DoS and DDos attacks on IoT devices

Adrian-Viorel ANDRIU
National Institute for Research and Development in Informatics - ICI Bucharest
adrian.andriu@ici.ro

Abstract: The Internet has opened a parallel platform for communications, exchange of information and goods. While the digital dimension may enrich our lives on many different levels, it leaves us vulnerable to new threats. Nowadays, because of insufficient security of IoT (Internet-connected Internet of Things) the number of DoS (Denial-of-Dervice) or DDos (Distributed-Denial-of-Service) attaks have grown from 3% to 6% in 2016. Almost 60% came from Asia, EMEA has 21% and the other 19% came from Americas. The main reason that most of the cyberattacks are originated from Asia is that the region has a weak infrastructure used to commit fraudulent acts. The NTT Security 2017 Global Threat Intelligence Report showed out all this aspects when it was published at the beginning of this month. At the base of the report were lots of factors and lots of resources. The numbers are impressive: networks containing 10,000 clients across five continents, 3.5 trillion security logs, and 6.2 billion attempted attacks and so on. Many sophisticated sensors kept track of cyberattacks for over six months. The favorite of the attacks was a special model of the video camera (over 66% of attacks).

Keywords: Denial of Service, Distributed Denial of Service, Internet of Things

INTRODUCTION

On the one hand, in the new era it is considered that interconnecting everything we will fell a small sense of well-living improvement and ease but on the other hand even before it was born this IoT it attracted a lot of criticism because of it's security no matter if we are talking here about hardware or software. The main reason was the attitude which was careless and resulted in exploitation of lots of vulnerabilities by hackers (D. Serpanos and M. Wolf,2017).

Fig. 1: *Introduction picture (Credit InformationAge)*

What DoS and DDoS Attacks Means? (Y. Lee, W. Lee, G. Shin, and K. Kim, 2017).

Before we proceed, let's understand what this DoS concept is. A Denial of Service or DoS attack is in fact very easy: it means an attempt to make a network or some online resources unusable suffocating them with requests that they would normally make. And there are lots of forms starting from authentication to download requests.

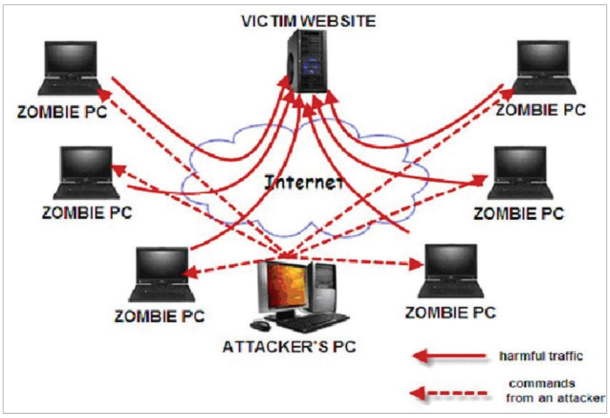

Fig. 2: *High-level approach of an DoS/DDoS attack (Credit ENISA)*

On the other hand, in Denial-of-Dervice attacks success can be achieved by sending too much traffic stream to different targets so that they become unstable or crash. Another point is that a single hacker having just one computer can not generate enough traffic in order to take down some major infrastructures so they search for help. They usually use the so called "botnet" or the "zombie army" or just a lot of compromised devices with different methods. Once the malware made and distributed by the attacker in installed on a computer that is "unsuspicious" for the network he can now concentrate in his real target: the resource he want to take down. The main disadvantage for us is that the internet is available 24/7 so the cyber-criminals can access their malware anywhere in the world at any time and the size of his army can vary from a few computers to hundreds of thousands of devices which are not sounding good. If we picture this on a global scale we can see that botnets can be used to target huge networks or vital systems such as government services or why not social media platforms and we have a lot of examples for DoS or DDoS attacks.

WHAT ARE IoT DEVICES?

(Y. ZHOU, C. JIAO, H. CHEN, L. MA, and G. HU, 2013).

When we say IoT or Internet of things we refer to a system made of many interconnected computing devices with the unique ability to put all the data recorded over a network without the human intervention or interaction with the computer. This definition evolved throughout the years because a lot of new technology appeared: real-time analytics, machine learning, commodity sensors, and embedded systems. But on the market when you say IoT you almost say products that help you to upgrade your house to the popular "smart home". This is now possible because of a large number of smart appliances such as: lighting fixtures, thermostats, home security systems and cameras and so on. All this sensors can be connected and supported by systems associated with this smart world: smartphones. This IoT concept has been looked badly since the beginning especially when it comes to security and most important, privacy because whether we want it or not, they are everywhere in our house.

DOES IoT HAVE A ROLE?

As stated and demonstrated by more specialties from around the world Internet of things is a growing ecosystem which is created by interconnected sensors, smart devices, complex infrastructures and state-of-the-art software. But what all of them do not have is security and the ability to defend themselves from cyber-threats.

So it is easy for those who want to put up a DoS attack on a IoT thing no matter if it is a software or a hardware product, he can simply hit the infrastructure and slip his malware in there.

We can not admit that the Internet of Things will not continue to develop and expand its separate hardware components and will exceed in number the mobile phones or even desktops . Conservative estimates that by 2030, we will have just around 50 billion internet-connected devices, the majority of which (almost 35 billion) will be IoT devices.

Those who support this trend think that IoT devices will be more than 90 billion by the end of the year 2030 but they also know the fact that almost 70% of the most commonly used devices continue to have security vulnerabilities.

HOW THEY ATTACK IoT DEVICES USING DoS METHODS?

Even if most of the IoT devices are fancy and looks expensive they are cheap manufactured. Because they use cheap hardware components they have a lot of vulnerabilities that remain in the final product. Even more is hard to upgrade the products firmware via wireless because the infrastructure is still at a low level.

A small number of manufacturers mean that if a single weak point of certain hardware is discovered the hackers could use the same exploit on a wide range of IoT devices. The main disadvantage is that this kind of devices are always connected to the internet so they can be assaulted with tons of malware until they

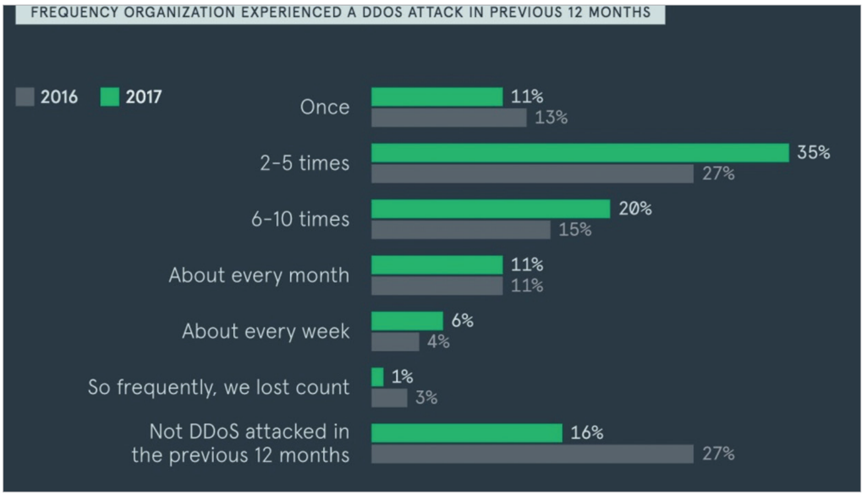

Fig. 1: Financial statistics (Credit ENISA)

gets infected. Maybe if we focus on filtering information when if passes through DNS we could prevent some of the attacks.

Anyway what makes hackers so powerful is their community entitled "Dark Web" where they share new tools or new discoveries. The best example is the code for the well-known Mirai , a program which can transform a no skill hacker in a real danger giving him control over many online devices so that he can lead a DDoS attack. And this was just the prelude for what was about to happen [https://en.wikipedia.org/wiki/Mirai_(malware)].

ATTACK OVER IoT USING DoS METHOD

As mentioned previous the Mirai malware is an easy to use tool which scans the network for those IoT devices which are still under the default password and drag them in a botnet. From there they are used to launch a DoS attack, for example in 2016 it was the biggest attack ever...so far.

Dyn Dns (or today's Oracle Dyn) was attacked through Mirai in 2016 by over 110 000 IoT devices (printers, DVRs or even IP cameras). The attackers sent DNS queries from tons of IPs. That Mirai botnet had no more than 400 000 infected devices that where able to generate more than 1tbps of traffic freezing the Dyn DNS servers and made them to not respond. Who suffered? Well companies like PayPall. Reddit, Twitter even Netflix were down for several hours. Nowadays IoT devices have a lot of applications so they take their vulnerabilities with them in many ares for example in 2017 a researcher in security discover a flaw in the WiFi network of a Norwegian Airlines flight.

THE DoS.... A GREAT ECONOMY

All over the globe companies said that they face an average of 8 DDoS attacks attempts and most of them are coming from unsecured IoT devices or so called "DDoS-for-hire" services. This services can raise an army of bots at your disposal all of this for just 20$ per hour. Ransom Denial of Service (RDoS) is also a growing business because more and more companies are paying for not being future victims of DDOS or DoS attacks.

All over the globe companies said that they face an average of 8 DDoS attacks attempts and most of them are coming from unsecured IoT devices or so called "DDoS-for-hire" services. This services can raise an army of bots at your disposal all of this for just 20$ per hour. Ransom Denial of Service (RDoS) is also a growing business because more and more companies are paying for not being future victims of DDOS or DOS attacks.

WHAT COULD YOU MAKE TO PREVENT ATTACKS?

No matter that you are a simple user or a corporate one there is a lot of precautions you can choose from in order to increase your security level. First you can reduce the risk of having your central server attacked by increase the number of servers and distribute them different duties. Secondly, but most important

Fig. 4: Cyber-security advices (Credit ENISA)

from my point of view is to set a new password for all your IoT devices. And do not forget to disable Universal Plug-and-Play (UPnP) setting because it is just like a nice invitation to any malware to enter in your infrastructure. Another advice is to disable Telnet and it's Remote Management because you avoid another computer to log on another device remotely. Try to keep up to date all the software and all the equipment by updating their firmwares regularly. A good tool like BullGuard will scan your IoT devices and will inform you if one of them in vulnerable to Mirai infections so you can get in touch with the provider or manufacturer for further updates. Also you may search the internet for the latest information about security of your IoT equipment.

CONCLUSIONS

Today the internet is vast and free and you can find information about anything especially about Internet of Things devices. As Bruce Schneier said we are facing a complex and continuous testing of critical internet services. And the majority of these attacks come from IoT devices because they have a lot of security problems that no one has bothered to solve yet. But this is about to change because the world is beginning to raise awareness that IoT represent a new attack vector for the hackers around the globe.

APPENDIX

LEARN FROM PAST MISTAKES

The Attacks (https://krebsonsecurity.com/2016/09/krebsonsecurity-hit-with-record-ddos/)

On 26 September 2016 "KrebsOnSecurity.com" was down for couple of hours because of a DDoS attack. This should not happened because the site has the protection of Akamai who later said that the attack was about 620gbps and came from a large botnet made with infected IoT devices. You can find more information about this attack on Brian Krebs on his personal blog.

In another blog is presented another DDoS attack, a more serious one. It has about 990gbps and over 145 000 compromised IoT devices involved. OVH said this in a tweet post of his founder Octave Klaba on 22 sept 2016.

Just after the attack of Krebs On Security a hacker put the code for the Mirai malware for free so now anyone could use it. The malware is dangerous because it transforms any unprotected IoT device into a bot in a vast network. All bots are controlled from a C&C (Command and Control Server) of the hacker.

The most controversial attack took place on 21 oct 2016 where the Dyn , a DNS provider faced a gigantic DDos attack. In first instance they believed that over 10 millions of IPs were involved but then after some investigations they found about 100 000 infected IoTs. The consequences of the attack were felt by popular companies such as Tumblr, Netflix, Amazon, etc.

REFERENCE LIST

D. SERPANOS AND M. WOLF .(2017). "IOT DEVICES," INTERNET-OF-THINGS (IOT) SYSTEMS, NOV.

HTTPS://KREBSONSECURITY.COM/2016/09/KREBSONSECURITY-HIT-WITH-RECORD-DDOS/

HTTPS://EN.WIKIPEDIA.ORG/WIKI/MIRAI_(MALWARE)

Y. LEE, W. LEE, G. SHIN, AND K. KIM.(2017). "ASSESSING THE IMPACT OF DOS ATTACKS ON IOT GATEWAY," ADVANCED MULTIMEDIA AND UBIQUITOUS ENGINEERING, PP. 252–257

Y. ZHOU, C. JIAO, H. CHEN, L. MA, AND G. HU.(2013). "TRAFFIC BEHAVIOR FEATURE BASED DOS&DDOS ATTACK DETECTION AND ABNORMAL FLOW IDENTIFICATION FOR BACKBONE NETWORKS," JOURNAL OF COMPUTER APPLICATIONS, VOL. 33, NO. 10, PP. 2838–2841, NOV.