Innofair 2019

On Ransomware and Resilient Backup Strategies

Author: Nikola Staykov

Supervisor: Yavor Papazov

science
innovation
FAIR

November 24, 2019

Contents

Abstract

Ransomware 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. By considering the strategies of the attackers, we can optimize our own backup strategy to counteract. This is taken into account in the second section.

1 Introduction

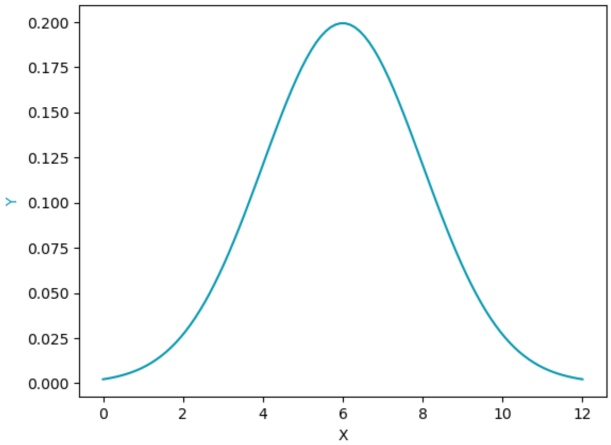
This project is structured in two main parts, considering respectively models for ransom optimization and backup optimization. By thoroughly examining both viewpoints in a situation, a full picture of the strategies of both the attackers and the victims has been created. Considering ways they can optimize their profit gives us insight on how to counteract such malicious behavior in order to reduce the effect of ransomware attacks.

2 Preliminaries

In this section are stated all the needed definitions and concepts one needs to fully understand the paper.

Definition 1. *Normal Distribution*, denoted by $N(\mu, \sigma)$, is a type of continuous distribution, such that μ, σ and σ^2 denote the mean, 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

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

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

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

Definition 6. *A Bernoulli trial* is a random experiment with two outcomes and fixed probability of failure and therefore success:

$$P(\text{success}) = p$$
$$P(\text{failure}) = 1 - p.$$

Definition 7. *A binomial distribution* is the statistical distribution of outcomes(success/failure) when conducting a number of independent Bernoulli trials. For n trials and success probability p the probability that exactly k of them are successful is:

$$P(\text{success} = k) = \frac{\binom{n}{k} p^k (1-p)^{n-k}}{2^k}$$

3 Ransom optimization

3.1 Introduction

Ransomware first appeared in 1989 in the form of the AIDS Troyan, aka PC Cyborg. The AIDS Trojan was pretty easy to overcome as it used simple symmetric cryptography and tools were soon available to decrypt 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, namely with the Archiveus Trojan and GPcode from 2006. Another turning point in the history of ransomware was the invention of bitcoin, and crypto-currencies as a whole, for several reasons, a few of them being anonymity, the transactions are fully automatable and the transactions are irrefutable[1].

In the recent years there have been some attempts to model the ransomware market. In [2], the authors have created a theoretical model, taking into consideration the number of users, who have backups, as well as other factors such as information spread and reliability of the ransomware.

In [3] a different approach has been explored, considering the possibility for bargaining and respectively a game between the victim and the criminals. This paper focuses on game theory and combinatorics.

There has also been considerable amount of effort dedicated to tracking the ransomware payments in the blockchain, as all of them are public. As a result, there is a public data record of such payments, provided by [4] and in [5] many one can observe many data-based conclusions not only concerning ransomware, but also the whole black market.

In this paper, the model is based on the one described in [2], but focuses on optimizing different parameters, unexplored in the aforementioned research.

3.2 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 ransomware 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.

3.3 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.

3.3.1 Sample size and error

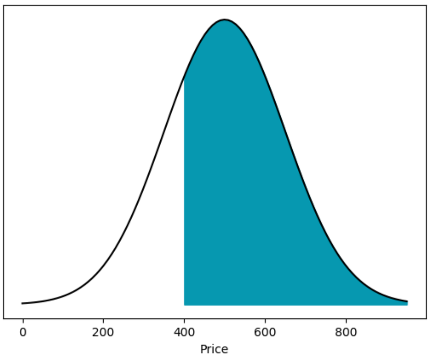
This section describes the mathematical model, used to optimize the error and draw conclusions about the sample size.

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

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



$\longrightarrow$

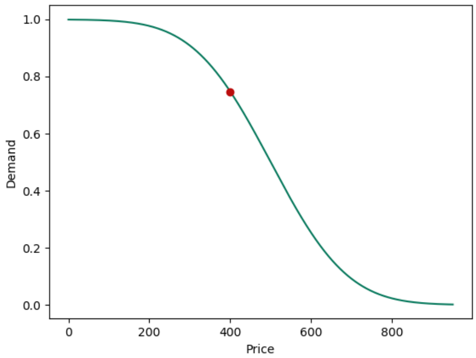


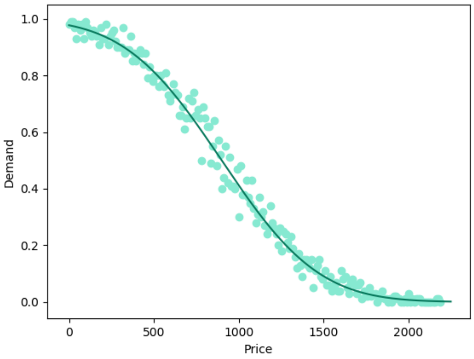
Figure 1: PDF

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.



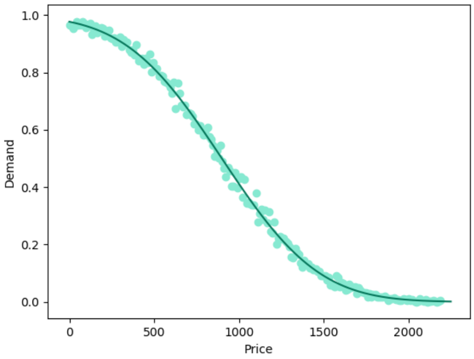


Figure 3: Sample size 100

Figure 4: Sample size 400

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

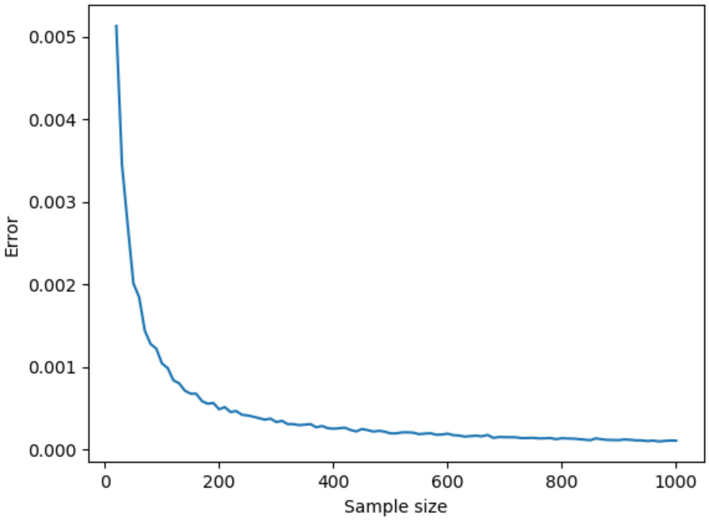


Figure 5: Sample size vs Error

3.3.2 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:

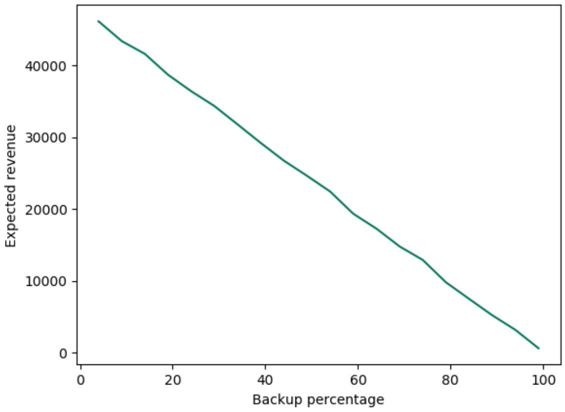
$$b = \begin{cases} 1 \text{ if the victim has backup,} \\ 0 \text{ if the victim does not have backup} \end{cases}$$

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



3.4 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 draw conclusions how to counteract.

4 Backup optimization

4.1 Introduction

When it comes to protection from ransomware, the most efficient method is building backups. This, however, has to be done regularly, as the effects after a potential attack will otherwise be insignificant. That is why it is important for backup protocols to be carefully build, considering both the risks of being attacked and the resources needed for the job. Furthermore, optimizing the backups can simultaneously increase the security level and save money.

In this section, a model for backing up data is considered in order to calculate the expected price. Such models, considering two options for backups: full and incremental, have been constructed and researched in the past[12][13]. We consider a cycle of backups, which repeats over between any two full backups and study how the intervals affect the expected price and how fast the effect of initial data, accumulated before the initial full backup, vanishes over time.

4.2 Theoretical setting

The idea behind the described model is to calculate and optimize the expected price of the recovery in case of an attack.

We will consider a backup as a structure, containing the following properties:

$$B \begin{cases} d\text{: the date on which the backup was made, as a day difference from a starting point} \\ p\text{: the probability that the recovery is unsuccessful for any reason} \\ r\text{: the price of trying to recover the data from the given backup} \end{cases}$$

Two types of backup will be considered:

1. Full backup: a backup of the whole database
2. Incremental backup: only saves the changes from the last backup

The backups from a certain type share common probability of failure and price for a recovery try.

In order for an incremental backup to be successful, all the incremental backups which precede it up to a full backup need to be successful as well as the full backup itself.

In this case data value should clearly be taken into account from a subjective point of view. Even though on the market some data may not be worth a lot, if it is essential for the functioning of a given company, it is clear that it will be willing to pay a lot to regain access to it immediately. Therefore, in the described model data value is considered as an ever-increasing amount, for the purposes of the research the "work rate", namely the data value generated in a day, of the company is taken as a constant. We will denote it with w.

The cost of a backup recovery will be considered as a sum of two factors:

- The cost of redoing the lost work, denoted with W
- The cost of the recovery process itself, denoted with R

. We define $W = \Delta t.w$, where with Δt we denote the difference in days between the successful backup and the disaster date and $R = \sum_{i=1}^{n} r_i$, where the number of attempted backups is n and

$$S = \Delta t.w + R,$$

Let the difference in days from the first backup to the disaster date be T. In case none of the backups are successful, we consider a variable W_T, corresponding to the price of redoing the whole work the company has done from the beginning. It is clear that $W_T > T.w$

4.3 Full backups only

When we only consider a set of full backups, the model is simply a Bernoulli distribution with finite trials, namely the number of full backups. We stop when we find a successful backup, starting from the latest and going to the last. Let us define the properties of a full backup(B_F):

$$B_F \begin{cases} p_F : \text{the probability of failure} \\ r_F : \text{the recovery trial cost} \\ t_F : \text{the days between two consecutive full backups} \end{cases}$$

Let k be the number of full backups made before the disaster date. Then:

$$k = \left\lfloor \frac{T}{t_F} \right\rfloor + 1$$

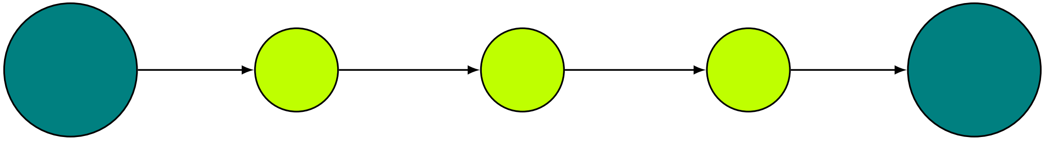
We can now define the expected backup cost:

$$E(T) = p_F^k \left(W_T + k.r_F\right) + \sum_{i=0}^{k-1} (1 - p_F).p_F^i \left(\left(\left\{ \frac{T}{t_F} \right\} + i \right) t_F.w + (i+1).r_F \right) \qquad (1)$$

This calculation is essential as incremental backups can only work when there is a working full backup and therefore the first thing we need to do is find the latest one. We can now move on to considering the incremental backups given a working full backup.

4.4 Incremental backups with a working full backup

We will now consider the case when we have a working backup and we are trying to recover additional data from the incremental backups.



Let us define the the properties of the incremental backup(B_I) in a similar fashion:

$$B_I \begin{cases} p_I : \text{the probability of failure} \\ r_I : \text{the recovery trial cost} \\ t_I : \text{the days between two consecutive incremental backups} \end{cases}$$

Let T_F denote the difference in days between the disaster date and the successful full backup and l denote the number of incremental backups we have to consider. We have two options for l depending on whether the latest full backup was successful:

$$l = \begin{cases} \left\lfloor \frac{T_F}{t_I} \right\rfloor, \text{if } T_F < t_F \\ \left\lfloor \frac{t_F}{t_I} \right\rfloor - 1, \text{if } T_F > t_F{}^1 \end{cases}$$

Note that the last full backup being successful is equivalent to $T_F < t_F$.

We are in the exact opposite situation with respect to the previous subsection. The process of recovering incremental backups continues until we conduct an unsuccessful attempt to recover the data, as this will mean none of the following backups can be used either. Note that we are reducing W since in the initial position we are willing to redo the work up to the working full backup. That being said, we are ready to calculate the expected price:

$$f(T_F) = (1-p_I)^l.((T_F - t_I.l).w + r_I.l) + \sum_{i=0}^{l-1}(1-p_I)^i.p_I((T_F - t_I.i)w + r_I.(i+1)) \quad (2)$$

Now we know how much the price will decrease when we use incremental backups and can build the whole picture using equations 1 and 2.

4.5 Overall expected price

For each summand in 1 we should add the effect of incremental backups, so we get new summands of the type:

$$P(W+R),$$

where P is the probability of a certain combination of events occurring, W is the cost of the data that has to be reworked and R is the cost of the recovery process. Incremental backups lower the cost of the data that has to be reworked but make R bigger. As mentioned before, there is only one case when the number of incremental backups we have to consider is different and it corresponds to the first full backup being successful. If the i-th full backup is successful[2]:

$$T_F = t_F\left(\left\{\frac{T}{t_F}\right\} + i - 1\right)$$

By combining equations 1 and 2 we get:

$$F(T) = p_F^k(W_T + k.r_F) + \sum_{i=0}^{k-1}(1-p_F).p_F^i\left(f(T_F) + (i+1).r_F\right) \quad (3)$$

Using the described equations 1 and 3, we can construct a graph of the expected price with and without incremental backups included.

[1] We can only try to recover incremental backups preceding the next full backup

[2] This corresponds to the $i-1$-th summand in the sum from equation 3

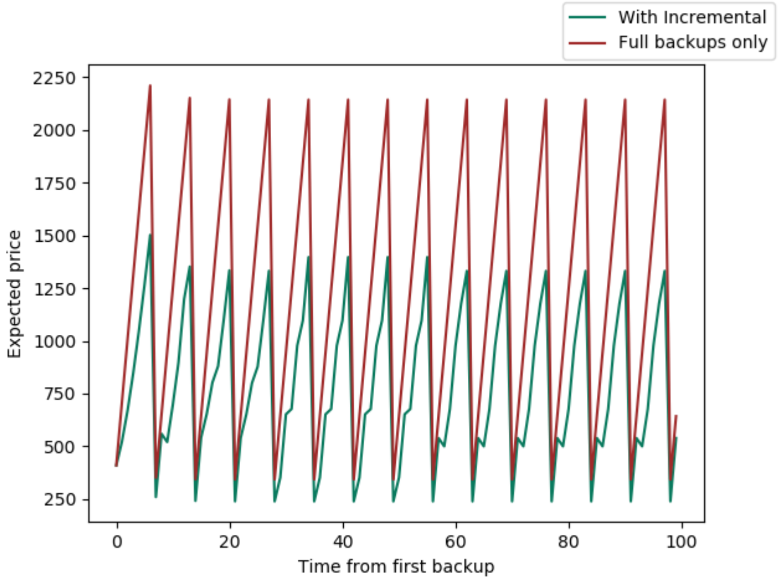


Figure 6: Full only and Whole model

4.6 Monte Carlo simulation

A Monte Carlo simulation has been build with python to generate random recovery processes with the described conditions of backup structure. The price of the recovery has been graphed with respect to the disaster date:

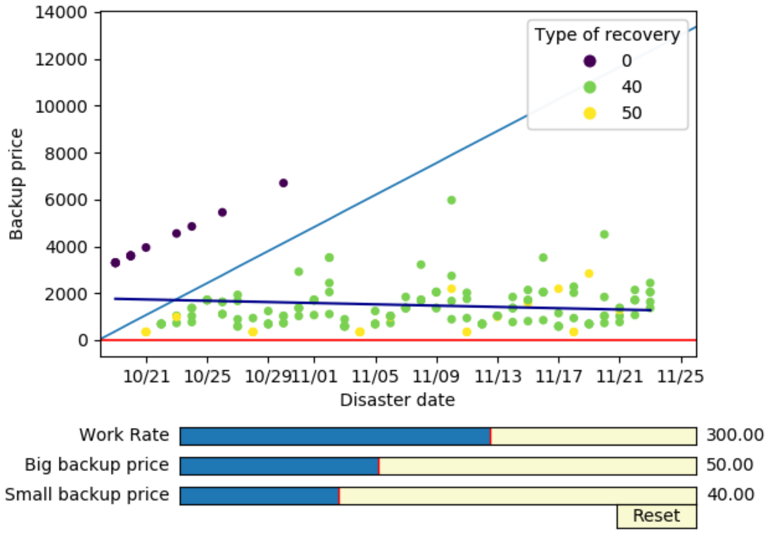


Figure 7: Sample size vs Error

The colors in Figure 7 represent the type of the last backup, which was successful during the recovery, full, incremental or non-existing.

In both Figure 6 and Figure 7 the data showed is for a weekly full and daily incremental backups

4.7 Results

A model for backing up data has been built to calculate the expected price of backup recovery. Furthermore, the effect of incremental backups has been shown, as opposed to a strategy using only full backups. A Monte Carlo simulation has been built and analyzed to demonstrate the real process of recovery.

5 Further development

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

- considering non-constant work rate for the backup model
- expanding the ransomware 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 for the ransomware model

6 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 HSSIMI and SRS for the opportunity to develop this project and the irreplaceable atmosphere of dedication and 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.

[12] S Nakamura, C Qian, S Fukumoto, and T Nakagawa. Optimal backup policy for a database system with incremental and full backups. *Mathematical and computer modelling*, 38(11-13):1373–1379, 2003.

[13] Cunhua Qian, Yingyan Huang, Xufeng Zhao, and Toshio Nakagawa. Optimal backup interval for a database system with full and periodic incremental backup. *JCP*, 5(4):557–564, 2010.