Experiment - 9

Date: 15/10/2025

ANALYSIS OF MALWARE

Aim:

To write a YARA rule to detect SpyEye (a banker-type malware) and verify detection by scanning a sample file.

Algorithm:

1. 1. Fill the 'meta' section with author name, rule description, date and version.
2. 2. In the 'strings' section, specify text strings or hexadecimal patterns characteristic of SpyEye.
3. 3. Define a 'condition' that uses the provided strings and optional file size thresholds.
4. 4. Run yara against the target file(s). If no output appears, SpyEye is not found.
5. 5. If yara reports a match, SpyEye (or a file matching the rule) has been detected.

YARA Script:

```
rule spyeye : banker
{
  meta:
    author = "Ben"
    description = "SpyEye X.Y memory"
    date = "2022-05-25"
    version = "1.0"
    filetype = "memory"

  strings:
    $g = "bot_version"
    $h = "bot_guid"

  condition:
    any of ($g, $h) and filesize > 50000
}
```

Output (example):

```
[root@localhost Downloads]# ll malware.exe
-rw-r--r--. 1 root root 148480 May 26 11:17 malware.exe

[root@localhost Downloads]# yara spyeye.yara malware.exe
```

spyeye malware.exe

Result:

The YARA rule matched the sample 'malware.exe', indicating the presence of strings associated with SpyEye. This demonstrates that YARA can be used to create concise detection rules for malware based on characteristic strings and additional conditions.