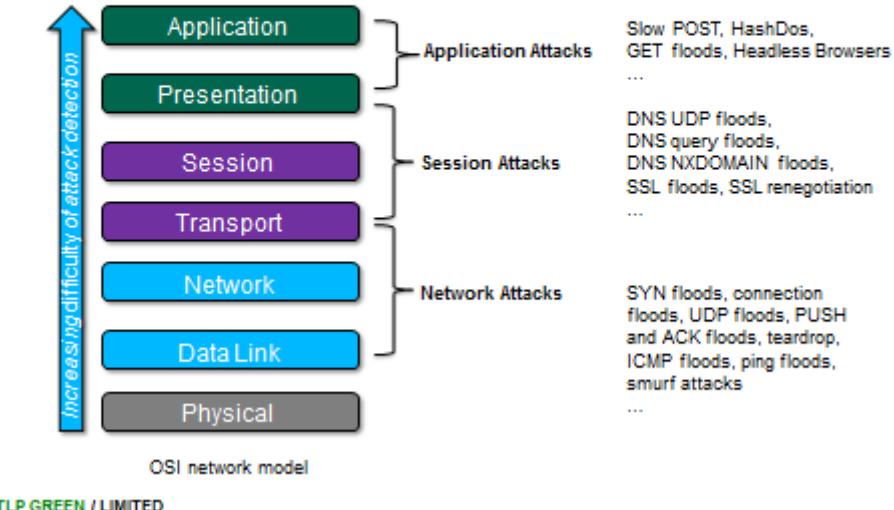


Figure 1: The layering of DDoS attacks on the OSI network model

According to [7], 34% of the enterprise, government, and education organizations reported that they have experienced DDoS attacks in 2015. Among those, over one-quarter indicated that they suffered more than 10 attacks per month, and about half say the attacks exceeded their total Internet capacity. The motivation that these organizations attribute to these attacks is shown in Figure 2.

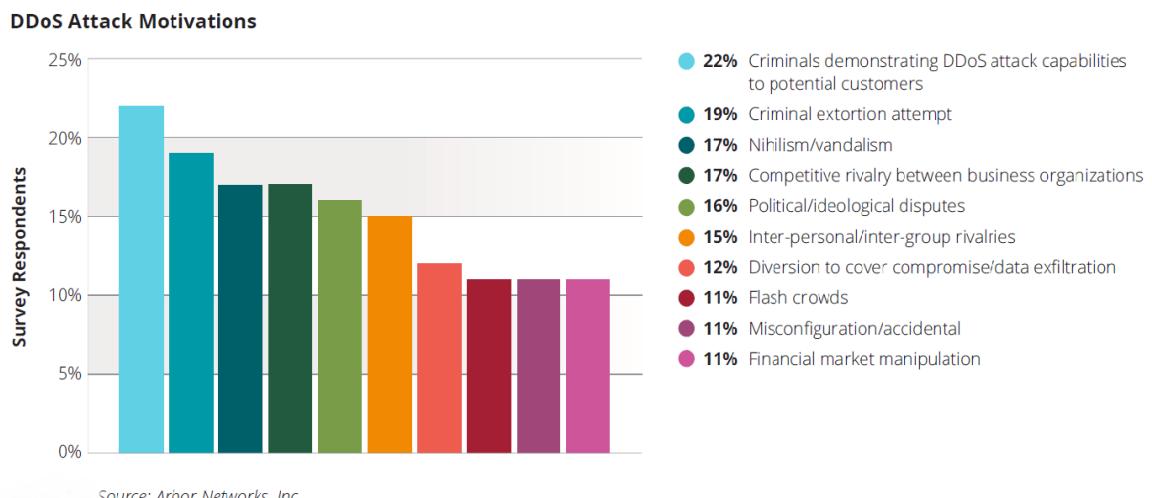


Figure 2: DDoS attack motivations

This data gives a predominant role in the DDoS attacks to **criminal organizations** in contrast to the information offered in the previous version of this white-paper, related to the year 2013 [8]. Although the source is also different, such attribution can be supported by the evidence that stresser tools/bots have been used much more often recently, in contrast with other typical *hacktivism* tools (such as the famous *LOIC*) used previously.

Regarding the attack size, in general the peak attack sizes and large attack frequency seem to have increased dramatically over the last years [7]. A graph of the tendency of the size of the DDoS attacks over the last several years is presented in Figure 3.

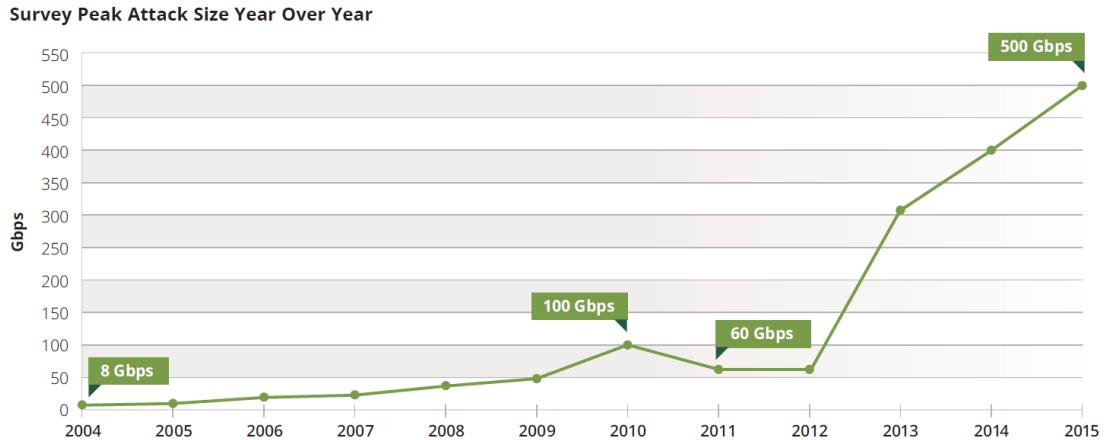


Figure 14 Source: Arbor Networks, Inc.

Figure 3: Size of DDoS attacks in the recent years

The latest data available for the third quarter of 2016 shows – versus the same quarter of 2015 – a 77% increase of the DDoS and a 138% increase of those bigger than 100Gps [7]. This trend is consistent with the recent attacks against the Krebs on Security blog and the French Internet service and hosting provider OVH reached 620 Gbps and 1.2 Tbps respectively. It confirms the trend of significant growth in the top-end size of DDoS attacks year-over-year.

UDP fragments and DNS reflection continued to be the largest portion of the DDoS. The two vectors are strongly correlated, because a considerable amount of the UDP fragmentation traffic is caused by DNS traffic. Combined UDP fragmentation and DNS floods grew by 4.5% in the third quarter of 2016, accounting for nearly 44% of the attack vectors reported by [7].

The evolution of the NTP protocol attacks presented in the quoted report is of special interest, because it seems that while the number of NTP attacks has grown over time, the amount of traffic generated by each attack has decreased significantly. This is because the number of vulnerable servers has stabilized, after decreasing significantly due to the patching. Also there started to appear a competition between the attackers for the remaining resources, since this attack has improved its popularity during the last two years. During 2014, when the NTP vulnerability was published, CERT-EU started a scanning campaign reporting to the constituency with a good rate of fixing the vulnerable servers. The same was done after that for DNS open resolvers and to prevent amplification attacks using the SNMP protocol.

On the other hand, stressers and botnets account for a large portion of the attack traffic in the largest attacks. Usually different techniques are used in these largest attacks. Among them, **Mirai botnet** has had a prominent role in the last few months. Rather than using reflectors, Mirai uses compromised IoT systems and generates traffic directly from those nodes. Mirai scans the Internet for telnet services using well-known weak passwords present in many devices. The code itself is downloaded during a telnet session using FTP. Mirai also terminates processes that belong to competing botnets and closes its own attack vector.

Mirai can be highly tailored. The first version was capable of ten different attacks. Half of its success is the use of the GRE protocol¹ as application layer attack. It is also resilient with respect

¹GRE protocol was developed by Cisco and allows to connect networks of different technologies through an IP network by encapsulating its datagrams over IP packets

to the availability of its C2 servers, and it has a great capacity of generating peak traffic without using reflectors/amplification, because it has available a big number of vulnerable IoT devices [4].

Due to the public release of the source code and its extensible nature, new versions of the code have been detected. In addition, according to statistics about the use of telnet service, they have skyrocketed in the last four months. It is than quite possible that we might see in the future attacks of several Tbps which might be the peak power of all the potential Mirai controlled devices on the Internet.

However, it is not easy to assess if (and if so - when) this potential threat will materialize. The attention received by Mirai after its release in the public domain might contribute to acceleration of the process described above related to the life cycle of the NTP amplifications attacks. It may lead to many attackers competing for controlling the same resources. Although in this case, the size of the potentially available resources to set up the attack is much bigger than in the case of NTP amplification attacks.

4 DDoS Mitigation

As mentioned, DDoS is one of the risks to be addressed in the organization Business Continuity Plan (BCP). The organization should start by assessing the likelihood of different scenarios and the business impact for the organization. Only after understanding the consequences of a DDoS and its likelihood, the accountable managers for the affected service can start and support the needed actions and plans to reduce the risk to a level they can accept.

Some of the aspects that have to be taken into account are common for risk assessment supporting BCP. Following suggested points should be reviewed specifically for DDoS mitigation in this analysis:

- On what IT assets the services depend on, and what are the relationships/dependencies between them. Ideally, it would be useful to have a dependency tree describing the connections between assets and services. For instance: knowing what databases are supporting what services, or what services might be affected, if it is decided to reduce the TTL in the DNS. Such information can be very useful in order to foresee the consequences of some mitigation techniques.
- What are the external nodes in the dependency trees and which underpinning contracts assure their availability. What are the contact points related to these resources to be reported to in case of a DDoS.
- What are the different scenarios that might be applicable concerning these dependency trees; which are the single points of failure; which assets are critical to support more than one service or the most critical service.
- What threats can be identified that can cause a fail in the dependency tree. Gathering further technical information about the assets and dependencies might help to foresee the type of DDoS that the organization is most vulnerable to. For example, it does not make sense to publish through a Content Delivery Network of resources with high dependency on dynamic content. Reviewing a DDoS attack which might target the assets that generate this dynamic content (such as the databases) might be more useful. In this phase, some controlled stress-tests might be helpful to point to the weakest link in the chain of dependencies.

Having all that information, one can start to select the mitigation techniques and controls to be implemented in the mitigation plan and its continuous improvement strategy.

In any case, CERT-EU recommends a formal approach to the risk assessment for those constituents which have been already attacked, as well as for those who have a high risk as result of a preliminary estimation. In order to achieve it, CERT-EU recommends to use the same risk assessment methodology that are used for the rest of IT security risk mitigation, but focus on the availability of the information, instead of on confidentiality or integrity.

Defending a site against a DDoS attack has both a fixed and a variable cost. The fixed costs come in the form of locations, servers, and engineering. The variable, or operational, costs include the bandwidth served and manpower needed to mitigate attacks for the time they are on-going [4]. From this perspective, mitigating DDoS is a business decision that should address what service should be still available under what kind of a DDoS attack and for how long. It is also important to support the proper mitigation plan with the proper budget allocations and to accept the residual risk. It is important to remember that starting by considering only or mainly technical aspects might be misleading.

4.1 Mitigation Techniques

It is important to underline that taking into account the strength of the latest attacks, it may be necessary to hire specialist services, if continuous availability under a powerful DDoS attack is the requirement of an organization. There have been several guides from different specialists published that show possible approaches to facing such attacks [9, 10]

Similarly to the list of types of attacks, the list of mitigation techniques does not try to be exhaustive. It only offers a summary that can be extended by specialized literature. Eventually, the techniques chosen should be tailored to reach the proper residual risk that the management can or has to accept.

- Blocking the attack via FW/IPS. It can be useful with Layer 7 DDoS attacks when they can be detected by signatures or when the source IPs make it feasible. On the other hand, these devices can be themselves targeted by network DDoS attacks, they are useless against reflective attacks, and in order to work properly against DDoS attacks they might need additional personnel training or specialist in the team.
- Auto-scale resources. Although theoretically possible in the cloud, might not be possible for the back-end. In addition, it might not be setup fast enough to mitigate the attack.
- Adding mitigation DDoS hardware. It may be very useful to detect application-layer attacks early, which is very important to avoid that the services get affected. On the other hand, it might require to setup a specialist team in-house or will add an important overhead to the network administrators.
- Publishing service through a Content Delivery Network. It can be useful to absorb volumetric attack for static content, but without other techniques might not address application-layer attacks.
- Hiring DDoS scrubbing services. Theoretically they are able to just send to the organization the *clean* traffic after absorbing the attack, because they are supposed to have the intelligence to detect and discard most of the DDoS attack types. However, they might need to be complemented with DNS and BGP solutions in order to be effective. In addition, considering the attack's peak bandwidth seen lately, it might be really expensive for the size of the resources required to mitigate such attack.

4.2 DDoS Mitigation Plan

An effective immediate response is difficult and may depend on third parties, such as ISPs and DDoS mitigation specialists. These external partners have large scale infrastructures and use a variety of technologies for identification, containment, and remediation. Therefore, DDoS attacks can sometimes be identified and mitigated before they reach the organization's premises. Additional tasks, especially in case of attacks on the network-layer, such as bandwidth prioritization and sinkholing may be performed at end-user/organization level.

The following list summarizes the proposed DDoS mitigation guide:

1. Preparation
 - contacts and procedures
 - ISP and specialized support
 - network & infrastructure setups
2. Identification
 - detection and alerting
 - attack analysis
 - motivation identification
 - mitigation acquirement/refinement
 - traceback
3. Containment
 - network modifications
 - content delivery control
 - traffic control
4. Remediation
 - bandwidth prioritization and blocking
 - traffic-scrubbing
 - sinkholing
5. Recovery
 - normal state verification
 - rollback
6. Aftermath
 - incident review and information disclosure
 - law enforcement

4.3 Proposed Course of Action per Mitigation Stage

4.3.1 Preparation

Contacts and procedures:

- Maintain contact information for team members and others within and outside the organization such as ISP, CDN services, response teams, and law enforcement authorities.
- Establish communication mechanisms. For data communications make sure that non-saturated lines will be used.
- Update the Recovery and Continuity Plan on new DDoS developments. Define a clear response escalation path.
- Ensure that the capacity of the entire infrastructure is not restricted by a single or limited number of resources.
- Dedicate Hardware and Software for DDoS mitigation (workstations, servers, network monitoring and analysis tools).

- Establish alternative service and Internet gateways.

ISP and specialized support:

- Update on ISP's mitigation services.
- Establish DDoS protection contracts and SLAs. Secure immediate activation of agreed services.
- Obtain a clear overview on infrastructure's performance in order to identify deviations derived from an attack.
- Establish specialized support from DDoS mitigation experts.

Network & infrastructure setups:

- Create ACLs for traffic prioritization.
- Set up alternative communication on critical services using VPN.
- Use Reverse path forwarding (RPF).
- Apply inbound and outbound traffic filtering.
- Introduce weak authentication phase prior to the actual on authentication protocols.
- Apply limits for:
 - ICMP packet rate,
 - SYN packet rate,
 - DNS TTL for the exposed systems,
- Secure network, operating systems, servers, applications and components.

4.3.2 Identification

Detection and alerting:

- Search for traffic patterns to expose known attacks (signature detection).
- Compare parameters of the observed network traffic with normal traffic (anomaly detection).
- Contact CERT-EU for early warnings and indicator notices.

Attack analysis:

- Identify the abused systems and services.
- Understand if you are the target of the attack or a collateral victim.
- Get a list of attacking IPs by tracing them onto the log files.
- Define the attack's profile by using network monitoring and traffic analysis tools.

Motivation identification:

- Make a list of potential DDoS attack initiators.
- Investigate possible motives.

Mitigation acquirement/refinement:

- Contact ISP to report the attack.
- Ask for assessment and visibility into the attack.
- Enable remediation measures.
- Notify executives and law enforcement services.

Traceback:

- If possible identify the inbound points (by ACLs, NetFlow or backscatter mechanisms).

4.3.3 Containment

Network modifications:

- Switch to alternative sites or networks using DNS or other mechanism.
- Distribute attack traffic across network of data centers.
- Route traffic on scrubbing services and products.

Content delivery control:

- Use caching/proxing.
- Enable alternative communication channels (VPN).

Traffic control:

- Terminate unwanted connections or processes on servers and routers.
- Configure outbound filters for reducing DDoS response footprint.
- Control content delivery based on user and session details.

4.3.4 Remediation

Bandwidth prioritization and blocking:

- Deny connections using geographic information.
- Deny connections based on IP and traffic signatures.
- Place limits on the amount of traffic, maximum burst size, traffic priority on individual packet types.

Traffic scrubbing:

- Use dedicated devices and modules with high-performing hardware that can support focused scrubbing algorithms.

Sinkholing:

- Attract DDoS traffic on the IP blocks advertised by the sinkhole to apply specialized analysis.

4.3.5 Recovery

Normal state verification:

- Verify that traffic is nominal with no sharp increases. Let a period of time since last violation before the traffic flow is considered normal.
- Ensure that the impacted services can be operational again.
- Ensure that your infrastructure performance is back to your baseline.
- Ensure that there are no collateral damages.

Rollback:

- Initiate suspended services, applications and modules.
- Rollback the mitigation measures.
- Announce the end of the incident.
- Revert to your original network.

4.3.6 Aftermath

Incident review and information Disclosure:

- Evaluate the effectiveness of response.
- Review the measures that could be taken to better address the incident response.
- Review and refine attack-handling tools and procedures taken during the incident.
- Create an incident review.
- Measure the operational impact and costs.

Law enforcement:

- Ensure the attack evidences are valid for forensic analysis.
- Collaborate with law enforcement services.

5 Conclusion

Until recently, DDoS attacks targeting on-line public services might have appeared to be mostly linked to *hacktivism*. Nowadays, it is not possible to find any important political movement or campaign without Internet presence. *Hacktivism* is simply a way protests and demonstrations have moved to Internet. Hence, it is likely that *hacktivism* (and the DDoS threat it is associated with) will play even more important role also in the future.

However, recent data gives a predominant role in the DDoS attacks to criminal organizations. With the increased use of stresser tools and botnets, much larger volumetric attacks are now possible. These new tools can be easily used for criminal purposes and for financial gain, but also possibly to **achieve political means** of certain groups, parties, or even **nation-states**. These possibilities have to be kept in mind when evaluating and deciding on how to prepare against the potential DDoS attacks.

Consequently, the main ideas that CERT-EU would offer for consideration in order to face such issues, are:

- Institutions should establish their availability requirements clearly. It might have different implications for critical services that must be available (even with legal implications), such as publications in the Official Dairy or on-line call-for-tenders than for resources that might support and explain public policies or political decisions.
- It is very important to know in advance the weakest links and bottlenecks that might threaten this availability requirements in case of a DDoS attack. In order to do that, a comprehensive risk assessment is highly recommended.
- Taking into account the latest attack strength, it might be required to hire specialist help or consultancy services to address demanding availability requirements. CERT-EU can help the constituency to analyze the proposals they might have from a vendor-neutral point of view.

Finally, in case of a DDoS attack, reporting the incident and investigating various aspects, such as the threat actors involved or the techniques used, can help for the global security on Internet.

6 References

[1] <http://www.incapsula.com/ddos/ddos-attacks/denial-of-service>

- [2] <https://www.flashpoint-intel.com/action-analysis-mirai-botnet-attacks-dyn/>
- [3] <https://krebsonsecurity.com/tag/ddos/>
- [4] <https://www.akamai.com/us/en/multimedia/documents/state-of-the-internet/q3-2016-state-of-the-internet-security-report.pdf>
- [5] <http://arstechnica.com/information-technology/2016/10/inside-the-machine-uprising-how-cameras-dvrs-took-down-parts-of-the-internet/>
- [6] <https://www.flashpoint-intel.com/new-mirai-variant-involved-latest-deutsche-telekom-outage/>
- [7] <https://www.arbornetworks.com/insight-into-the-global-threat-landscape>
- [8] <http://www.businesswire.com/news/home/20130912005038/en/NSFOCUS-Mid-Year-DDoS-Threat-Report-2013-Details>
- [9] https://www.imperva.com/docs/gated/WP_Incapsula_DDoS_Response_Playbook.pdf
- [10] http://www.cisco.com/c/en/us/products/collateral/security/traffic-anomaly-detector-xt-5600a/prod_white_paper0900aecd8011e927.pdf