SRS 2019

Ransomware Research Project

Author: Nikola Staykov

Supervisor: Yavor Papazov

August 13, 2019

Contents

Abstract

Malware 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.

1 Introduction

Malware first appeared in 1989 in the form of the AIDS Troyan, aka PC Cyborg. It was not hard to decrypt after 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,

2 Mathematical model

2.1 Mathematical preliminaries

2.2 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.

We will treat the act of decrypting the data of a given computer as a service and the ransom, respectively, will be the price of the service. The parameters and distributions in this model will surely differ from standard market

The model starts off with a mathematically described distribution for the willingness to pay (WTP) of the people. Even though we define it by ourselves, by putting ourselves in the place of the malware authors, we can try to find put what the distribution is by examining samples of people and how they respond to a given price.

3 Results

4 Further development

Acknowledgments

References

[1] D. Y. Huang, M. M. Aliapoulios, 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.

[2] 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.

[3] M. Paquet-Clouston, B. Haslhofer, and B. Dupont, "Ransomware payments in the bitcoin ecosystem," *Journal of Cybersecurity*, vol. 5, no. 1, p. tyz003, 2019.

[4] 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," 2015.

[5] T. Caulfield, C. Ioannidis, and D. Pym, "Dynamic pricing for ransomware,"

[6] A. Cartwright, J. Hernandez-Castro, and A. Stepanova, "To pay or not: Game theoretic models of ransomware," in *Workshop on the Economics of Information Security (WEIS), Innsbruck, Austria*, 2018.

[7] J. M. Harrison, N. B. Keskin, and A. Zeevi, "Bayesian dynamic pricing policies: Learning and earning under a binary prior distribution," *Management Science*, vol. 58, no. 3, pp. 570–586, 2012.

[8] J. Hernandez-Castro, E. Cartwright, and A. Stepanova, "Economic analysis of ransomware," *Available at SSRN 2937641*, 2017.

[9] A. Laszka, S. Farhang, and J. Grossklags, "On the economics of ransomware," in *International Conference on Decision and Game Theory for Security*, pp. 397–417, Springer, 2017.

[10] M. S. Lobo and S. Boyd, "Pricing and learning with uncertain demand," in *INFORMS Revenue Management Conference*, 2003.

[11] M. Rothschild, "A two-armed bandit theory of market pricing," *Journal of Economic Theory*, vol. 9, no. 2, pp. 185–202, 1974.