Economics of Cyber Security (WM0824TU)
Malware Domain List
Assignment Block 2 (Draft)

Clinton Cao, Jehan Da Camara, Sharif Jacobino and Sunwei Wang
Group - 9

September 17, 2017

1. Introduction

Malware is short for malicious software and it is used to cause harm to computer systems. A well known example of malware is a Trojan horse. This is a software that hides its true intention from the user of the system. Some other forms of malware include adware, ransomware, spyware, and much more.

All these type of malware has lead to various security issues e.g. privacy breach. The privacy of the user can be compromised by having the malware read files that contain personal information of the user, or the adversary can gain access to the webcam without permission. Another security issue that malware can cause is time and financial issues.

Let's look at the following example: The adversary has designed a ransomware, with the goal of earning money from the victims. Once the victim's computer is infected with the this ransonmare, it blocks the whole computer and does not allow the user of the computer to do anything. The only way to unlock the computer is to pay the adversary. The price, that the user will have to pay, might be very high. Another way to unlock the computer is to look for a professional that can remove the ransomware. The owner of the computer will first have to find the professional and then wait for them to remove the ransomware. This costs time and money.

2. Ideal Metrics

The ideal metrics for security decision metrics makers would be to cover the following aspects: the cost of security, benefit of security, and security level. The security level can be further divided into the following categories controls, vulnerabilities, incidents and prevented losses. In our case, we want to increase the security level by having less systems getting infected with malwares. Metrics are needed that would provide the following information:

- How likely a software is a malware?
- How likely a domain is a malicious domain?
- What kind of behaviours of the user is most likely to lead them getting their system infected?
- What kind of system are most likely to get infected?
- Does most malwares originate from the same country?
- What do most people do when their system is infected?
- How hard it is to remove the malware?

3. Existing Metrics Used in Practice

We have taken a look at different metrics (related to malwares) that are used in practice. A way to find malware on Android is to use the software complexity metrics, as proposed by Protsenko and Müller [2]. An example of software complexity metric is Mcabe's Cyclomatic Complexity.

NoticeBored has also provided different metrics that can be used to measure and report malwares [1] An example is the awareness metrics. With awareness metrics, people are evaluated on how familiar they are with certain malwares and whether they understand the risks. Another example is the coverage of antivirus software. This metrics evaluates how many systems are protected with an antivirus software.

4. Our Own Metric

5. Evaluation of the Proposed Metric

References

[1] NoticeBored. Management briefing on malware metrics.

[2] Mykola Protsenko and Tilo Müller. Android malware detection based on software complexity metrics. In *International Conference on Trust, Privacy and Security in Digital Business*, pages 24–35. Springer, 2014.