NIIT UNIVERSITY, NEEMRANA
DEPARTMENT OF COMPUTER SCIENCE AND ENGINEERING
THREAT INTELLIGENCE LAB

THREAT INTELLIGENCE LAB (CS-5202)

Yara Rule

2021-2022

Pradeesh Kumar.R
MT20ACS523

AREA DIRECTOR NAME
Dr. Debashish Sengupta

FACULTY NAME
Dr. Ashu Sharma

Table of Contents

Problem Statement

In this lab you need to create a Yara rule out of any malware family. you can download samples from https://github.com/InQuest/malware-samples.

do following task in lab

1. Create a Yara rule with .yara for selected malware.
2. Create a report with following details.
   description of malware
   description of Yara patterns (why have u chosen the pattern and why you think the pattern cannot occurs in clean file)
3. Create a folder (with ur id _presiding with ur name) which contains following
   created Yara rule
   report
   the samples chosen
4. Upload the created folder on git hub repo
5. Share the link

Malware Selected

Malware Sample Name: 2018-05-KPOT

Sample Location: malware-samples/2018-05-KPOT at master · InQuest/malware-samples · GitHub

Files Present:

- 36dcd40aee6a42b8733ec3390501502824f570a23640c2c78a788805164f77ce
- 67f8302a2fd28d15f62d6d20d748bfe350334e5353cbdef112bd1f8231b5599d

Virus Total Links

- https://www.virustotal.com/gui/file/36dcd40aee6a42b8733ec3390501502824f570a23640c2c78a788805164f77ce/detection
- https://www.virustotal.com/gui/file/67f8302a2fd28d15f62d6d20d748bfe350334e5353cbdef112bd1f8231b5599d/detection

Yara Rule

```
rule lab3exe
{
meta:
        Description = "Simple YARA rule to detect 2018-05-KPOT"
        Author = "Pradeesh Kumar.R (MT20ACS523)"
        Date = "2021-08-27"

strings:
        $str01 = "http://%s" wide ascii
        $str02 = "https://%S/a/%S" wide ascii
        $str03 = "HTTP Server URL" wide ascii
        $str04 = "password-check" wide ascii
        $str05 = "*.wallet" wide ascii
        $str06 = "*.rdp" wide ascii
        $sr01 = "9087654356.exe" wide ascii

        $reg01 = /(SMTP|POP3|IMAP)\s(User|Password|Port|Server)/ wide ascii
        $reg02 = /(HttpWeb|Web|Get)(Request|Response|Client)/ wide ascii


condition:
        all of ($str*)
        or all of ($sr*)
        and 1 of ($reg*)
}
```

Description of Malware

Both the files are PEXE - PE32 executable (GUI) Intel 80386, for MS Windows. KPOT Stealer is a “stealer” malware that focuses on exfiltrating account information and other data from web browsers, instant messengers, email, VPN, RDP, FTP, cryptocurrency, and gaming software.

Description of Yara Patterns

- $str01 and $str02 references a URL pattern in http and https
- $str03 references HTTP Server URL
- $str04 references to checking passwords
- $str05 references to .WALLET file belongs to the category of Data Files used in operating systems such as Windows 11, 10, Windows 7, Windows 8 / 8.1, Windows Vista, Windows XP. A WALLET file is a file encrypted by the CryptoMix, or CrypMix, virus, which is ransomware utilized by cybercriminals. It contains a user's file, such as a . PDF or . DOCX file, encrypted with AES encryption by the virus.
- $str06 references to RDP files mostly belong to Remote Desktop Connection by Microsoft Corporation. An .RDP file contains all of the information for a connection to a terminal server, including the options settings that were configured when the file was saved.
- $sr01 references a malicious exe file present in the sample
- $reg01 references to username, password, port 587 (SMTP – sending mails), 995 (POP3 – receiving mails) and 143 (IMAP - to retrieve email messages from a mail server) and server
- $reg02 references to request and respond data from a host server

Github Repository Location

CS-5202-Threat-intelligence/Lab3 at main · PradeeshKumar-NIIT/CS-5202-Threat-intelligence (github.com)

Conclusion

The malware is statically analyzed and yara rules has been created for the selected (KPOT V2) malware.

References

[1] Free Automated Malware Analysis Service - powered by Falcon Sandbox - Viewing online file analysis results for '36dcd40aee6a42b8733ec3390501502824f570a23640c2c78a788805164f77ce' (hybrid-analysis.com)

[2] Free Automated Malware Analysis Service - powered by Falcon Sandbox - Viewing online file analysis results for '67f8302a2fd28d15f62d6d20d748bfe350334e5353cbdef112bd1f8231b5599d' (hybrid-analysis.com)

[3] Use Ghidra to decrypt strings of KpotStealer malware – nullteilerfrei

[4] Sha256: 36dcd40aee6a42b8733ec3390501502824f570a23640c2c78a788805164f77ce - AlienVault - Open Threat Exchange

[5] Sha256: 67f8302a2fd28d15f62d6d20d748bfe350334e5353cbdef112bd1f8231b5599d - AlienVault - Open Threat Exchange