

Report

Writing a Yara Rule

Sakarie Sa'ad Osman (Sap iD:30025)

Riphah International University

Date: 19 May 2024

Table of Contents

Report.....	1
Executive Summary	3
Introduction:.....	4
Scope:.....	4
Methodology:.....	5
-YARA Rule:	6
-Python DummyCode	7
-Text File:.....	8
-CMD	9
Procedure	9
Conclusion:	10

Executive Summary

Overview:

A YARA rule is a set of conditions and patterns used to identify and classify malware or other types of files based on specific characteristics. YARA (Yet Another Recursive Acronym) is a tool widely used by security researchers and analysts to identify and classify malware samples.

Introduction:

In this project, I have written a Yara ruler for basic code in Python, I have initialized some strings in Python code, and the Yara rule is going to match the pattern that exists in the code with the pre-mentioned strings in the Yara rule.

Scope:

The analysis is focused on scanning the files dummycode.txt also dummycode.py using a set of predefined YARA rules written in YARA.

Yara Rule

Methodology:

Tools Used:

- YARA
- Text file (written in Visual Studio)
- Python File (Written in Visual Studio)
- CMD (Command Prompt)

Yara Rule

-YARA Rule:

```
rule CheckTheStrings
```

```
{
```

```
meta:
```

```
    description = "Simple Yara Code created to detect the strings present in the Dummy code  
saved in text file"
```

```
strings:
```

```
    $name = "Sample"
```

```
    $ip = "192.168.111.222"
```

```
    $hashValue = "1234567890987654321"
```

```
    $url = "https://sampleDomain.com"
```

```
condition:
```

```
    any of them
```

```
    /#($name or $ip or $hashValue or $url)
```

```
}
```

Yara Rule

-Python DummyCode

#Definig the Strings

Name = "Sample"

Ip = "192.168.111.222"

HashValue = "1234567890987654321"

Url = "https://sampleDomain.com"

#Printing the Strings

print(Name)

print(Ip)

print(HashValue)

print(Url)

Yara Rule

-Text File:

This also just contains the code in the Python file But in .txt file extension.

#Definig the Strings

Name = "Sample"

Ip = "192.168.111.222"

HashValue = "1234567890987654321"

Url = "https://sampleDomain.com"

#Printing the Strings

print(Name)

print(Ip)

print(HashValue)

print(Url)

Yara Rule

-CMD

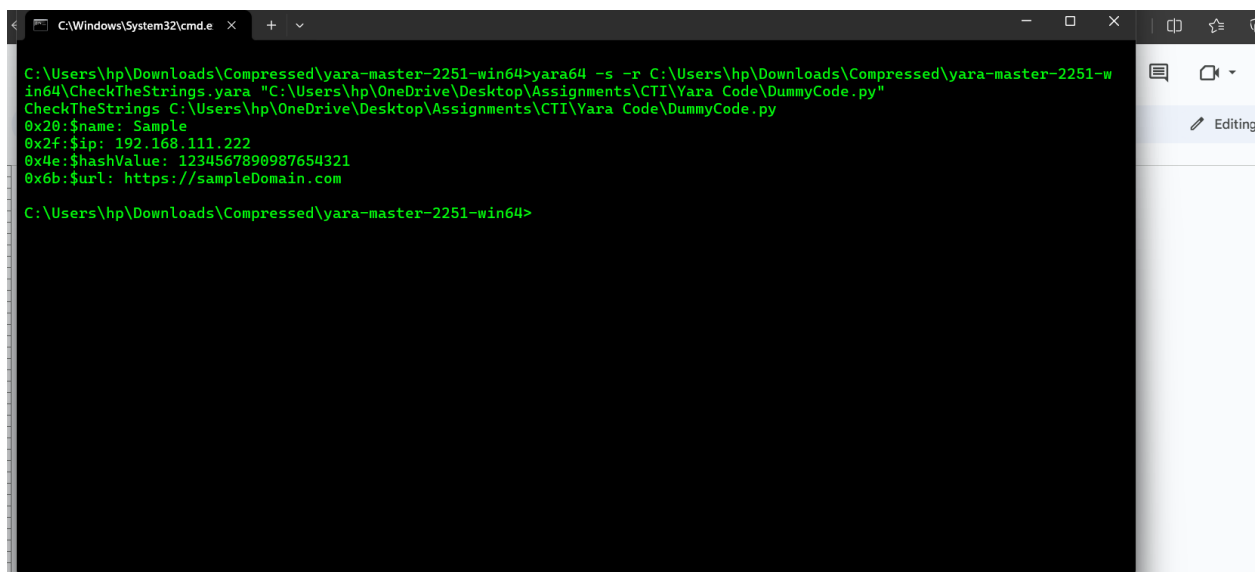
-Version: 4.5.0

Procedure

To run this YARA rule we use the cmd first we go to the Yara installed file path, then we follow that with **-s** for strings and **-r** for recursiveness, and then the Yara rule file location after that the code or the text that needs to be analyzed.

After that, the matched pattern will be shown if there is a match. But if you must have changed the strings in the code and the code in YARA does not match then some of the string will be missing from the matching pattern.

Here is the Output:



```
C:\Users\hp\Downloads\Compressed\yara-master-2251-win64>yara64 -s -r C:\Users\hp\Downloads\Compressed\yara-master-2251-win64\CheckTheStrings.yara "C:\Users\hp\OneDrive\Desktop\Assignments\CTI\Yara Code\DummyCode.py"
CheckTheStrings C:\Users\hp\OneDrive\Desktop\Assignments\CTI\Yara Code\DummyCode.py
0x20:$name: Sample
0x2f:$ip: 192.168.111.222
0x4e:$hashValue: 1234567890987654321
0x6b:$url: https://sampleDomain.com

C:\Users\hp\Downloads\Compressed\yara-master-2251-win64>
```

Yara Rule

Conclusion:

The YARA rule analysis successfully identified the presence of an IP address, URL, and hash within the target dummy code. These patterns are often indicative of network activity, web links, and file integrity checks, respectively.

In the above image is clear that all the strings are matched and all of them are shown here which means our Yara rule was successful and the strings are successfully matched.