**STATIC MALWARE ANALYSIS RUN BOOK**

**Step 1**:

|  |  |  |
| --- | --- | --- |
| 1 | Download the password protected sample in sandbox | password - Infected |

**Step 2**:

Check for internet connectivity ipconfig

**Step 3**:

Extract compressed sample

**Step 4**:

|  |  |  |
| --- | --- | --- |
| 1 | Check the extension of the file | Tools>Folder option>View>select hide unknown for known file type |

**Step 5:**

Change folder view to details

**Step 6**:

Drag and drop sample to HashCalc

**Step 7:**

|  |  |  |
| --- | --- | --- |
| 1 | Check Hash in virustotal | host machine |

**Step 8:**

|  |  |  |
| --- | --- | --- |
| 1 | Drag and drop sample to ExeinfoPE to unpack file | Executable |

**Step 9:**

|  |  |  |
| --- | --- | --- |
| 1 | Drag and drop packed and unpacked file in BinText | Check for strings |

**Step 10:**

|  |  |  |
| --- | --- | --- |
| 1 | Drag and drop packed and unpacked file in PE Studio | Check for dos header, dos stub, file header, optional header |