**DAY 0401 – Online banking malware Exercise**

Name: Click here to enter name.

Date: **Click here to enter a date.**

**GENERAL INSTRUCTIONS:**

* Passing rate is 85%.
* Save your exercises in a \*.zip file with the following format:
  + DayClick here to enter Day.–NameFormat.zip
    - Name Format: First Name + Initial of Last Name
    - Eg. Mark Zbikowski > Day0401-MarkZ.zip
  + The password for the zip file should be virus

**Part I: Malware Analysis**

**Extract the file in *banker.zip* inside the virtual environment.**

You may use **ProcessExplorer**, **InstallRite**, **SysTracer** and **HashMyFiles** to analyze the behavior of the file.

Execute the file banker.exe.

1. This malware drops a copy of itself. What is the file name and where is it located?

|  |
| --- |
|  |

1. This malware drops other component files. Provide full path and filename for these files.

|  |
| --- |
|  |

1. It adds a registry entry in HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Run. What is it? Paste the value and data below:

|  |
| --- |
|  |

**Part II: Network Analysis**

**Extract the file in *banking.zip* inside the virtual environment**.

1. Open ***GOLROTED.pcap*** using **Wireshark** and analyze the network traffic of the malware.
2. The malware sends the stolen information via email. Identify the email address of the attacker.

(HINT: You can use the filter ***smtp*** to load all the email related traffic. Find the ***Accepted*** response to identify the successful authentication.)

|  |
| --- |
|  |

1. In the message body, what are the data gathered by the attacker. Please also include the value of each data.

|  |  |
| --- | --- |
| Data Gathered (eg: IP Address) | Value |
|  |  |
|  |  |
|  |  |

1. After the email, it will download an executable file which is a GOLROTED malware. Please identify the following:
   1. Domain of the URL where malicious file is downloaded.

|  |
| --- |
|  |

* 1. Using VirusTotal, identify the TrendMicro detection name of the malicious file.

|  |
| --- |
|  |

1. Open ***Spoofed.pcap*** using **Wireshark** and analyze the network traffic of the malware.
2. The attack starts with the malware spoofing different websites including some banking sites. Identify the bank that was accessed by the user. What is the URL?

|  |
| --- |
|  |

1. Once the banking site is successfully accessed, this malware will try to spoof the website. What is the hostname of the C&C server it connects to?

|  |
| --- |
|  |

1. The C&C server will have different paths showing the strings of some of the websites it steals from. (The stolen data will be sent out using different paths depending on the website.) Provide at least three of these websites.

|  |
| --- |
|  |

1. What is/are the value(s) that the malware have stolen from the bank in Question 1? What is the full URL where it sends the stolen data?

|  |
| --- |
|  |