Towards a Taxonomy for Classifying Knowledge on Ransomware as a Service (RaaS) Specializations

Tim Smith[1][0000-0002-2914-8039] and Miloslava Plachkinova[2][0000-0003-0338-7813]

[1] 3116 Gerdin Business Building, 2167 Union Drive, Ames, IA 50011
[2] 560 Parliament Garden Way NW, Kennesaw, GA 30144

Abstract. Ransomware has become one of the most popular types of cybercrime due to the relatively low risk of obtaining a significant financial reward. Many organizations and governments choose to pay to get their data back, typically using cryptocurrency, which motivates even further individual offenders and criminal groups to develop the process of commoditizing ransomware. The current study adds knowledge to this new and still relatively unexplored domain. Our findings can be valuable to law enforcement officers to better differentiate the levels of involvement in a RaaS scheme and prosecute the individuals accordingly.

Keywords: Ransomware, Ransomware-as-a-Service, RaaS, Design Science Research, DSR, Theory of Organized Crime, Division of Labor, Specializations

1 Introduction

Cybercrime has been on the rise in the past few decades, and it is estimated that by 2025, it will cost the world $10.5 trillion annually [1]. Ransomware is one of the most lucrative crimes – between 2019 and 2020, ransomware attacks rose by 62 percent worldwide, and by 158 percent in North America alone [2]. An even more alarming trend is the fact that ransomware has now become a commodity and it is frequently being offered on the black market as Ransomware as a Service (RaaS). Just like Software as a Service (SaaS) products, RaaS gives relatively cheap and easy access to various types of malicious programs for a much smaller fee than the cost of creating it on your own – as little as $175 [3]. The growing impact of ransomware and its relatively easy access motivate us to further study the problem from an academic perspective by analyzing its complexity and multifaceted nature.

We posit that the first step in combatting RaaS is to provide a better understanding of the various actors involved in the process and to define the complicated nature of their relationships. The research question guiding this study is: "How can we classify knowledge on the various Ransomware as a Service specializations?" We answer it by identifying and describing the different roles individuals have within the RaaS

environment. We take a design science approach (DSR) [4] to create our taxonomy, as it giv

tiple stages and iterations of our work. First, to demonstrate the rigor of the current work and to frame the context, we utilize theory of organized crime. Second, we offered information on the recent RaaS trends affecting society

6. Creators are the authors of the various software tools and technologies

strategies and interventions that make such collaborations more complex, less efficient, and lacking in any obfuscation of legal liability.

The purpose of the current study was to classify knowledge on RaaS. We developed a taxonomy to explain the division of labor in a typical RaaS structure and add knowledge to this relatively new domain. The common underlying distinction between past ransomware and the emerging RaaS is that producers of the ransomware tools are now distanced from those using these tools to target and deploy them. We identify this emerging new organizational form as exhibiting an increased division of labor. Much like the evolution from craftsman-like work structures to specialized subdivision of labor that was the foundation of the industrial age, such dividing of labor greatly increases the productive capacity of these new RaaS organizational forms. The rise of such new organizational forms represents a significant new threat.

The taxonomy introduced in this paper can assist researchers by focusing on the specific behaviors, motivations, skill acquisition process, and means of coordination each role employs. Moreover, cybersecurity professionals can utilize this taxonomy to improve surveillance and monitoring processes and to communicate with other law enforcement agencies using a common understanding of the labor divisions that are emerging within such threats.

5 Limitations and Future Work

Our proposed taxonomy is among the first attempts to conceptualize the complex nature of RaaS and define the various roles and relationships between RaaS actors. Since most of the activities are illegal and taking place in communication channels hidden from the public, it is inherently difficult to obtain primary data. However, our next steps will focus on refining the taxonomy and evaluating it through qualitative data collection encompassing semi-structured interviews with security professionals and law enforcement officers. Following DSR best practices, we will use triangulation and will validate the taxonomy further by using it to explain recent RaaS attacks where sufficient information was made available to the public. As this is still research in progress, we have not

enforcement to better differentiate the level of involvement of the various RaaS actors.

References

1. Morgan, S. 2020;
Available from: https://cybersecurityventures.com/hackerpocalypse-cybercrime-report-2016/.
2. Jeffery, L. and V. Ramachandran. . 2021; Available from: https://www.pbs.org/newshour/nation/why-ransomware-attacks-are-on-the-rise-and-what-can-be-done-to-stop-them.
3. Granger, D. . 2017; Available from: https://www.recordedfuture.com/karmen-ransomware-variant/.
4. Hevner, A., et al., MIS Quarterly, 2004. **28**(1): p. 75-105.
5. Alra7 0 Td -