UNIVERSITEIT OF TWENTE

ECONOMICS OF SECURITY COURSE
AY 2018/2019

Internet of Things: Mirai

ASSIGNMENT 3

Authors:
Anna Prudnikova
Giovanni Maria Riva
Federico Casano
Sridhar Bangalore Venugopal

Contents

1 Introduction

During previous assignments there were identified and calculated:

- the security issue related to the given dataset;
- the problem owner and other possible actors, involved in security issue;
- what are the existing security measures and how they compare with our metrics;
- the different performances of different problem owners based on one chosen metric;
- the return on security investment for one particular issue owner;

The dataset underlines a huge security issue: the infection of IoT devices worldwide by the Mirai malware. Mirai infects IoT devices and turns them into remotely controlled bots. Each bot then autonomously scans for other potential victims, attempting to log-in via several bruteforcing techniques. The infected machines, all together, can perform different critical types of attacks such as DDoS attacks, spam or phishing campaigns.

At the same time, the botnet can also cause a number of issues not directly related to security concerns, such as losses in computational powers of systems, waste of power, latency and bandwidth issues. Therefore, the Mirai botnet problem, raised by dataset, could affect different actors such as companies, users, Governments and internet service providers (ISPs). For our particular dataset we identified the problem owner as Internet Service Providers, as the one, that is most affected by threats of botnets.

2 Study of the three actors facing the security issue

2.1 Concrete suggested countermeasures

For this assignment we are going to focus on 3 actors, that are the most involved in the analyzed problem:

1. **ISPs**, identified as problem owners;
2. **Governments**, that could influence the security issue, using their legal / authority power;
3. **Users**, that are IoT devices owners.

Each of them could implement different countermeasures to mitigate the threat which are listed in Table 1 below.

Actor	Countermeasure
ISP	Notifying users about identified infections
Government	Policy enforcement towards ISPs to fight against botnet threat
User	Change of default passwords and-or update firmware on a regular basis

Table 1: The identified main actors and the suggested countermeasures for the relative issue addressed

ISPs are capable to analyze logs from their network infrastructure and estimate suspicious malware activity, for example, via multiple log-in attempts through known targeted ports by Mirai.

Thus, using the log data collected, one way of notifying users about infections is to create a call center to warn customers about infections and avoid further damage (e.g. Mirai is non-persistent malware, which means it will be deleted from the device once the it is rebooted) [1].

Even though it is common to think that internet providers are main actors in fighting against bots, it is not completely true. The problem stands, that there exists the lack of legality and legitimacy. As an example, European Union regulations do not enforce internet service providers to detect infected devices within their networks and implement measures to isolate them from that network. This legal void brings forward an issue, that all anti-botnet actions are mostly performed on a voluntary basis and further creates a debate on the legitimacy and eventual legality of these measures. By so far, it is not clear, whether actors involved in security issue (including society) are ready to cooperate with ISPs to fight the botnets together. Most of the measures, that could be implemented by ISPs, such as traffic inspection (deep packet inspection) might be considered illegal, since they violate the privacy of people. [9]

To break this legal void, currently there exist a number of initiatives, so-called Anti-Botnet Initiatives, that are started by internet industries with a goal of helping citizens against botnets with the support of Governments. Such initiatives, for example, exist in Germany, The Netherlands, Finland, USA. Those initiatives have a positive effect on a botnet security issue (as was shown also in a previous assignment with our dataset), but while they are not applied in EU law, they cannot be entirely effective.

The main weakness of IoT devices, that allowed to hack those devices in the first place, was the usage of default passwords on those devices. That is why, it is crucial for users to change those passwords and update the firmware, as soon as they buy a new device. Normally, it is a simple task to perform and could be done with the help of provided together with the device manual.

Another measure, that ISPs could also implement, is information sharing. This measure doesn't require any costs, but at the same time can bring benefits for all actors involved in security issue. As was shown by Van Eeten in his studies of botnets infections [14] in Dutch ISPs, when all the ISPs received information about statistics on infection rates, they were able to fight botnets more efficiently. Information disclosure helps in remedying information asymmetries.

2.2 Distribution of costs and benefits for suggested countermeasures among the different actors

Quantitative costs and benefits (e.g. financial) can calculated directly but qualitative ones (e.g reputation) cannot. For our assignment we are going to focus on non-financial costs that are quantitatively computable.

ISPs We are going to start with ISPs. Costs of implementing the suggested countermeasures might include:

- hiring third parties to analyze the security level of ISP in order to understand if extra measures are needed, which tools to implement etc;
- time spent on organising call-centers and hiring staff to support call-center and notify users;
- extra work for engineers to perform log management or hiring extra engineers.

As was mentioned in previous report, there are mostly no direct benefits for ISPs to implement security measures, we can only estimate the prevented losses, that include:

- loss of existing clients' trust, that force them to change service provider (when customers are satisfied with quality of service of ISP they tend not to change providers);
- loss of reputation, that leads to less numbers of new clients (better reputation lead to more new clients);
- possible legal issues in case of SLA breaches or major incidents for companies, affected by bots.

Governments For Governments costs may include:

- time spent on developing and implementing policies;
- human resources to develop, implement policies and to regular check if the policies are actually implemented.

Benefits for Governments might include:

- people's content about their security and privacy.
- better standing among other countries (e.g. among EU countries).

Users In most cases there are no costs involved, assuming they have sufficient knowledge to change passwords and update / patch the firmware of devices. It is relatively easy to change password and doesn't take much extra time. On the other hand, users with little to no technical knowledge will face some costs due to external assistance to fix the problem.
At the same time benefits for user are many:

- no extra spending on energy and bandwidth consumption;
- less probability of their credentials to be stolen;
- no productivity loss of a device;
- no need to buy / repair / clean from a malware the IoT device, when it got infected.

2.3 Incentives for the actors

Governments. In this report we will focus on countries inside the European Union.

In 2013 the European Commission adopted the EU Cybersecurity Strategy aiming to protect Europeans online, increase the security of networks and improve the information security. EU invested more than 600M EUR for a six years project of research and innovation in cybersecurity finishing in 2020. The Commission has further strengthened its approach in the past years by including cybersecurity at the heart of its political priorities: trust and security are at the core of the Digital Single Market Strategy presented in May 2015, while the fight against cybercrime is one of the three pillars of the European Agenda on Security adopted in April 2015. Lastly in 2016, after three years of negotiations, the European Parliament marked the birth of the Directive on security of network and information systems (NIS Directive) to obtain a more secure online environment: including protection against Botnets. [4]

"But how the individual countries are reacting to these sets of regulations?". With regard to the NIS directive the majority of EU member states missed the deadline to transpose the EU directive into national law. The directive was approved by the representatives of the EU's 28 national governments but the same countries that accepted it before seem refuse it now. According to the directive, member states need to identify, before 9 November 2018, the operators of essential services (water, energy, transport, health and banking operations) do everything in their power to manage the risks of being hacked and report to the authorities if there is a cybersecurity breach.

As stated in a commission-run website, last updated on 19 September, the following countries are still in progress or have partially transposed the directive into national law: Latvia, Lithuania, Poland, Belgium, Austria, Hungary, Romania, Bulgaria, Greece, Ireland, France and The Netherlands (12 countries out of 28).

We can clearly affirm that almost half Europe is still working on implementing the NIS Directive. "Does it mean that those countries don't have incentives to apply the regulations?". Let us examine the step of the application of a Directive and the consequences for a country if it does not satisfy it.

The directives are European documents proposed by the Commission and endorsed by the EU Council and the Parliament. They do not produce direct effects on individuals, but instead produce an obligation for member states to adopt a national law, that contains the provisions of the directive. It is used instead of the regulation (which is directly applicable and effective even on private individuals, does not require state application), because the states can achieve the goals and apply the directive with a certain discretion, resorting to national regulatory and administrative instruments more suitable. What matters is the purpose and certain minimum standards that must be common to all states. If a member state does not apply the directive with its own national regulatory act, this directive produces direct effects on individuals if "self executing" with repercussions on the state itself. Furthermore, the Commission can open an infringement procedure against that state and sanction it economically. The infringement procedure consists of a first letter of delay, that urges the state to apply the directive, if it is not done, the state can be sanctioned . [8]

On 19 July, the commission announced, that it has sent warning letters, with two months to respond, to 17 EU member states, telling them to fully transpose the cybersecurity directive. [3]

In conclusion, we can infer that countries inside the European Union have economic and reputational incentives to fulfill cyber security requirements leading to a more cyber-secure ecosystem.

ISPs By allowing the growth of botnets inside their network ISPs will be seen as unreliable, which will significantly damage their reputation. The growth of botnet infection within ISPs lead to extra bandwidth consumptions, network productivity losses, possible SLA breaches and, in general, lost of customers trust. In their empirical study on spam and botnets, Van Eeten et al. (2010, p. 46) claim "because around 80-90% of all spam is issued by botnets, the origin of a spam message is very likely to indicate the presence of an infected machine". Thus, neglecting the infected computers in their own internal structure, ISPs not only do not eradicate the problem but rather allow it to grow. Ultimately, users of a particular ISP will start receiving constant and regular spam which undermines the professional reputation and reliability of an ISP (Spamhaus, 2014). [10]

To summarize, the incentive for ISPs to implement the countermeasure is to preserve their reputation to be able to keep customers satisfied and attract new clients.

Users End users, owners of IoT devices, have economic incentives and usability reasons to keep them secure and not under control of the botnet. To demonstrate that, we will focus on a report published by the University of California, Berkeley.

An infamous use of Mirai is depicted in the DDoS attack on 20 September 2016 on the Krebs on Security site which reached 620 Gbit/s. The Berkeley School of Information has calculated that, with the extra energy consumption and bandwidth costs, the botnet used in that attack would have cost device owners $323,973.75, or $13.50 for each device. The researchers of the University report that in tests on infected devices, they observed increases in electricity consumption, and "significant increases in bandwidth usage in infected devices when compared with non-infected devices operating normally".

They also found that "infected devices cause a degraded user experience for the device owner, as devices that are involved in attacks can interfere with the owner's use of both the device and the network to which it is connected". [2]

Furthermore in a worst-case scenario, with the Mirai botnet operating at peak power in a UDP DDoS attack, "The projected cost to consumers of this attack would be $68,146,558.13. Increased energy consumption accounts for just $855.00 of that total cost, with the rest accumulated from increased bandwidth consumption. The per-device cost to the consumer for this hypothetical worst-case scenario is $113.58."

2.4 The role of externalities

This part focus on both positive and negative externalities externalities generated from our countermeasures and incentives.

2.4.1 Negative externalities

Governments Incentives for policy enforcement are strong, However, negative externalities will affect citizens in higher taxes [6] and and also privacy.

ISP Among the many incentives motivating ISPs to intervene on the security issue, liability for violations is the most important one but the weakest. For this reason every company is exempted to effectively take action against customers' infections creating a negative impact on them. [11]

Users According to J.A.Chandler: «"Users do not face the full costs of their lack of computer security. This is particularly the case now that bot software is being designed to be minimally disruptive to the computer owner, so that bots may avoid detection and removal. Accordingly, average users fail to invest in security"». [7]

2.4.2 Positive externalities

Governments Governments are enforcing manufacturers to follow standards for security. However, customers still base their buying decisions on a price criteria rather than company's compliance. Governments need to raise awareness of customers in buying products compliant with secure standards of manufacturing.

Privacy of people has become vital, Governments are aiming to improve this right by imposing strong security policies and botnet sanitization provisions to providers to overcome the consequences that caused by the infections.

ISP ISPs investing in cyber security is not as effective as for their customers from an economic perspective. This market failure is a deterrent for service providers' incentive to invest. [12]

Users Unprotected IoT devices are the main cause for major cybersecurity attacks. However, adopting updating systems could still lead to negligible data breach for user. The interdependent security could be effective only, if there is high commitment of user's intervention. At the same time, updating process consumes more time and requires constant engagement from users.

3 Statistical analysis

3.1 First statistical analysis

First, we are going to focus on the metric, that shows overall (normalized) number of infected IP addresses within an ISP over 6 months.
The factors, that cause variances in this metric are as followed:

- attacker behaviour, this is an unpredictable factor, attacker can choose some random time to infect the devices and abandon the botnet after that;
- governmental policies enforcement (ex ante). In some countries the overall infections and variations in number of infected devices is much less, due to the fact, that those countries have policies and initiatives in place, that force and motivate them to implement security measures against bots;
- information asymmetries (e.g. lack of security awareness), no information sharing between companies. According to the content of video lecture, people buy IoT devices not caring about security, so they just tend to buy cheapest devices, not caring how secure they are;
- collaboration between ISPs. As with the example of governmental policies;
- producers of IoT devices, that don't care about security and just care about producing the cheap devices and selling more of them;
- implementation of security tools to mitigate the threat of botnets;
- the size of ISP.

Since we have data about the size of ISP, we can perform a statistical analysis to understand, if the normalized number of infected IP addresses is bigger for smaller ISPs. This is going to prove the theory presented in [13]. The first theory, based on absolute figures, is that for the bigger ISPs, the number of infected systems is also bigger. Most of the infected systems are located in major ISPs. But this theory is misleading. Relative figures show, that **larger ISPs in general have fewer infections per customer**. It could be explained by the fact, that larger ISPs have automated processes for identifying, notifying, and mitigating infected customers, which makes botnet mitigation more efficient on a larger scale.

Moreover, Van Eten et al. confirms the hypothesis by stating how larger, well-established ISP companies are easier to enforce legally to intervene on the issue. Small organizations, indeed, are effective only when collaborating, but this is difficult as they are short-lived and challenging to survey. [15].

3.1.1 Linear Regression Analysis

We further investigated the possible relation between the number of infections and size for each ISP as also suggested by [13] and [15] applying a a simple linear regression to our dataset.

The statistical test was performed in Excel (Appendix 1) and building our modeling as follow:

- We considered as *independent variable* X, the **size of the ISP** being unrelated among each organization;
- The *dependent variable* Y consists of the **number of infected ip addresses** for each ISP. It will determine the strength of the computed predictors (e.g. estimate the relationships between two variables);

The output of performed the linear regression contains statistical tables and visual plots of the calculation.

Table 2 shows the R Square which is the Coefficient of Determination, indicating how many points fall on the regression line.

Regression Statistics	
Multiple R	0.66803241
R Square	0.4462673
Adjusted R Square	0.44618808
Standard Error	545.101539
Observations	6992

Table 2: Output of the regression statistics computed for the chosen dataset

For our experiment, we took in consideration the R-square value 0.44 which means that 44% of our values fit to regression analysis.

The second part of the output shows Analysis of Variance (ANOVA) data as shown in Table 3.

ANOVA					
	df	SS	MS	F	Significance F
Regression	1	1673889904	1673889904	5633.41925	0
Residual	6990	2076978459	297135.688		
Total	6991	3750868363			

Table 3: ANOVA data

We obtained a *Significance F* less than 0.05 (5%) while the F value is equal to 5633 corresponding to a statistical significance of the regression.

Table 4 reports the coefficients data.

	Coefficients	Standard Error	t Stat	P-value	Lower 95%	Upper 95%
Intercept	41.776736	6.520939	6.406551	$1.58513E-10$	28.9937	54.55975
X Variable	$9.72104E-07$	$1.29517E-08$	75.05610	0	$9.4671E-07$	$9.97493E-07$

Table 4: Coefficients data

The computed coefficient *Y-Intercept* is 41.7 and the slope, which is identified as the X variable, is 9.72. The difference is 31.98. However, P value is 0 which is statistically significant (p<0.5).

Figure 1 contains information about the regression line calculated from the data which includes coefficient, standard error, t-stat, and probability values for the intercept. This graph shows the size of the ISP and the relative predicted number of infected IPs.

There is a high variability towards small sized ISP, while the trend decreases when the ISP reaches higher network dimension. This supports the theory, presented earlier, that smaller ISPs tend to have more infected devices within their networks.

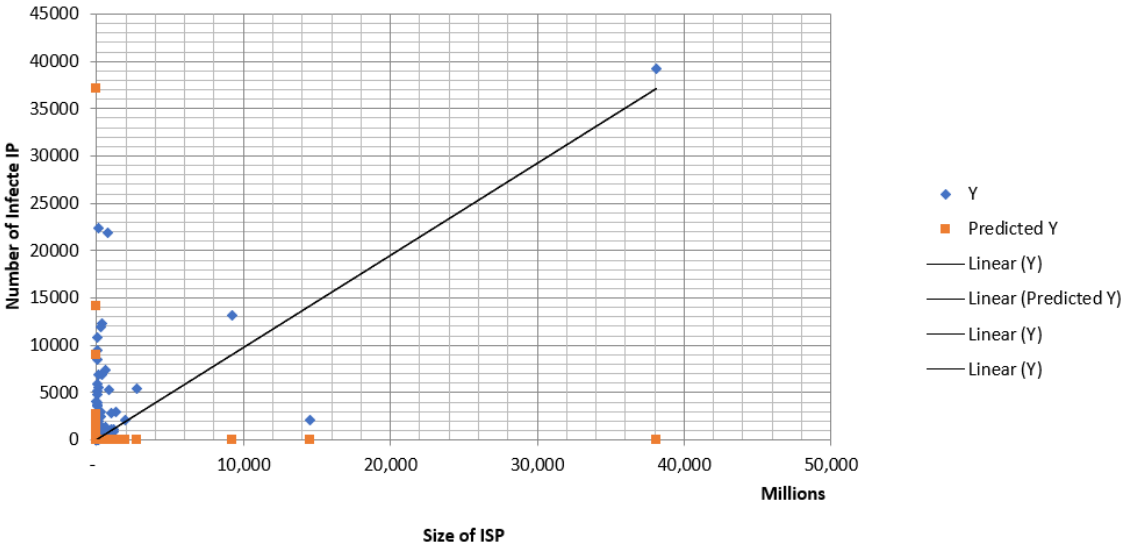


Figure 1: Distribution of infected IoT devices per country over days

3.2 Second statistical analysis

For the second case of statistical analysis, we are going to focus on another actor and another metric. The new chosen actor is Government, the metric is distribution of infections per days within country. The factors, that influence this metric are as followed:

- the level of ICT development of the country;;
- the existence of enforced policies to fight botnets;
- the involvement of ISPs in the process of fighting the botnets;
- overall level of country development (e.g. users in poorer countries tend to buy cheaper devices, that are more likely to be infected).

We are going to focus on the first factor - level of ICT development of the country. To analyze it, we are going to use the ICT development index of each country (IDI) [5]

Our goal is to understand, if there is a correlation between the level of ICT development in the country and the rates of infections in this country. For that, we are going to split all countries, presented in our dataset (in chosen sample there are total of 65 countries) in 2 categories: countries with high level of ICT development (IDI $>$ 7.0, 33 countries: Iceland, Korea, Swizerland, UK, Netherlands, Norway, Germany, USA, Italy etc) and countries with low level of ICT development (IDI $<$ 7.0, 32 countries: Hungary, Poland, Bulgaria, Argentina, Serbia, Chile etc). To further analyze the correlation we are going to use Pearson's chi squared test of independence.

We are going to test 2 hypotheses:

- Ho: the rates of infections do not depend on ICT development level in the country.
- H1: the rates of infections depend on ICT development level in the country.

In the table below there is presented data of the overall number of IP addresses infected in particular dates (chosen based on Mirai Timeline, presented in previous report), divided by 2 categories: countries with IDI higher than 7 and countries with IDI lower than 7.

	The number of infected devices in the dates of major infections according to Mirai Timeline							
	07.08.16	25.08.16	04.10.16	30.10.16	07.11.16	27.11.16 6	21.12.16	08.01.16
Countries with IDI higher than 7	365	375	666	890	1139	1469	979	770
Countries with IDI lower than 7	1866	1444	2341	4061	5867	4050	3775	2799

Table 5: The rates of infections in particular dates for 2 categories

We calculated value of χ^2 and were able to reject the H0 hypothesis by applying the formula of Pearson (presented in the slides).

The excel calculations could be found in Appendix 2. We calculated value of $\chi^2 = 255.5$ and df = 7. Then using the table for Pearson's square we obtained the χ^2 for (2, 0.05) = 14.07. As we can see, our result is bigger than the result from the table, that means that we reject the H0 hypothesis, in other words rates of infections within a country depend on the level of ICT development in this country. As we can see from our data, in countries with higher ICT development level, the infections rates are much less. It could be explained by the fact, that those countries are more likely to implement security measures, including measures to fight botnets, meaning less incentives for attackers to infect devices, located there.

4 Conclusion

During the assignment we identified three actors, involved in a security issues of Mirai botnet infections, such as ISPs, Governments and end users. For each actor we identified the one possible countermeasure, they could implement, and performed the cost-benefit quantitative analysis accordingly. For ISP the analyzed countermeasure was notifying the users about infections (be means of creating a call center), for Government it is policy enforcement and for users - changing the default passwords and patching / updating firmware of IoT devices.

Later on for those actors, we identified the possible incentives to take described countermeasures. For ISP the main incentive is to preserve their reputation, for Governments is to keep citizens content and make them feel secure, for users is to avoid direct costs involved, when their device is being compromised.

As a next step we identified the possible possible externalities for all actors.

Finally, we chose 2 actors and 2 metrics and for each of combination actor / metric we identified the factors, that could influence this metric. To analyze the influence of those factors, we performed statistical analysis by applying 2 different techniques.

For the first analysis, we focused on ISPs and the metric we introduced in previous assignment, focusing on the overall number of infected IP addresses within an ISP over 6 months. We chose to apply a linear regression statistical analysis to demonstrate the relation between the number of infected IPs considering the size of the ISP. Supported by the suggestions of previous works in [15] and in [13], we also found out a higher variability of infections for smaller companies where bigger ones tend to stick to the predicted trend. In other words bigger and well-established companies are more active in dealing with the issue while smaller ones, alone, tends not to be as effective performing worse.

For the second analysis, we focused on another actor, Government, and introduced the new possible metric - the distribution of infected devices per days in different countries. For this metric we identified a number of factors, that could cause variances and for a further analysis we decided to focus on the level of ICT development of a country. The result of analysis showed us, that the level of ICT development in a country and the rates of infections in those countries are strongly depended.

We came to a conclusion, that for countries with higher ICT development level, the infections rates are much less, than in countries with lower ICT development level.

References

[1] *How ISPs Could Combat Botnets*, 2010 (accessed September 18, 2018). https://www.technologyreview.com/s/418806/how-isps-could-combat-botnets/.

[2] *Botnet attack on one website costs IoT device owners $300k*, 2018 (accessed October 11, 2018). https://internetofbusiness.com/mirai-ddos-attack-on-security-news-website-costs-iot-owners-over-300000/.

[3] *EU countries miss cybersecurity deadline*, 2018 (accessed October 11, 2018). https://euobserver.com/digital/142493.

[4] *EU cybersecurity initiatives, working towards a more secure online environment*, 2018 (accessed October 11, 2018). http://ec.europa.eu/information_society/newsroom/image/document/2017-3/factsheet_cybersecurity_update_january_2017_41543.pdf.

[5] *Measuring the Information Society Report 2017*, 2018 (accessed October 11, 2018). https://www.itu.int/en/ITU-D/Statistics/Documents/publications/misr2017/MISR2017_Volume1.pdf.

[6] *Tax on Negative Externality*, 2018 (accessed October 11, 2018). https://www.economicshelp.org/micro-economic-essays/marketfailure/tax-negative-externality/.

[7] Jennifer A Chandler. Liability for botnet attacks. *Canadian Journal of Law and Technology*, 5(1), 2006.

[8] Paul Craig and Gráinne De Búrca. *EU law: text, cases, and materials*. Oxford University Press, 2011.

[9] Karine K e Silva. How industry can help us fight against botnets: notes on regulating private-sector intervention. *International Review of Law, Computers & Technology*, 31(1):105–130, 2017.

[10] Tobias Kickinger and Bruce Ramsay. Botnet detection and mitigation in isp environments. 2015.

[11] Shinya Kinukawa. Should isps be liable for negative externalities of botnets?, 2012.

[12] Henk Kox and Bas Straathof. Economic aspects of internet security. *CPB Background Document*, 2014.

[13] Jeroen Pijpker and Harald Vranken. The role of internet service providers in botnet mitigation. In *Intelligence and Security Informatics Conference (EISIC), 2016 European*, pages 24–31. IEEE, 2016.

[14] Michel van Eeten, Hadi Asghari, Johannes M Bauer, and Shirin Tabatabaie. Internet service providers and botnet mitigation: A fact-finding study on the dutch market. *Delft University of Technology*, 2011.

[15] Michel Van Eeten, Johannes Bauer, Hadi Asghari, Shirin Tabatabaie, and David Rand. The role of internet service providers in botnet mitigation an empirical analysis based on spam data. 2010.

Appendix 1. Linear Regression Analysis

SUMMARY OUTPUT

Regression Statistics	
Multiple R	0,66803241
R Square	0,4462673
Adjusted R Sc	0,44618808
Standard Errc	545,101539
Observations	6992

ANOVA

	df	*SS*	*MS*	*F*	*Significance F*
Regression	1	1673889904	1673889904	5633,419247	0
Residual	6990	2076978459	297135,688		
Total	6991	3750868363			

	Coefficients	*tandard Error*	*t Stat*	*P-value*	*Lower 95%*	*Upper 95%*	*Lower 95.0%*	*Upper 95.0%*
Intercept	41,7767365	6,52093974	6,40655154	1,58513E-10	28,99371603	54,559757	28,993716	54,55975701
X Variable 1	9,721E-07	1,2952E-08	75,0561073	0	9,46714E-07	9,9749E-07	9,4671E-07	9,97493E-07

RESIDUAL OUTPUT

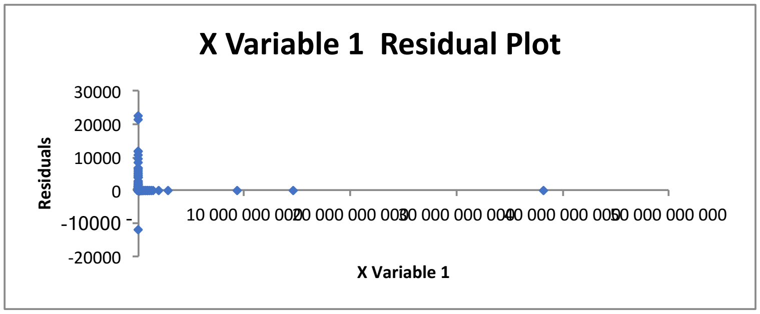
Observation	*Predicted Y*	*Residuals*	*ndard Residuals*
1	41,7784785	-34,778479	-0,0638064
2	41,7769854	-40,776985	-0,0748116
3	41,777732	-40,777732	-0,0748129
4	41,777732	-40,777732	-0,0748129
5	41,777732	-37,777732	-0,069309
6	41,7866909	-36,786691	-0,0674908
7	44,6455778	-18,645578	-0,0342081
8	41,777732	-40,777732	-0,0748129
9	41,777732	-40,777732	-0,0748129
10	41,7797228	-38,779723	-0,0711473
11	42,4456683	-13,445668	-0,0246681
12	41,777732	-40,777732	-0,0748129
13	41,8085904	-36,80859	-0,0675309
14	41,7789762	-35,778976	-0,065642
15	41,8021201	-28,80212	-0,0528419
16	41,7769854	-40,776985	-0,0748116
17	41,7926635	-39,792663	-0,0730057
18	41,7807183	-39,780718	-0,0729838
19	41,7769854	-40,776985	-0,0748116
20	41,7909215	-25,790921	-0,0473174
21	41,7774831	-38,777483	-0,0711432
22	41,7817137	-37,781714	-0,0693163
23	41,8085904	-39,80859	-0,0730349
24	41,8085904	-40,80859	-0,0748696
25	41,7769854	-40,776985	-0,0748116
26	41,777732	-40,777732	-0,0748129
27	41,7787274	-40,778727	-0,0748148
28	41,7772342	-39,777234	-0,0729774
29	41,7782297	-39,77823	-0,0729792
30	41,777732	-40,777732	-0,0748129
31	41,7926635	-40,792663	-0,0748403
32	41,7772342	-40,777234	-0,074812
33	41,7774831	-38,777483	-0,0711432
34	41,8344717	-28,834472	-0,0529012

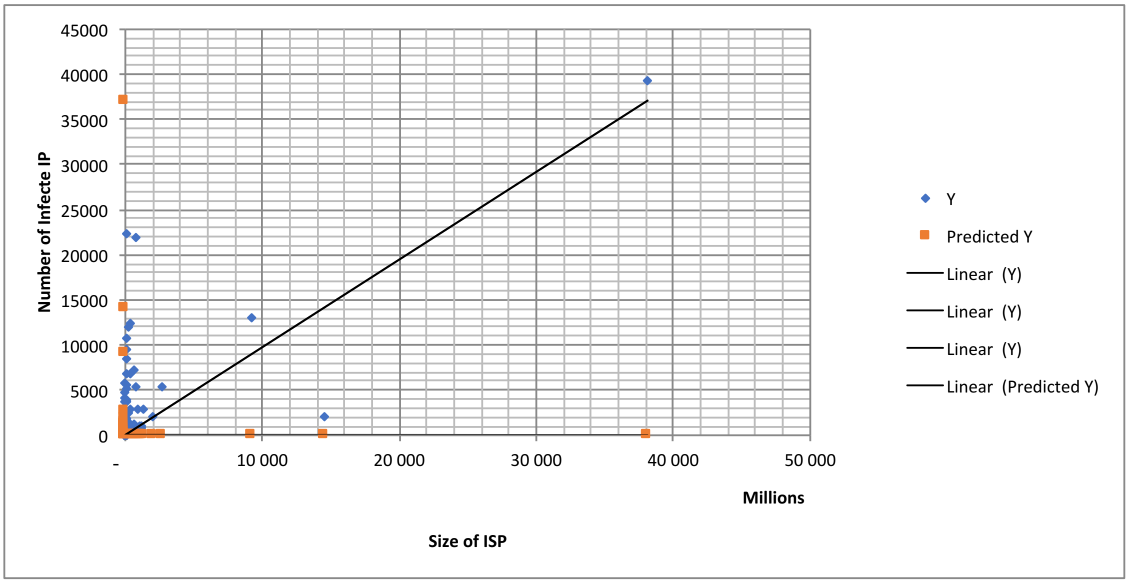
PROBABILITY OUTPUT

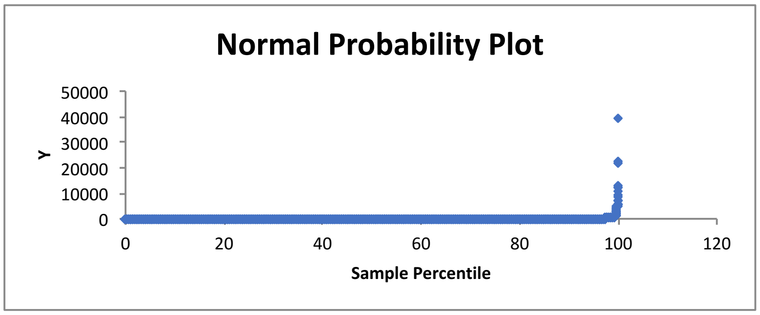
Percentile	*Y*
0,00715103	1
0,021453089	1
0,035755149	1
0,050057208	1
0,064359268	1
0,078661327	1
0,092963387	1
0,107265446	1
0,121567506	1
0,135869565	1
0,150171625	1
0,164473684	1
0,178775744	1
0,193077803	1
0,207379863	1
0,221681922	1
0,235983982	1
0,250286041	1
0,264588101	1
0,27889016	1
0,29319222	1
0,307494279	1
0,321796339	1
0,336098398	1
0,350400458	1
0,364702517	1
0,379004577	1
0,393306636	1
0,407608696	1
0,421910755	1
0,436212815	1
0,450514874	1
0,464816934	1
0,479118993	1

35	41,7769854	-40,776985	-0,0748116	0,493421053	1
36	41,7769854	-40,776985	-0,0748116	0,507723112	1
37	45,097505	-28,097505	-0,0515491	0,522025172	1
38	42,0395311	-37,039531	-0,0679546	0,536327231	1
39	41,777732	-40,777732	-0,0748129	0,550629291	1
40	41,7847	-40,7847	-0,0748257	0,56493135	1
41	41,7961475	-29,796147	-0,0546656	0,57923341	1
42	41,9439695	-37,943969	-0,069614	0,593535469	1
43	41,777732	-37,777732	-0,069309	0,607837529	1
44	41,7807183	-39,780718	-0,0729838	0,622139588	1
45	41,7802205	-27,780221	-0,050967	0,636441648	1
46	41,8165539	-34,816554	-0,0638763	0,650743707	1
47	41,777732	-39,777732	-0,0729783	0,665045767	1
48	41,7769854	-40,776985	-0,0748116	0,679347826	1
49	41,7787274	-39,778727	-0,0729801	0,693649886	1
50	41,7772342	-39,777234	-0,0729774	0,707951945	1
51	41,8245174	-38,824517	-0,0712295	0,722254005	1
52	41,8046087	-38,804609	-0,0711929	0,736556064	1
53	41,7859443	-35,785944	-0,0656547	0,750858124	1
54	41,7827091	-17,782709	-0,0326251	0,765160183	1
55	41,7787274	-39,778727	-0,0729801	0,779462243	1
56	41,7847	-38,7847	-0,0711564	0,793764302	1
57	41,777732	-40,777732	-0,0748129	0,808066362	1
58	42,5571569	6,44284308	0,01182037	0,822368421	1
59	41,7787274	-40,778727	-0,0748148	0,836670481	1
60	41,777732	-40,777732	-0,0748129	0,85097254	1
61	41,777732	-40,777732	-0,0748129	0,8652746	1
62	41,7814648	-28,781465	-0,052804	0,879576659	1
63	41,7772342	-39,777234	-0,0729774	0,893878719	1
64	41,7792251	-37,779225	-0,0693117	0,908180778	1
65	41,8456703	-17,84567	-0,0327406	0,922482838	1
66	41,7774831	-38,777483	-0,0711432	0,936784897	1
67	41,7772342	-39,777234	-0,0729774	0,951086957	1
68	41,8292457	163,170754	0,29936152	0,965389016	1
69	41,7769854	-40,776985	-0,0748116	0,979691076	1
70	41,8085904	-39,80859	-0,0730349	0,993993135	1
71	41,777732	-40,777732	-0,0748129	1,008295195	1
72	41,7787274	-40,778727	-0,0748148	1,022597254	1
73	41,7789762	-39,778976	-0,0729806	1,036899314	1
74	46,3681767	46,6318233	0,08555316	1,051201373	1
75	41,7847	-39,7847	-0,0729911	1,065503432	1
76	41,7789762	-32,778976	-0,060138	1,079805492	1
77	41,7807183	-40,780718	-0,0748184	1,094107551	1
78	41,8008758	-35,800876	-0,0656821	1,108409611	1
79	41,7971429	-15,797143	-0,0289823	1,12271167	1
80	41,7779808	-36,777981	-0,0674748	1,13701373	1
81	41,7807183	-37,780718	-0,0693145	1,151315789	1
82	41,7769854	-40,776985	-0,0748116	1,165617849	1
83	41,777732	-39,777732	-0,0729783	1,179919908	1
84	41,8185448	-26,818545	-0,0492027	1,194221968	1
85	41,8135676	-24,813568	-0,0455243	1,208524027	1
86	41,777732	-37,777732	-0,069309	1,222826087	1
87	41,7774831	-38,777483	-0,0711432	1,237128146	1
88	41,777732	-40,777732	-0,0748129	1,251430206	1
89	41,7847	-40,7847	-0,0748257	1,265732265	1
90	41,7784785	-37,778479	-0,0693104	1,280034325	1
91	41,9041521	-40,904152	-0,0750449	1,294336384	1
92	42,7960611	-34,796061	-0,0638387	1,308638444	1
93	41,7772342	-40,777234	-0,074812	1,322940503	1
94	41,7769854	-40,776985	-0,0748116	1,337242563	1
95	41,7926635	-40,792663	-0,0748403	1,351544622	1

96	41,7787274	-40,778727	-0,0748148	1,365846682	1
97	41,7784785	-34,778479	-0,0638064	1,380148741	1
98	42,0290791	39,9709209	0,07333272	1,394450801	1
99	41,7772342	-39,777234	-0,0729774	1,40875286	1
100	42,1589832	-34,158983	-0,0626698	1,42305492	1
101	41,7871886	-38,787189	-0,071161	1,437356979	1
102	41,7772342	-39,777234	-0,0729774	1,451659039	1
103	41,7769854	-40,776985	-0,0748116	1,465961098	1
104	41,777732	-37,777732	-0,069309	1,480263158	1
105	41,7769854	-40,776985	-0,0748116	1,494565217	1
106	41,9598964	-27,959896	-0,0512967	1,508867277	1
107	42,3535906	42,6464094	0,07824131	1,523169336	1
108	41,8085904	-40,80859	-0,0748696	1,537471396	1
109	41,7847	-39,7847	-0,0729911	1,551773455	1
110	41,777732	-40,777732	-0,0748129	1,566075515	1
111	41,7966452	-31,796645	-0,0583358	1,580377574	1
112	41,7787274	-40,778727	-0,0748148	1,594679634	1
113	41,7772342	-40,777234	-0,074812	1,608981693	1
114	41,7886817	-34,788682	-0,0638251	1,623283753	1
115	41,777732	-40,777732	-0,0748129	1,637585812	1
116	42,1507709	-4,1507709	-0,0076152	1,651887872	1
117	41,7886817	-39,788682	-0,0729984	1,666189931	1
118	41,7787274	-40,778727	-0,0748148	1,680491991	1
119	41,7939078	27,2060922	0,04991371	1,69479405	1
120	41,7774831	-38,777483	-0,0711432	1,70909611	1
121	41,7827091	-26,782709	-0,0491369	1,723398169	1
122	41,7919169	19,2080831	0,03524014	1,737700229	1
123	41,791668	-26,791668	-0,0491534	1,752002288	1
124	41,7966452	-36,796645	-0,067509	1,766304348	1
125	41,7772342	-39,777234	-0,0729774	1,780606407	1
126	41,7772342	-39,777234	-0,0729774	1,794908467	1
127	41,7807183	-40,780718	-0,0748184	1,809210526	1
128	41,7772342	-40,777234	-0,074812	1,823512586	1
129	41,7832068	-18,783207	-0,0344606	1,837814645	1
130	41,7906726	-37,790673	-0,0693327	1,852116705	1
131	41,7772342	-39,777234	-0,0729774	1,866418764	1
132	41,777732	-40,777732	-0,0748129	1,880720824	1
133	41,7769854	-40,776985	-0,0748116	1,895022883	1
134	41,7814648	-33,781465	-0,0619772	1,909324943	1
135	41,7769854	-40,776985	-0,0748116	1,923627002	1


X Variable 1 Residual Plot
30000
20000
10000
0
-10000
-20000
Residuals
10 000 000 000
20 000 000 000
30 000 000 000
40 000 000 000
50 000 000 000
X Variable 1


45000
40000
35000
30000
25000
20000
15000
10000
5000
0
Number of Infecte IP
-
10 000
20 000
30 000
40 000
50 000
Millions
Size of ISP
Y
Predicted Y
Linear (Y)
Linear (Y)
Linear (Y)
Linear (Predicted Y)


Normal Probability Plot
50000
40000
30000
20000
10000
0
Y
0
20
40
60
80
100
120
Sample Percentile

Appendix 2. Calculations for second analysis

	7.08.2016	25.08	04.10	30.10	7.11	27.11	21.12	08.01	
	Peak 1	**Peak 2**	**Peak 2**	**Peak 3**	**Peak 4**	**Peak 5**	**Peak 6**	**Peak 7**	
	J1	J2	J3	J4	J5	J6	J7	J8	**total**
I1 / Countries with IDI higher than 5.11	365	375	666	890	1139	1469	979	770	**6653**
I2 / Countries with IDI lower than 5.11	1866	1444	2341	4061	5867	4050	3775	2799	**26203**
total	**2231**	**1819**	**3007**	**4951**	**7006**	**5519**	**4754**	**3569**	**32856**

E11	451,7544132	O11	365
E12	368,3286766	O12	375
E13	608,886383	O13	666
E14	1002,526266	O14	890
E15	1418,642501	O15	1139
E16	1117,540388	O16	1469
E17	962,6358047	O17	979
E18	722,6855673	O18	770
E21	1779,245587	O21	1866
E22	1450,671323	O22	1444
E23	2398,113617	O23	2341
E24	3948,473734	O24	4061
E25	5587,357499	O25	5867
E26	4401,459612	O26	4050
E27	3791,364195	O27	3775
E28	2846,314433	O28	2799

16,6602207	4,23006709
0,1208338	0,03067997
5,35726424	1,36022131
12,6302532	3,20684939
55,1230688	13,9958698
110,531897	28,0642945
0,27818089	0,07063075
3,09768956	0,78651027

X^2	255,544531		
df	7		
x^2 (7 and 0.05)	14.07	< 255	they are not independent, we reject H0