A Continental Dependency of the Tinba Botnet

Wesley van der Lee
Faculty of Electrical Engineering, Applied Mathematics and Computer Science
Delft University of Technology, the Netherlands
As final submission for *Economics of Cybersecurity* in MSc. Computer Science specialization Cyber Security

***Abstract*—Botnets pose a real threat to society, as legitimate computer owners cannot fully control their infected computers. Moreover their computers are 'zombied' until they are used for malicious purposes, which may contain sending spam and committing banking fraud. Research on the botnets is needed in order to effectively mitigate these botnets. Research on botnets is mainly done by analyzing the functional characteristics and effects of botnets. Preliminary research on geographical incident data created the urge that some types of botnet occur mainly in one region or continent, this is in particular the case for the Tinba botnet in Europe.**

This paper provides a method to investigate botnets that deviate from the average geographical distribution and introduces the notion of 'continental dependency' in order to investigate this manner. Continental dependency is used to show that Tinba, with respect to geographical average botnet distribution (non-isolated), is indeed mainly represented in Europe.

***Index Terms*—botnets, Tinba, geographical botnet distribution, continental dependency.**

I. Introduction

A botnet consists of a network of 'zombied' computers. The computers are said to be 'zombied' because the rightful owner does not control the computers anymore. The person who does control the botnet, eventually controls the 'zombied' computer and he will probably abuse this control for malicious intentions [1]. Malicious intentions may imply banking fraud, sending spam, launching distributed denial of service attacks, etc. One of the possible ways to conduct banking fraud, is by stealing financial data and credentials. The Tinba botnet type family is one of many types of botnets that is able to collect this data and communicate this back to the corresponding Command&Control Center; a center where commands can be issued by the botnet owner [2].

Since a botnet's only intention is to be used for malicious purposes, these threats need to be mitigated. This can be achieved on the level of the end-user by applying anti-virus software, until the level of country regulations; the governance, where botnet mitigation strategies find the shape and funding that is needed in order to deploy an organized botnet mitigation strategy. The most pragmatic part of botnet mitigation strategies lie somewhere in the middle, on an the level where the so called Critical Internet Resources are located, on the level of Internet Service Providers (ISPs) and Autonomous Systems (Ass) [3]. While some ISPs and ASs lack the role of botnet mitigation due to financial shortcoming, effective botnet mitigation on this level depends on collaboration and exchange of resources (information) between ISPs and ASs.

Luckily there are ISP and AS collaboration platforms, one of which is The SpamHaus Project [4]. The main objection of the SpamHaus project is to maintain and provide a blacklist database of malicious hosts and IP-addresses, a DNSBL (Domain Name Server Blacklist). The hosts and IP-addresses are malicious because they are used for sending spam on a large scale and often achieve this because they host a botnet. The SpamHaus Project is able to exist because it extensively collaborates with many ISPs and has many sponsors, which can be seen on *www.spamhaus.org/organization/sponsors*. Together with ISPs, The SpamHaus project is able to conduct research on spam sending botnets, and is thus able to apply a level of mitigation.

It becomes apparent that botnet mitigation starts with understanding the botnet. This paper investigates geographical characteristics of botnets based on incident data retrieved from SpamHaus. The Tinba type botnet in particular will be the central point of discussion. Geographical characteristics are under investigation in a continental context, where possible classification of the botnet based on the botnet's geographical distribution may be the result. Since active botnets are the result of numerous factors, i.e. legislation, motivation and purposes, which determine the existing difference between all types of botnets, botnets should not be considered in isolation, but rather in a derivative of one another. For this reason this paper also talks about an average continental botnet distribution which may lead up to the introduced notion of continental dependency. Continental dependency will be introduced in section 4 and applied in section 5.

The further outline of this paper is as follows, section 2 provides a brief overview on literature on the Tinba botnet and existing information about geographical relevance for botnets. Section 3 states the research question regarding the Tinba botnet and to what extend this question can already be answered. Section 4 introduces the fine methodology which will be applied to deeper investigate the geographical distribution of botnets. In this section a formal definition of continental dependency will be given and justified. Section 5 discusses results that are retrieved after applying the proposed methodology. Section 6 states some encountered limitations during this research and provides some future work references. Section 7 will form a conclusion to answer whether or not continental dependency of the Tinba botnet holds.

II. Literature Review

There is limited literature available on either geographical classifications of botnets or in particular the Tinba type botnet. This section will discuss some researches that have tried to deeper investigate either one of the two areas of relevance to this paper.

The first and most informative data on the Tinba botnet is an empirical research conducted by Sood [5], where different financial botnets have been compared to one another. However this research mainly focusses on the HTTP characteristic of a botnet, one key characteristic is worth extrapolating from this paper. Namely the classification of the Tinba type botnet to be a financial botnet, is of essence for further conducted research. The classification Sood made regarding the Tinba botnet, enables further research to broaden the research perspective to also include financial botnets.

The Counter Threat Unit (CTU) of Dell SecureWorks has done some research regarding countries that are targeted by financial botnets, of which Tinba is one of them. In their work of last April, they conclude that financial botnets shifted more towards Asian countries, because banking security was less developed and implemented in these countries compared to others [6]. The Unit of Dell SecureWorks also plotted the number of incidents per country caused by a financial botnet. This figure shows that Tinba mainly targets the countries Japan and US and relatively speaking, leaves all other countries unharmed.

An even more recent study from the CTU of Dell SecureWorks, contradicts their preliminary findings from April. This new study states an increase of Tinba type botnet incident rate [7]. They conclude that this is an unexpected development in banking fraud. CTU states that many creators of financial pervasive botnets originate from Russia or other Eastern European countries and historically spoken, botnet owners are not keen to target banks in their own countries. This is mainly due to obvious legal prosecution reasons, where botnet owners tend to be easier prosecuted in their own country, because in that case there are no jurisdictional boundaries present. For some unexplainable reason, owners of the Tinba botnet breach this trend.

Supporting Dell's CTU's most recent work, Europol also concludes that the European Union will be a key target for cybercriminals, due to Europe's Internet-mediated economies and digitally advanced payment systems [8]. Europol concludes that especially European Union citizens will be will be subjected both to a larger volume of cyber-attacks, and to attacks from previously under connected areas of the world. The latter two even more than is the case compared to citizens of other continents.

Originating from May 2015, IBM Security Trusteer researchers discovered an infection campaign that mainly targets European banks [9]. Countries within Europe that suffer the most in numbers of incidents from this campaign are Poland, Italy, the Netherlands and Germany. According to the IBM researches, Tinba is just one of the many malware threats that have migrated to Europe after previously targeting banks in the United States. Incident reporting on news websites also contribute to this trend. News reports from 2014 related to Tinba mainly discuss U.S. banks to be victimized, such as [10], while more recent incident reports such as [11] mainly consider European countries to be a victim of the Tinba type botnet. This would suggest that specific targeting campaigns have moved from the United States to Europe.

Further research performed by Zhuang also shows a brief discussion stating a surprising result in their findings on the geographical distribution on spam sending botnets. They conclude that according to their methodology European countries as Spain, France and Italy contain more bots than Asian countries such as China and South-Korea. This is mostly due because Zhuang concludes that the number of bots in a country does not automatically mean a higher incident rate [12]. This seems true and relevant because botnets can be inactive, or send spam on a lower frequency basis in order to avoid suspicion. It is thus of essence to distinguish whether incident events or botnet sizes are discussed.

The last point of importance has been noted by Amoroso, where he states that information about botnet spreading tactics can be derived from the botnet's geographical distribution [13]. Given a geographical distribution, one can search for hints that caused the botnet to spread, i.e. some type of social engineering or lure. Although hints can be searched for, Amorose also states that in many cases a geographical distribution provides no useful information. The latter is due to the fact that botnet controllers tend to be 'randomly' spread across the whole world, because botnet distribution is driven by opportunistic hacking.

The main reason for botnets and in particular Tinba to exist is because of the spreading capabilities. The Tinba type botnet listens for commands originating from a Command&Control center (C&C center), and acts upon these commands. Moreover, since the purpose of Tinba is to steal (financial) credentials, logic dictates that these are also communicated back to the C&C center. Credentials are obtained by means of a Man-In-The-Browser attack, encrypted using a RC4 symmetric encryption and then communicated back to the C&C center [2]. The reason why this may be important is because reverse engineering of different Tinba botnet variants, shows the sets of encryption keys, which has then been used to determine the domains which Tinba uses to contact the C&C. The reason why this may be of geographic importance, is because all domains lead to a single IP address, located in Lithuania, a European country [2]. This same document also states that in 2012 more than `60.000` machines in Turkey alone appeared to be infected with Tinba.

In conclusion one can say that incidents due to Tinba on a more recent timeframe are manifested in European countries. This differs from incident data originating from one year earlier; where U.S. banks were mainly targeted by the Tinba type botnet. The discussed data of recent incident reports is often based on a direct number of registered or predicted incidents, never on a model where incidents are normalized

by some factors. Because of this reason, no other studies have significantly tried to map Tinba incidents to any hot zones or analyze thoroughly geographical distributions of Tinba.

III. Research Question

As becomes apparent from the previous sections, botnets pose a serious threat over the whole world. Some type of botnets are more widespread than other types of botnets. The *Conficker* type botnet is by far the largest botnet in absolute size [14]. An earlier study on incident data retrieved from The SpamHaus Project [4] contributes to the fact that Conficker is the largest botnet over the whole world [15]. This study also shows that other types of botnet are more existing in several countries and regions compared to other botnets. Although this study only focusses on the top 20 worst countries in the world, one may point out some interesting piece of trivia from the geographical distribution of the top 10 largest botnet types over the top 20 worst countries: The Tinba type botnet is mainly present in countries such as Russia, Poland, Denmark, Spain and Indonesia, and almost vacant in any other worse scoring countries. Except for Indonesia, one may conclude that all other countries are members of the European continent. For explanatory purposes, Figure 1 shows the result of the botnet type distribution of the top 20 worst scoring countries from [15].

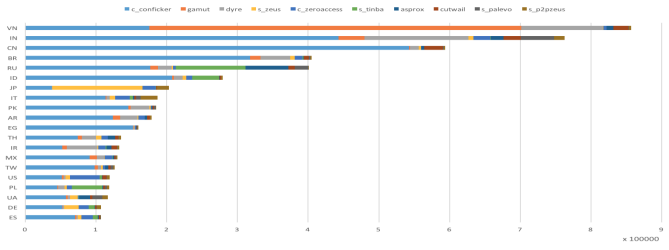

Fig. 1. Botnet Type Distribution of the top 20 worst scoring countries

The Tinba type botnet may or may not impact the European continent heavier than other continents. A geographical analysis on the distribution of certain botnets is useful in order to gain more insight and knowledge about the botnet. This in turn is needed in order to define botnet mitigation strategies. In order to determine whether the Tinba type botnet is a true European botnet, the geographical distribution of Tinba over whole world will be assessed. The main objective of this paper is to determine whether geography influences the distribution of the Tinba type botnet compared to other botnets. If a botnet is mainly present in a certain continent, for innovative purposes we say that a Botnet has a continental dependency to that continent. The main research question in this article is to determine whether or not Tinba has an continental dependency on Europe. In order to answer this question, one should formalize continental dependency, which will be done in the next section. As has been discussed before, Tinba mainly appears in European countries when the 20 worst scoring countries are considered. A preliminary hypothesis would therefore state that geography indeed influences the Tinba botnet distribution over the world, because Tinba mainly contributes to countries in one continent, namely Europe. The expectancy of Tinba to be mainly manifested in Europe, does not only follow from extrapolation of Figure 1, Dell SecureWorks also see an increase of Tinba incidents in European countries [7].

IV. Methodology

In order to conclude whether the Tinba botnet has a certain continental dependency, global incidents should be analyzed. This paper will continue on the obtained incident dataset from SpamHaus [4]. The dataset is compromised over 10 million registered incidents related to spam sending botnets. The provided information in the dataset is limited to approximately a month, the incidents occur between August 11, 2015 until September 12, 2015. For each incident a timestamp, country of source and a botnet type has been provided.

As the first step to be undertaken in order to analyze the dataset, for each country, the number of registered botnet incidents per different botnet type should be computed. This is the most essential part of the whole methodology, because all later phases of research depend on the ability of a mapping of types of botnets to continents. Secondly the number of incidents regarding the Tinba will be quantified. A quantification of the number of incidents of Tinba can be achieved by accumulating for each continent the number of incidents of all containing countries. This is needed in order to determine whether the urge for the hypothesis, namely that Tinba has an European continental dependency, is founded or not. The hypothesis has been conceived based on the fact that for the top 20 worst countries, the Tinba type botnet mainly occurs in countries that are a member of the European continent. The hypothesis might be false if Tinba just occurs in European countries that are in the top 20 worst rated countries, but can not be related to the rest of Europe. During this phase of analysis, for each continent we will also normalize Tinba occurrences by the number of Internet users. This is also of essence for the investigation on the continental dependency of Tinba, because the number of Tinba botnet incidents in Europe does not weigh equal to the number of Tinba botnet incidents in Oceania. The absolute number of incident occurrences is expected to be larger in any country with a higher Internet user population, than the number of incidents compared to an other country with a lower Internet user population. This case is analogue for continents.

After the distribution of Tinba incidents have been quantified all over the globe, in order to determine whether a botnet has a continental dependency, for which a formal definition will follow in a moment, the world distribution needs to be visually graphed per continent. However a certain plot of the Tinba distribution around different continents does not say anything when considered in isolation. Other types of botnets need to be considered as well. The latter is of utmost importance, because one can argue that botnets follow a certain continental botnet distribution, which then is just the average of all distributions of all botnets per continent.

If for example the number of incidents normalized by the number of Internet users, peak for some continent, this could only lead up to a continental dependency if other botnets on average do not contribute to that peak. To avoid conclusions based on false contributions, now is the moment to formally introduce continental dependency. Continental dependency for a certain botnet b and a certain continent c holds, if and only if the ratio of contribution of incidents of b in c by the sum of all botnet incidents from b not in c is greater than one. In formal notation:
Let B be the collection of all types of considered botnets and C be the collection of all continents. Continental dependency for a botnet type $b \in B$ in continent $c \in C$ holds iff:

$$\frac{\#(b,c)}{\sum_{i=1}^{|C|} \#(b,C_i)} > 1, \text{ where } C_i \neq c \qquad (1)$$

In this formal definition of continental dependency, $|C|$ is the size of C, which is most often 6 for $C = \{Europe, Asia, NorthAmerica, SouthAmerica, Africa, Oceania\}$ and $\#(b,c)$ is defined as the number of incidents of the dataset for botnet type b in continent c. In order to achieve statistical domestenic information, the number of incidents given by $\#()$-function have been normalized by:

1) the number of Internet users per continent, as has been discussed before;
2) the number of total botnet occurrences over all continents.

The latter normalization is of importance, because continental dependency states the geographical distribution of a botnet in comparison to the so called botnet 'blueprint' distribution: the distribution shape of all botnets on average. In the following section where the results are discussed, the reason why botnets per continent are also normalized by their total size becomes apparent.

V. Results

As described in the previous section, the first step to be undertaken is to make eligible sense of our dataset, we need to accumulate the number of incidents for each country and for each botnet type. A table of `232` countries by `106` known types of botnets is the result. Each entry in the table describes the number of registered incidents per country as a row and per type of botnet as a column. From this table a direct quantification of the Tinba botnet type can be made. Since the research in this paper is limited to the research of whether Tinba has an European continental dependencies, the incidents have to be accumulated for each continent. The continental accumulation and normalization is visible in Figure 2.

The first x-point in the figure is the non-normalized number of incidents. One can immediately derive from this figure that Europe as a continent contributes by far the most to the total number of incidents registered to the Tinba botnet. This fact highly supports the stated hypothesis that Tinba is overall represented in Europe. The sum of all Tinba incidents in other continents does not even outweigh half of the Europe incidents. Second continent in place of absolute Tinba incident

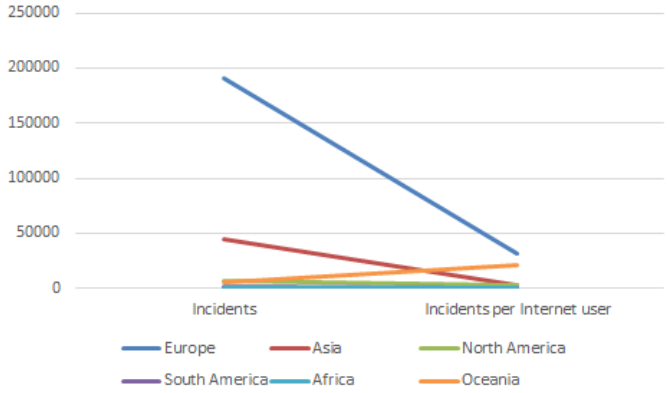

Fig. 2. Tinba Incidents per Continent

contributor is Asia. As explained in the previous section, a ranking of Tinba incident contributions is unfair based on direct incident quantification, such that the incident number is left non-normalized. This is unfair because Europe and Asia also contribute to most part of the internet population all over the world [16]. Logic would then dictate that it only seems reasonable that Europe and Asia both would contribute to most part of Tinba incidents. Hence the number of incidents have been normalized by the number of Internet users per continent, which is made visible on the second x-point. In order to remain a graphical overview, the results after normalization have been amplified with a constant factor (`100.000.000`). One can immediately conclude that both Europe and Asia drop in rate rapidly, while Oceania grows. This is a logical consequence after normalization with the number of Internet users per continent, because after extrapolation of [16], one can conclude that Europe and Asia respectively have more than 22 and 57 times the number of Internet users in Oceania.

A closer look on the normalized Tinba incident values in Figure 2, does not support the hypotheses. While Tinba incidents non-normalized initially occurred `3.2` times more in Europe than in all other continents together, after normalization the rate drops to only `1.2`. Is it then still a possibility to confirm the hypothesis? Or does the fact that after normalization the number of Tinba incidents only appear `1.2` more in Europe than in the rest of the world argue that there is no geographical relation tied to the Tinba botnet? It is then best practice to turn to the proposed methodology to investigate the continental dependency of a botnet proposed in the previous section.

Figure 3 maps incidents of the Tinba botnet to the corresponding countries of origin of incidents. Moreover, countries with a larger number of incidents are associated with a larger blue circle on the map, in order to depict the incident rate. Note that we are able to speak about an incident rate since all incidents have been recorded in the same timeframe. A preliminar view on the map also shows that Europe is the main victim of the Tinba botnets. This also contributes to the hypothesis that Tinba is mainly manifested in Europe.

Fig. 3. Tinba Incident Distribution over the World

Bot Type	Nr. of incidents
Conficker	4.062.868
Dyre	791.165
Gamut	700.524
ZeroAccess	359.261
Zeus	259.033
Tinba	249.903
Asprox	236.501
Palevo	179.129
Cutwail	174.158
p2pZeus	173.271
Kelihos	120.334

TABLE I
BOTNET TYPES AND THE TOTAL NUMBER OF REGISTERED INCIDENTS

However this map does support the hypothesis, at this point the reason why the determination of continental dependency should be conducted considering multiple types of botnets, becomes clear. It is namely impossible to draw any conclusions from this map, because the degree of variance of other types of botnets is not clear. If many other types of botnets follow a geographical distribution similar to the one depicted in Figure 3, then this might just be some overall botnet characteristic rather than a characteristic of the Tinba type botnet.

The method proposed to determine continental dependency for a botnet, first of all states that it should be compared to other botnets. Since the available dataset is comprised of 106 botnet types, it would be cumbersome and meaningless to investigate Tinba against all known botnet types from the dataset. These would have no meaning since many types of botnets comprised of too few incidents to derive the average botnet distribution, the so called 'blueprint' distribution as introduced in the previous section. For the empirical relevance of this study, the Tinba type botnet is compared to other botnets with a total incident count larger than 100.000 in order to conclude that their geographical distribution contributes to the blueprint distribution.

Table *I* shows the botnet types which have a higher overall incident occurrence of 100.000, so their geographical incident distribution becomes of significant relevance for the 'blueprint' distribution. Note that Tinba is in the list as well, so the geographical of Tinba is also significant, hence the geographical distribution of Tinba can be compared in a size meaningful way. Since Table *I* is compromised of 11 botnets, further discussion in this paper discusses only these 11 types of botnets: Conficker, Dyre, Gamut, ZeroAccess, Zeus, Tinba, Asprox, Palevo, Cutwail, p2pZeus and Kelihos.

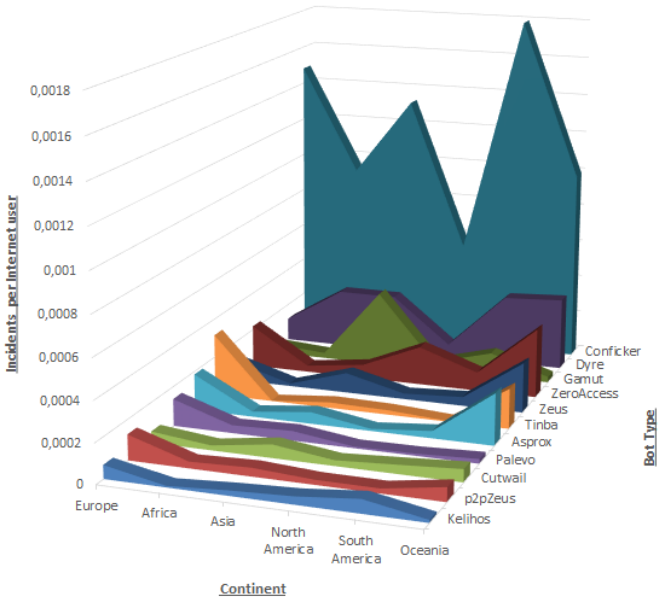

Fig. 4. Continental distribution of the largest botnets normalized with Internet users per continent

In order to determine continental dependency for the Tinba type of botnet, one shall first of all determine the geographical botnet distribution of all botnet types. This is shown in Figure 4, where the accumulated number of incidents for each continent have been normalized by the number of Internet users for that specific continent. From this figure, no meaningful data can be extracted about the Tinba botnet. This is mostly due to the fact that the Conficker type botnet consumes all graphical space. The reason for Conficker to consume that lot of space, is because Conficker is the largest botnet in size, which is commonly known [17]. For this exact reason, accumulated incident data per continent should not only be normalized with the number of Internet users per continent, but should also be normalized by the total incident occurrences of the botnet over the whole world. This is important because continents are not the only variables that are under investigation, but from this point, botnets are compared as well. Figure 5 shows these results normalized with respect to the global number of incidents per botnet type.

A close look at Figure 5 shows two different type of botnet distribution blueprints. One of which is essential for the shape of the global Tinba distribution. Botnets of this type of blueprint show a significant peak only in Europe and Oceania. Apart from Tinba other types of botnets that follow the same blueprint are ZeroAccess, Zeus, p2pZeus, Asprox and Palevo. Other botnets follow a second type of global distribution,

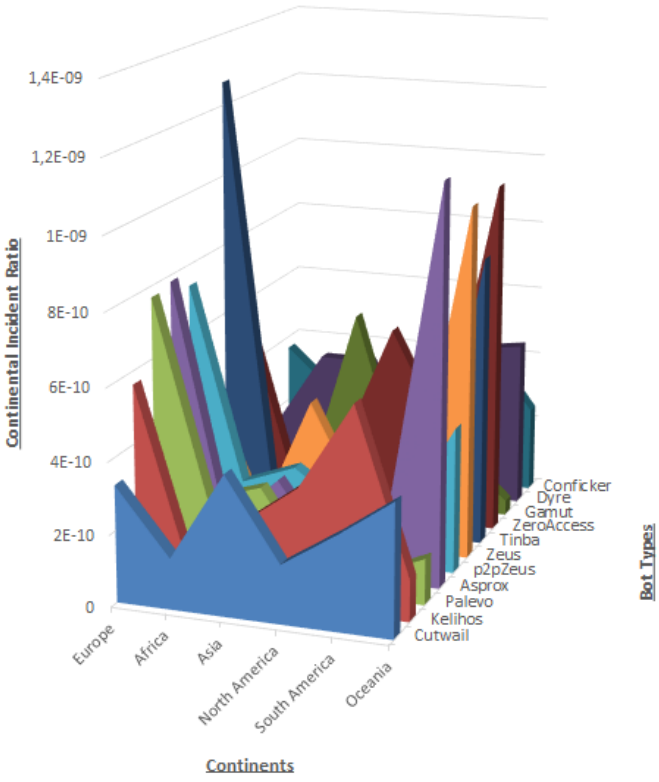

Fig. 5. Continental distribution of the largest botnets normalized with Internet users per continent and botnet size

where Asia significantly peak out and other continents score not significantly higher than Asia. Botnets corresponding to the latter described blueprint are Cutwail, Kelihos, Gamut, Dyre and Conficker. Since the purpose of this paper is to investigate whether the Tinba botnet has a continental dependency, rather than a classification of continental distributions, the distinction in blueprints will not be discussed any further.

It is of essence to compute per botnet type the incident rate of each continent compared to the sum of incident occurrences of all other continents, in order to determine whether the Tinba type botnet has a continental dependency to Europe. If the mathematical expression of section 4 (equation (1)) is applied to this resulting dataset then $C = \{$ *Europe, Africa, Asia, North America, South America, Oceania* $\}$ and $B = \{$*Conficker, Dyre, Gamut, ZeroAccess, Zeus, Tinba, Asprox, Palevo, Cutwail, p2pZeus and Kelihos* . Now for each botnet $b \in B$ the following is computed:

$$\frac{\#(b,c)}{\sum_{i=1}^{|C|} \#(b,C_i)}, \text{ where } C_i \neq c.$$

which results in a table that states for each type of botnet the continental representation ratio. Since the continental incident ratio should be larger than 1 for a specific type of botnet b in a certain continent c, for a continental dependency to hold, the continental representation ratio can be plotted per continent together with a boundary line on $y = 1$. The results are shown in Figure 6.

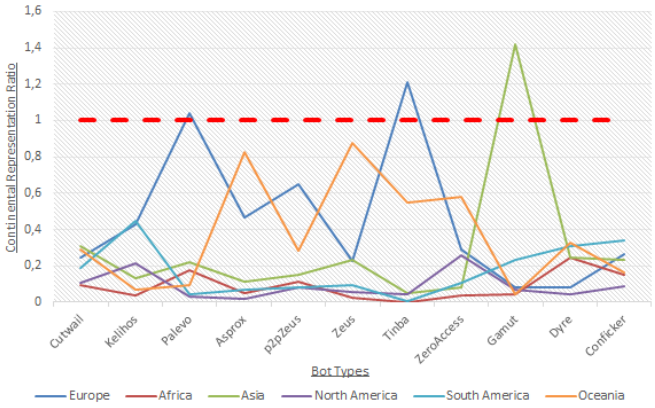

Fig. 6. Continent Representation Ratio for Top 11 Types of Botnets with Boundary Line

Figure 6 shows the continental representation level for each continent, where 11 botnet types have been considered. This figure also shows a boundary line. If some continent c for some botnet type b scores above the boundary line, this means that equation (1) from section 4 holds, thus stating that b has a continental dependency on c. From the figure can be derived that of the top 11 botnets, this only is true for 3 types of botnets, namely Palevo, Tinba and Gamut. The Palevo shows a tiny peak, just above the boundary line in continent Europe, we can thus state that the Palevo botnet has a continental dependency on Europe. Tinba shows a clear peak far above the boundary line, so Tinba is also continental dependency on Europe. Lastly the Gamut botnet has the highest peak even more significant above the boundary line for Asia, so Gamut has a continental dependency on Asia.

Since the main focus of this paper is about the geographical distribution of the Tinba botnet, the results about Palevo and Gamut will be disregarded for further discussion, but follow an analogue conclusion. This paper shows that for botnet type Tinba, the Continent Representation Ratio is higher than the boundary line on $y = 1$ for Europe, thus Tinba is continental dependent on Europe. But what does this say, for Tinba to be continental dependent to Europe? This means that the number of incident occurrences are that much represented by countries from the European continent, that the botnet type mainly has a right to exist, because it is manifested in this continent. The latter is based on the fact that all other continents together, cannot cause the ratio of occurrences with respect to the botnets' blueprint for a certain continent to be larger than the occurrences in the continent itself.

VI. Limitations

This section will state some limitations to the research that has been done in order to construct this paper. There are two interesting points that may be worthwhile to further investigate. First of all, Figure 5 visualizes the geographical distribution of different type of botnets. As stated directly after this

figure, one can extract two rough types of 'average blueprints' which can serve as a botnet classifier. Literature does not show botnet classification based on geography distribution with respect to these averaged 'blueprints', which may turn out to be very useful for further classification. As discussed in section 2, literature had shown that botnets tend to spread opportunistic rather than strategical. Because of this reason, Amoroso concludes that no useful data can be extracted from geographic botnet distributions. On the other hand, Figure 5 does provide two clear classifications of the distribution. It may turn out worthwhile to deeper investigate this matter. Future research should thus try to determine these different types of blueprints which then serve as a future classifier. More interestingly for future research is then to relate the geographical classification to other botnet characteristics in terms of identification and mitigation. The latter is of utmost relevance, because the main goal of researching a threat (in this case the botnet), is to gain insights in order to mitigate the threat.

The second limitation of this paper, is that the performed research is limited to continental classification. The same mathematics and normalization methods can be applied on a country-level perspective, where so called 'blueprints' of botnet distributions on country level can be created. For the introductory purpose of continental dependency, this paper chose not to discuss country level analysis, since this would dramatically increase the size and complexity of certain figures. Country level analysis would however show interesting pieces of trivia about certain botnets, especially types of botnets that already show a peek in the Continental Representation Ratio for a certain continents.

Thirdly, this paper has provided a methodology which can be used in order to show that a certain type of botnet and a continent are highly coupled together in terms of geographical incident occurrences. Central to the research question stated in this paper is the dependency of the Tinba type botnet and the European continent. Little research is available on why the Tinba type botnet is so tightly tied to the European continent, the most valuable future work recommendation would be to investigate why the Tinba type botnet is continental dependend on Europe.

VII. Conclusion

Early results, from a preliminary paper by Van der Lee et. al., on the construction of metrics to measure botnets, have shown a partial view of geographical distribution around the globe. Although there only have been 20 different countries considered in this partial view, one can immediately see that there is a strong relation between European countries and the Tinba type botnet. In order to investigate whether there indeed is a relation between the Tinba type botnet and the European country, absolute and non-normalized data on incidents are not sufficient enough. For this exact reason the notion of continental dependency has been introduced and justified in this paper. Continental dependency determines whether a botnet mainly exists in a certain continent compared to the existence of incidents in other continents.

As a result of the deeply conducted investigation, one can conclude that the Tinba type botnet indeed has a continental dependency on Europe, meaning that there is an incident occurrence relation based on geography for the Tinba type botnet. This data is also supported by existing literature. Europol not only predicted that European countries will be a hot zone regarding the number of cyber crimes, other papers also show a surprising increase of botnet incidents, and especially the number of Tinba incidents in Europe as concluded by Dell SecureWorks [7]. The results founded in this paper, only confirms to the found results. Moreover it has shown that next to Tinba, the Palevo botnet surprisingly turns out to be continental dependent on Europe as well. Apart from botnets that are continental dependent on Europe, the Gamut type botnet is continental dependent on Asia.

References

[1] L. Zhang, S. Yu, D. Wu, and P. Watters, "A survey on latest botnet attack and defense," in *Trust, Security and Privacy in Computing and Communications (TrustCom), 2011 IEEE 10th International Conference on*. IEEE, 2011, pp. 53–60.

[2] P. Kruse, F. Hacquebord, and R. McArdle, "Threat Report: W32.Tinba (Tinybanker) The Turkish Incident," http://www.trendmicro.nl/media/wp/tiny-banker-the-turkish-incident-whitepaper-en.pdf, 2012.

[3] D. DeNardis *et al.*, "The emerging field of internet governance," *Yale Information Society Project Working Paper Series*, 2010.

[4] https://www.spamhaus.org/.

[5] A. Sood, S. Zeadally, and R. Enbody, "An Empirical Study of HTTP-based Financial Botnets."

[6] "Banking Botnets Persist Despite Takedowns," *Dell SecureWorks Counter Threat Unit (CTU) Threat Intelligence*, p. 17, Jan 2015.

[7] "Popular Banking Trojan Attacks Top Russian Banks and Russian Payment Service Providers, Reports Dell SecureWorks," *Dell SecureWorks Counter Threat Unit (CTU) Threat Intelligence*, Nov. 2015.

[8] "Europe key target for cybercrime," *Computer Fraud & Security*, vol. 2011, no. 1, pp. 3–20, 2011. [Online]. Available: http://www.sciencedirect.com/science/article/pii/S1361372311700033

[9] O. Bach, "Tinba: World's Smallest Malware Has Big Bag of Nasty Tricks," https://securityintelligence.com/tinba-worlds-smallest-malware-has-big-bag-of-nasty-tricks, June 2015, accessed:November 6. 2015.

[10] T. Robinson, "Tinba variant aimed at U.S., international banks," http://www.scmagazine.com/tinba-variant-aimed-at-us-international-banks/article/371924/, September 2014, accessed:November 6. 2015.

[11] E. Kovacs, "New Variant of Tinba Banking Trojan Targets European Users," http://www.securityweek.com/

new-variant-tinba-banking-trojan-targets-european-users, June 2015, accessed:November 6. 2015.

[12] L. Zhuang, *Security inference from noisy data*. ProQuest, 2008.

[13] E. Amoroso, *Cyber Attacks: Protecting National Infrastructure*. Elsevier Science, 2012. [Online]. Available: https://books.google.nl/books?id=uwko5fHsexIC

[14] S. Shin and G. Gu, "Conficker and beyond: a large-scale empirical study," in *Proceedings of the 26th Annual Computer Security Applications Conference*. ACM, 2010, pp. 151–160.

[15] W. van der Lee, et al., "The SpamHaus Project: Defining Metrics for Botnet Measurement Based on a Cross-Sectional Dataset," http://wesleyvanderlee.nl/papers/10915.pdf, October 2015, unpublished.

[16] " World Internet Users and 2015 Population Stats," http://www.internetworldstats.com/stats.htm, 2015.

[17] H. Asghari, M. Ciere, and M. J. Van Eeten, "Post-mortem of a zombie: conficker cleanup after six years," in *24th USENIX Security Symposium (USENIX Security 15), Washington, DC*, 2015.