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 organizations. As a result, a new form of crime has emerged – ransomware as a service (RaaS). We examine this new phenomenon from a design science research (DSR) perspective and propose a taxonomy of RaaS labor division. Our goal is to identify and classify the roles of the different actors involved in 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 gives us useful guidance on the development, refinement, and evaluation of our artifact. Our findings can be used by law enforcement officers to better differentiate the levels of involvement in a RaaS scheme and prosecute the individuals accordingly.

2 Background

Ransomware is a malware category that exploits security vulnerabilities to hijack files and render data inaccessible. The perpetrators of such attacks demand ransoms be paid for users to regain access to these resources. This lucrative venue has been further expanded by RaaS, which is a franchise model that lets people without programming skills to become active attackers and engage in the ransomware economy. This approach allows ordinary people and smaller players an easier way into the criminal world while reducing the risk of exposure for the ones on top of the value chain. Various online services such as darknet marketplaces, social media, and messaging platforms have contributed to the rapid growth of RaaS. While previous studies have established success factors for ransomware [5] and the need for more public awareness about this crime [6], still very little is known about its commoditization. New advances in blockchain and distributed ledger technologies make it even easier for criminals to create and share ransomware.

Early instances of ransomware attacks were primarily conducted by individuals, or small groups, of hackers who focused primarily on the development and delivery of exploit tools [7]. With the rise of RaaS, we are witnessing the emergence of new organizational forms that greatly reduce the innate limitations of simple organizational structures. We posit that, although decentralized, the RaaS environment is actually a well-oiled machine, and we leverage organizational theory to explain its functions.

Although organizational theory was initially used to explain organized crime such as the mafia, loan sharks, or other criminal syndicates [8], we argue it is also relevant to organized cybercrime, as it is an extension of physical space. We utilize this theory to build the foundations of our taxonomy and to identify the key roles of RaaS members. This theory has already been operationalized to explain organized cyber-racketeering [9] and we are extending it to RaaS as well, because it addresses similar issues such as power dynamics, value added, communication, and even marketing approaches used by the criminals to advertise their services and activities. These studies support our argument to apply theory of organized crime to identify the various relationships between the actors involved in a RaaS enterprise. Our artifact, a RaaS labor division taxonomy, is built upon the idea of conceptualizing these interactions and examining them from a theoretical perspective.

3 Taxonomy Development

We take a DSR approach to develop the proposed RaaS taxonomy. We follow the four cycles (rigor, relevance, design, and change and impact) [10] to explain the multiple 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 to show the relevance of our artifact. Third, we use this knowledge to design our taxonomy. Finally, we demonstrate its value and potential impact to organizations and governments.

We designed the RaaS taxonomy as an evolving distributed network that seeks an optimal division of labor that produces the specializations we aim to classify. Specializations lead to achieving higher levels of production for any given set of resources and inputs, including RaaS. Therefore, understanding what the emerging RaaS specializations are will motivate new research into understanding new organizational dynamics that produce new, and more intensified cyber threats against organizations and governments.

Based on our literature review, relevant case studies, and publicly available information, we constructed the Taxonomy of RaaS Labor Division (Fig. 1). We developed this taxonomy via Saldaña's [11] two-cycle inductive coding process. First, all identified sources were coded for mentions of specific roles or specializations. Second, the diverse initial set of codes were clustered into categories of specialization. Our preliminary results show that the while a typical ransomware attack involves a single perpetrator or group, in a RaaS scheme, the role is subdivided into seven narrow specializations. Following is a discussion of each role.

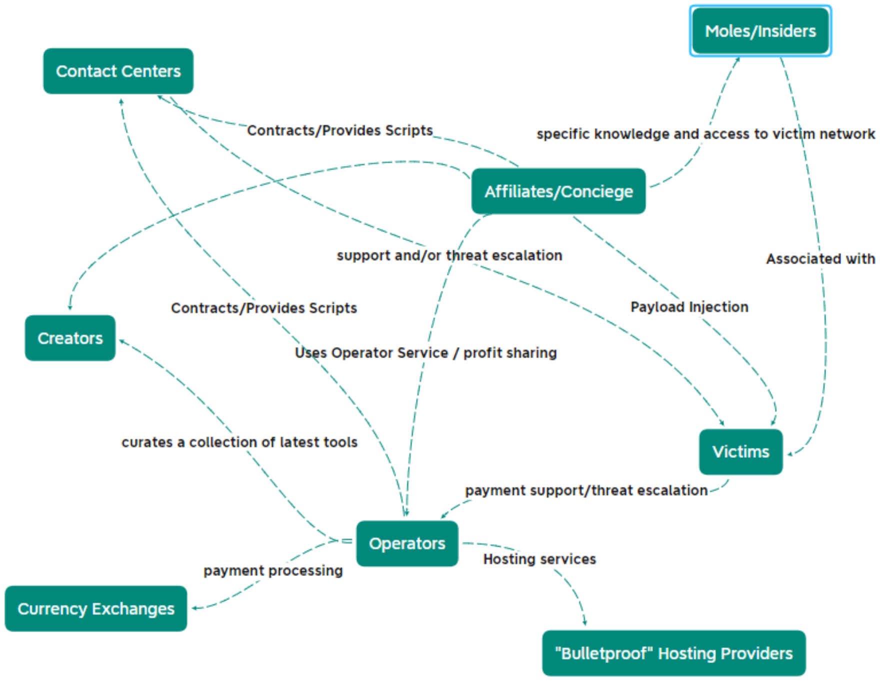
Moles/Insiders
Contact Centers
Contracts/Provides Scripts
specific knowledge and access to victim network
Affiliates/Conciege
support and/or threat escalation
Associated with
Contracts/Provides Scripts
Payload Injection
Creators
Uses Operator Service / profit sharing
curates a collection of latest tools
Victims
payment support/threat escalation
Operators
Hosting services
payment processing
Currency Exchanges
"Bulletproof" Hosting Providers

Fig. 1. Taxonomy of RaaS Labor Division

Creators: Creators are the authors of the various software tools and technologies that are used within RaaS. These include creators of exploit software and creators of software that unintendedly support such crime. An instance of this latter category includes software such as data cloning tools, pen-testing tools, encryption tools, and blockchain interface software.

Operators: Operators act as integrators that assemble various tools and create interfaces through which they enlist and interact with affiliates. Simpler forms of such interfaces include encrypted email and message boards, but more advanced forms include web portals through which affiliates can coordinate an attack directly.

Affiliates: Affiliates identify the target victim and initiate an attack. Affiliates utilize the interface provided by an operator and use specific details/knowledge of a victim. The specialized information affiliates obtain increase the chances of a successful attack.

Moles: The odds of success of a ransomware attack increase by incorporating specific knowledge and direct access to a victim system. Moles can collaborate with an affiliate or interface with an operator directly. Moles provide detailed information to assist attacks and often directly insert an exploit into victims' networks. Often, they could be disgruntled employees who bear a grudge against their employers.

Contact Centers: Contract centers serve two main functions. First, they provide support for ransomware victims to assist them in paying the ransom. Secondly, suppose a victim is not sufficiently motivated to pay a ransom to regain access to the encrypted data (i.e., they had backups or other copies of the data that they can use to recover from), in such cases, contact centers contact the victim to escalate by threatening the victim with releasing some of their data to the public. The contact centers generally use scripts provided by an operator.

'Bulletproof' Hosting Providers: With a separation between those that identify and initiate attacks from those that operate the RaaS service, a means of coordination using web-based interfaces is necessary. These sites are hosted by what is becoming known as 'bulletproof' hosting providers [12].

Currency Exchange(s): Victims of RaaS pay the ransom using various forms of cryptocurrency. Though RaaS perpetrators may 'spend' such proceeds directly via cryptocurrency, they must also exchange much of this into a local currency.

4 Discussion and Implications

Increased sophistication by cybercrime organizations is indicated by substantial functional specialization and division of labor [13]. Increased division of labor motivates increased specialization and efficiency [14], the broader distribution of responsibility and legal liability [15], new organizational forms and structures [10], and the increased capacity for RaaS groups to conduct larger and more sophisticated attacks [16]. Understanding the emerging state of such labor divisions and specialization will assist researchers and law enforcement focus on specific behaviors exhibited by specialized roles. Such understanding will help law enforcement develop preemptive 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 yet assessed the impact or change DSR stage, which will be our next goal once we refine the taxonomy and measure its utility.

6 Conclusion

Through increased specialization, RaaS is being delivered via a conglomeration of very specific and specialized participants. Our taxonomy defines the main functions that participants have, but not all configurations/organizations will achieve this level of segmentation, as often actors take on multiple roles. However, as organizational structures mature, we can expect such labor divisions to be more common. Our taxonomy introduces the emerging organizational structure and specializations that can be instantiated in any specific RaaS deployment. This is the first step in exploring a complex new phenomenon and the knowledge we provide can be beneficial to law enforcement to better differentiate the level of involvement of the various RaaS actors.

References

1. Morgan, S. *Cybercrime To Cost The World $10.5 Trillion Annually By 2025*. 2020; Available from: https://cybersecurityventures.com/hackerpocalypse-cybercrime-report-2016/.
2. Jeffery, L. and V. Ramachandran. *Why ransomware attacks are on the rise — and what can be done to stop them*. 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. *Karmen Ransomware Variant Introduced by Russian Hacker*. 2017; Available from: https://www.recordedfuture.com/karmen-ransomware-variant/.
4. Hevner, A., et al., *Design science in information systems research.* MIS Quarterly, 2004. **28**(1): p. 75-105.
5. Al-rimy, B.A.S., M.A. Maarof, and S.Z.M. Shaid, *Ransomware threat success factors, taxonomy, and countermeasures: A survey and research directions.* Computers & Security, 2018. **74**: p. 144-166.
6. Puat, H.A.M. and N.A. Abd Rahman, *Ransomware as a service and public awareness.* PalArch's Journal of Archaeology of Egypt/Egyptology, 2020. **17**(7): p. 5277-5292.
7. Simmonds, M., *How businesses can navigate the growing tide of ransomware attacks.* Computer Fraud & Security, 2017. **2017**(3): p. 9-12.
8. Southerland, M.D. and G.W. Potter, *Applying organization theory to organized crime.* Journal of Contemporary Criminal Justice, 1993. **9**(3): p. 251-267.
9. Jian, J., et al., *Organized Cyber-Racketeering: Exploring the Role of Internet Technology in Organized Cybercrime Syndicates Using a Grounded Theory Approach.* IEEE Transactions on Engineering Management, 2020.
10. Drechsler, A. and A. Hevner. *A four-cycle model of IS design science research: capturing the dynamic nature of IS artifact design*. in *Breakthroughs and Emerging Insights from Ongoing Design Science Projects: DESRIST 2016. St. John, Canada, 23-25 May*. 2016.
11. Saldaña, J., *The coding manual for qualitative researchers (2nd ed.)*. 2013, London, UK: Sage.
12. Goncharov, M., *Criminal hideouts for lease: Bulletproof hosting services.* Forward-Looking Threat Research (FTR) Team, A TrendLabsSM Research Paper, 2015. **28**.
13. Broadhurst, R., et al., *Organizations and cybercrime.* Available at SSRN 2345525, 2013.
14. Wainwright, R. and F.J. Cilluffo, *Responding to Cybercrime at Scale: Operation Avalanche--A Case Study*. 2017: JSTOR.
15. Thomas, K., et al., *Framing dependencies introduced by underground commoditization.* 2015.
16. Leukfeldt, E.R. and T.J. Holt, *Examining the social organization practices of cybercriminals in the Netherlands online and offline.* International journal of offender therapy and comparative criminology, 2020. **64**(5): p. 522-538.