The effect of socio-economic and socio-technical factors on the variability of the ZeuS Command and Control Centres

Anirudh Ekambaranathan
s1366432
9 November 2015

Economics of Security

1 TABLE OF CONTENTS

2 ABSTRACT

This paper looks at several socio-economic and socio-technical factors and analyses their correlation with the variability of online C&Cs. As a sample dataset the ZeuS C&Cs are analysed. The analysis is performed by calculating a statistical correlation on each factor and the number of C&C additions/removals on a per country basis. The socio-economic factors produce quantitative results using the Pearson's R Coefficient. And the socio-technical factor is analysed by a qualitative means.

3 INTRODUCTION

This paper analyses the correlation between Command and Control Centres (C&Cs) and various socio-technical and socio-economic factors. The paper mainly focuses on the Command and Control Centres (C&Cs) of the ZeuS Trojan. An analysis is performed regarding the variability of online C&Cs and how certain factors may affect this variability. These factors are taken out of the following indicators: Economy & Growth, Environment, Infrastructure, and Science & Technology. From these indicators the following factors have been chosen. Unemployment rate, Access to electricity, Internet users per 100 people, R&D expenditure, Researchers in R&D. Apart from these factors, the following factors may also influence the variability of online C&Cs: cybercrime rates and botnet takedown operations.

3.1 The security issue

The issue in question is the online C&Cs of the ZeuS Trojan. ZeuS is basically a crimeware kit which is used to steal sensitive credentials from online services. The C&Cs are being tracked by several services; the dataset this paper uses is retrieved from the abuse.ch [1] web service. These trackers show the ZeuS and Feodo C&Cs and also provide a list of ZeuS C&C removals.

Cyber criminals making use of either of the ZeuS Trojan must first buy the crimeware kit, which can be found on the black market. The Trojan itself is spread through various means such as phishing and malicious ads. A victim device which has the Trojan installed will communicate with a malicious dropzone and send sensitive information from the victim.

With more C&Cs online, more attempts will be made to spread the Trojan. The security issue is the vast number of C&Cs online as well as the unknowingness of people regarding Trojans, phishing attempts and other attempts of spreading the malware. To counter the problem of the ZeuS Trojan it is possible to educate people on cyber security and/or eliminate the number of C&Cs. However, there may be other factors which have an effect on the number of C&Cs, despite them being indirect.

3.2 Justification

This paper thus shines some light on factors which may indirectly affect the security issue of the number of C&Cs. By knowing these relations it becomes possible to combat C&Cs by other means as well, which may improve the overall effectiveness of e.g. botnet takedowns.

4 LITERATURE REVIEW

Research on botnets has been done extensively in the past. The dataset from the ZeuS and Feodo trackers however do not reveal much about the botnet infrastructure itself. It gives an indication of the distribution of the C&Cs.

There are many factors which may affect cyber security related events. Kleiner et al. (2013) [8] have written a paper where they tried to identify relationships between cyber security and national-level factors. The goal of the paper was to analyse the different factors involved in cybersecurity performance in different countries. The paper was not specifically focused on botnets, cyber security in general on international and national scale. The factors described in [8] can however also be used to as factors to describe the behaviour of C&C counts. The paper concludes the quantitative analysis by stating that to cyber security should, in the future, focus on international internet infrastructure and internet governance.

Next to Kleiner et al. other papers have looked at factors regarding botnets as well. For example [4] looked the role ISPs play in botnets. The paper also identifies different factors which play a role in botnet activity. However the perspective is from ISPs and how they play a role as intermediaries in botnets sending spam. The factors described are: security measures implemented by ISPs, virility of cyberattacks and user behaviour [4] .

The general trends of botnets are not extensively researched, however [11] provides an interesting discussion. According to [11] more and more botnets are switching to a peer-to-peer infrastructure, making them more resilient and harder to track and harder to take down. This may affect the way C&C counts behave after takedown operations. A takedown operation may therefore not completely stop a botnet threat, since there is always the possibility of revival, and this may affect the variability of online C&Cs in different ways. Also [3] gives an interesting view on botnets trends and motivation of botnet creators. Another paper looking at the trends of ZeuS is [2]. The paper investigates the techniques used in obfuscated malware. Furthermore the paper looks at the importance of anomaly detection in combatting ZeuS.

Not much research has been done on the behaviour of C&Cs of different malware. This paper will look at this behaviour, with respect to the ZeuS Trojan, and analyse this behaviour from a socio-economic and technical perspective.

5 RESEARCH QUESTION

The research question, this paper is concerned with, can be stated as: do socio-economic and socio-technical factors influence the variability of online C&Cs? This main research question can be answered by answering several sub-questions.

How does

- Unemployment rate
- Access to electricity
- Internet users per 100 people
- R&D expenditure
- Secondary school enrolment (% net)
- Cybercrime rates
- Botnet takedown operations

affect the variability of online C&Cs?

The factors are taken from the World Development Indicators [13]. There are many factors which are not discussed here, and therefore this paper does will not cover the entirety of socio-economic and socio-technical layers. It will solely focus on the factors described above. The factors are believed to be related to botnets, however whether this is actually the case is the subject of this paper. A justification for each factor is given in the hypothesis.

5.1 Objective

The objective of answering these questions is to find how different factors play a role in availability of C&Cs. Some factors are left out in the analysis, for example education and clearance rates of crimes. These factors fall beyond the scope of this paper, and the analysis thereof can be conducted in further research.

5.2 Hypotheses

Every factor may be related to the number of online C&Cs. The following sections give a justification for the pertinent factor and how it is believed to affect the security issue.

5.2.1 Unemployment rate

According to [10] an increase in the unemployment rate shows an increase in the number of crimes committed. This leads to believe that in times of high unemployment more C&Cs should be online. The matter may however be more complicated. Crimeware kits for ZeuS and Feodo are not relatively cheap. In times of unemployment people may be hesitant to make large investments. Furthermore, these types of crimes seem to be more related to people with a bigger technical understanding. For now it suffices to formulate the hypothesis as follows: an increase in the unemployment rate should show an increase in the number of online C&Cs.

5.2.2 Access to electricity

In countries with lower access to electricity it might not be beneficial for cyber criminals to set up C&Cs. Less access to electricity may also mean that fewer people are exposed to services based on electricity, and hence computer related services. This, however is still something that needs to be researched. If the above hypothesis holds, then the following can be stated: countries with lower access to electricity will probably show a lower contribution to the overall number of C&Cs.

5.2.3 Internet users per 100 people

With less Internet users per 100 people it means that a lower percentage of the people are involved in cyber related activities. The hypothesis is then that countries with a higher number of Internet users should show a higher number of online C&Cs.

5.2.4 R&D expenditure

A factor is needed to determine the technological progress rate of a country. This factor therefore used a proxy for that. The reason that not the original factor is used (technological progress rate), is because accurate data for that is scarce. R&D expenditure gives an idea as to what degree a country is involved with technological progress. The assumption made is that countries with a high R&D are technologically more developed. The hypothesis is then as follows: countries with a higher R&D expenditure should show a higher number of C&Cs.

5.2.5 School enrolment, secondary (% net)

This factor is supposed to give an idea to what degree a population is educated. A population which is less educated will be less aware of the technicalities involved in cybercrimes. The hypothesis is then as follows: countries with a higher school enrolment rate should show a higher number of C&Cs.

5.2.6 Cybercrime Rates

This factor is more complicated to analyse, since an increase in the number of C&Cs should show an increase in the cybercrime rates. However, this paper is about the analysis of the opposite. This factor is therefore about how increased cybercrime rates may serve as an incentive to set up more C&Cs. The hypothesis is that increased cybercrime rates might have a snowball effect and may therefore further incentivize setting up C&Cs.

5.2.7 Botnet Takedown Operations

Botnet takedown operations have a clear effect on C&C numbers. A botnet operation will immediately reduce the number of online C&Cs. However it does not tell anything yet about the behaviour of online C&Cs in the future.

6 METHODOLOGY

Initially the dataset provided by the ZeuS tracker is graphed and tabularized. The data is ordered such that an overview can be made which shows the number of additions of C&Cs and the number of removals per country.

Every factor described above, is seen as a factor which may influence the security issue. However, alone, they are only indicators. There are again factors which influence these indicators. It is important

to identify these factors so that major fluctuations can be rationally explained. The actors behind every factor is analysed to gain a better understanding between the relation of the factor and the security issue.

6.1 Quantitative measurements

Most of the measurements performed will be quantitative. A statistical correlation is performed between each factor and the number of C&Cs. Major fluctuations are taken separate and a separate statistical correlation is performed to see if that particular fluctuation can be explained. For example, a major decrease in the number of C&Cs and a takedown operation will be heavily correlated, which may not initially show when an annual correlation is calculated.

6.2 Qualitative

A statistical correlation may not necessary indicate anything. Therefore, analysing the actors involved and the nature of the factor, a possible causal relation is draw between the factor and the security issue. Only of this causal relationship exists, the statistical correlation will be significant.

7 FINDINGS

This section looks at the findings of each factor described in the previous sections. It analyses the actors involved which may affect that certain factor, and what the driving forces are behind that factor. It is important to understand the behaviour of the factor, since large fluctuations in these factors need to be translated to the behaviour of the security issue: the variability of C&Cs.

7.1.1 The ZeuS dataset

The ZeuS tracker provides information about when C&Cs have been initially discovered and when they have been removed. This provides a graph of how the additions of C&Cs have been behaving. See figure 1.

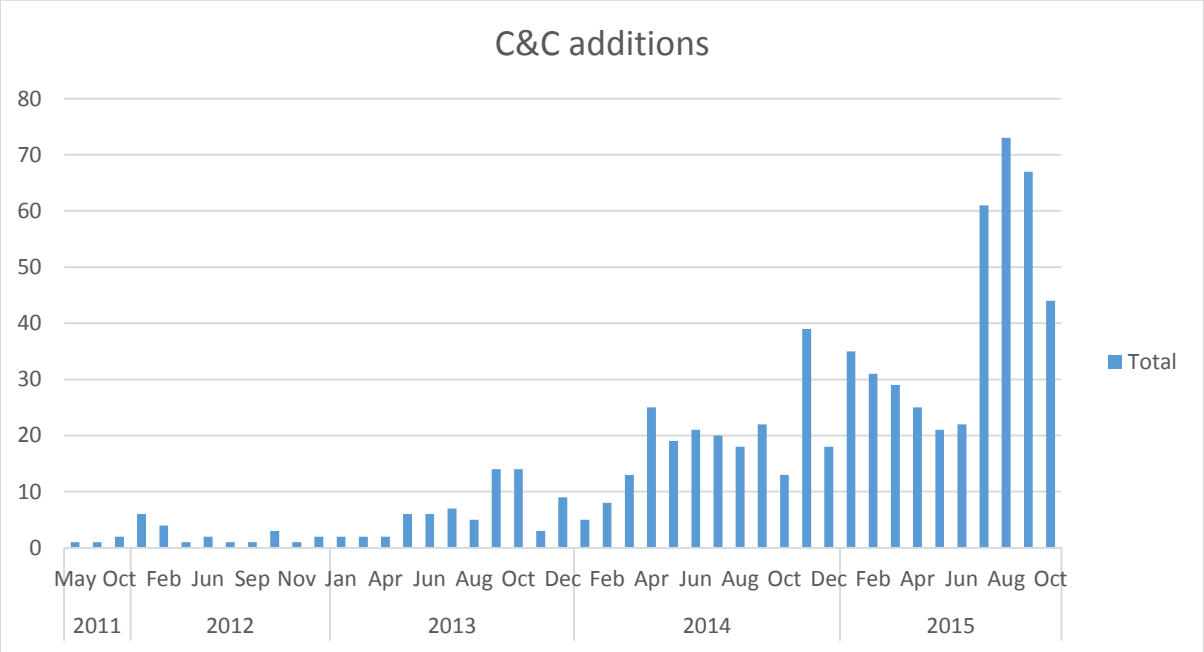

Figure 1: C&C additions over the years

Looking at figure 1 shows that in the years 2011 and 2012 ZeuS C&Cs increased slowly. In the years 2014 and 2015, the increase is larger. Figure 8 shows the removals of the C&Cs as well as how these removals have reacted to botnet takedown operations.

7.1.2 Unemployment rate

This dataset describes the percentage of people in a certain country which is unemployed but actively looking for and seeking employment.

7.1.2.1 Actors involved

The actors involved in unemployment are: the employee and the company. Unemployment happens when the company does not want to invest in a given employee anymore. The result is that the unemployed person has less money to spend and that the company saves money.

7.1.2.2 Driving factors

There are many factors which may cause unemployment. *Frictional unemployment* happens is caused by employees moving between jobs. *Structural unemployment* is caused by structural mismatches, for example geographic location of the job and the residence of the employee. *Real wage unemployment* is caused when the supply of labour is larger than its demand. *Voluntary unemployment* is caused when people by their free will choose not to work. *Cyclical unemployment* is caused when there is not enough demand for labour due to the economy being below capacity.

7.1.2.3 Causal correlation

Of the various factors mentioned above, not all of them have a causal relationship with the security issue. Based on the assumption stated above, frictional and voluntary unemployment is does not directly affect the security issue. These two causes for unemployment is directly under the control of the employee. The other forms of unemployment are not within the control of the employee. As stated in [10], unemployment causes an increase in the number of crimes.

7.1.2.4 Statistical correlation

Given that the U.S. produced the highest number of C&C additions the correlation was calculated between U.S. monthly unemployment rates and C&C additions. Other countries produced relatively few C&Cs which made those correlations negligible. Below are the tables showing the correlation between C&C additions/removals and monthly unemployment rates of the U.S.

Table 1: Correlation between C&C removals and U.S. monthly unemployment rates

	Count of C&C removals	*Unemployment U.S.*
Count of C&C removals	1	
Unemployment U.S.	-0.32611	1

Table 2: Correlation between C&C additions and U.S. monthly unemployment rates

	Count of C&Cs added	*Unemployment U.S.*
Count of C&Cs added	1	
Unemployment U.S.	-0.4484	1

The following scatter plots shows how the C&C additions/removals group against the unemployment rates.

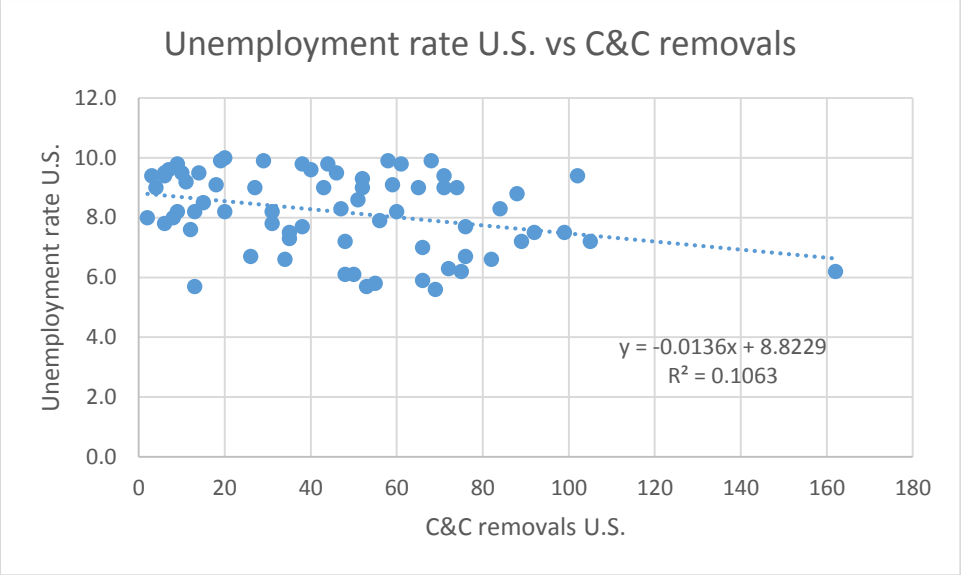

Figure 2: Unemployment rate U.S. vs C&C removals

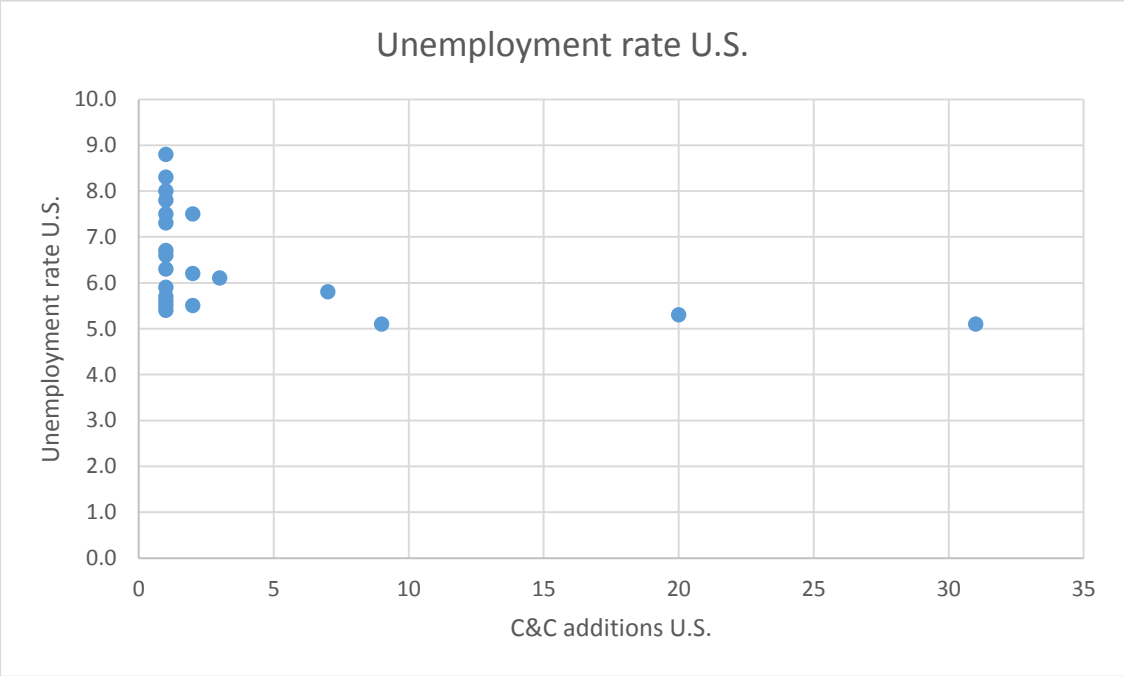

Figure 3: Unemployment rate vs. C&C additions

7.1.2.5 Analysis

Most of the C&Cs were produced by the U.S., therefore the choice was made to analyse the U.S. unemployment figures. These figures also give an idea of the health of the U.S. economy.

The correlation between seems at first to be relatively significant, with a Pearson's R coefficient of -0.45, which means that an increase in the unemployment rate shows a decrease in the C&C count and vice versa. This is not according to the hypothesis formulated in the previous sections. Statistically speaking it would mean that with unemployment rates increasing, criminals are less inclined to establish a C&C. This could be for reasons such as the cost of a C&C being too large.

However, on a closer inspection, looking at figure 2, there is not much variance in the number of C&C additions, and the number of small additions is paired with a large variance of unemployment rates. Furthermore, the unemployment rate should be able to tell something, if truly correlated, about large fluctuation in C&C additions. Thus meaning, in case of a large increase in the number of C&Cs, there should be a large drop in the unemployment rates. Plotting the graph of unemployment rates in the U.S., figure 3, it can be seen that this is not the case. The unemployment rate is gradually decreasing, there are no drastic fluctuations which would support the hypothesis that unemployment rates are correlated to C&C activity.

The unemployment rates have also been compared to the removal rates of C&Cs, since these removal rates give an idea of where C&Cs have been. However the scatter plot also shows a large randomness, which can also been seen in the Pearson's r coefficient of -0.32611.

The reason for a large negative correlation can be explained by the 'popularity' of the ZeuS C&Cs. In the beginning years, there are only a few additions of C&Cs every month. As ZeuS becomes more known, there is a growth in the number of additions. At the same time there is a decrease in the unemployment rate, which leads to a statistical correlation. However, there is not enough evidence of causal correlation to support the statistical correlation.

In short, unemployment figures do not show any statistical correlation with C&C variability as long as the unemployment figures as stable. C&Cs activity may be different during unstable economies, however that subject is beyond the scope of this paper.

Figure 4: Unemployment rate U.S.

7.1.3 Access to electricity

This dataset describes the percentage of the population which has access to electricity.

7.1.3.1 Actors involved

The actors involved are people with living accommodations, as well as companies and other organizations which are settled in buildings. Another main actor is the provider of the electricity. Furthermore, there are actors which may be involved, such as terrorists or criminals attacking electricity infrastructure.

7.1.3.2 Driving factors

Factors involved for households to choose electricity are quality of electricity supply and degree of electricity supply [7]. Access to electricity is also affected by uncontrollable disasters, such as power cuts and criminal attacks on electricity supplies. Another factor is national infrastructure of the pertinent country.

7.1.3.3 Causal correlation

No research has been conducted on the relationship between electricity access and cybercrime rates. However, countries with a higher access to electricity will have a higher number of servers available, allowing for criminals to set up more C&Cs.

7.1.3.4 Statistical correlation

The following graphs and tables show the correlations with access to electricity. Again the correlation has been drawn with both C&C additions as well as removals.

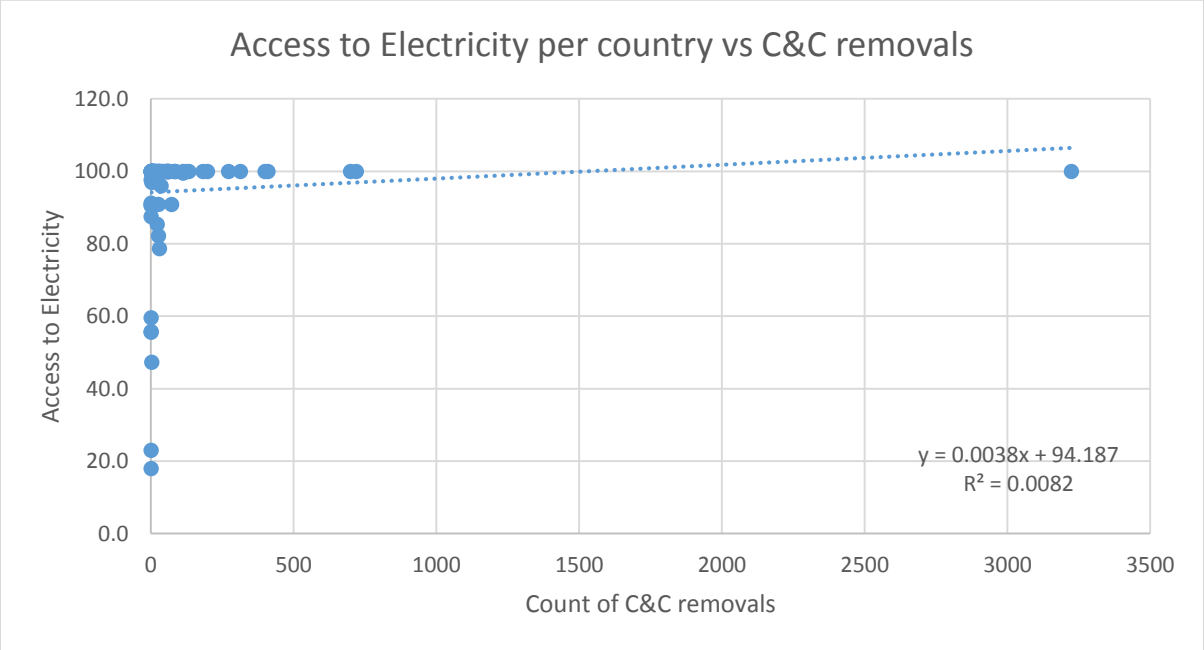

Figure 5: Access to electricity plotted against C&C removals

Table 3: Correlation between Access to electricity and C&C removals

	Count of C&C removals	*Access to Electricity*
Count of C&C removals	1	
Access to Electricity	0.090407	1

Table 4: Correlation between Access to electricity and C&C additions

	Count of C&C additions	*Access to Electricity per Country*
Count of C&C - additions	1	
Access to Electricity per Country	0.134141	1

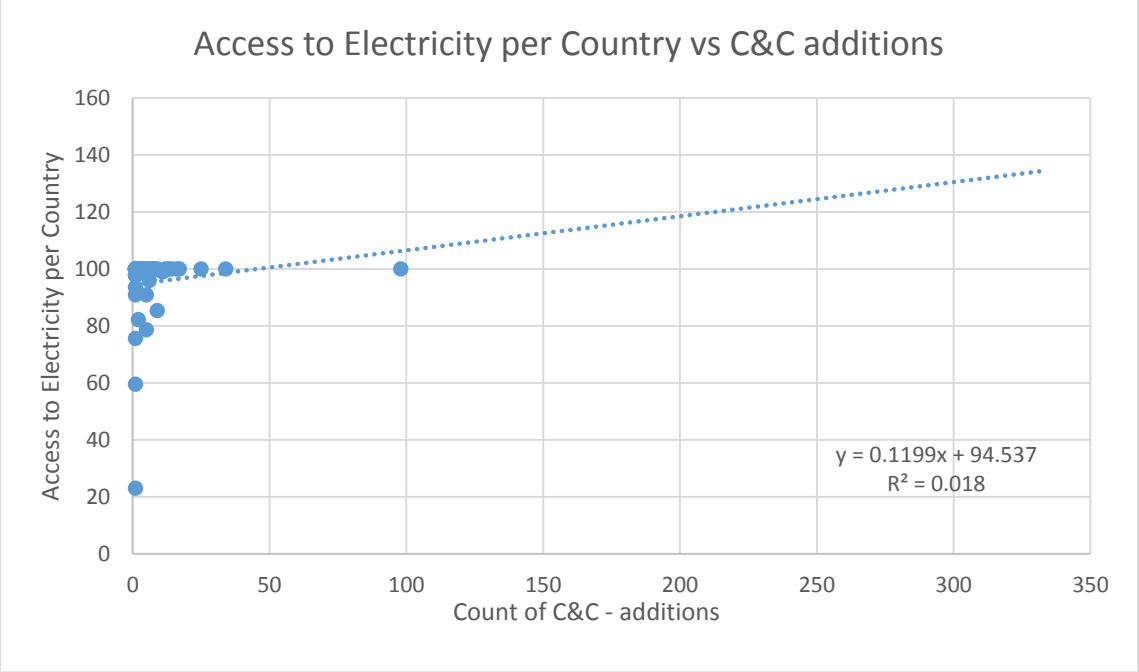

Figure 6: Access to electricity per country vs C&C additions

7.1.3.5 Analysis

It can be seen that the statistical correlation is nearly non-existent; the Pearson's R coefficient is 0.09 for C&C removals and 0.134 for C&C additions. The scatter plots also show a large randomness. The statistical correlation coefficient does not support the hypothesis stated in the earlier section. The difference in access to electricity per country does not statistically affect the security issue in any way.

One of the reasons this might be the case is the variability in the data of Access to Electricity. The variance between countries with a high access is very small. This means that the majority of the countries show a rate of 100. This lack of variance does not allow for an accurate analysis of correlation. The statistical analysis then is meaningless and fails to support any hypothesis.

7.1.4 Internet users per 100 people

This dataset describes people who have used the Internet in the past years. This may have been done from any electronic device such as, mobile phone, laptop, desktop etc.

7.1.4.1 Actors involved

The actors involved are mainly the residents of the pertinent country. However, governments and Internet Service Providers also play a role. Governments have the option to promote usage of internet. There are certain factors which may prevent this, for example, governments may have different priorities than Internet provision.

7.1.4.2 Driving factors

Factors which influence the internet usage are, the national cyber infrastructure, economic health, costs of Internet, number of ISPs etc. As can be seen, there are many variables involved when it comes to the number of Internet users.

7.1.4.3 Causal correlation

As the density of Internet users in a country increases, the number of people involved in cyber related activities increase, which again increases the chance of cybercrime rates. Crudely put, a country in which no one uses Internet will have almost no cyber (Internet) related crimes and country in which everyone uses Internet, will have a higher number of cyber (internet) crimes.

7.1.4.4 Statistical correlation

The World Development Index [13] provides the number of Internet Users per 100 people on a yearly basis for different countries. The correlation has be calculated for every year together with the total number of produced C&Cs per country. The reason for this is that the numbers are too scarce for the earlier years, which would render the correlation coefficient unreliable.

Table 5: Correlation between Internet users per 100 per country per year and C&C additions

	Count of C&C additions vs number of Internet users
Date	
2009	0.173567311
2010	0.178840691
2011	0.149560875
2012	0.201590421
2013	0.214318246
2014	0.222333623

7.1.4.5 Analysis

The statistical correlations are too small to statistically signify a relation. The numbers thus do not support the hypothesis formulated before. An increase in the number of Internet users per country does not statistically mean a larger number of C&Cs produced in that country.

Interestingly there seems to be an increase in the correlation in later years. Whereas the correlation was 0.17 in 2009, it was 0.22 in 2014. A reason for this could be that more data was available in later years than in earlier years and allowed for a more accurate analysis. The factor looked at the number of Internet users per 100 people in a specific country. Countries such as Iceland, have a rate of 95.0-98.0, meaning that nearly all people in the population use Internet. However, Iceland only produced 1 C&C in the past 5 years. Cases such as these lead to the hypothesis not being statistically supported.

Given that this factor is not enough to show a correlation, it might be more useful to analyse a factor such as the number of servers per country. That can be done in a subsequent research.

7.1.5 R&D expenditure

This dataset described capital and current expenditures which on research conducted to increase knowledge. This includes knowledge for the use of new applications, knowledge of society, humanity and culture [12].

7.1.5.1 Actors involved

The actors involved in R&D expenditures are companies, universities and governments. Companies and universities mostly have R&D departments. Governments may be involved in subsidising R&D. It can also be the case that governments have their own intelligence institutions which have an R&D department.

7.1.5.2 Driving factors

Factors involved in the R&D expenditures are, the type of companies, the number of universities, the economy of a country, the technical progress of a country etc. Again, this indicator has many factors which affect it. Also it leaves a lot of room for ambiguity. Large companies may place their R&D departments in poorer countries because of financial benefits. This, however falsely influences the metric.

7.1.5.3 Statistical correlation

The R&D expenditure rates have been correlated with the C&C additions to produce the Pearson's R coefficient. Table 6 shows the numbers. The R&D expenditure of every country has been correlated to the C&C count of every country.

Table 6: Correlation between count of C&C additions per country and R&D expenditure

	Count of C&C additions per Country
Date	1
2009	0.199266217
2010	0.2299209
2011	0.2034275
2012	0.225526759

7.1.5.4 Analysis

The numbers do not show a statistical correlation significant enough to support the hypothesis formulated in the former sections. The correlations also show no trend over the years and seem random. This means that countries with a larger R&D expenditures do not necessarily produce more C&Cs.

The R&D expenditure factor was used as a proxy to indicate technical progress. It is very well possible that this is not very accurate and thus compromises the analysis. A quick analysis can be done comparing the top ten C&C hosting countries with the top ten technically most advanced countries. This produces the following table.

Table 7: C&C and Technology rankings of countries

C&C and Technology rankings of countries			
ZeuS C&C count	Country	Country	Rank of Technological progress
98	United States (US)	Japan	1
34	Russian Federation (RU)	Finland	2
25	Netherlands (NL)	United States	3
17	Germany (DE)	South Korea	4
16	Ukraine (UA)	Germany	5
14	Canada (CA)	China	6
13	Thailand (TH)	Canada	7
12	Romania (RO)	United Kingdom	8
11	Vietnam (VN)	Philippines	9
10	Brazil (BR)	Russian Federation	10

It can be seen that countries which are part of the top most technologically advanced countries contribute to a larger number of C&Cs. For example, United States and the Russian Federation are in both lists. Bus then, the Philippines is does has not produced any C&Cs at all. The data is thus more complex than can be viewed at first glance. A complete analysis of this is subject of perhaps a subsequent research.

7.1.6 School enrolment, secondary (% net)

This dataset describes the ratio of the population which is of official age to attend secondary school and is attending secondary school. Secondary education is a continuation of primary education and is aimed at teaching the fundamentals of "lifelong learning and human development [12][13].

7.1.6.1 Actors involved

The main actors involved are the students, schools and governments. Secondary actors may be the parents, who are responsible for sending their children to school.

7.1.6.2 Driving factors

There are various reasons a child may or may not go to school. Reasons for not going to school are: lack of interest, lack of finances, no schools, etc. Children not going to school may do so because the parents do not have the financial means to send the child or need the child to help with work. Other reasons could also be that the child does not want to go to school. This may not always be a valid factor, since in various countries it is mandatory to go to school if you have not yet reach the age of an adult. Another reason might also be that there are no schools nearby, and this structural obstacle prevents them.

7.1.6.3 Statistical correlation

Below is a table showing various correlations between C&C additions and School enrolment rates per country. The enrolment rate of every country has been correlated with the C&C count of every country on a yearly basis.

Table 8: Correlation between School enrolment and C&C additions per year

	Count of Additions
Date	
2009	0.15081062
2010	0.06749712
2011	0.127652302
2012	0.132771773
2013	0.281022235

7.1.6.4 Analysis

The numbers do not show a significant statistical support of the hypothesis. The correlations are too small to signify anything. This means that the hypothesis that higher school enrolment rate show a larger number of C&Cs is not statistically supported.

There can be a number of reasons why this is the case. Firstly, the dataset provided by the World Development Index [13] did not have the rates for all countries. Countries such as India did not have any rates. This compromises the accuracy of the measurement.

Furthermore, countries such as Sweden and Iceland, have a large enrolment rate, however they do not produce many C&Cs. This does not mean that the hypothesis is not true, the causal correlation may still hold, however statistically it does not hold for the online ZeuS C&C variability.

Furthermore the correlation is higher in later years than in earlier years. This could be a result of more data being available regarding the C&C counts. In the years up to 2013 there were relatively few additions, compared to the years 2014 and 2015. This also means that the measurements are less accurate.

7.1.7 Cybercrime Rates

These rates are taken from the IC3 [5] and describe the number of complaints files related to cybercrimes.

7.1.7.1 Actors involved

The actors involved in this metric are the cyber criminals. It can possible be argued that another actor is the victim of the crime. Many cybercrimes go undetected, for reasons such as embarrassment or unknowingness. This does not affect the study of this paper.

7.1.7.2 Driving factors

There are many factors which affect the rates of cybercrimes. A complete analysis is beyond the scope of this paper.

7.1.7.3 Statistical correlation

The rates for Cybercrime have been taken from the IC3 source [5]. The dataset covers the monthly number of reported incidents in the year 2014. The year 2014 shows a large dataset for the C&C additions (1/5 of the total C&C additions over 5 years). Thus the sample data is large enough to calculate a correlation.

Table 9: Correlation between Cybercrime rates and C&C additions

2014	*C&C additions*	*Reported crimes*
C&C additions	1	
Reported crimes	-0.0588969	1

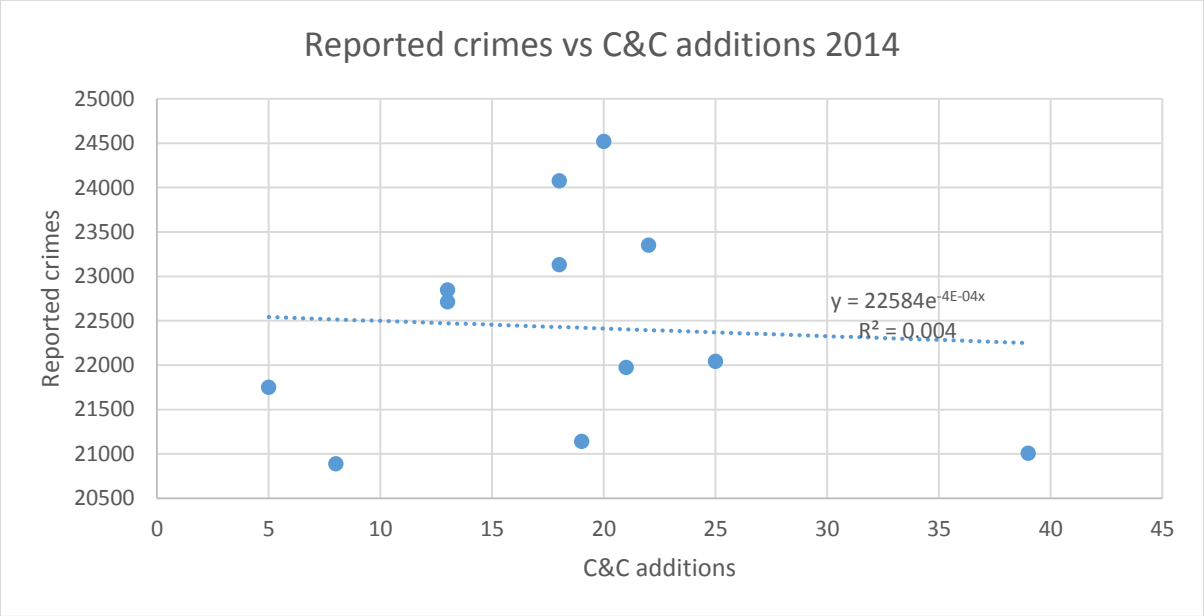

Figure 7: Grouping of C&C additions based on Reported Crimes in 2014

7.1.7.4 Analysis

The numbers show a statistically high low level of correlation. This would not support the hypothesis that either increases in C&Cs lead to higher crime rates or vice versa. The actual hypothesis bears the assumption of a snowball effect in botnet related cyber incidents. However, looking at the scatter plot, figure 6, reveals that there the Reported Cybercrimes behave randomly with respect to C&C counts.

Reasons for this are that cybercrime statistics are not limited to botnet related crimes. Furthermore, botnet related incidents may go unnoticed and therefore may never get reported. This leads to a certain asymmetry of information. It also shows that it is hard to relate actual evidence of criminal behaviour to the number of reported cases.

7.1.8 Botnet Takedown Operations

The list below provides several botnets and the dates of either when they were dismantled or a takedown operation was conducted on the pertinent botnet.

Table 10: Botnet takedowns and their dates

Date	Takedown operation
3FN	June 2009
Lethic & Waledac	February 2010
SpamIt Closure	July 2010
Bredolab	November 2010
Rustock	March 2011
Grum	July 2012
GameOver ZeuS	July 2014

7.1.8.1 Actors involved

There may be many different actors involved in a takedown operation. Examples are: law enforcement agencies, security companies, ISPs, governments and universities. These actors may cooperate to organize a takedown.

7.1.8.2 Driving factors

The main factor driving botnet takedowns is to tackle the security issue of C&Cs and people falling victim to malware.

7.1.8.3 Correlation and Analysis

The graph below shows the monthly removals rates of ZeuS C&Cs. Furthermore several major takedown operations or botnet closures have been marked.

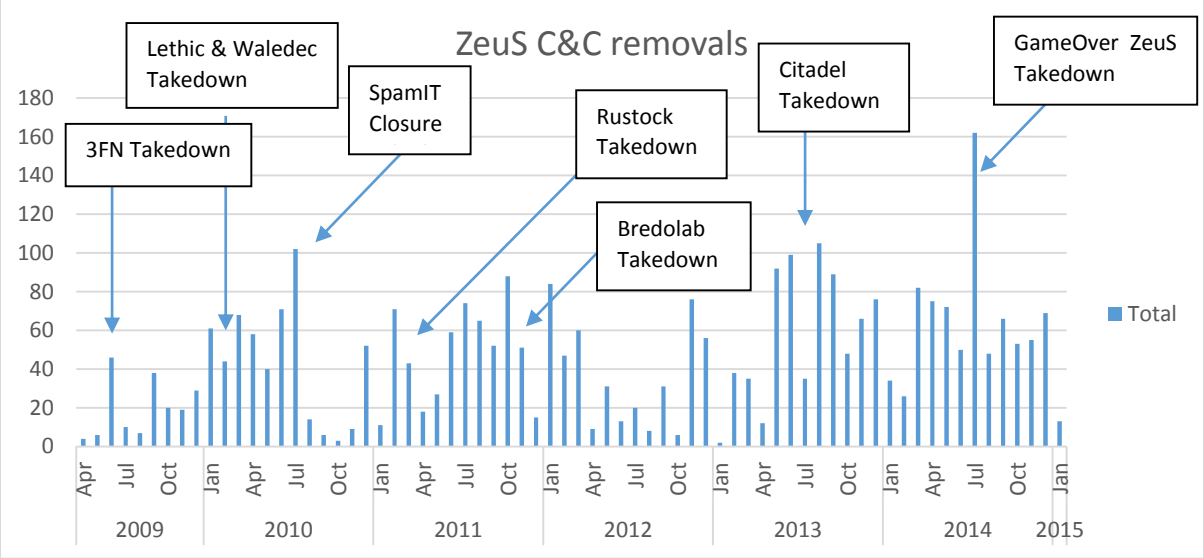

Figure 8: ZeuS C&C removals

It can be seen that the takedown operations directly related to ZeuS, the GameOver ZeuS takedown in July 2014, directly affected the removal rates. There is a large spike and a total of 162 removals were made. The previous record of the number of removals was 105, which occurred in August 2013. This new high occurred after a takedown operation by the FBI and Microsoft on the Citadel Botnet, which is a variant of ZeuS.

The graph shows that large takedown operations are correlated with a large number of removals. This is not the case for all operations. For example the Grum takedown, which is not on the graph, happened in July 2012. No significant amount of removals were noted in the ZeuS C&Cs.

However the way C&C counts behave after botnet takedowns varies significantly per operation or closure. For example, the closure of SpamIT shows a significant number of removals in the month of

July 2010. However, the number of removals drop significantly the months after. This, for example, is not the case with the Rustock takedown, where removals are high and steady, and only cool down in the second quarter of 2012.

It can also be noticed that the takedown operations of botnets which are versions of ZeuS produce a larger effect than botnets which are not related. For example the Rustock takedown has a smaller number of removals than the related GameOver ZeuS takedown.

7.2 Analysis of the results

Of the different socio-economic and socio-technical factors analysed, only few showed a statistical correlation. The unemployment rate showed a strong negative statistical correlation, however it was shown that this correlation was caused by other factors than real wage unemployment. The following factors: access to electricity, Internet users per 100 people, R&D expenditure, secondary school enrolment and cybercrime rates, do not show any significant statistical correlation.

The socio-technical factor of botnet takedowns was qualitatively analysed and it could be seen that takedown operations had an effect on the number of C&C removals. Botnet removals related to the botnet in question show larger effects.

7.2.1 Implications

The results imply that socio-economic factors do not influence the variability of online C&Cs. Factors such as employment, the economy and health of a country are not significantly related to C&Cs. This means that in order to gain a better understanding of C&Cs and their variability, research must be done in other areas. For example, the cyber infrastructure of a country might reveal more about the security issue in question.

7.2.2 Relevance of the results

This paper will help studies in the future to discern which factors play a role in botnets. C&C infrastructures is a complex subject. Knowledge about which factors may affect these structures may help in studies about botnets, criminal behaviour, cybercriminal trends etc.

7.2.3 Limitations

There were several limitation when conducting the experiments; mainly concerned with the dataset. Not all addition/removal entries were provided with country codes. This limited the sample size and reduced the accuracy of the analysis. Furthermore, the datasets of several factors were incomplete. For example the secondary school enrolments missed rates from countries such as India. The reason for this may be that such countries do not a have a system which classifies a secondary school. Furthermore, a lot of the data that was available was not actual; so did not include rates from 2015.

8 CONCLUSION

This paper looked at whether socio-economic and socio-technical factors influence the online variability of C&Cs. In particular the C&Cs of ZeuS were analysed. The security issue was identified as the increase of C&Cs, which leads to spreading malware as well as financial losses (in the case of the ZeuS Trojan).

Seven factors, which had a plausible causal correlation with the security issue, were analysed and statistically correlated to the dataset. Socio-economic factors did not show a statistical correlation with the dataset. The socio-technical factor, botnet takedowns, show a qualitative relation with the removals of C&Cs.

It can be concluded that socio-economic factors have very little, if not no, influence on the variability of online C&Cs. The limitations of the datasets did not allow for all factors to be analysed equally

accurate. However further research can look into factors which were not analysed here as well as include data which has thus far not yet been published.

9 REFERENCES

[1] Abuse.ch

[2] Alazab, M., Venkatraman, S., Watters, P., Alazab, M., & Alazab, A. (2012). Cybercrime: The case of obfuscated malware. *Lecture Notes of the Institute for Computer Sciences, Social-Informatics and Telecommunications Engineering*, *99 LNICST*, 204–211. http://doi.org/10.1007/978-3-642-33448-1_28

[3] Barroso, D. (2007). Botnets-the silent threat. European Network and Information Security Agency (ENISA), 15, 171.

[4] Eeten, M. Van, Bauer, J. M., Asghari, H., Tabatabaie, S., & Rand, D. (2010). The Role of Internet Service Providers in Botnet Mitigation An Empirical Analysis Based on Spam Data 1. *Workshop on Economics of Information Security*, *2010/05*, 1–31. http://doi.org/10.1787/5km4k7m9n3vj-en

[5] Federal Bureau of Investigation Internet Crime Complaint Centre (IC3). www.IC3.gov

[6] Financial Secrecy Index. https://www.financialsecrecyindex.com

[7] Kemmler, A. (2007). Factors influencing household access to electricity in India. *Energy for Sustainable Development*, *11*(4), 13–20. http://doi.org/10.1016/S0973-0826(08)60405-6

[8] Kleiner, A., Nicholas, P., Sullivan. K. (2013) Linking Cybersecurity Policy and Performance. Microsoft Trustworthy Computing.

[9] Ormerod, T., Wang, L., Debbabi, M., Youssef, A., Binsalleeh, H., Boukhtouta, A., & Sinha, P. (2010). Defaming botnet toolkits: A bottom-up approach to mitigating the threat. *Proceedings - 4th International Conference on Emerging Security Information, Systems and Technologies, SECURWARE 2010*, 195–200. http://doi.org/10.1109/SECURWARE.2010.39

[10] Raphael, S., & Winter-Ebmer, R. (2001). Identifying the Effect of Unemployment on Crime. *The Journal of Law and Economics*, *44*(1), 259–283. http://doi.org/10.1086/320275

[11] Rossow, C., Andriesse, D., Werner, T., Stone-Gross, B., Plohmann, D., Dietrich, C. J., & Bos, H. (2013). SoK: P2PWNED - Modeling and evaluating the resilience of peer-to-peer botnets. *Proceedings - IEEE Symposium on Security and Privacy*, 97–111. http://doi.org/10.1109/SP.2013.17

[12] United Nations Educational, Scientific, and Cultural Organization (UNESCO) Institute for Statistics.

[13] World Development Indicators. http://data.worldbank.org