**Lab 1 Scenario: Cuckoo**

**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://cuckoo.cert.ee/analysis/search/>

**Case 1**

MD5 Hash: 7e947e0c34fb2d16d0fe5ce989f03799

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 Yara rules were detected and what types were detected? / 檢測到多少條 Yara 規則以及檢測到哪些類型？

Answer / 回答:

4. What are the executable files created on the filesystem? /

在文件系統上創建的可執行文件是什麼？

Answer / 回答:

5. How many AntiVirus engines on VirustTotal were identified as malicious? / VirustTotal 上有多少反病毒引擎被識別為惡意？

Answer / 回答:

6. What is the Parent PID for the malicious file? / 惡意文件的父 PID 是什麼？

Answer / 回答:

7. What is the function\_name for the latest LdrGetProcedureAddress? / 最新的 LdrGetProcedureAddress 的 function\_name 是什麼？

Answer / 回答:

8. What are the module\_name(s) for the LdrLoadDll? / LdrLoadDll 的模塊名稱是什麼？

Answer / 回答:

**Case 2**

MD5 Hash: e87ac5f3c3628536df6f97de81ec28ab

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 Yara rules were detected and what types were detected? / 檢測到多少條 Yara 規則以及檢測到哪些類型？

Answer / 回答:

4. In the Cuckoo Log, how many files were uploaded and which had the biggest file length? / 在 Cuckoo Log 中，上傳了多少個文件，哪個文件長度最大？

Answer / 回答:

5. How many events likely contained encrypted or compressed data indicative of a packer and what where they? / 有多少事件可能包含指示加殼程序的加密或壓縮數據以及它們在哪裡？

Answer / 回答:

6. What regkey was unique from the other RegOpenKeyExW that were available? / 什麼 regkey 與其他可用的 RegOpenKeyExW 不同？

Answer / 回答:

7. What is the latest Process and its section\_name? / 最新的進程及其 section\_name 是什麼？

Answer / 回答:

**Case 3**

MD5 Hash: c800c8524d0f2531a6dfdfde2d4948af

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. What was the score for this file? / 這個文件的分數是多少？

Answer / 回答:

4. In the Cuckoo Log, what type of files were part of the Traceback and how did they affect the Cuckoo analysis? /

在布穀鳥日誌中，什麼類型的文件是追溯的一部分，它們如何影響布穀鳥分析？

Answer / 回答:

5. How many AntVirus engine on IRMA found this file to be malicious and which of them were Windows-based? / IRMA 上有多少 AntVirus 引擎發現此文件是惡意的，其中哪些是基於 Windows 的？

Answer / 回答:

6. What do the names from the AntiVirus engine on IRMA suggest the type of malware this file might be? / IRMA 上防病毒引擎的名稱表明該文件可能是何種惡意軟件類型？

Answer / 回答:

Open-ended or Research Questions / 開放式或研究問題:

1. What is an online tool that can identify if hashes, files, or URLs might be malicious? / 什麼是可以識別哈希、文件或 URL 是否可能是惡意的在線工具？

Answer / 回答:

2. Which type of malware analysis looks at the malware without executing it? / 哪種類型的惡意軟件分析只查看惡意軟件而不執行它？

Answer / 回答:

3. What would be an example of a location or tool that could help identify or extract a malicious file? / 可以幫助識別或提取惡意文件的位置或工具的示例是什麼？

Answer / 回答:

4. What would be the Linux command to find the md5 hash of a file? 查找文件的 md5 哈希的 Linux 命令是什麼？

Answer / 回答:

5. What would be the PowerShell command to find the SHA256 hash of a file? / 查找文件的 SHA256 哈希的 PowerShell 命令是什麼？

Answer / 回答: