Economics of Security

Final discussion for block 3, group 13 - IoT Honeypots

Rob van Emous, Rien Heuver & Patrick van Looy

Introduction

In this report we will first lay out well-defined metrics that remain from the report of last week. These metrics will be evaluated in the context of the provided dataset, in the hope that they may be used in evaluating the available risk strategies. Next, the problem owners are further defined and the risk strategies are presented as well as our interpretations of them combined with the metrics. Then we will look at other actors that are involved in our security issue, and whether these actors have means and incentives to assist the problem owner using the same or different risk strategies. Of all noted risk strategies, one will be chosen for a more in-depth Return on Security Investment (ROSI) calculation.

Metrics

Metrics based on dataset

As we are focussed on the ISPs, most metrics require the lookup of the ISP of IP-addresses in the dataset. This comes with two major difficulties.

1. Despite our best efforts, we could not find any affordable IP to ISP lookup service (or any equivalent service) that does not severely limit the number of lookup requests per timeframe. That is why for every ISP related metric, we had to limit ourselves to the top-10000 IP-addresses measured by total number of requests. Luckily, IP-addresses which did not make this list performed at most 29 requests in two months, thus seem to be of rather small interest to the ISPs.
2. As the honeypot dataset is more than a year old, due to DHCP churn: dynamic allocation of IPv4 addresses by ISP to their customers, quite some IPs will belong to different devices now. This decreases the significance of our ISP-related metric evaluation, but it does not decrease the value of the metrics in general. This issue is resolved when a more up to data honeypot dataset is evaluated using our metrics.

Using the data provided, we defined the following metrics that aim to help possible victim ISPs to identify themselves, prepare and act accordingly. The metrics are sorted to their positive informational and economic impact.

1a. Requests of top-10000 malicious devices per ISP over time

Using this[1] IPv4 address to geolocation API, we can discover both the location and the ISP of every top-10000 device. By looking at the total number of requests per ISP over time, an ISP would immediately see to what extent its network is currently affected and even more

[1] *Geolocation API* http://ip-api.com (Last accessed 01-10-2017)

importantly, how it performs compared to other (local) ISPs. This last competitive aspect is a big incentive for an ISP to actually take the issue seriously.

1b. Unique top-10000 malicious devices per ISP over time

This is related to metric 1a, but now instead of the total requests per ISP over time, we look into the number of unique malicious devices per ISP over time. This adds more informational value as it shows to what extent the ISP is dealing with a local-big-bandwidth and/or a distributed-small-bandwidth attack. The latter could indicate that a botnet of IoT devices is involved, rather than normal pc bots.

2a. Total requests per country over time

Using this[2] freely available IPv4 address to physical location database, we can discover the geographical distribution of the attackers. This gives insight into which countries yield most of the attack volume. If an ISP is located in this country, he can take accurate measures to discover whether this is also happening from or to its own network. As metrics 1a and 1b only take into account the top-10000 malicious devices, the added value of this metric is that it uses all data. It also has a drawback regarding the geolocation accuracy: only the country instead of specific ISP is known.

2b. Total unique malicious devices per country over time

This is related to metric 2a, but now instead of the total requests over time, we look into the number of unique malicious devices over time. Just like metric 1b when compared to metric 1a, it adds more informational value as it shows to what extent the ISP is dealing with a local-big-bandwidth and/or a distributed-small-bandwidth attack. The latter could indicate that a botnet of IoT devices is involved, rather than normal pc bots.

3 Attack strategy distribution of top-10000 malicious devices per ISP

From the dataset we have identified two major aspects of attack strategy both with its own two options resulting in four different attack strategies.

1. The first strategy aspect is the depth compared to the breadth of the attack. A deep attack focusses on a small number of devices which it tries to brute force. A broad attack tries a large range of devices only a small number of times.
2. The second strategy aspect is the sophistication of the attack. Thus whether the attacker is only trying to login to the device, or whether after logging in he actually tries to download and execute malware on the device.

By knowing the distribution of the four strategies over the ISPs, an ISP gets a great deal of information about which type of attacks are happening at its network. He can now take more effective measures to counteract the attacks.
Just like metrics 1a and 1b, this also shows how an ISP performs compared to other (local) ISPs and therefore results in added incentive via competition.

---

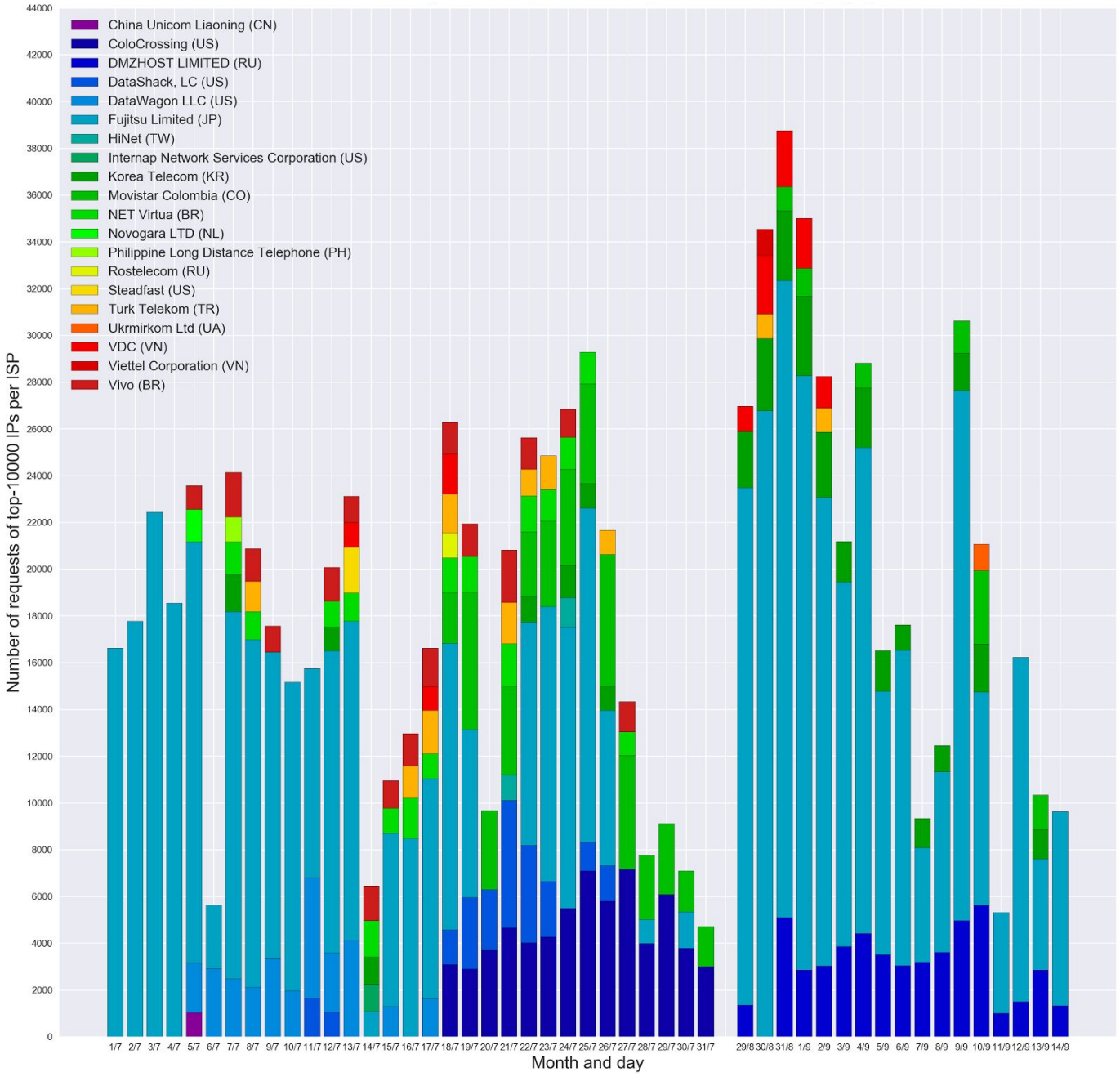
[2] *IP2Location lite database* http://lite.ip2location.com/database/ip-country-region-city-latitude-longitude (Last accessed 01-10-2017)

Metrics evaluation

Every metric has been evaluated on the whole 32GB honeypot dataset and the result of every evaluation is included as a CSV on our GitHub[3]. As most metric evaluations include too many different variables to be able to make a useful visualisation, we have reduced the number of devices, countries and/or ISPs in all visualisations based a metric-specific ranking.

1a. Requests of top-10000 malicious devices per ISP over time

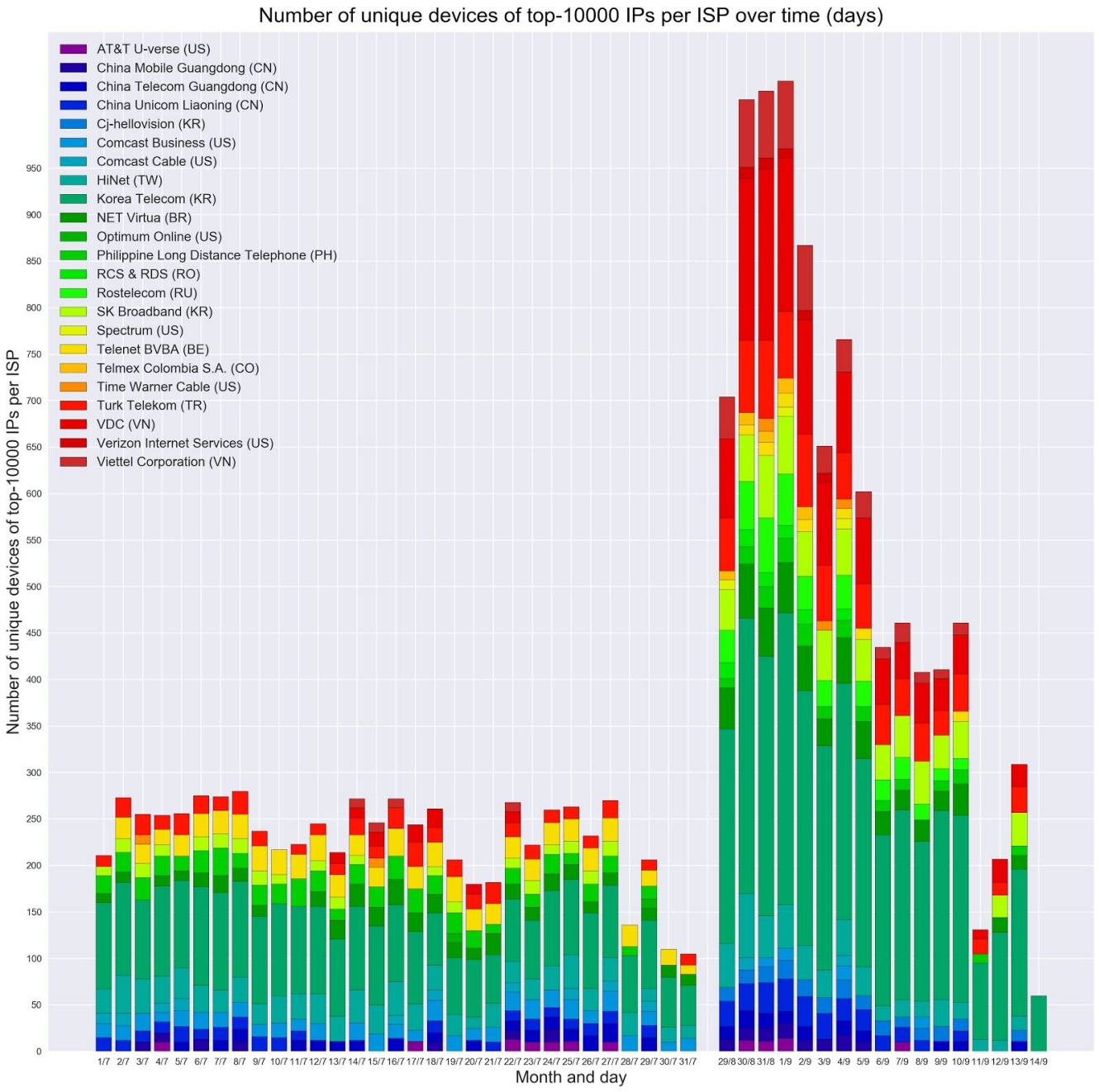
The figure below shows the metric evaluation. To reduce the number of ISPs in this figure, an ISP is only included on a certain day if its users performed more than 500 requests.



[3] *Our Github: 4TU-CybSec-EoS* - https://github.com/ProCessor00/4TU-CybSec-EoS

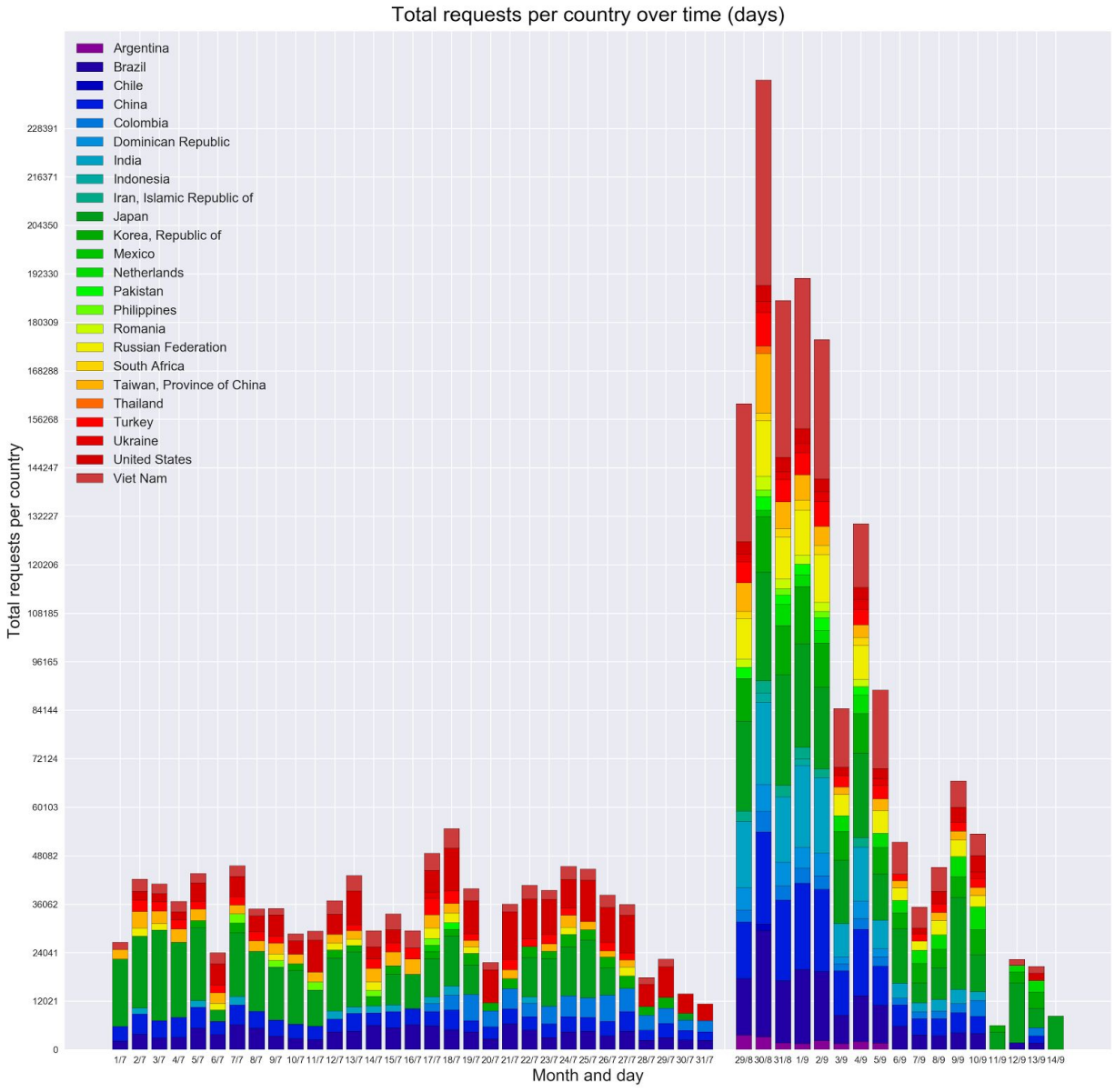
1b. Unique top-10000 malicious devices per ISP over time

The figure below shows the metric evaluation. To reduce the number of ISPs in this figure, an ISP is only included on a certain day if 15 or more of its users performed at least one request.



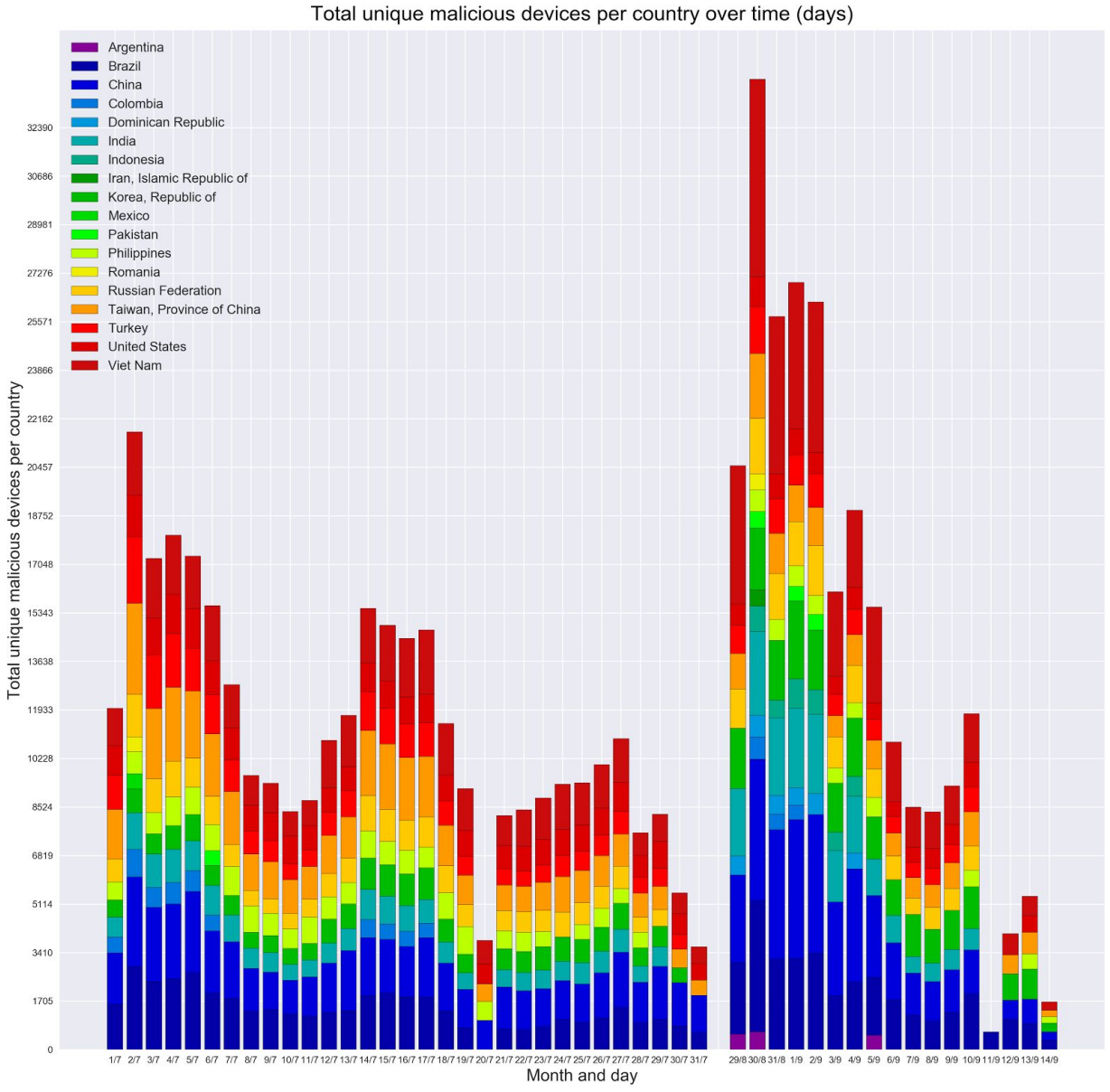
2a. Total requests per country over time

The figure below shows the metric evaluation. To reduce the number of countries in this figure, a country is only included on a certain day if its users performed more than 1500 requests.



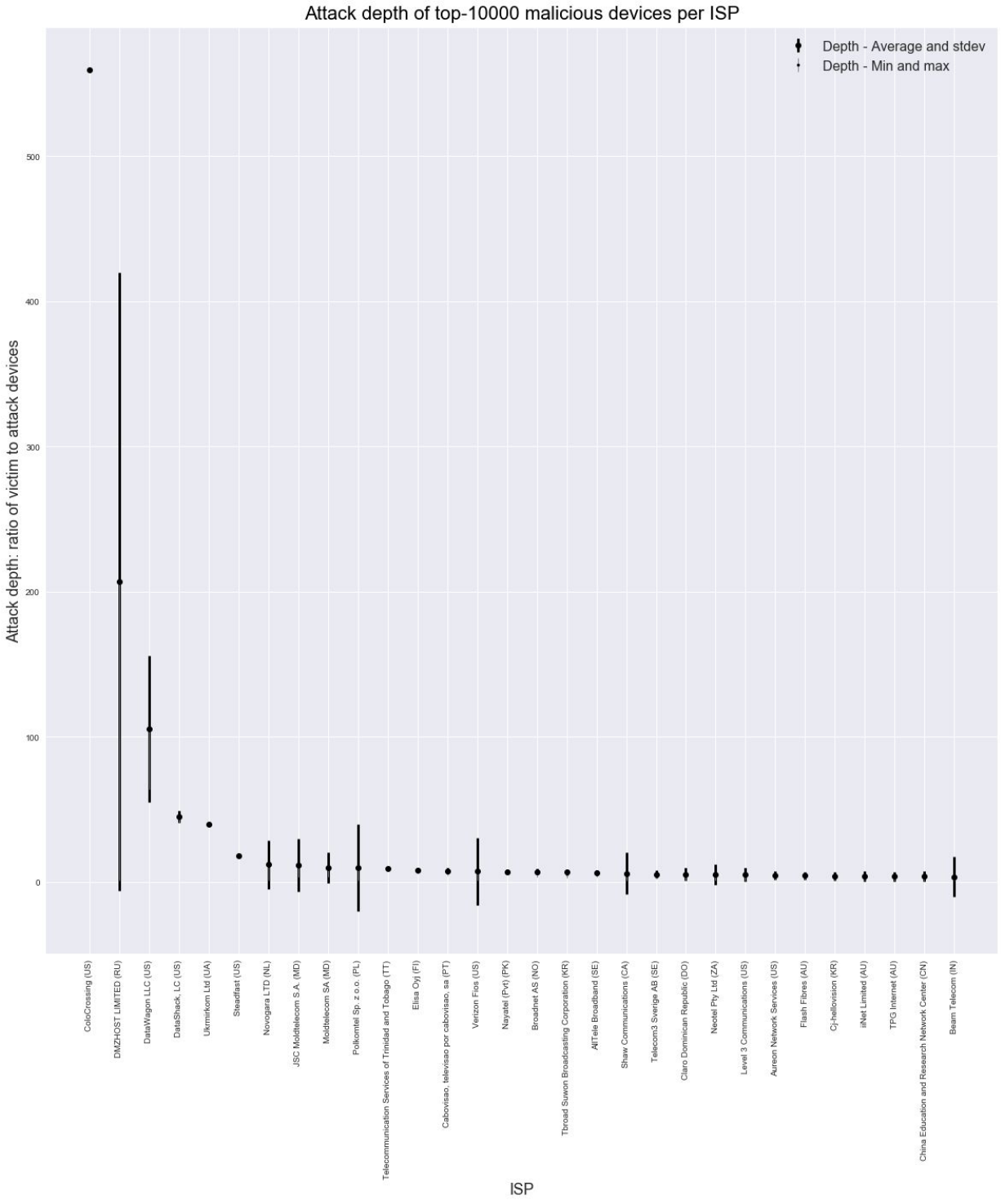
2b. Total unique malicious devices per country over time

The figure below shows the metric evaluation. To reduce the number of countries in this figure, a country is only included on a certain day if 500 or more of its users performed at least one request.

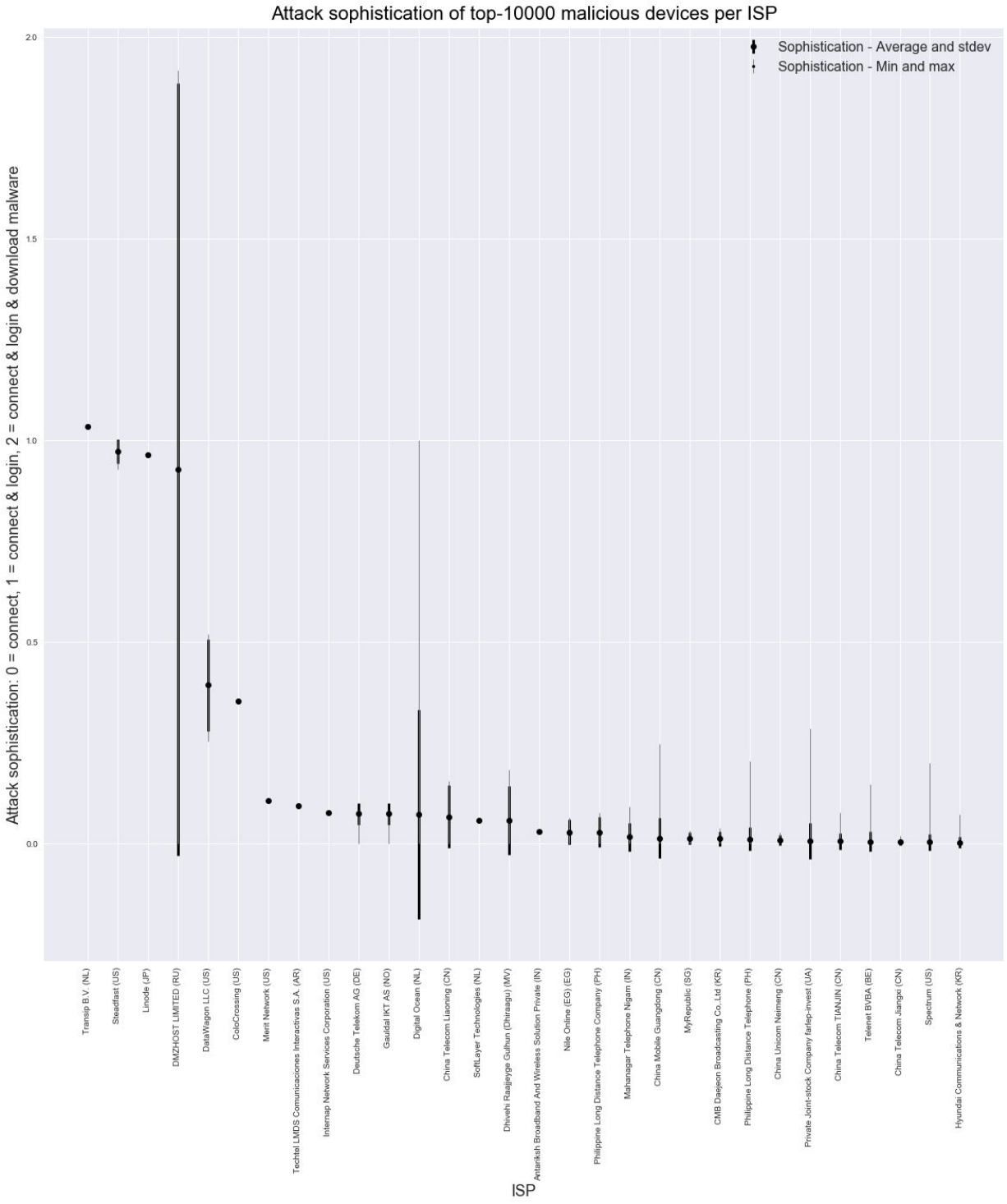


3 Attack strategy distribution of top-10000 malicious devices per ISP

The figure below shows the first aspect of the metric evaluation: the attack depth.



The figure below shows the second aspect of the metric evaluation: the attack sophistication.



Problem Owner

Before further investigating the problem owner, let's briefly recap the security owner which was defined in the assignment of last week. For improving the security of any system, it is very useful to know what type of attackers to expect, what kind of attack methods are used and what the target(s) of those attackers would be. The data needed for this analysis was retrieved by a honeypot mimicking an IoT device. With the increasing popularity of adopting more and more IoT devices in our lives, these same devices introduce new opportunities for attackers. We have seen that in late 2016 IoT devices were used for launching massive DDoS attacks after being infected by the so called Mirai Botnet[4].

These botnet-infected devices impose negative externalities. A botnet herder may infect thousands of IoT devices where the key here is that the harm on those infected devices is not necessarily just restricted to the owner of the device itself. In fact, it is often used for other purposes: to harm others, to send spam, to launch denial-of-service attacks or to infect other computers. As a result, you end up having a key part of the harm being felt by these other parties, and so there is not a strong incentive for the device owner to actually take actions, because they do not experience the consequences.

Besides the owner of a compromised IoT device and the possible target of an attack using these compromised devices, recent studies have shifted attention to key intermediaries, most notably, the Internet Service Providers (ISPs) that provide access to end users[5]. As explained by van Eeten et al.[6] ISPs form, to some extent, a natural control point for the effects of infected machines. Of course, the fact that ISPs can potentially mitigate this threat, does not mean that they should mitigate it. They are not the source of the externality but would have to bear substantial direct and indirect costs if they internalize the externalities of their customers. Nevertheless, the leading ISPs in the Netherlands have entered into a covenant that expresses their commitment to mitigate botnet activity in their own networks.

Of course ISPs will also have an incentive themselves since they do not want their network flooded due to these attacks which can cause slow connections or even downtime for the ISP's customers. Moreover, they will see their customers being both the victim and originator of the attack. Another advantage of focussing on ISPs is due to DHCP churn: dynamic allocation of IPv4 addresses by ISPs to their customers. Without knowing the IP update routines of ISPs, it is difficult to keep track of botnet bots.

Besides the establishment of alliances of ISPs in order to cooperatively fight against botnets, others are inspecting if it is actually possible to assign indirect intermediary liability to ISPs[7]. Although you might expect that liability should always be placed on the party that imposed a

---

[4] Thomas, K., Invernizzi, L., & Bursztein, E. (2017). Understanding the Mirai Botnet.
[5] Anderson, R., Böhme, R., Clayton, R., & Moore, T. (2008). Security economics and the internal market. *Study commissioned by ENISA*.
[6] van Eeten, M., Asghari, H., Bauer, J. M., & Tabatabaie, S. (2011). Internet service providers and botnet mitigation: A fact-finding study on the Dutch market. *Delft University of Technology*.
[7] Chandler, J. A. (2006). Liability for Botnet attacks. *Canadian Journal of Law and Technology*, *5*(1).

harm, this is not necessarily always the case. In particular, if the bad actor responsible for the harm is beyond the reach of the law, and there is some other third party in a good position to detect and mitigate the harm, then you can use indirect intermediary liability to assign responsibility to an innocent third party. In our case, ISPs are basically innocent third parties, however, they are in a good position to observe when their customers are infected.

Due to the above mentioned reasons we identified the ISP to be the best suitable candidate for the main problem owner. Especially if it ever becomes possible that an ISP can be held liable, there is even a bigger problem for the ISP. Later on in this report, we elaborate more on the other actors involved.

Risk strategies

When we investigate the possible risk strategies for the actors we just discussed we can identify a few interesting options. Following the general model, we can divide the options into four categories: acceptance, mitigation, transfer and avoidance. Immediately, we notice that options in two of the four categories are not sensible in this case. Accepting botnets can lead to serious degradation of an ISP's corporate image since customers are not interested in being part of spam campaigns, experiencing slow internet connection or even downtime. Moreover, they will simply switch to other providers when they are offered better terms there. The same holds for avoidance. Simply switching off services to not having to deal with possible attacks is not an option since providing internet access is the core business of an ISP. Therefore, two categories for risk strategies remain: mitigation and transfer. When choosing mitigation, an ISP can try to deploy the latest breed of intelligent, high-performance, DDoS and botnet defense solutions themselves. Not only does this help in mitigating attacks on their own network, they can also start offering DDoS mitigation as a service. On the other hand, favouring transfer of risk, they can choose a third party that offers DDoS protection as part of their service. Such specialised parties offering DDoS protection as a service can now effectively block DDoS traffic of all sizes and durations so that it never has a chance to impact their infrastructure, or its intended target, while legitimate traffic continues to flow. In the Netherlands, there is a collective project initiated by the *Stichting Nationale Beheersorganisatie Internet Providers* (NBIP, in English: National Internet Providers Association) called the *Nationale anti-DDoS Wasstraat* (NaWas, in English: National anti-DDoS Cleaning service). Collectively, ISPs joined forces and build a highly capable DDoS filtering services. ISPs who do not have sufficient funds to put these measures in place themselves, can route all their traffic through NaWas in case of an attack without having to pay high fees for the service as they would have with commercial parties offering such services.

Other actors and their risk strategies

Besides the ISP being an important actor in this situation as described above, a few other actors are in place as well. Most obvious are the product owner and the attacker. The prior being a consumer with an infected IoT-device and the latter being responsible for infecting devices. Besides these two obvious actors there is also the IoT-device manufacturer and possibly the actor with malicious intent making use of the botnet. The latter can be an

individual actor who for example hires an existing botnet to do his dirty work. This actor will in this section be referred to as the botnet-user. Each of these have certain risks and ways of mitigating these.

First of all, we have the product owner or consumer. This actor is usually oblivious of the situation: having an infected IoT-device. Since most of the time, the infected devices are used as a means to harm others, the product owner might not ever realise its device is infected. Since awareness comes before mitigation when assessing risks, most product owners will have no risk strategy at all.

Second of all there is the attacker. The foremost risk for attackers is to be caught; meaning they will be identified, held responsible and convicted for computer intrusion. There is also the, much less significant, risk of his/her work being too costly and thus not profitable, but since the investment into IoT-device hacking is rather small, this will not be any further regarded in this section. Thus an attacker needs to have a risk strategy aimed at preventing getting caught. To this extent an attacker might choose either to hide the attacks, or to take out its identity from the attack. We can see from the honeypot-data that hiding (automated) attacks will be a costly strategy, thus attackers will most likely focus on anonymisation of their attacks, for example by sending their attacks out from other bots, a public VPN or other comparable methods.

Third we have the IoT-device manufacturer. The risk for a manufacturer in this process is damage to its image. If many devices of a certain manufacturer get infected, customers get upset about this and this becomes public knowledge, the public image of the manufacturer is damaged which might hurt their sales. However, since customers are currently not picky about the security of their IoT-devices, this risk is not large for the manufacturer. A manufacturer might implement some security measures to mitigate the risk, but practice teaches that not many manufacturers do.

Last we have the prior explained botnet-user. This actor has much the same risk as the attacker. However, whereas an attacker will try to anonymise its attacks so law enforcement will not be able to track him/her, a botnet-user has a smaller desire to do so since its actions are not as trackable. Only once an attacker is compromised might the identity of the botnet-user get known to law enforcement. However, many attackers might have anonymity as a service on their botnet-product which in turn automatically helps the botnet-user mitigate its risks.

Regarding the above actors and their risks and mitigation strategies, we find that there is a certain liability-problem with the IoT-market. In most markets, the manufacturer will try hard to provide a secure product, for example with cars, door locks and laptops. In those markets, a consumer will want a safe product because of the risks for the consumer when its device gets compromised. The IoT-market is however much different in this sense, because consumers/product-owners are usually not the target of attack and thus hardly suffer from the consequences of having their device compromised. Since the customer does not care much about the security of the device, neither does the manufacturer. And this is the biggest cause of why IoT-devices are relatively easily compromisable.

Return on security investment

The return on security investment (ROSI) cannot be calculated easily for an ISP, since the costs of incidents are far from trivial. Currently, ISPs cannot be held liable for the consequences of botnets[7] as described earlier. Thus there is no obvious cost to an ISP when incidents occur. However, ISP-liability is a concept that is being looked into. To make this ROSI-calculation sensible we therefore estimated the costs of incidents as if an ISP would have been liable. The following numbers are based on acquirement costs of mechanisms over a period of three years.

As previously stated, costs of incidents are practically absent for ISPs. However, if an ISP were liable for botnet-originating incidents, meaning that infected devices causing the attack are originating from source addresses of the ISP, we base the ROSI for an ISP on an average of 200 botnet-related incidents per year and a loss expectancy per incident of $15.000 ($10.000 liability fine + $5.000 indirect costs). Thus the annual loss expectancy (ALE) $ALE = 200 \cdot 15000 = \$3.000.000$.

Since costs for installation of prevention mechanisms are highly speculative and accurate numbers are hard to identify for this use case, we imagine an ISP that can make use of NaWas as explained in the *Risk Strategies* section. That being said, we estimate that the NaWas could mitigate 95% of incidents annually. Let's say that the costs for being able to make use of NaWas are estimated to be $400.000 a year.

With these numbers we can calculate the ROSI as follows.

$$ROSI = \frac{ALE \cdot mitigation\ ratio - Cost\ of\ mechanisms}{Cost\ of\ mechanisms} = \frac{3000000 * 0.95 - 4000000}{4000000} = 612.5\%$$

According to this ROSI calculation, making use of the NaWas service is a very cost-effective solution. While these numbers might not be exactly accurate, it is of course imaginable that the ROSI for DDoS related issues in many cases is very high. Especially, in case of fines for liability issues, doing nothing is almost always a worse option.

Important to note: even though an ISP currently is not liable, investing in botnet prevention mechanisms could give a positive ROI on a relatively short notice since it introduces new business opportunities for an ISP. Then, an ISP could for example start offering DDoS-protection as a service to enterprises by filtering their incoming traffic.