Economics of Cybersecurity Block 3
Telnet scans

Calvin Hendriks - c.hendriks@student.utwente.nl
Christiaan van den Bogaard - c.h.m.vandenbogaard@student.utwente.nl
Sander Bakkum - s.bakkum@student.utwente.nl
Riccardo Colombo - r.colombo@student.utwente.nl

September 30, 2019

1 Introduction

In our last assignment, we analyzed a set of port scans performed by Shadowserver, specifically on port 23 and 2323. From the data set a security issue came to mind; vulnerable devices can become part of a botnet, like the one created by the Mirai malware, that is in turn used to perform DDoS attacks. After identifying the issue, we defined a set of metrics that could be used to measure the scale of the problem.

- What percentage of connection attempts requires authentication? In this case, we found out that 69.4% require authentication. For the other 31.6% it means that no authentication banner is displayed. Conclusively, this means that 69.4% is possibly vulnerable to the Mirai botnet as a dictionary attack can be launched.
- What percentage of connection attempts gets rejected? We found that 2.4% actively refuses the connection which mean that they absolutely can not be attacked.
- What percentage of device publishes sensitive software information? Analyzing this issue we determined that $\sim 61\%$ of the scanned IP addresses provide some information on either the running OS or the running service. Such information can be very valuable for an attack, helping him determine whether the device could be exploited.
- Patch adoption to a severe security vulnerability. This metric discussed the OS patch adoption rate for MikroTik devices.
  - What percentage of devices is vulnerable to CVE-2018-7445? This metric analyzed what is the fraction of IP addresses that have not updated their OS in the 5 months period following the disclosure of the patch.

  - Adoption rate of the patch fixing CVE-2018-7445. The metric analyzes the fraction of IP addresses which updated their OS over the four weeks following the release of the patch.

- What is the adoption rate of the different versions of OpenSSH? In this metric we analyze how recent are the versions of OpenSSH run on the scanned IPs and we give an indication on how many suffer from a serious vulnerability.

1.1 Problem owner

The problem owner is in most cases the party affected by the issue to be solved or the party who would benefit from a solution [1]. From this definition, one might think that the owners of the infected devices are the problem owner. However, since the owners of the hijacked devices often do not experience any problems and would also not really benefit from a solution, they are not our problem owners. The same is true for Internet Service Providers (ISP), since the amount of bandwidth used by a DDoS attack is extremely small compared by the bandwidth that normal users use by services such as streaming. The problem owner that we will focus on in this report are the DDoS attack victims. These parties are most affected by the issue, since they can suffer serious financial losses if hit by a DDoS attack. Therefore, they will also be the group that would benefit the most from a solution against such botnets and corresponding DDoS attacks.

2 Relevant differences in security performance

What relevant differences in security performance does your metric reveal? Evaluate these difference as shown with the metrics developed in the 1st assignment. (2 points)

What is your definition of security performance? And differences between what exactly? Our metrics measure how severe these botnets can become by looking at authentication and vulnerabilities. A hit on security performance will only be seen when these botnets launch their attacks.

3 Risk Strategies - Problem Owner

When considering the content of the class on risk management and applying it to the problem owner defined in section 1 it is possible to highlight how the problem owner can approach risk management by adopting one or more of the following risk strategies:

- Mitigate the risk. DDoS attacks can either leverage a vast number of connections to saturate the target infrastructure (*volumetric attacks*) or leverage application layer traffic to exhaust web servers' resources (*application attacks*). Traffic scrubbing services can be used to mitigate volumetric attacks; when anomalous rates of incoming traffic are observed, the incoming traffic is rerouted through the scrubbing infrastructure and then analysed by the scrubbing center where the malicious traffic is dropped and the genuine one is forwarded to the client infrastructure. On-premises appliances are instead commonly adopted to efficiently mitigate application attacks; it consists in in-line devices that can both detect and mitigate application attacks. Lastly, another possible mitigation strategy would be to subscribe to a DDoS CDN service.

- Accept the risk. Depending on the business and on the function of the IT infrastructure accepting the risk of a DDoS attack could be a viable solution. We will discuss in section 6 whether it would be more economically effective in our case to accept the risk or to mitigate it.
- Avoid the risk. We consider this strategy not to be viable in our case as it would consist in the problem owner abandoning the risky business, which we assume to be the core business of the company.
- Transfer the risk. This strategy involves transferring the risk to a third party, for instance to a cyber insurance company in exchange of a premium fee. However, as we analysed in class, the cyber insurance market suffers from few limitations and, although the market is growing [2] [3], it is not a popular solution yet. Therefore we consider this option not to be viable.

4 Other Actors Involved

The security issue analyzed in this paper is not only influenced by the problem owner but also by several other actors:

- IoT owners can affect the issue in multiple ways; for instance by buying more devices which could potentially become victims of a botnet increasing its power. Buying behaviour could also positively impact the issue; customers could in fact tend to sacrifice extra money to buy quality products which will be more secure. Furthermore, adoption of best practices such as network isolation and regular patching will positively impact the issue.
- Manufacturers can also influence the security issue in a positive way; the implementation of OTA updates, the increase of the security level in the design of new products can reduce the number of devices which can fall victims of a botnet. Moreover, groups of manufacturers could cooperate to define minimum security levels for the industry.
- ISPs can directly influence the issue by preventing IP spoofing on their networks but also indirectly by launching awareness campaigns to help IoT owners in making more informed choices.

- Governments have also an impact on the security issue as they could define minimum security levels for the industry, consider device owners also liable for the attacks, awareness campaigns.

5 Risk Strategies - Other Actors

IoT owners can choose to accept the risk. In the case of Mirai, IoT owners could still use their devices as intended. The main problem is when the C&C server orders the devices to DDoS a certain target. The Device will start DDoSsing the target and therefore generate a significant amount of traffic on the IoT owners network. However, completely throwing away the device wouldnt be a viable solution. Therefore, risk transfer could also be a strong solution. Transferring the risk to the manufacturer stating that the device does not meet security standards and therefore should be fixed. Furthermore, Mitigation can be done by using a firewall.

Manufacturers should mitigate the risk. They should patch the devices or repair the devices when a vulnerability is found. If this is not possible, owners should be notified about the broken security of devices.

This security issue can cause losses for ISPs, as an overcrowded network will make their users complain which result in loss of income and a loss of reputation. As mentioned before, ISPs can directly influence the issue by preventing IP spoofing on the network. These are active measures which is a mitigation risk strategy.

As the main issue in Mirai is that devices have default credentials or a completely open telnet port. This is all due to the weak security of those (cheap) devices. As there are product safety standards for products, why are there not any product security standards? A government could enforce these standards to European standardisation organisations.

6 ROSI

To determine the value of a mitigation strategy to a certain type of loss event, the ROSI equation can be used. The ROSI equation is as follows:

$$ROSI = \frac{ALE \times MitagationRatio - SolutionCost}{SolutionCost} \tag{1}$$

where

$$ALE = ARO \times SLE \tag{2}$$

In these equations, the included factors are defined as follows:

- **ARO**: Annual Rate of Occurrence - The estimated amount of loss events the company will endure over the course of a year.

- **SLE**: Single Loss Expectancy - Total expected amount of money lost in a single loss event.
- **ALE**: Annual Loss Expectancy - Annual expected financial loss resulting from a type of loss events.
- **Mitigation ratio**: The factor of loss events a chosen solution will prevent.
- **Solution cost**: The cost to implement the chosen solution per year.

For all of these factors, sensible estimates need to be made to be made to be able to produce a realistic ROSI value.

6.1 ROSI for DDoS victims

Since our problem owner is a DDoS victim, we need to define one. We define our victim as a company that hosts internet advertisements. It lets other companies place advertisements on websites connected to its network, and charges the placers of advertisements an amount per click. Websites that allow ads to be placed receive an amount of money per click. Advertisements are embedded in other websites and can be hosted statically. The analyzed solution to DDoS attacks is to host the ads in a Content Delivery Network (CDN). To be able to determine a loss per DDoS event, we need to know the size of our company. We define our yearly profit to be €365,000, or €1000 per day. We chose CloudFlare [4] as our proposed CDN provider.

Annual Rate of Occurrence

TODO
We are not sure yet how to determine the ARO from our data set (and perhaps extra data sets). We have a few problems:
This set contains only dutch IP addresses. How would we scale to worldwide?
And even if we have this infection rate, how would that tell us an annual rate of occurrence?

- Determine DDoS-rate by estimating a Mirai infection rate from our data set
- Include patch adoption rate if possible

amount of devices with authentication (from our metric) x amount of devices with default password (average/from paper) gives the amount of devices that could be infected by a botnet malware As users generally do not like advertisements an attacker might feel inclined to launch an attack against an ad network, thus preventing any ads on the network from being shown.

Single Loss Expectancy

To determine the loss of an isolated DDoS attack, we need to determine the length of such an attack. In Q2 of 2018, most attacks took less than 4 hours, and almost all attacks (98.8%) took less than 50 hours [5]. We set our Single Loss Expectancy to be at least the lost profit of a 4-hour attack and at most a 48-hour attack.

$$\begin{aligned} SLE_{min} &= (4/24) \times 1000 = 166,67 \\ SLE_{max} &= (48/24) \times 1000 = 2000 \end{aligned} \tag{3}$$

Mitigation ratio
By hosting all ads on a sufficiently large CDN like CloudFlare, all DDoS attacks can be mitigated. Thus the mitigation ratio in our case is 100%.

Solution cost
In order to have guaranteed 24/7 DDoS protection from CloudFlare, a business plan would be needed [6]. The costs for such a plan are €200 per month, or €2400 per year.

References

[1] C. Csáki, *The Mythical Decision Maker*, 01 2008.

[2] I. Journal, “State of the cyber insurance market— top trends, insurers and challenges: A.m. best.” [Online]. Available: https://www.insurancejournal.com/news/national/2019/06/18/529747.htm

[3] M. van Wieren, “Cyber insurance: What you need to know, and how to seize the opportunities.” [Online]. Available: https://www2.deloitte.com/content/dam/Deloitte/nl/Documents/financial-services/deloitte-nl-fsi-cyber-insurance.pdf

[4] CloudFlare, “Cloudflare - the web performance & security company.” [Online]. Available: https://www.cloudflare.com/

[5] Kasperky, “Ddos attacks in q2 2018.” [Online]. Available: https://securelist.com/ddos-report-in-q2-2018/86537/

[6] CloudFlare, “Cloudflare plans and pricing.” [Online]. Available: https://www.cloudflare.com/plans/