# Economics of Security

Final discussion for block 4, group 13 - IoT Honeypots

Rob van Emous, Rien Heuver & Patrick van Looy

# Introduction

In the first part of this report, we perform an analysis on the possible countermeasures for three actors in the case of IoT botnets. For each of the actors, we define concrete countermeasures that they could implement. For each countermeasure, we analyse the cost and benefit distribution between all different actors that implementing the countermeasure would entail. Using this distribution we will discuss for each actor if it has (enough) incentives to indeed implement this countermeasure and compare it with what is actually happening in society. Furthermore, we will reflect on externalities involved in IoT botnets and if no incentives for the actors are found, discuss whether there is indeed a market failure and which policies should be implemented to fix these market failures.

Besides that, we make an analysis on different factors influencing the variance in the metrics from our previous report and we perform a statistical analysis to evaluate the impact of these factors on the metric.

# Actor mitigation strategies

Quick recap of the issue at hand and the involved actors: we are analysing IoT-botnets capable of carrying out DDoS-attacks. In the other reports, six actors were identified: (1) the owner and (2) manufacturer of IoT devices, (3) the attacker that creates botnets of IoT devices, (4) the malicious user of those botnets, and (5) the victim of the IoT-botnet powered DDoS attacks. Finally, (6) the ISPs of either of the actors listed before.

## ISP

One of the main actors we previously identified is the internet service provider (ISP). An ISP establishes the links both between the attacker and the intermediary, and the intermediary and the victim. Since all traffic involved in botnet related attacks flows through one or more ISPs, ISPs are in an excellent position to either monitor attacks or take active steps against them.

### Countermeasure

For ISPs, the most obvious countermeasure would be to analyse traffic and decide whether it is malicious or benign. This may look like an ideal solution, however ISPs may not have any incentive of choosing this solution since it is going to involve lots of processing power. Moreover, since this solution raises privacy issues, it could be that in many countries this solution is not even permitted due to law and regulations. The easier solution may be one several hosting providers are already implementing: closing vulnerabilities. In this scenario, an

ISP scans each client at regular intervals. During this vulnerability analysis, it can determine if an IP address is vulnerable to botnet related attacks. If, for instance, an IoT device is found vulnerable, the owner is notified and asked to close the vulnerability. If the owner is unable to close the vulnerability or fails to comply, the ISP can choose to proceed to firewall the device so that the vulnerability can no longer be exploited. For IoT devices that are (mis)used this may involve blocking the port on which the device listens. This is an effective way of stopping, for instance, a DDoS attack before it becomes a problem.

## Distribution of costs and benefits

For this particular countermeasure, the cost & benefits distribution is a little more skewed. While it is the ISP that has to pay for the scanning infrastructure, the benefits are mostly reaped by the victims. There is, however, still the benefit of the ISP not taking part in botnet related incidents, which may prevent network congestion or network instability and improve (or not damage) reputation. This may already prove enough compensation for ISPs, since there are already ISPs that perform these checks.

## Presence of an incentive

As mentioned previously, there are at least two ways for an ISP to provide countermeasures against IoT botnets. The first is that of scanning their traffic for botnet fingerprints. For this end, a substantial amount of processing power is required. On the other hand, ISPs that provide this kind of protection to their customers, will have an advantage over other ISPs that do not, whereas if they do not provide this service, ISPs that do will hold an advantage over them. This can have an effect on the choices potential customers make, steering them towards or away from a said ISP. A simpler countermeasure is that of notifying an owner of  a vulnerable device, and blocking them completely if they fail to address the problem. However, the majority of the benefit of this countermeasure is for the target of a botnet related attack. This target does not have to be a customer of the ISP, meaning the ISP does not have the benefit from this directly. However, an ISP can still use this to show awareness of potential problems, which can make them seem more reliable to potential customers. This means there is an indirect incentive for the ISP.

## Externalities

For the second countermeasure, a party affected by externalities was already briefly mentioned. By warning their customers, and eventually blocking them entirely if the vulnerability is not fixed, it becomes more difficult for attackers to use customers (and their IoT devices) of that ISP for enlarging the botnet. This potentially means that there are less botnet related incidents, which is beneficial for potential victims, as the chances of being targeted by a botnet have decreased. Thus, this indirectly also affects a potential victim since it is less likely to be attacked.

# Consumer

The consumer or product-owner is the actor that has physical possession over the IoT-device.

## Countermeasure

Given that the consumer has an IoT-device connected to its local network which in turn is connected to the internet, there's a few countermeasures the consumer could take. For now we evaluate the relatively simple countermeasure of editing the default password. In the data we found that practically all attacks are targeted at default passwords for IoT-devices. Hence, changing the default password as a consumer is an effective mechanism.

## Distribution of costs and benefits

The costs and benefits of changing the default password are minimal for a consumer, given that the consumer can change the password. That is however a non-trivial requirement, since many IoT-devices are plug 'n play, or at least do not require heavy configuration. So if a consumer is unable to change the default password, either due to a lack of skill or simply because the manufacturer does not enable that feature, this countermeasure is not applicable by the consumer. That would be a problem in itself.

Now, assuming the consumer is able to change the default password, the only real cost is time investment to change the default password, which in turn should be minimal. The benefits are simple, the likelihood of the IoT-device getting compromised by attacks as seen in the data becomes zero.

## Presence of an incentive

The benefits of changing the password seem good for a consumer, since compromise is effectively mitigated. However, a consumer will only act on this countermeasure if he/she has a reason, incentive, to do so. And that's why many devices have the default password: a consumer has no real incentive to mitigate IoT-device compromise. If a consumer's device gets compromised, it might be used to attack third parties, but rarely the consumer itself. There is a small chance of course the IoT-device will be used to steal data from the consumer, but since this is a relatively rare occasion, there is no real incentive for the consumer to mitigate device compromisation.

## Externalities

In previous reports we described that IoT-botnets may cause network-problems for ISPs. Therefore, if consumers mitigate device compromisation, they have a positive externality on ISPs. Namely, a decrease in IoT-botnet size. On one consumer, this effect is of course very small for the ISP.

This decrease in botnet-size has a cascading effect, leading to another positive externality. Smaller botnets means smaller/less botnet-attacks. So this is a positive externality to botnet-victims as well.

Editing the default password on an IoT-device has the obvious negative externality for the attacker-role. Attackers will no longer be able to trivially compromise the device and thus use it for their (malicious) intentions.

## Manufacturer

The manufacturer is the actor that produces IoT-devices and their software.

### Countermeasure

As described in the section regarding the consumer, most attacks are targeted at default passwords. Therefore, an effective countermeasure would be to programmatically enforce changing the default password to something more secure (non-generic) on the devices the manufacturer sells. This way, their consumers will not have default passwords that are easily targeted by distributed attacks.

### Distribution of costs and benefits

The obvious cost of implementing this countermeasure is the manhours required to implement it. The software of the device needs to be updated in such a way that configuring the device now also requires to set its authentication credentials. These costs may vary immensely between manufacturers, depending on whether there is already a configuration setup in place and if so, how it was designed.

Next to that, there might be indirect costs. If customers do not want this enforced countermeasure and aware of it being in place, they might decide to buy a device from a different manufacturer, which in turn would reduce the revenue of the manufacturer.

However, consumers might not like the enforced countermeasure, they might like the increased security. The manufacturer could use this countermeasure in their marketing to show their device is more secure than competitors. This might in turn let consumers decide to buy their device which will increase revenue.

### Presence of an incentive

From a business point of view, the manufacturer will only implement this countermeasure if it will increase revenue/profits. Since consumers have no real incentive to regard security of their IoT-devices, it is hard to tell whether they will let the security outweigh the cumber of having to set the password. Therefore, it is hard to analyse for a manufacturer whether more or less consumers will buy their devices when the countermeasure is implemented. However, since there are also direct costs involved of implementing the countermeasure, it will likely not be profitable for manufacturers to implement this countermeasure. I.e. there is no financial incentive, thus no incentive, for a manufacturer to improve security of their devices.

### Externalities

The externalities for manufacturers are an expansion of those of the consumer. The same positive externality for ISPs applies, the positive externality for victims and the negative externality for attacker. All externalities are however much larger in effect. If a manufacturer enforces password configuration, all their future devices are mitigating compromisation. Their countermeasure therefore affects a large pool of devices whereas a consumer only affects one device at a time.

A consumer has two more externalities however, namely a positive and negative one for consumers. The positive one being that consumers now are better protected against device compromisation which in turn protects their data which theoretically could be targeted by an attacker (however unlikely). The negative externality is that the consumer now has to invest more time into configuring the IoT-device.

# Analysis of metric performance factors

In this section, the defined security metrics and their general analysis will be revisited and expanded to gain more understanding in the variance of metric performance. More specifically, the performance of one actor which in most cases is the unit of analysis in the metrics will be looked into. For readers which did not read the last two reports, a quick recap of the chosen metrics and the actors they focus on is provided first.

The following six metrics[1] were chosen:

- 1. Malicious devices per ISP over time[2].
  - a. Measured by total number of requests.
  - b. Measured by total number of unique attackers.
- 2. Malicious devices per country over time.
  - a. Measured by total number of requests.
  - b. Measured by total number of unique attackers.
- 3. Attack strategy distribution of the malicious devices per ISP[2].
  - a. Measured by attacker-victim ratio: Attack depth compared to the breadth.
  - b. Attack sophistication: connect → login → execute malware

### Identification of unit of analysis of the metrics

These metrics were chosen as they had to measurable using the provided IoT honeypot dataset and also be of value to the most important actors. The dataset did not contain information about victims or manufacturers, but mostly showed information about the attackers and their strategy. Next to that, the time information is very important for most actors to be

[1] The last report stated that five metrics were identified but it actually split the last metric in two parts. As this is essentially equivalent to having six metrics, the listing has been updated to reflect that.

[2] Due to the difficulty of mapping IP-addresses to ISPs (without having large financial resources), these metrics are only calculated for the top-10000 devices measured by the total number of requests in a two-month period.

able to compare attack volume and strategy over time with other data sources (like lists of active botnets) and to extrapolate the data for prevention.

To combine this with our problem owner: the ISPs, the unit of analysis chosen to be mostly this actor. On the other hand, metric 2 is focussed on the country of attackers. This is not an actor we are directly focussing on, but can also be seen as a less fine grained precision which is still of use to ISPs in that country. All in all, the actor, or unit of analysis in metric 1 and 3 is the ISP and in metric 2 this is the country.

## Identification of metric performance factors

As could be seen in the last report, the performance of different ISPs and countries in the defined metrics differed greatly. As these are cybersecurity metrics, it would be preferable if only the cyber resilience of these actors had an impact on the metric performance. We will now try to identify the aspects of cyber resilience of these actors that might influence their metric performance using a small set of ISPs and countries as an example. Next to this, suspected factors less related to cyber resilience will also be identified and taken into account. For every factor, it is indicated which metrics it is likely to affect.

### The average upload speed of the customers of an ISP

This factor has to do with the the total volume of traffic that the malicious users of an ISP can generate. More specifically, the more upload bandwidth the average user has, the more malicious requests it can do to our honeypot. Therefore, it is likely to directly affect metric 1a.

### The number of customers of an ISP

With an equal chance of any customer being malicious, when an ISP has more customers, it is likely that it also hosts more malicious customers. Thus, this factor will probably affect affect metric 1b.

### The distance of the ISP-country to the honeypot

This factor does not seem interesting at first sight, because the internet is not bound to country borders at all. Still, because of the speed of light, attacking victims on the other side of the planet does come with a several-hundred-millisecond round-trip-time penalty. When an attack is performed sequentially, this severely limits the amount of login tries an attacker can perform per second. Therefore, a victim which is geographically close might be more interesting to attackers. Next to that, bots in botnets often attack devices in the same (nationwide) network first, so that might also result in more geographically close attacks. This factor influences metrics 1a, 1b, 2a and 2b.

### Botnet activity over time compared attack volume / unique attackers

When botnets are more active on a global scale at a certain day, it is also more likely that one of those botnets attacks our honeypot. Thus both the total attack volume: metrics 1a & 2a and the number of unique attackers: metrics 1b and 2b could be affected. This factor however does not directly explain any metric performance for our units of analysis (ISPs & countries), but it does explain fluctuations in the total attack volume / # of unique attackers over time.

### Percentage of IPs of ISPs which are part of a botnet compared to attack volume / unique attackers

As the evaluation of metrics 3a and 3b have shown in the last report, the attacks on the honeypot are not really sophisticated. This indicated that most of the attacks are not targeted, but part of simple botnet behaviour: automatically trying to spread to different machines. Therefore, the percentage of ISP users which are part of a botnet will highly influence both the total attack volume: metrics 1a & 2a and the number of unique attackers: metrics 1b and 2b.

### Attack volume/unique IPs per time of the day compared to the timezone of the ISP

As most malicious machines will probably be turned on most during the day, the time of day in the timezone of the ISP (per timezone) will probably influence the volume and amount of attacks on the honeypot. The metrics itself however are not aggregated at minute or hour level, but at day level. Therefore, this factor does not really influence any of the metrics.

**Note**:
For metric 2, we can test all factors above on a country scale instead of ISP scale.

### Attacker behavior prediction

As bots do not quickly change their spreading/attacking behaviour, those attackers might be detectable in later in the dataset based on the data of the first few days. This could explain the attacker behavior per ISP over time and therefore influence metrics 3a and 3b.

### Strategy and/or sophistication of the attacks of certain botnets compared to the dataset

It might be possible to detect the behavior of certain botnets by the attacks in the dataset. This would show what botnets are (mostly) responsible for the attacks and therefore also explain the difference in attacker strategy and/or sophistication: metrics 3a and 3b.

## Impact of metric performance factors

The last subsection defined a number of factors that might influence metric performance. Based on the estimated impact of these factors and whether data gathering is feasible given the limited amount of information and time, two of these factors are picked for further analysis:

- The average upload speed of the customers of an ISP.
- The distance of the ISP-country to the honeypot

For these factors, data will be gathered to try to prove whether there is some impact on the metric performance and whether this impact is significant. Thus whether there is a significant (negative) correlation between the metric performance and the factor itself.

## Data gathering

For the first factor, the reports of Speedtest.net[3] and Testmy.net[4] are used which clearly list the average upload speed per ISP of a large number of ISPs. This can be combined with the results from metric 1a to find out whether any (significant) correlation exists. When every ISP was removed which was not in either of the sets, 55 ISPs were left. This is a lot less than the 1272 ISPs which were in the result set of metric 1a. However, as the ISPs which are left seem to be equally distributed around the globe, the result of the analysis is still deemed to be valuable.

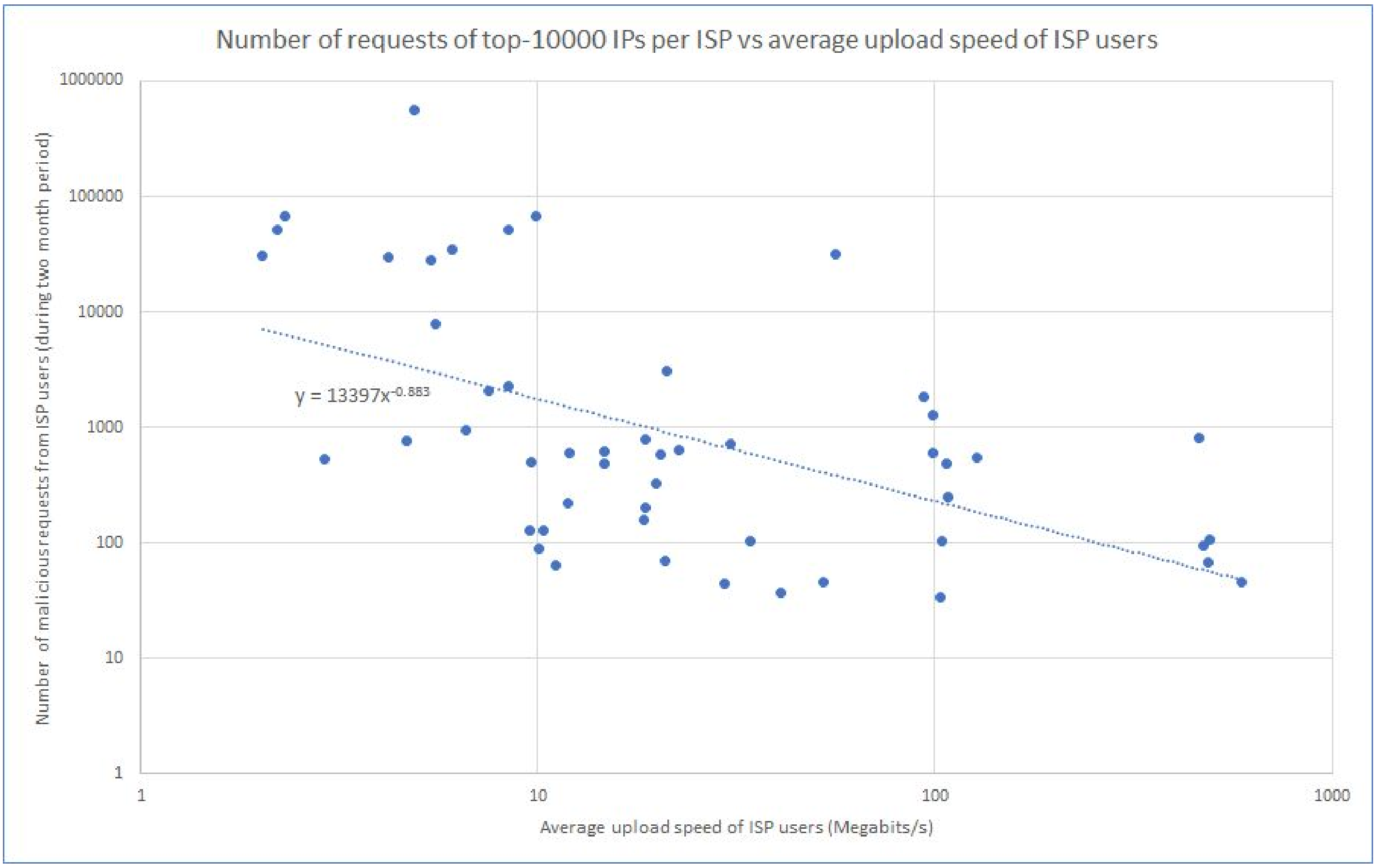
For the second factor, data is gathered using the WonderNetwork Ping statistics[5] to Tokyo which is the estimated location of the honeypot. This is combined with the results of metric 2a to find out whether any (significant) correlation exists. When every country was removed which was not in either of the sets, 67 countries were left. This factor is calculated for both the geographical distance as the ping time, as both of these factors could be of importance, but we cannot say in advance which one (or both).

For both factors, the Pearson correlation has also been calculated to test whether there indeed is a significant correlation. This function returns a value between -1 and 1. The absolute value indicates the extent to which the variables are correlated.

## Statistical analysis

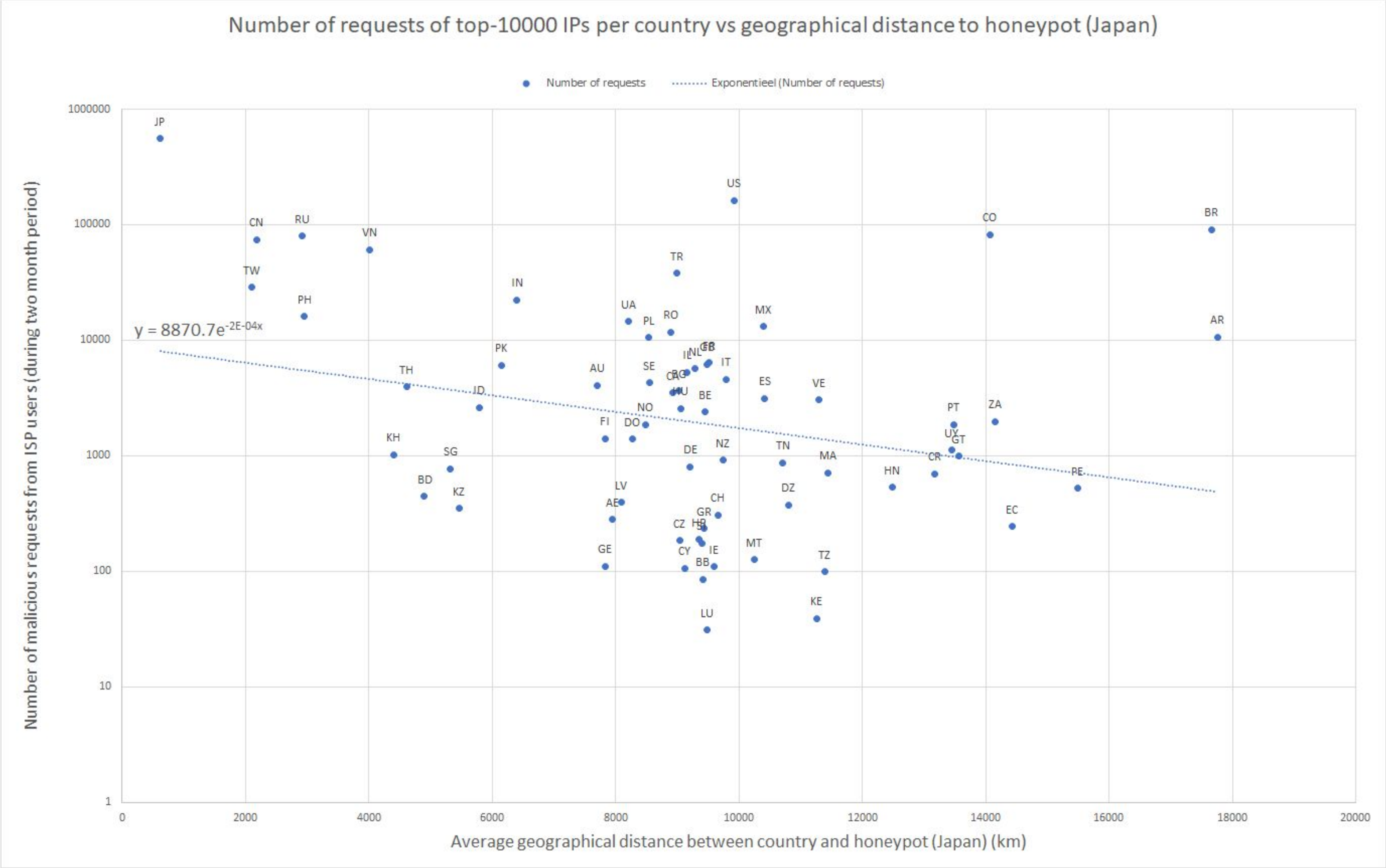
**First factor:** The average upload speed of ISP users is compared to the number of malicious requests from that ISP in a two month period (size of the honeypot dataset) to see whether they are related. As you can see in the figure below, these two variables indeed seem to be linearly related when plotted on a logarithmic scale:

- Pearson correlation = -0.118



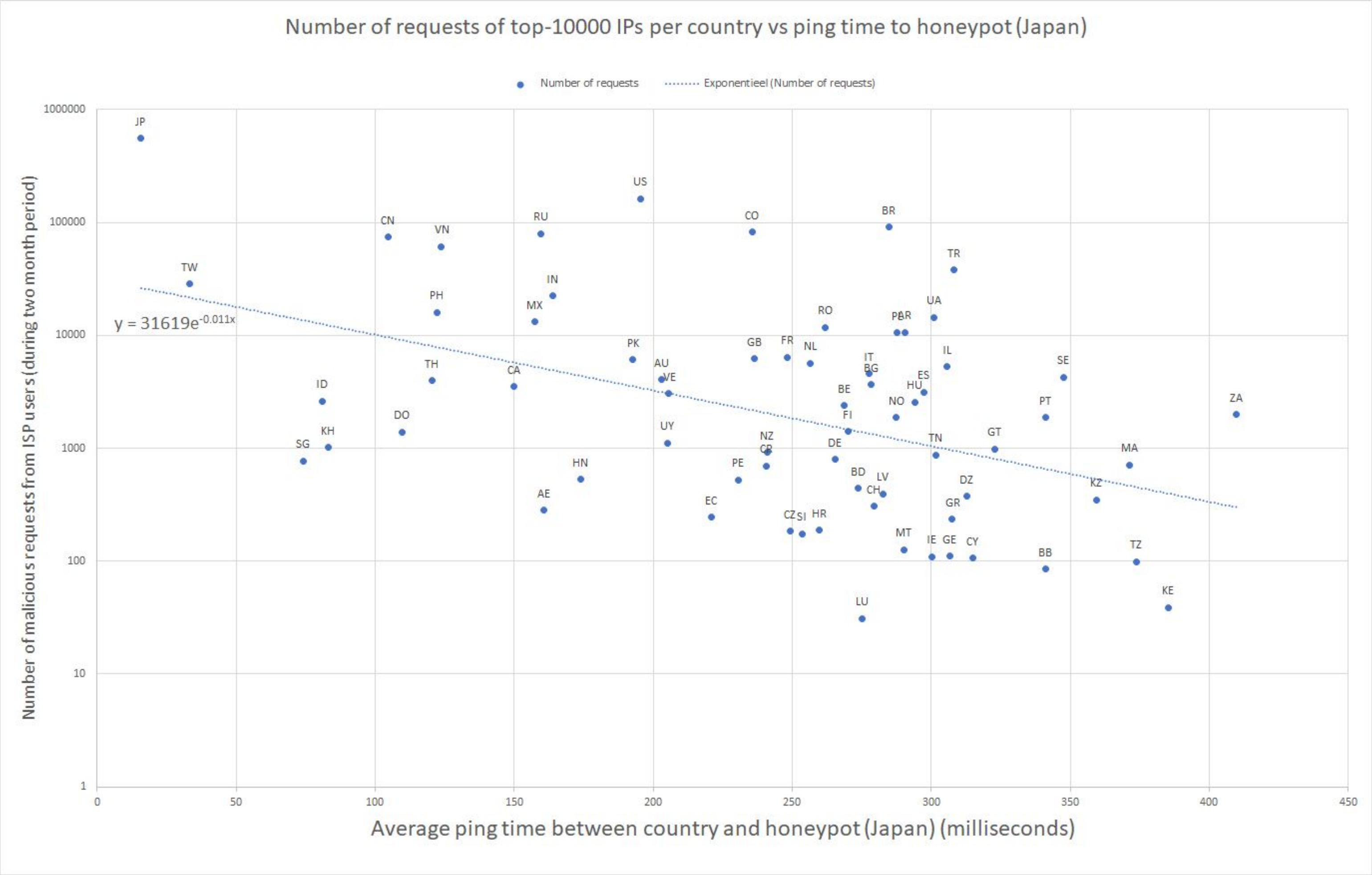
**Second factor - distance aspect:** The number of requests of top-10000 IPs per country is compared to geographical distance to honeypot (Japan) to see whether they are related. As you can see in the figure below, these two variables indeed seem to be linearly related when plotted on a logarithmic scale

- Pearson correlation = -0.308



**Second factor - ping time aspect:** The number of requests of top-10000 IPs per country is compared to the ping time to honeypot (Japan) to see whether they are related. As you can see in the figure below, these two variables indeed seem to be linearly related when plotted on a logarithmic scale.

- Pearson correlation = -0.389



## Conclusions and discussion

As you can see the first factor indeed shows a weak negative correlation with the results of metric 1a, but as the number of data points is relatively low (55) for this type of test, this value cannot be said to be significant with certainty. When more ISPs would have been taken into account (about 500), with the same correlation value, we would be more certain that the correlation is significant. In that case, it shows when this factor is not taken into account, the metric performance per ISP/country does not accurately show the performance, but is skewed. This can be solved by dividing the ISP/country performance of a certain metric by this factor.

For example: the results of metric 1a could be that users of the made up ISP 'SpeedAndPower' perform 10% more requests to the honeypot that that of the average ISP. This could indicate a problem, but when the average user of this ISP has a 15% higher upload speed than the average user of the average ISP, we are a lot less certain there is a problem at all.

Thus, we could update metric 1a to be something along the lines of: “Malicious traffic volume per ISP over time divided by the average upload speed per ISP”.

For the second factor, the negative correlation is more strong (-0.3 compared to -0.1) for both the ping and distance measure, but due to the limited amount of data points, this value still can not be said to be significant with certainty. If it would have been significant, like in the adaptation of metric 1a above, metric 2a could be adapted to be something like: “Malicious traffic volume per country over time divided by the average distance/ping time from this country to the honeypot”.