EXPLAINING THE DIFFERENCES IN GEOGRAPHICAL DISTRIBUTION OF BOTNETS

Kevin Joseph Syauta
Faculty of Technology, Policy and Management
Delft University of Technology
kevinjosephsyauta@student.tudelft.nl

Abstract

Botnet, or a network of compromised machines, shows a rather negative side-effect of the world's connectivity. By using the compromised computers (bots), many attacks such as spamming, distributed denial of service attacks and click frauds can be easily launched with relatively low cost. Using a private dataset from Spamhaus, this paper tries to find a pattern to explain the geographical distribution of prominent botnets worldwide, by taking into account specific profiles of a country, for example its GDP and its software piracy rate, as well as how the botnet propagates. The results of this paper shows that there is hardly a recurring pattern across different types of botnets, and that these results sometimes contradict with existing findings. Moreover, the factors listed are not enough to explain why botnets are very disparately distributed. Nonetheless, this paper offers many new insights on the distribution of botnets.

I. INTRODUCTION

A botnet (agglomeration of "robot network") is a network formed by machines compromised by malware. Most of the time, these networks are formed unwillingly and unknowingly. It is estimated that 16 to 25 percent of computers connected to the Internet are actually part of botnet [1]. A botnet can range from a couple hundred computers to a few million computers. There are three main components of a botnet [2]: First is the botmaster, which is a person or a group of actors who build and control the botnet. Second, the architecture or infrastructure of the botnet, also known as the Command & Control (C&C) infrastructure. The third component is the network of compromised computer (the "bots").

Botnets are growing concerns because of the potential malicious ends they can bring. These include distributed denial of service (DDoS) attacks against critical targets, malware dissemination, phishing, and click fraud [3]. According to the FBI, botnets have caused over USD 110 billion losses globally up to 2014, with an astonishing rate of 18 new victims per second [4]. A number of botnets have even become a household name, for instance Conficker, which has infected almost every countries in the world, and Zeus, which is more associated with financial attacks. This paper strives to extract information available from the distribution profile of several noticeable botnets. This information will be based on an analysis of a private dataset that captures a snapshot of worldwide

botnets distribution for 30 days. This paper will be organized as follows: Section II will discuss the necessary literature and underlying theory behind botnets, along with its distribution and infection vectors. Section III and IV will respectively present the objective, the research questions, and the methodology of this research. Section V will give a thorough presentation of the results of this research and a discussion on them. In Section VI, the limitations of the research will be explicitly given, and Section VII will conclude the paper with answers to the research questions.

II. LITERATURE REVIEW

II.1 Evolution of botnets and cybercrime

Botnets have not always been notorious. Up to 2004, most bots are connected using Internet Relay Chat (IRC), and were used to log into chat rooms/channels [5]. The Eggdrop botnet is regarded as the most popular IRC botnet. Although most of the time they run on Windows computers, some localized versions of bots also run on Unix and Linux. Then came the era of peer-to-peer (P2P) bots, which marked the transition from a rather benign use of bots to more malicious uses. An example is the Storm worm which was taken down in 2008. More recently, the communication structure of botnet shifted to websites using HTTP (Hypertext Transfer Protocol), which began with advancements in exploit kits to install softwares on remote machines. A famous example of HTTP botnet is Zeus.

Botnets are now closely intertwined with cybercrime. They even have been associated as a "cyborg crime" [2]. Botnets are especially attractive to cyber criminals because they come with high efficiency but at a low cost [6]. When formed, botnets are then used to launch attacks at specific targets. For example, some botnets fall under the category of 'banking botnets' because they attack financial institutions and their customers [7]. Oftentimes they also attack payment service providers and e-commerce institutions. These banking botnets include Dyre, Gozi, Bugat, Zeus (and Gameover Zeus), Tinba, Shylock, and many others.

Botnets are also used to send spam emails. In its latest report, Symantec estimates that there were 28 billion spam emails circulating in 2014, which make up almost 60% of all emails sent in that year. 74% of these spam emails were sent by botnets [8]. There have been a number of newsworthy cases regarding spam, for example the McColo case with its Rustock botnet in 2008, Bredolab botnet which had many servers located in The Netherlands, and the Grum case which showed that botnet infrastructure can actually shift [6].

Although it is not always the case, but botnets can also be used to launch DDoS attacks. These attacks are mostly launched to incur damage at the victim, but they can also be revenge-driven, to gain popularity in a certain community or for material gain [9]. Examples of botnets which have been previously used for DDoS attacks are Agobot, SDBot, RBot, and Spybot [10].

There are more examples of malicious ends that botnets can bring but for now these examples are deemed as sufficient to paint a picture of the potential damage that botnets can entail.

II.2 Botnet infection vectors and distribution

Botnets come with different infection vectors and propagation mechanisms; that is the way they propagate and spread throughout the world. This Symantec summarizes most popular propagation mechanisms into ten different types, namely [8]:

1. Executable file sharing
2. File transfer
3. Remotely exploitable vulnerability
4. File transfer via email attachment
5. File transfer via non-executable file sharing
6. P2P file sharing
7. SQL
8. File transfer via instant messenger
9. File transfer via HTTP, embedded URL, or email message body, and
10. File transfer via MMS attachment

These propagation mechanisms are crucial in determining how easily a worm to create bots can spread and form a vast network. However, propagation mechanisms are not the only factor that determine the distribution of botnet. Sometimes, geographical locations and a country's profile also play important role in. In the case of spam botnets for example, bots located in certain countries are sold for a higher price on the black market. The underlying notion is that bots located in more developed countries will have better Internet connection, and therefore be able to send more spam in the same amount of time [11]. However, other researchers do not agree with this, stating that the less-developed countries are actually more infected with spam botnets than developed countries [12].

A country's wealth also plays important role in its propensity of being targeted. For example, banking botnets tend to target financial institutions in developed countries with sizable populations and wealthy residents [7]. Bots located in a richer country are believed to be more advantageous in certain cases, for instance in the case of an information stealing-botnet [12].

Software piracy is also associated with the occurrences of bots in a country. The majority of cracks and serial number generators are circulated with the intention of infecting computers with malware [13]. Therefore, it is expected that higher number of software piracy in a country will directly correlate with the number of bots in that country, especially in malwares with executable file sharing as its main propagation mechanism. Percentage of individuals using the Internet is depicted as part of ICT intensity and usage and is a metric to measure the development of ICT in a country [14]. This metric may show relation towards the number of bots located in a country.

III. OBJECTIVE AND RESEARCH QUESTIONS

The objective of this research will be to explore the different patterns of geographical distribution that emerge with different types of botnets. More specifically, the connection between botnet propagation mechanisms

and the distribution patterns will be discussed. Consequently, the research questions that will be explored in this research are:

1. Are there any distinguishable patterns or outlying data points of geographical distribution for different types of botnets?
2. How can propagation mechanisms and the country's profile (wealth, software piracy and percentage of individuals using the Internet) explain the distribution pattern of different types of botnets?

The answers to these questions will hopefully provide additional insights in understanding why botnets flourish in certain countries and why they wither in others, and spark ideas for future researches to understand more about botnets.

IV. METHODOLOGY

To carry out this research, a private dataset provided by The Spamhaus Project will be analyzed. This dataset is a cross-sectional snapshot of worldwide active botnets list, capturing data from August 11, 2015 until September 12, 2015. Containing more than five and half million entries, this dataset covers a multitude of parameters, including source IP (Internet Protocol) of the infected machine, identity of the Autonomous System (AS) associated with the bot, the country in which the bot is located, as well as the timestamp when the connection made by the bot was connected. It is also worth mentioning that this research is an extension of the Block 2 group assignment. In that assignment, only a descriptive picture of the geographical distribution was provided, without further analysis on what may have caused the difference in the distribution.

This research will be executed in a combination of quantitative and qualitative manner. From the available data, a subset of majority botnet types will be distilled. Each type of botnet will be plotted in a scatter plot against the size of Internet users in different countries. While these plots will provide a view of the non-normalized data, a normalized view of the data will also be provided. They will come in the form of scatter plots of ratio of compromised machines in a country against the penetration rate of a country (percentage of Internet users in proportion to the total population). Both types of scatter plots will be further analyzed qualitatively in an exploratory fashion. By making use of various technical reports and news articles, different factors will be explored to explain the differences in the distribution pattern.

V. RESULTS

Before plotting the necessary data, the types of botnets that contribute the most to the dataset are identified. This is done to give a meaningful analysis without getting bogged down at relatively 'small' botnets that do not require as much attention as the major ones. There are 31 different types of botnets identified in the dataset. Top 20 most infected countries are identified, and the ten most prevalent types of botnets in these 20 countries are listed. This data notably contributes to 96% of the dataset. Table 1 shows the top 10 types of botnets, and Table 2 shows the top 20 countries along with the number of infected computers. To provide a consistent analysis, this 'global' top 20 ranking will be used for all botnets, instead of a different ranking for each type of botnet.

Table 1 Top 10 types of botnets

Rank	Name
1	Conficker
2	Gamut
3	Dyre
4	Zeus
5	ZeroAccess
6	Tinba
7	Asprox
8	Cutwail
9	Palevo
10	Gameover (P2P Zeus)

Table 2 Top 20 countries

Country	# of total occurrences of top 10 botnets
VN (Vietnam)	856,843
IN (India)	762,814
CN (China)	593,620
BR (Brazil)	404,935
RU (Russia)	400,903
ID (Indonesia)	279,349
JP (Japan)	202,936
IT (Italy)	186,849
PK (Pakistan)	185,244
AR (Argentina)	178,249
EG (Egypt)	160,178
TH (Thailand)	135,639
IR (Iran)	133,038
MX (Mexico)	130,214
TW (Taiwan)	126,325
US (USA)	119,268
PL (Poland)	118,309
UA (Ukraine)	116,777
DE (Germany)	107,295
ES (Spain)	107,220

The first type of scatter plot is built by mapping number of occurrences in each country of each type of bot against the number of Internet users in that country. As the database spans from mid-August 2015 until mid-Sep-

tember 2015, the number of Internet users is estimated using the number of Internet users in that country as recorded in 2014 and extrapolated using the estimated annual growth rate. All external data was harvested from Internet Live Stats[1].

Another important piece of information is the ratio of Internet users compared against the total population in a specific country. This is referred to as penetration rate. This metric provides a normalized view of a country's ICT intensity and usage. The second type of scatter plot is based on this metric, but instead of the total occurrences in a country, it will be mapped against the ratio of victimized machines in that country. For the sake of simplicity, the latter shall be referred to as 'infection ratio'. It is estimated by dividing the number of occurrences with the number of Internet users in that country. Although this ratio may not be highly accurate, it is consistent with the data used for the first type of scatter plots, and therefore does not infuse additional biases. The software piracy rate data of each country will also be analyzed, as well as the Gross Domestic Product of the each country as a measure of its wealth. Table 3 below provides all the country-related information that have been described.

Table 3 Country profile for top 20 countries.

Country	GDP based on current prices (2015, in billion USD)[2]	Software piracy rate (2013) [15]	Penetration rate (estimation for August 2015)
Ukraine	90.1	83%	37.49%
Taiwan	518.8	38%	46.03%
Thailand	373.5	71%	28.84%
Pakistan	271	85%	10.84%
Iran	1,381.7	N/A	28.29%
Poland	481.2	51%	67.15%
Argentina	578.7	69%	59.74%
Spain	1,221.4	45%	74.38%
Italy	1,819	47%	59.92%
Vietnam	198.8	81%	42.97%
Egypt	N/A	62%	48.34%
Indonesia	872.6	84%	16.72%
Mexico	1,161.5	54%	41.13%
Germany	3,371	24%	86.78%
Russia	1,235.9	62%	59.27%
Brazil	1,799.6	50%	53.37%
Japan	4,116.2	19%	86.03%
India	2,182.6	60%	19.19%
USA	17,968.2	18%	86.75%
China	11,384.8	74%	46.03%

[1] http://www.internetlivestats.com/internet-users-by-country/
[2] https://knoema.com/nwnfkne/world-gdp-ranking-2015-data-and-charts

Below are the scatter plots for each of the botnet type identified as the top 10 in the dataset, followed by an analysis of the plots.

V.1 Conficker

Conficker, also known as Downadup, Downup, or Kido, is "one of the largest botnets ever seen" [16]. It broke out in November 2008 and lived in Microsoft Windows computers by exploiting vulnerability MS08-067. The initial version was named Conficker A by the Conficker Working Group, and it has ever since evolved into respectively Conficker B, C ,D, E in the period between November 2008 until April 2009. Thereafter, large scale cleanup efforts had been initiated in infected countries, including the formation of the so-called Conficker Working Group[3]. Notwithstanding the fact that it is now inactive, Conficker remains as one of the largest botnets residing in millions of machines worldwide [16].

As reported in [17], Conficker spreads using two major vectors: infecting random hosts and infecting nearby hosts. The latter has been suggested as more dominant in promulgating the worm. There are several interesting abilities that enabled Conficker to infect hosts nearby, as follows [17]:

1. Ability to infect other hosts in the same subnet. This is what made Conficker A spread quickly within corporations [18].
2. An ability to infect hosts in the nearby subnets. Particularly one of the main propagation method in Conficker B [16].
3. An ability to infect portable storage devices. Conficker uses autorun-worm techniques in USB drives [19].

Even more interesting, Conficker has an algorithm to create a unique list of 250 random domain names every three hours [17]. By registering any of these random domain names, the villains behind Conficker could communicate with any of the computers they had infected [19].

There has been prior work on studying the distribution trend of Conficker. It was mentioned that North America used to be the main contributors of botnets, but in 2011 the position was taken over by Asia and South America**.** [17]**.** Scrutinizing the Spamhaus dataset will provide a current view of where most of the infected machines are currently located. The scatter plots of occurrences of Conficker bots in the top 20 countries and its infection ratio measured against penetration rate are given in Figure 1 and Figure 2 respectively as follows.

[3] http://www.confickerworkinggroup.org/

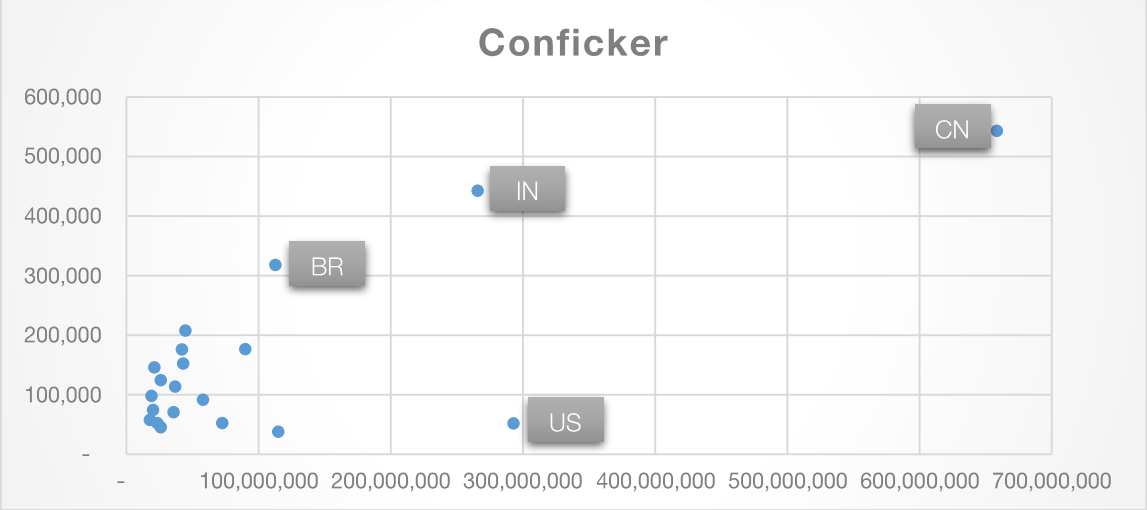


Figure 1 Occurrences of Conficker bots in the top 20 countries

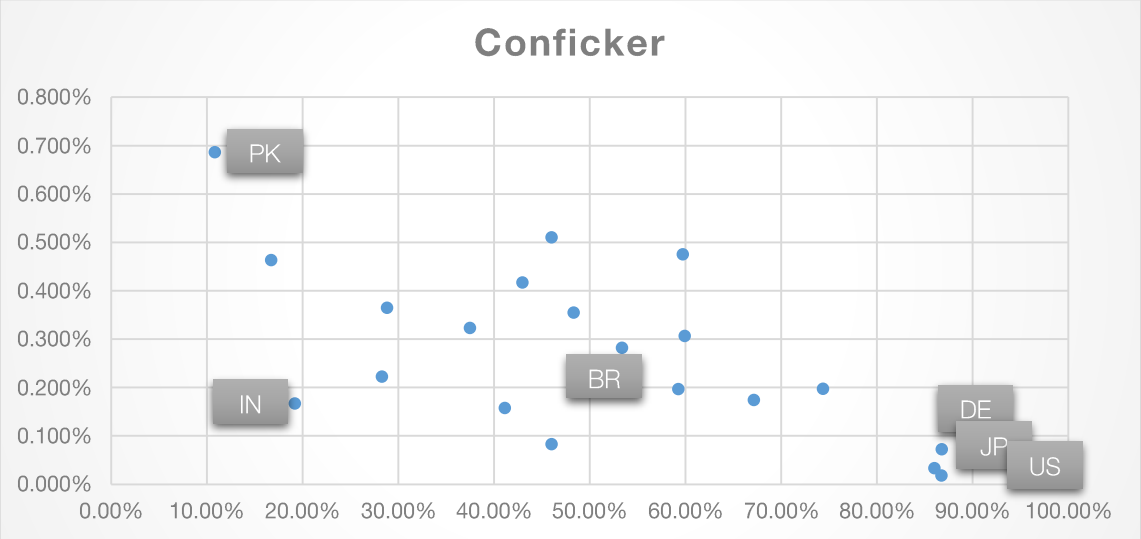


Figure 2 Infection ratio of Conficker in the top 20 countries

Conficker is identified in more or less 200,000 different machines in most of the top 20 countries, except for Brazil, India, China. This is consistent with [17]. However, a unique trend is also found in U.S. Although it has almost 300,000 million Internet users, there are only slightly more than 50,000 victimized machines found there. Figure 2 shows that there is a downward trend in the relationship of infection ratio and penetration rate.

There has been particularly a lot of attention paid to Conficker and China. Various new articles reported that it is suspected that Conficker originated from China due to its uncanny similarity with an older virus called Nimda [20] [21]. In its peak, China hosted more than 25% of all Conficker-infected machines worldwide, and its ISPs hosted 1 out of 7 Conficker infections. [22]. However, these are not strange facts considering the behavior of Chinese Internet users. A survey in 2010 showed that nearly 17 million computers in China are unprotected, apart from the fact that Windows XP piracy is high in China. [23].

U.S, Germany, Brazil and Japan all have released public countermeasures in rendering Conficker powerless. For example, US Computer Emergency Response Team published an alert page specifically containing instructions on how to protect computers from Conficker and to disinfect them once it was too late[4]. German users took a rather proactive approach by visiting the website of Germany's Anti-Botnet Advisory Center, *botfrei.de* [16]. Brazilian domain registration and IP assignment body, *registro.br* took actions to block registration of domains to be used by Conficker variants [24]. *Registro.br* is a part of the Brazilian Internet Steering Committee, *CGI.br*. Japan fought Conficker through its anti-botnet initiative, Cyber Clean Centre (now ACTIVE) [16]. These facts might explain the low infection ratio in these countries, despite the fact that they contribute to much of the Conficker occurences in the dataset.

As for India, the low infection ratio cannot be linked with any cleanup efforts. Early reports show that there are around 25,000 PCs infected in India [25], while the dataset reveals almost 450,000 infected PCs. This means that even if there were one, the cleanup effort in India is not effectively carried out. By 2012, Conficker is listed in as one of the top 10 threats in Pakistan [26]. The same source reported that Pakistan has been improving its condition as the number of computers connecting to Windows Update and Microsoft Update has substantially increased compared to 2011. It can be concluded that the high infection ratio is due to the relatively low penetration rate in Pakistan (10.84%) compared to the number of infected machines.

V.2 Gamut

Being far less popular than Conficker, there is very little information available on Gamut, which is suspected to have been active since early 2013 [27]. It is downloaded by a Trojan downloader that arrives as an attachment from a spam email message. The C&C servers are linked to Ukrainian domain names, which point back to one specific hosting service provider based in Russia [27]. Gamut is a spambot, meaning that it is used to send spam email messages. One single Gamut spambot is capable of sending at least 60,000 messages per day, mostly targeting job seekers [27]. These emails come with a link which will direct victims to a dodgy job website where they are asked to sign up. Despite being categorized as a Risk Level 1 (Very Low) threat by Symantec[5], it seems that Gamut has been building its arsenal around the world since first discovered. The scatter plots of occurrences of Gamut spam-bots in the top 20 countries and its infection ratio measured against penetration rate are given in Figure 3 and Figure 4 respectively as follows.

[4] https://www.us-cert.gov/ncas/alerts/TA09-088A
[5] https://www.symantec.com/security_response/writeup.jsp?docid=2014-031006-1618-99

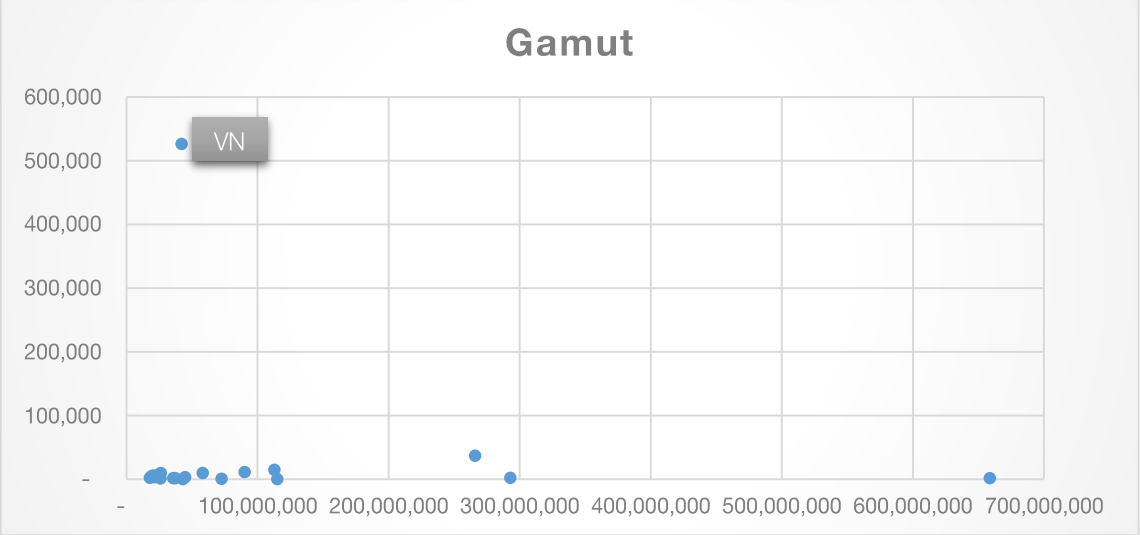


Figure 3 Occurrences of Gamut in the top 20 countries

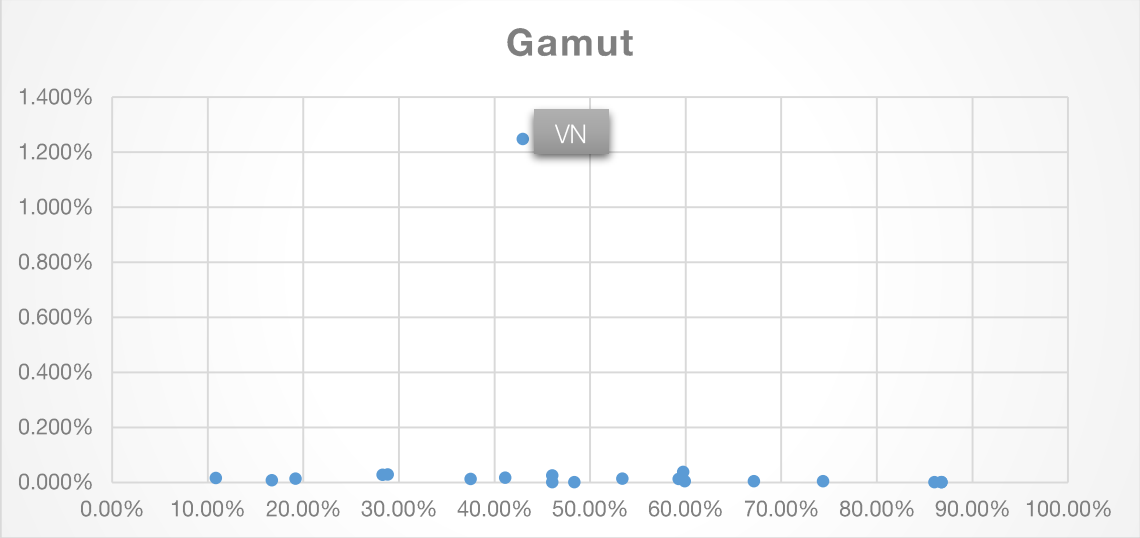


Figure 4 Infection ratio of Gamut in the top 20 countries

All of the countries, except for Vietnam, are diagnosed with fewer 100,000 infected machines, which corresponds to not more than 0.05% of infection ratio. This means that in the case of Gamut, there is no relation between infection ratio and penetration rate. Vietnam eye-catchingly stands out in the chart as the most infected country with Gamut spambots from the rest of the top 20 countries. This fact might explain why Vietnam is listed as the #1 spam-sending country in the world, with more than 328 million spam emails sent out in July 2015[6]. This is in line with the presence of approximately 525,000 Gamut-infected machines in Vietnam. Why Vietnam is very susceptible to Gamut is yet to be discovered. However, since October 2012, Vietnam's 'anti-spam law' (called Decree 77) has been put in practice to provide several means to limit spamming, and was renewed with the controversial

[6] According to www.spamrankings.net, July 2015

Decree 72 since September 2013 [28]. This however shows that Vietnam, although being one of the less wealthy countries in the Top 20 list, is a big nest for spam sending bots.

V.3 Dyre

Dyre, or Dyreza is a financial Trojan that was first unearthed in June 2014 and is now "the main financial Trojan threat" [29] following major takedown of older financial malwares such as Gameover Zeus, Shylock, and Ramnit. A technical report from Symantec released in June 2015 gave the following description for Dyre: "…one of the most dangerous financial Trojans, capable of defrauding customers of a wide range of financial institutions across multiple countries…a highly developed piece of malware, capable of hijacking all three major web browsers and intercepting internet banking sessions in order to harvest the victim's credentials and send them to the attackers… a multi-pronged threat and is often used to download additional malware on to the victim's computer. In many cases, the victim is added to a botnet which is then used to send out thousands of spam emails in order to spread the threat further afield." [30].

Dyre's main infection vector is spam emails, which come in the form of a business document, voicemail, or fax messages. These emails come with an attached archive (bank statement or invoice) or a web link, which actually contains Upatre downloader. Upatre downloader is one of the main downloader-type threats. When it is clicked, Dyre will be installed in the victim's computer. Dyre is also capable of performing a man-in-the browser attack, using techniques such as redirecting victim to a fake page asking for credentials, or performing web injection on the fly [30]. Primary targets are customers of bank in English-speaking countries. UK- customers of Barclays, Royal Bank of Scotland, HSBC, and clients of Bank of America and Citibank in US have all been targeted by Dyre [31]. In a recent report by [32], United States is listed as the most affected country, followed by Canada, Australia, and United Kingdom. Customers of electronic payment services and digital currencies users are also targeted. Moreover, Dyre expanded its battleground by starting to attack careers- and HR- related websites [30]. Dyre is also constantly evolving: its new variants are exploiting a patched Windows vulnerability [33] and are using semi-random names to evade detection. [34].

The scatter plots of occurrences of Dyre malwares in the top 20 countries and its infection ratio measured against penetration rate are given in Figure 5 and Figure 6 respectively as follows.

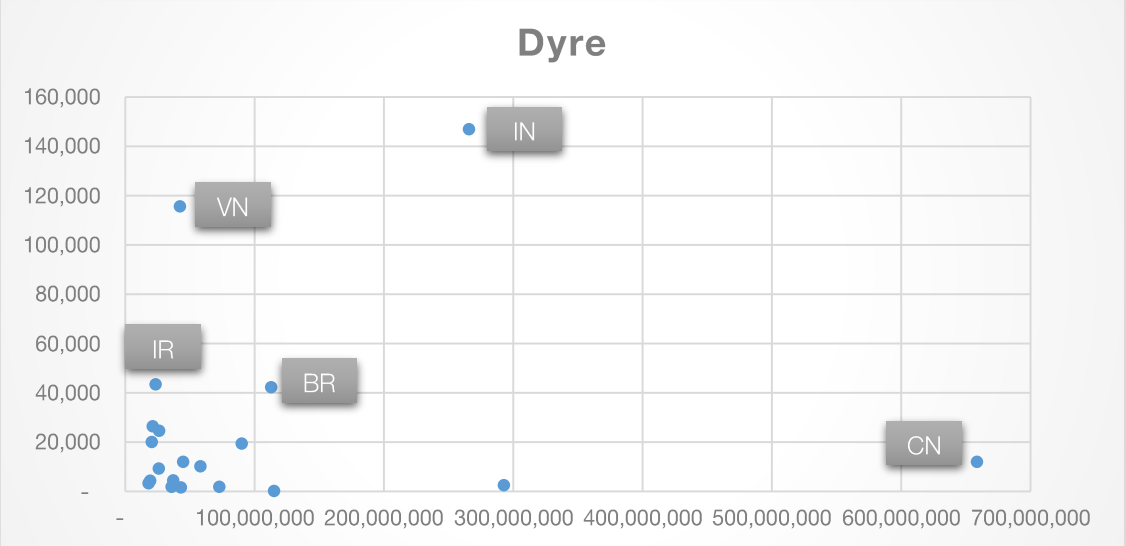


Figure 5 **Occurrences of Dyre malwares in the top 20 countries**

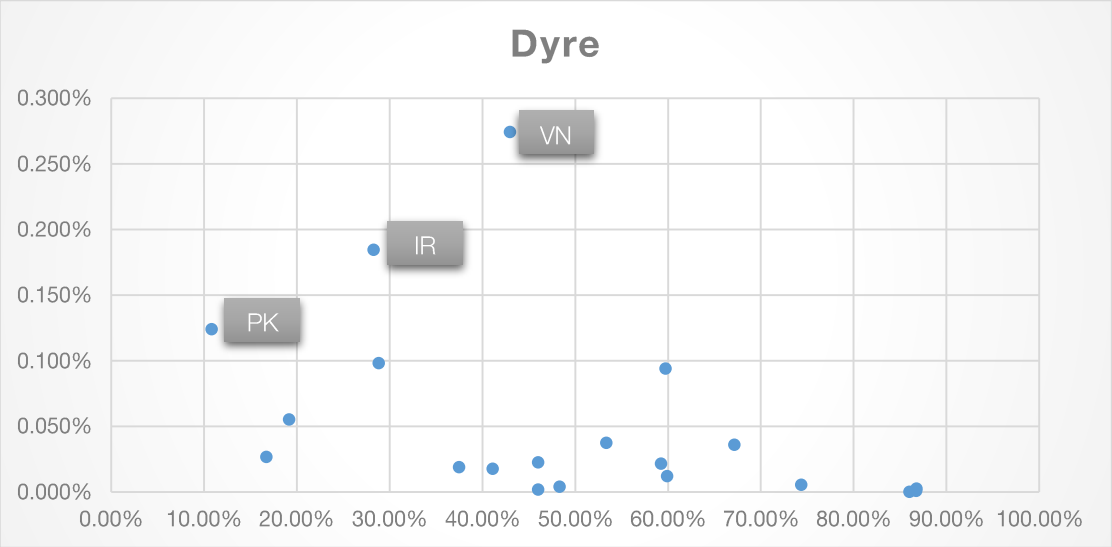


Figure 6 **Infection ratio of Dyre malwares in the top 20 countries**

Figure 5 reveals that most countries have 20,000 to 40,000, with the exception Iran and Brazil (slightly above 40,000), and Vietnam and India (more than 100,000 occurrences). Both Figure 5 and Figure 6 clearly indicate that Dyre malwares are concentrated in Asia. This is counterintuitive with the description of targeted countries (UK and US). An additional look at the dataset reveals that there are only 601 and 2,509 infected machines in the UK and US respectively. This is still significantly fewer than Vietnam and India. This can be partially explained by differences in dataset used in [32] and Spamhaus. Blueliv used a single honeypot to collect more than 35,000 Dyre bots, while Spamhaus covers more ground by using sinkholes which collect more than 500,000 Dyre bots. A difference in the analysis magnitude is expected, and hence the difference. However, this finding is also partially supported by Blueliv: India is listed as the sixth most affected country and Vietnam is also listed as one of the most affected

country in Australian-targeting campaign[7]. While in the first quarter of 2015, 39% of infections were attributed to European users, Asia Pacific users were targeted by 44% of Dyre-infected emails in May 2015 [35]. This trend is expected to continue, as being able to break into European banks' strict regulations means breaking Asian banks is far easier.

V.4 Zeus

Zeus (sometimes stylized as ZeuS) is a financial malware package that is readily available, which can be purchased for as low as USD 700 and even freely traded. [36]. It has existed since 2007 in computers with Microsoft Windows, but there are also variants for Blackberry and Android smartphones since 2012, making it the most widespread banking Trojan [37]. Zeus' main purpose is to steal online credentials by performing four main actions: gathering system information; stealing protected storage information, FTP passwords, and POP3 passwords; stealing online credential information as specified by a configuration file; and contracting the C&C server for additional tasks to perform [36] [38]. Zeus and another financial botnet, SpyEye, are allegedly responsible for a collective loss of up to $100 million [39].

The lifecycle of Zeus can be described into four different operations [38]. Firstly, it attempts to infect the computer to gather all information it can harvest from the computer (e.g. email, banking, social networking credentials) using means such as redirecting to phishing websites. This is also known as the Man-in-the-Browser attack. Secondly, the bot gathers information about a local network. Next, it attempts to spread through the means of sending spam emails to user's address book or social networking sites. Finally, it integrates to its C&C server to perform Denial of Service attacks and mass spamming. Other than that, Zeus' "commander" will use the banking credentials to steal money from the victim's accounts, or sell it to bigger criminal infrastructures for fraud operations [37]

Zeus is spread worldwide and generally found in countries where malware is most prevalent. In October 2009, Zeus was detected in almost every country in the world, with worst concentration in U.S and Japan [36]. During 2009-2013, there were at least 818 U.S. domains infected, followed by 187 domains in Germany, and 166 domains in the UK. [37]. However, in 2010 Federal Bureau of Investigation (FBI) managed to arrest more than 100 suspected members of cybercriminal network behind Zeus [40].

The scatter plots of occurrences of Zeus malwares in the top 20 countries and its infection ratio measured against penetration rate are given in Figure 7 and Figure 8 respectively as follows

[7] One type of nomenclature identified in Dyre uses the following format: Day-Month-Country-Index (DDMMCCI). For example, a bot named 1401us1 correlates to a U.S targeting campaign launched at January 14 [32].

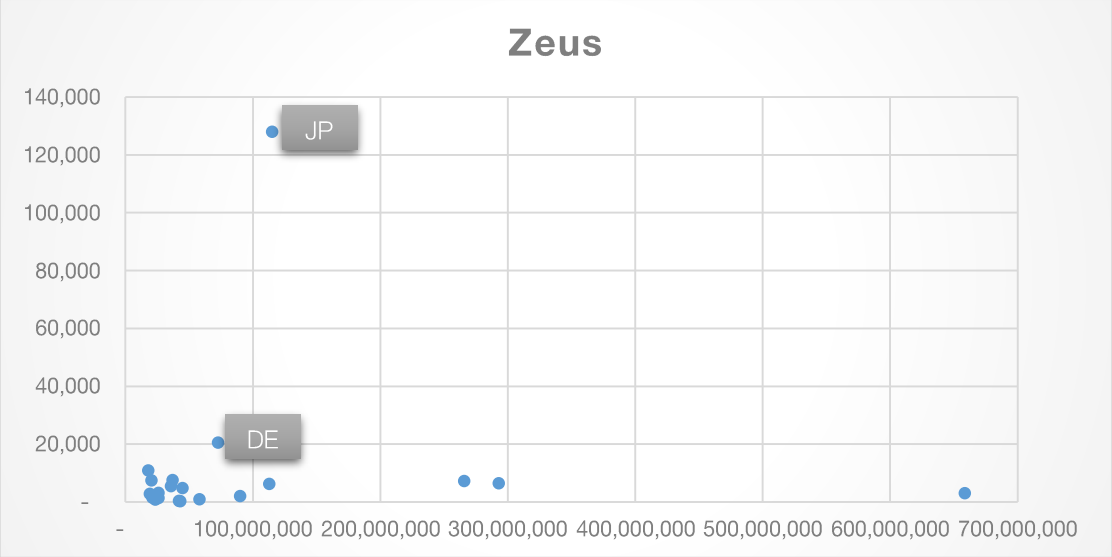


Figure 7 Occurrences of Zeus malwares in the top 20 countries

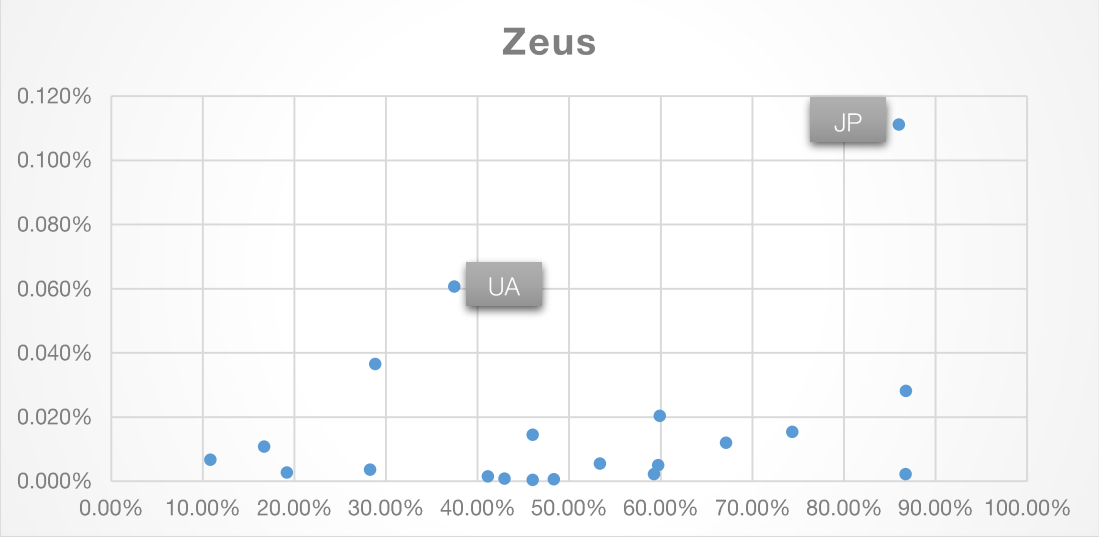


Figure 8 Infection ratio of Zeus malwares in the top 20 countries

Figure 7 shows that most of the top 20 countries regardless of the number of Internet users they have, are diagnosed with a somewhere below 20,000 infected machines. Germany has slightly more than 20,000 victimized machines but an irregularity is observed in Japan, which has almost 140,000 victimized machines. The overall low occurrences in most of the countries might be explained by the success of Microsoft's anti-Zeus tool, which has been able to remove at least 281,491 instances of Zeus from 274,873 PCs in October 2010 [41]. However, Symantec reported an outbreak in 2013 stating that Japanese online banking customers have become one of the main target since then [42]. Using web injection technique, it targeted five major banks in Japan. This shifted the gravity of the problem from Europe and U.S to particularly Japan. Indeed, since 2009 Japan has been heavily infected by Zeus with more than 44,298 occurrences recorded in October 2009 [36]. It is expected that the attacker uses Blackhole exploit kit to install Zeus in Japan.

Figure 8 shows an interesting upward trend between infection ratio and penetration rate. Although the slope is not high, it can be seen that there is a positive correlation between infection ratio and penetration rate. Statistical test of this relation is beyond the scope of this report and there will be more observations (i.e. data for countries) needed to confirm this preliminary guess.

V.5 ZeroAccess

ZeroAccess is one of the world's largest botnet with a P2P communication structure, with the primary motivation of financial fraud through pay-per-click advertising. As of August 2013, there are 1.9 million computers infected by ZeroAccess worldwide, with more than 800,000 compromised machines active on the Internet on any given day [43]. The top 5 countries contributing to the total number in August 2013 are U.S (35.1%), Japan (9.3%), India (5.6%), Italy (4.9%), and Canada (4.1%)[8] [44]. Some researches argue that ZeroAccess has been active since as early as 2009 [43], but some argue that the major versions have not really been active until 2011 [45]. ZeroAccess is mostly concentrated in the US and is responsible for losses to advertisers at USD 2.7 million per month [46]. There are four distinct variants of ZeroAccess: Version I (Type I, II, and III), and Version II (Type IV). ZeroAccess uses three vessels for monetization: pay-per-install (up to USD 120,000 for the featured version), Bitcoin mining, and click fraud [45]. Specifically, it utilizes two modules to carry out the click-fraud: auto-clicking and search-hijacking (by fetching advertisements relating to real search queries made by the user [43].

ZeroAccess employs two infection vectors to replicate itself to multiple machines: exploit packs and social engineering [47]. It has become a popular payload to Blackhole exploit packs. An exploit pack usually comes as a series of PHP scripts stored in a web server under the attacker's control. When a victim's browser accesses the loaded website, the server backend will attempt to exploit a vulnerability on the target machine and execute the payload. The second infection vector is through a bunch of social engineering mechanisms. A common factor between all these mechanisms is convincing a victim into clicking an executable file which they should not. Usually these files come in the form of a crack or Keygen, which are placed on upload sites and torrents and are given misleading filenames.

On 5 December 2013, Microsoft in cooperation with Europol's European Cybercrime Centre (EC3), the FBU, and leaders in technology industry successfully executed a takedown operation on ZeroAccess in a quest to disrupt the operation of the criminal network behind ZeroAccess. They tried to disinfect 1.3 million compromised PCs by taking control of 49 domains associated with ZeroAccess, following a court order on a related civil suit [48]. However, two researchers argued that this move is ineffective, claiming that the P2P communication channel remained intact and that 62% of the infrastructure is still "alive and well" [49].

Following the disruption, ZeroAccess was in dormant mode until March 2014. A research team from Dell recorded activities of ZeroAccess from March 2014 until early July 2014, before it went to dormant mode again. In January 2015, significant activity was again recorded, involving 55,208 unique IP addresses [50]. This time, ZeroAccess' presence was imminent in Japan (15,322 IPs), India (7,446 IPs), Russia (7,101 IPs), Italy (3,649 IPs), and U.S (2,540 IPs). It was also present in Brazil, Romania, and Venezuela.

[8] Complete pie chart is given in Appendix 2

The scatter plots of occurrences of ZeroAccess in the top 20 countries and its infection ratio measured against penetration rate are given in Figure 9 and Figure 10 respectively as follows.

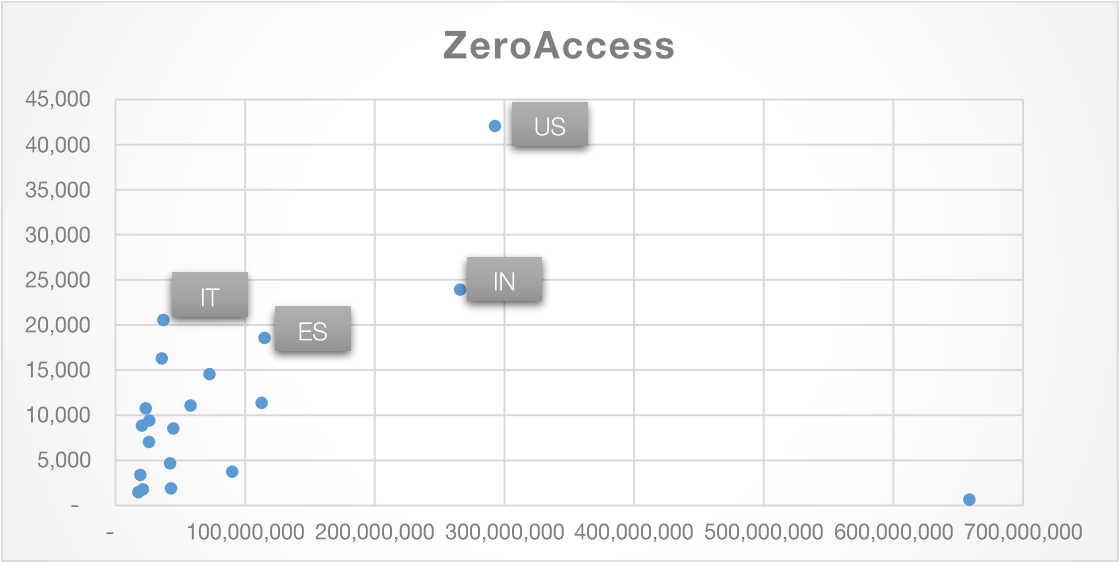


Figure 9 Occurrences of ZeroAccess in the top 20 countries

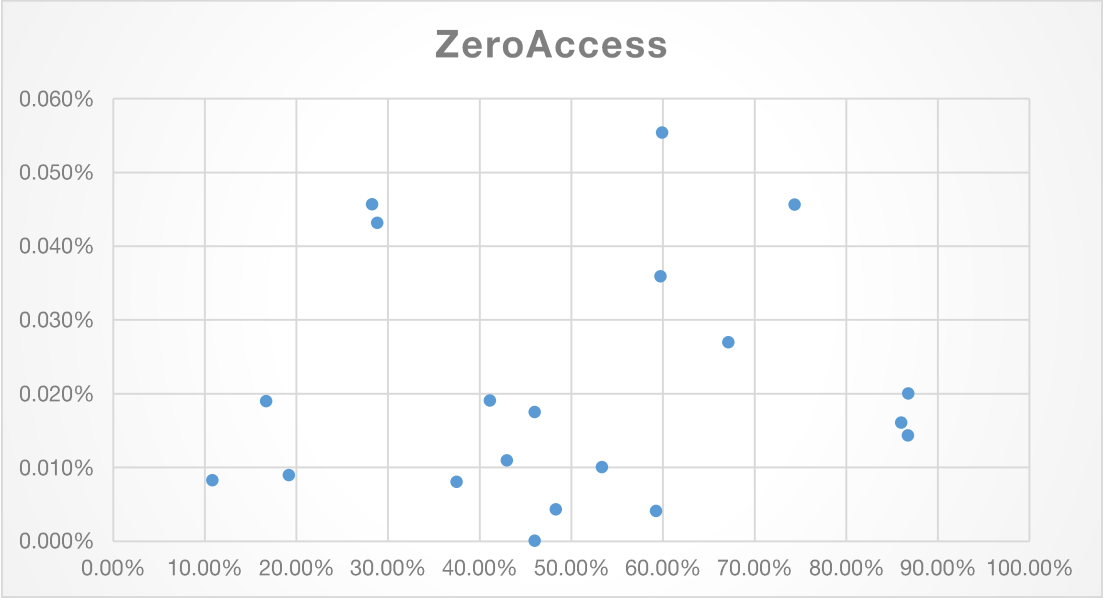


Figure 10 Infection ratio of ZeroAccess in the top 20 countries

Firstly, it has to be taken into account that the number of infected machines as measured in the dataset has shown fluctuation from 1.9 million in August 2013 to 55,000 machines in January 2015, and rose again to 220,000 machines in August 2015. Due to the complexity of the peer-to-peer network architecture, ZeroAccess is not yet fully eliminated. U.S still shows up as the most infected country in the list, with nevertheless far fewer victimized machine. There are approximately 42,000 machines according to the dataset compared to 667,000 machines in

August 2013. The dataset also shows that Canada (not in the Top 20 countries) has significantly fewer number of infections, coming in at slightly more than 3,000 instances.

Figure 10 shows an interesting pattern between infection ratio and penetration rate. Countries with relatively high penetration rate (approximately ≥ 60%) tend to have higher infection ratio compared to those with relatively lower penetration rate. This is aligned with the distribution data of ZeroAccess in August 2013 and January 2015 which shows that the Trojan is prevalent in countries with high penetration rate (e.g. USA, Italy, Japan, Germany, etc.). However, there are also irregularities: Thailand and Iran have high infection ratio. These countries were not visible in the distribution map in 2013, which means that ZeroAccess may be targeting new countries. Ever since the Microsoft takedown in December 2013, there has been little coverage of ZeroAccess in the media. The results from Spamhaus dataset might explain where ZeroAccess is now headed.

V.6 Tinba

Tinba is a member of the banking botnet family, which is still very active globally as of now. First discovered in 2012, it is aptly named ("Tiny Banker") due to its small size (25 kb, ten times smaller than other such malwares). Tinba 1.0 was leaked in July 2014 and was believed to originate from Eastern Europe. Its successor, Tinba 2.0 (released in September 2014) is a very popular botnet kit among cybercriminal gangs, being traded frequently amongst these groups. With a domain generation algorithm, Tinba 2.0 is being distributed through spam email and exploit kits, targeting many financial institutions, webmail services, social networking sites, and other organizations around the world [51]. Being a rootkit, it is impossible to be removed manually by users.

Tinba is highly dynamic. According to a joint report from Cyber Security Intelligence Services (CSIS) and Trend Micro released in 2012, Tinba was highly concentrated in Turkey, with more than 60,000 identified unique infections [52]. However, in a report from October 2014, it is revealed that Tinba mainly targeted Australian banks, in addition to German, Spanish, Finnish, and Swiss banks [53]. In May 2015, IBM Security Trusteer discovered that Poland, Italy, The Netherlands, and Germany are in the European radar of Tinba [54]. Very recently (November 3, 2015), Dell released a media alert stating that high-profile Russian banks and payment service providers are on the hit list of Tinba [51]. Besides that, customers of Shinkin financial institutions in Japan are being targeted as well. A sinkhole data on October 15, 2015 from abuse.ch involving 32,805 unique IP addresses gives the following distribution profile for Tinba[9]: Russia has 34.5% of the infected IP address, making it the most infected country on the list. Poland comes in second with 22.0%, followed by Indonesia (7.2%), Spain (6.5%), and Canada (5.6%).

The scatter plots of occurrences of Tinba in the top 20 countries and its infection ratio measured against penetration rate are given in Figure 11 and Figure 12 respectively as follows.

[9] For a visualization and the top 10 rank of this sinkhole data, please refer to Appendix 3.

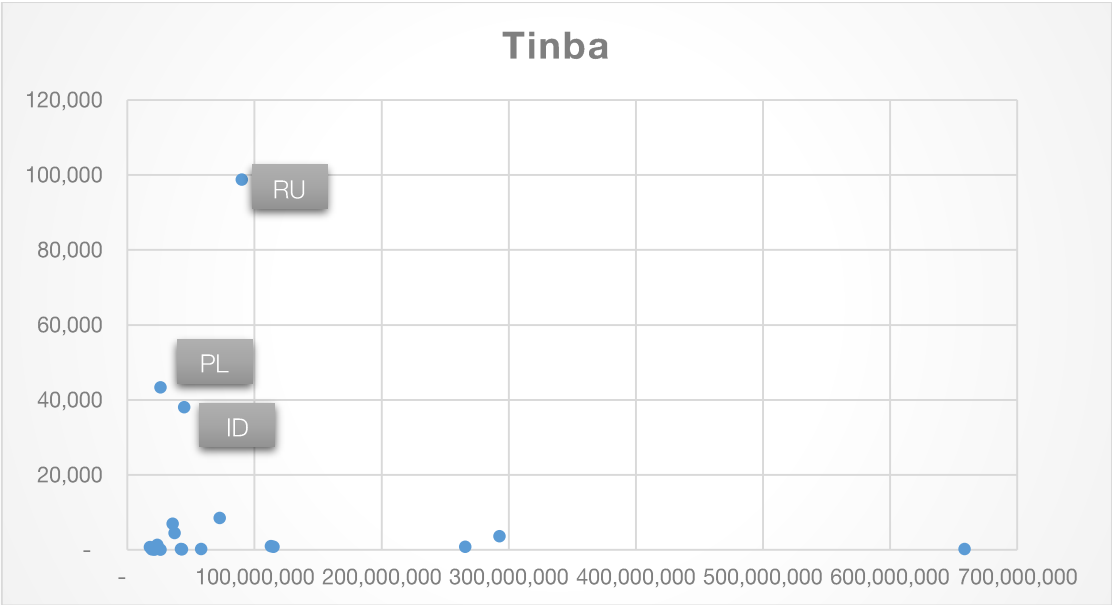


Figure 11 Occurrences of Tinba in the top 20 countries

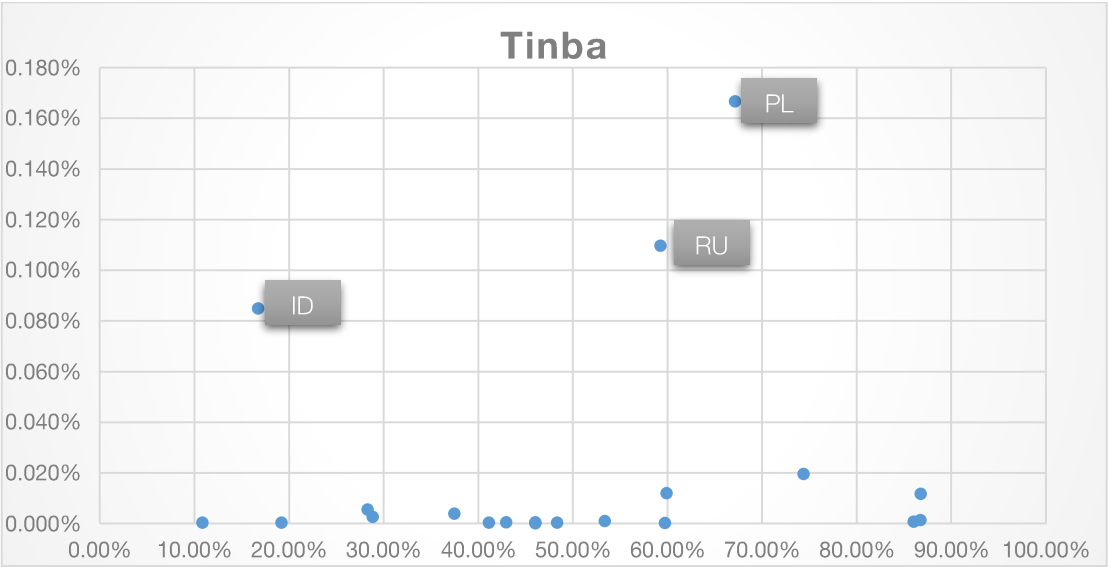


Figure 12 Infection ratio of Tinba in the top 20 countries

Figure 11 and 12 basically convey the same story: Russia, Poland, and Indonesia are the three most infected countries by Tinba. The rest of the countries are not as severely impacted as these three; the same pattern as reported by Dell SecureWorks recently. There is extensive news coverage within the first week of November saying that Russian banks are being targeted by Tinba. This means that before the news broke out, Spamhaus has already caught traces of Tinba's exodus into Russia. A deeper look in its configuration files reveals that the Trojan is now configured to specifically one of the biggest bank in Europe (which is located in Russia) and two popular Russian payment service providers [51]. This is however counterintuitive with historical facts. For example, past malwares would oftentimes exit or uninstall themselves from computers with Russian as the primary language, or those with Cyrillic keyboards. Another fact is that Russia has been arresting cyber criminals, as in the case of Carberp [55],

which would make the cyber criminals less enthusiastic to attack Russia. A Dell SecureWorks researcher suggests that the shift could be attributed to the hostility between the Ukraine and Russia, which means that their law enforcers might not join hands again as they did during the Carberp arrest [56].

The presence of Tinba in Poland has been detected by the national Computer Emergency Response Team (CERT), CERT Polska since 2014, but not in 2013 [57]. In fact, it was the most popular banking Trojan in June 2015, but leveled up to become the most common malware in July 2015, 'beating' other prominent botnets such as Conficker and Sality[10]. According to its annual report, CERT Polska believed that Tinba used web injections in online bank websites to steal one time passwords. This is indeed a recurring technique used in other banking Trojans.

V.7 Asprox

Asprox is a botnet involved in phishing scams and SQL injection attacks into websites in order to spread malware. It was first discovered in 2007 and mostly arrived in victim's computer in the form of an email attachment.F. In the early days, it was notorious for sending phishing emails, but after a successful takedown in 2008, Asprox's operation was essentially banished [58]. After its demise, Asprox resurrected again and has been used as one of the most prevalent attack vectors for SQL injections in huge waves [59]. In June 2010, its large campaign was again disrupted, and ever since it has gone into lower-scale operations. These operations include scams involving packet senders such as FedEx, UPS or DHL. Asprox is also linked to several high-profile SQL injection attacks, including the one that hit Sony Playstation in 2008 [60].

A 2009 study revealed that there are different locations in which the Asprox bots are detected. More than one-third of the Asprox bots responsible for SQL injections were located in China, while the majority of the infrastructure that hosted malicious Javascripts and drive-by downloads was pinpointed in US [61]. Even more interesting, in the latter case, the delivery hosts would check to see if the default language in the visiting browser was Chinese, and not infect the browser in that case. In 2013, Asprox started its campaign again under the name Kuluoz, sending malicious emails embodied in fake court notices, package delivery messages, voicemail service notifications, current events, and online deals [62]. During this period, the campaign was mostly identified in North America. Kuluoz accounted for 80% of all malware activities in October 2014 as recorded by Palo Alto Networks [63]. Its success is owed to its self-propagation feature and its selection of e-mail themes hinting at social engineering of targets. According to SC Magazine, after peaking in 2014, Asprox has basically disappeared in August 2015 [64].

The scatter plots of occurrences of Asprox in the top 20 countries and its infection ratio measured against penetration rate are given in Figure 13 and Figure 14 respectively as follows.

[10] CERT Polska tweeted two charts showing the ranks of different malwares in Poland in June 2015 and July 2015. These charts are provided in Appendix 4.

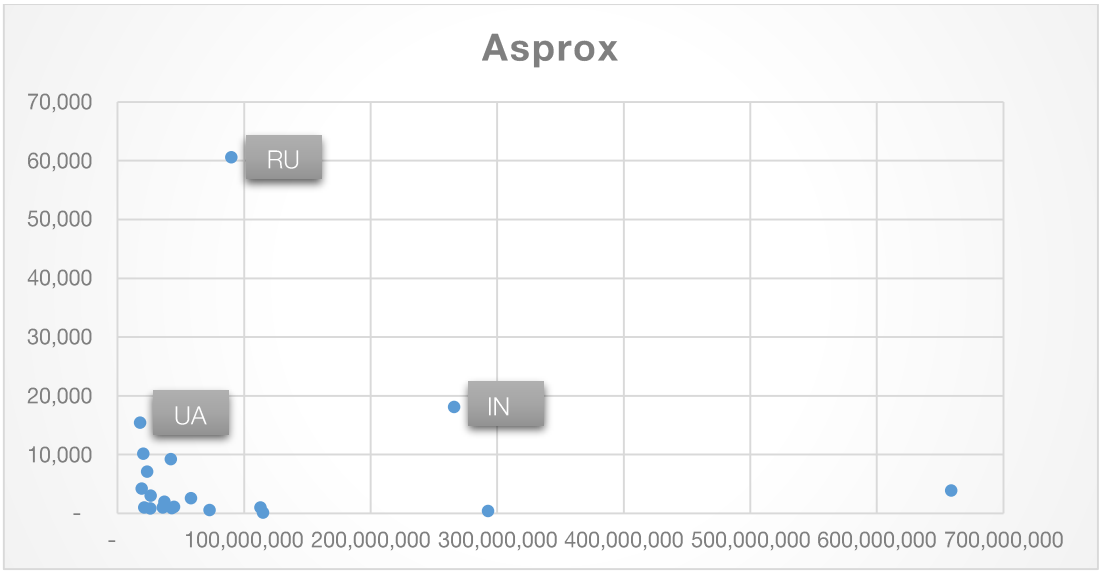


Figure 13 Occurrences of Asprox in the top 20 countries

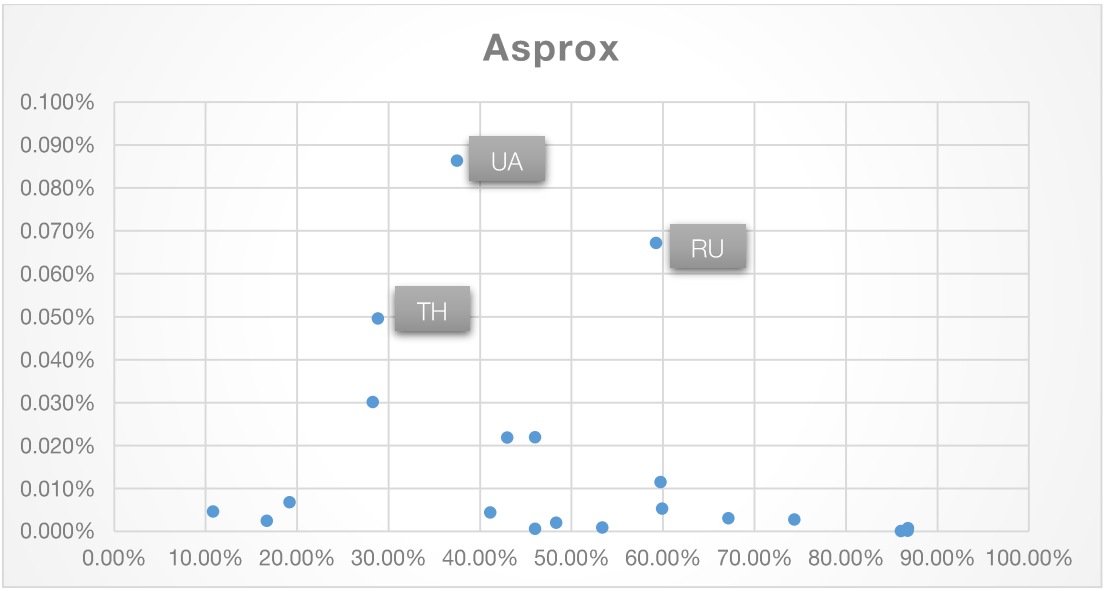


Figure 14 Infection ratio of Asprox in the top 20 countries

Figure 13 shows that most of the countries in the list have less than 20,000 victimized computers, except for Russia. Figure 14 shows an interesting pattern. The infection ratio tends to go up in countries with low to medium penetration rate, but decreases in medium to high penetration rate. However this guess will have to be tested further with more data points and preferably with historical data. Most of the technical reports and research papers that have been written put emphasis on its technical capability to perform SQL injections and its evolution over the years. As for geographical distribution, little research has been done on where the bots are located. Instead, researchers were apparently more interested in finding out the countries where the phishing campaigns are located. However, remembering that Asprox is considered as currently inactive, there might be few studies in the future on this botnet.

V.8 Cutwail

Cutwail is a spambot, mostly used to send spam emails. It was first detected in the wild in 2009 and is believed to have originated in Russia [12]. Cutwail is closely related to Pushdo, a Trojan component that is used to install Cutwail into victims' computers. Cutwail is also related to Zeus and FakeAV, because when a system is infected with Cutwail, it also downloads a Zeus or Fakeav malware as well [65]. Infection channels of Cutwail include direct downloads from the Internet, dropped by other malware, or spammed via email. A study in 2009 claimed that Cutwail is the second-largest spam botnet worldwide, capable of sending approximately 7.7 billion spam emails per day, with Russia being its main target [66]. The content of the email messages sent by Cutwail included pornography, online pharmacies, phishing, money mule recruitment, and malware (typically Zeus) [11]. Cutwail bots have also been used to perform distributed denial of service (DDoS) attacks towards various government agencies and commercial sites.

In 2010, Pushdo/Cutwail was mostly identified as coming from India, followed by Vietnam, Russia, Pakistan, and Egypt respectively, although the bulk of the traffic was coming from France and U.S. [67]. A 2011 study involving 2,536,934 IP addresses showed that the highest concentration of bots from a total was in India (38%), followed by Australia (9%), Russia (4%), Brazil (3%), and Turkey (3%). A possible explanation for the preference of India is that because the cost per bot is cheaper than those in other geographic region. Evidently, infected American computers are more valuable than Indian computers due to a widely held belief that they have better and more reliable Internet connection. Based on a 2014 research by TrendMicro, Vietnam was identified as the highest spam-sending country of Cutwail, followed by India, France, and China [68]. These spams are mostly aimed at U.S., China, U.K., and Japan. Early this year, Fidelis Cybersecurity released a report stating that the highest infection rate has shifted to Asia-Pacific region, especially in countries with high software piracy rate [69]. The top 5 most infected countries are India, Indonesia, Turkey, Vietnam, and Thailand. Taking into account Pushdo's favored infection vector (email), high piracy rate becomes a viable explanation for the high infection rates in the top 5 countries.

The scatter plots of occurrences of Cutwail in the top 20 countries and its infection ratio measured against penetration rate are given in Figure 15 and Figure 16 respectively as follows.

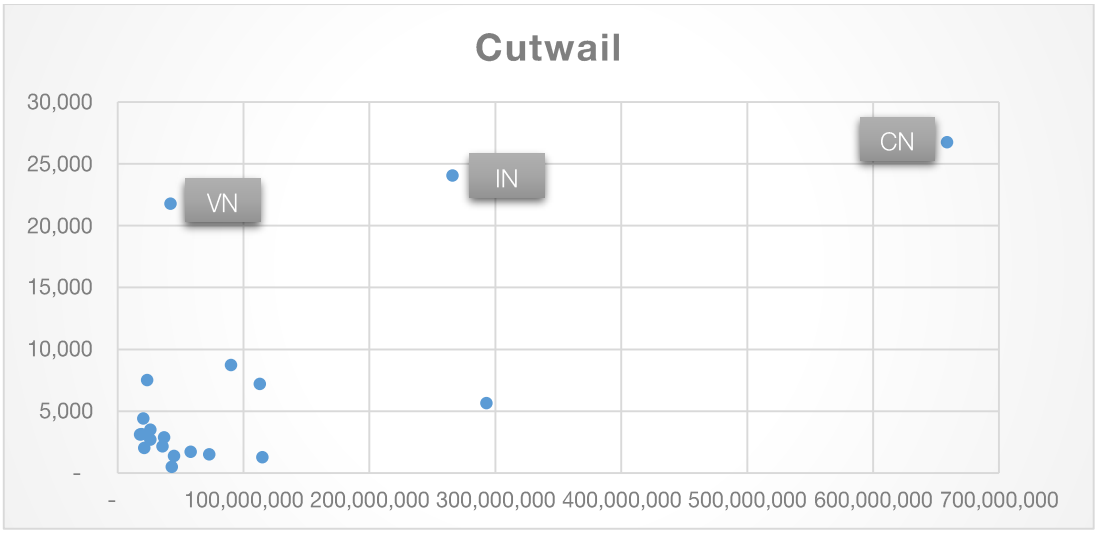


Figure 15 Occurrences of Cutwail in the top 20 countries

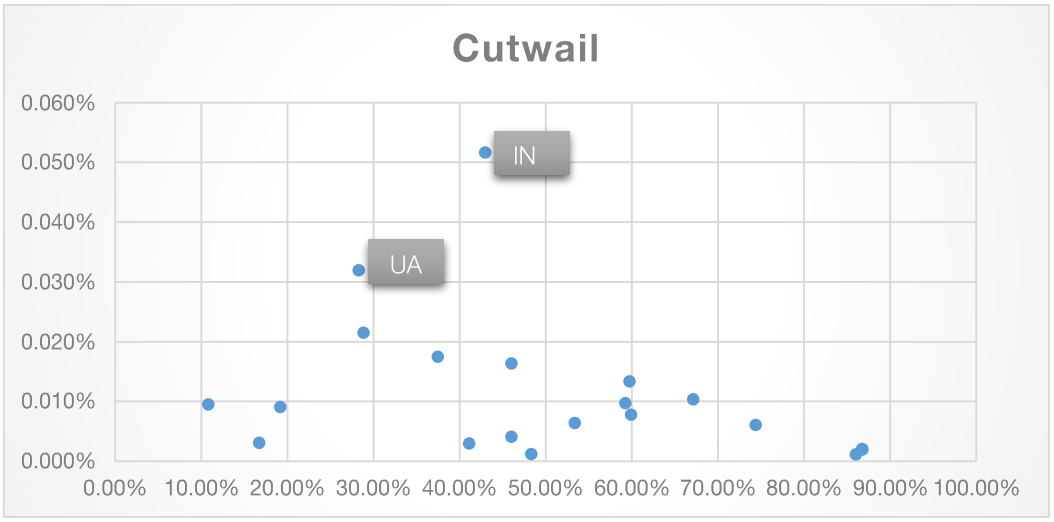


Figure 16 Infection ratio of Cutwail in the top 20 countries

Figure 15 shows a different profile from the findings of Fidelis Cybersecurity. China is shown as the most infected country in the list[11]. This difference can be explained by Spamhaus sinkhole concentrated on accumulating botnets identified as Cutwail, while Fidelis' sinkhole accumulated those identified as Pushdo. Despite these differences, the two are closely related and therefore can explain the presence of each other. Another notable remark is that India and Vietnam are also identified by Spamhaus as members of the most infected countries, showing an intersection between the two different data sources. Figure 16 shows a weak negative relationship between infection ratio and penetration rate. Indeed, the notion of high software piracy to explain high infection rate seems more appealing, and needs to be further explored. Nevertheless, the idea that the concentration of these bots is saturated in Asia is confirmed by the Spamhaus dataset.

[11] China's software piracy rate in 2013 was 74% [15]

V.9 Palevo

Palevo, also known as Rimecud, is a worm which is a part of a bigger botnet called Mariposa ('butterfly' in Spanish). The worm has been around since 2009, but notably made the news in 2010. It is capable of spreading over network shares, USB drives, instant messaging networks and P2P shares [70]. Besides, it can also download updates and additional malware and execute remote tasks from a command and control network. Once infected, Palevo can receive remote commands to perform DDoS attacks, password theft in major browsers, browser cookies theft, and many other malicious actions.

Palevo uses four main propagation vectors: USB and removable drives, P2P file sharing, network shares, and instant messaging programs (particularly MSN Messenger). In 2010, a major outbreak with the instant messaging infection happened, with rates of infection exceeding 500 percent growth per hour in several countries, such as Romania, Mongolia or Indonesia [71]. In February 2010, the criminals behind Mariposa botnet - of which Palevo is a component – were arrested. At that time, there were approximately 15,550,850 compromised unique IP addresses [72]. However, following the sharp decline post-takedown, Palevo seemed to resurge again starting Q3 2010 until Q1 2011 [73]. The Swiss security blog, *abuse.ch* recorded that there were still 89 active Mariposa C&C servers.

A 2013 data from McAfee showed that Palevo was concentrated in Germany (11%) and Brazil (11%), followed by Russia (8%) and India (8%) [74]. According to the latest data from abuse.ch, there are 11 C&C servers of Palevo recently tracked. 5 of these C&C servers are located in U.S and 2 are from Ukraine. Poland, The Netherlands, China, and Canada each contributes one C&C server.

The scatter plots of occurrences of Palevo in the top 20 countries and its infection ratio measured against penetration rate are given in Figure 17 and Figure 18 respectively as follows.

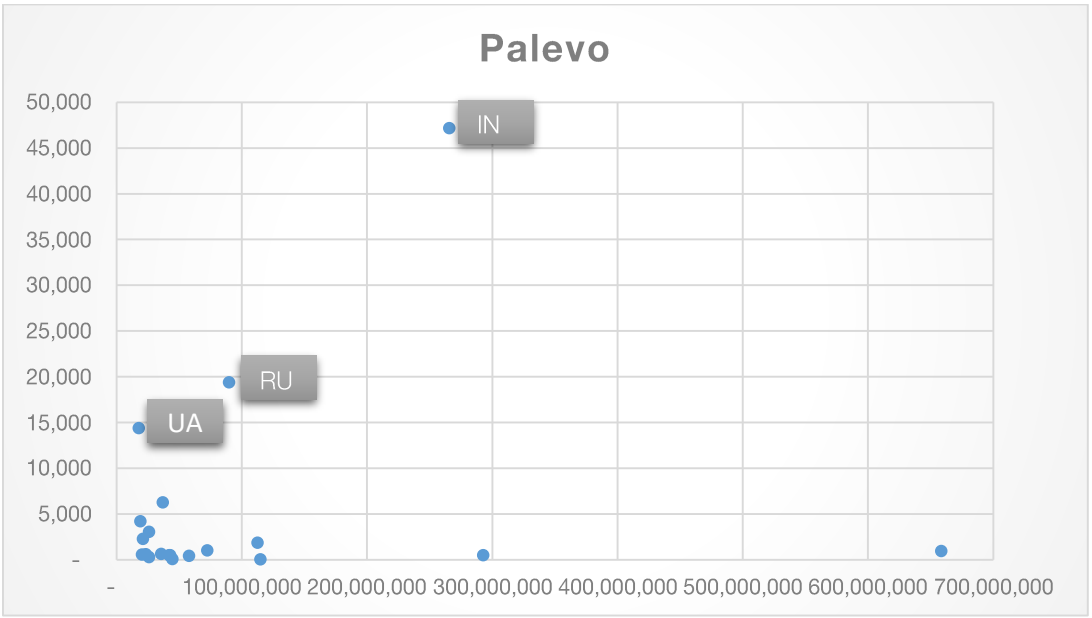


Figure 17 Occurrences of Palevo in the top 20 countries

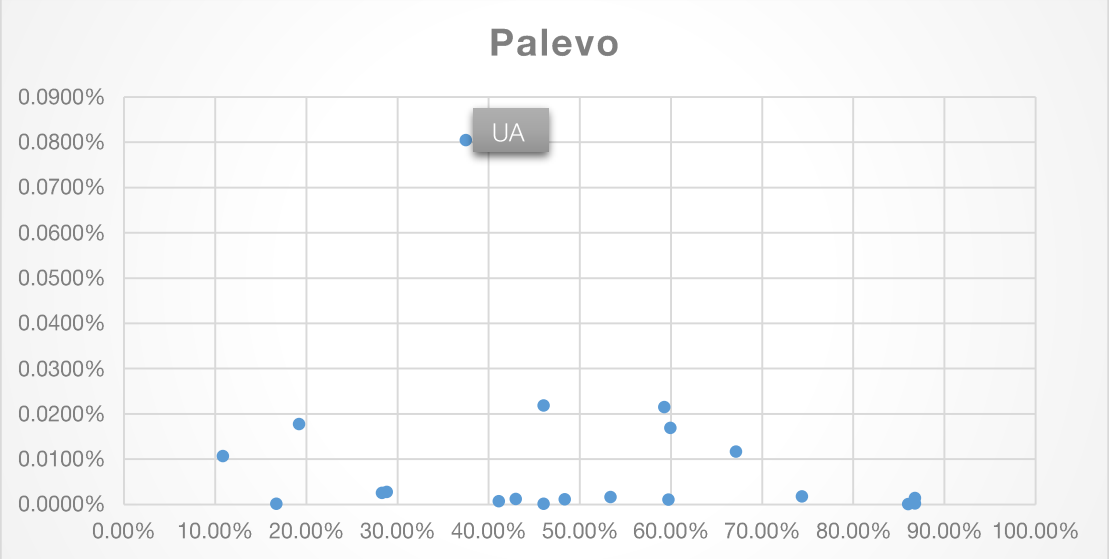


Figure 18 Infection ratio of Palevo in the top 20 countries

Figure 17 and Figure 18 show that India has the highest number of infections, followed by Russia, and Ukraine. The rest of the countries have relatively low infections. Figure 18 shows weak trend of positive correlation between infection ratio and low penetration rate, but a negative correlation with high penetration rate. The high infection ratio in Ukraine is supported by the fact that two of the most active C&C server for Palevo were detected in Ukraine.

V.10 Gameover (P2P Zeus)

Gameover is a P2P version of the Zeus botnet. Although it lived a relatively short lifetime (September 2011 – June 2014), Gameover Zeus was responsible for financial losses ranging from USD 10,000 up to USD 6,900,000 [75]. These losses were incurred through a variety of ways, including spam, infection, account takeover, fraud, international wire, DDoS attacks against financial institutions, cashout, and laundering funds. Gameover Zeus is known to be distributed via Cutwail botnet [76]. Gameover operators also often dropped other malware, such as CryptoLocker. The group behind Gameover was mainly composed of Russian and Ukrainian criminals, and this group also worked with third party actors to set up the systems.

Another interesting fact from Gameover Zeus is that it attacked less 'orthodox' governments, such as Georgia, Turkey, and Ukraine. In all these countries, Gameover targeted the government and especially the intelligence agencies. In an infographic from Symantec, U.S. and Italy are indicated as the hotspots of Gameover Zeus[12]. In May 30, 2014, the FBI, UK NCA (National Crime Agency), and Europol started "Operation Tovar", a joint effort to dismantle Gameover Zeus. This operation is still an ongoing effort. The operation has brought down the number the infections. The Shadowserver foundation has dedicated a special page[13] to monitor the progress of this

[12] Please refer to Appendix 5
[13] https://goz.shadowserver.org/stats/

operation. Indeed, since its takedown in May 2014, the presence of Gameover Zeus took a nosedive from 326,196 infected machines in June 2014, down to 52,196 infected machines in October 2015.

The scatter plots of occurrences of Gameover Zeus in the top 20 countries and its infection ratio measured against penetration rate are given in Figure 19 and Figure 20 respectively as follows.

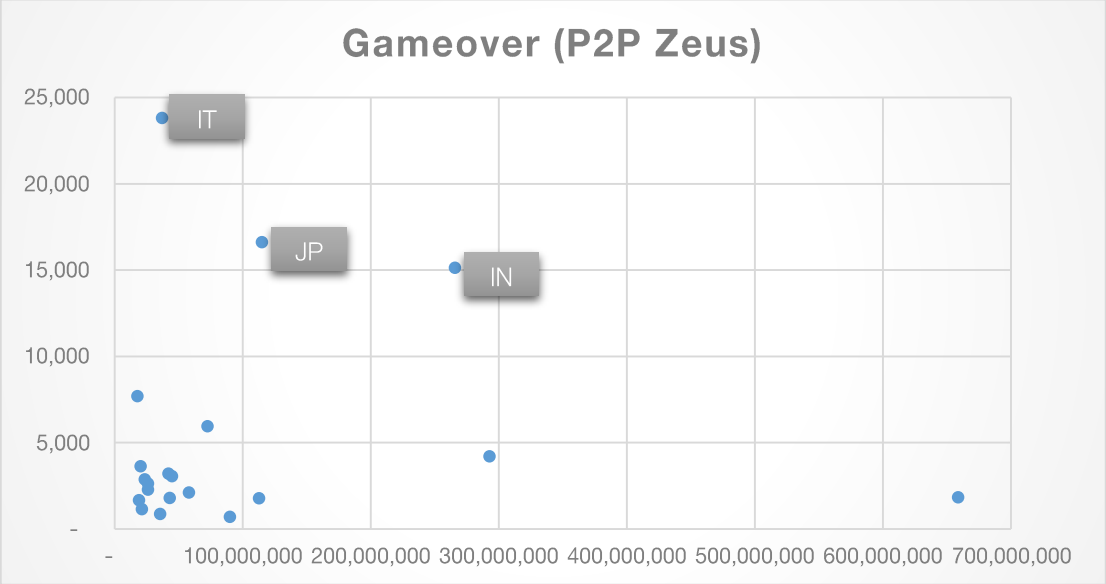


Figure 19 Occurrences of Gameover Zeus in the top 20 countries

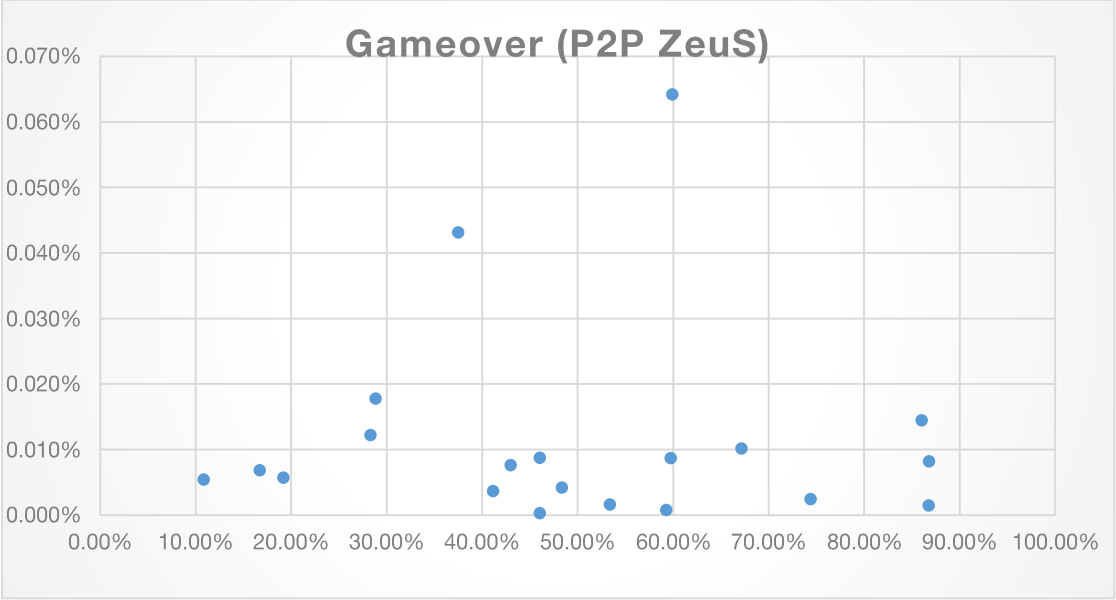


Figure 20 Infection ratio of Gameover Zeus in the top 20 countries

It is shown in Figure 19 that most of the countries listed below have enjoyed the benefits from Operation Tovar, namely having lower than 10,000 infections. Three countries stand out as having relatively high infection: Italy, India, and Japan. This is almost consistent with The Shadowserver statistics, with the only difference being Japan is identified as the most infected country followed by Italy and India. Clearly, the U.S is no longer identified

as the most infected country after the takedown effort. However, Italy still shows up in the most infected countries list. Japan, which has been badly hit by various banking malwares in the past, will need to put a rigorous cleanup effort in place to vindicate its reputation. Figure 20 does not show a meaningful relation between infection ratio and penetration rate. This can be partially explained by the fact that the infections in most countries are only 'residual', meaning that in very little cases do we encounter new infections. This is indeed supported by The Shadowserver dataset that shows a declining worldwide trend in Gameover Zeus infection from June 2014 until October 2015.

The fact that Gameover Zeus is mostly transmitted through Cutwail raises an interesting question: Does the data of Cutwail and Gameover Zeus show any relation, namely the countries where Cutwail are identified the most are the countries from where Gameover Zeus are being sent most? The answer to this question, however, is not simple. Cutwail is not exclusively used to send Gameover Zeus. Cutwail is also used to send Upatre downloader, which in turn will download Dyre. A further refining of a complete dataset will be needed to analyze this relationship and segregate which spams contain which malware. However, the Spamhaus dataset still provides a good picture of which countries still need further cleanup action after the massive takedown effort.

VI. LIMITATIONS

In conducting this research, there have been several, sometimes unavoidable, limitations that clearly influence the outcome of the research. Internally speaking, the Spamhaus dataset that is available contains only a snapshot of timeline, which forces the research to be a cross-sectional one, instead of a longitudinal one. Had there a more comprehensive dataset available, this research would have been able to answer more long-term related questions such as: How does the trend of botnet X look for the past half year or past year? Can the future trend of botnet Y be predicted using the available dataset? etc.

In order to compensate for the lack of 'long-term' dataset, the author has resorted to publicly available external data source in the Internet. However, this effort also bore few fruits, for several reasons. Firstly, there is no comprehensive dataset that tracks the fluctuation of each botnet since it was first detected until recently. In most of the cases, the author could only find snapshots for a specific period of time. Moreover, these snapshots come from different sources, which might provide a somewhat distorted view of the history of the botnet. Secondly, even if there were such dataset, they are not publicly available in the Internet. Researchers may prefer to keep the dataset undisclosed, perhaps for confidentiality and ethical reasons. Thirdly, the use of multiple data sources is sometimes good in triangulating the validity of a particular data, but in this case, by doing so the author ran into the risk of inconsistency. Although very difficult to achieve, compiling the historical data of a botnet into a centralized source would help in constructing an unbiased view in this research.

VII. CONCLUSIONS

The results of this research reveal that there is not a discernable pattern from which a strong conclusion can be derived from all types of botnets analyzed. The distribution of these botnets differ from each other and therefore each of them needs to be studied within a contextual level. The plots of infection ratio-penetratrion rate also do not paint a consistent image across the different types of botnets. In most of the cases, generally there are

relatively low level of infections for most of the countries compared to one, two, or three countries that stand out from the rest. Therefore, it is more expedient to study where these "irregularities" appear and dig into these phenomena.

Notwithstanding the irregularities, there are still many insights (albeit inconsistent) that can be gained from the results of Section V. For example, it is imminent that Conficker's distribution can be much attributed to software piracy, because it flourishes in countries with high rate of software piracy. This in turn, correlates with the propagation mechanism of Conficker, which is through an executable file. These types of executables are often masked as cracks and serial keys to bypass software authentication mechanisms. This pattern is also visible in the distribution of Cutwail, but not with ZeroAccess. Although it also relies on executable files as an infection vector, ZeroAccess is mostly injected through social engineering techniques. This shows that software piracy alone cannot explain why several botnets are very prolific in certain countries, although the propagation mechanisms are similar.

Another interesting insight is related to spam-sending botnets. For instance, Gamut's presence is especially high in Vietnam but not in other countries. While there has been contrasting opinions on whether spam-sending bots prefer to inhabit developed countries or not, the results here show that Gamut is ubiquitous in a country with relatively average penetration rate. This is also happening with Cutwail, which prospers more in China and India, countries with relatively low to medium penetration rate. This may provide new evidence on spam-sending botnet rampaging countries that might not have superb Internet connectivity.

Lastly, it is also thought-provoking to analyze the behavior of banking botnets in the list. According to the existing research, it is expected that these botnets (especially those with information-stealing capabilities) might prefer to infect computers in wealthy countries. The reasons for these botnets attacking certain have been independently discussed, but there is an inconsistency between the different banking botnets. For example, Dyre is found in India, but also Vietnam. These countries differ a lot in GDP. Zeus, however, is highly present in Japan, which is considerably wealthy compared to other countries. Tinba has just started to attack Russia, but also Poland and Indonesia, countries that rarely show up in the hit list of banking botnets. A preliminary suggestion is to conduct more extensive research to see whether these banking botnets actually prefer to attack certain continents instead of just countries, or whether a country's wealth is just

The bottom line is these factors cannot be looked in isolation, one or more factors need to be collectively taken into account in order to explain the unique distribution of a specific type of botnet. There are a lot of other factors that were not taken into account in this research, for example language barrier. Do specific types of botnet only attack English-speaking countries or those using Latin alphabet, or do specific types of botnet actually attack countries that speak totally different languages to mask the whereabouts of its origin? These are ideas for more research in the future. Nevertheless, the results of this research can provide additional insights and challenge many widely-held beliefs in explaining the behavior of botnets. By understanding these different factors, policy-makers and security researches can formulate more comprehensive solutions to tackle specific botnets.

REFERENCES

[1] S. S. Silva, R. M. Silva, R. C. Pinto and R. M. Salles, "Botnets: A survey," *Computer Networks,* vol. 57, pp. 378-403, 2012.

[2] W. van der Wagen and W. Pieters, "From Cybercrime to Cyborg Crime: Botnets as Hybrid Criminal Actor-Networks," *British Journal of Criminology,* vol. 55, no. 3, pp. 578-595, 2015.

[3] M. Feily, A. Shahrestani and S. Ramadass, "A Survey of Botnet and Botnet Detection," in *Third International Conference on Emerging Security Information, Systems and Technologies, 2009. SECURWARE '09.* , Athens, 2009.

[4] A. Stevenson, "Botnets infecting 18 systems per second, warns FBI," 16 July 2014. [Online]. Available: http://www.v3.co.uk/v3-uk/news/2355596/botnets-infecting-18-systems-per-second-warns-fbi. [Accessed 8 November 2015].

[5] Z. Bu, P. Bueno, R. Kashyap and A. Wosotowsky, "The New Era of Botnets," McAfee, 2013.

[6] H. Tiirmaa-Klaar, J. Gassen, E. Gerhards-Padilla and P. Martini, Botnets, Springer, 2013.

[7] Dell SecureWorks, "Banking Botnets Persist Despite Takedowns," Dell SecureWorks, 2015.

[8] Symantec, "Internet Security Threat Report," Symantec, Mountain View, 2015.

[9] E. Alomari, S. Manickam, B. Gupta, S. Karuppayah and R. Alfaris, "Botnet-based Distributed Denial of Service (DDoS) Attacks on Web Servers: Classification and Art," *International Journal of Computer Applications,* vol. 49, no. 7, pp. 24-32, 2012.

[10] V. L. Thing, M. Sloman and N. Dulay, "A Survey of Bots Used for Distributed Denial of Service Attacks," in *IFIP International Federation for Information Processing, Volume 232, New Approaches for Security, Privacy and Trust in Complex Environments*, Boston, Springer, 2007, pp. 229-240.

[11] B. Stone-Gross, T. Holz, G. Stringhini and G. Vigna, "The Underground Economy of Spam: A Botmaster's Perspective of Coordinating Large-Scale Spam Campaigns," in *4th USENIX Workshop on Large-scale Exploits and Emergent Threats*, Boston, 2011.

[12] J. Iedemska, G. Stringhini, R. Kemmerer, C. Kruegel and G. Vigna, "The Tricks of the Trade: What Makes Spam Campaigns Successful?," in *IEEE Symposium on Security and Privacy 2014 Workshops*, San Jose, 2014.

[13] M. Kammerstetter, C. Platzer and G. Wondracek, "Vanity, Cracks and Malware: Insights into the Anti-Copy Protection Ecosystem," in *Proceedings of the 2012 ACM Conference on Computer and Communications Security*, Raleigh, 2012.

[14] A. Kleiner, P. Nicholas and K. Sullivan, "Linking Cybersecurity Policy and Performance," Microsoft Trustworthy Computing, 2013.

[15] The Software Alliance, "BSA Global Software Survey," The Software Alliance, 2014.

[16] H. Asghari, M. Ciere and M. J. van Eeten, "Post-Mortem of a Zombie: Conficker Cleanup after Six Years," in *Proceedings of the 24th USENIX Security Symposium*, Washington, D.C., 2015.

[17] S. Shin, G. Gu, N. Reddy and C. Lee, "A Large-Scale Empirical Study of Conficker," *IEEE Transactions on Information Forensics and Security,* pp. 676-690, 2012.

[18] The Rendon Group, "Conficker Working Group: Lessons learned," 2011.

[19] M. Hypponen, "The Conficker Mystery," 2009.

[20] S. R. Hunt, "Conficker worm believed to have originated from China," 30 March 2009. [Online]. Available: http://www.tgdaily.com/security-features/41883-conficker-worm-believed-to-have-originated-from-china. [Accessed 2 November 2015].

[21] J. McEntegart, "Reports: Conficker From China, Easily Detected," 30 March 2009. [Online]. Available: http://www.tomshardware.com/news/Conficker-Worm-China-Antivirus-virus,7413.html. [Accessed 2 November 2015].

[22] R. McMillan, "Chinese ISP hosts 1 in 7 Conficker infections," 17 December 2009. [Online]. Available: http://www.computerworld.com/article/2522107/network-security/chinese-isp-hosts-1-in-7-conficker-infections.html. [Accessed 2 November 2015].

[23] O. Fletcher, "China Reports Millions of Conficker Worm Infections," 2010. [Online]. Available: http://www.pcworld.com/article/194380/article.html. [Accessed 2 November 2015].

[24] L. Desiderá, "Anti-botnet Initiatives," in *APWG CeCOS VII*, Buenos Aires, 2013.

[25] S. Mittal, "India has around 25,000 PCs infected with Conficker," 7 April 2009. [Online]. Available: http://techwhack.co/conficker-india/. [Accessed 2 November 2015].

[26] T. Rains, "The Threat Landscape in Pakistan: One of the Most Active in the World," 23 January 2013. [Online]. Available: http://blogs.microsoft.com/cybertrust/2013/01/23/the-threat-landscape-in-pakistan-one-of-the-most-active-in-the-world/. [Accessed 2 November 2015].

[27] R. Mendrez, "Gamut Spambot Analysis," 4 March 2014. [Online]. Available: https://www.trustwave.com/Resources/SpiderLabs-Blog/Gamut-Spambot-Analysis/. [Accessed 2 November 2015].

[28] M. Palatino, "Decree 72: Vietnam's Confusing Internet Law," 8 August 2013. [Online]. Available: http://thediplomat.com/2013/08/decree-72-vietnams-confusing-internet-law/. [Accessed 2 November 2015].

[29] Symantec Security Response, "Dyre emerges as main financial Trojan threat," 23 June 2015. [Online]. Available: http://www.symantec.com/connect/blogs/dyre-emerges-main-financial-trojan-threat. [Accessed 3 November 2015].

[30] Symantec, "Dyre: Emerging threat on financial fraud landscape," Symantec, Mountain View, 2015.

[31] J. Leyden, "Dyre times ahead: Zeus-style trojan slurps your banking login creds," 8 July 2015. [Online]. Available: http://www.theregister.co.uk/2015/07/08/dyre_banking_trojan_spam_surge/. [Accessed 3 November 2015].

[32] Blueliv, "Chasing cybercrime: Network insights of Dyre and Dridex Trojan bankers," Leap in Value, 2015.

[33] S. Singh and Y. Wang, "Dyre Banking Trojan Exploits CVE-2015-0057," 7 July 2015. [Online]. Available: https://www.fireeye.com/blog/threat-research/2015/07/dyre_banking_trojan.html. [Accessed 3 November 2015].

[34] E. Kovacs, "Dyre Trojan Uses Semi-Random File Names to Evade Detection," 24 August 2015. [Online]. Available: http://www.securityweek.com/dyre-trojan-uses-semi-random-file-names-evade-detection. [Accessed 3 November 2015].

[35] A. Carman, "Dyre malware infections surge in 2015," 02 June 2015. [Online]. Available: http://www.scmagazine.com/trend-micro-documents-new-malware-infections/article/418266/.

[36] N. Falliere and E. Chien, "Zeus: King of the Bots," Symantec Security Response, 2009.

[37] S. Tajalizadehkhoob, H. Asghari, C. H. Gañán and M. J. van Eeten, "Why Them? Extracting Intelligence about Target Selection from Zeus Financial Malware," in *13th Annual Workshop on the Economics of Information Security, Pennsylvania State University*, Pennsylvania, 2014.

[38] L. M. Ibrahim and K. H. Thanoon, "Detection of Zeus Botnet in Computers Networks and Internet," *International Journal of Information Technology and Business Management,* vol. 6, no. 1, pp. 84-89, 2012.

[39] A. K. Sood, S. Zeadally and R. J. Enbody, "An Empirical Study of HTTP-based Financial Botnets," *IEEE Transactions on Dependable and Secure Computing,* vol. PP, no. 99, 2014.

[40] BBC, "More than 100 arrests, as FBI uncovers cyber crime ring," BBC, 2 October 2010. [Online]. Available: http://www.bbc.com/news/world-us-canada-11457611. [Accessed 4 November 2015].

[41] G. Keizer, "Microsoft's anti-Zeus tool cleans quarter-million PCs," Computerworld, 18 October 2010. [Online]. Available: http://www.computerworld.com/article/2513356/security0/microsoft-s-anti-zeus-tool-cleans-quarter-million-pcs.html. [Accessed 4 November 2015].

[42] Symantec Security Response, "Zeus Now Setting its Sights on Japanese Online Banking Customers," Symantec Official Blog, 11 February 2013. [Online]. Available: http://www.symantec.com/connect/blogs/zeus-now-setting-its-sights-japanese-online-banking-customers. [Accessed 4 November 2015].

[43] P. Pearce, C. Grier, V. Paxson, V. Dave, D. McCoy, G. M. Voelker and S. Savage, "The ZeroAccess Auto-Clicking and Search-Hijacking Click Fraud Modules," 2013.

[44] Gadgets 360, "India ranks third among ZeroAccess botnet infected countries: Symantec," NDTV, 4 October 2013. [Online]. Available: http://gadgets.ndtv.com/internet/news/india-ranks-third-among-zeroaccess-botnet-infected-countries-symantec-426399. [Accessed 4 November 2015].

[45] A. Neville and R. Gibb, "ZeroAccess Indepth," Symantec, 2013.

[46] P. Pearce, V. Dave, C. Grier, K. Levchenko, S. Guha, D. McCoy, V. Paxson, S. Savage and G. M. Voelker, "Characterizing Large-Scale Click Fraud in ZeroAccess," in *Computer and Communications Security 2014*, Arizona, 2014.

[47] J. Wyke, "ZeroAccess," Sophos.

[48] Microsoft News Center, "Microsoft, the FBI, Europol and industry partners disrupt the notorious ZeroAccess botnet," Microsoft, 5 December 2013. [Online]. Available: http://news.microsoft.com/2013/12/05/microsoft-the-fbi-europol-and-industry-partners-disrupt-the-notorious-zeroaccess-botnet/. [Accessed 4 November 2015].

[49] M. J. Schwartz, "Microsoft Fails To Nuke ZeroAccess Botnet," Dark Reading, 10 December 2013. [Online]. Available: http://www.darkreading.com/attacks-and-breaches/microsoft-fails-to-nuke-zeroaccess-botnet/d/d-id/1113008. [Accessed 5 November 2015].

[50] Dell SecureWorks, "ZeroAccess botnet resumes click-fraud activity after six-month break," Dell, 29 January 2015. [Online]. Available: http://www.secureworks.com/resources/blog/zeroaccess-botnet-resumes-click-fraud-activity-after-six-month-break/. [Accessed 5 November 2015].

[51] Dell SecureWorks, "Popular Banking Trojan Attacks Top Russian Banks and Russian Payment Service Providers, Reports Dell SecureWorks," 3 November 2015. [Online]. Available: http://www.secureworks.com/assets/pdf-store/other/Media-Alert-Popular-Banking-Trojan-Attacks-Top-Russian-Banks_3.pdf. [Accessed 5 November 2015].

[52] P. Kruse, F. Hacquebord and R. McArdle, "W32.Tinba (Tinybanker): The Turkish Incident," CSIS & Trend Micro, 2012.

[53] P. Asinovsky, "Tinba Malware Analysis," F5, 2014.

[54] O. Bach, "Tinba: World's Smallest Malware Has Big Bag of Nasty Tricks," 9 June 2015. [Online]. Available: https://securityintelligence.com/tinba-worlds-smallest-malware-has-big-bag-of-nasty-tricks/#.VXai4fnF-Sr. [Accessed 5 November 2015].

[55] C. Osborne, "Suspected hackers behind Carberp botnet, Eurograbber arrested," 5 April 2013. [Online]. Available: http://www.zdnet.com/article/suspected-hackers-behind-carberp-botnet-eurograbber-arrested/. [Accessed 5 November 2015].

[56] B. Stone-Gross, Interviewee, *Why Tinba Trojan Is Now a Global Concern.* [Interview]. 4 November 2015.

[57] CERT Polska, "CERT Polska Report 2014," NASK, Warsaw, 2015.

[58] N. Villeneuve, J. d. Torre and D. Sancho, "Asprox Reborn," Trend Micro, 2013.

[59] L. Wichman, "Mass SQL Injection for Malware Distribution," SANS Institute, 2010.

[60] D. Danchev, "Sony PlayStation's site SQL injected, redirecting to rogue security software," 2 July 2008. [Online]. Available: http://www.zdnet.com/article/sony-playstations-site-sql-injected-redirecting-to-rogue-security-software/. [Accessed 5 November 2015].

[61] Y. Shin, S. Myers and M. Gupta, "A Case Study on Asprox Infection Dynamics," in *Detection of Intrusions and Malware, and Vulnerability Assessment*, Springer, 2009, pp. 1-20.

[62] A. Stewart and G. Timcang, "A Not-So Civic Duty: Asprox Botnet Campaign Spreads Court Dates and Malware," 16 June 2014. [Online]. Available: https://www.fireeye.com/blog/threat-research/2014/06/a-not-so-civic-duty-asprox-botnet-campaign-spreads-court-dates-and-malware.html. [Accessed 5 November 2015].

[63] Unit 42, "Threat Trend: Threat Landscape Review," Palo Alto Networks, Santa Clara, 2014.

[64] R. Abel, "Asprox botnet mostly disappeared in 2015," 14 August 2015. [Online]. Available: http://www.scmagazineuk.com/asprox-botnet-creators-may-be-on-hiatus-after-botnets-not-detected-all-year/article/432740/. [Accessed 5 November 2015].

[65] Trend Micro, "Threat Encyclopedia: Cutwail," 20 August 2013. [Online]. Available: http://www.trendmicro.com/vinfo/us/threat-encyclopedia/malware/CUTWAIL. [Accessed 5 November 2015].

[66] A. Decker, D. Sancho, L. Kharouni, M. Goncharov and R. McArdle, "Pushdo/Cutwail Botnet: A Study on the Pushdo/Cutwail Botnet," Trend Micro, 2009.

[67] Dragon Research Group, "Pushdo distribution," Dragon Research Group, 2010.

[68] M. Casayuran, "CUTWAIL Spambot Leads to UPATRE-DYRE Infection," TrendMicro, 16 October 2014. [Online]. Available: http://blog.trendmicro.com/trendlabs-security-intelligence/cutwail-spambot-leads-to-upatre-dyre-infection/. [Accessed 8 November 2015].

[69] Fidelis Threat Advisory, "Pushdo It to Me One More Time," Fidelis Cybersecurity, 2015.

[70] McAfee, "McAfee Labs Threat Advisory: Rimecud," McAfee, 2011.

[71] BitDefender, "Extremely aggressive worm chokes instant messaging," 3 May 2010. [Online]. Available: http://www.bitdefender.com/news/extremely-aggressive-worm-chokes-instant-messaging-1514.html. [Accessed 6 November 2015].

[72] DefenceIntelligence, "Mariposa Botnet Briefing".

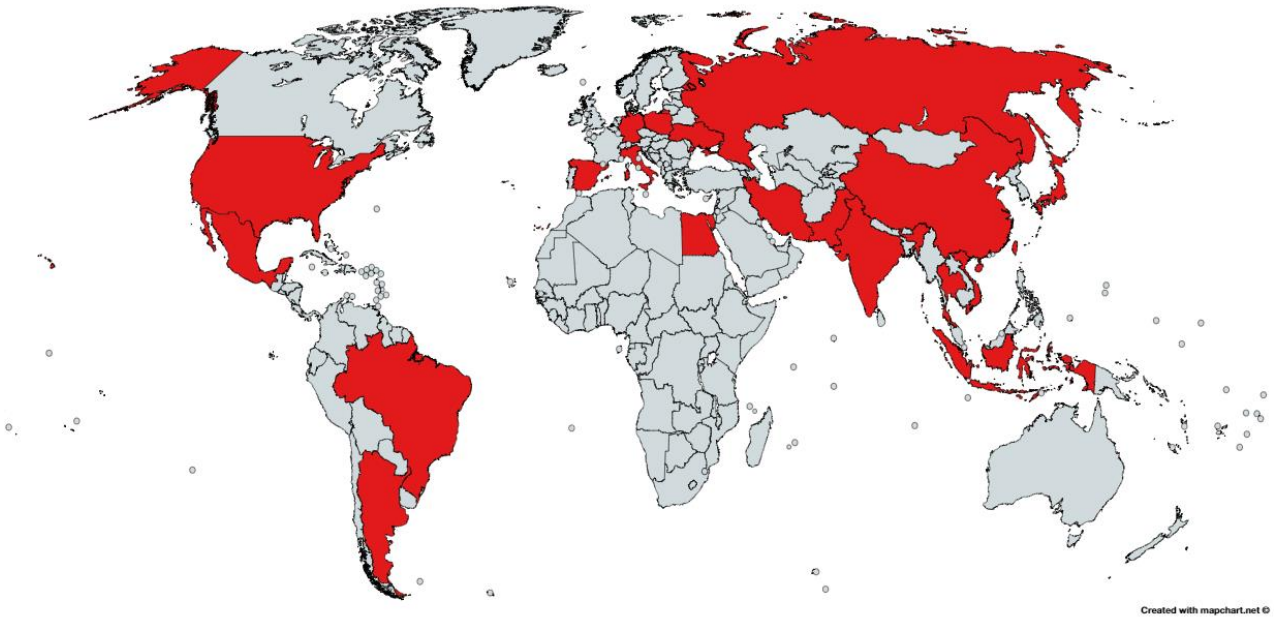
[73] J. De La Torre, "Mariposa/PALEVO on the Rise Again," 25 May 2011. [Online]. Available: http://blog.trendmicro.com/trendlabs-security-intelligence/mariposapalevo-on-the-rise-again/. [Accessed 6 November 2015].

[74] Intel Security, "W32/Rimecud," McAfee, 22 July 2013. [Online]. Available: http://www.mcafee.com/threat-intelligence/malware/default.aspx?id=237984. [Accessed 6 November 2015].

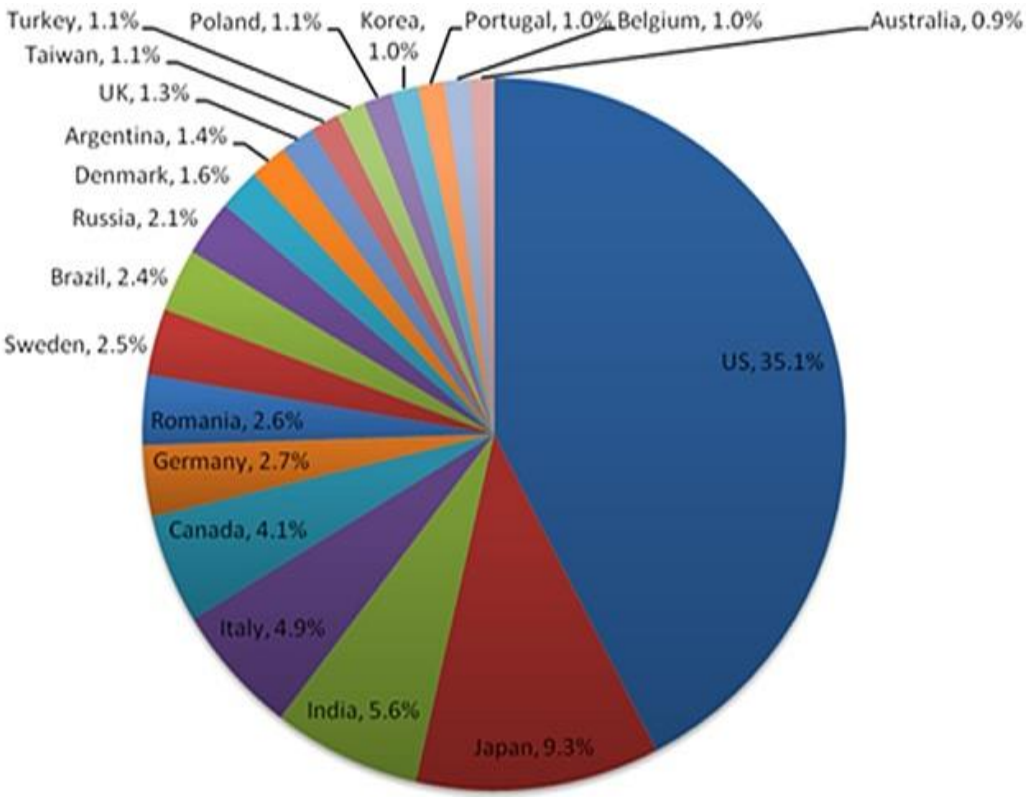
[75] M. Sandee, T. Werner and E. Peterson, "Gameover Zeus – Bad Guys and Backends," 5 August 2015. [Online]. Available: https://www.blackhat.com/docs/us-15/materials/us-15-Peterson-GameOver-Zeus-Badguys-And-Backends.pdf. [Accessed 7 November 2015].

[76] B. Stone-Gross, "The Lifecycle of Peer-to-Peer (Gameover) ZeuS," Dell SecureWorks, 23 July 2012. [Online]. Available: http://www.secureworks.com/cyber-threat-intelligence/threats/The_Lifecycle_of_Peer_to_Peer_Gameover_ZeuS/. [Accessed 7 November 2015].

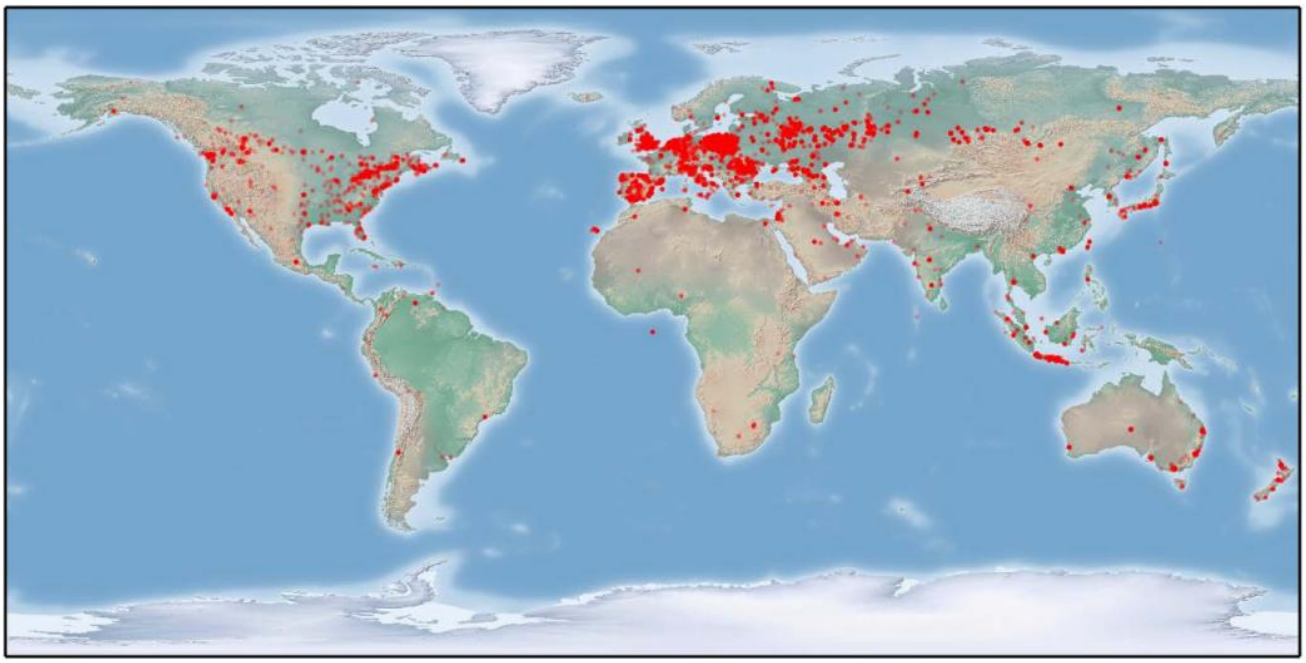
Appendix 1 Top 20 countries



Appendix 2 Distribution of ZeroAccess per August 2013 [44]



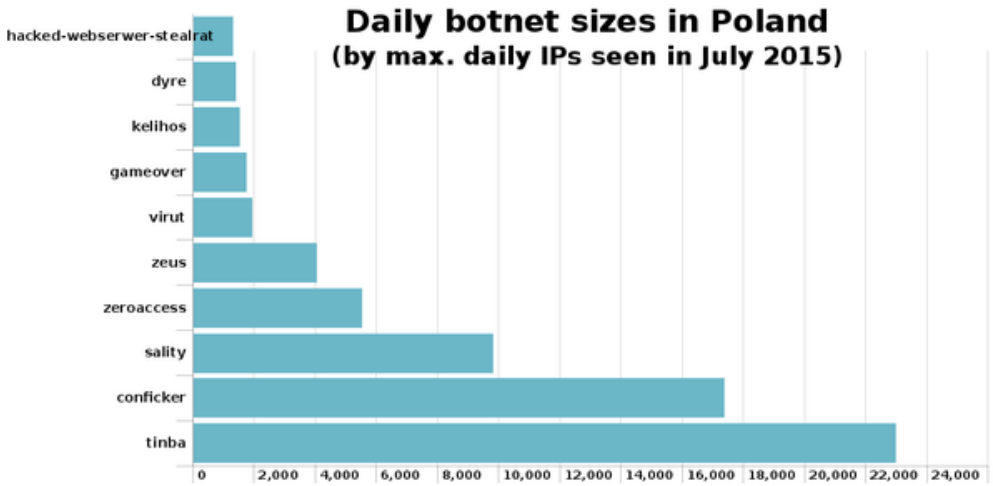
Appendix 3 Map and ranking of Tinba 2.0 infections on October 15, 2015 [51]

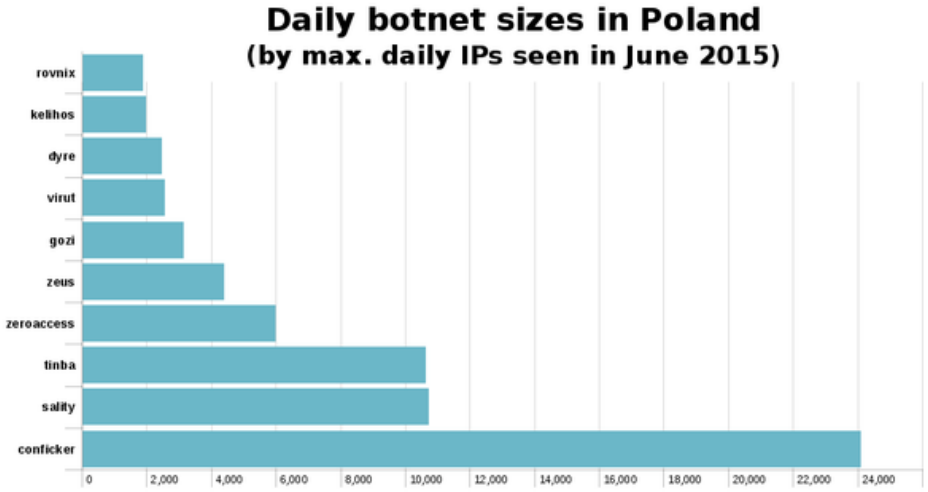


Top 10 affected countries:

1. Russia (34.5%)
2. Poland (22.0%)
3. Indonesia (7.2%)
4. Spain (6.5%)
5. Canada (5.6%)
6. Romania (5.0%)
7. Germany (2.6%)
8. Australia (1.8%)
9. United Kingdom (1.8%)
10. Japan (1.7%)

Appendix 4 Ranking of top botnets in Poland, June 2015 and July 2015





Appendix 5 Top 6 countries affected by Gameover Zeus 2013/2014