Security Metrics in the field of Malware Domains

Draft

Niels Gijsen, Noah Goldsmid, Samiksha and Jeroen Weener

September 2018

1 Assignment description

Security metrics can gear up the system to fight against the malwares, while weak security metrics can damage the system severely! They are the defensive pillars of any electronic machinery that is prone to malware attacks. The strength of security measures against any malwares defines whether the right amount of money has been spent on it or not, whether the time devoted to install those measures is worth or not or be it any extra effort added for it. Any program without security measures is vulnerable to attacks (intense damage to property/person!), thus security measures give the programs a right direction, by right direction we mean protection against virus, malwares, etc. Distinct metrics need to be applied on different modules of a program and for that prioritizing each metric is essential- therefore "Security is a process". During Block 2, we learned the importance of measuring cybersecurity and the challenges to create meaningful metric. However, metrics are necessary to show how security activity contributes directly to security goals; measure how changes in a process contribute to security goals; detect significant anomalies in processes and inform decisions to fix or improve processes.

1.1 Data set

The data set is available at `http://www.malwaredomainlist.com/mdlcsv.php` and contains 2289 entries. It does not list the column names. These are (in order):

1. Date (UTC)
2. Domain
3. IP
4. Reverse Lookup
5. Description
6. -

7. ASN (autonomous system number)
8. -
9. Country Code

2 Introduction

In this report the reader will be presented with security metrics in the field of malware domains. First, we take a look at the context of malware domains. Then, a look will be taken at the different security metrics. We start by showing what metrics would be ideal and explain why they are not usable in practice. We will then give an overview of metrics that actually are used in practice. Lastly, we provide the reader with a few proposed metrics. The usability and effectiveness of these metrics will be discussed in the Conclusion.

3 Context

This report looks into a dataset of 'malware domains' from malwaredomainlist. The dataset consists of domain names that are known to be used in cyber crime. Most of the domains in the list are involved in phishing, botnets or other malicious activities. Accurate measurements on these datasets can help improve automated detection of malicious domains. This is very useful for end-user protection.

4 Metrics

4.1 Ideal Metrics

Each metric has its own biases, therefore an ideal metric would be a aggregation of multiple robust metric and prevention strategies. A comprehensive security plan is the most powerful way to gauge security.

4.2 Metrics used in Practice

Most literature available on malicious domains is on detection of malicious domains. Metrics in these papers often have the goal to determine if a domain is malicious or benign. For example Bilge et al. uses the domain metrics of: % of numerical characters, % of the length of longest meaningful substring.

4.3 Metrics that can be designed from the dataset

- Distribution of domains per domain extension (.com .org .ru etc.)
- Distribution of domains per country

- Distribution of domains per ASN
- Distribution of domains per malicious type (malware/phishing/spam etc.)
- Distribution of malicious type per country
- Distribution of malicious type per domain extension
- Distribution of file extensions (.html .exe etc.)
- Distribution of malicious type over time.
- Number of reports over time.
- Domain extensions over time

5 References

- Jaquith, Andrew. Security metrics: replacing fear, uncertainty, and doubt. Pearson Education, 2007.
- url: https://zeltser.com/anti-malware-metrics/