Computer Science 491/691
Malware Analysis
Homework 7
Assigned: May 1, 2019
Due: May 8, 2019

Name: Sai Sasaank Srivatsa Pallerla
ID: HG13015

How to turn this in for grading: You can edit your answers right into this file. Email it to the TAs as described in class. Make sure your name appears in the body of the document.

Instructions for installing YARA on Windows XP:

- Download and install the Microsoft Visual C++ 2010 Redistributable Package from https://www.microsoft.com/en-au/download/confirmation.aspx?id=5555
- Download YARA 3.4.0 from https://www.dropbox.com/sh/umip8ndplytwzj1/AAAj-WhDCvLxWFn17Of8aS_pa/older%20versions?dl=0&preview=yara-3.4.0-win32.zip
- Add the folder containing yara32.exe to your $PATH environment variable.

Download hw7_dataset.7z and extract it. The password is “infected”.

YARA documentation:

- https://yara.readthedocs.io/en/v3.4.0/gettingstarted.html
- https://yara.readthedocs.io/en/v3.4.0/writingrules.html
- https://yara.readthedocs.io/en/v3.4.0/modules/pe.html

Shared command example:

```
for filepath in ramnit_*; do strings $filepath | sort | uniq; done | sort |
uniq -c | sort -nr | less
```

Ramnit YARA rule:

```
import "pe"

rule Ramnit {
  strings:
    $s1 = "KyUffThOkYwRRtgPP" fullword ascii
    $s2 = "Srv.exe" fullword ascii
    $b1 = { 60 E8 00 00 00 00 5D 8B C5 81 ED ?? ?? ?? ?? 2B }

  condition:
    uint16(0) == 0x5a4d and
    all of ($s*) and
    $b1 at pe.entry_point and
    pe.sections[pe.number_of_sections - 1].name == ".rmnet"
}
```

**Part 1**

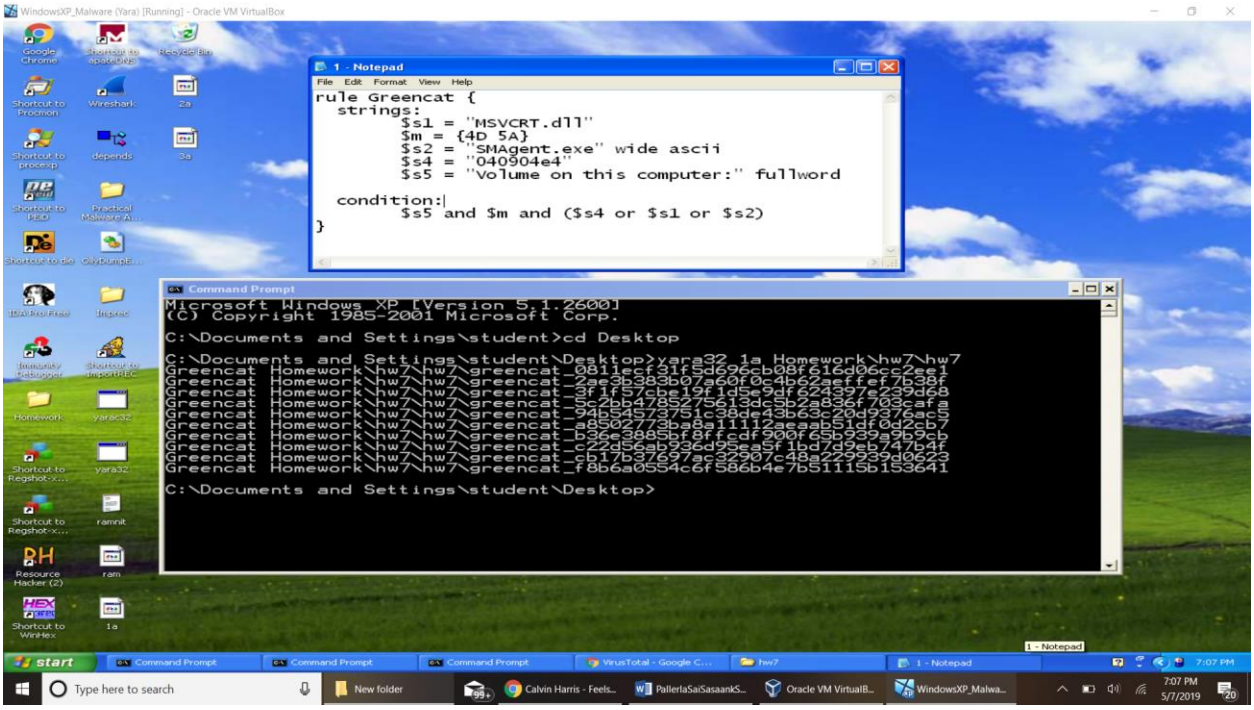
Write a YARA rule for the greencat family that meets the following conditions:

- Matches all ten greencat malware samples in the hw7 dataset
- Does not match any other malware samples in the hw7 dataset
- Checks that the file begins with the “MZ” magic bytes
- Contains at least five strings
- Uses at least two of the following modifiers: nocase, wide, ascii, fullword

Provide the YARA rule below. Then, in a few sentences, describe your design choices for the YARA rule.

```
rule Greencat {
 strings:
        $s1 = "MSVCRT.dll"
        $m = {4D 5A}
        $s2 = "SMAgent.exe" wide ascii
        $s4 = "040904e4"
        $s5 = "Volume on this computer:" fullword
 condition:
        $s5 and $m and ($s4 or $s1 or $s2)
}
```

Looking at the strings section of the malware files in greencat family, I found an exe file, a dll file which is not a windows dll, a random string with numbers and a string with “volume word in it which I thought would be unique. For the condition we were supposed to look for magic bytes and I knew for sure s5 was unique, so I used “and” condition, for the resti was looking for any one s4,s2,s1 strings so I used “or”.



**Part 2**

Write a YARA rule for the xtremerat family that meets the following conditions:

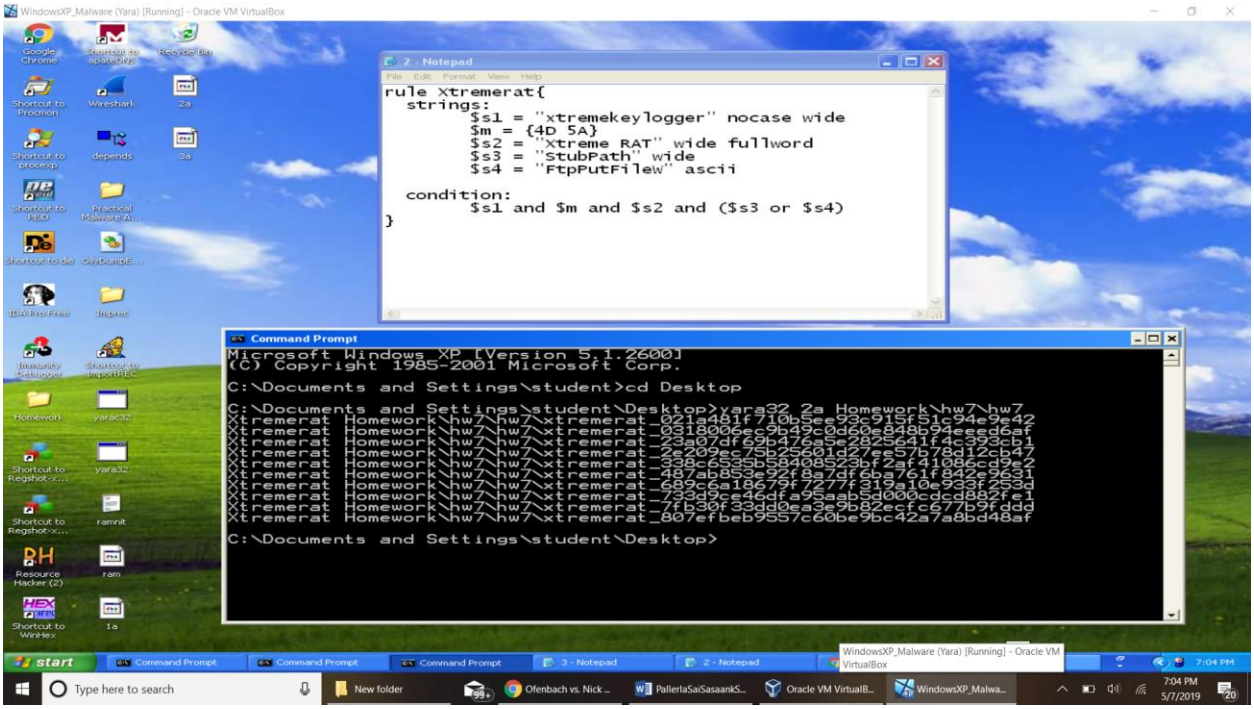
- Matches all ten xtremerat malware samples in the hw7 dataset
- Does not match any other malware samples in the hw7 dataset
- Checks that the file begins with the “MZ” magic bytes
- Contains at least five strings
- Uses at least three of the following modifiers: nocase, wide, ascii, fullword

Provide the YARA rule below. Then, in a few sentences, describe your design choices for the YARA rule.

```
rule Xtremerat{
 strings:
        $s1 = "xtremekeylogger" nocase wide
        $m = {4D 5A}
        $s2 = "Xtreme RAT" wide fullword
        $s3 = "StubPath" wide
        $s4 = "FtpPutFileW" ascii

 condition:
        $s1 and $m and $s2 and ($s3 or $s4)
}
```

Looking at the strings section of the malware files in xtremerat family, I found s1 and s2 to be unique. For the condition we were supposed to look for magic bytes (m) and s1,s2 being unique I used “and” condition, for the rest I was looking for any one of s3,s4 to be true, so I used “or”.



**Part 3**

Write a YARA rule for the poisonivy family that meets the following conditions:

- Matches all ten poisonivy malware samples in the hw7 dataset
- Does not match any other malware samples in the hw7 dataset
- Checks that the file begins with the “MZ” magic bytes
- Contains at least two strings
- Contains at least one byte sequence
- Uses at least two of the following modifiers: nocase, wide, ascii, fullword
- Uses the “at” and “pe.entry_point” keywords

Provide the YARA rule below. Then, in a few sentences, describe your design choices for the YARA rule.

```
import "pe"
rule Poisonivy{
 strings:
        $s2 = "^-m-m<|<|<|M" ascii
        $s3 = "StubPath" ascii
        $b = {B8 00 04 40 00 FF D0 6A 00 E8 00 00 00 00 FF 25 00 02 40 00}
 condition:
        uint16(0) == 0x5a4d and
        $s2 and $s3 and
        $b at pe.entry_point
}
```

For this question I had to use the pe module, so I imported pe. Looking at the strings section of the malware files in poisonivy, I found s2 and s3 to be unique, b has the byte sequence at the entry point which doesn’t change for any of the malware files in poisonivy family, so I didn’t have to use magic characters. For the condition part i used int16(0) which looks for the first two bits in the hex for magic number and I used “and” because s1,s2,b are unique to xtremerat family.