Metric design for botnet mitigation

Santiago Aragón*, Daniel Meinsma*, Pallavii Jagannatha* Owais Ahmed*,
* University of Twente, Nederlands

***Abstract*—**

***Keywords*—**

I. What security issue does the data speak to?

It is impractical and very expensive to defend against every possible vulnerability [1]. Therefore, decision-makers must design and implement effective security strategies about where and when to invest time and money [2]. To make decisions on security investments, models are used and these models are build on security metrics [3]. Since the definition of these metrics are the basis of a good security model and therefore, they are a key element to produce valuable information for the decision-makers. For example, not all vulnerabilities will be attacked, thus knowing the most likely attack vectors is key in planning effective security measurements [1].

One way of gathering attacker information is by using *honeypots*. Honeypots are isolated and monitored systems that emulate to be vulnerable in order to attract attackers and track their behavior [4], i.e., attack attempt data could be used to define metrics that capture different aspects of attacker behavior. In particular we take a closer look to *Elastichoney* [3] project. It emulate to be a elasticsearch server suffering of a remote code execution (RCE) vulnerability identified as CVE- 2015-1427. This vulnerability allow attackers to execute Java based code by querying the server [5]. Furthermore, the Elastichoney project have gathered data over two months and tracked about 8k attempts to attack from over 300 unique IP addresses [3].

In Elastichoney logs the major security issue that can be found is *Botnet Infection* attempts, i.e. when a botnet machine is trying propagate the botnet by infecting another machine.

In this work we take a look to two different parties who have great incentive to know about the attacking behavior of botnet infection, namely *Internet Service Providers (ISP's)* and *Enforcement agencies*.

Botnet infection is a major security issue for ISP's, because 27% of the overall unwanted traffic on the Internet can be attributed to botnet-related spreading activity [6]. And this is a great loss in productivity for ISP's. On the other hand, law enforcement agencies (LAE) would counter this security issue, because botnets are heavily used as a platform for various criminal business models like sending spam, committing click fraud, harvesting account credentials, launching denial-of-service attacks, installing scareware and phishing [7].

In the rest of this paper we discuss ideal and state-of-the-art metrics that measure different aspects of botnet infection and how these metrics can be used by ISP's and enforcement agencies to make effective security investments. Finally, we propose, implement compare and evaluate our own metrics.

II. What would be the ideal metrics for security decision makers?

The security issue defined in section I have distinct effects depending on the issued party. For each party, we identify how the botnet infection (BNI) is negatively influencing their interests, as well as a set of ideal metrics which could help each party to derive better decisions to take the more effective counter measures to mitigate their problem while maximizing the return on security investment.

a) ISP: For this party it is of main interest to avoid misuse of resources i.e. the ISP would like to block not legitim incoming traffic to its network while the botnet's victim would like to maintain availability of its resources.

- *Botnet growth.* The growth and propagation trend are an ideal tool to quantify and predict the cost of malicious activity within the ISP network.
- *Resources (un)availability cost.* The ISP would like to know how much traffic of botnet infection activity is passing through his network. If is able to distinguish botnet activity from user activity he could measure how much resources are being misused and estimate the cost of having botnet inside his network and therefore justify the investment on security countermeasures.
- *Network infection rate.* The ISP could quantify his subnet infection rate prevention and reaction policies would be better targeted, i.e., if the subnet x.x.x.0 is heavy infected the ISP could target only this portion his network.

b) LAE: This party is interested in prevent, prosecute and punish the entity behind a security issue, i.e., to prevent BNI is of main interest to transfer the risk from the BN victims to the ISP and/or to encourage the zombies machines to increase their security protection, while for prosecution and punishment it is important to have mechanisms to understand and hunt down the BN.

- *BN geographical and digital location.* With geographical and digital location metrics the interested party could measure the infected population in a particular region either in the physical or digital world, i.e. how many infected machines are in the south of Chine, or how many infected machine does a ISP have.
- *BNI target machines.* By characterizing which kind of machines are the weakest link in a network, the LAE could launch prevention campaigns describing which kind of machines are more probable to become part of a botnet, i.e., operative system version, browser, etc.

III. What are the metrics that exist in practice?

In the previous section we have seen which kind of metrics would be ideal for different parties facing the botnet issue. Before going to the metrics proposed for each party by this paper, first a list is presented of metrics that are already used by honeypots for botnet detection:

c) Network Telescope: This is a control metric.

A block of Ip addresses from the entire range of IPv4 addresses are unassigned to hosts. This network is called "darknet". These block of ip addresses are still advertised on the internet through Border gateway(BGP) protocol making it BGP reachable. If any host from anywhere in the world(on the internet) sends a packet to one of these addresses, this packet would travel all over the world, would reach the router that advretises this routes, would be silently dropped (without any repsonses) but this would be logged. Network telescopes would be used to observe this internet traffic. By definition, this traffic is unsolicited since it does not have any hosts assigned to the addreses.Most of this unsolicted traffic would be malicious i.e traffic from malware, traffic from infected hosts that randomnly scan entire internet address space and so on [8].

Enforcement agencies use this to create metric out of samples of telescope data containing security event signatures. This metric would inform about possible network attacks, botnet activities and other misconfigurations.

d) Network Fingerprinting: This is a control metric.

With this method, one can create a metric that states which hosts communicates to which hosts. For example, one can track all the IP addresses , the honeypot communicates to. The honeypots will only communicate to the controller and in a peer to peer botnet , the honeypots will create multiple other members of the botnet [9].

Enforcement agencies use this to create metric which contains information of traffic logs that are automatically processed to extract a network fingerprint, the targets of any DNS requests, the destination IPaddresses, the contacted ports (and protocols), and whether or not default scanning behavior was detected. This would be used to differentiate between different types of botnets for example if the honeypot is part of a traditional command and control botnet [6].

e) IRC related features: This is a control metric.

With this method, one can create metric that differentiates between a member of a IRC type botnet and a non-infected member because these type of botnets send and receive signature commands over IRC channels [6].

Enforcement agencies use this to create metric which contains information of initial password to establish an IRC session with the server, the format of the nickname and username chosen by the bot, the particular modesset, and which IRC channels are automatically joined (with associated channel passwords).This is used to identify infected members(botnet) in the network [6].

Network fingerprinting and IRC related features provide enough information to join a botnet in the wild [6].

f) Longitudinal tracking: This is an incident metric.

With this method, one can create metric where you can visualise the number of attacks originating from a particular geographical location [6].

Enforcement agencies use this to create metrics containing information about geographical location to track the location of origination of a specific botnet.

g) DNS tracking: This is an incident metric. This method is almost the same as Longitudinal tracking, but instead of tracking the geographical location, this method tracks the domain names [6].

Enforcement agencies use this to create metrics containing information about domain names. This is used to probe the caches of a large number of DNS servers in order to infer the footprint of a particular botnet (total number of DNS servers giving cache hits) [6].

h) Botnet resources tracking: This is an incident metric.

In figure 1,you can see different resource aspects of botnet and each of these resources can be used to create metrics which differentiates between different types of botnets [9].

Enforcement agencies uses this to create metrics for each resource to characterize different botnets. It contains information about distinguishing characteristics. For example, peer-to-peer botnets would have network characteristics like distinctive communication graph, higher command latency and so on [9].

i) Signature tracking: This is a prevented losses/impact metrics.

Enforcement agencies uses this to create a metric that tracks the infection rate of a specific botnet by using the signature of a specific botnet, for example a trojan horse and its backdoor port as signature [10].

IV. A definition of the metrics you can design from the dataset

We define a number of metrics that can be used to characterize the data set of RCE vulnerability. For each metric, we can define qualitative levels and quantitative levels for which a numerical value is associated with each level. These metrics represent the intrinsic characteristics of the vulnerability. They can be used to measure the exploitability factor and impact to the infected systems. The following metric definitions will help us critically analyze the nature and characteristics of attacker behavior, the means of predicting the level of attack, the severity of the incident and resources needed to mitigate the impact of this vulnerability.

j) Access Vector:: It measures how the vulnerability is exploited, for instance, locally or remotely. The more remote an attacker can be geographically, the greater the chances of vulnerability being exploited throughout the network attack. The input for this metric will include the number of attacks coming from various counties and also pinpointing the regional locations according to cities. This metric will help measure the scale of attacks coming from a particular geographical location. Furthermore, we can assess to block the IP ranges as per the geographical source of the attack coming from to mitigate the risk of potential impacts to critical infrastructure.

k) Scale of Attack:: It will measure the growth in number of attacks executed daily. We will use this data to analyze the daily trends in the level and strength of attack exploiting the vulnerability. This will be beneficial to measure the effectiveness of mitigating controls for business continuity of core

systems and applications and the protection of confidentiality, integrity and availability of data.

l) Significant Attack Method:: We will use this metric to assess the nature of attack by measuring the number of GET and POST request types / methods. A GET request is used to retrieve standard, static content like images and data from a web server while POST requests are used to access dynamically generated resources that will involve server side application processing. This will help us understand the aim of attacker whether to inundate the server or application with multiple requests that are each as processing-intensive as possible. Because the attack is most effective when it forces the server or application to allocate the maximum resources possible in response to each single request.

m)Number of Attacks/Recon:: We use this metric to classify the number of server contacts as either an "attack" (attempt at actually doing something bad) vs "recon" (which we assume is just a test to see if the instances are vulnerable). This is vital to assess the severity of attack and look into number of false positive / negative.

n) Top Attackers:: We can view the top source IPs that were most prominent during the attack, simply by analyzing the number of attacks against each unique IP. This could be useful for reputation analysis of zombies involved in the attack and identification of IPs to block as a preventive action.

o) Probability of Attack:: We compare the number of attacks coming from particular operating systems, web browsers and the content type used to exploit the vulnerability. The combination of these features help to calculate the probability of attack by using historic data analysis on the basis of most significant attacks using such tools and applications.

V. An evaluation of the the metrics you have defined. This should include graphical representations of the metrics (e.g., histograms, scatter plots, time series, bar charts).

References

[1] M. Rosenquist, "Prioritizing info security risks with threat agent risk assessment." Intel Information Technology, 2009.

[2] W. A. J. S. B. Sonnenreich, "Return on security investment (rosi) – a practical quantitative model." Journal of Research and Practice in Information Technology, 2006.

[3] R. Böhme, "Security metrics and security investment models," in *Advances in Information and Computer Security*. Springer Berlin Heidelberg, 2010, pp. 10–24.

[4] P. Wang and et al., "Honeypot detection in advanced botnet attacks," in *nternational Journal of Information and Computer Security 4.1*. USENIX, 2010, pp. 30–51.

[5] Common vulnerabilities and exposures:cve-2015-1427. [Online]. Available: https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-1427

[6] M. Abu-Rajab and et al., "A multifaceted approach to understanding the botnet phenomenon," in *Proceedings of the 6th ACM SIGCOMM conference on Internet measurement*. ACM, 2006.

[7] R. Anderson and et al., "Measuring the cost of cybercrime," in *The economics of information security and privacy*. Springer Berlin Heidelberg, 2013, pp. 265–300.

[8] van Rijswijk-Deij. and et al., "Dnssec and its potential for ddos attacks: A comprehensive measurement study," in *Proceedings of the 2014 Conference on Internet Measurement Conference*. ACM, 2014.

[9] Grizzard, J. B., and et al., "Peer-to-peer botnets: Overview and case study," in *Proceedings of the first conference on First Workshop on Hot Topics in Understanding Botnets*, 2007.

[10] M. Andreolini and et al., "Honeyspam: Honeypots fighting spam at the source," in *Proceedings of the Steps to Reducing Unwanted Traffic on the Internet on Steps to Reducing Unwanted Traffic on the Internet Workshop. USENIX Association*. USENIX, 2005.