

SRS 2019

---

# Modeling Ransomware

---

*Author:* NIKOLA STAYKOV

*Supervisor:* YAVOR PAPAZOV

August 6, 2019

**Contents**

<b>1</b>	<b>Introduction</b>	<b>2</b>
<b>2</b>	<b>Mathematical model</b>	<b>2</b>
2.1	The simple one . . . . .	2

# Abstract

## 1 Introduction

## 2 Mathematical model

### 2.1 The simple one

This model describes the spread and 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. Parameters:

1. Realization
2. P-profit
3. s-number of people who received the spam
4. d-coefficient of people who would download the ransomware
5. b-coefficient of people having backups
6. c-coefficient of people willing to pay with respect to infected
7. r-ransom, to be optimized
8. E-expenses
9.  $P_b$ -price of spam campaign(/1000 mails)
10.  $T_a$ -Affiliate tax percentage

$$U = \ln(R); \quad P = s * d * b * c * r; \quad E = \frac{P_b * s}{1000} + T_a * P$$

## References

- [1] K. Thomas, D. Huang, D. Wang, E. Bursztein, C. Grier, T. J. Holt, C. Kruegel, D. McCoy, S. Savage, and G. Vigna, “Framing dependencies introduced by underground commoditization,” in *Workshop on Economics of Information Security*, WEIS, 2015.
- [2] D. Y. Huang, M. M. Aliapoulos, V. G. Li, L. Invernizzi, E. Bursztein, K. McRoberts, J. Levin, K. Levchenko, A. C. Snoeren, and D. McCoy, “Tracking ransomware end-to-end,” in *2018 IEEE Symposium on Security and Privacy (SP)*, pp. 618–631, IEEE, 2018.
- [3] A. Kharraz, W. Robertson, D. Balzarotti, L. Bilge, and E. 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*, pp. 3–24, Springer, 2015.
- [4] M. Paquet-Clouston, B. Haslhofer, and B. Dupont, “Ransomware payments in the bitcoin ecosystem,” *Journal of Cybersecurity*, vol. 5, no. 1, p. tyz003, 2019.