L-021

Discussion about Requirements Gathering for Proposing a Forensic Ransomware Behavioral Analysis Methodology

João Ribeiro[1,2,a)] Yamaguchi Yukiko[3] Hirokazu Hasegawa[4] Hajime Shimada[3]

Abstract: The strife against the ransomware threat on the cybersecurity landscape is still a demanding and challenging endeavor for law enforcement and DFIR personnel. Border limitations, lack of resources and of international cooperation, loss of data, complexity of incidents, to name a few, are some of these challenges. In this scenario, it is vital that a proper methodology for analyzing the behavior of malware used by actors in ransomware incidents is established, with an emphasis on the software component and with the main goals of answering key forensic questions in mind - authorship and materiality, such that law enforcement agencies and the prosecution are better able to conduct investigations on the cyberspace and present cases with probative value that hold in court. This paper attempts to establish the requirements for such a methodology.

Keywords: Ransomware, Digital Forensics, Malware Analysis, Cybercrime

1. Introduction

The ransomware threat, although facing a decline in absolute number of cases in the last year [1], still remains a global menace to governments and private companies around the globe, proving to be one of the most detrimental hindrance to the integrity and to the image of institutions and businesses worldwide. Even though advances in the field of cyber security in the form of malware detection and prevention have been developed, often systems are breached and compromised, due to a multitude of factors.

When initial compromise succeeds in breaching the defenses of an information system (e.g. IDS, EDR), an incident generally follows. Private cybersecurity companies and/or law enforcement may be called upon to act, with or without technical assistance from the victim's Security Operation Center (SOC) or Digital Forensics and Incident Response (DFIR) teams. In the case of effective law enforcement response, physical and digital evidence may be collected, such as Firewall, EDR, SIEM, Active Directory solutions log files and so on. Then, personal computers and electronic devices are imaged, among many other routine procedures performed, so that all the collected data is prepared to be analyzed in an controlled, appropriate lab setting. In this context and considering the case of a ransomware incident, a thorough analysis of the piece of software associated with the more prominent aspect of the attack (the compromise of data) can be a source of valuable insight to not only understanding the dynamics of an incident itself, but also to contributing to law enforcement agencies in their ongoing fight against organized cybercrime. In this light, a proper forensic behavioral analysis could play a paramount role, by means of extracting, from the ransomware program, information that could contribute to the identification of actors and to the elucidation of the inner workings of criminal groups behind the RaaS (Ransomware as a Service) business model.

The challenges of law enforcement in the cybersecurity domain are well documented [2], [3]. From heterogeneous legal systems spanned across multiple countries, lack of international cooperation, to the inherent technological difficulties, such as the lack of established and robust methodologies for analyzing data, law enforcement operators are often unable to properly tackle the ransomware threat. In order for the investigative and prosecutorial bodies to pursue indictment and to present a case with probative value against cybercriminals, besides the usual chain of custody and thorough adherence to pertinent legal procedures, the basic legal conditions of materiality and authorship need to be established. Authorship of a crime is typically understood as the state or fact of being the author of an offense punishable by law [4]. In the cybercrime domain, this also involves the origin and means of access (physical and/or electronic), such as computer device, smartphone, network, user account information, and so on. As for materiality, it is generally understood as the proof of the existence of a crime [5]. In the digital world, this comprises the entirety of the physical and digital evidence that has some logical connection to the case at hand.

For law enforcement and prosecutorial bodies, the process of establishing (or stating the absence of) authorship and materiality in criminal case are vital to the processes of investigation and indictment. In this light, a comprehensive analysis of the software component used on a ransomware attack can directly aid actors in achieving this result, by making use of malware analysis resources, tools and techniques, leveraging Threat and Law Enforcement Intelligence, as well as Open Source Intelligence -

[1] Graduate School of Informatics, Nagoya University, Nagoya, Japan
[2] Criminalistics Institute, Civil Police of Federal District, Brasília, Brazil
[3] Information Technology Center, Nagoya University, Nagoya, Japan
[4] Center for Strategic Cyber Resilience Research and Development, National Institute of Informatics, Tokyo, Japan
[a)] assisribeiro@net.itc.nagoya-u.ac.jp

OSINT, in addition to other available resources.

Converging but differing from the usual focus of malware analysis, where the goal is prevention and detection, here the technical analysis would be aimed towards the answering of key forensic questions of materiality (i.e. what, when and how) and authorship (i.e. who) in the context of (mainly) cybercrime law enforcement. More specifically, ransomware incidents. For that, it is felt the need for a proper analysis methodology to be established.

This paper attempts to establish the requirements for such a methodology, by breaking down the key forensic concepts of authorship and materiality into points to look for and to guide the process of a behavioral forensic analysis, where its main object of scrutiny is a ransomware binary and the desired end result is a forensic report containing the sought out forensic answers. Additionally, in order for an effective analysis, the methodology should include a proper set of methods and techniques to handle and/or circumvent analysis obstacles such as the employment, by malware authors, of evasion and obfuscation techniques. Finally, as with any forensic analysis methodology, it should comply to the rigors and soundness needed for establishing probative value in court. The rest of this paper is organized as follows. The requirements for establishing ransomware forensics are discussed in Sections 2 to 4. Then, in Sections 5 and 6, considerations are made when designing a ransomware analysis methodology. Finally we conclude the paper in Section 7.

2. Authorship

In order to understand how, from a malware binary utilized or present in a case of ransomware, law enforcement actors and digital forensics professionals can obtain data that could lead to establishment of the authorship of a crime or incident, it may be helpful to think of the malicious software as the means and the *modus operandi* that attackers use to achieve the intended result of extortion and/or threat of data exfiltration.

A malicious actor in an cyber-attack setting, after going through the phases that comprise the stages of compromise, usually start acting on objective [6]. In the case of ransomware, that typically involves the deployment of a ransom binary to encrypt the victims data, while also performing data exfiltration and achieving further IT infrastructure disruption. Therefore, by analyzing a ransomware binary and looking for, among others, the presence of certain elements or references, useful information about the authorship of a ransomware incident might be obtained.

- **Networking**. IP addresses, domain names and logical ports used or referred by the malware to achieve communication with the outside world (e.g. with C2 server or a beacon);
- **Exfiltration Logistics**. Uses of, or references to, any Service Provider accounts, access tokens, or credentials utilized for hosting exfiltration services and/or exfiltrated data (e.g. MEGA.io);
- **Extortion Logistics - Communication Channels**. Uses of, or references to, any SNS or accounts utilized for enabling communication for extortion purposes between the victim and attacker, including e-mail accounts (e.g. Proton Mail);
- **Extortion Logistics - Payment Channels**. Uses of, or references to, electronic payment information or cryptocurrency wallets addresses;
- **OSINT Correlation**. Use of, or references to, identifiers or data that could be correlated with OSINT sources and to a specific actor or a ransomware group.

By determining and specifying network behavior of a ransom malware involved in an incident, law enforcement and DFIR actors can gain valuable insight into how a malware establishes and maintains connection to and from a device in a compromised network to other devices or to the global network. Although it can be argued that in many scenarios such identifying data may not be actually found at the ransom binary itself, and instead be found through analysis of other artifacts (such as application and security solutions log files) or other malicious software (such as scripts and RATs - Remote Access Tools), the analysis of the ransomware binary can be a complimentary source of information amidst an ongoing investigation or incident response.

This information can be used to gain a better understanding of how the incident took place, and serve as an addition source for requesting information about an user (suspect) from Internet Service Providers - ISP (IP address, logical port) and Application Service Providers - ASP (IP addresses, domain registration contact, etc.). The same can be said about the use or references to services, credentials, accounts or other identifying data (here defined as data can be used to identify an individual without reference to other data [7]) by malicious actors as channels for data extortion or exfiltration or as payment mediums, since they all usually have contact information associated with (despite the widespread use of anonymization and CaaS - Crime-as-a-Service - tools [8]). Furthermore, by correlating the gathered data with OSINT sources, interested actors can hopefully further augment the knowledge base of ransomware actors or groups and thus be better equipped to deal with international cybercrime.

3. Materiality

As for materiality, in order for one to, from a ransomware binary, make technical assertions of forensic value in the context of digital forensics and law enforcement, the questions to be answered are the ones aimed at clarifying and scrutinizing the inner workings of a piece of malware used as a means to perform criminal activity. In more simple terms, the questions to be answered are “What”, “How” and “When”.

- **Compromise of Data**. Determine, after deployment, installation and/or execution of the malware, if the victim’s data is made unrecoverable, unusable, or otherwise unavailable. If so, determine if a cryptographic scheme is used by the malware to achieve this result;
- **Cryptographic Scheme**. If a cryptographic scheme is employed by the malware, determine if the data is encrypted, and if so, determine the cryptographic key scheme employed and how does the malware targets (or ignores) specific files, backup copies (e.g. local or cloud, Volume Shadow Copies), as well as determine how does the malware handle file size and contents (e.g. full file encryption or header and footer encryption only);
- **Encryption Process**. If a cryptographic scheme is used by the malware to encrypt data, determine what encryption al-

gorithm is employed and its proprietariness, that is, if it employs a industry standard algorithm or a novel encryption algorithm;

- **Data Recoverability**. Determine the extent of data compromise, that is, which type of data is encrypted and assert the conditions for data recoverability (e.g. only with the attacker's private encryption key; encryption key can be found in volatile memory; data recoverable by exploring a vulnerability in the cryptographic scheme, etc.) Additionally, outline the algorithm of a decryption software (decryptor);
- **Data Exfiltration**. Determine if the malware achieves data exfiltration, and the type and content of data exfiltrated (e.g. documents, photos, text files, etc.);
- **Data Exfiltration Logistics**. If data is exfiltrated by the malware, determine how is data sent (i.e. protocols and logical ports used), and assert the rate (volume) of data exfiltration, and whether or not this exfiltration is automated or not;
- **Data Exfiltration Intelligence**. Determine if, at a given moment in time, information related to the distribution and/or selling of a victim's sensitive (exfiltrated) data can be correlated to OSINT sources (e.g online leak of data made public);
- **Threat Intelligence** Determine if the malware displays any type of behavior (e.g. life-cycle) that can be linked to a specific ransomware developer or RaaS - Ransomware as a Service group, and determine if this information can be correlated with OSINT sources;
- **Threat Logistics Intelligence**. Determine if a malware binary communicate with a Command & Control (C2) server and assert the model of communication employed (e.g. centralized, P2P, etc.) as well as the technical specifications of such communication (e.g. protocol type, logical ports, etc.);
- **Indicators of Compromise Assessment**. Determine if the malware make changes to the operating system to render it resources unrecoverable, unusable, or otherwise unavailable (e.g. the malware stop user applications and intercepts network traffic). Determine if the malware makes changes to the underlying system to achieve persistence;
- **Target specificness**. Determine if the malware target specific computer architectures (e.g. bare metal, vitalized) or specific Operating Systems. If, so assert whether this information may be used to infer the specificness of the attack (i.e. can it be inferred, from the malware, behavior information indicating that it was designed for an specific combination of target and its infrastructure, with or without the use of privileged or undisclosed information).

By better understanding the behavioral aspect (*modus operandi*) of a ransomware program involved in cyber incidents, interested actors are better equipped to identify trends in malware development designed for criminal activity and hopefully increment the cyber crime knowledge base comprised of actors and groups in the RaaS ecosystem. As for the assessment of data recoverability, it can serve as tool for estimating the extent of the damage done to the digital assets of an individual, company or government body, while still providing an assessment that could be relevant in civil (common law) repercussions as well (e.g. data protection cases).

As for threat intelligence and the assessment of data exfiltration and its logistics, along with its correlation with OSINT sources, they can contribute to a deeper understanding of the *modus operandi* of malicious actors from an external (outside-in) perspective, specially with the use of alternative protocols for data exfiltration and novel, stealthier techniques [9]. The same can be said about the assessment of other behavioral aspects of the ransomware such as indicators of compromise and target specificness, as these can provide an insight at how the incident carried out from within the network and IT infrastructure of a victim. This is specially relevant considering the rise of Living-Off-The-Land techniques [10].

4. Implied requirements

As malware authors typically utilize a series of detection and evasion techniques in their malicious programs to hinder analysis difficult or inconvenient for the analyst, it is paramount that a proper analysis methodology is able to effectively circumvent those obstacles in the most forensically sound way possible. For dealing anti-analysis, anti-forensics, anti-reverse engineering techniques, code obfuscation, *packing*, and so on, countermeasures would need to be applied in order to further the scrutiny of the malicious software, as analysis is typically done in virtualized environments for security and convenience reasons. In this light, the implications of using anti-anti-analysis countermeasures such as function hooking/patching, user activity simulation (i.e. for dealing with UI-based evasion techniques), memory manipulation, network emulation and so on should be discussed and properly assessed. The driving force for the use of these techniques, beyond the main goals of answering the key forensic questions of authorship and materiality in the context of DFIR and law enforcement is to facilitate the analysis process in a non detrimental manner.

As such, an attempt at presenting a non-exhaustive list of some of the possible obstacles that would need to be circumvented in the analysis process are presented as follows.

- **Packing**. Determine if the malware (plain binary executable) is *packed*, and perform the necessary steps of unpacking, (e.g decryption, decoding) such that the malware can properly (statically) analyzed;
- **Obfuscation**. Consider and perform, in the most forensically sound manner possible, the use of deobfuscation techniques to handle obfuscation transformations [11] employed by a malware developer that (potentially) hold forensic value.
- **Anti-analysis and evasion**. Consider and perform, in the most forensically sound manner possible, the use of anti-anti-analysis and anti-evasion countermeasures to facilitate or enable analysis that would be otherwise unattainable.

5. A Methodology for Forensic Ransomware Behavioral Analysis Methodology

Given the goals of answering in a satisfactorily manner the previously established goals and requirements, the authors propose the development of a methodology for forensic ransomware behavioral analysis, where the main applicable scenario would be in the context of ongoing cybercrime investigations and law en-

forcement operations, but also pertinent to Digital Forensic and Incident Response scenarios involving ransomware incidents.

The object of analysis of the methodology is a malware binary executable collected in a law enforcement or DFIR case and associated with a ransomware incident, along with any correlated files such as encrypted documents, ransom notes, and so on. In the case of a lack of a binary sample (due, for an example, anti-analysis techniques employed by the malware in the victim's digital infrastructure), disk images, volatile memory dumps and other auxiliary media may be used, granted that a proper assessment and consideration of the limitations of the results is made.

The end result of the methodology would be a forensic report focused on shedding light into the behavioral aspect of a ransomware program and in explaining both how it achieves the results, in a technical way, intended by its author (or attacker) and also offering invaluable insight into its author (or attacker). This information, the authors believe, would be helpful for law enforcement and prosecutorial bodies fighting cybercrime.

Although the current initial formulation of the requirements gathering is intended to cover some of the most prominent aspects of malware behavior concerning forensic and legal implications in the context of law enforcement and incident response, the authors recognize that they are not exhaustive, and serve as baseline to aid cybercrime investigations and prosecutorial activities. The correlation of data obtained and compiled can also be a source of valuable information for Global Threat Intelligence and can help IT and Cybersecurity professionals to get a better grasp of their adversaries in the cyberspace.

Considering that a substantial amount of malware [12] typically employs packing as an initial anti-analysis artifice, the authors feel that research guided towards the problem of packed ransomware mentioned in the previous section is a promising candidate and starting point for future research work. More specifically, the goal is to establish a methodology for dealing with packed ransomware that, using an heuristic approach, tries to: 1) identify the type of packing used; 2) set a proper boundary between the unpacking stub and the original code; 3) Obtain a working (unpacked) sample suitable for static analysis.

6. Additional Considerations

Given the initial outline and rationale of the proposed methodology presented, it is felt that a few technical considerations about the object, environment and the presentation of the results of the methodology are due.

- **Object of Analysis - Sensitiveness of Data**. Due to the nature of the proposed usage scenario and applicability, no malware samples or compromised files may be submitted to any online malware analysis or sandbox environments, for the obvious risk of exposing sensitive data about a victim of an incident (e.g credential and password information);
- **Analysis Environment**. Considering the physical and technical limitations of dealing with multiple incident scenarios, and although the desirability of performing analysis on computer systems and environments that are as close as possible to real world scenarios is undeniable, the criterion of choice for the analysis environment setup (e.g. OS, virtualization scheme), is mainly that of security and feasibility of analysis;
- **Analysis Toolset**. The criterion of choice for the programs and tools used for performing analysis would be mainly focused on the quality and the promptness of the desired results. Whenever viable and not detrimental to the promptness of analysis, open source or free tools are preferred.
- **Results**. The methodology shall present its results in a clear and coherent manner, such that the acquired information is intelligible and discernible without disregard for technical correctness.

7. Conclusion

In this study, We propose a gathering of requirements for the development of a forensic behavioral ransomware analysis methodology to be used mainly in law enforcement and DFIR scenarios involving ransomware cases, where answers to the forensic questions of authorship and materiality are actively sought by cybercrime investigation and prosecutorial bodies, as well as by interested cybersecurity professionals.

In the proposed approach, an analysis methodology constituted of the gathered requirements could yield information that could aid interested actors in establishing authorship by considering key aspects such as networking, exfiltration and extortion logistics with regards to use or reference to identifying data that can be requested, by law enforcement authorities, to ISPs and ASPs. There is also the need for consideration of forensic implications, given the proposed usage case scenario as shown in past sections.

Finally, additional considerations about the object, methods and the results of the proposed methodology were made, while implementation and evaluation decisions building such a methodology are left out as future work. At the same time, a study on the unpacking of ransomware samples in the proposed analysis outline is suggested for upcoming, prospective research.

References

[1] SonicWall: 2023 SonicWall Cyber Threat Report (2023).

[2] Arifi, D.et al.: Cybercrime: A Challenge to Law Enforcement, *SEEU Review*, Vol. 15, No. 2, pp. 42–55 (2020).

[3] Reyes, A. et al.: *Cyber crime investigations: Bridging the gaps between security professionals, law enforcement, and prosecutors*, Elsevier (2011).

[4] Sales, S. J. S.: *Dos tipos plurissubjetivos*, Del Rey (1996).

[5] Rodrigues, C. V. et al.: Perícia criminal: uma abordagem de serviços, *Gestão & Produção*, Vol. 17, pp. 843–857 (2010).

[6] Yadav, T.et al.: Technical aspects of cyber kill chain, *Security in Computing and Communications: Third International Symposium, SSCC 2015, Kochi, India, August 10-13, 2015. Proceedings 3*, Springer, pp. 438–452 (2015).

[7] Insider, L.: Identifying Data definition (2023).

[8] Wainwright, R.et al.: *Responding to Cybercrime at Scale: Operation Avalanche–A Case Study*, JSTOR (2017).

[9] Mitre: Exfiltration over Alternative Protocol (2023).

[10] Barr-Smith, F. et al.: Survivalism: Systematic analysis of windows malware living-off-the-land, *2021 IEEE Symposium on Security and Privacy (SP)*, IEEE, pp. 1557–1574 (2021).

[11] Xu, H. et al.: Layered obfuscation: a taxonomy of software obfuscation techniques for layered security, *Cybersecurity*, Vol. 3, No. 1, pp. 1–18 (2020).

[12] Muralidharan, T. et al.: File Packing from the Malware Perspective: Techniques, Analysis Approaches, and Directions for Enhancements, *ACM Computing Surveys*, Vol. 55, No. 5, pp. 1–45 (2022).