# Elastichoney

Daniel, Owais, Pallavi and San Diego

September 19, 2015

## 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]

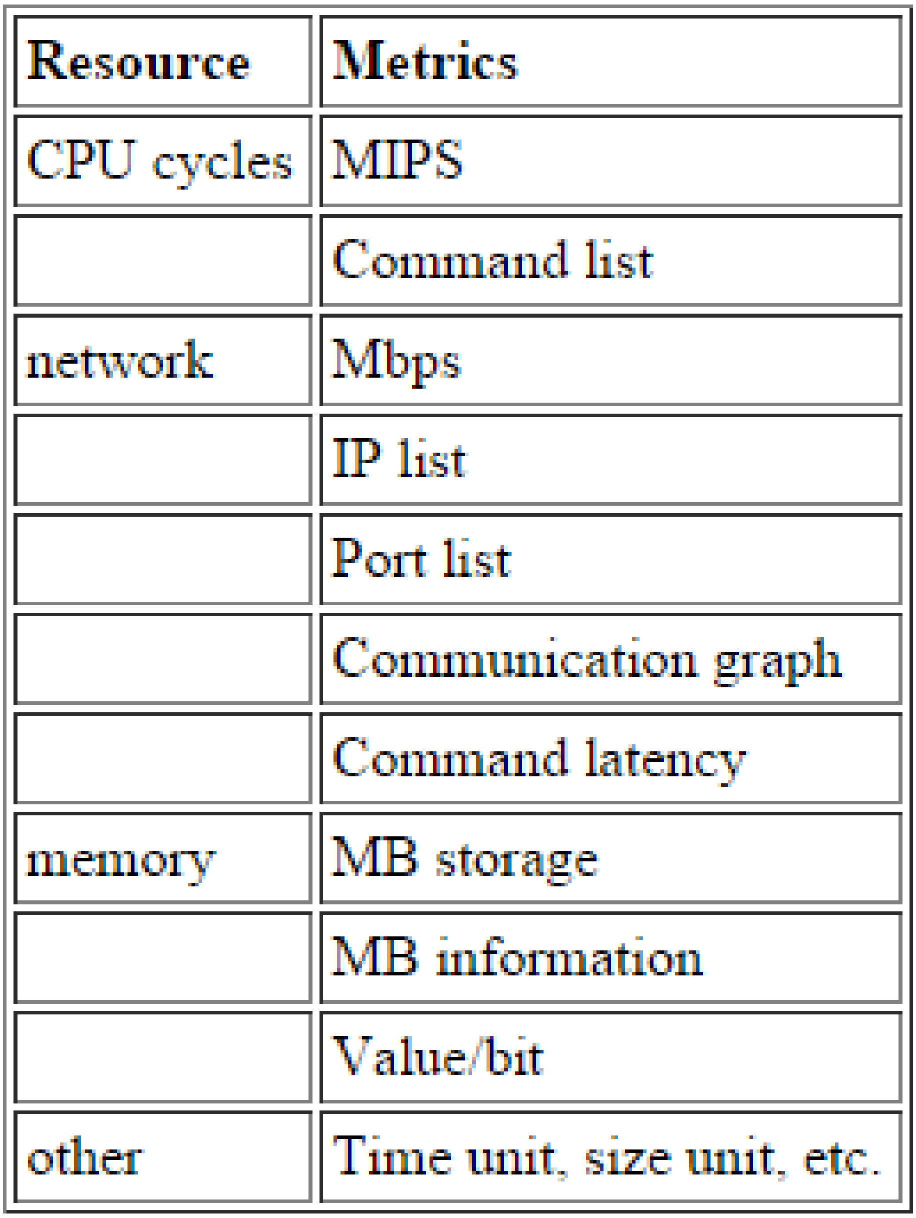
One of the major security issues that the digital world is currently facing is "BOTNETS". In the paper "Measuring the cost of cybercrime" you can read that:

> "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:

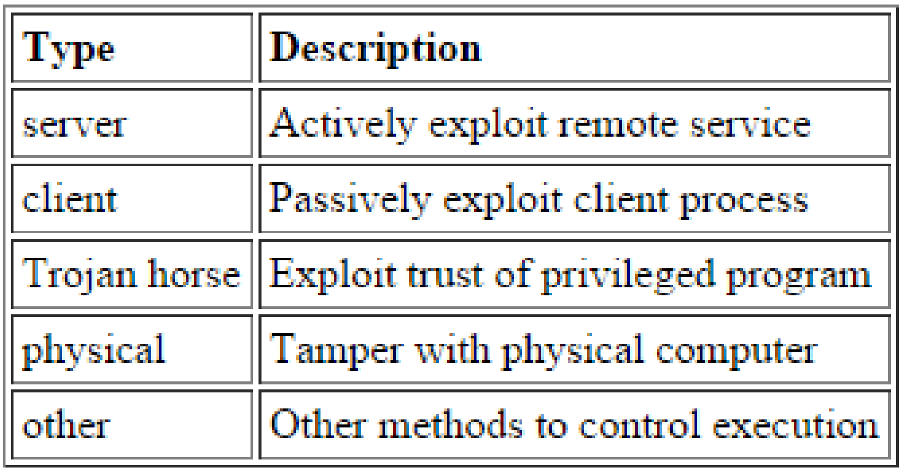
The same operation steps are performed on multiple different files: 1. Downloading the file using the command wget, 2. Making the file location accessible by using the command chmod 777, 3. Executing the file, 4. Removing the file using the command rm. Operations on files were requested by multiple different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

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



| **Resource** | **Metrics** |
|---|---|
| CPU cycles | MIPS |
|  | Command list |
| network | Mbps |
|  | IP list |
|  | Port list |
|  | Communication graph |
|  | Command latency |
| memory | MB storage |
|  | MB information |
|  | Value/bit |
| other | Time unit, size unit, etc. |

Figure 1: Botnet Resource requirements and Metrics



| Type | Description |
|---|---|
| server | Actively exploit remote service |
| client | Passively exploit client process |
| Trojan horse | Exploit trust of privileged program |
| physical | Tamper with physical computer |
| other | Other methods to control execution |

Figure 2: Infection Vectors

## 2 What are the metrics that exist in practice?

The following is a list of metrics used by honeypots to detect botnet activity:

-Network Fingerprinting: With this methods, you can create a metric that states which hosts communicates to which hosts. For example, you can track all the IP addresses , the honeypot communicates to . This is interesting because using this method , you can differentiate between different types of botnets for example if the honeypot is part of a traditional command and control botnet. 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.[4]

-IRC related features: With this method, you can create metric that differentiates between a member of a member of a IR C type botnet and a non-infected member because these type of botnets send and receive signature commands over IRC channels.[5]

-Longitudinal tracking: With this method, you can create metric where you can visualise the number of attacks originating from a particular geographical location.[5]

-DNS tracking: This method is almost the same as Longitudinal tracking, but instead of tracking the geographical location, this method tracks the domain names.[5]

-Port Scan tracking from IDS logs: With IDS logs, you can view how many times a host tries to communicate with the honeypot and deduce if a port scan is active and create a metric that state show many port scans each communicating host performs.[7]

-Botnet resources tracking: 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[4]

-Botnet infection vectors: This method is almost the same as the botnet resources metrics but in this metrics, you differentiate between infection vectors of different types of vectors. See figure 2 and an extra example might be phishing.[4]

Signature tracking: In a few methods seen above, we have seen metrics that could differentiate between different types of botnets and if we use a signature of a specific botnet, for example the backdoor port of a trojan horse that it uses , we can create a metric that tracks the infection rate of that specific botnet.[6]

-DNS sinkhole: If a honeypot gets infected by a traditional command and control botnet and uses a DNS server to communicate with this honeypot ,one can try to change the DNS location of the botnet controller to DNS location of the honeypot. This results in all the other members of the botnet in the same DNS server communicating to the honeypot instead of the botnet controller which results in a precise mapping of all the members of the botnet in the DNS server.[7]

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.