Human Factors in Cybersecurity, Vol. 91, 2023, 1–9
https://doi.org/10.54941/ahfe1003714

Deployment of Ransomware Detection Using Dynamic Analysis and Machine Learning

Juan A. Herrera-Silva and Myriam Hernández-Álvarez

Departamento de Informática y Ciencias de la Computación, Escuela Politécnica Nacional, Ladrón de Guevara E11-25 y Andalucía, Edificio de Sistemas, Quito 170525, Ecuador

ABSTRACT

Ransomware's growing impact is powered by dedicated criminal teams working within an organized business framework. Because of the amount of sensitive information stored on devices and the cloud while transferring over the networks, malware detection, especially ransomware, has become a primary research topic in recent years. In this paper, we present a dynamic feature dataset with 50 characteristics that are ransomware related and with low correlation pairwise. The link to the dataset is included. Using this dataset, machine learning models are generated implementing Random Forest, Gradient Boosted Regression Trees, Gaussian Naïve Bayes, and Neural Networks algorithms obtaining average ten-fold cross-validation accuracies between 74% and 100%. Processing times range between 0.15 sec and 25.47 secs, allowing a fast response to avoid encryption. These models are applied to new artifacts to effectively detect possible incoming threats.

Keywords: Ransomware detection, Dynamic analysis, Encryptor, Locker, Features, Dataset, Machine learning, Timeline of the ransomware evolution

INTRODUCTION

Ransomware's growing impact is powered by dedicated criminal teams working within an organized business framework. Because of the amount of sensitive information stored on devices and the cloud while transferring over the networks, malware detection, especially ransomware, has become a primary research topic in recent years. A ransomware-like attack uses a set of stages to infect a system; it starts with the device's distribution and infection. This malware searches for files to infect. It encrypts files, requests ransom, and threatens exposure to the affected victim's sensitive information in case of non-payment.

Ransomware malware continues to grow and transform; it took advantage of the anonymity provided by the growing popularity of cryptocurrencies. After the switch to crypto-ransomware, ransomware continued to evolve, adding features like countdown timers, ransom amounts that increase over time, and infection routines that allow it to spread through networks and servers.

This work provides human factors researchers with a better understanding of Ransomware behavior. Therefore, by generating Machine Learning based detection models, our proposed method will enable its discovery before its infection, protecting the privacy of people's information and reducing its exposure and extortion.

Ransomware History

Like any threat, ransomware is in continuous evolution. Like most malware, its goal is not to be detected or generate the most significant possible impact on infrastructure. Today, people are not only talking about cyber criminals demanding money but about threat actors (ATP - Persistent Advanced Threat), who can encrypt information and enter a system to perform espionage, capture sensitive information, or gain access to inside information.

Depending on the actor, an attack can use different techniques to enter the network. Methods include using e-mails, exploiting some vulnerability in a system exposed to the Internet, and infection some trusted websites operated by members of an organization, among other techniques.

Consequently, with that purpose, the attacker has a wide range of malware on the black market. One such service is currently provided by the Emotet malware, which was initially known as a banking Trojan. For its polymorphic versatility and ability to reach the end-user in a more friendly way via e-mail, an Office-type document, or some JavaScript file. It can be downloaded from Internet repositories. In this way, attackers use Emotet as a dropper; a Trojan is used to install other types of malware on the operating system.

Figure 1 presents a timeline of the most representative changes in ransomware and its evolution from 1989 to 2022. The ransomware selected for constructing the final dataset and the experimentation with learning models is highlighted in yellow. Those related to detection with deployment are highlighted in green in Figure 1. Ransomware has evolved and is increasingly dangerous. Nowadays, there are more forms of extortion. The attackers not only hold data hostage and ask for ransom but also extort with the threat of publishing the sequestered data.

Ransomware Taxonomy

Ransomware can be classified according to the kind of victim it tries to affect, the method of infection, the mode of communication with the command-and-control server, and the type of malicious activity it performs on a computer asset. For the development of our research, we focus on this last type of classification. There are two families of ransomware depending on the type of activity carried out on computer assets: Locker ransomware and Crypto ransomware.

Locker ransomware blocks access to the computer system to close access to its users until they pay a sum of money (Oz *et al.*, 2022), (Hassan, 2019), (Richardson and North, 2017). The threat posed by this type of ransomware depends on the lock it implements. Some examples only block access to the

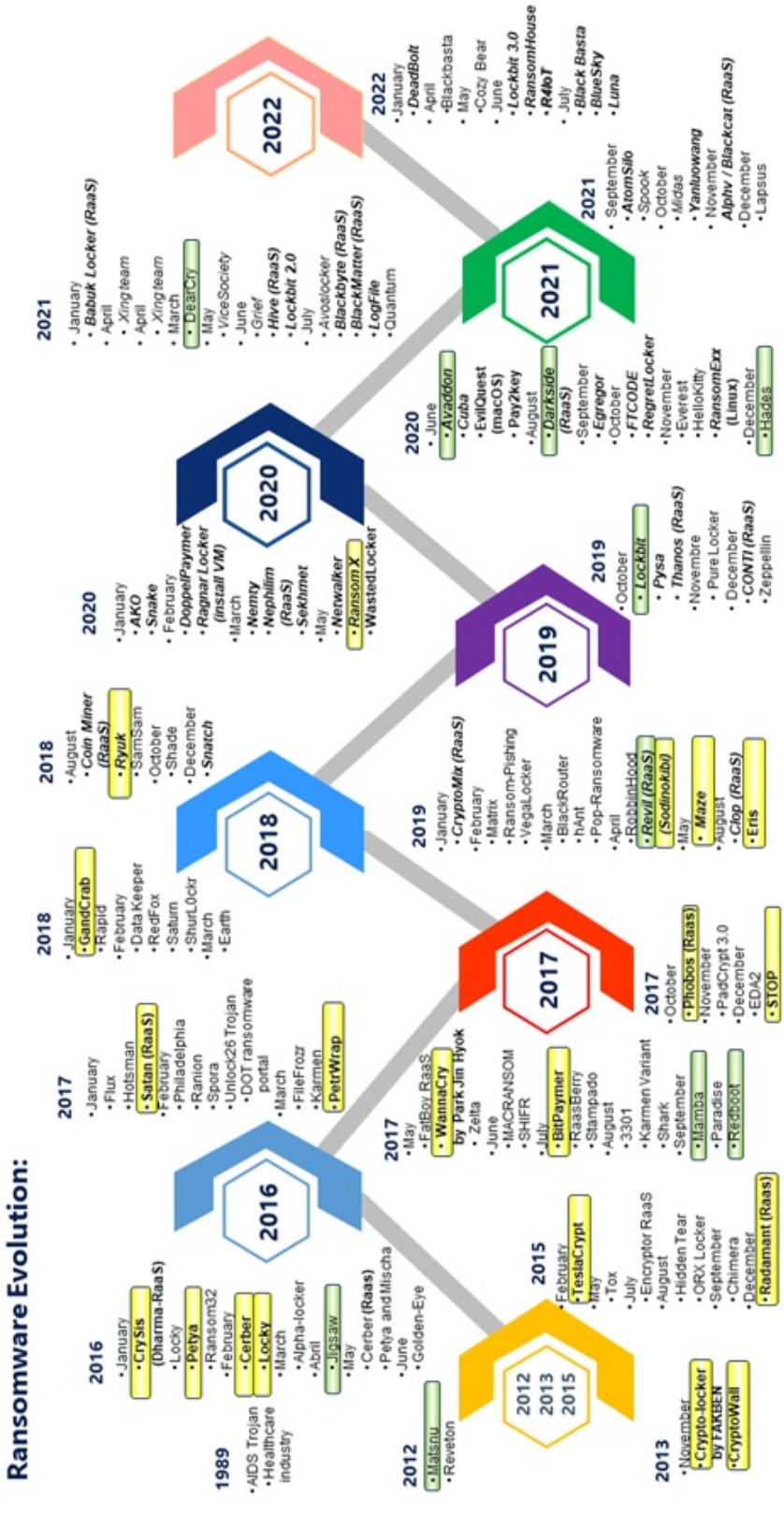

Figure 1. Timeline of the evolution of ransomware.

graphical interface, which makes them less effective. In contrast, others act directly on the Master Boot Record of a system, which makes it much more dangerous (Richardson and North, 2017).

Crypto ransomware encrypts files found within a computer system, rendering them completely unusable and inaccessible until a sum of money is paid (Oz *et al.*, 2022), (Hassan, 2019), (Richardson and North, 2017), (Gonzalez and Hayajneh, 2017). This type of ransomware represents a higher threat than the Locker family since the infected files remain completely inaccessible even if the ransomware is removed from the computer system (Hassan, 2019).

Examples of this type of malware use symmetric, asymmetric, and hybrid encryption techniques to encrypt files and protect the cryptographic keys (Richardson and North, 2017). Some variants steal the information hosted on a system and threaten the affected parties with the publication or sale of the information in case the demanded money is not paid (Dimaggio, 2022).

Ransomware Analysis

In general, malware analysis is studying, observing, and dissecting malicious software to determine its purpose, origin, and functionality (Gadhiya, Bhavsar and Student, 2013). The analysis of this type of software is necessary to develop techniques that facilitate the detection of malware and tools that allow it to be counteracted. The analysis could be classified as static or dynamic.

Static analysis focuses on studying a malicious software artifact without running it (Gadhiya, Bhavsar and Student, 2013). Within a basic static analysis process, several activities are carried out, such as evaluating the software artifact in question within various antiviruses, searching within a binary file for readable text strings, and examining the artifact's metadata, among others.

The dynamic analysis concentrates on executing the malicious artifact within a controlled environment. This execution allows us to observe and monitor the behavior of the malware in the controlled environment and determine the changes it has made on it (Gadhiya, Bhavsar and Student, 2013), (Ray and Nath, 2016). Since a malicious artifact is going to be executed in this analysis, it is necessary to have a controlled and safe environment to be able to guarantee that, after executing it, counterproductive results are not obtained, such as the infection of neighboring networks or the infection of the computer that is running the malware.

For this purpose, simulators, emulators, or sandboxing are used (Ray and Nath, 2016). In this way, the dynamic analysis seeks to obtain information on the execution of the artifact in question, such as system calls, modified system registries, files created, altered, or deleted, network connections established, network protocols used, and modifications to the file system. Our research focuses on the dynamic analysis of ransomware using a sandbox to obtain information on ransomware behavior and goodware software artifacts.

Related Work

Many ransomware studies use samples from VirusShare[1], theZoo[2], and hybridanalysis.com, among other sources. They form repositories with different ratios between the number of benign and ransomware artifacts. Some repositories include general malware artifacts. As far as we know, no studies have a complete dynamic feature dataset that can be used to generate machine-learning models like the one developed in the present research.

The present paper presents a deployment of machine learning models generated using a dynamic feature dataset obtained from running ransomware artifacts in an isolated environment. This paper contains the current Introduction. The second section corresponds to Materials and Methods, which explains the use of a cuckoo sandbox to obtain 50 dynamic features and the machine learning algorithms implemented to generate models to identify goodware and ransomware. The third section shows the dataset, the modeling process using the chosen machine learning algorithms, and the deployment results. The last section presents the conclusions.

MATERIALS AND METHODS

Our research conducts dynamic analysis using a sandbox (cuckoo). A sandbox allows for collecting information about the behavior of the artifact executed within it. Additionally, a feature extraction tool was developed to select different attributes to generate the models to be evaluated. From the total of 326 features, 50 characteristics are chosen, as marked with an X in Figure 2, taking into account the ransomware affected and using a correlation matrix to select those attributes with no redundant information.

According to Figure 2, the following attributes were selected from the cuckoos json file. They form part of our dynamic feature dataset: family, proc_pid, file, urls, type, name, ext_urls, path, program, info, families, description, sign_name, sign_stacktrace, arguments, api, category, imported_dll_count, dll, pe_res_name, filetype, pe_sec_name, entropy, hosts, requests, mitm, domains, dns_servers, tcp, udp, dead_hosts, proc, beh_command_line, process_path, children, tree_command_line, tree_process_name, command_line, regkey_read, wmi_query, directory_enumerated, regkey_opened, log, file_created, action, dll_loaded, file_read, regkey_written, apistats, and errors. These attributes are affected by ransomware and do not have a significant correlation pairwise.

Machine learning algorithms were tested to generate models to recognize ransomware. There were implemented: Random Forest, Gradient Boosted Regression Trees, neural networks, and Gaussian Naïve Bayes. Once the models are developed, cross-validation is carried out with 10 splits to validate each model effectively. Once this validation is done, we obtain the metrics of Precision, Recall, F1, and the confusion matrix to validate the results of each model.

[1]https://www.impactcybertrust.org/dataset_view?idDataset = 1271

[2]https://github.com/ytisf/theZoo

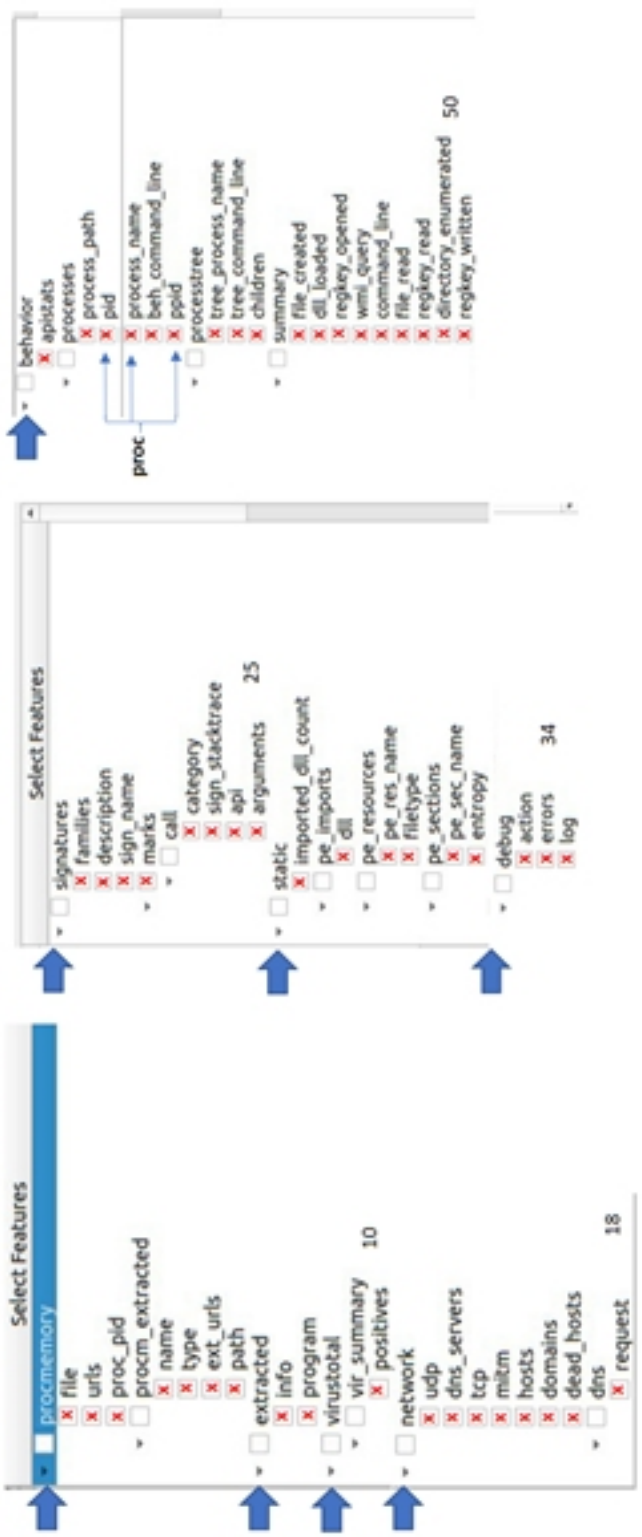

Figure 2. Dynamic characteristics extracted from the json file generated in a cuckoo sandbox.

DATASET, MODELING, AND DEPLOYMENT

For the dataset, we obtain a matrix where each row has information about an artifact, and each row cell corresponds to a feature of that artifact. This process produces a matrix of 2000 rows and 50 columns. This dynamic feature dataset can be found at https://github.com/Juan-Herrera-Silva/Paper-SENSORS.

This dataset generates the models using machine learning algorithms. For the machine learning algorithms Random Forest and Gradient Boosted Trees, we used 100 estimators or trees. For the neural network, we chose three layers with 100 neurons in each. We selected SELU as an activation function because it runs a little faster. Table 1 shows the performance of the classifiers.

Processing times for the model obtaining are fast enough to avoid encryption between 0.15 sec and 25.47 secs. The best performance algorithms are Random Forest and Gradient Boosted Regression Trees, and slightly lesser values were obtained using neural networks with three layers with 100 neurons each. Gaussian Naïve Bayes has lower performance but runs faster than the other algorithms.

The prediction of new artifacts requires generating a csv file with the previously described tool. Once you have the corresponding csv file, we use the ml_predictor.py and dl_predictor.py programs to make predictions with any generated models, whether in the repository or not. The content of these files is concise enough to change the directories of csv files and models to execute the deployment.

Our architecture allows analyzing the behavior of an artifact since it is created in a file system. It considers the sandbox environment for the dynamic analysis of an artifact, the information extraction tool obtained from this study, and the machine learning models to be used to classify the analyzed artifact, as shown in Figure 3.

Analyzing an artifact by deploying the models starts with introducing a file into the computer, for example, through a network. The creation of the file in the operating system is detected. The client opens a WebSocket type

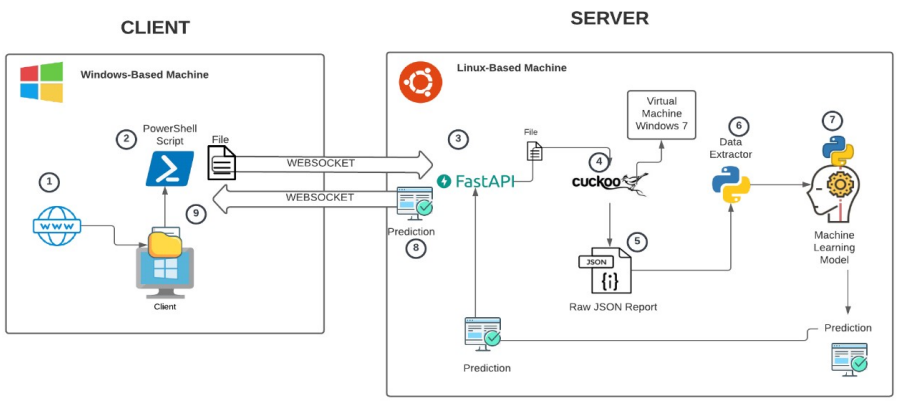

Figure 3: Deployment architecture.

Table 1. Performance of the classifiers.

Algorithm	Average ten-fold cross-validation Accuracy	Precision (%)			Recall (%)			F1 (%)			Processing time (secs.)
		G	E	L	G	E	L	G	E	L	
Random Forest	100	99.86	100	100	100	99.831	100	99.93	99.91	100	3.9
Gradient Boosted Regression Trees	100	99.74	100	100	100	99.66	100	99.86	99.98	100	25.47
Gaussian Naive Bayes	74.00	71.11	88.86	52.43	93.62	58.03	38.29	80.83	70.21	4.26	0.15
Neural Networks	99.8	99.8			99.8			99.8			6.99

connection with the server and sends the file. The server starts the dynamic analysis process using the cuckoo sandbox tool and saves the information in a json format. The feature extraction tool obtains the characteristics to input into the machine learning models. The model provides the classification and sends it through the WebSocket connection to the client to take action if necessary, i.e., if ransomware is detected.

CONCLUSION

In this article, the authors have developed a dataset composed of the dynamic features of locker and encryptor ransomware and also characteristics extracted from goodware. The attributes were selected with the criteria that they are related to the effects of ransomware. In the literature, it was found that a ransomware dataset with these characteristics was needed because the ones that are publicly accessible do not have dynamic features of the artifacts but only fixed signatures. Most datasets are only a compilation of malware and goodware and do not present features.

In the deployment, predicting new artifacts requires applying the generated models, whether in the repository or not. The programs allow changing the directories of csv json files and models to readily execute them in the production stage.

Performance results are high, allowing fast and correct detection of locker and crypto-ransomware.

This work will contribute to human factors researchers with a method for protecting private and confidential information to avoid the affectation of public and private sectors which are affected today by Ransomware attacks.

ACKNOWLEDGMENT

The authors would like to acknowledge the funding provided by Escuela Politécnica Nacional, Dirección de Investigación. Quito – Ecuador.

REFERENCES

Dimaggio, J. (2022) 'A history of Revil', 1(January 27), pp. 1–6.

Gadhiya, S., Bhavsar, K. and Student, P. D. (2013) 'Techniques for Malware Analysis', International Journal of Advanced Research in Computer Science and Software Engineering, 3(4), pp. 2277–128.

Gonzalez, D. and Hayajneh, T. (2017) 'Detection and prevention of crypto-ransomware', 2017 IEEE 8th Annual Ubiquitous Computing, Electronics and Mobile Communication Conference, UEMCON 2017, 2018-Janua, pp. 472–478. doi: 10.1109/UEMCON.2017.8249052.

Hassan, N. A. (2019) 'Ransomware Revealed: A Beginner's Guide to Protecting and Recovering from Ransomware Attacks', Access, IEEE, p. 2.

Oz, H. et al. (2022) 'A Survey on Ransomware: Evolution, Taxonomy, and Defense Solutions', ACM Computing Surveys. Associationfor Computing Machinery, 1(1). doi: 10.1145/3514229.

Ray, A. and Nath, A. (2016) 'International Journal of Advance Research in Computer Science and Management Studies Introduction to Malware and Malware Analysis: A brief overview', (November). Available at: www.ijarcsms.com.

Richardson, R. and North, M. (2017) 'Ransomware: Evolution, Mitigation and Prevention', International management review, 13(1), pp. 10–21.