**Lab 2 Scenario: Hybrid-Analysis**

**You are given hashes and need to determine if they are malicious.**

您將獲得哈希值，需要確定它們是否是惡意的。

<https://hybrid-analysis.com/#homepage-search-simple>

**Case 1**

SHA256: 8bcbe24949951d8aae6018b87b5ca799efe47aeb623e6e5d3665814c6d59aeae

1. Is this a malicious file? /

這是惡意文件嗎？

Answer / 回答:

2. What is the file name? / 文件名是什麼？

Answer / 回答:

3. Which Operating System is this file made for?

該文件是為哪個操作系統製作的？

Answer / 回答:

4. What are the main categories defined in the Incident Response Risk Assessment? / 事件響應風險評估中定義的主要類別是什麼？

Answer / 回答:

5. How many different types of TTPs (tactics, techniques, and procedures) were found in the MITRE ATT&CK™ Techniques Detection? / 在 MITRE ATT&CK™ 技術檢測中發現了多少種不同類型的 TTP（戰術、技術和程序）？

Answer / 回答:

6. How many Suspicious Indicators were identified for T1056.004 and what are their main categories? / 為 T1056.004 確定了多少個可疑指標，它們的主要類別是什麼？

Answer / 回答:

7. Which compiler was used to create this file? / 使用哪個編譯器創建此文件？

Answer / 回答:

8. What were the File Imports DLLs? / 什麼是文件導入 DLL？

Answer / 回答:

**Case 2**

SHA256: 020f1fa6072108c79ed6f553f4f8b08e157bf17f9c260a76353300230fed09f0

1. Is this a malicious file? /

這是惡意文件嗎？

Answer / 回答:

2. What is the file name? / 文件名是什麼？

Answer / 回答:

3. How many files are associated with this malware? / 有多少文件與此惡意軟件相關聯？

Answer / 回答:

4. What type of malware is this (Windows or Linux)? / 這是什麼類型的惡意軟件（Windows 或 Linux）？

Answer / 回答:

5. What is the MITRE ATT&CK™ Techniques Detection that corresponds with this malware? / 與此惡意軟件對應的 MITRE ATT&CK™ 技術檢測是什麼？

Answer / 回答:

6. How many Malicious Indicators were found and what categories do they fall under? / 發現了多少惡意指標，它們屬於哪些類別？

Answer / 回答:

7. How many Suspicious Indicators were found and what categories do they fall under? 發現了多少可疑指標，它們屬於哪些類別？

Answer / 回答:

8. Where there any extracted strings, and if so, how many? 哪裡有提取的字符串，如果有，有多少？

Answer / 回答: