Accounting for Variation in Spam Effectivness

Shaddi Hasan, Aurojit Panda, Colin Scott

July 27, 2013

1 Introduction

Cybercrime today is a profit-driven enterprise. Viewing computer security through the lens of business incentives in this way helps guide the efforts of policy-makers and researchers, since the effectiveness of countermeasures is directly related to their effect on cybercriminals' profit motives, the root causes of cybercrime.

In this respect, understanding the structure of the cybercrime marketplace is a crucial task for the security community. Recent work provides some insight into different aspects of this so-called "underground economy", such as PPI pricing factors [1], as well as the supply [2] and demand [3, 4] for spam.

One striking finding from this line of work is that the value placed on various resources used in cybercrime – *e.g.* infected zombie machines or spam targets – appears to vary by the level of economic development of the country where the resource is located. For example, PPI prices cited in [**?**] indicate that the price of a bot machine in the United States costs *1-2 orders of magnitude* more than a bot located in "Asia"[1].

Understanding what drives this variation is vital to understanding the cybercrime underground economy. Variation in pricing could be due to *supply-side* factors, such as increased availability, or it could be due to *demand-side* factors, such as targets in certain locations being more lucrative; the final market price of a resource is driven by both. Untangling the significance of supply-side and demand-side factors from this market price is a fundamentally challenging problem without access to cybercriminals' accounting information.

Unable to directly measure the influence of each of these factors, the research community has turned to an indirect approach to this problem. For example, price variation in PPI prices driven by supply-side factors can be corrolated with the density of vulnerable computers in a given geographic region.

In this paper, we attempt to use this indirect measurement approach to analyze one facet of cybercrime: spam. A spammer places a higher demand on users for whom they are able to get higher revenue per spam conversion. Likewise, the marginal cost of spamming resources (*e.g.* bots in a particular IP address block) is related to how easily those those resources can obtain conversion from their spam targets.[2] We focus on the latter, the supply-side characteristics of spam.

In particular, we investigate a finding from the Spamalytics data [3]: both click and conversion rates for spam differs by geographic region. Our hypothesis is that this is due variation in the type of spam filtering place between the spammer and the user's inbox, a supply-side factor.

More specifically, our hypothesis is that spam filtering rates across email domains can be correlated with the level of development of the country in which they are located, as measured by GDP (PPP) per capita. We developed this hypothesis based on the observation that Indian and Pakistani visitors accounted for a disproportionate amount of spam click-throughs measured in the Spamalytics study. If our hypothesis were true, we would have direct evidence that mail servers in poor countries are more susceptible to spam than those in rich countries. We would also have indirect evidence that cybercrime pricing variation is driven by supply-side factors, since decreased usage of anti-spam technology is an indication of decreased sophistication of a country's general network security infrastructure.[3]

Our measurements have shown that our hypothesis does not appear to be true: we find no significant correlation between the level of income of a country and the resistance to spam demonstrated by domains hosted in that country, as measured by multiple independent metrics of spam resistance. In particular, we found no relationship between country income level and spam accept rates, spam click-through rates, deployment rates of anti-spam systems, rates of inferred blacklist usage per domain, or

[1] broadly defined by the source

[2] We assume all people have equal probability of click on a spam message that reaches their attention.

[3] By "indirect evidence" here, we mean only that such a finding would suggest that this may be true, or at least worthy of further investigation; we do not make any claim in this paper to answer the high-level supply versus demand question.

SMTP server software versions.

We describe these measurement results in the remainder of this paper. We first describe related work in Section 2. Section 3 describes the datasets that we used, as well as the underlying assumptions used throughout this project. Section 4 describes our experimental methodology. We consider the implications of our results, the cross-validation relationship of our individual experiments, and the shortcomings of our study design in Section 5 before concluding in Section 6.

2 Related Work

We consider three categories of related measurement studies and methodologies: spam blacklisting measurement, studies of spam in developing regions, and geolocation.

Spam Blacklisting. The work that is closest to ours is [3]. Our primary data source comes from the Spamalytics email traces. Spamalytics gathered statistics without regard to national boundaries, and while some of their analysis shows that people in certain countries are more likely to click through on receiving spam, no analysis was done to measure the precise reason. Samalytics also analyzed the rate at which a few DNS blacklists were updated, and how quickly MX agents responded to these updates. While these studies gave substantiative answers to the rate at which blacklists were updated and their use, the analysis was not motivated by differences in economic background, and took a broader view than our study. Our analysis complements this global analysis, by testing the hypothesis that this difference in click-through rates was based on the efficiency of blacklisting across countries, rather than purely on cultural differences.

We attempt to measure the effectiveness of DNS blacklisting, and other spam filtering techniques across countries. The effectiveness of DNS blacklisting in general has been well-studied, particularly in [5] and [6]. Studies such as [7] have shown a noticeable reduction in spam, and the change in distribution that can be attributed to the advent of DNS blacklisting.

As demonstrated by [8], DNS-based blacklists are not entirely effective. This is due in part to botnet operators using evidence of blacklist listing to measure the effectiveness of their SMTP servers. Other projects ([9]) have also suggested alternate detection mechanisms for spam based on DNS blacklisting, where they explore the effects of such blacklisting, in particular demonstrating a mechanism for content-independent recognition of spam, based on a belief that botnets can easily tailor e-mails to individual users, and broad content based spam filtering can be easily defeated.

Spam in Developing Regions Developing countries stand out for several reasons in analyzing spam. According to a 2005 OECD[4] report [10], spam has an even greater adverse effect on developing countries: because of limited resources and bandwidth, spam incurs a greater percentage cost for both users and network operators. In addition, developing nations tend to lack important organizational and legislative infrastructure to combat spam, such as CERTs or anti-spam legislation [11]. Indeed, non-OECD countries are actually some of the largest sources of outgoing spam as well [12], with India, Russian, Indonesia, and Brazil accounting for over 25% of worldwide spam. Developing world users have been specifically targeted by spam campaigns [13], suggesting that putting spam in this population's inbox is worthwhile for spammers. Attitudes towards spam are complex. While some users react to spam as a nuisance [11], others make substantial income from spam activities (e.g. the *419 scam*, which is typically conducted without the use of bulk email software) [14].

Geolocation. We rely on geolocation to determine the country-of-origin for client IP addresses. Several geolocation data sources exist, including delay measurements [15], DNS name matching [16], and commercial databases [17]. It has been demonstrated by [15] that IP geolocation can locate an address to within about 400 kms, however for our purpose country-level geolocation suffices.

3 Data

Our main results in this paper are derived from the Spamalytics data [3]. Specifically, we examine (i) spam messages sent by the Storm botnet, each containing the anonymized e-mail addresses at which spam was targeted and the recepient's full domain, (ii) positive delivery reports, asynchronously received from users' mail servers, and (iii) click data from the fake spam website administered by the Spamalytics researchers.

Because the Spamalytics researchers did not have access to the worker bots sending the spam messages, our data does not include SMTP network trace data such as TCP connection failure codes or original DNS records. We therefore found it necessary to re-resolve all DNS records for our analysis. Doing so four years later raises some concern that domains may have changed MX servers or may no longer exist. We addressed this to an

[4] Organization for Economic Co-operation and Development, an organization of 34 countries intended to stimulate economic progress and world trade

extent by eliminating all reports, and instructions to non-existent MX servers, we however do not account for MX servers that have moved. We describe the logistics of this effort below.

Measurement Infrastructure. We parallelized the task of resolving DNS records for user domains across 75 Vicci servers [18]. We found this level of parallelism necessary to finish the measurements in a reasonable timeframe, as there were over 19 million unique email domains in the Spamalytics dataset.

MX records. We first resolved MX records for each of the 19,488,876 domains in our dataset. Of these, 10,371,346 (53%) domains did not have an MX record registered in the DNS. We observe that a large number of domains are using third-party mail services such as gmail, which partially explains the low number of MX records found. We also suspect that the large number of unregistered domains is largely due to churn over the last four years since the Spam was originally sent. We performed the DNS resolutions twice to verify that our UDP probes were not dropped due to congestion; our second measurement round only found a small percentage increase in responses (.1% of total domains), indicating that packet loss was not a problem.

A records. We then resolved A records for each listed MX server, and found 4,843,504 unique IP addresses (46.7% of MX records). It appears that many MX servers do not have an associated A record. We again performed the resolution twice to verify that our probes were not experiencing packet loss, and found only a small increase in successful responses on the second measurement round.

Geolocation. Finally, we geolocated these IP addresses to a particular country using MaxMind's DNS-name based geolocation database [17][5] Our results are shown in a heat-map in Figure 2. In the figure, red signifies there were no servers in those countries, darker colors signify more servers. As can be observed a majority of these servers are in the United States. Figure 3 shows the distribution of MX servers across different locations. While only 0.1% of the servers are in *low income* countries, and 1.3% of servers are in *lower-middle income* countries, we believe these numbers reflect the actual truth on where IT infrastructure is located. Overall our data contained over 8.3 million servers, and hence we find that about 20000 of these servers are located in low and lower-middle income countries, which should be a sufficient population for us to draw some conclusions from our data.

Correlation. The positive delivery reports from users' mail servers are delivered asynchronously back to the sending worker, which reports them back to the original proxy. Since workers might be talking to more than one proxy over the period of observation, there are successful reports for which we have no corresponding instruction, and there might be instructions for which we have been unable to observe successful delivery. To reduce bias because of these effects, we first filter out all instructions and reports associated with workers for whom we don't have at least one instruction, and one report, *i.e.*a worker must appear to have both reported successful delivery at some point, and received instructions at some point. Furthermore, we eliminate all successful report for which we don't have a corresponding instruction.

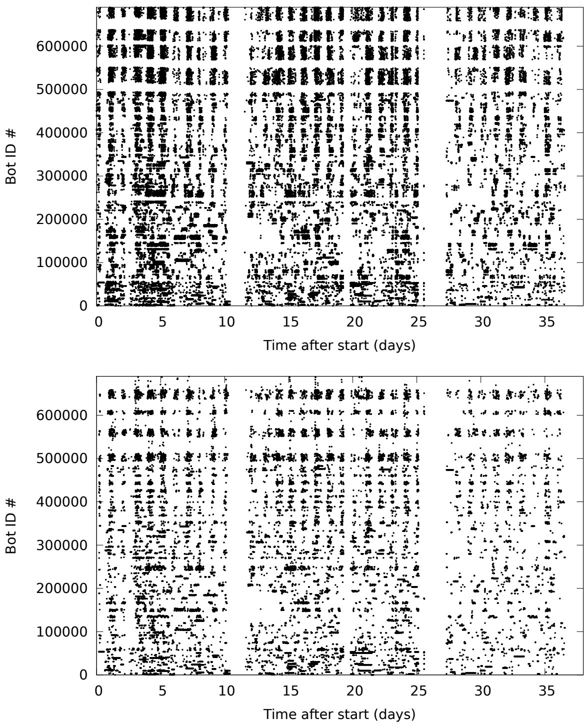

Figure 1: Each point represents a batch of spam instructions (top) or delivery reports (bottom) seen in dataset. Bot ID # is an arbitrary unique identifier assigned to each bot. Horizontal empty spaces signify a bot that was seen infrequently in the dataset.

In order for the spammer to obtain a conversion, their spam message must get through three main filtering steps:

1. The spam message must be accepted by the recipient's mail server, bypassing *IP blacklisting*.
2. The message must reach the recipient's inbox, bypassing *content-based filtering*.

[5] We are not overly concerned with the accuracy of this geolocation method, since we are only interested in categorizing the location of MX servers by broad economic classification

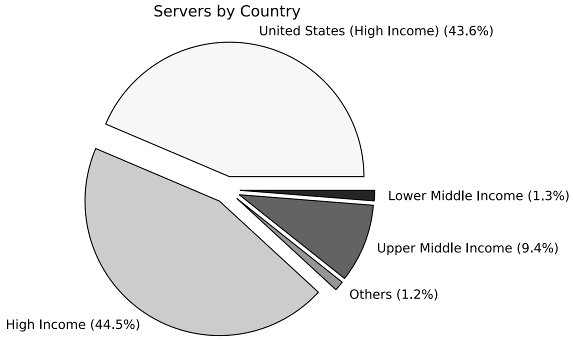

Figure 3: Location of MX servers by income level

3. The user must deem the message worthy of their attention, bypassing *user training and education*.

Our data includes messages that bypass filters (1) and (3). Without visibility into individual mail servers, we have no way of knowing what spam messages were delivered by then filtered based on their content before being presented to the user.

We separately looked at the batch structure of instructions and reports, and used that to investigate the prevalence of blacklisting.

3.1 Assumptions

Recall that our goal is to verify whether there is correlation between the sophistication of anti-spam IT infrastucture and the economic standing of the country in which the mail server resides. In answering this questions we make the following assumptions:

1. Spam filtering occurs either before a spam message is positively accepted by by users' mail server (IP blacklisting) or before the email enters users' main inboxes (Bayesian filtering), but not at any other point.

2. The organization responsible for configuring anti-spam protection for a domain is located in the same country as the geolocation result of the IP address of the domain's MX server.

3. All email users are equally likely to click on a spam message given that it has appeared in their inbox.

4 Methodology

In this section we present the analysis we performed to verify our hypothesis: we examined spam delivery (§4.1) and click (§4.2) rates normalized by country, the prevalance of explicit anti-spam mechanisms (§4.3), evidence of IP blacklist additions over time (§4.4), and finally the relative age of SMTP server version numbers (§4.5).

4.1 Spam Delivery Rates

Directly measuring security sophistication of mail servers is hard since countermeasures in use do not necessarily expose a publicly visible signature. Given this shortcoming, we rely on a measurement of the probability that a mail server accepts spam e-mail as one of our metrics of security sophistication. It is possible that a mail server might accept an e-mail that is filtered out by Bayesian filtering further down the line, however these effects are nearly impossible to measure without user involvement. There might also be other reasons, for instance a non-existent username, for mail delivery failing; given a sufficiently large sample, these effects should have minimal effect on our results.

We rely on data collected for the Spamalytics [3] project, as described previously. The Spamalytics data is collected by interposing between the botmaster's HTTP proxies and worker bots by controlling a few of the proxy bots. Worker bots can connect to several proxy bots, many of which are not under observation. This implies that there are instructions for which we receive no delivery reports, and there are delivery reports for which we have no instructions. While one cannot correct for these sources of bias completely, we attempt to reduce their effect in a couple of ways. Firstly we only use entries for worker bots for which we have both instructions, and successful delivery reports. It is possible that filtering in this manner might eliminate cases where a bot receives no successful responses, however the chances of this should be reasonably low. Such filtering eliminates 11% of the instructions, and 9% of reports. In addition, we also filter any reports for which we do not have a corresponding request. In particular we eliminate reports for those usernames, and domains for which we did not observe an instruction. This eliminates 6% of the reports.

We show our results from these computations in Figure 4, binned by income levels as defined by the World Bank [19]. Each bar represents spam delivery rates for countries in a particular income group. One can observe that the rates are fairly similar, and that no obvious correlation can be observed between income levels and delivery

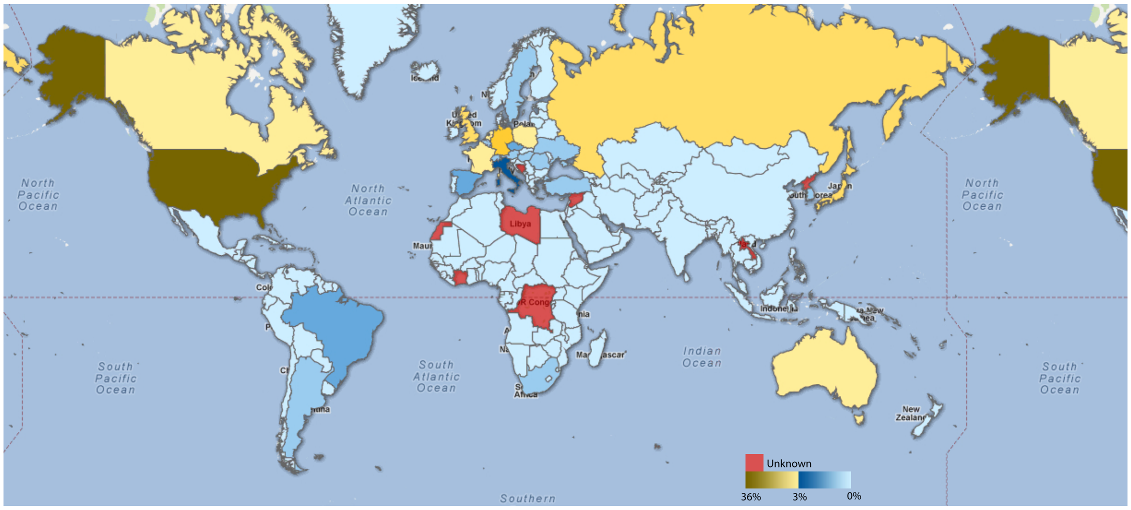

Figure 2: A heat map showing the location of MX servers in our data. The colors show the percentage of all MX servers in our data located in a certain country

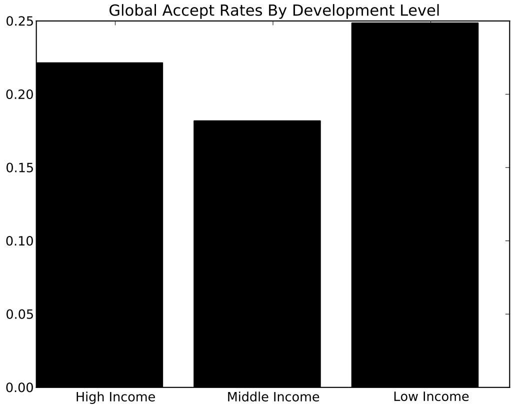

Figure 4: Spam Delivery Rates grouped by Income

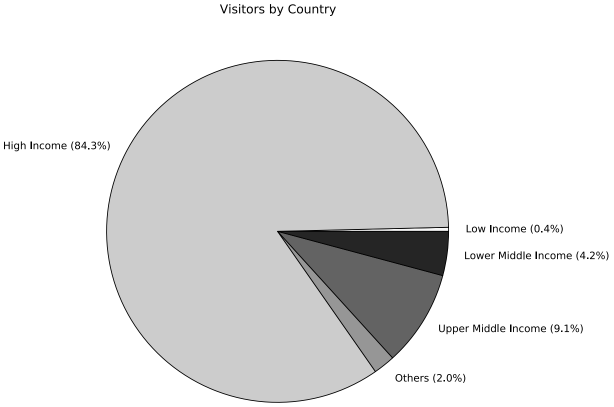

Figure 5: Location of visitors by income level

rates.

4.2 Clickthrough rates

In addition to spam instructions and delivery reports, we also had access to visitor logs from the fake spam website run by the Spamalytics researchers. While the anonymized data did not allow us to correlate delivery reports with visitors, we decided to measure probability that someone clicks on a link given a delivery report. This measurement provides an estimate of how much spam that is delivered to a server is likely to actually be seen. In particular, once an MX server accepts an e-mail, the e-mail might still be subject to content-based filtering and other filters which might prevent a user from looking at a spam e-mail. While it is also possible that user education also contributes to the likelihood that an individual in a particular country would click on a link, we have no data to measure this, particularly given the high variance in user education that could exist worldwide.

As stated in the Spamalytics paper, the authors observed relatively few visitors to their website compared to the volume of spam messages sent. This lack of visitors makes it harder to analyze some of this data given the sources of bias listed above. Figure 5 gives a breakdown

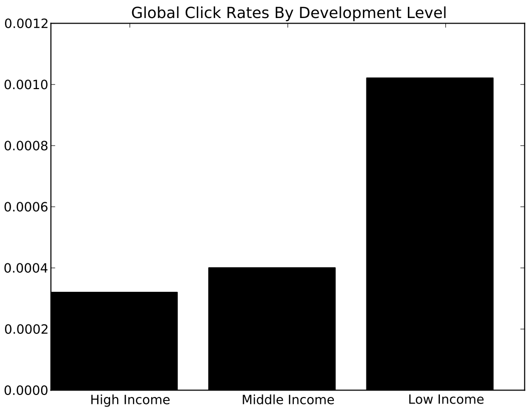

Figure 6: Click Rates by Income Levels

of where visitors came from, however our click log contains about 43,000 data points, and hence any conclusions we draw from these logs might be suspect. Figure 6 shows the observed click-rates. While the probability does appear to increase, one should note that these numbers vary between 0.02% and 0.1%, and are based on about a 170 click events for low income countries. We believe the data shows that the probability of visiting a page from countries with disparate income levels is roughly identical, and that we have no indication that there exists a correlation between income levels and click-through rates.

4.3 Explicit antispam deployment rates

One direct way to measure usage of anti-spam technology is to simply harvest obvious clues of anti-spam usage from DNS records for mail servers. While most mail servers have generic MX record names (e.g., `mx.example.com`), several mail server names were explicitly set with spam in mind. For every email domain from our original dataset of Storm instructions, We harvested mail servers whose name contained the words "spam", "fakemx", or "barracuda", as well as those whose MX record mapped to `localhost`.

These keywords are not a comprehensive set of all indications that a mail server is configured to block spam, but they do offer a basic indication of deployment rates of anti-spam technologies. In terms of language support, our dataset only contains domain names that use English characters. While we do use names of servers in non-English speaking countries, "spam" appears to be a commonly borrowed word from English. [6]

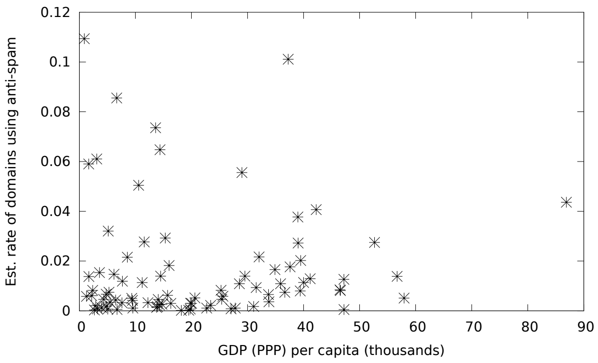

Figure 7: Anti-spam deployment rates versus GDP (PPP) per capita.

We considered all MX domain names which contained the words "spam", "fakemx", or "barracuda" to be indicative of domains which employed anti-spam technology. In addition, we also considered mail servers whose MX record mapped to `localhost` to be configured to prevent spam. We found approximately 190,000 unique domains whose mail servers matched these filters; these domains were distributed across 117 countries.

Figure 7 shows the relationship between percentage of domains which show evidence of anti-spam usage per country versus each country's GDP (PPP) per capita. Using a linear regression, we found $r^2 < 0.0001$ (Pearson correlation), suggesting no correlation between these two variables. With the weaker Spearman rank correlation coefficient, we obtained $\rho = 0.145$, again not statistically significant.

Admittedly, our set of filters is likely quite noisy: certainly many anti-spam devices don't advertise their existence in their MX record, and many anti-spam devices that do advertise were not included in our filter. In order to determine whether this low correlation resulted from such noise, or if there were some tenuous underlying relationship, we analyzed how the Spearman coefficient value changed as additional data was added to the plot. Intuitively, if there were some underlying relationship between these two variables, the explanatory power of the independent variable (in this case, GDP per capita) should remain constant as more data is added. In contrast, if there were actually no relationship, we would expect that the correlation coefficient would tend towards zero as more data was added. Indeed, the latter is what we observe, as shown in Figure 8. The fact that ρ varies between positive and negative before tending towards zero lends credence to the lack of any relationship between these two

[6] For example, the relevant page in the language-specific Wikipedia for French, German, and Spanish is titled "spam".

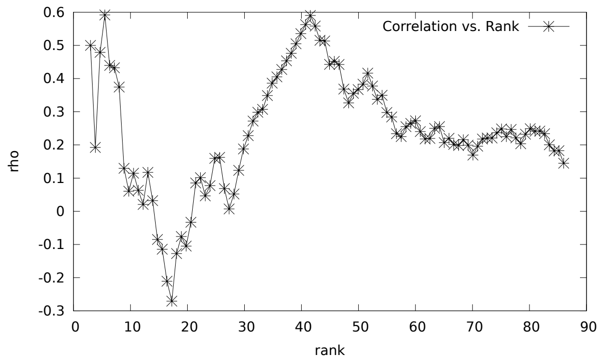

Figure 8: Spearman rank correlation coefficient versus rank included in calculation. Countries were ranked by GDP (PPP) per capita, and the correlation coefficient was calculated for each of the top N countries, where $N > 3$.

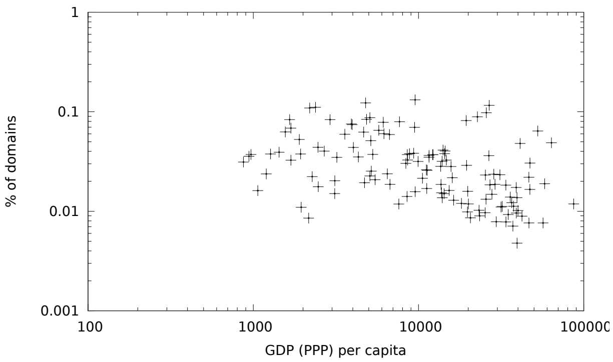

Figure 9: Percentage of domains showing evidence of blacklist usage per country versus GDP (PPP) per capita. Note the log/log axes.

variables.

4.4 Evidence of Blacklist Additions Over Time

If a domain is using IP blacklisting, it is likely to accept spam from a bot at first, and then stop accepting spam from that bot after it "learns" the bot's IP address is that of a spammer. This suggests a method to infer evidence of blacklist usage by a domain given a log of sent spam and spam delivery reports.

We can directly apply the structure of the Storm botnet data to employ this method. Storm issues spamming instructions in batches, and bots report successful deliveries in batches as well. If we see a delivery report from a domain, but see no further responses to subsequent delivery instructions, we define the domain as having "evidence of blacklist usage" (EBL).

As with all our metrics, this is only a rough estimate. The fact that our dataset may be missing arbitrary batches of both instructions and reports means that we may overestimate blacklist usage, since a missing batch of reports could cause a domain to meet our definition of EBL. Moreover, our definition of EBL does not capture all behaviors of a site that using blacklisting. For example, a site could subscribe to a blacklist feed on which a bot is present before that bot ever sends the site spam; in our data, this would manifest itself as simply an unacknowledged delivery attempt, and could cause the site to show no EBL. Similarly, a bot may avoid being added to a blacklist long enough for it to send a site multiple batches of spam. In this case, the site would be in fact using blacklisting, but because we cannot differentiate between a blocked delivery, a failed delivery, and simply a missing batch of spam delivery reports, we cannot include such behavior in our definition of EBL. As before, we only considered in this analysis bots for which we observed both spam instructions and spam delivery reports, which removed approximately 1,000 domains from consideration (these were domains which were *only* included in spam instructions or delivery reports for bots from which we only saw one type of report). Nevertheless, this metric provides a rough estimate that should manifest our original hypothesis if it in fact were to hold.

Figure 9 shows the result of this analysis. Once again, we find only weak negative correlation between EBL rates and per capita income: $r^2 = 0.195$ for linear regression using log/log scales. We note that we obtained a stronger correlation using this exponential model rather than a linear model ($r^2 = 0.113$).

4.5 SMTP Server Version

It is considered best system administration practice to continually update software versions as new security patches are released. As an additional method of testing our hypothesis that the sophistication of IT infrastructure differs by a country's economic standing, we gathered SMTP transfer agent version numbers for all MX servers in our dataset. If SMTP servers administrated in the developing world are running out-of-date software versions, it is likely that those domains also lack sophisticated spam blacklisting infrastructure.

Upon initiating a connection, SMTP servers are required to display their software agent, per RFC 2121. We initiated TCP connections to port 25 for all 1,599,979 unique mail server IP addresses in our dataset. Of these,

-	SM-H	SM-M	SM-L	EX-H	EX-M	EX-L
Rank1	08/06 (24.06%)	08/06 (28.33%)	08/06 (55%)	04/07 (62.94%)	04/07 (76.42%)	04/07 (90.0%)
Rank2	07/04 (15.493%)	12/09 (18.19%)	07/04 (10.84%)	10/08 (30.43%)	10/08 (15.82%)	10/08 (10.0%)
Rank3	05/08 (12.80%)	05/08 (10.25%)	07/04 (10.00%)	05/11 (5.52%)	11/09 (3.40%)	N/A (0.00%)
Total	31543	5459	120	73508	6016	20

Table 1: SMTP version numbers for Sendmail and Exim. H, M, and L stand for “High Income”, “Medium Income”, and “Low Income”, respectively.

we were able to successfully connect to 684,114 (42.7%). We suspect however that our connection attempts were rate-limited at some point, since a second run of the measurements uncovered many more successful connections. The detailed results of the STMP agents we found are shown in the appendix.

We examined variation in version numbers for the top two most popular SMTP servers that displayed version numbers in Table 1, Exim and Sendmail. Our results show that there is very little variance in SMTP software version numbers across economic boundaries.

5 Discussion

The analysis discussed previously indicates that the Spamalytics data, does not indicate a correlation between a countries income levels and the sophistication of spam prevention infrastructure in that country. As we explain in the next subsection, some of our analysis might be colored by changes in the landscape since 2008, when the original data was collected, however nothing we have found would indicate that there is such a correlation. One potential explanation for this, based on observations about versions of SMTP servers, is that most low, and lower-middle income countries have relatively new infrastructure, and because of the model used by the software industry, and open source software, new infrastructure relies on deploying software that is current at that point. For instance, for both Sendmail and Exchange we saw a little more than 10 different versions for Low Income countries, while for High Income countries over 60 versions were reported. In addition the rise of e-mail outsourcing services like Google Apps, and others, which will handle e-mail for an organization for free, makes it less likely that an entity in a low income country would want to maintain their own SMTP servers, rather than shipping the responsibility to companies like Google, which tend to have better infrastructure, and care more about security. For the rest of this section, we reiterate what each of our measurements was attempting to show, show links between them, and after that we discuss some shortcomings of our methodology.

Our methodology for establishing correlation between income levels and sophistication of anti-spam measures relied on measuring the effect of infrastructure at two places. Firstly we wanted to see if there was a correlation between delivery rates, *i.e.*the probability that spam e-mail sent to a user on a server in a particular country will actually be accepted by the receiving MX server. This rate indicates whether DNS blacklisting is used by mail servers, and how frequently these blacklists are updated. Our results seem to indicate that these numbers look similar for high and low-income countries, and are in fact lower for middle income countries. This generally leads us to conclude that there is not a correlation between income and the use of DNS blacklisting.

DNS blacklisting is however relatively easy to deploy and use, and uses little in terms of computational power. Our next metric looked at clickthrough rates for spam. Even after a MX server accepts an e-mail, the e-mail might still be subject to Bayesian filtering, or other anti-spam techniques, and might in fact have been accepted as a way to carry our counter-intelligence, and train such filters. If e-mail is accepted for any of these reasons, or is filtered by any of these filters, it is unlikely to lead someone to visit the website. Since each URL was crafted for a specific e-mail address, it is unlikely that there are other sources of traffic clouding these measurements. Given the assumption that most users are equally likely to visit such links upon receiving spam, we would expect countries with worse infrastructure to have higher click through rates. While our analysis does show a small steady increase in clickthrough rates as income levels fall, these increases are modest, and might reflect the smaller amount of data available for this method. While it is hard to draw any conclusions given the paucity of data, and the small probabilities, it does not appear that a user on a server located in a low income country is significantly more likely to see spam when compared to someone on a server located in a significantly richer country. This seems to indicate that the people who do run their own servers are equally likely to invest in computational infrastructure, filtering products, and other such security infrastructure.

Given these negative results, and the noisy data we had access to, we also attempted to cross-validate our results by trying to directly quantify the prevalence of filtering technology across countries. In particular we measured deployment rates for servers specifically dedicated to anti-spam activity, evidence of blacklist usage, and looked into what agents were used in various countries. The deployment rates for anti-spam measures helps quantify how much investment is made directly towards detecting, and preventing spam, and given that these measures might require dedicated machines, and maintaining software that isn't essential to the functioning of an organization, such deployments are a direct economic measure of investment towards preventing spam. We find no evidence that one is more likely to find these counter-measures in richer countries vs poorer ones, thus reinforcing our findings so far.

The structure of instructions and responses from Storm allows us to try and see if there is evidence that DNS blacklisting is in fact used at a site. This information helps cross-validate our results for delivery rates, since our original explanation for why delivery rates might vary was based on the effect of DNS blacklisting. Our results seemed to indicate a weak negative correlation between income and blacklist usage, and thus reinforce our findings thus far. We also looked at version numbers for MX agents in various countries, to see if poorer countries were significantly more likely to use older, and hence less secure versions. While many agents do not advertise version information, in cases where we did find version information, the versions used in the developing word did not differ significantly from versions in the developed world. Also while these versions were not always the newest, with the most prevalent Sendmail version being over 6 years old, we believe this might reflect established best-practices with regards to versions which are particularly secure, or are better tested. None of our cross-validation seems to have indicated anything different from our original results.

5.1 Shortcomings of methodology

Much of our analysis is based on information gathered by the Spamalytics project over 4 years ago, and on server information gathered by us over the last few months. This difference in time period might significantly affect our results, since the current global distribution of servers might be vastly different today, especially given that services like Google Apps were not popular in early-2008. Furthermore, over this time period many of these sites might have updated their software, and perhaps a study done now would observe significantly different delivery rates, thus leading to vastly different results.

Our data is extremely noisy. In particular a failure to deliver to a particular SMTP server can mean multiple things, including DNS blacklisting, a temporary problem with the server, an invalid username, or other problems. Furthermore, acceptance by a SMTP server might not necessarily mean that e-mail has not been blacklisted, and is not being accepted by specialized devices for training spam filters or for other reasons. While our measures of delivery rates are good approximations for the actual rate, we do not have a good way of correcting for these biases, nor for measuring how likely they are.

Lastly, only a small percentage of our data comes from low income, and lower-middle income countries, both of which are groups of interest for this study. While this distribution is reasonable given economic factors, available infrastructure, and other factors, this might have significant effects on our results.

6 Conclusion

This paper showed that there is no evidence to support the hypothesis that spam is more prevalent on servers in poorer countries when compared with richer ones. We do this by showing a lack of correlation between spam delivery rates and income levels, and between clickthrough rates and income levels. We further validate our results by looking at prevalence of anti-spam measures, use of DNS blacklisting and versions of MX servers used in countries with varying income levels. Our analysis fails to find any support for the hypothesis, and all our metrics seem to indicate that anti-spam measures are spread fairly evenly across countries.

As future work it would be interesting to measure the prevalence of other security measures across countries with different economic situations. In particular mail servers are usually owned by large companies providing infrastructure to a wide variety of people, and are perhaps more likely to be maintained similarly across countries, as opposed to personal computers, or other targets owned by individuals. Another possible direction for future work would be to carry out this analysis with more recent data, so that the measured delivery rates reflect software currently in use.

References

[1] J. Caballero, C. Grier, C. Kreibich, and V. Paxson, "Measuring pay-per-install: the commoditization of malware distribution," in *Proceedings of the 20th USENIX conference on Security*, SEC'11, 2011.

[2] K. Levchenko, A. Pitsillidis, N. Chachra, B. Enright, M. Félegyházi, C. Grier, T. Halvorson, C. Kanich, C. Kreibich, H. Liu, *et al.*, "Click trajectories: End-to-end analysis of the spam value chain," in *Security and Privacy (SP), 2011 IEEE Symposium on*, IEEE, 2011.

[3] C. Kanich, C. Kreibich, K. Levchenko, B. Enright, G. M. Voelker, V. Paxson, and S. Savage, "Spamalytics: an empirical analysis of spam marketing conversion," in *Proceedings of the 15th ACM conference on Computer and communications security*, CCS '08, 2008.

[4] C. Kanich, N. Weaver, D. McCoy, T. Halvorson, C. Kreibich, K. Levchenko, V. Paxson, G. Voelker, and S. Savage, "Show me the money: Characterizing spam-advertised revenue," in *Proceedings of the 20th USENIX Security Symposium, San Francisco, CA*, 2011.

[5] A. Ramachandran, D. Dagon, and N. Feamster, "Can dns-based blacklists keep up with bots?," in *CEAS*, 2006.

[6] C. Dietrich and C. Rossow, "Empirical research on ip blacklisting," in *CEAS*, 2008.

[7] J. Jung and E. Sit, "An empirical study of spam traffic and the use of dns black lists," in *Proceedings of the 4th ACM SIGCOMM conference on Internet measurement*, IMC '04, 2004.

[8] A. Ramachandran, N. Feamster, and D. Dagon, "Revealing botnet membership using DNSBL counter-intelligence," in *Proceedings of the 2nd conference on Steps to Reducing Unwanted Traffic on the Internet - Volume 2*, 2006.

[9] A. Brodsky and D. Brodsky, "A distributed content independent method for spam detection," in *Proceedings of the first conference on First Workshop on Hot Topics in Understanding Botnets*, 2007.

[10] OECD Task Force on Spam, "Spam Issues in Developing Countries," tech. rep., Organization for Economic Co-operation and Development, 2005.

[11] W. Chigona, A. Bheekun, M. Spath, S. Derakhashani, and J. Van Belle, "Perceptions on spam in a south african context," *Internet and Information Technology in Modern Organisations: Challenges & Answers*, vol. 2069, 2005.

[12] "M86 security Labs, Spam source by country." "http://www.m86security.com/labs/spam_statistics.asp", 2011.

[13] S. Kannan, "Social networking sites prone to virus attacks," *The Hindu*, 2009.

[14] J. Burrell, "Problematic empowerment: West african internet scams as strategic misrepresentation," *Information Technologies and International Development*, vol. 4, no. 4.

[15] E. Katz-bassett, J. P. John, A. Krishnamurthy, D. Wetherall, T. Anderson, and Y. Chawathe, "Towards IP geolocation using delay and topology measurements," in *In IMC*, 2006.

[16] N. Spring, R. Mahajan, and T. Anderson, "Quantifying the causes of path inflation," in *IN ACM SIGCOMM*, 2003.

[17] "Maxmind Inc."

[18] "Vicci: A programmable cloud-computing research testbed.," 2011.

[19] "Country Income Groups (World Bank Classification)," 2011.

7 Appendix

We show the popularity of SMTP transfer agents across our dataset in Figure 7. We were able to initiate a TCP connection with 684,114 out of 1,599,979 (42.7%) unique mail server IP addresses in our dataset. The table show that there is a long tail of SMTP transfer agents.

Server Type	Counts	Percentage
Anonymous or Uncategorized	236811	34.603%
Microsoft Exchange	129662	18.947%
PostFix	104432	15.260%
Exim	83547	12.208%
Sendmail	42989	6.282%
MDaemon	12691	1.854%
MailEnable	11677	1.706%
IdeaSmtpServer	9877	1.443%
Barracuda	9570	1.398%
Symantec	4723	0.690%
SonicWALL	4060	0.593%
MailMarshal	3271	0.478%
IMail	3103	0.453%
smtpd	2982	0.436%
Lotus	2591	0.379%
IceWarp	2201	0.322%
Kerio	2037	0.298%
Qmail	1908	0.279%
Sun Java	1703	0.249%
Sophos	1641	0.240%
Omega	1234	0.180%
CommuniGate	1122	0.164%
XMail	1084	0.158%
Merak	816	0.119%
ArGoSoft	791	0.116%
WinWebMail	775	0.113%
Surge	667	0.097%
XWall	650	0.095%
RaidenMAILD	632	0.092%
FireWall	602	0.088%
Winmail	571	0.083%
InterScan	454	0.066%
GroupWise	396	0.058%
SecurityGateway	342	0.050%
NetBox	307	0.045%
Lyris	278	0.041%
EIMS	267	0.039%
Access Enforcer	261	0.038%
Mirapoint	248	0.036%
Sherlock	237	0.035%
Windows SMTP	209	0.031%
Extreme	175	0.026%
Spartacus	160	0.023%
ExpressMail	141	0.021%
Scalix	118	0.017%
SmoothZap	112	0.016%
Ecelerity	85	0.012%

Table 2: Successfully Connected SMTP Transfer Agents.