An Empirical Study of Ransomware Vulnerabilities Descriptions

Claudia Lanza, Abdelkader Lahmadi, Fabian Osmond

An Empirical Study of Ransomware Vulnerabilities Descriptions

Claudia Lanza[1], Abdelkader Lahmadi[2] and Fabian Osmond[3]
[1]*Università della Calabria, Italy*
[2]*Université de Lorraine, CNRS, Inria, LORIA, 54000 Nancy, France*
[3]*Cybi SAS, 54600 Villers-Lès-Nancy, France*
claudia.lanza@unical.it, lahmadi@loria.fr, fabian.osmond@cybi.fr

Keywords: Threat Analysis, Ransomware, Vulnerabilities, Security Knowledge Management.

Abstract: Cyber threat awareness requires the building of an accurate knowledge and analysis of the vulnerabilities used by the attackers and their respective attack toolkits. Ransomware are today one of the most significant threats faced by information systems and their number continues to grow. They are a type of malware targeting the information system by locking its equipment and users data and claiming a ransom for its release. They have been becoming more and more sophisticated and mainly relying on software vulnerabilities to access and lock the system data. In this paper we have carried out an empirical analysis of the Common Vulnerabilities Enumeration (CVE) exploited by known ransomware using a semantic annotation technique in order to create the condition from which to start to build a knowledge base of ransomware behaving processes. The main focus of this paper is towards the way vulnerabilities are commonly exploited by ransomware, their sharing ratio and the definition of their common causes and impacts. We have built a database, by scrapping multiple publicly available security reports, which associates each known ransomware to its used vulnerability contained in the CVE. We have applied a semantic annotation methodology which encompasses a semantic analysis of the CVE dataset through a pattern recognition process. This latter has enabled the extraction for each CVE of its key features, i.e., the cause, the performed exploit action and effect, as well as its impact. In the resulting collected and extracted knowledge we show a twofold analysis, statistical and semantic, of the CVE descriptions and their extracted features.

1 INTRODUCTION

Ransomware are considered as a major threat faced by information systems and their users (Oz et al., 2022). They are a subset of malware targeting these systems to lock or deny access to their data while requesting a ransom payment to release them. The number of ransomware continues to grow, the MS-ISAC in USA observed a 74% increase in year-over-year reported incidents from Q1-Q2 2022 to Q1-Q2 2023 (Multi-State Information Sharing and Analysis Center, 2023). Besides, a total of 449 million dollar has been at least extorted in 2023 by ransomware groups according to the firm Chainalysis (Chainalysis, 2023). The attack phases of a ransomware usually rely on phishing and malvertising as initial access vector, followed by exploiting service vulnerabilities for deployment, privilege escalation and lateral movements until the step of data exfiltration and ransom payment request. This operational model is studied by a large body of works in the literature while focusing on a specific or a subset of known ransomware (Oz et al., 2022). These existing studies are mainly carried on the binary code of ransomware by using static or dynamic analysis to discover their tactics, techniques and procedures (Maigida et al., 2019; Chen and Bridges, 2017).

However, no study exists in the literature that covers a comprehensive analysis of the CVEs exploited by ransomware to clearly identify a better understanding of these key characteristics in their infection and propagation operations. We believe that this missing study is important to build proactive defense solutions and provide guidelines for fixing vulnerabilities that may be exploited by a ransomware.

This paper aims to study the vulnerabilities exploited by known ransomware using their respective textual descriptions provided in the CVE standard published by the MITRE organism. This study pro-

Authors equally contributed to this work, however Claudia Lanza specifically dealt with section , 3.2, 4.2 and 5, Abdelkader Lahmadi with section 1, 2, 3.3 and 4.1., and Fabian Osmond with section 3.1

vides a better understanding of these vulnerabilities regarding their CVSS scoring, their distribution over years and how they are shared by ransomware. Besides, we made a semantic analysis of these descriptions regarding their key features including causes, actions, effects and impacts. We defined these key features to be extracted from each CVE description using a semantic pattern-based configuration.

To the best of our knowledge this is the first paper that makes an analysis of vulnerabilities used by ransomware. The main contributions of our paper are summarized as follows: (i) known ransomware vulnerabilities (CVE) dataset construction from which we have compiled a corpus containing their vulnerabilities descriptions; (ii) proposal of a semantic analysis methodology for extracting from each vulnerability description its key features by using a semantic annotation process; (iii) statistical and semantic analysis of these CVEs to provide a more accurate knowledge on their usage and sharing between ransomware. The purpose is to identify the major causes and impacts ransomware generate while exploiting certain vulnerabilities included in CVE.

The remainder of this paper is structured as follows. We begin with the related works in Section 2. Successively, we present and detail our analysis methodology of the collected CVE exploited by ransomware in Section 3. The results of the analysis are provided in Section 4. Finally, we draw conclusions in Section 5.

2 RELATED WORKS

In this section we provide some representative works related to ransomware analysis and their associated methods. A large body of studies exists in the literature addressing ransomware analysis by using mainly static and dynamic techniques (Oz et al., 2022; Beaman et al., 2021) to understand their components and behaviours. The static analysis techniques rely on available data collected from ransomware samples to identify their patterns (Hsiao and Kao, 2018). The dynamic analysis techniques rely on the execution of ransomware in sandboxes or controlled environments to identify their processes action (Monika et al., 2016; Or-Meir et al., 2019). Both techniques are used to build ransomware detection signatures from the identified behaviours including the accessed files, sequences bytes, the running processes, the contacted servers, etc. The two techniques can be also used jointly to better characterize the behaviour of a ransomware and build more accurate detection signatures (Pranshu Bajpai, 2020). However, these techniques and their numerous existing studies are focusing on the analysis of the behaviour of a ransomware using collected samples. They have not studied a global behaviour of ransomware by analysing their exploited vulnerabilities, as we address in this work.

There are few studies which analysed the behaviour of ransomware using threat models of attack phases (Tatam et al., 2021; Dargahi et al., 2019) to classify them. In (Tatam et al., 2021) the authors identified four main threat modelling approaches including asset-centric, system-centric, threat-centric and data-centric approaches to analyse the security vulnerabilities and risks of a host, an application and a network service. They identified different techniques that can be used for building such models including graphical and formal approaches, such as, ATT@CK, Kill Chain, CAPEC, etc. In (Dargahi et al., 2019) the authors propose to rely on the Cyber Kill Chain (CKC) model to align ransomware features. Their goal is to provide a fine-grained information about each attack step carried out by a ransomware regarding this model. In their study they mainly identified some common features of known ransomware and they mapped them on the attack techniques for each step in the Kill Chain. Although, their approach provides a better analysis and a taxonomy of ransomware compared to existing works, they have not studied features related to the exploited vulnerabilities. In (Bajpai and Enbody, 2023) the authors propose a more adapted Kill Chain for ransomware to better represent ransomware activity. For instance, they show that Installation and C2 phases are not a necessary part of ransomware activity. They relied on an extensive review of state-of-the-art incident report and their own experience to develop the analysis and response framework. In (Mirza et al., 2021) the authors also propose to rely on the Kill Chain model to analyse ransomware. They mainly analysed four ransomware strains which are *Petya, Mamba, Cerber* and *WannaCry* to extract from them common and unique features for their early stage detection. They primarily show that the unique features are mainly the vulnerabilities that they exploit and the common features are related to the propagation and covert steps within a single machine or over the network. Our work is in line with this methodology by making a more thorough and in-depth analysis of exploited vulnerabilities by ransomware to verify those that are common and unique for each of them.

Only few works have studied the vulnerabilities in terms of CVE standard exploited by malware. In (Acar et al., 2019) the authors partially analysed the CVE exploited by a subset of 158 malware samples. They mainly relied on CVE labels associated to mal-

ware from Microsoft and Kaspersky sources. They observed that 158 samples use at least one vulnerability with CVE and noted some discrepancy between the labels from the two sources. In their work they found that attackers tend to rely on recent exploits and new CVEs and many malware appear only few days after the release of some CVE. Several other works have also studied the ransomware individually by analysing their respective exploited CVE (Kerns et al., 2022; Lim et al., 2023; Aljaidi et al., 2022).

In (Lim et al., 2023) the authors analysed the available CVE records and they made statistical analysis of them regarding their existing metrics (CVSS, access, complexity, affected products) and types. During their study they highlighted the CVE related to ransomware and found that most of them have a high CVSS score and the most common types are those of *Execute Code*. Their conclusions are close to our findings in this work, but we show more complete results regarding the types of CVE used by ransomware and how they are shared between them.

3 METHODOLOGY

In this section we detail our methodology regarding the construction of the vulnerabilities corpus by collecting their usage by ransomware through the consultation of multiple security reports. Subsequently, we present the key features extraction process from the textual descriptions included in the CVEs by using a semantic annotation process.

3.1 Corpus Construction

At first we have created a dataset containing a list of known ransomware and their associated exploited CVEs. The dataset has been built manually by taking into account the reliability of the sources (Zagrebelsky, 1984), in our specific case those spreading information about the ransomware activities. In detail, the corpus has been compiled by checking security reports and news publicly available on the main cybersecurity portals, as the Community Emergency Response Team (CERT) [1], The European Union Agency for Cybersecurity (ENISA) [2] or the Agence nationale de la sécurité des systèmes d'informationANSSI (ANSSI) [3]. The different security and cyber threat intelligence related information sources we consulted are represented in Table 1.

CVEs associated to each ransomware by using multiple sources have been validated by domain experts in the field of cybersecurity in order to verify the reliability of the mapped data. Our dataset contains a total number of **161 ransomware** which have been detected in a time-span going from **2007 to 2023.**

Using this dataset, with the purpose of manually creating a training set as first step to support the next machine learning operations, we selected a subset of 95 representative ransomware according to the sampling presented in Table 2 and built from that a text corpus of their respective CVEs. We used this corpus for manually annotating the CVEs descriptions mapped with given ransomware and extract from them key features of each vulnerability regarding the *causes*, *impacts*, *exploit actions* and *effects*.

3.2 Semantic Annotation

The annotation takes its ground from the typical development observed during a cyber threat, in our specific case a ransomware. In detail, it usually takes advantage from a *vulnerability*, it has a certain likelihood to be exploited and a condition by which is propagated in a given platform, it bears a given *impact* and behaves in a way - *action* - that leads to some *effects*. This ransomware-attack-behaviour chain has been formalized using the annotation tool Prodigy[4], an active learning system that works by using SpaCy language libraries to perform the syntactic tagging tasks. Indeed, through Prodigy users can attribute to each of the properties detected in source corpora a specific tag. The perspective has targeted to creation of a group of patterns meant to be generalized over a large set of data to infer knowledge about the ransomware information once having to deal with new upcoming vulnerabilities.

Patterns represent the morphosyntactic construction through which a sentence is texturally analysed in its parts. Training a model though patterns allows to formalize a set of rules to be applied on a source documentation and automatically systematize the knowledge domain towards the use of the data within a semantic framework. (Condamines, 2008) deals with the recurrent lexicon characterizing the level of linguistic variation within given specialized frameworks. Indeed, the retrieval process regarding the isolation of some fixed expressions, i.e., patterns, according to the author, results a simpler task when addressing fields of knowledge marked by a highly technical way of sharing textual information. The specificity proper to sector-oriented documentation enhances the identification of recurrent semantic structures because of the

[1] https://community.fema.gov/PreparednessCommunity/s/welcome-to-cert?language=en_US

[2] https://www.enisa.europa.eu/

[3] https://www.ssi.gouv.fr/

[4] https://prodi.gy/

Table 1: Information sources used for building our source corpus.

Type	**Information sources**
Cyber Security organisation reports	reports from CERT, ENISA, ANSSI, CISA, etc.
Cyber security forums	KrebsOnSecurity, BleepingComputer, etc.
Specialized cyber security web sites	Threatpost, DarkReading, Hackread, TheHackerNews
Cyber security bulletins	Security alert reports by software and hardware providers
Reports from cyber security companies	Symantec, MacAfee, Kaspersky Lab, et CrowdStrike
Community forums on cyber security	Reddit: */r/netsec*, */r/ransomware*

Table 2: The selected sample corpus of ransomware.

Year	Number of Ransomware	Number of CVEs	Ransomware status
2007	1	2	oldest
2010	13	383	oldest
2012	6	97	oldest
2015	9	120	old
2017	18	105	old
2019	28	62	old
2021	25	98	current
2023	5	9	new

lexical fixity. The pattern-based configuration to be applied onto specialized corpora can support the development of an entangled network of semantic relationships (Roesiger et al., 2016) which, in turn, can facilitate the automatic creation of knowledge organization systems, such as ontologies or thesauri (Lanza, 2022). (Auger and Barrière, 2008) offer an extended overview of some of the main existing works published on this subject addressing the patterns as supporting structures which interrelate two entities linked together by a semantic relation, as well as (Fortunee, 2021) presenting a set of tools and techniques employed in the literature for annotation tasks. (Meyer, 2001) states that these semantic recurrent chains are constituted by a *"linguistic and paralinguistic elements that follow a certain syntactic order, and that permit to extract some conclusions about the meaning they express."* (2001:237).

The tags (see Figure 1) for our specialized corpus made of CVEs descriptions have been established as follows:

- **Cause:** usually associated to the vulnerability that allows an attack, e.g, "buffer overflow", "use after free", "integer overflow" or "mishandles negative offsets during decoding";
- **Impact:** how the attack, e.g., "code execution", "denial of service" or "obtain privilege rights" is impacting certain infrastructures;
- **Action:** the expression of the attack, how it has been executed, e.g., "crafted web site", "crafted tiff image", or "sending a handcrafted message";
- **Effect:** the consequences of the attack, e.g., "overrides a valueof function" or "triggers access to a deleted object".

In particular, our methodology is based on the assumption that the sentences under analysis with the

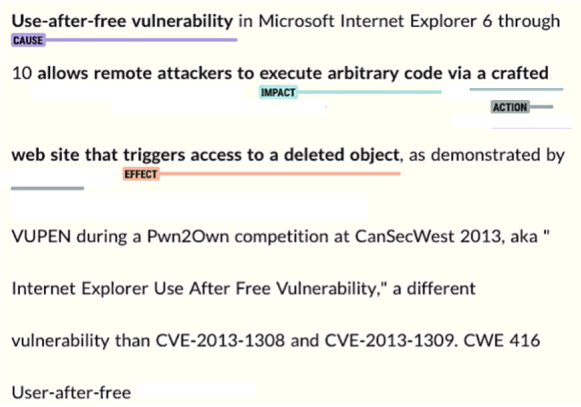

Figure 1: Named entities annotated in CVEs' descriptions.

annotation tool have to follow a fixed schema. This latter represents the pattern configuration for the *cause*, *impact*, *action* and *effect* tags in order to train a model to be run over a larger number of CVEs' descriptions and automatically detect the information needed for the knowledge organization system development. The fixed schema has implied certain trigger morphosyntactic units which have represented the key elements to isolate and recognize the desired information meant to be formalized in the next tags. In this way the data, within the CVEs' descriptions, which were not compliant with the chain rules have been discarded. The chain contains both the main tags included in the training set and the patterns to identify them to train the model. Its structure is depicted in Figure 2.

In the case of this research activity's abovementioned tags the patterns have followed this construction:

- **CausePattern:** e.g., LEMMA (buffer) + LEMMA (overflow) | ADJ (unspecified) + LEMMA (vulnerability) | VERB (infinitive: due) + PREP (to) + NOUN;
- **ImpactPattern:** e.g., PREP (to) + V (execute | perform) + ADJ (arbitrary) NOUN (code);
- **ActionPatter:** e.g., LEMMA (via) + PREP (a) + NOUN | + VERB (gerund: involving) + ADJ (crafted) + NOUN (JavaScript) + NOUN;
- **EffectPattern:** e.g., PRON (that| which) + V (lead | leverage)+ PREP (to) + NOUN

Figure 2: Patterns schema.

3.3 Normalization

Once having extracted a set of annotation labels of different features, we applied a normalization process to replace labels with their respective semantic equivalent expressions. For instance, extracted features, such as *arbitrary code execution* and *code execution* result semantically equivalent. In this process we used a transformer based neural network to compute similarities between each pairs of extracted features.

4 RESULTS

We analysed the set of ransomware-vulnerabilities to identify their semantic links with respect to the extracted labels. We also performed a statistical analysis of these vulnerabilities regarding their usage and sharing between ransomware.

4.1 Statistical Analysis

We firstly analysed the distribution of the severity of the exploited vulnerabilities by ransomware regarding their Common Vulnerability Scoring System (CVSS) score. The objective of this analysis is to study the scoring levels of these vulnerabilities to better understand whether ransomware are only relying on high score CVSS vulnerabilities. Figure 3 depicts for each CVSS score range the percentage of vulnerabilities. We mainly have observed that about 45% of vulnerabilities have a CVSS score greater or equal than 9 with half of them with a score equal to 10. About 28% of vulnerabilities have a score less than 7. These low score vulnerabilities are usually not fixed or have low fix priority. Hence, our study confirms that CVSS score is a inefficient prioritization approach for fixing vulnerabilities since ransomware may exploit those with low scores.

Secondly, we have analysed the distribution of the number of vulnerabilities exploited by each ransomware. As depicted in Figure 4, we have observed that about 30% of ransomware are using a single vulnerability. The majority of ransomware, nearly 79% of them, are exploiting less than 10 vulnerabilities. Only a single ransomware, i.e., *CK*, is exploiting a high number of vulnerabilities of 79. The reason

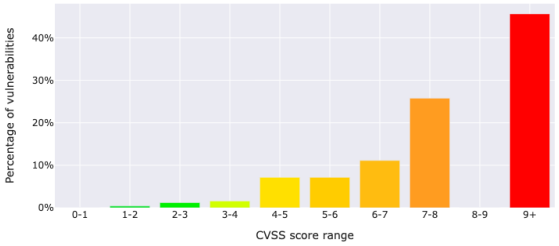

Figure 3: Distribution of ransomware exploited vulnerabilities by CVSS score range.

is that *CK* is an exploit kit used by multiple ransomware. Other ransomware, such as, *CRY*, *CHINA LEAK*, *TESLACRYPT*, *RUSSIA LEAK* are also exploiting high number of vulnerabilities of 60, 49 and 32 respectively.

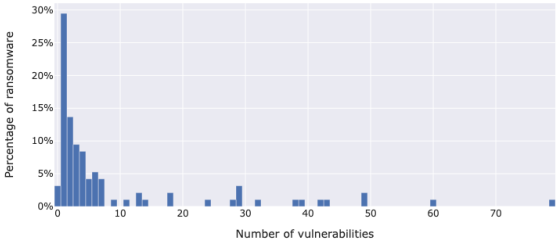

Figure 4: Distribution of the number of vulnerabilities exploited by ransomware.

We have analysed then the number of ransomware exploiting each vulnerability (CVE) to identify the most exploited vulnerabilities. Figure 5 shows the distribution of CVEs by the number of their respective ransomware. We have observed that the most exploited vulnerabilities are *CVE-2015-7645* and *CVE-2015-5119* associated with 15 ransomware. These two vulnerabilities affect Adobe Flash Player and allow attacker to remotely execute arbitrary code.

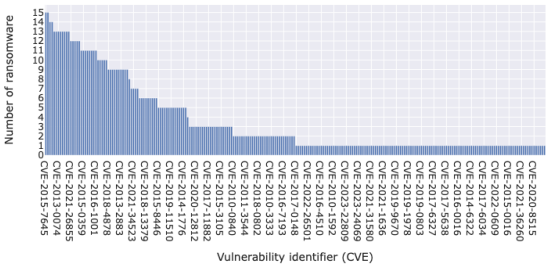

Figure 5: Distribution of CVEs by the number of ransomware exploiting each of them.

The count of the vulnerabilities by their respective number of ransomware exploiting them is depicted in Figure 6. We have observed that around 120 vulnerabilities, which represents about 50% of the total number of vulnerabilities, are exploited, each of them by a single ransomware. Only the aforementioned 2 vulnerabilities are exploited by a high number of ransomware, 15. We have found that the majority of ransomware are using their own specific vulnerabilities and few vulnerabilities are exploited by many ransomware.

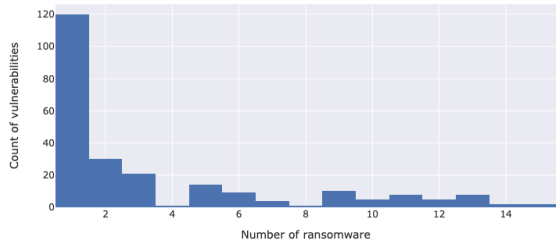

Figure 6: Count of vulnerabilities by their respective number of ransomware.

Figure 7 depicts the sharing ratio of vulnerabilities by their respective number of ransomware. This ratio is computed using the count of vulnerabilities shared between the ransomware. For instance, the *CK* ransomware is sharing 77 vulnerabilities with the others. We have observed that 14 ransomware have a sharing ratio of 0, i.e., they don't share any others' vulnerability. 31 ransomware are sharing a single vulnerability with the others.

Figure 7: Sharing ratio of ransomware vulnerabilities.

4.2 Semantic Analysis

From a semantic point of view the annotation process over the ransomware behaving chains show interesting results in terms of common retrieved causes, impacts, actions and effects between certain vulnerabilities and ransomware.

In a first analysis step, we have built the co-occurence matrix between extracted causes and impacts for exploited CVEs. Figure 8 shows a partial view of this matrix with the highest co-occurence values. We have mainly observed that the impact label *execute code* has a high co-occurence with *double free*, *buffer overflow*, *heap overflow* and *integer overflow* labels, which are known to be the major causes of arbitrary code execution. Also, the label *unspecified vulnerability* has high occurrence values with the impact labels *denial of service, execute code, affect confidentiality*. However, in such descriptions the vulnerability causes remain unknown or not publicly available to avoid exploitation when disclosing the associated CVEs.

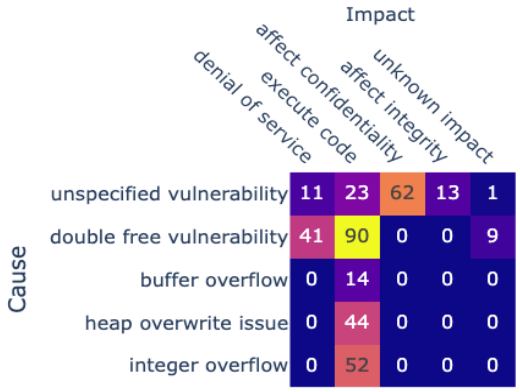

Figure 8: Co-occurence matrix of extracted cause and impact features.

By exploiting the semantic annotations executed through Prodigy we carried out the analysis by building a semantic graph with Gephi (Bastian et al., 2009). The study of the semantic relations relied on the node degrees of the *cause* and *impact* labels, hereby reported as the ones expressing the highest sharing ratio between ransomware and CVE, respectively depicted in Figures 9 and 10. We have observed that both of them have globally low degree distribution with 16 *cause* nodes and 23 *impact* nodes with a degree value of 1. Only *double free - cause* has a node degree of 22 and *affect confidentiality - impact* has a node degree of 15. Therefore, we can deduce that both of them are the common semantic labels of the analysed ransomware CVEs.

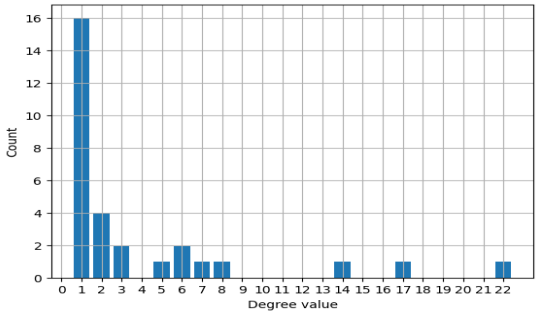

Figure 9: Distribution of the *cause* node degrees in the semantic graph.

Table 3: Communities detected and the associated ransomware.

Community	(%)	Ransomware
1	23,48 %	CRY, REVETON, TESLACRYPT,LOCKY, CERBER...
2	16,29 %	MICROSOFT-WORD-INTRUDER, DOTKACHEF, MAZE, ANCALOG...
3	15,91 %	IRAN LEAK, LAPSUS$, NEBULA, DARKSIDE, NIGHT SKY...
4	12,88 %	CK, PETYA, WHITEHOLE BLACKBYTE, SUNCRYPT...
5	10,61 %	RUSSIA LEAK, SODINOKIBI, WANNACRY, BLACK KINGDOM, SEKHMET...
6	9,47 %	NORTH KOREA LEAK, HOLYGHOST, DOPPELPAYMER, CHEERSCRYPT, AKO...
7	4,92 %	ALPHV, CHAOS, AVOSLOCKER, ASN.1, and HELLOKITTY
8	2,27%	UEFI

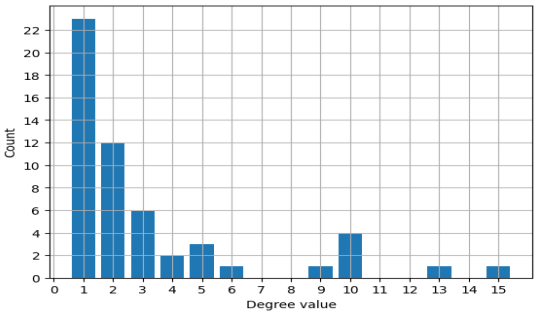

Figure 10: Distribution of the *impact* node degrees in the semantic graph.

We have also applied the community detection algorithm available in Gephi over the semantic graph to identify the number of communities. The communities detected have been 14 (see Figure 11), in Table 3 we report the first most consistent ones with the main (i.e., with the highest weighted degree score) corresponding aggregation of ransomware.

The information retrieval of the most common *causes*, *impacts*, *actions* and *effects* associated to ransomware exploiting certain vulnerabilities are outlined in a excerpt of semantic annotation mapped data, namely the connections semantically detected in *NEBULA* (see Figure 12) ransomware with the established main tags of our annotation process.

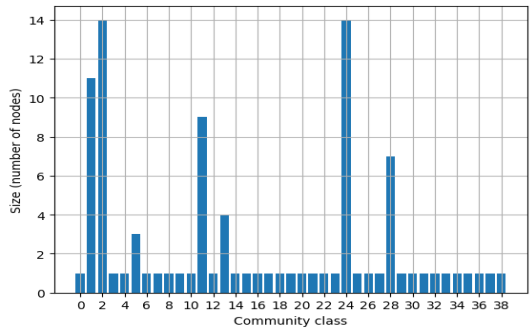

Figure 11: Ransomware communities detected from the semantic graph and the associated size.

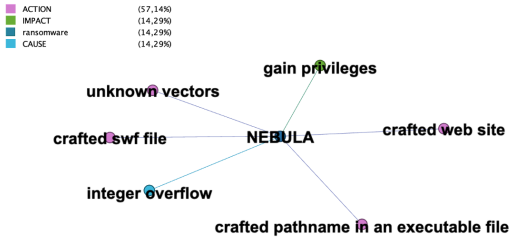

Figure 12: Connections detected in the annotated texts between the NEBULA *ransomware* and the *impacts*, *causes* and *actions*.

5 CONCLUSION

In this paper we provided a comprehensive analysis of vulnerabilities defined in the CVE standard and exploited by known ransomware by using our own dataset collected from different publicly available sources. We mainly provided statistical and semantic analysis of these CVEs to show their association to the main attack patterns executed by given ransomware in a predefined time-span. We have observed that ransomware do not only exploit high CVSS score CVEs, but also many of them rely on low score vulnerabilities. Besides, the sharing ratio of CVEs between ransomware is not high and many of them they are using unique CVEs. For future works we plan to extend our dataset with tactics, techniques and procedures (TTP) features for each CVE exploited by a ransomare to better characterize and classify them.

ACKNOWLEDGEMENTS

This study has been realized thanks to the co-financing by European Union - FSE REACT-EU, PON Ricerca e Innovazione 2014-2020.

REFERENCES

Acar, A., Lu, L., Uluagac, A. S., and Kirda, E. (2019). An analysis of malware trends in enterprise networks. In *Information Security*, pages 360–380.

Aljaidi, M., Alsarhan, A., Samara, G., Alazaidah, R., Almatarneh, S., Khalid, M., and Al-Gumaei, Y. A. (2022). Nhs wannacry ransomware attack: Technical explanation of the vulnerability, exploitation, and countermeasures. In *EICEEAI*, pages 1–6.

Auger, A. and Barrière, C. (2008). Pattern-based approaches to semantic relation extraction: A state-of-the-art. *Terminology*, 14:1–19.

Bajpai, P. and Enbody, R. (2023). Know thy ransomware response: A detailed framework for devising effective ransomware response strategies. *Digital Threats*, 4(4).

Bastian, M., Heymann, S., and Jacomy, M. (2009). Gephi: An open source software for exploring and manipulating networks.

Beaman, C., Barkworth, A., Akande, T. D., Hakak, S., and Khan, M. K. (2021). Ransomware: Recent advances, analysis, challenges and future research directions. *Comput. Secur.*, 111(C).

Chainalysis (2023). Update: Crime down 65% overall, but ransomware headed for huge year thanks to return of big game hunting. https://www.chainalysis.com/blog/crypto-crime-midyear-2023-update-ransomware-scams/. Accessed: 2023-10-22.

Chen, Q. and Bridges, R. A. (2017). Automated behavioral analysis of malware: A case study of wannacry ransomware. In *16th IEEE ICMLA*, pages 454–460.

Condamines, A. (2008). Taking genre into account when analyzing conceptual relation patterns. *Corpora*, 3.

Dargahi, T., Dehghantanha, A., Bahrami, P. N., Conti, M., Bianchi, G., and Benedetto, L. (2019). A cyber-kill-chain based taxonomy of crypto-ransomware features. *Journal of Computer Virology and Hacking Techniques*, 15(4):277–305.

Fortunee, M. (2021). *Comparative Study Of Annotation Tools And Techniques*. PhD thesis, Afribary.

Hsiao, S.-C. and Kao, D.-Y. (2018). The static analysis of wannacry ransomware. In *20th ICACT*, pages 153–158.

Kerns, Q., Payne, B., and Abegaz, T. (2022). Double-extortion ransomware: A technical analysis of maze ransomware. In *Proceedings of FTC*, pages 82–94.

Lanza, C. (2022). *Semantic Control for the Cybersecurity Domain: Investigation on the Representativeness of a Domain-Specific Terminology Referring to Lexical Variation*. CRC Press.

Lim, J., Lau, Y. L., Ming Chan, L. K., Tristan Paul Goo, J. M., Zhang, H., Zhang, Z., and Guo, H. (2023). Cve records of known exploited vulnerabilities. In *8th ICCCS*, pages 738–743.

Maigida, A. M., Abdulhamid, S. M., Olalere, M., Alhassan, J. K., Chiroma, H., and Dada, E. G. (2019). Systematic literature review and metadata analysis of ransomware attacks and detection mechanisms. *Journal of Reliable Intelligent Environments*, 5(2):67–89.

Meyer, I. (2001). Extracting knowledge-rich contexts for terminography: A conceptual and methodological framework. In *Recent Advances in Computational Terminology*, pages 279–302. John Benjamins.

Mirza, Q. K. A., Brown, M., Halling, O., Shand, L., and Alam, A. (2021). Ransomware analysis using cyber kill chain. In *8th FiCloud*, pages 58–65.

Monika, Zavarsky, P., and Lindskog, D. (2016). Experimental analysis of ransomware on windows and android platforms: Evolution and characterization. *Procedia Computer Science*, 94:465–472.

Multi-State Information Sharing and Analysis Center (2023). Renew your ransomware defense with cisa's. https://www.cisecurity.org/insights/blog/renew-your-ransomware-defense-with-cisas-updated-guidance. Accessed: 2023-10-22.

Or-Meir, O., Nissim, N., Elovici, Y., and Rokach, L. (2019). Dynamic malware analysis in the modern era—a state of the art survey. *ACM Comput. Surv.*, 52(5).

Oz, H., Aris, A., Levi, A., and Uluagac, A. S. (2022). A survey on ransomware: Evolution, taxonomy, and defense solutions. *ACM Comput. Surv.*, 54(11s).

Pranshu Bajpai, R. E. (2020). Dissecting .net ransomware: key generation, encryption and operation. *Network Security*, 2020(2):8–14.

Roesiger, I., Bettinger, J., Schäfer, J., Dorna, M., and Heid, U. (2016). Acquisition of semantic relations between terms: how far can we get with standard NLP tools? In *5th Computerm*, pages 41–51, Osaka, Japan.

Tatam, M., Shanmugam, B., Azam, S., and Kannoorpatti, K. (2021). A review of threat modelling approaches for apt-style attacks. *Heliyon*, 7(1):e05969.

Zagrebelsky, G. (1984). *Il sistema costituzionale delle fonti del diritto*. UTET, Turin.