SRS 2019

Ransomware Research Project

Author: Nikola Staykov

Supervisor: Yavor Papazov

August 13, 2019

Contents

Abstract

Malware is a type of computer virus, which encrypts the files on a given system and asks for a ransom in order for them to be decrypted. Ransomware authors have no way of knowing their victim's data value, or more precisely what people *think* their data costs. They can, however, make small surveys before launching the main campaign, in order to estimate the aforementioned distribution. This paper explores a model in order to find the most suitable parameters for such a survey. This approach is key to finding the best price for the ransom.

1 Introduction

Malware first appeared in 1989 in the form of the AIDS Troyan, aka PC Cyborg. It was not hard to decrypt after the files but this case set the ground for a lot of the modern threats. With the coming of the Internet age, ransomware returned with new power,

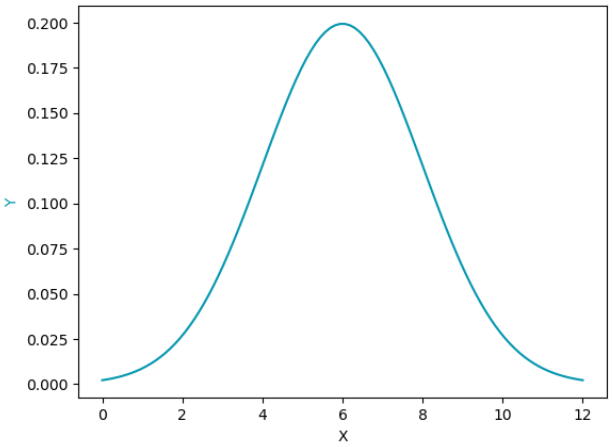
2 Mathematical model

2.1 Mathematical preliminaries

Definition 1 (Normal distribution). *Denoted with $N(\mu, \sigma)$, this is a type of continuous distribution, where:*

- *μ is the mean (in this case also mode and median)*
- *σ is the standard deviation*
- *σ^2 is the variance*

The graph of this function forms a curve, often called informally bell curve. It has maximum $(x, f(x))$ at $(\mu, \frac{1}{\sigma\sqrt{2\pi}})$:



Definition 2 (Standard value (aka Z-score)). *Consider a normal distribution $N(\mu, \sigma)$. The standard value of a given x is computed by $\frac{x-\mu}{\sigma}$ and evaluates how many standard deviations away from the mean the given value is.*

Definition 3 (Probability density function). *For a continuous random variable x, a probability density function describes the probability a random variable x to appear in any interval. Formally it is defined by:*

$$P(x < X \leq x + \Delta) = F_X(x + \Delta) - F_X(x)$$
$$f_X(x) = \lim_{\Delta \to 0} \frac{F_X(x + \Delta) - F_X(x)}{\Delta}$$

Definition 4 (Error function). *The error function is encountered in integrating the normal distribution, it takes z-score as a parameter:*

$$erf(z) \frac{2}{\sqrt{\pi}} \int_0^z e^{-t^2} dt$$

2.2 The approach

This model describes the spread and calculates the optimal ransom for a ransomware attack, distributed exclusively via botnets, without the key component of spreading to every computer in the network. This variant of the attack is relatively cheap to initiate, but has low efficiency.

We will treat the act of decrypting the data of a given computer as a service and the ransom, respectively, will be the price of the service. The parameters and distributions in this model will surely differ from standard market

Consider the distribution for the willingness to pay (WTP) of a given target group. This is the maximum price someone would pay for their data. By putting ourselves in the place of the malware authors, we can try to find out what the distribution is by examining samples of people and how they respond to a given price. This tests, however, cost us valuable time since the awareness of people rises constantly. So the question is, how many and how big test should we conduct in order to model the distribution with reasonable error and in the same time not lose too much time?

For a given size of the sample group, we calculate the error of a set of sample "customers" from the mathematically described function of the demand curve, derived from the distribution of WTP. Starting off low, we gradually expand the sample group size, estimating the expected error, via a Least squares approach, at each step.

2.3 The model

We assume people's data value follows a normal distribution and link it to a random variable $p \sim N(500, 150)$. The probability density function(PDF)[3] of a normal distribution $N(\mu, \sigma)$[1] is:

$$\frac{1}{\sigma\sqrt{2\pi}} e^{-\frac{(x-\mu)^2}{2\sigma^2}}$$

In order to calculate the demand function(as a probability) from the PDF(denoted with $f(k)$) for a given price k, we need to calculate:

$$\int_k^\infty f(x)d(x)$$

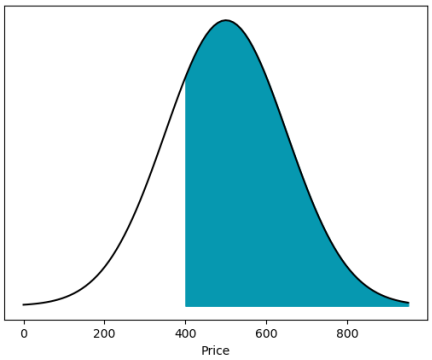


Figure 1: PDF

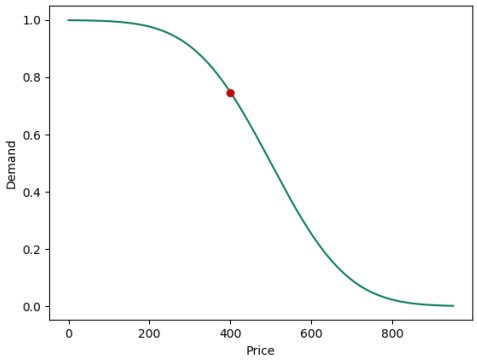


Figure 2: Price vs Demand

We note that the integral must indeed be calculated up to infinity, but after k reaches $\mu + 3\sigma$, the resulting integral is negligibly small. Doing this for the whole probability distribution function gives us the demand curve with respect to what percent of the people would pay. Let us denote the demand curve function with $F(x)$:

$$F(x) = \begin{cases} \frac{1}{2}\left(1 - Erf\left(\frac{z}{\sqrt{2}}\right)\right) \text{ if } x > \mu, \\ \\ \frac{1}{2}\left(1 + Erf\left(\frac{z}{\sqrt{2}}\right)\right) \text{ if } x < \mu \end{cases}$$

With that our mathematical function is well-defined and we can continue to examine experimental data.

The parameter we aim to optimize is the number of people each sample group consists of. Knowing the actual mathematical function we aim to describe gives us the possibility to evaluate the errors from the experimental data with maximum accuracy.

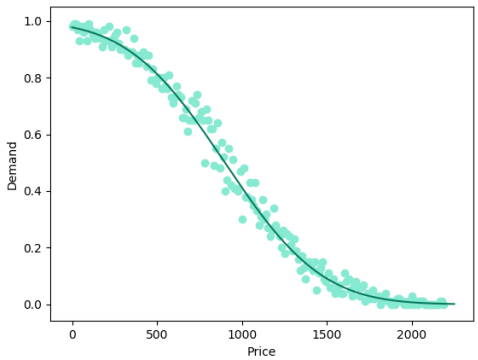


Figure 3: Sample size 100

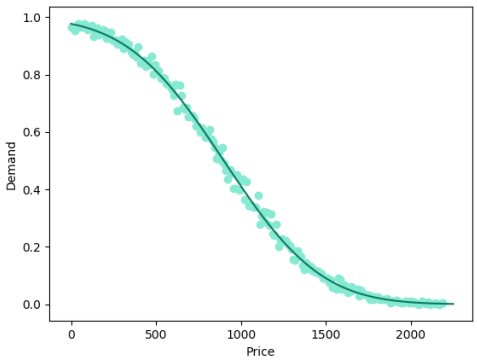
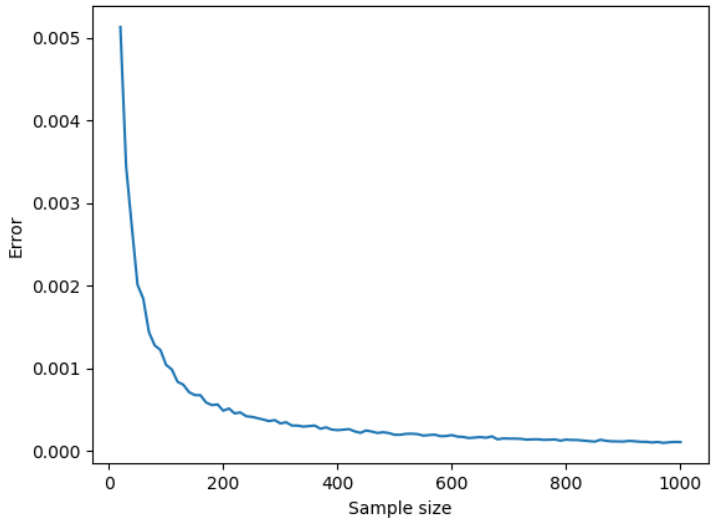


Figure 4: Sample size 400

Gathering information on the sample size and the corresponding errors, we can plot the changes.



3 Results

4 Further development

Acknowledgments

References

[1] Tristan Caulfield, Christos Ioannidis, and David Pym. Dynamic pricing for ransomware.

[2] Danny Yuxing Huang, Maxwell Matthaios Aliapoulios, Vector Guo Li, Luca Invernizzi, Elie Bursztein, Kylie McRoberts, Jonathan Levin, Kirill Levchenko, Alex C Snoeren, and Damon McCoy. Tracking ransomware end-to-end. In *2018 IEEE Symposium on Security and Privacy (SP)*, pages 618–631. IEEE, 2018.

[3] Amin Kharraz, William Robertson, Davide Balzarotti, Leyla Bilge, and Engin Kirda. Cutting the gordian knot: A look under the hood of ransomware attacks. In *International Conference on Detection of Intrusions and Malware, and Vulnerability Assessment*, pages 3–24. Springer, 2015.

[4] Masarah Paquet-Clouston, Bernhard Haslhofer, and Benoit Dupont. Ransomware payments in the bitcoin ecosystem. *Journal of Cybersecurity*, 5(1):tyz003, 2019.

[5] Kurt Thomas, Danny Huang, David Wang, Elie Bursztein, Chris Grier, Thomas J Holt, Christopher Kruegel, Damon McCoy, Stefan Savage, and Giovanni Vigna. Framing dependencies introduced by underground commoditization. 2015.

[6] A Cartwright, Julio Hernandez-Castro, and Anna Stepanova. To pay or not: Game theoretic models of ransomware. In *Workshop on the Economics of Information Security (WEIS), Innsbruck, Austria*, 2018.

[7] J Michael Harrison, N Bora Keskin, and Assaf Zeevi. Bayesian dynamic pricing policies: Learning and earning under a binary prior distribution. *Management Science*, 58(3):570–586, 2012.

[8] Julio Hernandez-Castro, Edward Cartwright, and Anna Stepanova. Economic analysis of ransomware. *Available at SSRN 2937641*, 2017.

[9] Aron Laszka, Sadegh Farhang, and Jens Grossklags. On the economics of ransomware. In *International Conference on Decision and Game Theory for Security*, pages 397–417. Springer, 2017.

[10] Miguel Sousa Lobo and Stephen Boyd. Pricing and learning with uncertain demand. In *INFORMS Revenue Management Conference*, 2003.

[11] Michael Rothschild. A two-armed bandit theory of market pricing. *Journal of Economic Theory*, 9(2):185–202, 1974.