**Nwachukwu Edumanichukwu**

**CYBR 445 - Advanced Incident Detection and Response  
Module 9 Lab – Ghidra, YARA, and Sigma**

**Based on your execution of the simple.exe program and examination of the FUN\_00401000, what do you think this program does?**

**The program reveals a flag after the correct serial numbers have being entered.**

**What are we looking for?**

**Serial numbers**

**Simple.exe Serial Number:**

**1234-4321-6789-9876**

**Simple.exe Flag:**

**{\_REIsAGreatSkill\_}**

**Harder.exe Serial String:**

**FXzu8wXjhwjy&**

**What is the actual password/serial number once it is decoded?**

**ASup3rSecret!**

**What is the harder.exe flag? It is in the form of {\_xxxx…\_)}.**

**{\_KeepPractingToGetBetterAtRE\_)}**

**Simple.exe**

**String 1: tilskASaGeEIrRl**

**String 2: 1234 – 4321 – 6789 - 9876**

**String 3: {\_%c%c%c%c%c%c%c%c%c%c%c%c\_}**

**String 4: !This program cannot be run in DOS mode.**

**String 5: 4D 5A 90 00 03 00 00 00 04 00 00 00 FF FF 00 00**

**Harder.exe**

**String 1: FXzu8wXjhwjy&**

**String 2: F``kKm\^odibOjB`o=`oo`m<oM@**

**String 3: 1234-4321-6789-9876**

**String 4: !This program cannot be run in DOS mode.**

**String 5: 4D 5A 90 00 03 00 00 00 04 00 00 00 FF FF 00 00**

**simple.exe filesize: 104 KB**

**harder.exe filesize: 104 KB**

**Text of your two YARA rules:**

**rule simple {**

**meta:**

**author = “Nwachukwu Edumanichukwu”**

**description = “Analyst2 test simple.exe Test”**

**date = “07/10/2023”**

**version = “1.0”**

**sharing = “TCP:WHITE”**

**strings:**

**$string1 = “tilskASaGeEIrRl”**

**$string2 = “1234 – 4321 – 6789 - 9876”**

**$string3 = “{\_%c%c%c%c%c%c%c%c%c%c%c%c\_}”**

**$string4 = “!This program cannot be run in DOS mode.”**

**$string5 = { 4D 5A 90 00 03 00 00 00 04 00 00 00 FF FF 00 00 }**

**condition:**

**$string1 and # $string1 exists in the file and match the next condition**

**$string2 and # $string1 exists in the file and match the next condition**

**$string3 and # $string1 exists in the file and match the next condition**

**$string4 and # $string1 exists in the file and match the next condition**

**$string5 at 0 and # $string5 exists in the file and is found at the first two bytes of the file**

**filesize < 200KB # the file must be less than 200KB.**

**}**

**rule harder {**

**meta:**

**author = “Nwachukwu Edumanichukwu”**

**description = “Analyst2 test harder.exe Test”**

**date = “07/10/2023”**

**version = “1.0”**

**sharing = “TCP:WHITE”**

**strings:**

**$string1 = “FXzu8wXjhwjy&”**

**$string2 = “F``kKm\^odibOjB`o=`oo`m<oM@”**

**$string3 = “1234-4321-6789-9876”**

**$string4 = “!This program cannot be run in DOS mode.”**

**$string5 = { 4D 5A 90 00 03 00 00 00 04 00 00 00 FF FF 00 00 }**

**condition:**

**$string1 and # $string1 exists in the file and match the next condition**

**$string2 and # $string1 exists in the file and match the next condition**

**$string3 and # $string1 exists in the file and match the next condition**

**$string4 and # $string1 exists in the file and match the next condition**

**$string5 at 0 and # $string5 exists in the file and is found at the first two bytes of the file**

**filesize < 200KB # the file must be less than 200KB.**

**}**

**Screenshot of successful simple.exe scan**

**I was not able to get any match. A screenshot of a computer code

Description automatically generated**

**Screenshot of successful harder.exe scan**

**I was not able to get any match. A close-up of a computer code

Description automatically generated**

**SIGMA Rule:**

title: Potential Password Exposure (via cmdline)  
author: Adam Swan  
tags:  
  - attack.t1552.001   
  - attack.credential\_access  
logsource:  
  product: windows  
  category: process\_creation  
detection:  
  selection:  
    Image|endswith:   
      - '\notepad.exe'  
      - '\word.exe'  
      - '\excel.exe'  
      - '\wordpad.exe'  
      - '\notepad++.exe'  
    CommandLine|contains:  
      - 'pass' #pass will match on password, including password is redundant  
      - 'pwd'  
      - 'pw.' #pw.txt, etc.   
      - 'account' #accounts,   
      - 'secret'  
      - 'details' #I included plural details based on experience  
  condition: selection

**Elastic Query:**

**A screenshot of a computer

Description automatically generated**

**Splunk:**

A screenshot of a computer

Description automatically generated