WM0824TU Group 9
Block 3

Chris Berg, 4216776
Martin Koster, 4371011
Radinka Yorgova, 4952545
Wilko Meijer, 4224426

October 8, 2018

1 Problem owner

The security issue that becomes clear from the mirai badpackets [1] dataset is the spreading of the mirai malware by infecting new IoT (Internet of Things) devices and increasing the size of the corresponding botnet(s). The problem owner of such a security issue is the person or persons that are responsible or most affected by the security issue. A logical choice for the problem owner would be the owners of the infected IoT devices, since they have direct control over the devices that are contributing to the spread of the malware. However, these owners, in most cases, aren't aware that their devices are infected, wouldn't know how to fix the infections, and aren't suffering many consequences from the infections. Therefore we argue that the Internet Service Providers (ISP's) are the problem owners of this security problem. The ISP's control the networks that are used for spreading the malware, so they are able to detect and stop malicious network traffic. Furthermore, there are much less ISP's than owners of IoT devices, so it is easier to tackle the security issue in a coordinated and effective manner. Lastly ISP's are also harmed by this security issue, since malicious traffic in their network causes reputation damage. So because ISP's are in the best position to fix the security issue, they are the problem owners.

2 Security performance of different metrics

In our current study we propose the following metric: The total amount of IPv4 addresses showing behaviour related to Mirai malware infection newly observed per ISP over time.

Ideally we would also like to normalize this metric on the amount of IPv4 addresses registered in the AS's owned by the ISP's. However, it turned out to be too hard to find reliable data on the amount of IPv4 addresses within an AS. So, because we aren't able to normalize the data we can't discuss why some of the ISP's have more IP addresses showing behavior related to infections than others. Furthermore, we assume that the data given by the source are reliable and we do not take into account possible abnormalities caused by data collection.

It is infeasible to plot all the results from applying the metric on the dataset. Therefore in Figure 1 a random selection of ISP's is plotted and, to highlight some further differences (or similarities) across the world, in Figure 2, Figure 3, and Figure 4 ISP's operating on the same continent are plotted.

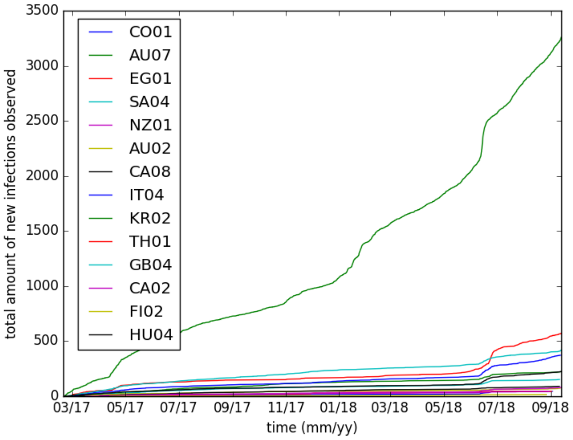


Figure 1: Metric applied on a random selection of ISP's

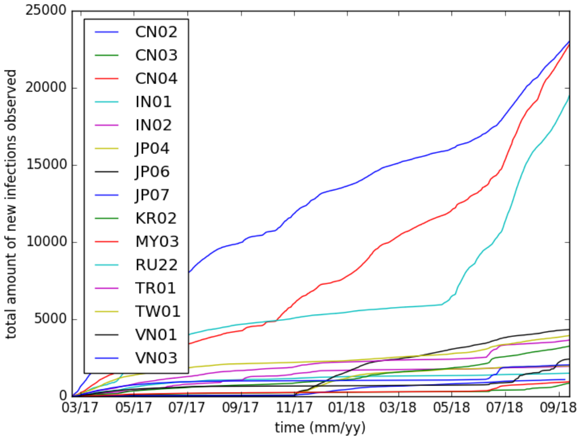


Figure 2: Metric applied on ISP's operating in Asia and Oceania

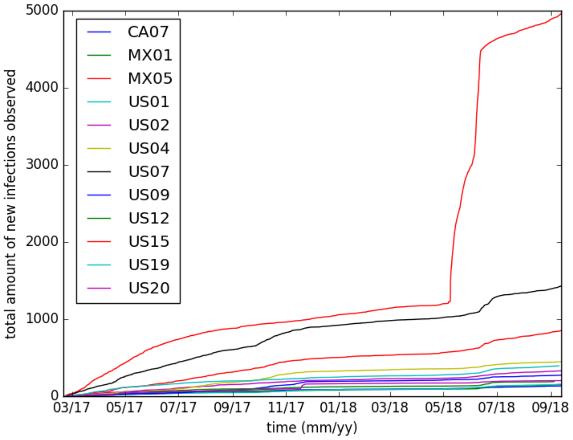


Figure 3: Metric applied on ISP's operating in North America

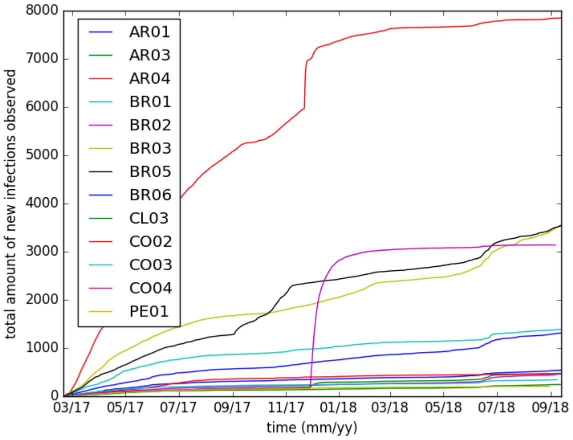


Figure 4: Metric applied on ISP's operating in South America

As becomes clear from the plots, most of the ISP's follow a similar pattern globally, the total amount of new infections detected increases steadily, so there is little change in the rate of new infections within the network of the ISP. However, around July 2018, the rate at which new infections are detected increases, to later level off again to previous rates. The fact that this is visible for almost every ISP suggests a change in tactics of the attacker. All these plots reveal some interesting deviations from this standard behavior, below some of those are listed and their possible causes are evaluated.

Sudden very large increase In Figure 3, one ISP has a sudden very large increase in a short amount of time of the amount of IP addresses showing behavior related to infecions, a similar very large increase is also visible in Figure 4 for two ISP's. Possible reasons for this can be: a change in policy by the ISP, which reduces the limitation of the spread of the security issue. Other reasons might be a previously unknown vulnerability being exploited, as seems to be the case for MX05 in Figure 3, which is the ISP Telmex. A news article from 30 April 2018 talks about vulnerable routers in their network, about the same time as the infection rate starts to go up.[4]

Change in infection rate For some ISP's the infection rate changes against the trend of other ISP's, for example this becomes visible in the Asia plot (Figure 2) where plots that were at first parallel to others, start crossing the other plots, indicating a change in infection rate. This could for example be caused by change in a security policy of the ISP, an increase in vulnerable devices in their network, due to a router 'upgrade' or changed attacker behavior.

Infection rate of 0 For some ISP's the plots eventually become a flat line, meaning that there are (almost) no new infections observed. Examples of this can be found in the Asia (Figure 2) and very obvious for one ISP in South America (Figure 4). It's happening after a big spike, e.g. the one of July 2018. A possible reason for this can be that ISP's started to worry about the rate at which the malware was spreading and took radical action, like disabling port 23 (telnet) which is often used for spreading the Mirai malware. [3]

3 Risk Strategies for the problem owner

The problem owner can follow several risk strategies to reduce the spread of the malware. This would become visible in the metrics by a change in how many new infections are observed, as this would imply a change in the rate the malware spreads. An ISP is a security provider, as their core business is IT and security comes second to their core business, so their decisions are business-driven. The business of an ISP is selling connections to the Internet, this often means that people pay for their connection to the internet, but not for the amount of traffic they generate. However, some business clients and most ISP's themselves (except for a few at the very top), pay a rate related to how much traffic they generate. [2] An increase in network traffic, thus will increase the cost of running the network. Since most of the IoT devices will be owned by private users, the ISP will have to deal with most of the increased cost themselves. Increasing rates probably won't be understood by most costumers.

Taking this into account, possible risk strategies for the problem owner are:

- Risk reduction - Investing in detection and blocking of malicious traffic, reducing the security issue and decreasing the loss incurred by the security issue.

- Risk reduction - Investing in awareness campaigns of malware infections for device owners, thus tackling the source of the problem and reducing the security issue.
- Risk acceptance - Doing nothing against the spread of the malware, accepting the risk; accepting increased cost and possible reputation damage.
- Risk transfer - Charging costumers based on the traffic they generate, thus transferring the risk of extra traffic related cost. This does not address the risk of reputation damage, which is accepted in this strategy.
- Risk transfer - Seek insurance for any botnet/malware related damages, thus transferring the risk to an insurer.

Risk avoidance is not an option for the ISP as the security issue is embedded in their core business: providing Internet access.

In [5], research is done in the amount of influence ISP's have in controlling the botnet in The Netherlands. There is stated that around 80% of the infected machines are located in a network which are hosted by the major Dutch ISP's. So ISP's indeed have a high influence and can be a potential control point for detecting the botnets. This report also states that 14 ISP's with a market range of 90% have signed an agreement to put botnet mitigation controls into place. So in the Netherlands they are really making steps for risk mitigation. This is clearly not the case for many other countries in the dataset.

4 Other Actors and their Risk Strategies

There are also other actors besides the problem owner that influence the security issue as defined in chapter (1). The actors are all parties able to influence the spread of the botnet. These parties are the device owners, manufactures, attackers and government. All the strategies of these actors are totally different from the strategies of the problem owner which you saw earlier. The problem owner is more focused on trying to decrease the potential losses from a botnet attack where the other actors are more focused on mitigating and decreasing the botnet.

- Owners of infected devices - As stated in the previous section, the owners are not all likely to take steps against the botnet. Due to the fact that most of them don't even know their device is infected and even if they know, they don't experience a lot of loss from it. Their risk strategy is then risk acceptance. The only exception is when the botnet has been used for spreading ransomware and besides that there are also people who are willing to mitigate the risk of the botnet. In [6] they describe a few steps which an owner of an infected device can apply, which are all risk mitigation steps. Except for one which is risk avoidance, by discontinuing the use of the infected device.

- Manufacturers of infected devices - Due to the fact, that more and more IoT devices are purchased, there is a bigger threat for the botnets to increase their size. The manufacturers of these IoT devices need to take more measurements to prevent attacker from infecting their devices [10]. All of these measures will be risk mitigating. A simple action would be to stop using a default login. Of course, there will always be some manufacturers who don't take these steps and will accept the risk. Unless this will be mandatory by the law, which brings us to the next point.

- Government - The government cannot influence the botnet spreading directly, except for their own infected device of course. But they can make a difference indirectly. They can make regulations or initiate changes to the law to limit the spread of botnet [9]. Think of a regulation that manufacturers need to secure their products against this kind of attacks. The same will also hold for ISP's. An example of this, which is already put in place, is the blocking of port 32 at nighttime by the Korean government. These actions of the government will also be risk mitigating strategies.

- Attackers - The attackers play also a very important role in the spreading of the botnet, but they won't have incentive to mitigate the risk since they are behind the whole attack.

On overall, there are many actor who apply risk mitigating actions against the spreading of botnets. This has been increasing over time, because the threat is becoming bigger since there are more IoT devices purchased. However there are still a lot of actors who accept the risks. So because of the increasing threat and large number of actors who accept the risks, the risk is not reduced and maybe even increased.

5 Return on Security Investment

This section is about the estimation of the Return Of Security Investment (ROSI). Section 3 described a few risk strategies which the problem owner could apply. The risk acceptance strategies are simply not an option for ISP's since the risk will affect their core business. Also risk transfer is not optimal because in this case they will also accept the risk but they will cover the risk through an insurance or the increasing fee of customers. So the strategy this section will take into account for estimating the ROSI is the risk reduction (or risk mitigation).

ROSI indicator is defined by

$$ROSI = \frac{benefit - cost}{cost} = \frac{ALE_0 - ALE_1 - cost}{cost}, \quad (1)$$

where ALE_0 and ALE_1 are the annual lost expectancy correspondingly without and with security measures. To be able to derive ROSI of this risk strategy, the costs of this strategy need to be estimated, as well as the impact and the frequency of an attack. First we focus on the costs and in the next section on the benefits.

5.1 Cost estimation

In general the costs of implementing the strategy are classified as direct and indirect.

Security controls are the lower bound of the costs for every risk reduction strategy. They include direct and indirect costs as follows:

- **direct costs**:
  - expenses for acquisition of the detection and blocking hard- and software on end users like anti-virus scanners, firewalls, routers, embedded home network security in routers, etc. They are mainly one time cost;
  - costs for acquisition of Network Intrusion Detection Systems (IDS). Such a system monitors/examines network traffic for malicious activity such as distributed denial of service (DDoS) attacks, certain forms of malware and policy violations. It can take actions as sending an alarm, dropping detected malicious packets, resetting a connection or blocking traffic from the offending IP address. It prevents from known intrusion signatures, but also from some unknown attacks due to its database of generic attack behaviors. This system is for the ISP use.
  - costs for installation of the security system (mainly labor hours) - one time cost;
  - costs for maintenance of the security software/hardware (mainly labor hours) – continuous.
- **indirect costs** - the monetary equivalent of time lost due to:
  - forgotten passwords after enforced changes;
  - the inconvenience of transferring data between different security zones
  - incompatibilities between security mechanisms

Here we list other costs which are not necessarily security controls. They are also under the main classification of direct and indirect costs:

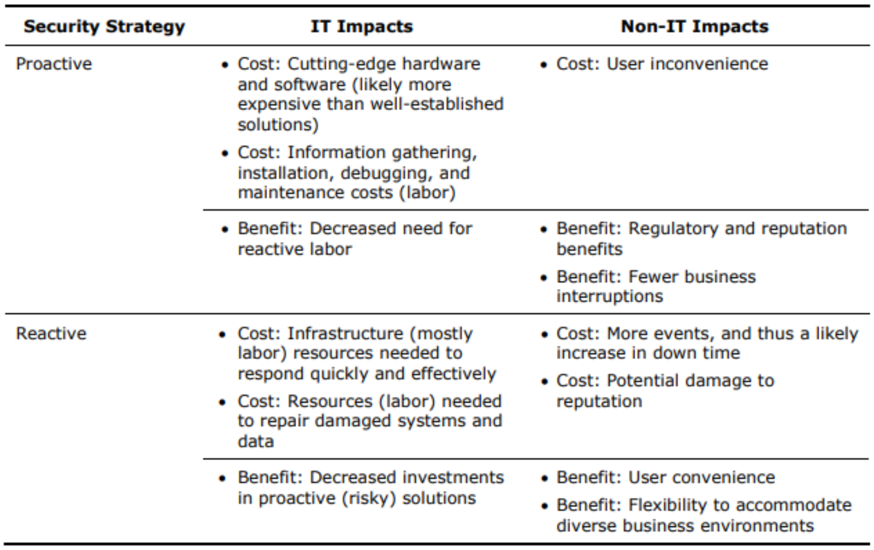
- **direct**:
  - training for the personnel;
  - awareness campaign within the staff of the ISP;

- **indirect**:
  - missed opportunity costs – costs because of enforce confidentiality of information (denied access to information) that is relevant for business decisions and because of this missed opportunities.

  This will be out of the scope of this report to estimate these costs. For this we have to dive in all the detection and blocking security controls and estimate for all those techniques the benefits.

In figure 5 you see a good overview of the general costs and benefits which comes with such a security investment according to [7].

Figure 5: Comparison of IT and Non-IT costs and benefits



Security Strategy	IT Impacts	Non-IT Impacts
Proactive	• Cost: Cutting-edge hardware and software (likely more expensive than well-established solutions) • Cost: Information gathering, installation, debugging, and maintenance costs (labor)	• Cost: User inconvenience
	• Benefit: Decreased need for reactive labor	• Benefit: Regulatory and reputation benefits • Benefit: Fewer business interruptions
Reactive	• Cost: Infrastructure (mostly labor) resources needed to respond quickly and effectively • Cost: Resources (labor) needed to repair damaged systems and data	• Cost: More events, and thus a likely increase in down time • Cost: Potential damage to reputation
	• Benefit: Decreased investments in proactive (risky) solutions	• Benefit: User convenience • Benefit: Flexibility to accommodate diverse business environments

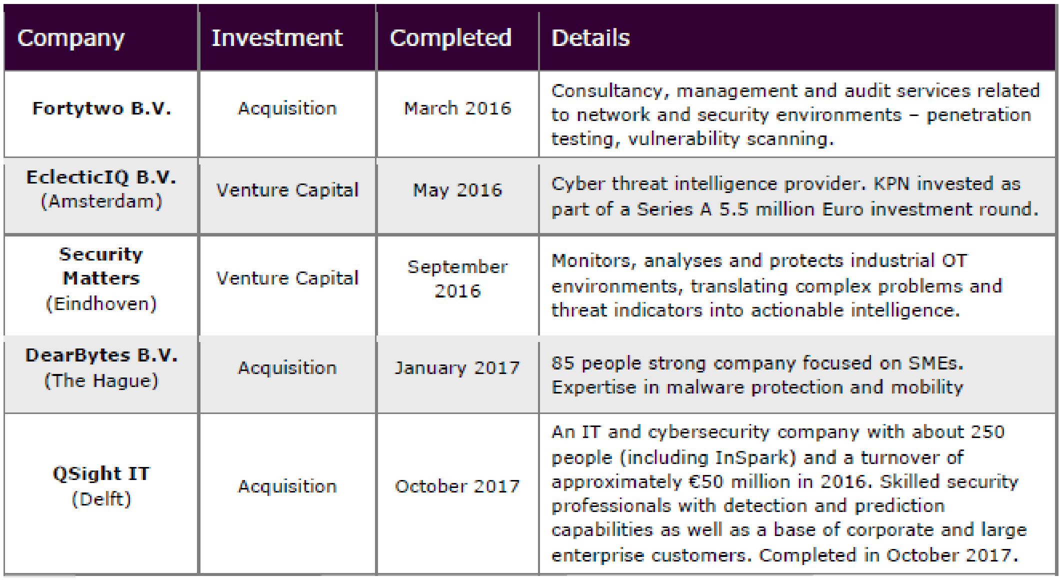
Figure 6 gives an overview of the security investments of KPN during the 2016-2017 after their experience of the 2012 attack [11]. Most of them are long term investments. As you may see not all the investments have a real financial figure in the provided data. Therefore we use hypothetical data in our security strategy. To get an impression about the percentage which they have invested we have to mention that in 2016 KPN generated €6.8 billion in revenues with an EBITDA margin of 39.7 % [1]. Looking at the figures in 6, we estimate the security investments of KPN to be around 1% of their revenue.

This is one example for an investment in cybersecurity. To generalize our calculations we use the data for the global ISP industry published on [12] and

[1] EBITDA = Earnings Before Interest And Taxes + Depreciation + Amortization and EBITDA Margin = EBITDA/Total Revenue

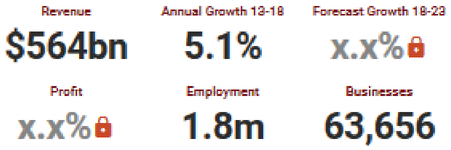
given on Figure 7, extrapolating on the KPN data gives us a total cost estimate of 1% of the total revenue or $5.6 billion annually.

Figure 6: Security acquisitions and VC investments of KPN



Company	Investment	Completed	Details
Fortytwo B.V.	Acquisition	March 2016	Consultancy, management and audit services related to network and security environments – penetration testing, vulnerability scanning.
EclecticIQ B.V. (Amsterdam)	Venture Capital	May 2016	Cyber threat intelligence provider. KPN invested as part of a Series A 5.5 million Euro investment round.
Security Matters (Eindhoven)	Venture Capital	September 2016	Monitors, analyses and protects industrial OT environments, translating complex problems and threat indicators into actionable intelligence.
DearBytes B.V. (The Hague)	Acquisition	January 2017	85 people strong company focused on SMEs. Expertise in malware protection and mobility
QSight IT (Delft)	Acquisition	October 2017	An IT and cybersecurity company with about 250 people (including InSpark) and a turnover of approximately €50 million in 2016. Skilled security professionals with detection and prediction capabilities as well as a base of corporate and large enterprise customers. Completed in October 2017.

Figure 7: Industry Statistics & Market Size



Revenue	Annual Growth 13-18	Forecast Growth 18-23
$564bn	5.1%	x.x% 🔒
Profit	**Employment**	**Businesses**
x.x% 🔒	1.8m	63,656

5.2 Benefit

Now we know the estimated and hypothetical costs of such a security investment. But an important question now is, how much benefit will this security invest give the ISP back? To answer this question we first have to determine the impact/frequency of the threat with and without the security investment.
For this we can use the dataset. We have access to all the new infections and their corresponding AS number. From this we can get all the new infections an ISP gets in a certain amount of time. In 8 the time period is 14 days.

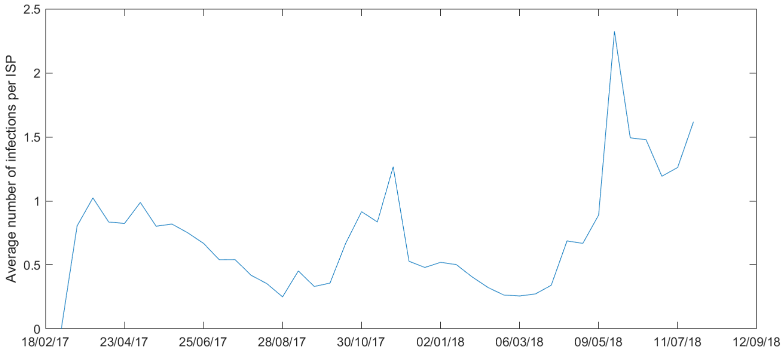


Figure 8: Average amount of new infections per ISP, per 14 days

From this we can get the average amount of new infections of an ISP. Which gives an average of 20 per year. With the use of the security investment this frequency would probably be lower. For this outcome there are no accurate on estimates available. We have to make an hypothesis for this. We assume that there will be significant less infections but not too much, because not every infection will have the same signature. Which makes it more difficult for the ISPs to detect these infections. Because we can not see the decrease of the infections accurately we make an estimation in the form of a normal distribution with its mean around 70%. This means that it is most probable that the frequency is 70% less.

The impact on the ISPs are not very concrete, because their main loss is in the form of reputation. However companies suffer a lot of loss when they experience an attack from such a botnet. So indirect those infections will affect the companies. As stated in [7] the loss of a company is estimated between $12,000 and $24,000. And the amount of attacks per day on all companies is on average 20,000 per day according to [8].

As we have seen the new infections are on average 70% less, we approximate this will also hold for the attacks per day on a company. So on average the new amount of attacks per day will be around 14.000. The impact of an attack against the companies will not change. When an attack comes through (which has a fewer frequency now), the security investment of an ISP will not affect the companies.

5.3 Conclusion

To conclude above findings we have to compare the costs with the benefits. As we have seen in subsection 5.1 the costs for security investments by ISP's globally per year is around $5.6 billion. Without the security investment the loss for companies will be approximately 20 000 times $12 000 to $24 000, which gives a loss between \$240 000 000 and \$480 000 000 per day for all the companies. With the security investment there will be on average 14 000 times \$12 000 to \$24 000, which gives a loss between \$168 000 000 and \$336 000 000. This results in average benefit between \$72 000 000 and \$144 000 000. Plugging these numbers into the ROSI calculation we get the following result:

$$\begin{aligned}
ALE_0 &= 365 \cdot \$240\,000\,000 \text{ to } 480\,000\,000 = \$87.6 \text{ billion to } \$175.2 \text{ billion}\\
ALE_1 &= 365 \cdot \$168\,000\,000 \text{ to } \$336\,000\,000 = \$61.32 \text{ billion to } \$122.64 \text{ billion}\\
\text{cost} &= \$5.6 \text{ billion}\\
ROSI &= \frac{\$87.6 \text{ billion to } \$175.2 \text{ billion} - \$61.32 \text{ billion to } \$122.64 \text{ billion} - \$5.6 \text{ billion}}{\$5.6 \text{ billion}}\\
&= 3.7 \text{ to } 8.4
\end{aligned}$$

As becomes clear from this calculation there is a huge benefit to the entire economy for investment in security by ISP's, the return on investment can be as high as 8.4 times the investment. The problem is that these benefits are for companies and not for the ISP's themselves. As we have seen in subsection 5.2 the impact on ISP's is negligible except for the reputation loss. So the incentives for an ISP to implement this security investment are not great. Therefore, to make this investment viable, either the cost of security investment should come from the companies instead of the ISP, or the ISP should be forced to invest without benefits. This is where the government plays a big part, as also discussed in section 4. When the government make regulations with regard to this subject, either that ISP's have to implement some security investment or that the industry should contribute to the cost that the ISP's have, this will help the victims of botnet attacks a lot.

References

[1] Mirai-like Botnet: Bad Packets Report, https://mirai.badpackets.net/, accessed 13 Sep 2018

[2] W. Dai and S. Jordan, ”ISP Service Tier Design,” in IEEE/ACM Transactions on Networking, vol. 24, no. 3, pp. 1434-1447, June 2016

[3] Antonakakis, Manos, et al. ”Understanding the mirai botnet.” USENIX Security Symposium. 2017.

[4] Zack Whittaker, ”Over a million vulnerable fiber routers can be easily hacked”, https://www.zdnet.com/article/over-a-million-vulnerable-fiber-routers-can-be-easily-hacked/, accessed 5 Oct 2018.

[5] Michel J.G. van Eeten, Hadi Asghari, Johannes M. Bauer, and Shirin Tabatabaie (2011) ”INTERNET SERVICE PROVIDERS AND BOTNET MITIGATION.”

[6] NJCCIC (2018) ”Botnets”. https://www.cyber.nj.gov/threat-profiles/botnets/#STRATEGIES-TO-PREVENT-AND-MITIGATE-POTENTIAL-IOT-COMPROMISE

[7] Gallaher, M. P., Rowe, B. R., Rogozhin, A. V., & Link, A. N. (2006). Economic Analysis of Cyber Security. RESEARCH TRIANGLE INST (RTI) RESEARCH TRIANGLE PARK NC.

[8] https://ddosmon.net/insight/ accessed 6 Oct 2018

[9] Howard Solomon. (2018). Governemts should use buying, regulatory power to fight botnets: Expert.

[10] Bill Hull. (2018). IoT risk and the smart factory: Building cyber resilience

[11] A custom report for KPN, Patrick Donegan, Principal Analyst, Harden-Stance, February 2018

[12] www.ibisworld.com/industry-trends/global-industry-reports/telecommunications/internet-service-providers.html