Economics of Cybersecurity
Assignment 1, draft

Vishan Baldew, Christan Veenman, Martijn Cligge and Stephan Kool

Delft University of Technology, Delft

1 Introduction

With the introduction of The Onion Router (TOR) networks that allow for anonymous navigation of the website, illegal marketplaces - commonly referred to as darknet markets or cryptomarkets - have seen a rise in popularity [4]. The first of its kind, Silk Road, gained attention in popular media and is now shut down. Currently active darknet markets such as Silkroad2, the RealDeal and AlphaBay are used to offer products and services ranging from drugs and child pornography to stolen accounts and zero-day exploits. The availability and exchange of various software vulnerabilities such as zero-day exploits is a significant security issue for both public and private companies, but also for governmental institutes who make use of the software [5]. The infamous Stuxnet computerworm used several 0-days to infect Iranian nuclear reactors whilst being state-sponsored. [1]. Cases like Stuxnet, DigiNotar and many other cases provide enough foundation for organizations to think about the current risks and the assets that they want to protect.

2 Context and scoping

2.1 The Real Deal crypto market

The Real Deal crypto market is one of many crypto markets for selling illegal goods and services. The data we use for the analysis is part of a web archiving attempt and can be found at https://archive.org/details/dnmarchives. What Differentiates the Real Deal market is that is has distinct categories for cyber weapons, unlike other platforms such as the more well-know Silk Road2 which were also in the data. We found clearly distinct categories for Accounts, zero-day weaknesses and Remote Access Trojans (RATs). The offer is made in a forum-like structure with each unique offer having its own link and description. The prices are listed in Bitcoins.

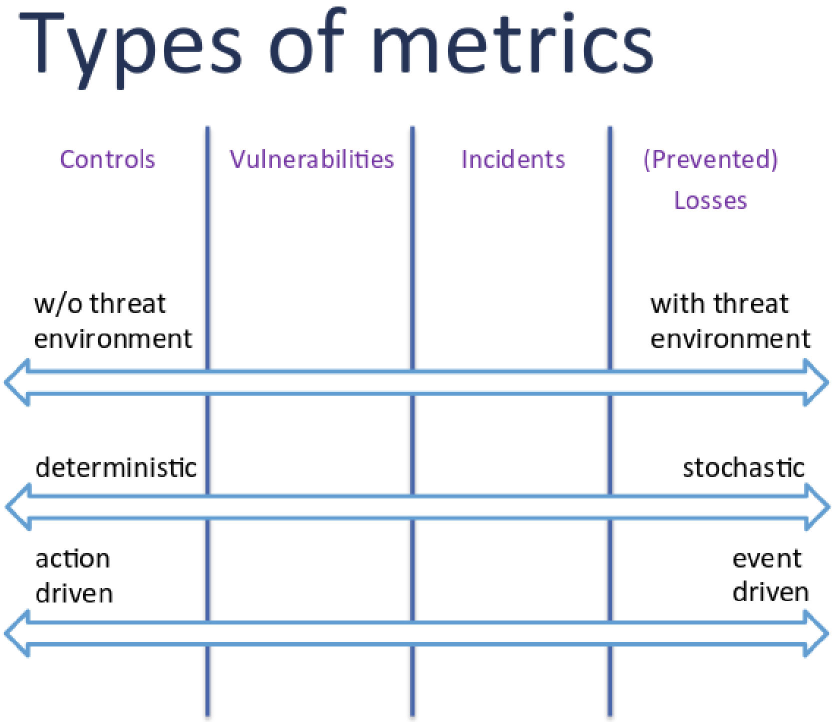
2.2 Stakeholders

A metric needs to serve a purpose and, as such, a stakeholder. This assignment takes the perspective of a defender whose software might be at risk. The aim is to create a metric that serves the defender in making decisions, such as where to look for vulnerabilities, increase control measures, increase mitigation measures or whether or not to buy an exploit themselves in order to patch it. Other stakeholders are the suppliers of the cybercrime products and the buyers of these products.

3 Methodology and future steps

As a first step, the framework proposed by Böhme [2] will be used to come up with a set of ideal metrics for a defender. This is followed up by a discussion on the best achievable metrics in the section state of the art metrics. Finally, the authors explore what metrics are possible to build with the actual data in the data from the real deal crypto market.

4 Metrics



4.1 Ideal Metrics

We used the framework provided in the lectures to come up with some ideal metrics. To help decision-makers deal with some key issues, certain metrics should be in place. The framework, as displayed in figure 1, contains four key metrics that act as latent constructs for the level of security in an organization. Most of the current risk assessment mostly have metrics based on the control metrics characteristics [2] [6]. This is not ideal, since it does not provide the decision-makers a complete overview of the level of security in their organizations.

- *Controls*
  Control metrics measure the level of control measurements that an organization has implemented [6]. It can show whether control measurements are put into place, and the level of maturity of the implemented control measurements. Examples could be the percentage of systems with formal risk assessments in an organization, or the percentage of systems with tested security controls[3].
- *Vulnerabilities*
  Vulnerabilities metrics are the metrics that quantify the amount or level of vulnerabilities. A vulnerability is a weakness in the controls of an organization that could be influenced by cyber attacks. An example of such a metric is the number of identified cyber risks and their severity, or the percentage of weak passwords (non-compliant passwords)[3].
- *Incidents*
  Incidents are events in which security is compromised in some form [2]. An example of a metric that falls in this category is the no. of software patches that have been released for a certain system per year.
- *Prevented losses*
  Prevented losses can be seen as a benefits of security in which an incident and the related losses are prevented [2]. An example of a metric that falls in this category is the no. of leaked user accounts per year.

4.2 State of the art Metrics

Research to state of the art metrics will be performed in a future version of this assignment.

4.3 Metrics from our Data

In the Real Deal cryptomarket dataset, we were able to discriminate by type of cyber-product, ranging from simple spam, account databases to 0-day exploits. Each of these contain a date, a price and a description for its respective purpose. A defender for a company can check for two

Latent variables The best measurable variable in the data set is the price. We think the price is a latent variable for two mechanisms. First, an offer-demand mechanism and secondly a value-based pricing mechanism.

Supply and demand First of all we take a look at the supply of unique suppliers. When there is a high supply of a cyber-crime asset, the price will be likely to drop and the cyber-crime asset is more likely to be bought and used. The supply metric is a combination of the average amount of unique cyber-crime assets in a within a certain time period, in combination with the price metric.

Value-based pricing Value-based pricing is a price mechanism where the price of the final cyber crime asset is based on the value to the attacker, e.g. what the impact is the attacker can achieve with such an attack. For example, a 0-day exploit that allows to achieve full control of any Windows system is valued more than a 0-day exploit that makes a fairly unknown and unused type of router reboot because of a kernel panic. For a defender, the unusually high pricing of a cyber asset measured as being in the upper 25% of historical pricing could be used as a metric for the possible impact of an exploit.

4.4 Future steps

To finalize this assignment we will research and provide state of the art metrics. Furthermore, we will refine the metrics from the dataset by doing more analysis. We will do this by analyzing our dataset and reflecting on the effectiveness and usefulness of the proposed metrics.

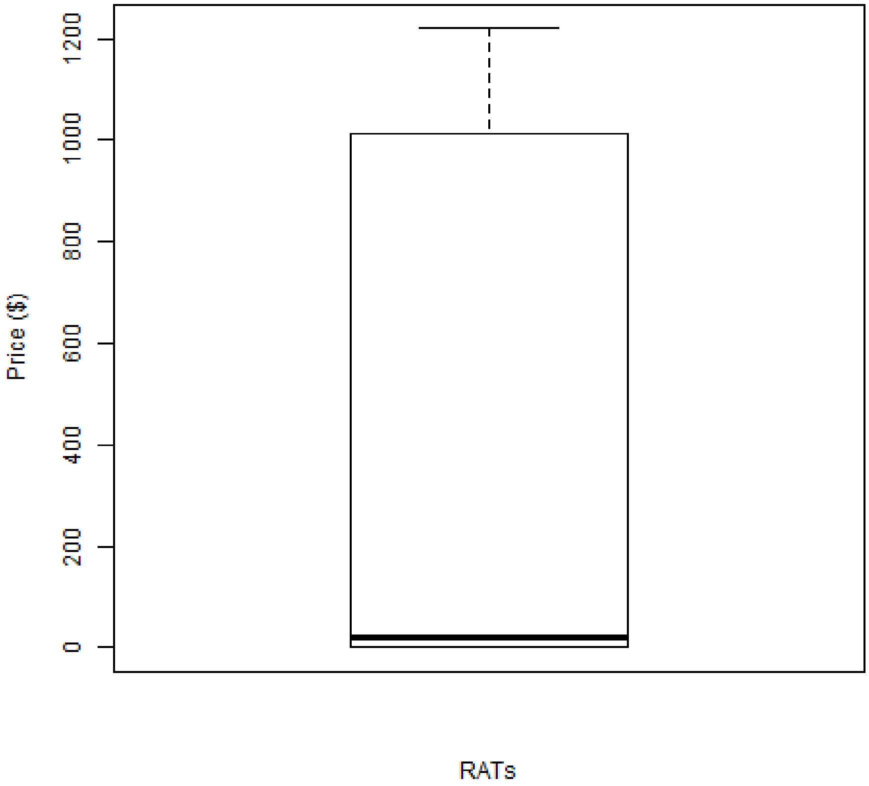
4.5 Conclusion

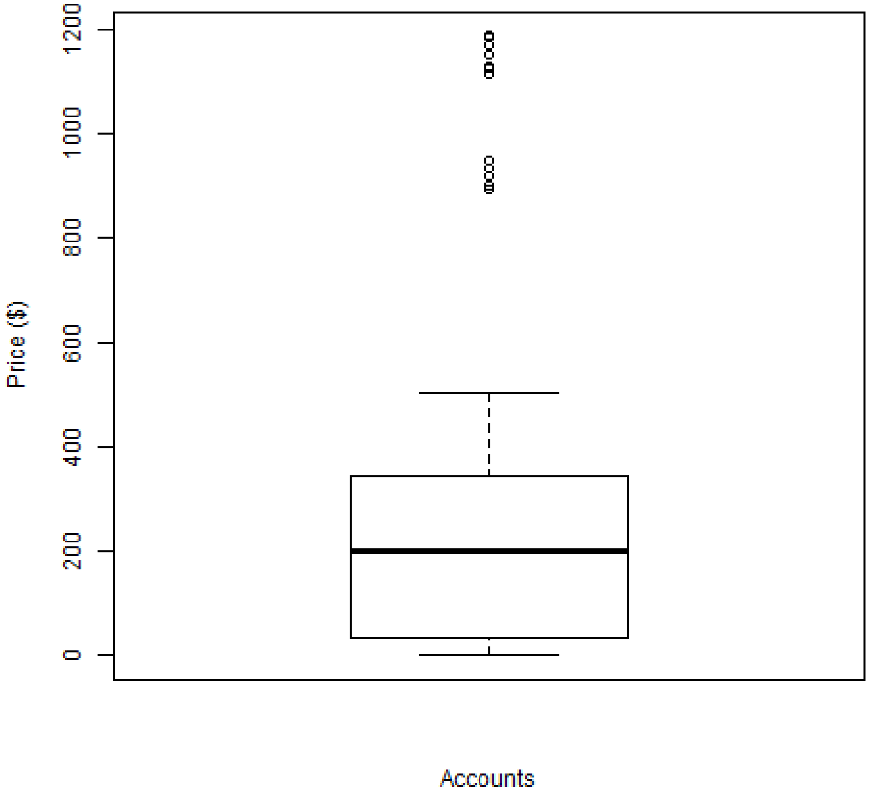
References

1. Falliere, N., Murchu, L. O., & Chien, E. (2011). W32. stuxnet dossier. White paper, Symantec Corp., Security Response, 5, 6.
2. Rainer Bhme, Security Metrics and Security Investment Models, Advances in Information and Computer Security, Lecture Notes in Computer Science Volume 6434, pp 10-24, 2010
3. Zed Abbadi, Security Metrics, what can we measure?, The Public Company Accounting Oversight Board. Retrieved on 24-9-2016 from
4. Owenson, G. H., & Savage, N. J. (2015). The tor dark net. Global Commission on Internet Governance, (20).
5. McGraw, G. (2004). Software security. IEEE Security & Privacy, 2(2), 80-83.
6. van Eeten, M. (2016) Economics of cybersecurity: Measuring security levels. Slides Published on Blackboard TU Delft. http://delftxdownloads.tudelft.nl/EconSec101x-EconomicsCybersecurity/Week

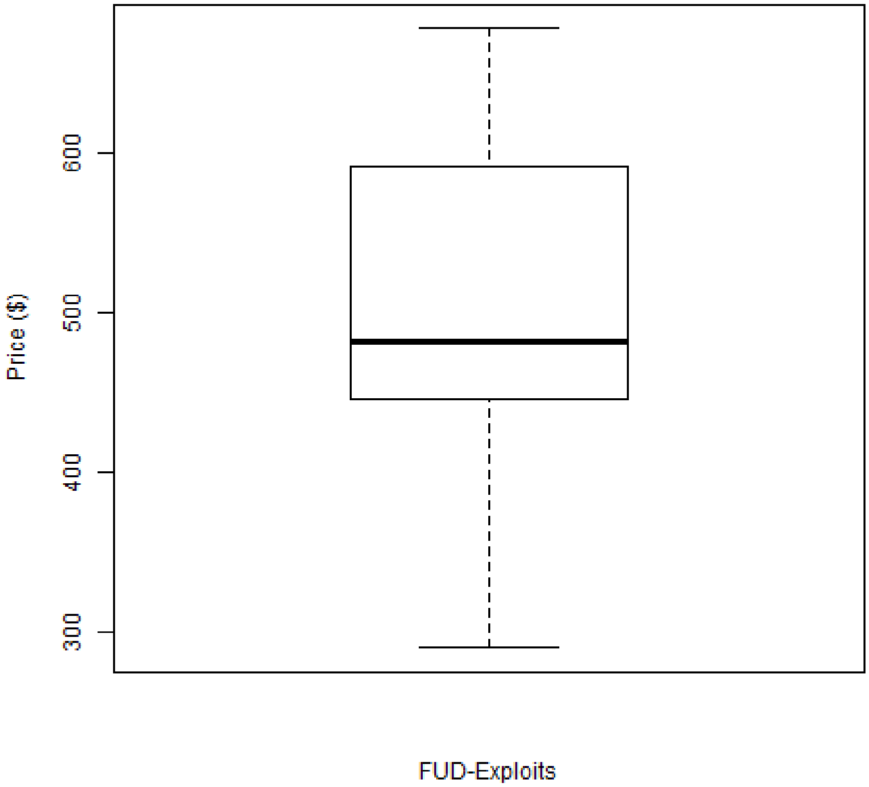
A Appendix 1: Histograms

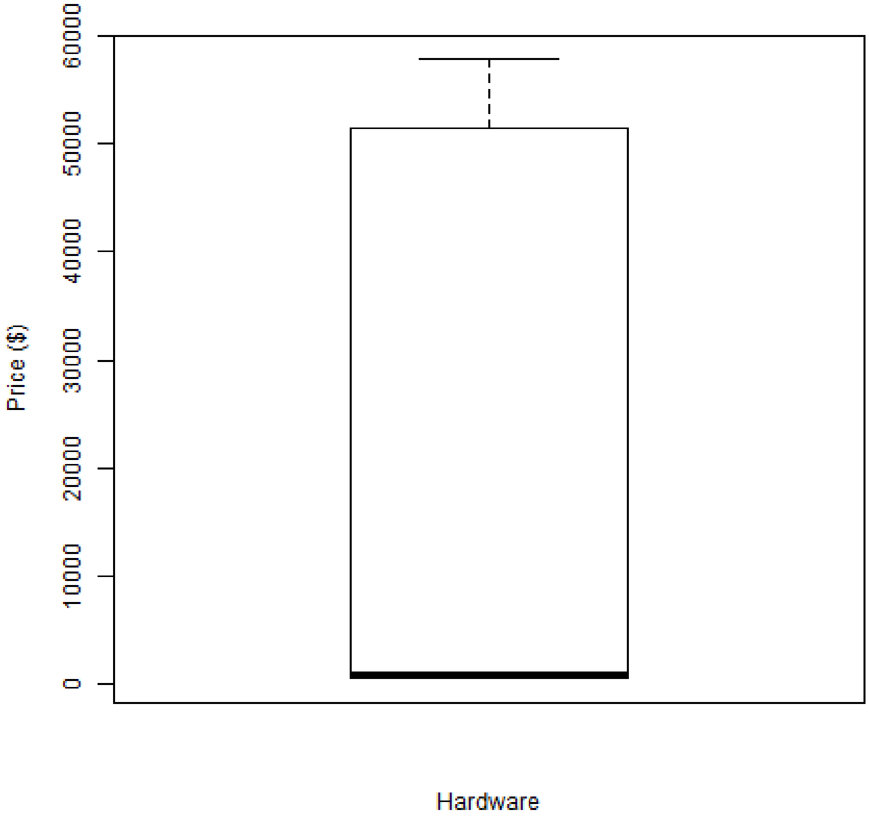
This section contains the pricing of each category of cyber crime assets or exploits.

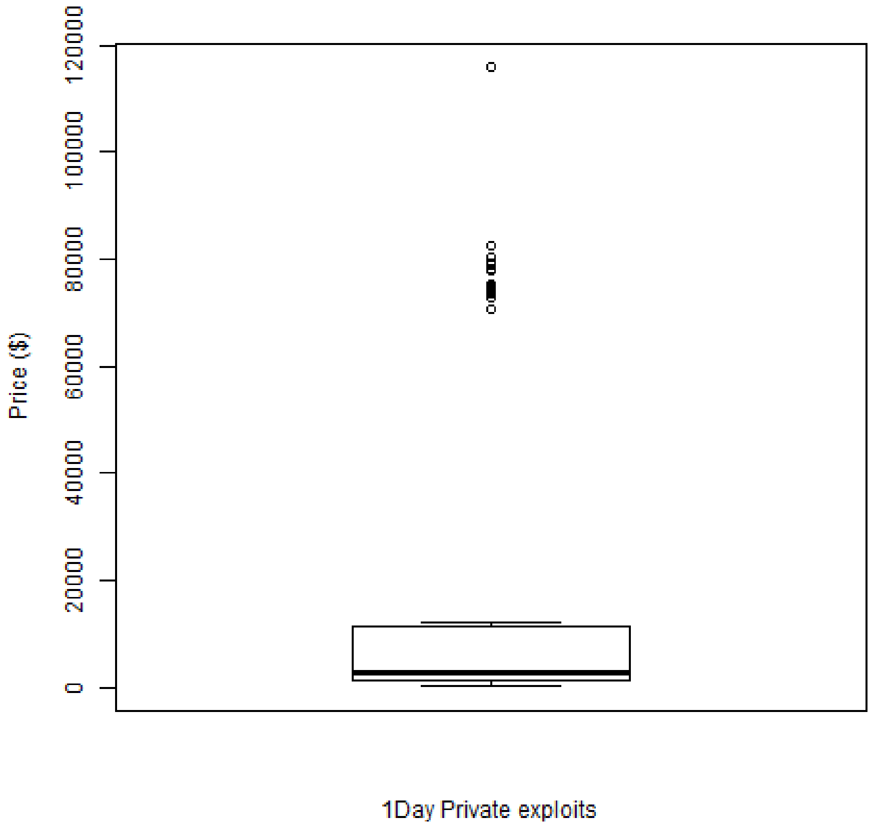

Price ($)
0
200
400
600
800
1000
1200
RATs

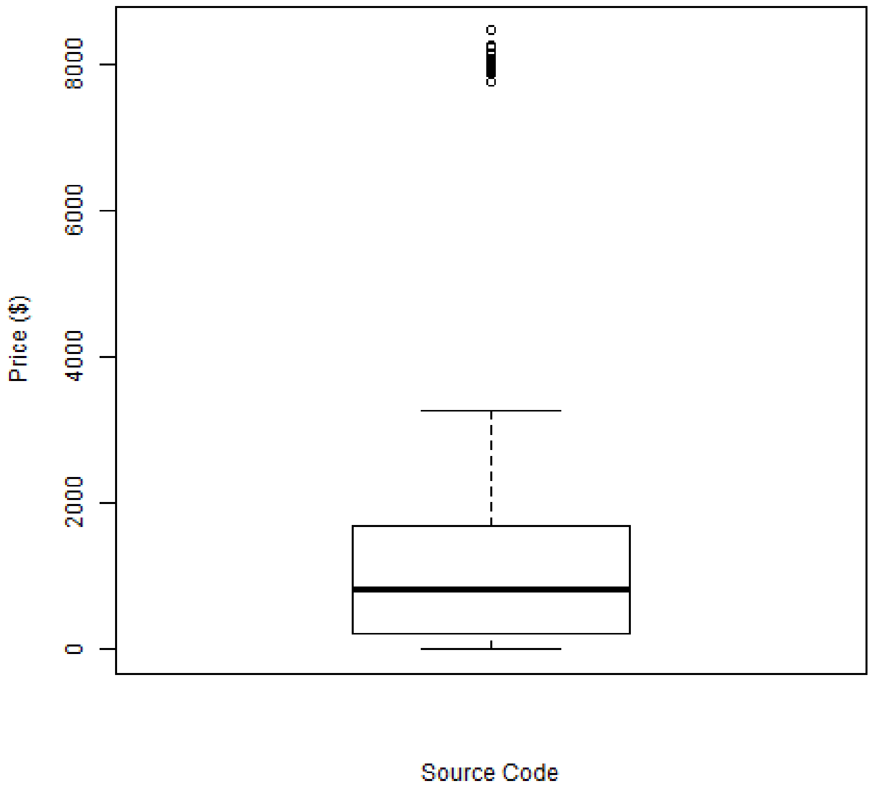


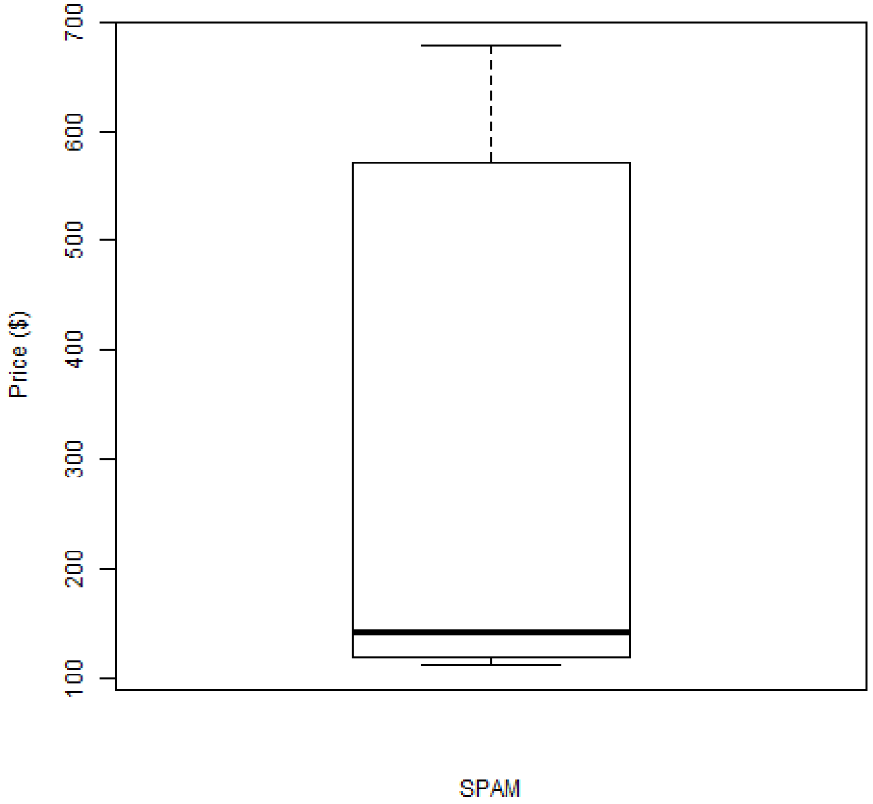
Price ($)
0
200
400
600
800
1000
1200
Accounts

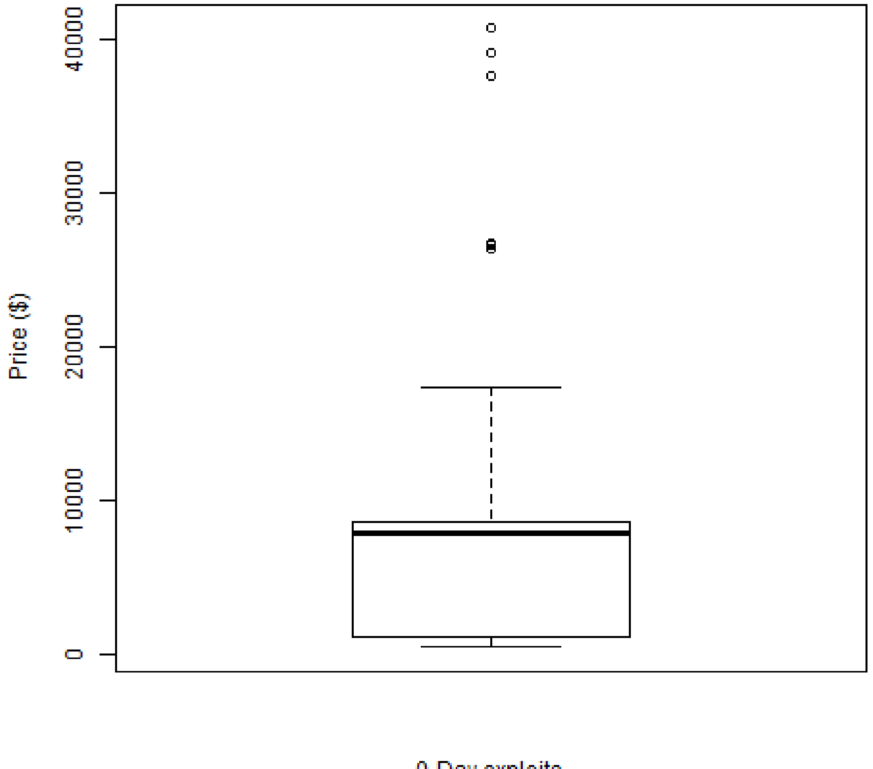

Price ($)
300
400
500
600
FUD-Exploits


Price ($)
0
10000
20000
30000
40000
50000
60000
Hardware


Price ($)
0
20000
40000
60000
80000
100000
120000
1Day Private exploits


Price ($)
0
2000
4000
6000
8000
Source Code


Price ($)
100
200
300
400
500
600
700
SPAM


Price ($)
0
10000
20000
30000
40000
0-Day exploits