SRS 2019

Ransomware Research Project

Author: Nikola Staykov

Supervisor: Yavor Papazov

September 21, 2019

Contents

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. Друг повратен 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.

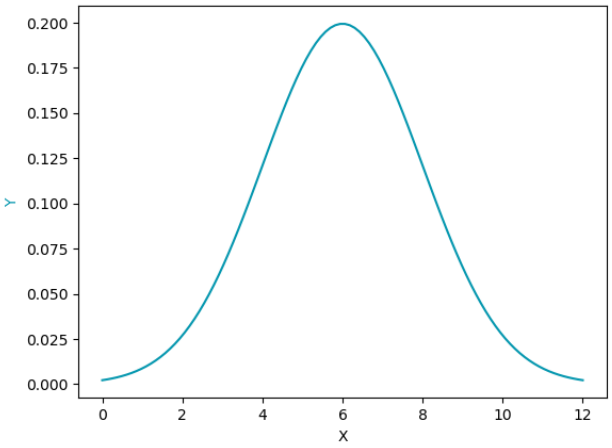
Моделът в настоящата разработка е базиран на описания в [2], но се фокусира върху оптимизирането на параметри, които не са разгледани в споменатата статия.

2 Preliminaries

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

Дефиниция 1. *Normal Distribution*, означена с $N(\mu, \sigma)$, е вид continuous distribution, където с μ, σ и σ^2 са означени средното аритметично, стандартната девиация и вариацията съответно.

Графиката на тази функция образува крива, често наричана също камбанна крива. Тя има максимум $(x, f(x))$ в $\left(\mu, \frac{1}{\sigma\sqrt{2\pi}}\right)$:



Дефиниция 2. Consider a normal distribution $N(\mu, \sigma)$. *Стандартната стойност*, или *Z-score*, на дадено x показва колко стандартни девиации е то от дадената средна стойност. Пресмята се по формулата $\frac{x-\mu}{\sigma}$.

Дефиниция 3. За дадено разпределение the *probability distribution function* $F(x)$ показва вероятността стохастична променлива, следваща разпределението, да е по-малка или равна на x

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

Дефиниция 4. The *Probability density function* на непрекъсната стохастична променлива x, описва вероятността дадена стохастична променлива x да се окаже в произволен интервал. Формално се дефинира чрез

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

Дефиниция 5. *The error function* е резултат на интегрирането на normal distribution, тя приема z-score като параметър и пресмята интеграла между фиксирана точка и средната стойност за разпределението.

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

3 Approach

Този модел описва разпространението на ransomware вирус. Намира оптималната цена на откуп за ransomware атака, която използва единствено botnets, без ключовия компонент на разпространяване на всеки компютър в мрежата. Този вариант на атаката е сравнително евтин за осъществяване, но има ниска ефективност. Третираме декриптирането на файловете на даден компютър като услуга, а откупа като нейната цена, съответно.

Разглеждаме разпределението на Желанието за плащане (ЖЗП) на дадена тестова група. Това е максималната сума, която някой би платил за данните си. Поставяйки се в позицията на престъпниците се опитваме да открием разпределението чрез изследването на тестови групи от хора и как те реагират на дадена цена. Тези тестове обаче ни струват ценно време тъй като осведомеността на хората се показва постоянно. Искаме да разберем колко и колко големи тестове трябва да провеждаме, така че да направим модел на разпределението с приемлива грешка и в същото време без да губим твърде много време.

За даден размер на тестовата група, изчисляваме грешката на дадена група от "потребители" от математически описаната функция на кривата на търсенето, която извличаме от разпределението на ЖЗП. Започвайки с малка група, постепенно увеличаваме размера на тестовата група, изчислявайки и грешката чрез метода на най-малките квадрати на всяка стъпка.

4 Model

Тук математическата страна на модела е разгледана подробно, показвайки как са достигнати резултатите и закюченията. Секцията е разделена на две смислови части, съответстващи на параметрите, които моделът изследва.

4.1 Sample size and error

Тази секция описва математическия модел, използвам за оптимизиране на грешката. Изведени са заключения относно размера на тестовата група.

Приемаме, че стойността на данните на хората следва нормална дистрибуция и я свързваме със стохастичната променлива $p \sim N(500, 150)$. The probability density function (PDF) на нормална дистрибуция $N(\mu, \sigma)$ е

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

За да изчислим функцията на търсене $f(k)$ от PDF за дадена цена k, трябва да изчислим

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

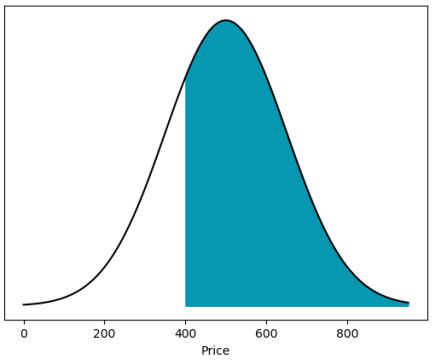


Figure 1: PDF

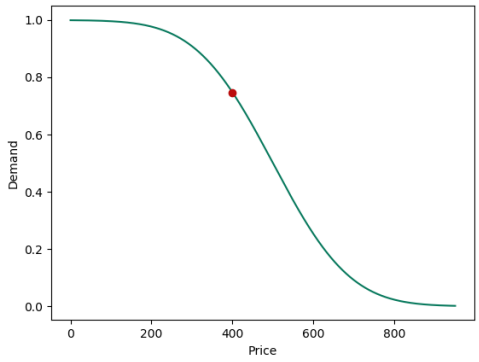


Figure 2: Price vs Demand

Отбелязаме, че интегралът трябва да бъде изчилсен до безкрайност, но след като k стигне $\mu + 3\sigma$, резултатът става пренебрежимо малък. Правейки това за цялата probability distribution function получаваме кривата на търсенето чрез процента хора, които биха платили. Нека означим кривата на търсенето с $F(x)$:

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

Искаме да оптимизираме броя хора във всяка тестова група. Математическата функция, която искаме да опишем ни дава възможността да изчислим грешките от експерименталните данни с максимална точност.

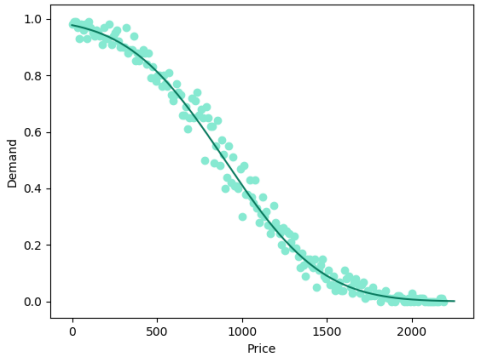


Figure 3: Sample size 100

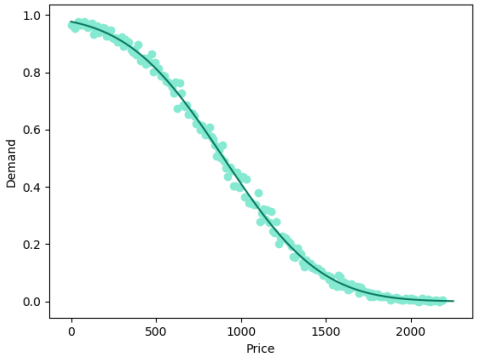


Figure 4: Sample size 400

Събирайки информация за размера на тестовата груап и грешките, съставяме графика, която показва тези промени.

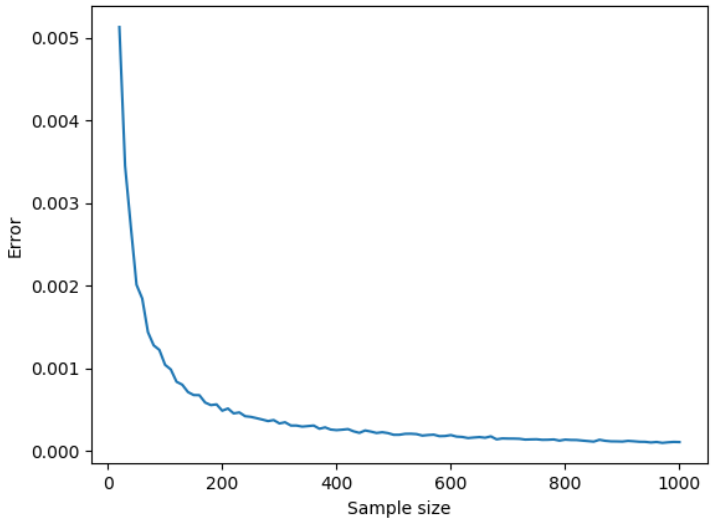


Figure 5: Тестов размер и грешка

4.2 Backup function

В тази секция описваме функция, отговаряща за вероятността за присъствието на backup. Изчислен е ефектът и фърху очакваната печалба.

Първо нека дефинираме the backup iterator b:

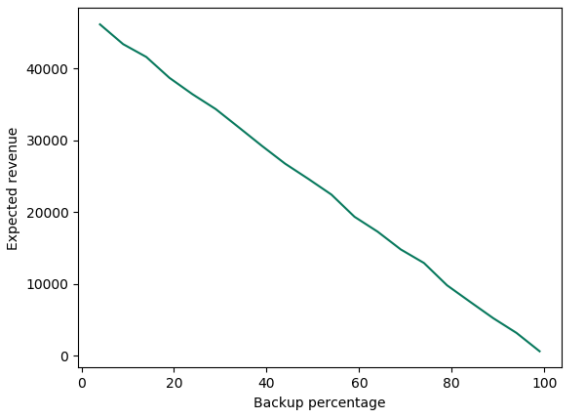
$$b = \begin{cases} 1 \text{ if the victim has backup,} \\ 0 \text{ if the victim does not have backup} \end{cases}$$

Сега нека дефинираме желанието за плащане (ЖЗП):

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

Тук цената на backup е означена с c, а цената на данните на жертвата- с d_x.

Както и по-рано, изчисляваме очакваната вероятност даден човек да плати цена x. Приемаме, че вероятността конкретна жертва да има backup е константа p и изследваме как промяната на тази стойност влияе на очакваната печалба. Чрез събраните данни създаваме графика, която показва връзката между двете променливи.



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.