SRS 2019

Моделиране на рансъмуер

Автор: Никола Стайков

Ментор: Явор Папазов

28 септември 2019 г.

Съдържание

Абстракт

Рансъмуер е вид компютърен вирус, който критптира файловете на дадена система и изисква да бъде платен откуп, за да бъдат декриптирани. Приемаме, че създателите на рансъмуер 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 Въведение

Рансъмуер 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, рансъмуер се завръща с нова сили, а именно с the Archiveus Trojan и GPcode от 2006. Друг повратен момент в историята на рансъмуер 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 бекъпи, както и други фактори като разпространението на информация и надеждност на рансъмуер. 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 рансъмуер 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 рансъмуер, но и до целия черен пазар.

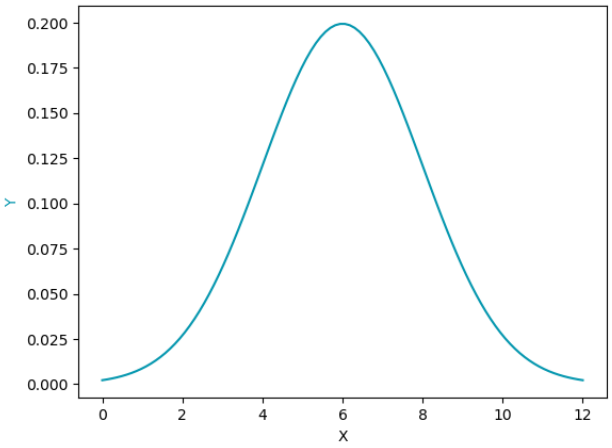
Моделът в настоящата разработка е базиран на описания в [2], но се фокусира върху оптимизирането на параметри, които не са разгледани в споменатата статия.

2 Теория

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

Дефиниция 1. *Нормално разпределение*, означено с $N(\mu, \sigma)$, е вид непрекъснато разпределение, 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. Разглеждаме нормално разпределение $N(\mu, \sigma)$. *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 *функцията на разпределение* $F(x)$ показва вероятността стохастична променлива, следваща разпределението, да е по-малка или равна на x

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

Дефиниция 4. *Плътност на разпределение* 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. *Грешка от първи род* е резултат на интегрирането на нормално разпределение, 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 Подход

Този модел описва разпространението на рансъмуер вирус. Намира оптималната цена на откуп за рансъмуер 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 Модел

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 Размер на тестовата група и грешка

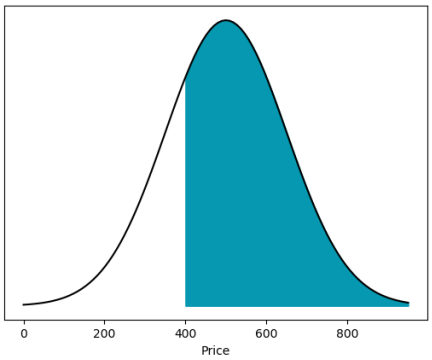
Тази секция описва математическия модел, използвам за оптимизиране на грешката. Изведени са заключения относно размера на тестовата група.

Приемаме, че стойността на данните на хората следва нормална дистрибуция и я свързваме със стохастичната променлива $p \sim N(500, 150)$. Вероятностната плътност (ВП) на нормална дистрибуция $N(\mu, \sigma)$ е

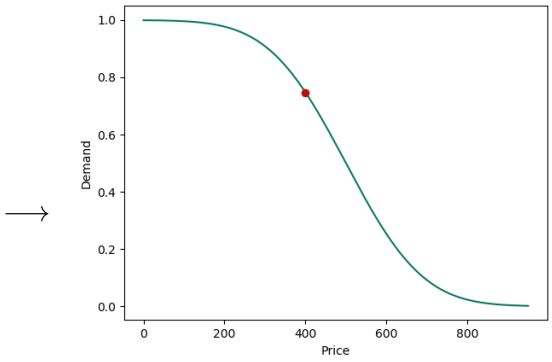
$$\frac{1}{\sigma\sqrt{2\pi}} e^{-\frac{(x-\mu)^2}{2\sigma^2}}.$$

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

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



Фигура 1: ВП

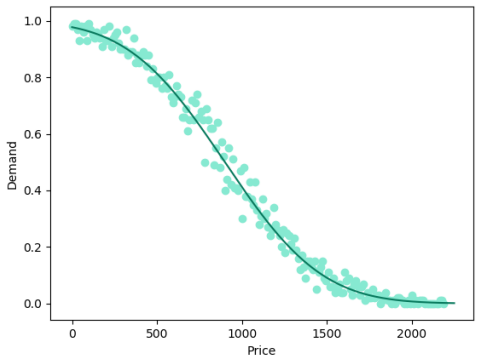


Фигура 2: Цена и търсене

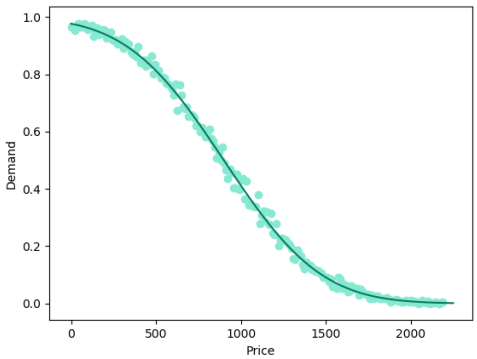
Отбелязаме, че интегралът трябва да бъде изчилсен до безкрайност, но след като k стигне $\mu + 3\sigma$, резултатът става пренебрежимо малък. Правейки това за цялата функция на разпределението получаваме кривата на търсенето чрез процента хора, които биха платили. Нека означим кривата на търсенето с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

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

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.

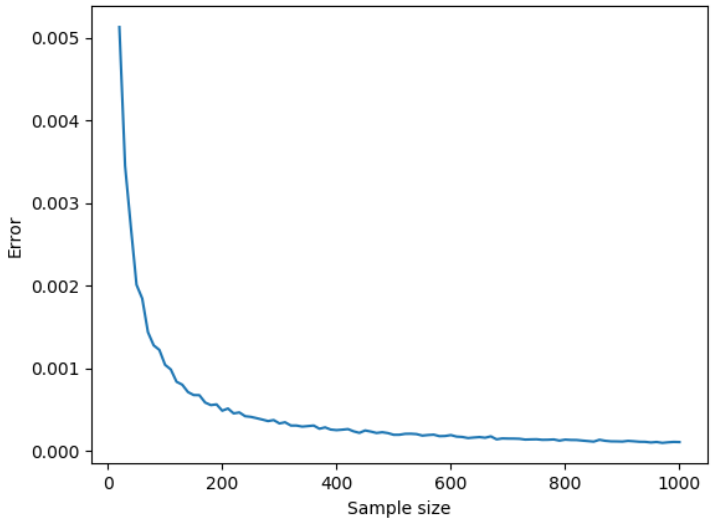


Фигура 3: 100 човека в групата



Фигура 4: 400 човека в групата

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



Фигура 5: Тестов размер и грешка

4.2 Бекъп функция

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

Първо нека дефинираме бекъп итератора b:

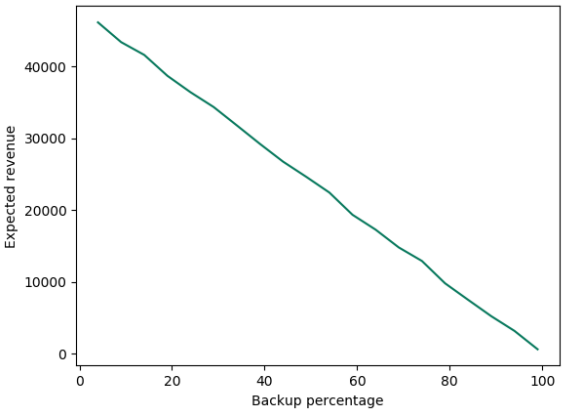
$$b = \begin{cases} 1 \text{ ако жертвата има бекъп,} \\ 0 \text{ ако жертвата няма бекъп} \end{cases}$$

Сега нека дефинираме желанието за плащане (ЖЗП):

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

Тук цената на бекъп 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 бекъп 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. Измерената грешка е относителна.



5 Резултати

Изследвахме как размерът на тестовата група влияе на грешката на експерименталните данни и също как процента на защитените с бекъпи влияе на очакваната печалба. Моделът се фокусира на оптимизирането на цената на откупа, но авторът вярва, че за да можем да предприемем подходящи предпазни мерки срещу атаки от този вид, трябва да разбираме всеки ход на престъпниците. Поставяйки се на мястото на извършителите е ключово за целта. Допълнителни резултати, като връзката между очакваната печалба и броя на хората с бекъпи може да ни помогне да стигнем до подходящи подходи за справяне със заплахата.

6 Бъдещо развитие

Авторът предвижда бъдещето развитие а проекта в няколко посоки, а именно:

- търсене на връзка между бекъпите и ЖЗП разпеделението
- разширяване на модела с цел да описва по-сложен начин на разпространение между машините в дадена система
- използването на разултатите и данните на други подобни разработки с цел подкрепянето на проекта с реални данни[4]
- разглеждане на динамичен модел за определяне на цената.

7 Благодарности

Искам да благодаря на своя ментор, Явор Папазов, и на Константин Делчев за безотказната помощ в избора на темата на проекта и последващото му развитие, за снабдяването ми с всички нужни материали за запознаването ми с темата, както и за изслушването на въпросите ми. Искам също да благодаря на Станислав Харизанов за професионалните съвети.

Литература

[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.