SRS 2019

Ransomware Research Project

Author: Nikola Staykov

Supervisor: Yavor Papazov

September 20, 2019

Contents

1 Introduction **2**

2 Preliminaries **3**

3 Approach **4**

4 Model **4**

4.1 Sample size and error 4

4.2 Backup function 6

5 Results **7**

6 Further development **7**

7 Acknowledgments **7**

Abstract

Ransomware е вид компютърен вирус, който критптира файловете на дадена система и изисква да бъде платен откуп, за да бъдат декриптирани. Приемаме, че създателите на Ransomware не знаят цената на данните на техните жертви, или по-точно колко техните жертви "мислят", че струват данните им. Те могат да правят малки проучвания преди да започнат основната кампания с цел да определят гореспоменатото разпределение. Този проект разглежда модел, чрез който да бъдат определени оптималните параметри за едно такова проучване. Този подход е ключов за намирането на оптималната цена за откупа.

1 Introduction

Ransomware се появява за първи път през 1989 под формата на the AIDS Troyan, познат също като PC Cyborg. The AIDS Trojan е бил доста лесен за преодоляване, тъй като използва симетрична криптография, и скоро са били разработени начини файловете да бъдат декриптирани, но този случай поставя началото на развитието на много от модерните заплахи. С навлизането на Интернет, ransomware се завръща с нова сили, а именно с the Archiveus Trojan и GPcode от 2006. Другповратен момент в историята на malware е създаването на биткойн, и крипто-валутите като цяло, по много причини, някои от тях бидейки анонимността и автоматичните и невъзвръщаеми транзакции[1].

В изминалите години е имало опити да бъде направен модел на пазара на malware. В [2], авторите са създали теоретичен модел, взимайки предвид броя потребители, които имат backups, както и други фактори като разпространението на информация и надеждност на ransomware. В [3] е изследван различен подход, който разглежда възможността за допълнително уговаряне на цената като игра между жертвата и престъпниците. Тази разработка се фокусира на теория на игрите и комбинаторика.

Доста усилия са положени и за проследяването на плащания, свързани с ransomware в блокчейн, тъй като всички те са публични. В резултат на това има публични данни, свързани с тези плащания, предоставени от [4] и в [5] човек може да се запознае с много заключенияв, подкрепени с данни, отнасящи се не само до ransomware, но и до целия черен пазар.

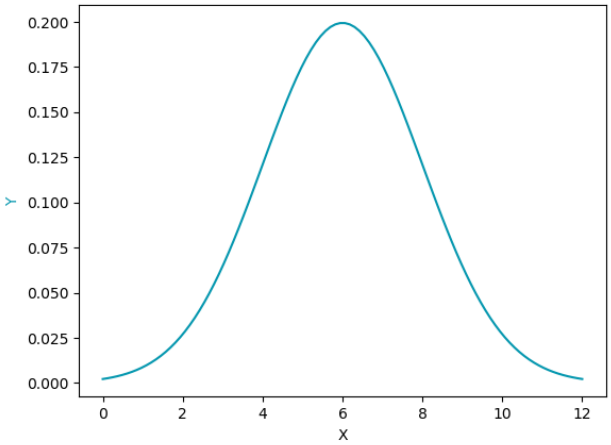
Моделът в настоящата разработка е базиран на описания в [2], но се фокусира върху оптимизирането на параметри, които не са разгледани в споменатата статия.

2 Preliminaries

В тази секция са включени всички дефиниции и концепции, които са нужни за цялостното разбиране на проекта.

Definition 1. *Normal Distribution*, означена с $N(\mu, \sigma)$, е вид continuous distribution, където с μ, σ и σ^2 са означени с, the standard deviation and the variance, respectively.

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



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

Definition 3. For a given distribution the *probability distribution function* $F(x)$ calculates the probability that a random variable, following the distribution, is less or equal to x

$$F_X(x) = \mathbb{P}(x \leq X).$$

Definition 4. The *Probability density function* of 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

$$\begin{aligned}\mathbb{P}(x < X \leq x + \Delta) &= F_X(x+\Delta) - F_X(x)\\ f_X(x) &= \lim_{\Delta \to 0} \frac{F_X(x+\Delta) - F_X(x)}{\Delta}.\end{aligned}$$

Definition 5. *The error function* is encountered in integrating the normal distribution, it takes z-score as a parameter and calculates the integral between a fixed point and the mean of the distribution

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

3 Approach

This model describes the spreading of a ransomware virus. It 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 treat the act of decrypting the data of a given computer as a service and the ransom as the service price, respectively.

Consider the distribution of 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 try to find 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. We strive to determine how many and how big tests 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 the Least Squares Approach, at each step.

4 Model

Here the inner workings of the model are stated in detail, showing how the results and conclusions were reached. The section is divided into two parts, corresponding to the parameters the model explores.

4.1 Sample size and error

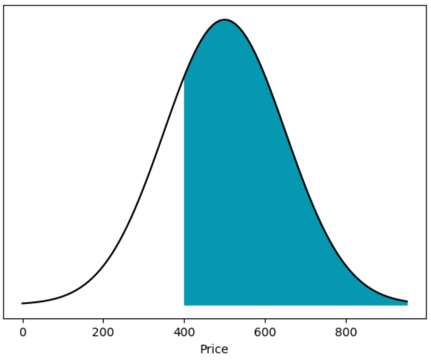
This section describes the mathematical model, used to optimize the error and draw conclusions about the sample size.

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) of a normal distribution $N(\mu, \sigma)$ is

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

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

$$\int_k^\infty f(x)\,\mathrm{d}\,x.$$



$\longrightarrow$

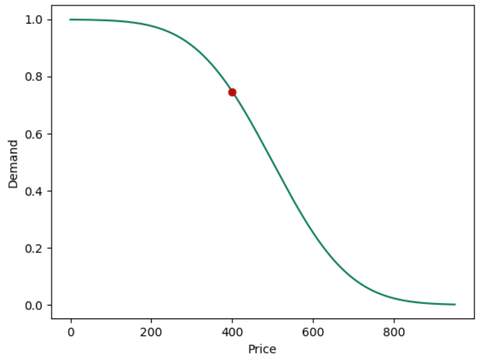


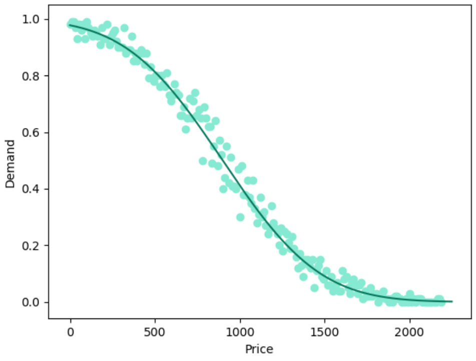
Figure 1: PDF

Figure 2: Price vs Demand

We note that the integral must 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 $F(x)$:

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

We aim to optimize 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.



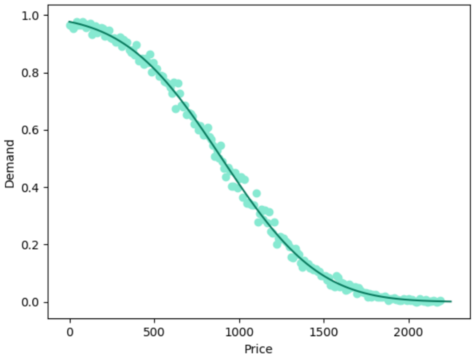


Figure 3: Sample size 100

Figure 4: Sample size 400

By gathering information on the sample size and the corresponding errors, we plot the changes in the error.

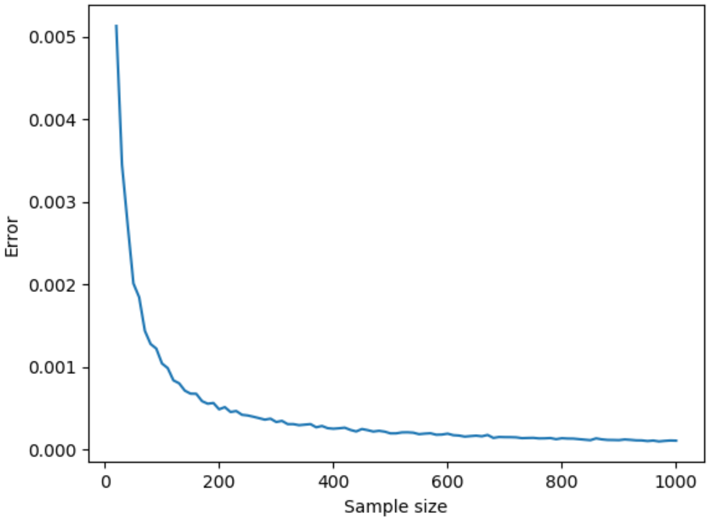


Figure 5: Sample size vs Error

4.2 Backup function

In this section a function, describing the use of backups, is described. The effect on revenue is calculated.

First let us define the backup iterator b:

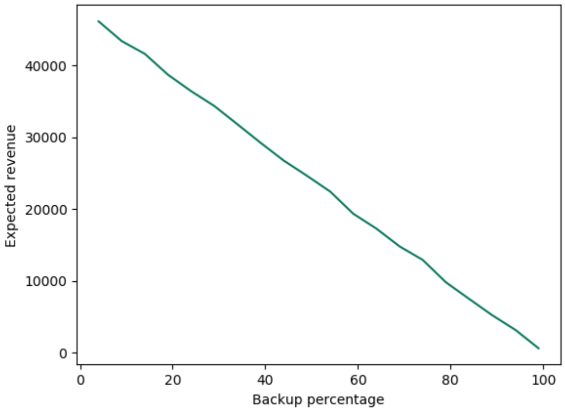
$$b = \begin{cases} 1 \text{ if the victim has backup,} \\ 0 \text{ if the victim does not have backup} \end{cases}$$

Now let us define the willingness to pay (WTP) function:

$$P(x) = \begin{cases} d_x \text{ if } b_i = 0, \\ c \text{ if } b_i = 1 \end{cases}$$

Here the cost of backup is denoted with c and the value of the victim's data - with d_x.

As earlier, we can calculate the expected probability of people paying a ransom of price x We assume that the probability that a single victim has backup follows is p and explore how changing this value affects the expected profit. With the gathered data, we create a plot to show the correlation between the two variables



5 Results

We have explored how the sample size affects the expected error between the statistical and experimental data and have explored how backups affect expected revenue. The model mainly focuses on optimizing the ransom prize, but the author truly believes that in order for us to be able to take countermeasures against ransomware attacks, we need to understand their every move. Putting ourselves in their shoes is essential to the purpose. Additional results, such as the distribution of expected revenue with respect to backup percentages, can help us to draw conclusions how to counteract.

6 Further development

The author considers several future development directions for the project, namely:

- considering the use of backups and its influence on the WTP distribution
- expanding the model to describe more complex way of distributing the ransomware
- using the results and databases of related studies in order to back the project with real data[4]
- considering a dynamic pricing model

7 Acknowledgments

I want to thank my mentor, Yavor Papazov, and Konstantin Delchev for the enormous help with the choice of the research subject and for providing me with all the necessary material to get familiar with the topic, as well as listening to my questions along the whole way. I extend my gratitude towards Victor Velev, Victor Kolev and Stefan Hadzhistoikov for the support I got from them when I needed it the most. I also want to thank Stanislav Harizanov for the professional expertise.

References

[1] 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.

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

[3] 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.

[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] 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.

[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.