Economics of Cybersecurity Block 4
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

October 14, 2019

1 Introduction

In previous assignments, we discussed the security issue behind telnet scans, the creation of IoT botnets and the DDoS attacks launched from them.

In this assignment, we aim at understanding the factors influencing the variance in security performance in relation to a metric. We will investigate the underlying reasons behind the existence of variances in a metric.

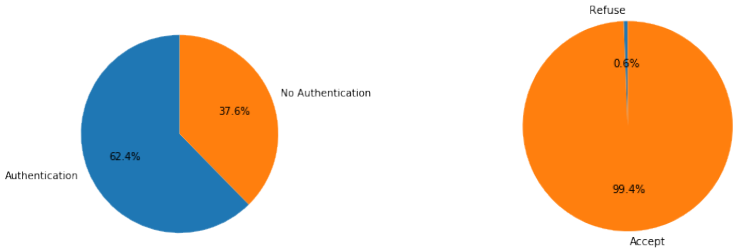
1.1 Metric: vulnerability per ISP

1.1.1 Authentication per hostname

This metric gives insight in the percentage of devices that require authentication when a telnet connection is established. This means, that these devices are *possibly* vulnerable to Mirai, as it used a dictionary attack. In the devices that do not have authentication, we do not know what is the case. In most cases its either a rejected connection or a whitelist. In the previous assignment, it was the aggregated result over al hosts. This now is separated and the top 5 hosts are shown. It is separated by parsing the hostname and stripping the domains, while keeping the top level domain and second level domain e.g. kpn.nl.

1.1.2 Refused connections per hostname

An important defense mechanism of these devices is whether the connection is rejected. If there is an extra layer of defense in place, such as a firewall, these devices can not be infected to be part of the botnet. Also, this metric was computed over the whole range of hosts, this now is split into the different hosts and the top 3 biggest hosts are shown.

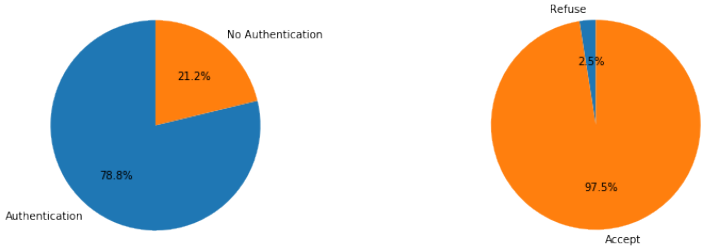


(a) (b)

Figure 1: Authentication required and Connection refusal for kpn-gprs.nl

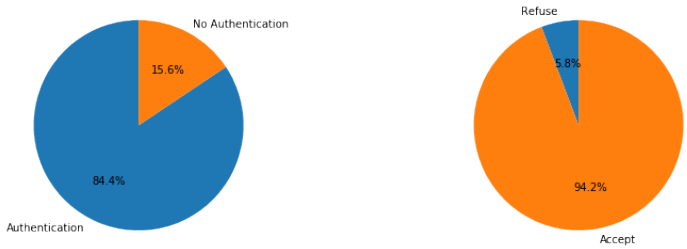
(a) (b)

Figure 2: Authentication required and Connection refusal for versatel.nl



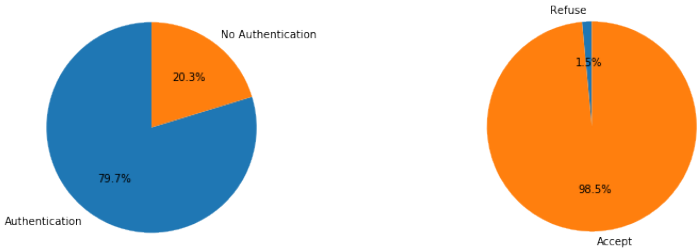
(a) (b)

Figure 3: Authentication required and Connection refusal for kpn.net



(a) (b)

Figure 4: Authentication required and Connection refusal for routit.net

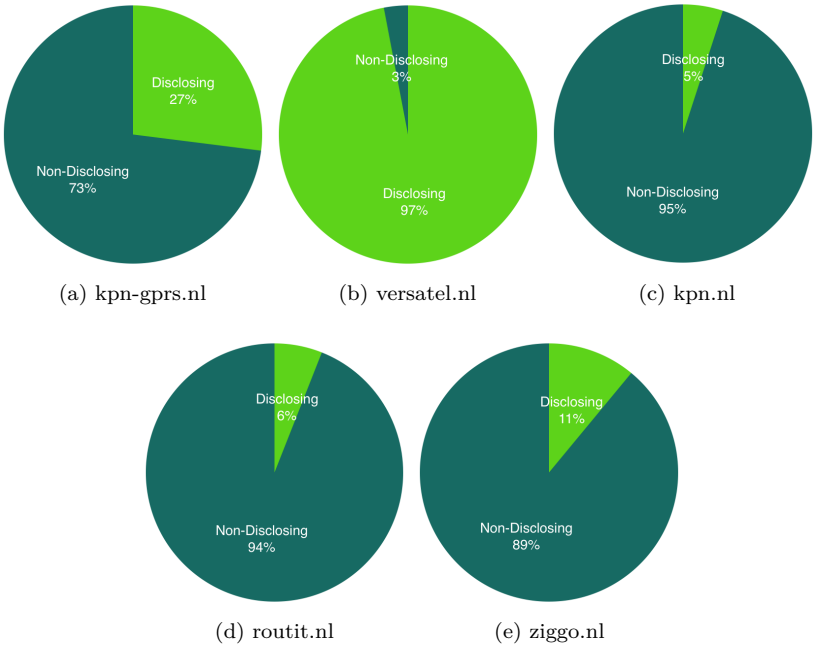


(a) (b)

Figure 5: Authentication required and Connection refusal for ziggo.nl

1.1.3 Information disclosure per hostname

Fingerprinting represents an important step in designing a strategy to victimize machines on the internet. Pieces of information such as the running operating system or the running service are of extreme importance to determine what vulnerabilities the device is prone to and what exploit tools could be used. The metric, as it was designed in the previous assignment, showed the overall percentage of the machines that disclose some kind of information about their running os/service. We have now rearranged it to show the percentage of disclosing machines for the top 5 hosts, the results are shown in fig. 6.



(a) kpn-gprs.nl (b) versatel.nl (c) kpn.nl

(d) routit.nl (e) ziggo.nl

Figure 6: Fraction of disclosing IPs for the top 5 hosts

2 Actors involved in the security issue

In this section, several of the actors involved in our security issue are analyzed. We expand upon a possible countermeasure, the costs and benefits involved and the presence of externalities with the proposed countermeasure.

2.1 End users of IoT devices

The end users of the devices are the largest group of actors which do not directly suffer from the security issue. However, with a solid countermeasure this security

issue can be mitigated completely. If there are no insecure IoT devices, then no botnet of IoT devices can be created.

2.1.1 Countermeasure: configuring a firewall

The main problem with publicly accessible IoT devices is that they are not behind a firewall. In most cases, customer routers have a built-in firewall but this not correctly used. For example, when UPnP is enabled or ports are forwarded, the IoT devices still are publicly accessible. If this firewall is not present or simply not working, a new customer router should be provided.

2.1.2 Costs, benefits and incentives

The first solution, disabling UPnP will have no direct cost. The main problem however, is that most consumers do not know how to do this or even that they have to do this. The incentive to do this is not present, so this will need to be done by the ISP as the consumer routers are mostly supplied by their ISP. If there is no firewall present, a new consumer router should be requested from the ISP which also does not have direct costs for the consumer. In both cases, there are no direct costs for the consumer. The main issue is that the incentive to request or configure the firewall is not present.

2.1.3 Externalities

A positive externality is that the costs for ISPs for the prevention of DDoS attacks such as IDS's are less as the botnet sizes are shrinking due to better protected devices due to Firewalls. Furthermore, the costs for target companies are less as the DDoS attacks are gradually smaller.

A negative externality is that the costs for ISPs are increasing thus indirectly increasing costs for consumers. The ISPs will possibly need to supply new routers for consumers.

2.2 Internet Service Providers

Internet Service Providers can play a role in the mitigation of DDoS attacks against its customers. Internet Service Providers that offer bandwidth capacities to their customers that are large enough to be able to for example stream high-quality videos have to have a large amount of total bandwidth available (to be divided among their customers). However, while an ISP might have a large total bandwidth capacity, this capacity is tiered down to cities, areas and even blocks of streets. When a customer's home connection is attacked by a sufficiently large DDoS attack, this might affect other home connections on the same street or in the same area as well.

2.2.1 Countermeasure: black hole routing

To mitigate the loss of internet connection for other customers, an ISP could implement a black hole routing mechanism. The ISP would need some kind of detection mechanism to determine that one of their customers (or even a range of customers) is under attack, after which the ISP could simply drop all traffic with the detected maleficent characteristics to the target IP range until the attack volume decreases. Simply put: all access to a customer's self-hosted service that is under attack is blocked temporarily to protect the internet connection of other customers.

2.2.2 Costs, benefits and incentive

For the ISP, costs are relatively low compared to other DDoS mitigation strategies. A detection mechanism needs to be set up that can either notify a network administrator to approve certain routes to be blocked, or the detection mechanism can control the lower-tier routers automatically so minimal human oversight is needed. The ISP would only have to refund (part of) their fees to a single customer for their experienced downtime, instead of to a significantly larger part of their network. As a fully-automated system primarily requires a one-time investment to develop or purchase and does not require much maintenance, an ISP certainly has an incentive to implement such a system. They could not only significantly reduce refunds for downtime, but also relieve stress on their customer support department during attacks. When an ISP is large enough, the indirect costs related to a DDoS attack outweigh the direct costs of implementation of a black hole routing system.

The direct victim of the attacks is less well off. Their hosted service is blocked for the entirety of the attack duration, thus they would lose all expected revenue for their hosted service during this time period. The factors a potential attack victim would consider are the extra costs involved in hosting their service on an external server with more advanced DDoS protection, the expected profits they would make from their service, and potentially other (vital) services they are hosting from the same internet connection.

For all other customers however, internet access is not affected. They suffer no losses. Prospective customers have an incentive to become part of an ISP that implements a black hole routing mechanism. Firstly because their own connection is protected from attacks against the rest of the network. Also, because their ISP makes less overall costs, the monthly subscription fees to individual customers is kept relatively low.

2.2.3 Externalities

As other customers than the attack victim are not directly involved in the solution, the fact that their network connectivity is unaffected from a DDoS attack can be seen as a positive externality. They benefit from the ISP protecting themselves against DDoS attacks on other customers.

A negative externality that comes paired with a black hole routing system is that this method ultimately does exactly what the attackers intend: denial of service of the target service. If an attacker knows that an ISP implements such a system, they can be confident that their DDoS attack will succeed as long as the traffic volume is high enough.

2.3 Manufacturers

2.3.1 Countermeasure

2.3.2 Costs, benefits and incentives

2.3.3 Externalities

3 Influences on Security Performance

3.1 Factors

3.1.1 Industry

The variance in the security performance might be caused by the Industry in which the company owning the devices is active.

Table 1: SLD & NAICS & SIC

SLD	NAICS	SIC
kpn-gprs.nl	517310	481302
versatel.nl	518111	737401
kpn.net	518210	737415
routit.net	518210	737415
ziggo.nl	518210	737415

2002 NAICS codes:
517310 : Telecommunications Resellers
518111 : Internet Service Providers
518210 : Data Processing, Hosting, and Related Services

3.1.2 Size of company

Another factor that might have influence on the security performance difference we see is the size of the company who owns the devices. Large companies tend to spend more money on IT security.

3.2 Collect data for one or several of these factors

For both the factors, industry and company size, we can use our dataset for information on the amount of devices per industry that belong to the metric.

For the data on the company size, we will use publicly available revenue data and categorize the different companies.
Since this dataset is from 2018, the devices behind the versatel domain belong to the swedish company Tele2. Revenue 2018:
KPN: 5.64 billion euro [1]
Tele2: 2,18 billion euro [2]

Table 2: Devices requiring authentication per NAICS industry

	Type of industry		
Authentication?	517310	518111	518210
Yes			
No			

Table 3: Devices accepting connections per NAICS industry

	Type of industry		
Accept?	517310	518111	518210
Accept			
Refuse			

Table 4: Devices disclosing software information per NAICS industry

	Type of industry		
Disclose?	517310	518111	518210
Yes			
No			

3.3 Statistical analysis

Based on the factors described above, we have set up a number of hypothesis which we are going to explore using Pearson's χ^2, which shows if there is a relation between factors, and Cramer's V to see how strong the relation is.

- H_1 = Type of industry and amount of devices that require authentication are independent.
- H_2 = Type of industry and amount of devices that refuse the connection are independent.
- H_3 = Type of industry and amount of devices that disclose sensitive information are independent.
- H_4 = Company revenue and amount of devices that require authentication are independent.

- H_5 = Company revenue and amount of devices that refuse the connection are independent.
- H_6 = Company revenue and amount of devices that disclose sensitive information are independent.

4 Conclusion

References

[1] KPN Group, "Kpn jaarverslag 2018," 2019, accessed on 14.10.2019. [Online]. Available: https://jaarverslag2018.kpn/

[2] Tele2 AB, "Tele2's annual report 2018," April 2019, accessed on 14.10.2019. [Online]. Available: https://www.tele2.com/media/press-releases/2019/tele2s-annual-report-2018