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).* They can detect those systems that have been infected with malicious bots, notify the same to Internet users and use various remediation(remove, disable, or otherwise render a bot harmless) techniques. ISPs hold a unique position(DNSBLs, honeypots, darknets, passive DNS, traffic flow based and log analysis techniques) in fighting botnets because of their role as provider of IP connectivity, which gives them the ability to act upon the bot traffic and their access to the end users (to contacting them, or asking them to install certain software, etc).Mitigating the effects of and remediating the installations of malicious bots will make it more difficult for botnets to operate and could reduce the level of botnet activities in general and/or on a particular Internet Service Provider's network [1]. Industry collaborative efforts like the Internet Engineering Taskforce (IETF) and the Messaging Anti-Abuse Working Group (MAAWG) have prepared sets of best practices for the remediation of bots in ISP networks. ISPs can opt for Firewall and security policy changes at the network level, can go for Port 25 management, walled gardens to quarantine infected users, can filter Inbound and outbound email and distribute secure ICT infrastructure to users to mitigate botnet infection [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.* If ISPs do not take any measures, it would translate into bandwidth being eaten up by botnet activities which would urge them for investments in infrastructure expansion, and hence ISPs must consider investing on this issue. As all security comes at a cost, the ISPs choose their measures based on their mix of incentives and cost perception. The two 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, this is going to be expensive when each ISPs try to have one for 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 better deal 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.* When ISPs cleans up botnet malware from the network, users' demand for network access and thus ISP's profits can increase because of the elimination of negative factors. However, ISPs have limited incentives to invest in botnet mitigation. At the same time, if the clean-up cost per user largely raises the access fee, the demand and ISP's profits can also decrease [3]. The revenue of ISPs are not directly affected by the botnets and ISPs would probably welcome some external funding in the efforts to fight botnets. In this direction, a government-sponsored program would be of great help to ISPs[example: Australia and Germany]. In the case governments are unwilling to fund these initiatives, ISPs need 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 help ISPs deploy detection and remediation mechanisms and would of help in fighting botnets [4]. If liability for violations of cyber security is imposed on ISP, it may overreact. Because detecting and cleaning up botnet malware in users' computers are costly, ISP may rather choose to disconnect users whose computers are vulnerable to malware infection [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.* The costs involved in cleaning up of botnet infected systems affect ISP's behavior. If the cost is sufficiently low, ISP can have an incentive to voluntarily help its users without disconnecting those users. If the cost is not low enough for ISP to have an incentive to do this, imposing liability on ISP can have the following two effects on consumer surplus. The first effect is an increase in consumer surplus. Imposing liability on ISP removes 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. The second one is a decrease in consumer surplus. Imposing liability on ISP raises access fee or purges botnet-infected users, which result in a decrease in on-line users and thus positive externalities. If the clean-up cost is sufficiently high, the latter effect dominates the former one, and thus imposing liability on ISP results in decrease of both ISP's profits and consumer surplus. If ISPs can have an incentive to disconnect users vulnerable to botnet malware even without liability if users' preferences for precautions against malware is sufficiently different. In this case, securing the network by disconnecting vulnerable users makes it possible to charge other users the access fee high enough to increase

ISP's profits. However, if the clean-up cost is sufficiently allow, cleaning up malware from infected computers without disconnecting any users can be more profitable to ISP because letting vulnerable users be on-line makes positive externalities larger than disconnecting them [5].

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, 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, 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.

B. Statistical analysis of the underlying factors

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 as we show in figure 3 and in [8] at the end 2014 *Windows 2000* only had less than the 0.05%. On the other hand, we would like to analyze the number of vulnerabilities of different software vendors, in figure 2 we can see the to number of vulnerabilities in the top 50 products of each vendor, again Windows 2000 is not in the most vulnerable systems, however, when we look at the details we can see that 42% of all the vulnerabilities in this OS are of the Code Execution (CE)type and there is at least 16 exploits published.

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

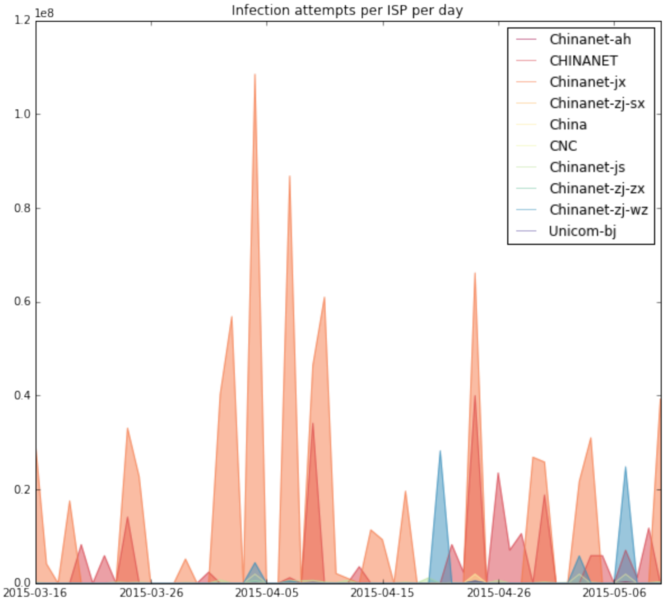
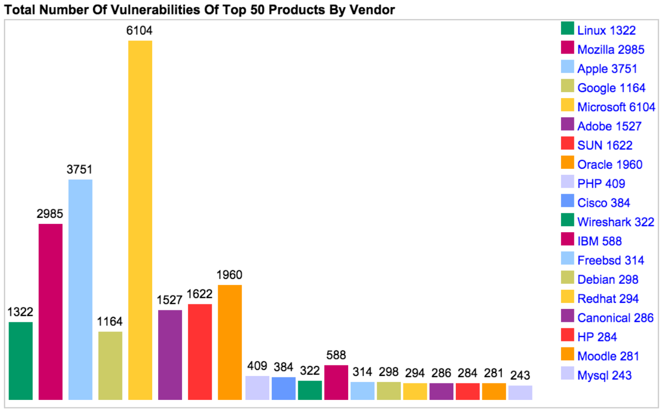


Fig. 2: Number of vulnerabilities per vendor [9]



References

[1] 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.

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

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

[4] 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.

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

Fig. 3: OS market share

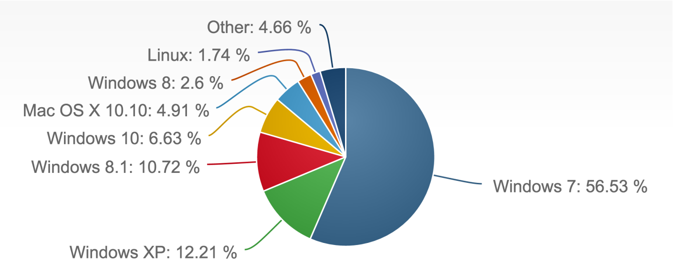
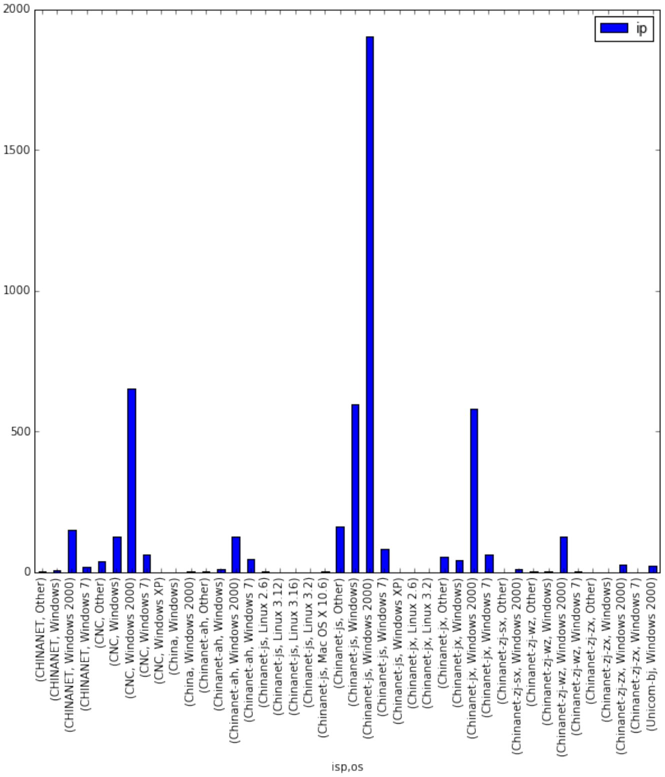


Fig. 4: OS distribution among the more active ISP's ASs



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

[9] CVEDetails. Top 50 products by total number of distinct vulnerabilities. [Online]. Available: https://www.cvedetails.com/top-50-products.php?year=0