Risk analysis of botnet evolution

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

I. Who is the problem owner of the security issue as measured in your first assignment?

Botnet infection and evolution is a security issue that affects many parties in cyberspace, i.e. ISP, LAE, cloud and hosting providers, botnet victims and zombie machine owners. Each party receive a different kind of harm because of this security problem. However, not every party can visualize the real dimension or even be able to fight against the problem, since they may have a limited and narrow scope. We name the ISPs as the problem owner because they have a wider scope of the problem and they get direct consequences against their business model when a botnet evolves and propagate within their network.

II. What relevant differences in security performance does your metric reveal?

In this section we analize the output of the metrics proposed in [**?**]. Based on this output we compare the performance of the distinct Autonomos Systems (AS) owners. We detail how the security performance can me compared using applying the metrics to a subset of the the problem owners i.e. ISPs in China.

A. BN propagation

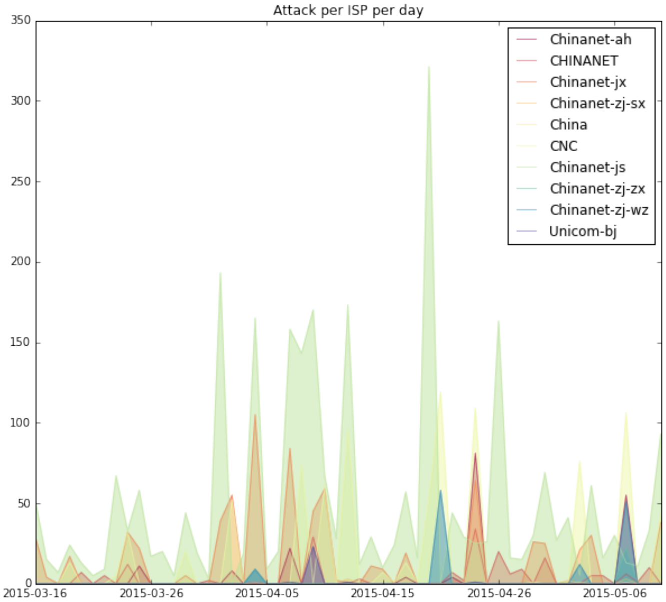
It measures the number new IPs where the BNI attempts are being performed. It is useful to see the aggregate growth of the BN, and to help to infer a BNI rate. This metric can be used to measure the evolution of the botnet in side a network. Since each ISP know the number of clients this metric can be normalized using this value. If an external party would like to compute and compare its perfromance using this metric, the normalization can be performed using the number of IP available addresses.

B. BNI attempts

It measures the number of attacks executed daily. We will use this data to analyze the BN activity. This metric could be useful to measure the effectiveness of mitigating controls. To analyze the security performance of the problem owner, we compare the activity comming from ISP networks and the activity comming from other service providers such as cloud providers and hosting providers. As we can see in figure 2 the majority of the activity is comming form ASs which belongs several ISP, however, as we can see in the before mentioned figure, the service providers also are suffering a misuse of their resourses.

In figure 1 we show the attemts to infect the ellastichoney honeypot that are coming form the top 10 most active AS that belong to ISPs.As we see the more infected ISP is Chinanet but within its network the AS called Chinanet-js, located in the province of Zhejiang. This metric is aimed to be used by the problem owners, since further normalization is needed to get more accurate information, i.e. the market penetration per ISP per region.

Fig. 1: Attacks per day in diferent AS of the ISPs

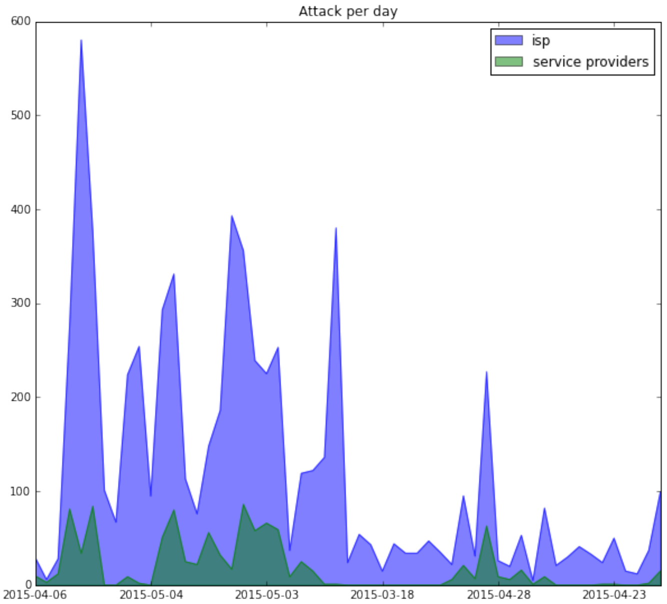


III. What risk strategies can the problem owner follow to reduce the security issue as measured in your first assignment?

As we define in section I the security issue that we analyze in this work is botnet infection and we call the ISPs the owners of this problem. They are interested to avoid their resources, i.e. bandwidth, to be misused, since bandwidth efficiency is a key resource in their business model. Thus, to mitigate the risk of having propagation of botnets inside their network they need to either be able to stop the propagation with in their infrastructure or work with their subscribers to reduce subscribers risk to become a bot.

The former strategy can be described as a risk avoidance strategy since, the problem owner should invest in security solutions to detect, filter and block malicious traffic, i.e., firewall and security policy changes at the network level, "walled garden" system to quarantine or to limit Internet usage

Fig. 2: Activity coming from ISPs and other service providers



for subscribers that continue to show evidence of malicious activity.

The latter strategy could be implemented by a either by risk transfer or by a risk avoidance approach. The risk transfer strategy could be implemented by issuing a charge the subscriber if he is part of a botnet. Since we can assume that the subscriber is not willing to pay extra fees to the ISP, he is indirectly encourage to enhance his equipment's security, i.e. subscriber awareness will grow and updates and patches will be applied when its required. By applying this strategy the ISP is transferring the risk and therefore the cost of taking countermeasures to the subscriber.

The implementation of the latter strategy could also be implemented by taking a risk avoidance approach. If the ISP is willing to absorb all the cost of enhancing the subscriber's security protection and increasing subscriber awareness, i.e., launching a subscriber awareness campaigns and by assuring that the subscribers have the proper security setup and software updates. The software security enhancement could be done by sending a technician to a subscriber location to properly setup their equipment.

IV. What other actors can influence the security issue as measured in your first assignment?

Historically, responses to propagation of botnet-infections within the Internet ecosystem have relied heavily on ISPs, but recently remediation efforts have evolved to include other stake holders / actors to tackle our security issue. These actors have direct involvement with end-user machines to help mitigate the impact of the security issue and have increasingly recognize the long-term impact of malware upon their customers and online services. These actors include:

- *Vendors of Operating Systems / Softwares.* Most of the botnet infections are rooted in exploiting vulnerable code in operating system and application software. Since the software market dominates with more characteristics, ease of use, compatibility and features in an application rather than the importance of security thus causing negative externalities. The cost of security gets high due to vendor costs causing reduction in their rewards, therefore more incentives should be provided for them to make cheaper and secure software to compete with free insecure software.
- *Domain Registrars.* Domain registrars can be effective against blocking compromised domains for hosting phishing sites, command and control servers, poisoned and malware delivery sites.
- *Vendors of Security Services.* End-users rely heavily on antivirus solutions to secure their systems from threats and vulnerabilities that might harm their privacy and security. Botnet infections provide vendors an ever-growing market for them to sell their products. However, the capabilities of antivirus solutions to mitigate the risks of malware are far less than the expected outcome.
- *Cloud & Hosting Service Providers.* There is an increasing growth in botnet infections caused by using cloud service providers and web hosting services due to the technological and infrastructural advantages for attackers to use such tools and techniques. It is of prime importance for such service providers to scan and filter traffic used for spreading malware and vulnerable applications.
- *End-Users.* End-users comprise of home / individuals users and small to medium businesses employees. They create negative externalities caused by risky online behavior and not deploying preventive controls such as antivirus and security software.

V. Identify the risk strategies that the actors can adopt to tackle the problem

Vendors of operating systems should provide tools that provide on-demand and real-time scanning of systems to help remove viruses, spyware, and other malicious software. These valuable applications should be bundled with the operating systems as part of the effort to mitigate the risks from botnet infection attempts. They cannot be a complete replacement to antivirus and antispyware applications used that scan and monitor known viruses and spyware, however they can be a vital resource to provide ongoing protection from a trusted source. An effective and up-to-date software firewall at the OS level can be an effective protection barrier between the users system and the Internet. OS Vendors should provide a sandbox environment to run unverified programs that may contain malicious code downloaded from unverified solution providers, untrusted users and untrusted websites. Software providers that provide email, social networking and instant messaging facilities should enforce strong filtering of content and attachments to mitigate the risk of botnet infections delivering malware that are presumed to be pictures or movies by the end users. Users should be limited to restricted access to applications and OS features, unless all security settings are hardened and the systems are patched with the most current updates.

To establish every network connection to a particular host, computers have to preform DNS lookup. Domain registrars can use methods such as packet filtering to filter traffic towards banned IPs by blocking access to certain servers from a list of banned or suspected bad domains. Attackers abuse the DNS system to avoid detection by using devious tricks such as fast-flux. In the fast-flux technique, bots continuously register and deregister their IP addresses for a particular domain. Each request by a user to access a malicious site will result in accessing a different bot and possibly different ISP. The only option to combat fast-flux is for the registrar to suspend the bad domain, which has its own positive and negative incentives in doing so. Another proactive approach that registrars can adopt is automated abuse handling and actively responding to external domain suspension requests from financial service providers and other authentic sources of information like intelligence agencies and ISPs.

Most major vendors like Microsoft are providing free tools to remediate the effects of botnet infections, and help users to combat against cyber criminals for their online privacy and security. However, there is a need for more user awareness for better protection and prevention from botnet infections. Once notified by ISPs about infected machines, user must take remedial actions to remove malicious software from their systems. Even when the related malware have been removed, users must take actions and steps to fully recover the systems to a stable state. Remediation is a critical step to curb the impact of bots, though it is recognized that without tools and processes to harden the devices and prevent reinfection, bot infections will repeatedly reoccur.

With ever growing incentives and motives behind spreading infections to run large networks of distributed botnets, the techniques and technologies are changing rapidly with time. Vendors of security services such as antivirus solution providers should put more effort on research and develop solutions to detect, prevent and mitigate the impact of botnet infections. Although the existing practices, tools and techniques to mitigate botnet infections are being tackled to a greater extent compared to the past, however attackers are coming up with clever new ways of exploiting vulnerabilities to spread their networks via botnet infections. Many infections are quite hard to remove, as they may disable windows update, as well as block access to the websites and update servers of antivirus and security software vendors.

VI. Pick one of the risk strategies identified previously and calculate the Return on Security Investment (ROSI) for that particular strategy

In this section we detail one of the risk strategies proposed in III, an hypothetical Chinese ISP X who owns 15% of China's Internet users [1], namely X has 97 million users. Lately their security team has realized that the botnet infection rates are growing within their network, and since they can not transfer the risk to the subscribers because the Chinese is a very competitive market, they decide to absorb the cost of enhancing the subscriber's security protection and increase subscriber awareness.

The fist step is to calculate the cost of a security awareness campaign cost on average around \$0.80 per user per year [2], thus the amount invested is \$77.6 millions per year. In second place, X would like to provide technical support to setup in a proper way the security configurations and to validate that their systems are up-to-date for each subscriber. According to [3] the average cost per hour of a technician is \$15. If the average time a technician spends in at a subscribers location is 1 hour twice a year, X needs to invest 3 billion for the second mechanism.

To estimate the benefits of following this strategy we use the return on security investment (ROSI). The ROSI is defined as follows:

$$ROSI = \frac{ALE - mALE - CoS}{CoS}$$

where ALE is the Annual loss expectancy defined as

$$ALE = ARO * SLE$$

$mALE$ is the modified ALE after applying the risk strategy and ARO is the Annual Rate of Occurrence and measures the probability that a risk occurs in the year, and SLE is the Single Loss Expectancy that represents the amount of money that a risk occurs [4].

The SLE is calculated as follows, the average bandwidth used by botnets is 14,181,240 GB for DDOS and spam [5], [6], attacks per year, the cost per GB for a ISP is \$0.034 [7], thus the average cost for botnet bandwidth misuse is the $SLE =$\$482,158

We define two scenarios, the first one X only applies the user awareness campaign, in the second one, the ISP applies technical support approach. The $CoS_1 = \$97,000,000$ and the $CoS_2 = \$3,000,000,000$

Even when the impact of a user awareness campaign is hard to measure, in [8] mention that might help to reduce at least 10% of the incidents, thus we assume that $ARO_1 - mARO_1 = 90\%$. For the second scenario we can assume a higher impact since the risk reduction is in hands of the technicians and not in the subscribers hand, i.e. $ARO_1 - mARO_1 = 30\%$.

Therefore the ROSI calculation is the following:

$$ROSI_1 = \frac{(0.9) * 482,158 - 77,600,000}{77,600,000} = -99\%$$

$$ROSI_2 = \frac{(0.9) * 482,158 - 3,000,000,000}{3,000,000,000} = -99\%$$

As we can see both strategies are not convenient to the ISP X since the cost of applying any of them is higher than the economic harm that the botnet could perform. However, in this calculation the economic harm performed to the botnet attacks, i.e. DDOS or spam victims, are not taken into account and this economic impact is normally higher than the cost of applying such policies. In this case to be able to transfer the risk from the victims to the ISPs the regulator entity should enforce policies that persuade the ISP to implement stronger security countermeasures against botnet infection.

REFERENCES

[1] Reuters. China's internet population hits 649 million. [Online]. Available: http://www.reuters.com/article/2015/02/03/us-china-internet-idUSKBN0L713L20150203

[2] ACMA. An overview of international cyber-security awareness raising and educational initiatives (2011). [Online]. Available: http://www.galexia.com/public/research/assets/gc381_acma_cybersecurity_publication_version_20110517_galexia_web/print-index.html

[3] Payscale. Computer technician salary. [Online]. Available: http://www.payscale.com/research/US/Job=Computer_Technician/Hourly_Rate

[4] ENISA, "Introduction to return on security investment," 2012.

[5] ACZoom. Spam taking up most of the internet bandwidth? [Online]. Available: http://www.aczoom.com/blog/2013-01-07/spam-taking-up-most-of-the-internet-bandwidth

[6] ARBOR. Arbor networks' atlas data shows the average ddos attack size increasing. [Online]. Available: http://www.arbornetworks.com/news-and-events/press-releases/recent-press-releases/5451-arbor-networks-atlas-data-shows-the-average-ddos-attack-size-increasing

[7] M. Brain. What does a gigabyte of internet service really cost? a look at the worst case scenario. [Online]. Available: http://blogs.howstuffworks.com/brainstuff/what-does-a-gigabyte-of-internet-service-really-cost-a-look-at-the-worst-case-scenario.htm

[8] I. Winkler. Security awareness can be the most cost-effective security measure. [Online]. Available: http://www.csoonline.com/article/2131999/metrics-budgets/security-awareness-can-be-the-most-cost-effective-security-measure.html?page=2