CDIS: Case Study #3 - Mirai

José Donato, donato@student.dei.uc.pt, 2016225043

***Abstract*—In the last years Internet of Things (IoT) became a hot topic mainly because of its vast usability for cheap price. However, for IoT devices to be cheap some features have to be ignored. As usual, the security is sacrificed. This decision made this type of devices vulnerable to the most common and simple attacks. Targeted malware for IoT started to appear (Mirai, for example) making possible to gain control over those devices and group them into botnets powerful enough to take down almost any website in the internet. In this case study I analysed the history of Mirai (a botnet of IoT devices) and its victims.**

I. Introduction

Mirai is a malware that infects IoT devices turning them into a network of remotely controlled bots called **Mirai Botnet**. It is also important to define IoT as any device that is connected to the internet, it can be a smart fridge, an IP Camera, smart television, etc. The devices alone are simple but joined together create distributed network powerful enough to bring down any website.

I tried to support my case study on valuable references (KebrsOnSecurity - a security blog that was attacked by a Mirai Botnet and performed an intensive analysis about this topic [4]; Understanding The Mirai Botnet - study submitted to Usenix [6]; among others).

About the structure of this article, I tried to construct a timeline of events that led up to one of the largest DDoS attacks in history against a DNS provider - Dyn [1]. I start by talking about the events that preceded the Mirai creation in Section II. Following to its creation in Section III and its usage (namely the attacks carried out) in Section IV. Finally, in Section V I talk about the concerns about IoT technology and how we can protect against Mirai-like botnets. In the last section VI, as expected I conclude the study.

II. Previous To Mirai

Around 2015, Minecraft was one of the most popular games that gathered millions of players. In order for players to play with or against each other, minecraft servers were needed. Someone would host them but its security was crucial to prevent them from being shutdown by a random user, for example. That is where companies like ProxyPipe [2] or **ProTraf** [3] entered. They were created specifically with the goal of assuring minecraft servers' protection. There was no problem with this until Mid-2015 when ProTraf was rightly accused of targetting ProxyPipe (with Distributed Denial-of-Service attacks) with the aim of preventing ProxyPipe from providing its service (security of minecraft servers) and, consequently, stealing ProxyPipe customers. Even though ProxyPipe CEO told the clients it was ProxyPipe behind the attacks they did not care because they were losing money [5].

This event is important because it was the first appearance and usage of the Mirai Botnet. Later confirmed, ProTraf CEO, **Paras Jha**, was boasting himself in online forums under the alias ”Annas-Senpai” confirming he was the one behind the attacks that would cost ProxyPipe between 400k and 500k dollars. He also confirmed that we was doing this attack with more than 200 thousand IoT devices that he gained control exploiting default telnet credentials.

It is important to note that although this was not the first attack using IoT devices (other botnets already existed: qbot, bashlite), this was the first time we met Mirai and it was completely linked to the ProTraf company: a company trying to offer mitigation services for DDoS attacks (the same ones they were doing) [7].

III. Creation of Mirai

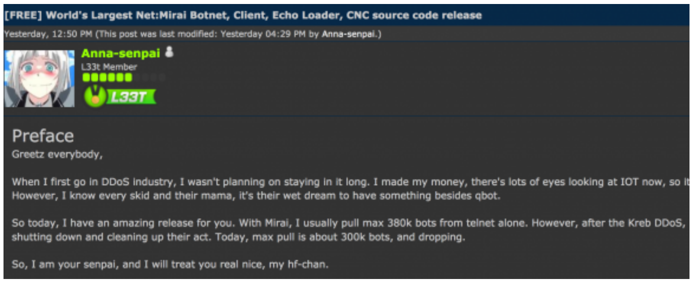
As confirmed in the last section, ProTraf had in his possession a botnet of more than a quarter million of IoT devices. Paras Jha, ProTraf CEO, took advantage of weak security in this type of devices (factory-default credentials) to gain access and control over them. The malware propagate through rapid scanning, i.e., the bot sends fingerprintable port scans and tries to search for vulnerable devices (vulnerable devices are devices that use default credentials and they can be any type of IoT device but most commonly IP Cameras, DVRs and Routers). If the device is indeed vulnerable, it gets infected and from that point it joins the botnet [6]. One of the most important characteristics of this malware is that it has an aggressive propagation, i.e., one infected host is constantly scanning the web for other IoT devices to infect. Once the devices are infected they are forced to participate in DDoS attacks or whatever the command control server (the attacker) demands.

Out of curiosity, this botnet and malware were named Mirai because of the interests of its creator, Paras Jha, in the anime series with the same name [5].

It was later confirmed that the malware was coded in Go (also known as Golang) by Paras Jha and the propagation was coded in C, a language which Josian White, the other ProTraf co-founded, mastered [5]. At first, the authors rented the botnet to commit attacks (some of them are talked about in the next section IV). For a certain amount of money, they would lease some part of their powerful botnet to perform whichever attacks the client would desire. As a note, this service is similar to what is called today ”booter/stresser services” [12] where you can perform multiple DDoS attacks capable to take offline multiple websites for 15 dollars per month.

Of course this is illegal and the creators were later tried for these activities [16].

On September 2016, after one of the biggest attacks performed by Mirai (IV-D), in an attempt to distance themselves from the attacks that were being carried out, Jha made the Mirai code open source. Obviously, this decision made things even worse leading to the creation of dozens of Mirai forks [6] later on responsible for attacks (Dyn attacked talked in Section IV-F is one example).



[FREE] World's Largest Net:Mirai Botnet, Client, Echo Loader, CNC source code release

Yesterday, 12:50 PM (This post was last modified: Yesterday 04:29 PM by Anna-senpai.)

Anna-senpai

L33t Member

Preface

Greetz everybody,

When I first go in DDoS industry, I wasn't planning on staying in it long. I made my money, there's lots of eyes looking at IOT now, so it
However, I know every skid and their mama, it's their wet dream to have something besides qbot.

So today, I have an amazing release for you. With Mirai, I usually pull max 380k bots from telnet alone. However, after the Kreb DDoS,
shutting down and cleaning up their act. Today, max pull is about 300k bots, and dropping.

So, I am your senpai, and I will treat you real nice, my hf-chan.

Fig. 1. Paras Jha under the alias ”Anna-senpai” bragging about his botnet in the day he released the source code

IV. Mirai Consequences - Attacks

In this section I tried to explain different important points about several attacks where the Mirai botnet was responsible for. I started by talking about the attack against ProxyPipe in subsection IV-A which explains clearly what is the only option for a ”small” company to compete against this powerful attacks. In subsection IV-B a fraudulent scheme is explained. In the following subsections other mirai-related attacks are explained and I finish with subsection IV-F for the attack that, in my opinion, is the most important one related to Mirai.

A. *ProxyPipe*

As said before, in Mid 2015, the first target of Mirai botnet was ProxyPipe, ProTraf competitor company. Constant DDoS attacks made ProxyPipe customers change to the competitors even though they were the responsibles for the attack.

Unable to obtain the resources capable to resist against these attacks or the money to out source the problem to other DDoS mitigation firm, ProxyPipe's CEO turned to the only other option available overcome the attack. Talking to the providers that were hosting the botnet or partions of the botnet, i.e., the companies that were responsible for providing connectivity to the Mirai control server (the one responsible for giving ”orders” to the botnet).

Analysing IP addresses tied to the attacks, ProxyPipe was able to trace the control server back to a hosting provider in Ukraine named BlazingFast.io [13]. This company was known for hosting botnet control networks. Unfortunately and expectably, ProxyPipe got no answers from them and they needed to level up on the chain. They tried the company responsible for providing BlazingFast DDoS protection. Even though they answered and told that they killed the servers responsible for the attacks, they lied and did not answer anything else from that point. Later on, they kept trying and it was not until the fifth ISP upstream of BlazingFast that they got success. This time, the ISP promptly had the control server killed. Having no control system means that all the bots controlled by this system can no longer join the network reducing its overall firepower. This resulted in reducing the botnet power to 80Gbps, a value that ProxyPipe could handle at the time.

It is important to note that the Mirai Botnet has a server controller that gives ”orders” to the botnet, if it gets killed as it happened in this attack, the botnet loses control over the IoT devices reducing its power. In the other hand, if Mirai Botnet had a peer-to-peer infrastructure [7] where any node (IoT device) act both as a command controller (server) and receiver (client) it would be way harder to stop the it.

B. *Click Fraud*

Around the same time, Jha was renting the botnet to whoever paid. One of the most common usages was to perform click fraud attacks. In this type of attack, a company pays a website to host their advertisement and the automated bots click the ad resulting in huge losses for the company [7]. Of course detecting whether the click is legitimate or illegitimate and this one of the biggest problems related these botnets. Since they are distributed it is hard to take conclusions.

This attack costs advertisers billions of dollars each year, in 2017, click fraud costed 16.4 billions of dollars [11]. Specifically to Mirai they leased access to the botnet to do click fraud. Later on, the author plead guilty to this actions. Jha agreed to give up 13 bitcoins (at the time around 17 thousand dollars a piece) which sums up to around 200 thousand dollars at the time [16].

It is also known a case where one person named Dalton Norman paid to carry out this attack using the botnet. The prosecutors claimed that he made over 30 bitcoins. It is also known that Mirai authors received around 200 hundred bitcoins leasing their botnet to do this scam [16].

C. Rutgers University

During the fall semester of 2015, Rutgers University [14] received DDoS attacks. Curiously, during this time Jha was studying Computer Science in this exact same university.

Even though he denied the attacks at the beginning, he ended up pleading guilty to those as well [15]. For this attack against his university, Paras Jha got 6 months of confinement and 8.6 million of dollares in fines [17].

D. Krebs Blog

On September 22, 2016 Krebs Website [4] was forced to go offline for four days because of Mirai DDoS attacks [5]. This was the first big known attack from Mirai. It reached 632 Gbps and it was the largest DDoS attack until that moment [6].

The motivations for this attack can be easily found. This website main purpose is to study and analyse cyber attacks and other cybersecurity-related topics and there are multiple posts where the Krebs Author, Brian Krebs, denounces several attackers. One of the creators admitted that the attack on this blog was paid by a customer who rented tens of thousands of mirai-infected systems. Most likely, the customer who bought the botnet was one of the people Krebs reported in his website. Jha also admitted that it was his botnet that performed this attack in image 1.

It was after this attack that Paras Jha made Mirai Code open source (topic talked in Section III). Most probably this happened because the attack against Krebs website was the biggest Mirai attack (and DDoS attack) until that point and brought too much attention.

E. OVH

At the same time that Krebs was being attacked, OVH - a hosting provider [18] - was also attacked by Mirai. This attack against the french hosting provider measured in almost 1Tbps [19]. The ability to carry out two attacks of this size at the same time reveals the power never seen before of this botnet.

F. Dyn

This was the attack that gathered most of my attention maybe because it was the biggest DDoS attack ever seen until that moment. It happened during October 2016 and reports say it peaked at 1.2Tbps [8]. Before talking about the attack we need to understand what Dyn is and why their service is so important to the web.

> "Dyn, also known as DynDNS, is a very large DNS provider that caters to multiple prominent customers (PayPal, Netflix, SalesForce, Deutsche Telekom, TripAdvisor, LinkedIn and more)." [10]

This service is important because without it there are no domain name resolution, i.e., when a user types *netflix.com* in browser, if the DNS service is down, the process of translating this url into the end-server IP address would not happen. Summing up, without DNS users cannot access the websites unless they know the long IP addresses by heart and, consequently, the internet would break.

Knowing this service importance it is easy to understand how this attack took down some of the most popular websites in United States (Github, Netflix, AWS, among many others). In the image below we can see the outages in United States caused by this attack:

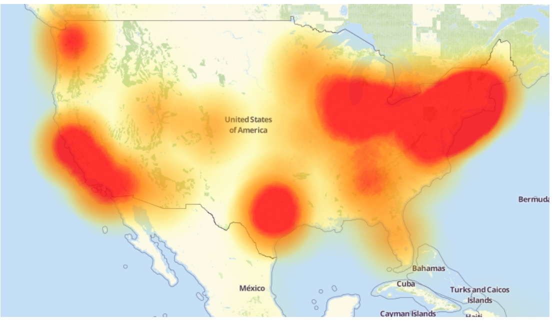


Fig. 2. Outages caused by Mirai attack against Dyn [20]

This was a sophisticated attack targeting the port 53

(DNS) of Dyn Managed DNS infrastructure and Mirai botnet was the primary source [8]. Dyn came under attack in three different waves of DDoS attacks during eight hours combined [10]. In the first one, they started to see an increase of bandwidth in certain DNS servers and because of this abrupt increase the Dyn's Engineering and Operations team put more than the automated responses in place. They used techniques such as traffic-shaping, re-balancing of the traffic, etc. Mitigation efforts were fully deployed and the attack subsided after but not before the end-users noticed it. Later, a second wave globally distributed happened. More efforts by the team were put on the pitch and they managed to stop the attack again deploying their defenses techniques globally [8].
According to CNBC [9], there was a third and final wave. Reports say that packet flow bursted something between 40 and 50 times higher than normal (and could have been a lot more without Dyn Engineer team mitigation efforts) [8].
In my opinion, the code replication (forks created) because of open sourcing Mirai lead up to this catastrophic attack. At that time, not only did Mirai authors have access to a powerful botnet, but others who used the open sourced code. This resulted in an attack involving more than 300,000 devices globally distributed [7].
Analyzing this attack we can come to some conclusions:

1) because the botnet is globally distributed, it is really hard to distinguish harmful from real traffic
2) it is really hard to defend against DNS attacks because of its amplification effect - request generates responses way bigger (a response is from 10 to 20 times bigger than the request). Also, DNS uses UDP protocol that is connectionless what makes it even harder
3) legitimate queries increase the congestion. At some moment, the legitimate users end up congesting even more the system
4) Mirai-like botnets are a huge threat to today's web - IoT devices are evolving and are everyday more powerful resulting in botnets with enormous capability
5) dns service is a point of failure, its failure implies the malfunction of all the other services that depend on it (in this attack, the websites that went offline)
6) defenses (mitigations techniques) are not mature as the ones used against http attacks - this is primarly because DNS attacks are harder to defend. Because defenses are so hard to implement, in the beginning companies had their own DNS server and now they outsource this problem to companies like Dyn.

Work must be done to change this paradigm and make sure that if a similar attack happens we are prepared.

V. Future

Even though the Mirai authors were caught, Mirai-like botnets still exist and remain dangerous. In fact, they are mutating. After the source code was released, other malware variants were born. Some examples are [7]:

- Puremasuta: weaponize bug in D-Link devices
- OMG strain: transform IoT devices into a TOR network resulting in proxies that allow cybercriminals to remain anonymous
- Reaper: compromise IoT devices faster than Mirai. It also targets more devices and has greater control over them

As we saw in the last section, these botnets are capable of (but not limited to):

- attack ISPs making impossible for legitimate users to use the internet
- send spam email
- click frauds
- DDoS attacks against any website

The botnet studied in this article (Mirai) highlight the fact that IoT devices did not learn from the previous problems in web security [6]. Bad practices in systems development continue to be used (factory-default credentials, for example).

Before jumping into how we can protect ourselves in the future, we need to understand what made possible these attacks:

1) infected IoT devices do not stop working and sometimes the infection is not even noticeable to the device owner. The users may have no reasons to secure/update/reboot their devices. In some cases, a reboot may not even remove the malware since it can be powerful enough to infect the system again after rebooting
2) 1.5 billions of devices identical to those that make up the botnet are sold each year [7] - there is still room for lot more devices to get infected and converted into botnets
3) rent a service (booter/stresser) capable to DDoS multiple websites is as low as 15 dollars per month
4) there is no global entity enforcing IoT security standards. The reference [21] has a list of standards and frameworks for security in IoT. However,

there is still the need to enforce them. Regulation is needed. Devices manufactures must follow a standard to avoid simple mistakes such as default passwords, for example

5) there was no global law enforcement for cybercrime until Interpool (International Criminal Police Organization) recently introduced cybersecurity [22]
6) there are lot of end-of-line devices: old devices neglected by manufactures will still be connected to the internet and vulnerable to common malware (unable to do updates, won't be possible to patch its vulnerabilities)
7) it is really hard to track attackers, they use techniques (for example, Fast Flux) to hide the domains used to download malware or host phishing sites. However, doing intensive analysis such as the one did by Krebs Blog in [5] can help to unveil the attackers. This possible because most of the attackers like to brag about what they do (even under alias can be easy to link them) as we can see in image 1.

The next and last big question is how can we improve and protect ourselves from Mirai or similar botnets? In the following enumeration I provided my opinion in five main points:

1) Providers and companies must share knowledge and mitigation methods to prevent these attacks. For example, Dyn must share the techniques they used to successfully mitigate the DDoS attacks and ProxyPipe must share what they did in order to stop the attack (talked about in IV-A)
2) Related to the previous point, Interpool and companies or ISPs receiving attacks must help each other.
3) Companies cannot rely on a single dns provider - it is a single point of failure. Although it can be a challenge, DNS redundancy may be necessary
4) Security hardening, IoT needs to embrace common practices that are currently used on web - usage of specific IoT security standards [21]. Practices such as auto-updates, strong and non-default passwords, only necessary ports open must be embraced.
5) Legislation can help. In fact, previous this year, in January 2020, California governor required that all IoT devices must have reasonable security features. The governor said that if companies want to sell those devices in California, they will need to improve their security [7].

To sum up, when developing sensitive systems like IoT devices, we need to embrace security techniques such as *Security By Default* and *Security By Design* even if it means that the systems will be a little more expensive or a little less efficient. It is important to note that following security standards [21] will help achieving these desired systems.

VI. Conclusion

These attacks brought up the fragilities of internet security and the vulnerabilities in IoT devices. Because IoT devices are only getting more powerful, we need to make sure that they are also getting more secure making impossible for them to be converted into a botnet capable of shutting down the internet. Work must be done and shared so we can start using IoT for its supposed goal without worrying that the devices will turn on us one day.

References

[1] Dyn DNS and Web Application Security are Critical for Infrastructure Security — Oracle Dyn https://dyn.com/

[2] ProxyPipe — Next Generation DDoS Mitigation https://www.proxypipe.com/

[3] WebArchive of Protraf Solutions https://web.archive.org/web/20160318145928/https://www.protrafsolutions.com/

[4] Krebs on Security https://krebsonsecurity.com/

[5] Who is Anna-Senpai, the Mirai Worm Author? — Krebs on Security https://krebsonsecurity.com/2017/01/who-is-anna-senpai-the-mirai-worm-author/

[6] Antonakakis, Manos, et al. "Understanding the mirai botnet." 26th USENIX Security Symposium (USENIX Security 17). 2017.

[7] What is the Mirai Botnet? — Cloudflare https://www.cloudflare.com/learning/ddos/glossary/mirai-botnet/

[8] Dyn Analysis Summary Of Friday October 21 Attack — Dyn Blog https://dyn.com/blog/dyn-analysis-summary-of-friday-october-21-attack/

[9] Third cyber attack underway against internet firm https://www.cnbc.com/video/2016/10/21/third-cyber-attack-underway-against-internet-firm.html

[10] Dyn DDoS Attack — Red Button https://www.red-button.net/blog/dyn-dyndns-ddos-attack/

[11] Businesses could lose 16.4 billion to online advert fraud in 2017 https://www.cnbc.com/2017/03/15/businesses-could-lose-164-billion-to-online-advert-fraud-in-2017.html

[12] DDoS for Hire — Booter, Stresser and DDoSer — Imperva https://www.imperva.com/learn/application-security/booters-stressers-ddosers/

[13] BlazingFast — Your Reliable Hosting https://blazingfast.io/

[14] Home — Rutgers University https://www.rutgers.edu/

[15] Former Rutgers student admits to creating code that crashed internet - nj.com https://www.nj.com/education/2017/12/rutgers_student_charged_in_series_of_cyber_attacks.html#incart_river_mobile_home

[16] Mirai IoT Botnet Co-Authors Plead Guilty — Krebs on Security https://krebsonsecurity.com/2017/12/mirai-iot-botnet-co-authors-plead-guilty/

[17] Mirai Co-Author Gets 6 Months Confinement, 8.6M in Fines for Rutgers Attacks — Krebs on Security https://krebsonsecurity.com/2018/10/mirai-co-author-gets-6-months-confinement-8-6m-in-fines-for-rutgers-attacks/

[18] Global Cloud Service Provider — OVHcloud https://www.ovh.pt/

[19] The Largest DDoS Attack in history just happened... and it didn't work. https://www.thesslstore.com/blog/largest-ddos-attack-in-history/

[20] Downdetector https://downdetector.com/

[21] IoT Security Standards Frameworks - SENKI https://www.senki.org/operators-security-toolkit/sp-security/iot-security-standards/

[22] Cybercrime https://www.interpol.int/Crimes/Cybercrime