Analysis of the network externalities and important factors in the variance of Botnet Infection

Santiago Aragón, Owais Ahmed, Pallavii Jagannatha
University of Twente, Nederlands

I. Mitigation of Botnet infection by the involved diferent actors

A. Risk strategies of the involved actors

- *Vendors of Operating Systems and Softwares.* Vendors of Operating Systems should develop and ship free specialist applications along with their products to prevent, detect and mitigate the impact of malware that are used for botnet infections. These applications should be able to detect malicious code and traffic in real-time and update the root server for newly found threats to help the general users to get updated from one newly found threat.
- *End Users.* End users can attend free online awareness campaigns and trainings to have better awareness of the impacts of botnet infections and change their operating and work habits while browsing and downloading online content. Users should be aware to keep their operating systems and application software updated. Their conscious approach for being vulnerable to security threats may help the users to browse the Internet in a safe and secure manner, helping to mitigate the growth of botnet infections.
- *Internet Service Providers (ISPs).* ISPs can detect the systems infected with malicious bots, notify respective users and use various remediation techniques like removing, disabling, or otherwise rendering a bot harmless to address the problem. Since ISPs provide IP connectivity, they can act upon the bots' traffic and can control bots' access to end users. ISPs can follow sets of best practices for the remediation of bots prepared by Internet Engineering Taskforce (IETF) and the Messaging Anti-Abuse Working Group (MAAWG). ISPs can go for security policy changes at the network level, can use walled gardens to quarantine infected users, can filter Inbound and outbound email and can distribute secure ICT infrastructure to users to mitigate botnet infection [1]. Remediating the installations of malicious bots and mitigating the effects would make it more difficult for botnets to operate and would reduce the level of botnet activities on a particular Internet Service Provider's network [2].

B. Cost-benefit analysis

- *Vendors of Operating Systems and Softwares.* The major benefit from bearing the cost of developing tools to provide prevention, detection and real time monitoring of malware and virus infections would be consumer satisfaction and development of a stronger brand with a trust factor of developing secure products. This will help the organization to enhance product sales and compete in the market with a unique selling point of shipping software with better protection from cyber threats both online and offline. There would be less reputational damage due to bad press and potential loss of sales.
- *End Users.* Since users will only have to invest and bear a one time cost to purchase antivirus and security software, hence the benefits of such an investment will be far greater and have a cascading effect until its use. However, there is no cost to changing their responsible use and online behavior that is rather more effective to mitigate the growth of botnet infections. There are many way in which users pay in the form of information theft, financial theft, intellectual property and loss or degradation of services.
- *ISPs.* Botnet activities would result in ISPs' bandwidth being eaten up which would urge ISPs to invest on the expansion of infrastructure, and hence it would be cost effective for ISPs fight this issue. The ISPs choose their measures based on their mix of incentives and cost perception. The two steps involved in above stated mitigation efforts would be better detection and remediating the installations of malicious bots. The data feeds that the ISPs are currently using, does not give them adequate intelligence on the total number of infected machines in their network. There are additional data sets that ISPs can make use of to improve their intelligence, and this is going to be expensive when each ISPs try to have one by itself. It is possible to invest less by building one platform for all ISPs, rather than each ISP building a platform on its own. A centralized, shared clearinghouse might be an efficient way to drastically improve the intelligence that ISPs are using to protect their networks and customers against modest cost [Ex: The Australian Communications and Media Authority (ACMA) has established a clearinghouse that aggregates numerous data feeds and transforms them into weekly reports for each Australian ISP] [3]. The second option, improving the mitigation of infected machines, focuses on ways to enable ISPs to deal better with infected customers. Sharing tools and procedures would be helpful in here. The critical issue will be to reduce the cost of customer contact and support. The more efficient an ISP can deal with a customer, the more infections it can take action

on, within the same amount of resources [3].

C. Analysing the incentives

- *Vendors of Operating Systems and Softwares.* The market for lemons that Akerlof described explains that because buyers can't distinguish the quality of high vs low, they refused to pay a premium price for high quality goods. Vendors of Operating Systems and software may encounter the same market features since the market for secure software is a market for lemons. Vendors may market and try to sell their software as secure but it is hard for an end user to understand and believe this, compared to the alternative cheaper options. Because of that, it will eventually have a lesser return on the vendors' investment to mitigate the security issue, if buyers can't be convinced that it is more secure and safe for their productive use. Buyers look at features that they can measure the quality of, such as user interface and price. So, vendors put more effort on satisfying the customer base through features and benefits that can actually be observed, that leads to a bad outcome because security is not emphasised as it should be.
- *End Users.* Users may change their behaviour if they are given some kind of protection to use the machines, which can cause a moral hazard because they will take security less seriously. User are actually paying for security software to mitigate the risk rather than actually solving the problem.
- *ISPs.* ISP's profits can increase when they clean up botnet malware from the network which would result an increase in users' demand for network(bot-free) access. At the same time, if the clean-up cost per user largely raises the access fee, the demand for network access and ISP's profits can also decrease [3]. Because detecting and cleaning up botnet malware in users' computers are expensive, ISPs may rather choose to disconnect users whose computers are vulnerable to malware infection [4]. Hence, some external funding in an effort to fight botnets would encourage ISPs. In this direction, a government-sponsored program have been helpful to ISPs in the past[example: Australia and Germany]. In the case governments are unwilling to fund these initiatives, ISPs have to find a way to make them, at the very least, cost neutral if not cost positive [3]. Considering the increasing trend of botnet ad-fraud attacks and the consequently increasing loss of ad revenue for Ad networks, Ad Networks have economic incentives to fight botnets. However, Ad Networks are not in the best position to thwart botnets themselves and thus ANs might be willing to subsidize the ISPs to achieve that goal. Such cooperation would motivate and financially help ISPs to deploy detection and remediation mechanisms to help fight botnets [5].

D. Network Externalities

- *Vendors of Operating Systems and Softwares.* Vendors of Operating Systems and software create positive externalities since their role to mitigate the security issue can have a big impact to lower the cost of security investments by ISPs and other actors. In most cases software monopolies limit the available product choice and thus it becomes a moral and social responsibility of organizations to take appropriate measure to ensure security considerations in their software products. Vendors look at what insecure software costs them instead of the total cost of insecure software because, they miss a lot of the costs: all the money we, the software product buyers, are spending on security.

- *End Users.* Botnet infected machines create negative externalities caused by risky online behavior and not deploying preventive controls such as antivirus and security software. These externalities are partly absorbed by ISPs, organizations and other users. A botnet herder who may infect thousands of other users may end up playing a key part of the harm being felt by other users. The harm of those machines is not just restricted to the infected computers, but in-fact often used for other purposes to send spam, to infect other computers and to launch denial of service attacks. Therefore, there is a very less incentive for the botnet-infected user to clean up because they do not actually experience much harm themselves.

- *ISPs.* It is easy to see that ISPs create positive externalities mainly to three different parties: to their subscribers, to the possible victims of a botnet attack and to owner of the AS being targeted by a botnet attack. Investing on this security problem, the ISPs will decrease the size or stop the botnet growth, thus having a negative impact on the botnet future attacks and, therefore, creating benefits to the future victims of a botnet attack and for the owner of AS where the victim is allocated. Furthermore, ISPs tend to have an incentive to voluntarily help its users in cleaning up of botnet infected systems if the cost involved is sufficiently low. Otherwise, imposing liability on ISPs can have the following two effects on consumer surplus. The first effect would remove negative externalities from the network and makes accessing the network more attractive, which results in an increase in on-line users and thus positive externalities. This would cause an increase in consumer surplus. The second effect would raise access fee or purges botnet-infected users, which result in a decrease in on-line users and thus positive externalities. This would cause a decrease in consumer surplus. Also, if the clean-up cost is sufficiently low, cleaning up malware from infected computers without disconnecting any users can be more profitable to ISPs because letting vulnerable users be on-line makes positive externalities larger than disconnecting them. However, If the clean-up cost is sufficiently high, securing the network by disconnecting vulnerable users makes it possible to increase their profits by charging other users a high access fee [4].

II. Explaining the variance in botnet infection between ISP

We recall from our previous work the definition of the metric used to quantify botnet infection (BNI) problem, namely *BNI attempts* which measures the number of attacks executed daily. In figure 1, we show the output of this metric for different Autonomous Systems (AS) ran by ISPs. It is normalized by the address space of each AS, however, in order to explain the variation between ASISP's in this section we identify, analyze and statistically describe the factors behind the variance of the metric defined before.

A. Identifying the underlying factors

To successfully identify the factors behind the BNI attempts variance first we would like to give an intuition of how does this security issue propagates within a network. A botnet is more likely to try more infection attempts if a it is either active, big or both. The likelihood infection of a potential zombie machine is mainly influenced by the following two factors: how close the potential new member is (w.r.t. euclidean or geodesic [6] distance) and how secure is the his system. The former factor type, the distance between a zombie machine and a potential new member of the botnet might be represented by the geographic distance or the logical distance within a network topology, i.e. the type of network in which the zombie machine is connected (Wifi public hot-spot, home network, enterprise network), the Internet penetration in the country or region (High Internet penetration rate may lead to club effect behaviors [7]).

The latter factor type, the security of the potential zombie machine might depends on different software and hardware variables, i.e. operative system (OS) and application vulnerabilities, software updates (issued patches of known vulnerabilities for a particular version), hardware reliability (backdoor presence), user awareness.

Furthermore, there are other factors that are not specific of this security issue and, therefore, the variance of the metric but related to human behavior, i.e. seasonal behavior of infection attempts, or related to country reality, i.e. pirate software penetration or illegal content downloads rate.

B. Statistical analysis of the underlying factors

In figure 2 we show the correlation of different factors such as piracy rate [8], windows OS penetrations, [9], Internet penetration [10]. In table I we show Pearsons correlation coefficient of the aforementioned variables in relation with the botnet infection attempts.

The motivation to use windows market share as a factor is the high penetration of this OS in the world, i.e., more than 70% of the OS are Windows distributions [11].

In figure 4 we show the distribution of OS along different AS, as we might the most common OS in every AS is *Windows 2000*, however, this OS is far to be the most deployed OS [11] at the end 2014 *Windows 2000* only had less than the 0.05%.

We also analyze the relation between the growth in infection per day and the number of unique IPs used. In figure 3 we can see the strong [12] correlation between this two variables and the density of this relation in the diagonal.

We can observe from table I that the Internet penetration is correlated in a negative way to the number of infection attempts and also to the amount of illegal software in the country. In the other hand, the presence of Windows distribu-

Fig. 1: Infection attempts per day in different AS of the ISPs normalized by address space and multiplied by 10^9

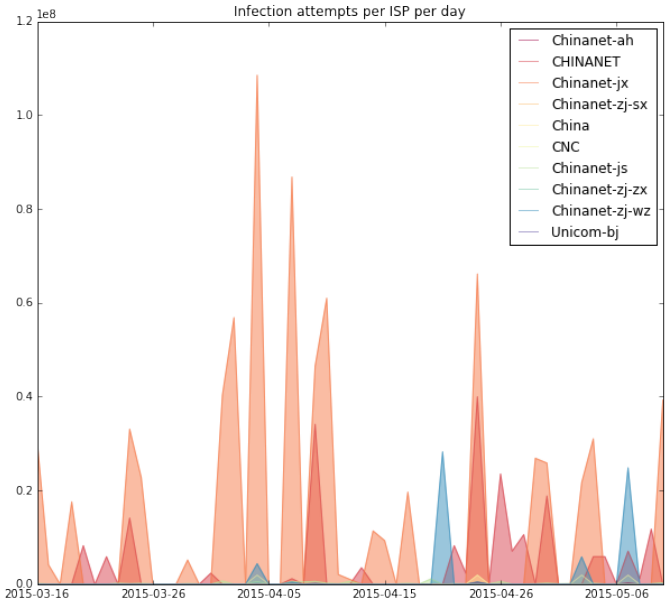


Fig. 2: Different factors against Botnet infection attempts. In the diagonal the density of the factor is showed.

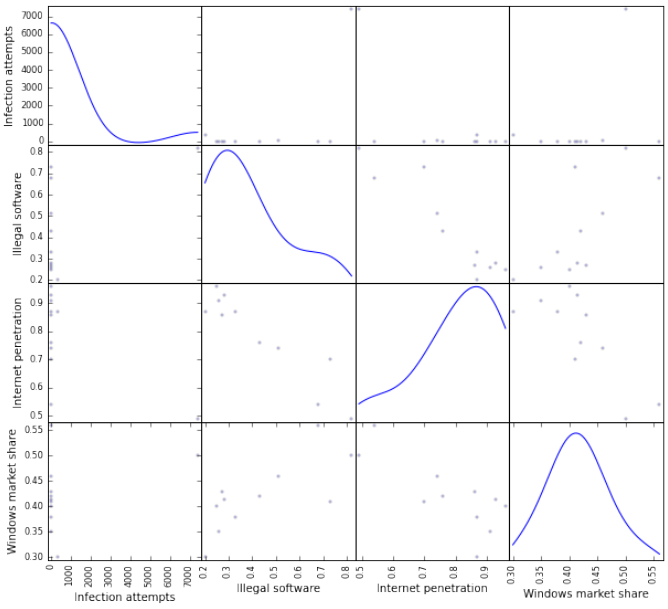


TABLE I: Pearson's correlation

	Infection attempts
Illegal software	0.57
Internet penetration	-0.61
Windows market share	0.35
Unique IPs	0.54

tion shows a moderate positive correlation with the infection attempts even when this coefficient was expected to be higher given OS distribution in the dataset. Illegal software presence per country and unique are valuable factor while explaining the behavior of the aforementioned metric since they present a strong correlation with the infection attempts.

The overall behavior of the Botnet Infection attempts are ruled by a variety of factors, we would like to highlight that the country related statistics, i.e. illegal software rate, Internet penetration and Windows market share, present a natural bias originated in the distribution of the dataset used to perform this analysis, however we have the statistical tools and methodology presented before is not data dependent and can produce significant results by explaining the behavior of different datasets representing the same security issue.

Fig. 3: Infection per day vs Unique IPs

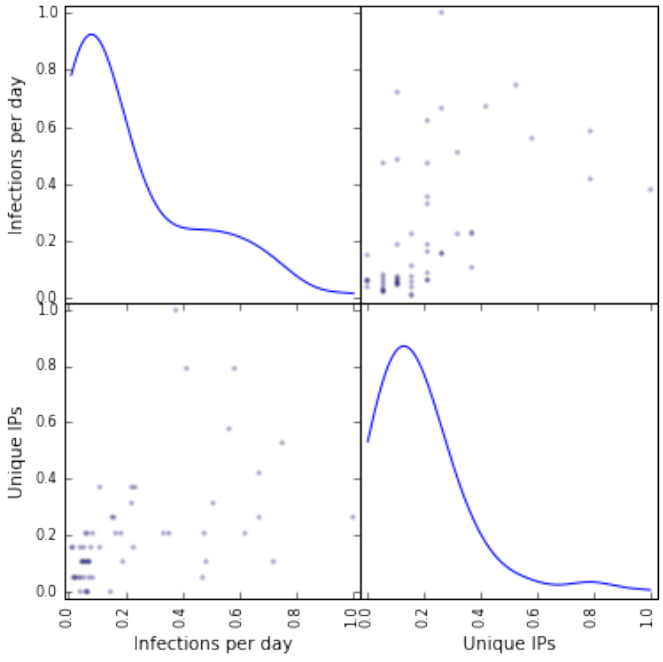
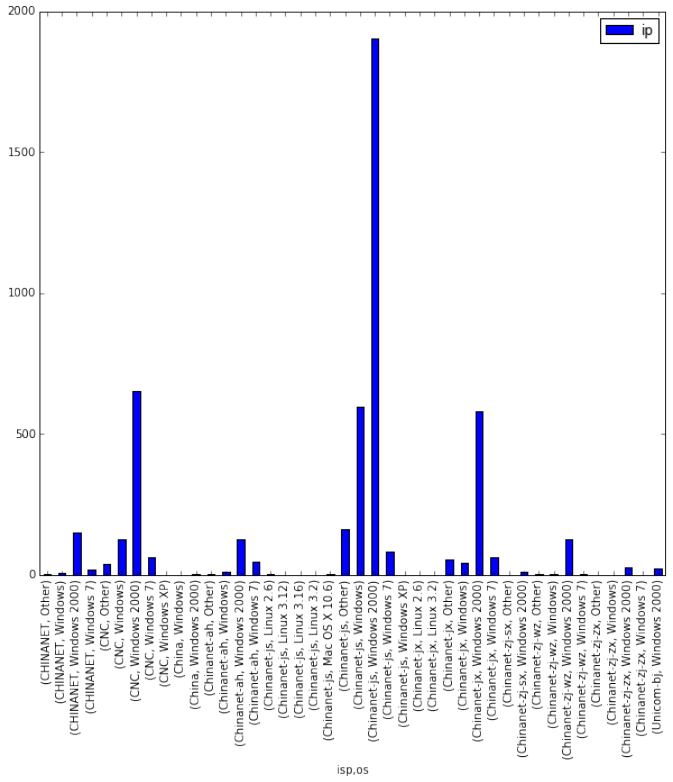


Fig. 4: OS distribution among the more active ISP's ASs



REFERENCES

[1] S. Charney, "Collective defense: Applying the public-health model to the internet," *Security & Privacy, IEEE*, vol. 10, no. 2, pp. 54–59, 2012.

[2] R. Anderson, C. Barton, R. Böhme, R. Clayton, M. J. Van Eeten, M. Levi, T. Moore, and S. Savage, "Measuring the cost of cybercrime," in *The economics of information security and privacy*. Springer, 2013, pp. 265–300.

[3] H. Asghari, "Botnet mitigation and the role of isps," *DelftUniversity of Technology*, 2010.

[4] S. Kinukawa, "Should isps be liable for negative externalities of botnets?" 2012.

[5] N. Vratonjic, M. H. Manshaei, M. Raya, and J.-P. Hubaux, "Isps and ad networks against botnet ad fraud," in *Decision and Game Theory for Security*. Springer, 2010, pp. 149–167.

[6] Wolfram. Geodesic graph. [Online]. Available: http://mathworld.wolfram.com/GraphGeodesic.html

[7] A. Saidi and A. Abdessatar, "Access and communication pricing and club effect," *International Journal of Business and Social Reseach*, vol. 3, pp. 48–64, 2013.

[8] Nationmaster. Piracy level rate. [Online]. Available: http://www.nationmaster.com/country-info/stats/Crime/Software-piracy-rate

[9] T. WorldBank. Traffic analysis report- os breakdown per country. [Online]. Available: https://stats.wikimedia.org/wikimedia/squids/SquidReportCountryBrowser.htm

[10] ——. Internet users(per 100 people). [Online]. Available: http://data.worldbank.org/indicator/IT.NET.USER.P2

[11] Netmarketshare. Desktop operating system market share. [Online]. Available: https://www.netmarketshare.com/operating-system-market-share.aspx?qprid=10&qpcustomd=0

[12] J. Wright. Statistics. [Online]. Available: http://faculty.quinnipiac.edu/libarts/polsci/Statistics.html