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

Botnet infection is a serious threat for a number of entities: end users, businesses, websites, Internet Service Providers (ISPs), Cloud providers and Law Enforcement Agencies. Consequently, thwarting botnets would benefit all these entities. However, the problem of botnet infection in general cannot be solved exclusively by any of these entities alone. In this direction, we propose that each entities should take measures to fight the botnet growth.

B. ISPs

1)Internet Service Providers 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. 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)ISPs are in the best position to detect the presence of a botnet and to take measures against it. ISPS can use technical means that can slow the botnet down. An example for this would be consuming its resources. ISPs can take these measures by performing Denial of Service attacks against Command-and Control Servers of the botnet, trapping and holding connections from infected machines, or blocking of malicious domains.

C. Cloud Providers

To have cloud infrastructure in which configuration constantly evolves to confuse attackers without significantly degrading the quality of service. Proposed solutions may increase the cost for potential attackers by complicating the attack process and limiting the exposure of network vulnerability in order to make the network more resilient against novel and persistent attacks. This can be done by using following technologies: Polymorphism- Develop the novel cloud defence polymorphism techniques to protect cloud infrastructures from attackers[Use botnet polymorphism techniques, i.e., server-side polymorphism and malware polymorphism], Agility- Develop the rapid provisioning technologies of cloud resources to provide high resource availability to cloud customers[Investigate botnet agility behaviours] and Poisoning Prevention- Develop the tamper evident technologies that make unauthorized access to the protected cloud resources easily detected[Probe botnet poisoning mechanisms].

D. End Users

End-users comprise of individuals users and small to medium sized businesses. Home users have to start using antivirus and firewall software as part of personal botnet mitigation measures. Small to medium businesses should fight botnet in association with ISPs by coming up with various 'best practice recommendations' regarding Internet security. It is win-win for both the entities.

E. Cost-benefit analysis

F. Analysing the incentives

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.

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.

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.

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.

Cloud Service Providers:

The customers pay for the cloud services, there is(legal) objections to any attack(botnet) on their data and the price of Cloud services would continue to drop if bot activities on the Cloud affect users. Cloud service providers are legally bound to protect legitimate users of Cloud services from botnet infection. Cloud Service Providers have economic incentives to fight botnets.

End Users:

Home users are well aware of the consequences of botnet infection due to their valuable data, money and productivity at stake, and some of them join arms in fighting botnets. It might also be that unlike ISP, these home users can directly enjoy the incentives of having protected machines. On the other hand, it is about security versus availability, speed, or usability in their business and finally, the monetary benefits of security measures not being very explicit might not motivate all the users to do the same.

Mid and small sized businesses relying on online services suffer as they lack necessary resources to offer safe financial transactions for their customers and their bigger concern would be about their turnover and staying competitive, rather than investing on botnet mitigation.

G. Network Externalities

ISPs:

The costs involved in cleaning up of botnet infected systems affect ISP's behaviour. 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 low, 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.

Cloud Providers:

End Users: Home and SMB users create the most negative externalities which is partly absorbed by ISPs (Internet service providers) and FSPs (financial service providers). The risky online behaviour in combination with not employing security software would result in this externality. This can happen if an user doesn't understand how malware works, and often don't know when they become infected. They do not understand the degree of harm botnet infection can potentially cause and they don't consider paying security software as economical.

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 [1] 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 [2]).

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

B. Statistical analysis of the underlying factors

References

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

[2] 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.

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