An Evaluation of Yara and Strelka and How They can be Used to Improve Generic Incident Response Plans for Efficient Crisis Responses in Businesses

Martin Georgiev
School of Design and Informatics
Abertay University
DUNDEE, DD1 1HG, UK

ABSTRACT

In modern days, cyber-attacks are becoming increasingly sophisticated with samples combining multiple capabilities and newer malware strains constantly appearing. To react, corporations create Incident Response Plans - policies and actions which should be undertaken to mitigate or counter infections with malicious software. Unfortunately, most companies' Response Plans are generalised and cover malware by types, rather than specific samples. This may prove disastrous if an infection is caused by malware disguised as a different type (such as a wiper with similar symptoms to ransomware) as it may cause catastrophic damages.

This project aims to solve the issue of generalised Incident Response Plans by providing simple malware analysis and digital forensic methodology to companies which can use the obtained intel to create Yara rules, increasing their security by scanning files and promptly identifying them by their signatures. The data will then be utilised to design different modules to counter specific samples, increasing both the speed and efficiency of the recovery.

Keywords

Incident Response Plan, Malware Analysis, Digital Forensic, Yara, Strelka, Ransomware, Wiper, Fileless Malware

1. Introduction

Cyber-attacks are becoming more popular, with the number of affected companies and organisations increasing yearly. Compared to the second quarter of 2021, the average weekly attacks on the Education sector have gone up by 53% (2,315 attacks), 44% for the government and military sector (1620 attacks) and 60% for the healthcare sector (1342 attacks) (CheckPoint, 2022) (Table 2.1). To tackle this, many firms create their Incident Response plans (IRP from here on) – detailed guides on what should be done to prevent attacks and how to tackle the issue in pre- and post-infectious situations. However, in an event of an attack, most of them do not make any changes to the IRPs and wait for external digital forensic companies to assess the situation first before taking any preventative actions. This may result in delayed countermeasures and affect systems in unprecedented ways as certain malware can disguise as different types. In such cases, companies may respond promptly by conducting simple digital forensic and malware analysis altering parts of their IRP based on the malware's capabilities.

2. Background

Malicious software (malware) is a term covering harmful software in its entirety. Many types fit in the beforementioned term, some of the most frequent being Trojan horses, ransomware, spyware, fileless malware (Sudhakar and Kumar, 2020) and wipers. Such software can cause major damage to both organisations and their users (including the data they store on their devices), as well as financial catastrophes and lawsuits even on an international scale. With cyber-attacks increasing every year (Table 2.1), organisations have started developing courses of action which can be taken to mitigate an infection or take appropriate countermeasures if one is to occur. Such plans are called Incident Response Plans.

Highest Average Weekly Attacks per Organisation by Industry – Global Q2 2022			
Education	Government	ISP/MSP	Healthcare
2315 (+53%)	1620 (+44%)	1397 (+29%)	1342 (+60%)

Table 2.1 – Highest attacks per organisation in Q2 2022 by CheckPoint.

2.1 Incident Response Plans and Their Disadvantages

A vital part of a company's ability to deal with a cyber-attack is the Incident Response Plan. Such plans are created in cooperation between a specialised team and the executives. They consist of different rules and what courses of action should be taken to mitigate or respond to a certain crisis. However, many IRPs are generalised and require the organisation to wait for a digital forensic company to analyse their network and sample any malware that has infected it. Because of this, companies may be affected in a negative way depending on the crisis. This may happen with new versions of malware or disguised malicious software. The latter may refer to two different types. The first could be a sample impersonating a benign process. They may be difficult to identify unless their actions are closely monitored. The second may refer to malware acting as a completely different type (i.e., **NotPetya**, a wiper disguised as ransomware). Slow and inappropriate countermeasures may be critical for organisations infected by such malicious software as they can harm the company on both physical/infrastructural and on intellectual levels, possibly even leading to lawsuits. A good way to make IRPs more efficient is by using a simple malware analysis methodology and implementing **Yara** and **Strelka** to scan newly downloaded files.

2.2 Yara and Strelka

Yara also called the “Swiss knife” for malware researchers, is designed to aid analysts and normal users in the identification and classification of malware samples. The tool is versatile and powerful, allowing researchers to create rules, which can represent different malware sub-categories or even separate samples, based on textual and/or binary patterns present within the malicious software. Furthermore, its well-written documentation and multi-platform capabilities (**Windows**, **Linux**, and **Mac OS X** or even through Python scripts), make the tool easy to understand and work with by both beginners and cybersecurity professionals. The created rules can be used to scan specific files or entire directories, giving an appropriate alert if a specific pattern is matched.

Strelka is a modular open-source enterprise file scanner, which can be configured to scan large amounts of data for incident response and detection of malicious files. The tool in itself is not a detection engine, but it makes use of fifty different scanners – footer, hash, header, XML, Yara, etc. All fifty scanners work simultaneously to provide the analysts with detailed metadata. Furthermore, Strelka can make use of custom Yara rules for more accurate pattern matching. The tool can also be paired with a **SIEM** (Security Information and Event Management) such as **Splunk** or **Logpoint**, allowing analysts to better understand the environment without the need for direct data gathering.

2.2 Aims

The project aims to create a modular IRP (Wyk and Forno, 2001; Johnsen, 2004) based on intel obtained from analysing multiple malware samples with a malware analysis (Monnapa, 2018) and forensic methodology and show why generalised response plans may be flawed in certain situations. The methodology can be used by organisations to analyse samples as soon as an infection is identified and acquire vital information regarding its capabilities (Nguyen and Goldman, 2010; Higuera, 2020). The methodology will be as follows:

- Copy the sample in a virtual testing environment (**Flare VM** paired with **Remnux**)
- Conduct basic static analysis of the malware
    - Examine the hash values
    - Examine imported libraries and functions
    - Find strings of a human-readable text
- Conduct basic dynamic analysis
    - Detonation symptoms and conditions
    - Network propagation
    - Host-based indicators and persistence
- Attempt to reverse engineer the samples
- Attempt to alter or prevent the execution of the malware

Afterwards, the obtained information can be used in a multitude of ways, two of which are to provide it to the hired digital forensic organisation to increase the speed of the analysis; and to create rules with Yara and scan new files for their signatures before opening them. Additionally, the scanning process can be automated with Strelka, which will help with the time-consuming procedure. With this, the IRPs can also be reworked to better fit the specifics of the infection and minimise the damage.

In the end, the acquired information will be used to create more situationally specific IR Plans by altering parts of the initially provided generic plan. Doing so will provide companies with the ability to critically analyse and alter their response plans if needed, whilst creating various IR Plan “modules” for different malware families which can be removed or included based on the infection (Shinde and Kulkarni, 2021).

3. Methodology

3.1 Generic Incident Response Plan

Thorough research will be conducted to analyse many Incident Response Plan creation techniques and management. The created plan will include generalised pre- and post-infection countermeasures for specific situations and malware types.

3.2 Setup the Testing Environment

As the paper is made for businesses, a quick and simple environment setup guide will be provided. It will include how to obtain FlareVM and Remnux, how to set up different tools (i.e., Inetsim) and a separate virtual subnet that has no access to the physical host or the internet. This will provide the organisation with a safe testing environment, isolated from the company’s intranet, extranet, and the wide web.

3.3 Basic Static Analysis

The basic static analysis section will cover show what steps an organisation should be taken to conduct a simple analysis without executing the obtained sample. This includes hash extraction and identification in VirusTotal, string extraction with Floss and imported library/functions examination with PEStudio. Checking a sample’s hash in VirusTotal can help to quickly identify common malware and its capabilities. The human-readable string extraction will be useful for creating Yara rules. It will also allow them to identify samples with changed names based on specific strings (i.e., wnry for WannaCry). PEStudio analyses the entire binary file and lists all recognised blacklisted libraries and functions which could be used for malicious purposes. Knowing them will also provide knowledge of how the sample may function.

3.4 Basic Dynamic Analysis

This section will show organisations how executing malicious software in a safe environment can supply them with information on its symptoms, detonation conditions, as well as host and network-based indicators. To examine the host- indicators, a tool called Procmon will be used. It allows an analyst to examine the processes on the local system – what files/registers/directories are created, deleted, or altered. For network propagation, FlareVM will be used together with tools in Remnux. Inetsim, a tool in Remnux, will simulate a DNS and DHCP server. The generated traffic can then be captured and examined with Wireshark – whether it tries to communicate with a domain or other hosts on the network. Additionally, TCPView will be used n FlareVM to monitor if the sample opens any ports and attempts to establish any TCP or UDP communications with other machines.

3.5 Advanced Static Analysis

The advanced static analysis phase will show how simple reverse engineering techniques can be used to obtain more information regarding how the malware operates. This, of course, is a more advanced topic so organisations who would like to tackle malicious software on such a level would be required to invest in their cybersecurity departments or even create specialised teams who will handle malware samples. Reverse engineering an executable file requires a disassembler such as Ghidra. Loading the samples in the tool will show the assembly code and an interpretation of it in C++. The code can then be examined to get an in-depth understanding of how malware work works – network propagation capabilities, payload phases, encryption, security evasion (Afree. Aslam, Ahmed, 2020), etc.

3.6 Advanced Dynamic Analysis

Advanced dynamic analysis of a malware sample includes preventing or altering the execution flow of its processes. To achieve this, the software should be loaded in a debugger (such as x32dbg) and manually debugged. Successfully preventing the normal operation of the sample can be considered as a complete or partial killswitch – something which can help not only the affected company but many other users and organisations.

3.7 Yara rules and Strelka Automation

The obtained intel from the malware analysis methodology can be used to create detailed Yara rules. Yara allows a user to scan files for specific signatures (specific strings within the binary file or even the hash) and leave appropriate messages if a match is identified. Yara can then be combined with Strelka to automate the process and scan larger amounts of data. Additionally, Strelka makes use of many other scanners which can identify even more information about the sample's metadata - something which can be used to further enhance the existing Yara rules.

3.8 Creating IR Modules

Using the beforementioned intel, separate modules will be created based on the analysed samples. The modules can be removed and included in the incident response plans to better suit the type of infection. This will allow the company to make use of the knowledge, whilst efficiently responding to the infection.

3.9 Evaluation

The initially created generic IRP will be compared to the modular version in specific situations (different malware types), showing both the advantages and disadvantages of using generalised and specifically tailored IRPs to tackle cyber catastrophes. This will include the efficiency of how different infections can be mitigated, whether they will help with more prompt malware identification and isolation and how user and company data can be protected.

3.10 Results

The project will provide companies with a template of a modular incident response plan. The modules will be based on information obtained through simple malware analysis and digital forensic methodology – different symptoms, capabilities, network propagation, etc. The modules will provide corporations with in-depth pre- and post-infection policies on how to read the analysed samples. Additionally, Yara rule samples based on the findings of the methodology will be included. Organisations can use the methodology to expand the Yara rules and create additional modules to counter other malware.

4. Summary

Incident response plans provide a standardised way for companies and organisations to tackle cyber-attacks. More generalised plans can be efficient and useful for pre-infection countermeasures. However, creating more specialised IR Plans based on finding more information regarding what has caused the infection can be beneficial for taking faster and more specific actions.

5. REFERENCES

Sudhakar and Kumar, S. (2020). An emerging threat Fileless malware: a survey and research challenges. SpringerOpen, [online]. doi:10.1186/s42400-019-0043-x. [Accessed 11 October 2022].

Afreen, A., Aslam, M. and Ahmed, S. (2020). Analysis of Fileless Malware and its Evasive Behavior. International Conference on Cyber Warfare and Security (ICCWS), [online]. doi:10.1109/iccws48432.2020.9292376. [Accessed 11 October 2022].

Shinde, N. and Kulkarni, P. (2021). Cyber incident response and planning: a flexible approach. Computer Fraud & Security, [online]. doi:10.1016/s1361-3723(21)00009-9. [Accessed 11 October 2022].

Johnsen, S.O., Røstad, L., Haugset, B. and Dahl, M.B. (2004). From Incident Response to Incident Response Management. SpringerLink, [online]. doi:10.1007/978-0-85729-410-4_20. [Accessed 11 October 2022].

Wyk, K; Forno, R. (2001). Incident Response - Incident Response [Book]. O'Reilly, [online] Available at: https://www.oreilly.com/library/view/incident-response/0596001304/index.html [Accessed 11 October 2022].

Monnapa, K A. (2018). Learning Malware Analysis [Book]. Packt, [online]. Available at: www.packt.com [Accessed 11 October 2022].

Nguyen, C; Goldman, J. (2010). Malware analysis reverse engineering (MARE) methodology & malware defence (M.D.) timeline. ACM Digital Library, [online]. Available at: https://dl.acm.org/doi/abs/10.1145/1940941.1940944 [Accessed 11 October 2022].

Higuera, J. (2020). Systematic Approach to Malware Analysis (SAMA). MDPI, [online]. Available at: https://www.mdpi.com/2076-3417/10/4/1360/htm [Accessed 11 October 2022].

Checkpoint. (2022). Check Point Research: Weekly Cyber Attacks increased by 32% Year-Over-Year; 1 out of 40 organizations impacted by Ransomware. [online] Check Point Software. Available at: https://blog.checkpoint.com/2022/07/26/check-point-research-weekly-cyber-attacks-increased-by-32-year-over-year-1-out-of-40-organizations-impacted-by-ransomware-2/. [Accessed 11 October 2022].