POSTER: How Attackers Determine the Ransom in Ransomware Attacks

Tom Meurs
University of Twente
Enschede, Netherlands
t.w.a.meurs@utwente.nl

Marianne Junger
University of Twente
Enschede, Netherlands
m.junger@utwente.nl

Abhishta Abhishta
University of Twente
Enschede, Netherlands
s.abhishta@utwente.nl

Erik Tews
University of Twente
Enschede, Netherlands
e.tews@utwente.nl

***Abstract*—Ransomware may lead to massive economic damage to victims [13]. However, it is still unclear how attackers determine the amount of ransom. In this poster we empirically study the ransom requested by attackers in ransomware attacks. We analysed 371 ransomware attacks reported to the Dutch Police between 2019 and 2021. Our results indicate that attacker's effort and opportunity are important predictors for the ransom requested. The goal of the poster is to invite other researchers for collaboration.**

***Index Terms*—Ransomware, cyber attacks, criminal revenue, police reports**

1. Introduction

Ransomware attacks have become more prevalent over the past years [1]. Even though most ransomware attackers are financially motivated [9], the actual financial gains made by attackers are still unclear. This poster abstract aims at introducing a dataset that could be used to empirically study the ransom requested by attackers.

The Rational Choice Perspective (RCP) [2], [3] states that criminal decision-making is based on weighing the costs and benefits of an attack. Costs could be effort or risk of being caught by Law Enforcement. Benefits is mostly money, but could also be reputation. Based on RCP, we hypothesise that ransom requested depends on how much effort attackers put in a ransomware attack. Furthermore, there might be an increase of requested ransom over the years because improved anti-virus scanners might make it more difficult to perform ransomware attacks and therefore require more effort.

A complementary approach is the Routine Activity Theory (RAT) [10]. RAT focuses on the opportunities for attackers provided by context. From RAT it follows that victims with more money provide the opportunity for attackers to earn more money and therefore will demand higher ransom [6]. Furthermore, opportunity might vary between seasons [12], so requested ransom could also vary between seasons.

Summarizing, attacker's effort and opportunity could influence ransom requested (Figure 1) .We propose the following hypotheses:

- H1: If attackers put in more effort they will ask a larger ransom
- H2: There is an increasing trend of requested ransom over the years
- H3: High revenue of victims should lead to larger requested ransom
- H4: The requested ransom varies over the different seasons

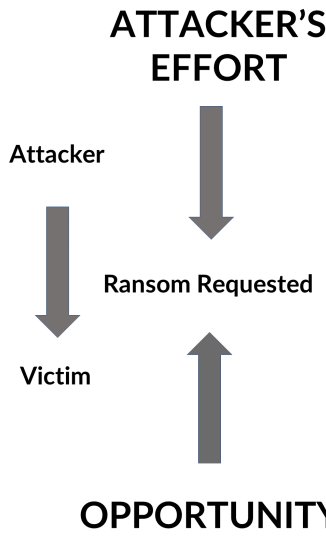

Figure 1: Theoretical framework

2. Methods

2.1. Sample

We investigated 371 ransomware attacks registered by the Dutch Police between 2019 and 2021. Ransomware attacks on individuals as companies were included in the sample. Ransomware attacks with victims outside the Netherlands, but reported to the Dutch Police, were excluded from this study.

2.2. Measures

To measure requested ransom information about the ransom at first contact with victims was collected. From the 371 observations, 172 attacks (46 %) reported ransom demanded by attackers. If ransom demanded was unknown, this was mostly (52 %) because attackers wanted victims to contact them to inform them about the ransom and the victim did not want to do so. In our analysis we perform analysis to see if there is selection bias of the unknown requested ransomware.

To measure effort information was collected on several variables.

a) Ransom note. We noted whether the criminals wanted to first have contact with the victim before informing what ransom they requested, from here defined as targeted ransom note (categories: yes/no). Yes means that first contact with the attackers was required to obtain information about the ransom. No means that the ransom was stated on the ransom note.

b) Exfiltrated of data measured whether data from the victim were exfiltrated (categories: yes/no).

c) Collaboration with other criminals, measures whether the attackers made use of RaaS [12] or whether they collaborated with other groups to perform the attack (categories: yes/no).

d) What type of access was used to infiltrate victim's network (categories: exploit/phishing/different),

e) Network Attached Storage measures whether attackers targeted the Network Attached Storage device (categories: NAS, yes/no).

f) Furthermore, the name of group that executed the attack was included if more than 5 attacks were observed, the rest was aggregated to the variable 'different'. We assumed that groups vary in the amount of effort used in attacks, and therefore might also vary on the required ransom.

To measure opportunity information was collected on several other variables: We noted

a) Company size, which was based on staff and

b) Yearly revenue.

Additional variables included:

c) Insurance (categories: yes/no),

d) Economic sector (categorized by the Dutch Chamber of Commerce),

e) Type of victim (categories: corporate/governmental/individual) and

f) Backups (categories: no/yes, but not possible to recover of data/yes, but could partially recover data / yes, and could fully recover data).

Temporal aspects were:

g) Season and

h) Year.

We assume that the context provides more opportunities when there are higher profits to be made: a victim with high revenue might be able and willing to pay a higher ransom. We did not have particular expectation on seasonality.

2.3. Analysis

First, we analyse selection bias on whether the requested ransom is known and correct with Heckman's two-step procedure [4], [7]. Second, we performed multiple imputation analysis using the R-package Mice [5]. Third, stepwise regression was performed on different models to find a parsimonious model. From explanatory analysis we found that ransom demanded, yearly turnover and staff were highly skewed, so we take the logarithm.

3. Results

Our final model (1) from the stepwise regression:

$$\begin{aligned} Log_{10}RR = 1.44 + 0.72DE + 1,03TR \\ + 0.51RaaS – 0.99NAS \\ + 0.32Log_{10}REV – 2.25IMR + \epsilon \end{aligned} \quad (1)$$

Where RR is the ransom requested, DE is data exfiltrated $\in \{0,1\}$, TR is targeted ransom note $\in \{0,1\}$, RaaS $\in \{0,1\}$, NAS $\in \{0,1\}$, REV is yearly turnover, and IMR is inverse Mills Ratio. IMR is the correction for the selection bias.

The coefficients should be interpreted as follows (Figure 2): 3034 euro is the geometrical mean. If data was ex-filtrated, the ransom requested would be +430% above the geometrical mean. If the ransom note was targeted, the ransom requested would be +980%. If the group was RaaS, the ransom requested would be +220%. If the attack targeted a NAS, the ransom requested would be -90%. An increase of the yearly turnover with 1% would increase the ransom requested with 0.32 %. Finally, the negative IMR means that the expected RR observed in this sample is lower than the expected RR in the population.

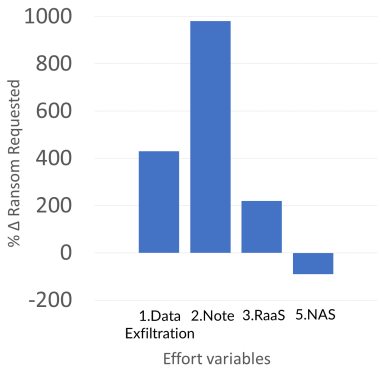

Figure 2: Significant results of effort variables on ransom requested.

No heteroskedasticity was found in (1) (Breusch-Pagan (6) = 10.171, p = 0.12). Residuals ϵ are normaly distributed (Shapiro-Wilk=0.993,p=0.08). To test the sensitivity of the imputation of missing values we performed the same regression on ransom requested without the observation with missing values and found the same coefficients to be significant ($\alpha = 0.05$).

The IMR was esimated using the probit regression:

$$RR_B = \gamma_1' IR + \gamma_2' TR + \nu \quad (2)$$

Where $RR_B \in \{0,1\}$ is whether the ransom requested was known in this sample, IR is whether there was a Incident Reponse company helping the company to recover after the attack and targeted ransomnote whether the criminal first wanted to make contact with the victim before telling how much ransom they requested for the decryption keys. With (2) we can estimate γ and therefore the IMR :

$$IMR = \frac{\phi(\hat{\gamma_1}' IR + \hat{\gamma_2}' TR)}{\Phi(\hat{\gamma_1}' IR + \hat{\gamma_2}' TR)} \quad (3)$$

For a detailed explanation why (2) and (3) lead to

unbiased, consistent and efficient estimators in (1) when selection bias is present, we refer to [5].

In conclusion, data exfiltration, targeted ransomnote, RaaS, NAS, revenue predict the ransom requested by attackers in ransomware attacks. Insurance, sector, backups, corporate/governmental/individuals and ransomware group, year and season do not influence the ransom requested.

Our results indicate that criminal effort and victim's company size influence the ransom demanded, but that temporal aspects did not effect the amount of ransom demanded. Furthermore, we found selection bias in this sample: the ransom requested in the population should be larger than in the present sample. Surprisingly, having backups did not effect the ransom requested. Also companies being insured did not lead to higher requested ransom, although this might be the result of low amount of observations. Furthermore we also did not find a relationship between year and season and ransomware requested.

4. Discussion and Conclusion

In this study we modeled the way ransomware actors determine how much ransom they demand during a ransomware attack. Regarding our hypotheses we found:

- H1: If attackers put in more effort they will ask a larger ransom, as expected.
- H2: There is no increasing trend of requested ransom over the years, in contrast with expectations
- H3: High revenue of victims should lead to larger requested ransom, as expected
- H4: In contrast with previous findings does the requested ransom not vary over the different seasons

Furthermore, we found there was a selection bias regarding requested ransomware in this sample and that the observed requested ransomware was an underestimation for the true requested ransomware in our sample.

There are at least two potential limitations concerning the results. First, the selection of attacks registered to the Dutch Police may be a (biased) subset of all attacks in the Netherlands. However, if the Dutch Police notices that there are Dutch victims who did not notify the Police, they will pro-actively contact the victim. A second potential limitation is that for some variables there was a lot of missing information.

Despite these limitations, this study is the first to systematically analyse ransomware with different ways of measuring effort and contextual variables. Whereas past researchers have used around 50 attacks and mostly companies who were the victim [8], the present study analyzed 371 attacks with individuals, companies and government as victim.

Although the generality of the current results must be established by future research, the present study has provided clear support that RCP and RAT are applicable to ransomware attacks. These findings suggest several courses of action for policy makers and Law Enforcement. First, improve prevention by reaching out to potential high-risk victims. Second, frustrate the ransomware process by increasing efforts of attackers for a successful ransomware attack.

References

[1] Oz, H., Aris, A., Levi, A., Uluagac, A. S. (2021). A survey on ransomware: Evolution, taxonomy, and defense solutions. arXiv preprint arXiv:2102.06249.

[2] Hechter, M., Kanazawa, S. (1997). Sociological rational choice theory. Annual review of sociology, 23(1), 191-214.

[3] Cornish, D. B., Clarke, R. V. (1989). Crime specialisation, crime displacement and rational choice theory. In Criminal behavior and the justice system (pp. 103-117). Springer, Berlin, Heidelberg.

[4] Heckman, J. J. (1979). Sample selection bias as a specification error. Econometrica: Journal of the econometric society, 153-161.

[5] Van Buuren, S., Groothuis-Oudshoorn, K. (2011). mice: Multivariate imputation by chained equations in R. Journal of statistical software, 45, 1-67.

[6] Galinkin, E. (2021). Winning the Ransomware Lottery: A Game-Theoretic Model for Mitigating Ransomware Attacks. arXiv preprint arXiv:2107.14578.

[7] Bushway, S., Johnson, B. D., Slocum, L. A. (2007). Is the magic still there? The use of the Heckman two-step correction for selection bias in criminology. Journal of quantitative criminology, 23(2), 151-178.

[8] Yuryna Connolly, L., Wall, D. S., Lang, M., Oddson, B. (2020). An empirical study of ransomware attacks on organizations: an assessment of severity and salient factors affecting vulnerability. Journal of Cybersecurity, 6(1).

[9] Hassan, N. A. (2019). Ransomware revealed: a beginner's guide to protecting and recovering from ransomware attacks. Apress.

[10] Cohen, L. E., Felson, M. (1979). Social change and crime rate trends: A routine activity approach. American sociological review, 588-608.

[11] Junger, M., Wang, V., Schlömer, M. (2020). Fraud against businesses both online and offline: crime scripts, business characteristics, efforts, and benefits. Crime science, 9(1), 1-15.

[12] Huang, K., Siegel, M., Madnick, S. (2018). Systematically understanding the cyber attack business: A survey. ACM Computing Surveys (CSUR), 51(4), 1-36.

[13] Oosthoek, K., Cable, J., Smaragdakis, G. (2022). A Tale of Two Markets: Investigating the Ransomware Payments Economy. arXiv preprint arXiv:2205.05028.