RADAR: Ransomware Auto-Detection At Runtime

Kimia Saedi
ks152@rice.edu

Weijie Huang
wh31@rice.edu

Abstract

Ransomware attacks have been a huge threat for personal and business data safety. The malicious person usually launches denial-of-access attacks to user files to request for ransom payments. As the number of victims increases with the year, it is important to introduce detection methods to avoid property loss in the early stage. Recent state-of-art works tend to utilize Cuckoo Sandbox for information gathering. In this project, we will propose RADAR that integrates Intel's dynamic binary instrumentation framework (Pin) as well to collect more comprehensive data. The runtime information will be classified by a supervised learning trained model. We will evaluate the performance of RADAR by the end of this project.

1 Introduction

Ransomware is a type of malicious software (i.e., malware) that usually blocks users from controlling the computer or accessing files to request ransom payments. It often uses hard-to-crack methods to encrypt files, forcing victims to pay to regain access to their data. WannaCry, [2] one of the most famous ransom attacks in recent times, has caused incalculable damage worldwide, which impacted countless computers in companies, organizations and governments. According to a recent survey, [4] 73% of the cybersecurity professionals reported that their organization was attacked by ransomware, which is 33% more than the statistics in 2021. Moreover, 63% of the respondents reported that the attackers might have been lurked in their networks for up to six months, which emphasizes the significance of early detection against potentially malicious behavior.

In recent years, researchers have proposed several patterns, metrics and detection algorithms to identify and/or capture ransomware features. [3, 5, 8, 9] Most state-of-art works utilize Cuckoo Sandbox, [1] an open-source sandbox tool with powerful logging capabilities, to record and analyze invocations of system APIs. However, Cuckoo can only capture high-level interactions, while memory-based operations may also be essential for ransomware identification. In this project, we aim to propose RADAR, an automated ransomware detection tool at run time. We will utilize Pin, [7] a robust binary instrumentation tool for x86/64 machines, to assist Cuckoo with information gathering. Then we will propose a supervised learning model to detect ransomware-like behaviors from the collected runtime features. We will evaluate the model with both ransomware and ordinary programs to test the model accuracy.

2 Background

A malware detector typically uses static and dynamic analysis techniques to evaluate a sample's behavior and risks. Static analyses are done before execution. Considering that, they struggle to analyze obfuscated code which is the case in most threats. Dynamic analyses have shown better results for malware detection because they track the malware behavior and activities by executing the malware sample. In this work, we use data collected from Cuckoo Sandbox plus Pin in order to run dynamic analysis.

UNVEIL [6] is a novel dynamic analysis system for detecting ransomware attacks and recognizing their behaviors. UNVEIL is a rule-based ransomware detector that monitors access patterns in terms of I/O traces and alarms on ransomware-like behavior while our approach is more general purpose in this work we propose a data-driven automated ransomware detector based on machine learning techniques however it is possible to improve turn into a powerful Intrusion Detection System (IDS).

3 Methodology

In this work we aim at, first, finding the most indicative characteristics of ransomware attacks exploiting their dynamic behavior, second, using the extracted feature vector of labeled attack and benign traces we then explore the most effective supervised learning algorithms to detect such malware. For that we make use of cuckoo sandbox reports that generate the high-level data including static information such as imported DLLs, compilation time, etc., and dynamic information such as sequence of processes, API calls and their frequency also some behaviour signatures in form of flags combined with the Pin trace data that comprises low-level memory access patterns. After data collection phase for each sample run we input the resulted dataset into a data mining tool called WEKA for benchmarking the machine learning algorithims with measuring the accuracy metrics. Having that in mind we hypothesis that with regard to the sequential nature of program traces the Attention-based solution might be the most effective technique to charactrize malwares.

4 Project Plan

We divide the project into three phases:

Phase 1: Data collection. By Oct 21, we will figure out the workflow for raw runtime data, which consists of two parts: Cuckoo logs and instrumented outputs. The former one is trivial. For the latter part, We will insert function calls to a runtime library, *LibMemorizer*, to record memory allocations/deallocations/accesses. The runtime data will be dumped into a file for later analysis.

To better observe the program behavior, we need to grasp the information of the function caller. We will carry out experiments on Windows, so it is essential to develop an auxiliary tool to parse the symbol table. Similar to ELF, Windows executable files have a header structure to identify the file layout. This way, we can identify the specific functions who perform probably malicious operations.

Phase 2: Feature extraction. By Oct 31, we will count the collected data and extract the characteristics that could be fed to the network model. In other words, we will provide a ransomware behavior dataset for model detection. Then, we will propose and build the network to learn the ransomware patterns from the characteristics by Nov 15.

Phase 3: Training and evaluation. After building the dataset and network, we will train the model and test the effectiveness of the detection. We will try to make efforts to optimize the model performance. In the end, we might produce a full workflow for RADAR.

References

[1] Cuckoo sandbox-open source automated malware analysis.

[2] The malware is thought to have been created with tools stolen from the us national security agency. *BBC News* (May 2017).

[3] CHEN, Q., ISLAM, S. R., HASWELL, H., AND BRIDGES, R. A. Automated ransomware behavior analysis: Pattern extraction and early detection. *ArXiv abs/1910.06469* (2019).

[4] CYBEREASON. *Ransomware The True Cost to Business* (2022).

[5] HOMAYOUN, S., DEHGHANTANHA, A., AHMADZADEH, M., HASHEMI, S., AND KHAYAMI, R. Know abnormal, find evil: Frequent pattern mining for ransomware threat hunting and intelligence. *IEEE Transactions on Emerging Topics in Computing 8*, 2 (2020), 341–351.

[6] KHARAZ, A., ARSHAD, S., MULLINER, C., ROBERTSON, W., AND KIRDA, E. UNVEIL: A Large-Scale, automated approach to detecting ransomware. In *25th USENIX Security Symposium (USENIX Security 16)* (Austin, TX, Aug. 2016), USENIX Association, pp. 757–772.

[7] LUK, C.-K., COHN, R., MUTH, R., PATIL, H., KLAUSER, A., LOWNEY, G., WALLACE, S., REDDI, V. J., AND HAZELWOOD, K. Pin: Building customized program analysis tools with dynamic instrumentation. *SIGPLAN Not. 40*, 6 (jun 2005), 190–200.

[8] MORATÓ, D., BERRUETA, E., MAGAÑA, E., AND IZAL, M. Ransomware early detection by the analysis of file sharing traffic. *J. Netw. Comput. Appl. 124* (2018), 14–32.

[9] VERMA, M. E., AND BRIDGES, R. A. Defining a metric space of host logs and operational use cases. *2018 IEEE International Conference on Big Data (Big Data)* (2018), 5068–5077.