1 What security issue does the data speak to?

Companies and people have more and more problems defending against cyber incidents. It is not possible to defend against all possible cyber attacks, so people have to make strategic decisions on where to invest in their security. Making strategic decisions about security requires us to have a clear understanding of these security issues and for this there is a great need for security metrics. [1]

To be able to make metrics, we need reliable data . One way getting reliable data about cyber threats is capturing cyber attacks with a honeypot. Honeypots are systems made vulnerable intentionally to attract attackers to get inside the system to track their activities.[7]

This paper proposes meaningful metrics based on the logs from the honey pot called "Elastichoney". Elastichoney is a low-level honeypot which contains RCE Remote code execution vulnerability -CVE- 2015-1427, which allowed attackers to execute java based code in the search bar of the honeypot. The log files of this honeypot contains data collected over two months and tracked about 8k attempts to attack from over 300 unique IP addresses. [2]

One of the major security issues that the digital world is currently facing is "BOTNETS". In the paper "Measuring the cost of cybercrime" you can read that:

> "Botnets provide a versatile platform for a variety of criminal business models, including sending spam, committing click fraud, harvesting account credentials, launching denial-of-service attacks, installing scareware and phishing". [3]

The authors of this paper think that the logs of Elastichoney tracks the activities of one or more botnets, because the following attack patterns can be found in the logs:

The same operation steps are performed on multiple different files: 1. Downloading the file using the command wget, 2. Making the file location accessible by using the command chmod 777, 3. Executing the file, 4. Removing the file using the command rm. Operations on files were requested by multiple different sources.

These attack patterns hints at distributed automated attacks, which is a clear indicator of botnet activity.

1) Böhme, Rainer. "Security metrics and security investment models." Advances in Information and Computer Security. Springer Berlin Heidelberg, 2010. 10-24.

2) http://jordan-wright.com/blog/2015/05/11/60-days-of-watching-hackers-attack-elasticsearch/

3) Anderson, Ross, et al. "Measuring the cost of cybercrime." The economics of information security and privacy. Springer Berlin Heidelberg, 2013. 265-300.

4) Grizzard, Julian B., et al. "Peer-to-peer botnets: Overview and case study."Proceedings of the first conference on First Workshop on Hot Topics in Understanding Botnets. 2007.

5) Abu Rajab, Moheeb, et al. "A multifaceted approach to understanding the botnet phenomenon." Proceedings of the 6th ACM SIGCOMM conference on Internet measurement. ACM, 2006.

6) Andreolini, Mauro, et al. "Honeyspam: Honeypots fighting spam at the source."Proceedings of the Steps to Reducing Unwanted Traffic on the Internet

on Steps to Reducing Unwanted Traffic on the Internet Workshop. USENIX Association, 2005.

7) Wang, Ping, et al. "Honeypot detection in advanced botnet attacks."International Journal of Information and Computer Security 4.1 (2010): 30-51.