How can we improve security against DDoS attacks? A case study: The DyN Attack in 2016

*

Josué Magaña Moreno, 754822
Aalto University
Espoo, Finland
josue.maganamoreno@aalto.fi

César Iván Olvera Espinosa, 754806
Aalto University
Espoo, Finland
cesar.olveraespinosa@aalto.fi

Pernille Lous, 755737
Aalto University
Espoo, Finland
pernille.lous@aalto.fi

ABSTRACT

The DDoS cyberattack targeted to Dyn in 2016 has been one of the biggest distributed denial of service attacks ever launched which affected the availability of the most important internet services including social networks, streaming, online banks, online stores, etc. making almost impossible to share and analyse what was happening at the moment.

It was launched by taking advantage of the vulnerable and insecure Internet of Things (IOT) devices. This attack also used a strategy of sending different kind of attacks at the same time by using between 50 thousand and 100 thousand of source devices. Nowadays, there are many types of mechanisms against this kind of attacks. However, these are difficult to implement and that is why we need to offer a protection plan that considers security measures before and after this kind of cyberattacks.

In this paper we aim to investigate the DyN attack and use the case study in order to research possible strategies and improvement to prevent these type of attacks; additionally the suggestions to cope with Industrial Internet of Things and Internet of Things, IIoT and IoT.

KEYWORDS

Cybersecurity, DDoS attack, Internet of things, DyN attack, Industrial Internet of Things

ACM Reference Format:
Josué Magaña Moreno, 754822, César Iván Olvera Espinosa, 754806, and Pernille Lous, 755737 . 2019. How can we improve security against DDoS attacks? A case study: The DyN Attack in 2016: . In *Proceedings of 2019*. ACM, New York, NY, USA, Article 4, 12 pages. https://doi.org/10.475/123_4

1 INTRODUCTION

Today, cybersecurity is one of the most discussed topic around the world. Even we hear about cyber attacks, importance of good passwords and leaks of information; yet many people ignore the serious harm that lack of security can cause to them [13]. Attack against industrial control systems together with Industrial Internet of Things (IIoT) and Internet of Things (IoT) — also called *ubiquitous computing* — represents a great threat [18] and these attacks are increasing heavily [4]. Devices in both the heal care sector, oil platforms and much more

*The full version of the author's guide is available as `acmart.pdf` document

2019, Case study: ,

ACM ISBN 123-4567-24-567/08/06.
https://doi.org/10.475/123_4

are all connected to the Internet are vulnerable to cyber attacks. Distributed denial of service (DDoS) attacks are on the increase and is a major danger towards both IIoT and IoT [15],

The main objective of a DDoS attack is to saturate a web server, making real users cannot enter because the server can not cope with so many requests for information. The most frustrating thing is that usually the attacker does not win anything, but the big problem with DDoS attacks is the overwhelming burden associated with them.

The servers can be protected against these attacks with filters that reject badly formed or modified packages with false IPs so that only legitimate packages arrive at the server. The measures are not infallible and the server can always end up saturated if the attack is sufficiently massive and well prepared.

To give us an idea of the magnitude necessary for a DDoS to be effective, we can observe the traffic of a server over time. Traffic during the attack (in green) is so large that normal server traffic is barely visible.

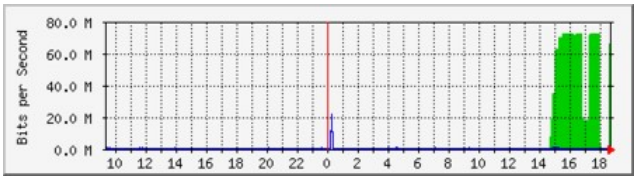

Figure 1: The traffic of a server

Basically, a DDoS attack can only cause the fall of the web, but depending on the kind of webpage and this can be a catastrophe of great losses or not so many. If the web page is simply informative, it will not be so affected, but if the web generates money (online stores, advertising), the owner stops making money while it falls.

1.1 Reason for the attacks

During the last 20 years, distributed denial of service attacks have been used for different purposes:

- *Financial.* The attackers extort the companies to pay ransoms in exchange for not executing or stopping the DDoS attack.
- *Politicians.* Others, on the other hand, have been made for these purposes. Examples of this are the threats and attacks of the hacktivist group Anonymous. One of his appearances was at the end of April 2018, when they saturated the information site of Nicaragua's Government as a demonstration of support for the demonstrations that the opposition was carrying out in that Central American country.
- *The sensation of power and fun.* For others, these are its main motivations. An example is the case of Mafiaboy, a 16-year-old boy who in the year 2000 set out to affect the availability of the CNN site. It could also impact Amazon, Yahoo, eBay, among other companies.

In addition, over the years there are more vulnerabilities and different ways of committing the attacks, causing a greater impact than the one suffered in October 2016 to Dyn. For example, on February 28, the collaborative development platform GitHub suffered what was at the time the largest DDoS attack in history (1.35 terabits per second), and four days later, on March 4 this year, A website in the United States, whose name was not revealed, received an even larger attack (1.7 terabits per second).

In this paper we aim to analyse a case study of *The Dyn Attack* from 2016 which is a DDoS attack again a domain name system (DNS) provider. The goal is to present and analyse the case, do a minor literature study and hereby be able to answer the two following research questions:

- *What solutions can we use to prevent attacks like the Dyn Attack?*
- *How can we improve against DDoS attacks?*

We aim to use the published news in order to understand the case of the DyN attack; afterwards, we will investigate the issues using the existing academic literature.

The paper is structured as follows: First we present the case study, the DyN Attack and the concept of the

attack, then Section III briefly describes how this study was conducted, Section IV presents Related Work, Section V contains the Discussion in which improvements and prevention are presented. In Section VI we discuss the validity of the paper briefly, before we conclude the paper in Section VII.

2 CASE STUDY, THE DYN ATTACK

The Dyn Cyberattack was an attack that occured on October 21, 2016 that was done by a series of denial-of-service attacks (DDoS attacks), which targeted systems operated by the Domain Name System (DNS) provider called **Dyn**.[1]

The attack itself caused a lot of services and internet platforms to be unavailable for a lot of users in North America (USA and Mexico) as well as in some parts of Europe, where the groups new world hackers and anonymous claimed responsibility for the attack, but there wasn't too much provided evidence. [2]

2.1 Related concepts

Before going deeper on the Dyn cyberattack it is important to describe some concepts referred in the case description which are: The Domain Name System and the DDoS attack and Mirai Malware.

2.1.1 Mirai Malware. Mirai is malware that infects smart devices that run on ARC processors, turning them into a network of remotely controlled bots or zombies. This network of bots, called a botnet, is often used to launch DDoS attacks. Malware, short for malicious software, is an umbrella term that includes computer worms, viruses, Trojan horses, rootkits and spyware.[6]

2.1.2 Domain name system (DNS). The domain name servers are the equivalent of a phone book but for internet; they maintain a directory of domain names and then they translate all of them to IP addresses; an IP address is a numerical label assigned to a device connected to the computer network which uses the Internet Protocol for communication.

The Domain Name System, or DNS, is the system that hooks up your browser with the website you are looking for. Essentially, each site has a digital address, a place where it lives, as well as a more friendly URL. For example, blog.kaspersky.com lives at the IP address 161.47.21.156. [17]

2.1.3 Distributed denial-of-service (DDoS) attack. Other important concept that needs to be developed is a DDoS attack, which is an attempt made by cybercriminals to halt the normal traffic in a service, server or a network by overwhelming the target or its structure with a flood of internet traffic.

These attacks are effective because they use a lot of computer systems and IoT devices, principally, as their sources to attack, which gives the possibility to affect more in less time. [5]

From a high level, a DDoS attack can be imagined as a traffic jam that is disturbing regular traffic from arriving at its desire destination.

2.2 Timeline and Impact

2.2.1 Timeline. The attack happened in three waves according to Dyn; the first DDoS attack began at 11:10 (UTC)[2] and was resolved by 13:20. The second occurred between 15:50 and 17:00 UTC and internet users started to report difficulties accessing websites. A third attack began in the night 20:00; at 22:11, Dyn reported that they had resolved the issue.

2.2.2 Impact. The first wave affected the East Coast. The second one affected users in California and the Midwest, as well as Europe. The third wave was mitigated by the efforts of Dyn. [11]

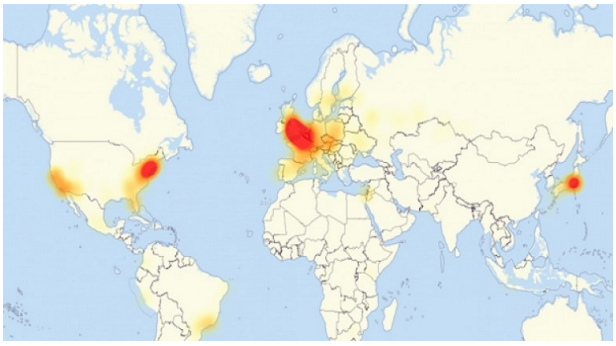

Figure 2: A map of internet outages in Europe and North America caused by the Dyn cyberattack (as of 21 October 2016 20:45 UTC) Source: Dyn

[1] DynDNS is an USA company founded in 2001.

[2] UTC: Coordinated Universal Time

2.2.3 Affected Services. Around 85 companies of well-known internet platforms and services were affected by the attack, some of them were: twitter, amazon, netflix, spotify, Airbnb, Box, Boston Globe, New York Times, Github, Reddit, Heroku, FreshBooks, Netflix, Etsy, Time Warner Cable, etc.

The damage was about 110 million of dollars, where the DNS provider took the responsibility of the damage.

2.3 The attack

As a DNS provider, Dyn provides to end-users the service of mapping an Internet domain name — when, for instance, entered into a web browser — to its corresponding IP address.

During the attack, at the beginning, a big inclination in the bandwidth consumption was witnessed at some Dyn DNS infrastructure, which imitated a situation like that of a DDoS attack. The Engineering and Operations team of Dyn implemented few mitigation protocols but the attack began to target the US-East region. This abrupt large volume of data was originated from various source IP addresses and were destined for destination port 53, where the data packets were composed of TCP and UDP packets. [9]

Even that the second attempt was made with the same set of attack vectors and protocols used in the first attack, it was capable to disrupt the functionalities of Dyn again.

2.3.1 The DDos Cyberattack. The distributed denial-of-service (DDoS) attack was accomplished through a large number of DNS lookup requests from tens of millions of IP addresses, someone purposely forces too many bits of information to a server all at once, rendering it function less and making the the whole system overwhelmed. The activities are believed to have been executed through a botnet consisting of a large number of Internet-connected devicesâĂŤsuch as printers, IP cameras, residential gateways and baby monitorsâĂŤthat had been infected with the Mirai malware.

The DDoS attack force included 50,000 to 100,000 internet of things (IoT) devices such as cameras and DVRs enslaved in the Mirai botnet. [7]

2.4 Understanding the attack

The attacked prevented customers from reaching more than 1,200 domains Dyn was in charge of, the last statement leads us to the next question: *How was it possible to disrupt so many sites with just three fast attacks?*

As mentioned, Dyn reports that some of the attacks came as part of the Mirai virus, which means the attack came via IoT devices like web-connected network security cameras instead of desktop computers.

In order to try to understand the attack involving the DDoS, the mirai and the IoT devices, it is useful to check the anatomy of a botnet attack from criminal to target which is composed by four steps: *Infection, sending, retrieving and attacking.*[10]

- *Infection.* Criminal infects any IoT device with mirai malware, in this case the devices are more like: cameras, baby monitors, etc.
- *Sending.* Criminal sends attack orders to servers.
- *Retrieving.* The infected IoT device retrieves the orders.
- *Attacking.* The infected IoT device carries out the orders attacking to the target (DyN company and partners).

It is important to mention that the thing that made this attack particularly potent was that Dyn is not just a targeted company but a key part of the internet supply chain used by many internet companies, leading to outages âĂŞ in this case, everyone who is dependent on Dyn.

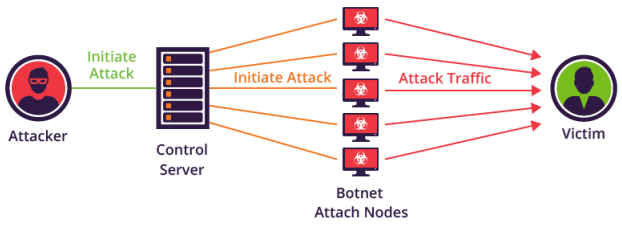

Figure 3: The anatomy of a DDoS; Source: Incapsula

The figure above shows how a botnet, when repeated

over thousands of users, can overwhelm internet systems and lead to a DDoS attack like the one delivered to Dyn. ItâĂŹs a surprisingly simple concept that, when executed, hijacks a benign Internet lookup tool for its own nefarious purpose.

There is some tricky part in the DDoS method and it is that the requests are coming from a wide range of user-agents and IP addresses and this makes the attack distributed and divided in plenty of sub-attacks; so then it is easier to affect more in less time (efficient cyberattack).

With the mentioned method the attack itself is coming from a vast network of zombies or botnets devices. On the other hand, ther is also a term called "DoS" that is just standing for "Denial of Service" and avoiding the distributed and the difference is that every attack is originated from the same IP address.

With the DoS method, security systems are easily able to detect and block the attack than with the DDoS, and this is because the cybersecurity system just needs to block the IP address and in the DDoS it is almost impossible because it is coming for a lot of addresses, so then we need to see later how to mitigate and overcome this kind of attacks as the one in 2016. [8]

2.4.1 DDoS mitigation. As mentioned before, going against a DoS attack is not difficult at all, but once it becomes distributed (i.e. DDoS) it is pretty hard to mitigate and reduce the attack and this is because by the time an attack starts the attacker already knows the origin IP address where a site is content resides.

So, it is too late by the time to get behind a service to secure the system like cloudflare or another reverse proxy service; the funcion of these services is to "hide" the origin IP addres, so then the cybercriminals cannot see it; however, if they have found it already before then the damage is done; then the protection options are hard and then it is time to try to get behind a DDoS protection service and move the origin server without forgeting to update the domain name server (DNS) records. [8]

Later, during the discussion it is going to be mentioned how to overcome these attacks before and after and more about measures that can be taken.

Actually, it is important to add that after the Dyn Cyberattack in 2016, during a conversation with **John Shier**[3] he explained that "there are actually a few different types of DDoS attacks", *Volumetric, protocol based, and application based*; and there are some nuances between each one of them.[3]

- *Volumetric.* Sheer volume; this kind of DDoS attack launchs as much information, requests, etc. at a site as possible so then the system becomes unable to process any other request.
- *Protocol Based.* Exploit a specific protocol. This type of DDoS attack figures out the specific way of how a site is processing traffic so then the attack exploits it to disallow the site making the site unable from processing the traffic.
- *Application based.* An application level attack. In this one somebody does something to the application level that it cannot handle in order to get the web server attacked.

It is important to mention that most of the attacks done to Dyn where of the volumetric type.

2.5 The Role of IoT during the attack

One important trend involved in the cybernetic world is that day after day, people and industries are acquiring more devices and connecting them to the network; Gartner forecasts that at the end of 2019 there will be approximately 14.2 billion connected things and two years later, it will increase in more than 25 billion[20]; this idea of connecting devices together is called Internet of Things (IoT), where they have the ability to transfer data over a network without human interaction.

The research in Internet of Things is increasing and the key issues that have gotten more importance for IoT applications, after the Dyn Cyberattack in 2016[19], are privacy and security; and it is true that the more connected devices we have, the more problems in the area that can be developed.

A DDoS is a very popular type of attack. And using

[3]Senior Security Expert at Sophos.

smart devices in such attacks is appealing for criminals, as we have already mentioned, the Internet of Things is buggy and vulnerable. That is not likely to change in anytime soon.

As seen until now, it is pretty clear that one important tool for the cybercriminals are people's devices, which are part of the IoT, so let's move one to that area in trying to define more about an IoT and the role that they had during the attack and that they have nowadays.

2.5.1 Definition and characteristics of IoT. Nowadays, there are plenty of definitions of IoT and this is because the concept is involved in a lot of areas and it changes in the way you look at it: the application perspective, technological perspective, industrial contexts, benefits, social context, etc. So in order to try to try to figure out one definition we need to talk about the caracteristics of IoT. [14]

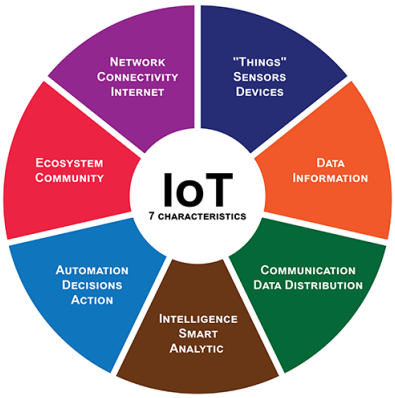

Figure 4: Characteristics of IoT: Internet of Things; Source: Nordigi

As seen in the previous figure, most of the IoT definitions emphasize different characteristics.Here are some of the elements that the IoT definitions generally have in common. [14]

- *Conectivity.* Avoiding the type of definition of IoT, everybody talks about a network of devices, sensors or objects; so then the concept of conectivity is always in any IoT definition.
- *Things* Units, physical objects, sensors, devices, endpoints, the physical world, the list is long. They are all terms to describe an important part of a network of "things". Some also add words as smart or intelligent to the devices. A little more accurate, it is correct to say that there are "things" that contain technology that gives them an additional ability to "do something", such as measuring temperature or humidity levels, capturing location data, recording sound, sensing movement, or capturing any other form of action and context, which can be registered and converted into data.
- *Data.* Data information is part of the intelligent notion of IoT, and approaches the essence of IoT.
- *Comunication.* The data collected from different kind of IoT devices have to be communicated all the time and converted into useful information.
- *Intelligence and action.* The real intelligence and action sits in the analysis of the data and the smart usage of this data to solve a challenge, create a competitive benefit, automate a process, and improve something.
- *Automation.* There is always automation involved in the process in order to create a better environment and improve necessities.
- *Ecosystem.* It is important to mention that the environment is also important for the IoT, because it is more than just apps, it involves people and community.

2.5.2 Security of the IoT devices. As mentioned before, the IoT devices were affected by the mirai malware turning them into botnets and developers of smart gadgets (that were the most affected) sometimes forget to mention to the users to change passwords on cameras, routers, printers or other kind of devices and sometimes they don't even let the user does that. This makes the Internet of Things devices vulnerable and perfect targets to be part of the network of botnets.

Today somewhere between 7 and 19 billion devices are connected to the World Wide Web. According to conservative estimates, that figure will reach between 30 and 50 billion in the next five years. [12]

But even in the next five gears these devices will not be powerfully protected. Besides that, gadgets compromised by Mirai are still active and more and more are joining everyday.

DDoS attacks are effective and efficient. But there are steps that users can take to protect their IoT devices from being hijacked. To protect against another attack like the one that happened in 2016, at a minimum make sure to change the default username and password on your IoT devices. Taking small measures means you can better protect your devices from being taken over and used in an attack.

We will talk more about the measures and security stuff during the discussion as well.

2.5.3 The Internet of Everything: IoE. Even if it has been mentioning a few times during the article, it is really important to take care of the IoT, because they are the future and the principal reason of these kind of attacks.
During the future, IoT devices will increase a lot and until they will turn from IoT to IoE (internet of everything), where the human is part of this and it is a concept emphasised on machine-to-machine (M2M) communications to describe a more complex system that also encompasses people and processes.

[**?**]

3 RESEARCH DESIGN

This study is carried out with the use of a simple and short systematic literature review. We have chosen specific keywords to search through the academic libraries using Google Scholar[4] to access libraries such as IEEE[5], Elsevier [6] etcetera.

Examples of keywords used are: **"cyber security", "encryption", "data protection", "DNS attack", "DyN attack"**. We did not necessarily choose the newest papers, but instead the most accurate fitted for the topic, since some of knowledge is still useful despise its age. This could be instance be topics and papers about Internet of Things, which concept is still the same even the technology has developed heavily.
We tried as much as possible to stay off weak or vague news sites and instead used the news to follow the DyN case, but not to investigate academically.

[4]scholar.google.com
[5]https://ieeexplore.ieee.org/Xplore/home.jsp
[6]https://www.elsevier.com/

4 RELATED WORK

The past ten years industrial controls systems have seen an absolute increase in the use in the industry. This is used for all kind of work processes and can be everything from accessing real-time data from a distributed system to logistics. Today, many of these distributed controls systems are using protocols like Ethernet, TCP/IP, and HTTP. Unfortunately, these are critical components that makes it easier for to interfere and harm the system due to lack of security and isolation. Out of the many Internet hosts, many are only lightly secured and the security in general are not high [4].

Industrial internet of things (IIoT) is heavily increasing in order to improve management and make work processes easier and more smooth. The industry shift towards a way more cyber orientated working process and to control the physical processes with the help of virtual processes. IIoT is set to grow and add $14.2 trillion to the glocal economy by 2023 [18].

However, these additionally causes the working process and system to be vulnerable to to attacks; it is almost impossible to secure every system against all kind of attacks. Internet of Things represents normally a treat to the private user, treating privacy, convenience or comfort which we saw in the DyN Attack; where both private printers and webcames were attacked. IIoT represents a different kind of treat. The attacks are in this manner heading to hurt the supply chain. This could be healtcare services, food supply chains, mining, logistics or even firefighting [18]. Therefore, it is also impossible to determent how to prevent any kind of attacks, because each of them is individual and tailored.

5 DISCUSSION

In this section we present the discussion and we aim here to answer the two research questions that drove this study. The research questions are presented in the subsections and hereafter we discuss the found research.

5.1 What solutions can we use to prevent attacks like the Dyn Attack?

The important thing in this aspect is that the organizations have a cyberattack protection plan that includes the before, during and after the cyber attack. For this, the protection plan is divided into four phases: *prevention, detection, response, and recovery.*[16]

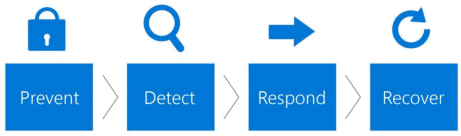

Figure 5: The Protection Plan

5.1.1 Prevention. Currently, there is no computer environment that is not vulnerable to cyber attack, but we can try to prevent malware from attacking the devices. In addition, attackers increasingly develop threats that are more difficult to detect and solve. For this reason, it is advisable to have manuals of preventive measures that reflect good practices on how to handle information leakage, define security policies or access control systems. Another important aspect is to develop training plans or courses on cybersecurity for employees of organizations so that they are trained to identify possible attacks. They are the main entrance of cyber attacks more than 80% of the time.

5.1.2 Detection. A critical stage in any entity since good management of the detection phase of a cyberattack can suppose a significant reduction of its impact within an organization. It makes use of the company's computer security strategy, a document which includes the main steps to be taken in case of suffering a threat ranging from the detection itself, the measures to be taken to minimize the effects, the affected equipment, etc. In addition, it is vital to inform users about this attack so that they follow the established protocol and especially to all the individuals involved in the response team immediately. In this phase, the main measures that must be taken are completely technical since it is essential to have continuous monitoring of the systems to detect any malicious input.

5.1.3 Reponse. In this phase of the protection plan, it is time to respond to the incident and inform both employees and clients and partners, who must know the extent of the attack and, if necessary, they will have to take some security measures such as It may be to change access codes and be predisposed to report the event. To this end, a comprehensive communication strategy must be put in place that covers each of these areas.

5.1.4 Recovery. Once detected the cyber attack and removed from the computer system is the time to carry out a recovery plan by returning to the system as it was before the incident. To this end, technical measures to recover information must be implemented, such as backup solutions, backup copies, decryption programs, among others. It also serves to draw conclusions from what happened and identify what aspects can be improved in terms of cybersecurity so that this situation does not happen again.

5.2 How can we improve against DDoS attacks?

Gartner analyst firm affirms that the prevention of DDoS attacks should be: *"a standard part of disaster recovery planning and business continuity and should be included in all internet services when the business depends on the availability of the Internet connectivity."* [1]

Organizations today have a large number of technologies at their disposal to prevent cyber attacks, many of which are mature and easy to implement. Examples include intrusion prevention systems (IPS), which are designed to detect and block malicious activity on the network before the damage occurs; anti-distributed denial of service (DDoS) solutions, which protect against one of the most common threats to server availability; and identity and access management. If you know your environment well enough to distinguish the difference between normal traffic and abnormal traffic, preventive controls are often very effective. However, it would be a mistake to think that they are infallible: hackers are always looking for new ways to avoid them.

As such, it is important for organizations to adopt a defense-in-depth model: if hackers manage to bypass a layer of security, they must still have others standing in

their way before they can cause a problem. Of course, prevention does not only have to do with technology but also with the implementation of security measures to protect information from unauthorized use and disclosure, modification or destruction, whether accidental or intentional. Security policies dictate how and when updates should be implemented, and how emergency patches are applied to keep your systems updated.

To achieve well-prepared planning, you must identify the parts of the network most likely to be attacked by DDoS, such as Internet bandwidth, firewalls, intrusion prevention, load balancer or servers. In addition, it is necessary to closely monitor these potential points of failure, and evaluate whether they should update or optimize their performance and resistance. Finally, those responsible should know their traffic, since it can control what can and what can not be seen should scan and monitor both incoming and outgoing traffic to gain visibility in unusual volumes or designs that can identify target sites or reveal botnets within the network. There are few defense approaches used to combat DDoS attacks, but none of them is perfect. Some of the steps to prevent these attacks are the following.

5.2.1 Buy more bandwidth. The most basic step that can be taken to make the infrastructure "DDoS-resistant" is to make sure there is enough bandwidth to improve peaks in traffic that can be caused by malicious activities. In the past, it was possible to avoid DDoS attacks by making sure you had more bandwidth at your disposal than any attacker could have. But with the increase in amplification attacks, this is no longer practical. Instead, buying more bandwidth now raises the level that attackers must overcome before they can launch a successful DDoS attack, but buying more bandwidth is not a DDoS attack solution

5.2.2 Build redundancy in your infrastructure. To make it as difficult as possible for an attacker to successfully launch a DDoS attack against their servers, you have to make sure to distribute them in several data centers with a good load balancing system to distribute the traffic between them. In addition, these data centers must be in different countries, or at least in different regions of the same country. For this strategy to be truly effective, it is necessary that the data centers are connected to different networks and that there are no obvious bottlenecks or single points of failure in these networks.

The geographical distribution and topography of the servers will make it difficult for an attacker to successfully attack more than one part of the servers, leaving the other servers affected and able to take at least some of the additional traffic that the affected servers would normally handle.

5.2.3 Configure the network hardware against DDoS attacks. There are simple changes in the hardware configuration that you can perform to help prevent an attack. For example, configuring your firewall or router to remove incoming ICMP packets or block DNS responses outside of your network (by blocking UDP port 53) can help prevent certain volumetric attacks based on ping and DNS.

5.2.4 Implement anti-DDoS hardware or software modules. The servers must be protected by network firewalls and more specialized web application firewalls, in addition to using load balancers. Many hardware vendors now include software protection against DDoS protocol attacks such as SYN flood attacks, for example, by monitoring how many incomplete connections exist and eliminating them when the number reaches a configurable threshold value.

You can also pull the software modules specific to some web server software to provide some DDoS prevention functionality. For example, Apache 2.2.15 is delivered with a module called "mod_reqtimeout" to protect against attacks from the application layer, such as the Slowloris attack, which opens connections to a web server and then keeps them open for as long as possible by sending partial requests until the server can not accept more new connections.

5.2.5 Implement a DDoS protection device. Many security providers, including NetScout Arbor, Fortinet, Check Point, Cisco, and Radware, offer devices that are located in front of network firewalls and are designed to block DDoS attacks before they can take effect. They do this using several techniques, which include carrying out the baseline of traffic behavior, then blocking abnormal traffic, and blocking traffic based on known attack signatures.

The main weakness of this type of approach to preventing DDoS attacks is that the devices are limited in the amount of traffic they can handle. While high-end devices can inspect traffic that reaches speeds of up to 80 Gbps or less, today's DDoS attacks can easily be an order of magnitude larger than this.

5.2.6 Protect your DNS servers. Do not forget that a malicious actor can disconnect web servers by doing DDoS to DNS servers. Therefore, it is important that DNS servers have redundancy, and placing them in different data centers behind load balancers is also a good idea. A better solution may be to move to a cloud-based DNS provider that can offer high bandwidth and multiple points of presence in data centers around the world. These services are specifically designed with DDoS prevention in mind.

5.2.7 We can all help prevent. One of the main actions to be carried out is to create awareness to the users of the impact that this type of attacks has and that they can participate in it without being aware of it. That is why there are some simple and general safety tasks that you can carry out at home, at school or at work. To make life more difficult for criminals.

- *Patch early, patch often.* You must keep the router's firmware updated. Also, have the latest updates of the operating systems of the devices.
- *Disable remote access to the Internet of Things (IoT) devices such as cameras and printers.* Some connected devices allow external users to log in by default, which is useful for troubleshooting, but even more practical for criminals. If the device allows you to restrict access to your local network only, make sure the option is activated.
- *Change the passwords of the device so that it has no default value.* Many devices come preconfigured with user names and passwords that can be found with a search engine. A default password is as bad as no password.
- *Learn to scan our own network to detect security holes.* Tools like Nmap can help find holes before criminals do. It is legal to test our own network, so you can also find out if there is an obvious problem first.
- *Consider testing an industrial-strength home firewall.* For example, Sophos Firewall Home Edition is free. Although a spare computer and some technical experts are required to configure it, keeping updated with protection against the latest hacking threats.

5.3 How to cope specifically with IIoT Attacks

Attacks against internet of things, and especially industrial internet of things can do massive harm and both are on the increase. This could be both health care systems, oil transporters or national banks. Depending on the context, different solutions might be available. However, some suggestions to improve the security are [18]:

- Data should be distributed (block chain technology)
- Use encryption
- Control third party access

Additionally, especially for Industrial Internet of Things, it is suggested to install sensors to the devices, that track sudden differences that might be related to an attack. This could be: pipe pressure, oil flow speed or sudden changes in temperatures [18]. This is important in order to catch and register a possible attack in the area of IIoT and IoT.

6 VALIDITY

In this paper we have aimed to thrive for as much academic material as possible. With that said, we still use several home pages which describes the procedure and happening of the DyN attack. Our sources of information are quite limited since this is not a case study we observe ourselves, but instead drawing conclusions from existing literature. Therefore, no triangulation process has been able to be followed.

7 CONCLUSION

Cybsecurity is a hot topic these days and even the security treat is high, many Internet hosts and devices in both Industrial Internet of Things and Internet of Things are not secured. This we was in the case of

the DyN attack which present a major lack of security and the consequences within, This paper represents a short and brief literature review which presents the case study of the DyN attack from 2016. The case study is used to investigate how we can improve the cybersecurity and prevent attack from DDoS-related attacks in the future.
We aimed to answer the following research questions:

- *What solutions can we use to prevent attacks like the Dyn Attack?*
- *How can we improve against DDoS attacks?*

Our study shows that **prevention** can be increased with a well-constructed protection plan; this should consists of *Prevent* which aims to highen education, define security policies. Secondly to *Detect* is about detecting the actual attack. This is conducted with continuous monitoring of the system in order to detect the attack. Additionally, the affected users have to be informed. Thirdly, we should *Respond* which includes an communication strategy in order to inform clients and employees on how to deal with the affected areas. Finally, we *Recover*. This includes technical measures to recover information must be implemented, such as backup solutions, backup copies, decryption programs,

On the other hand, the **improvement of DDoS** attacks specifically, the improvement is much harder. No software system today can be secured in every possible way. However, there are some options in order to improve the security. Block chain is one option in which we distribute our data across different data centres, countries and networks. Firewalls are another option and finally we can use encryption in order to secure against attacks. Security specifically designed for Industrial Internet of Things, we found out that block chain and encryption can still be used. Additionally, one solution is to install sensors on the industrial devices in order to track rapid or sudden changes in for instance temperature, pipe pressure of oil flow speed.

Cyber attacks cannot fully be prevented, but during this study we did find options in order to improve the security and in the future be able to better respond to domain name system attacks, such as the DyN attack in 2016.

REFERENCES

[1] T. Armerding. 2016. *DDoS attack on Dyn could have been prevented.* URL:https://www.csoonline.com/article/3137544/ddos-attack-on-dyn-could-have-been-prevented.html
[2] Various Authors. 2019. *2016 Dyn cyberattack.* URL:https://en.wikipedia.org/wiki/2016_Dyn_cyberattack
[3] Jonathan Blackwood. 2016. *Everything You Need to Know About the Dyn DDoS Cyberattack.* URL:https://www.channelpronetwork.com/article/everything-you-need-know-about-dyn-ddos-cyberattack
[4] Eric Byres and Justin Lowe. 2004. The myths and facts behind cyber security risks for industrial control systems. In *Proceedings of the VDE Kongress*, Vol. 116. Citeseer, 213–218.
[5] Cloudflare. 2019. *What is a DDoS Attack?* URL:https://www.cloudflare.com/learning/ddos/what-is-a-ddos-attack/
[6] Cloudflare. 2019. *What is the Mirai Botnet?* URL:https://www.cloudflare.com/learning/ddos/glossary/mirai-botnet/
[7] Tim Greene. 2016. *How the Dyn DDoS attack unfolded.* URL:https://www.networkworld.com/article/3134057/how-the-dyn-ddos-attack-unfolded.html
[8] Janna Hilferty. 2017. *The Anatomy of a DDoS.* URL:https://techgirlkb.guru/2017/08/the-anatomy-of-a-ddos/
[9] Scott Hilton. 2016. *Dyn Analysis Summary Of Friday October 21 Attack. 2016.* URL:http://dyn.com/blog/dyn-analysissummary-of-friday-october-21-attack/
[10] NCTA The Internet and Television association. 2016. *Understanding the Dyn DDoS Attack.* URL:https://www.ncta.com/chart/understanding-the-dyn-ddos-attack?share_redirect=%2Ftopics#colorbox=node-2825
[11] Daniel Irimia. 2016. *DDoS Cyber Attack on Dyn DNS Disrupts Websites in Eastern US.* URL:https://www.daniel-irimia.com/2016/10/22/ddos-cyber-attack-on-dyn-dns-disrupts-websites-in-eastern-us/
[12] Kaspersky. 2016. *How to not break the Internet.* URL:https://www.kaspersky.com/blog/attack-on-dyn-explained/13325/?campaign=tcid_admitad_e21786e116356ee7da6ecb5fc3fd0431_240682_x4&ADDITIONAL_reseller=tcid_admitad_e21786e116356ee7da6ecb5fc3fd0431_240682_x4
[13] Elmarie Kritzinger and Sebastiaan H von Solms. 2010. Cyber security for home users: A new way of protection through awareness enforcement. *Computers & Security* 29, 8 (2010), 840–847.
[14] Nordigi. 2017. *What is the IoT?* URL:https://nordigi.no/index.php/en/blog/55-what-is-the-iot
[15] Charles P Pfleeger and Shari Lawrence Pfleeger. 2002. *Security in computing.* Prentice Hall Professional Technical Reference.
[16] M. Salonaho. 2015. *4 steps to combat cyber attacks in a digitalized world.* URL:https://perspectives.tieto.com/blog/2015/04/4-steps-to-combat-cyber-attacks-in-a-digitalised-world/
[17] Network Solutions. 2014. *What Is A Domain Name Server (DNS) And How Does It Work?* URL:http://www.networksolutions.com/support/what-is-a-domain-name-server-dns-and-how-does-it-work/
[18] Lachlan Urquhart and Derek McAuley. 2018. Avoiding the internet of insecure industrial things. *Computer law & security*

review 34, 3 (2018), 450–466.

[19] Rolf H Weber. 2010. Internet of Things–New security and privacy challenges. *Computer law & security review* 26, 1 (2010), 23–30.

[20] Kai Zhao and Lina Ge. 2013. A survey on the internet of things security. In *2013 Ninth international conference on computational intelligence and security*. IEEE, 663–667.