課題３：マルウェア動的解析ログ分析

[Q3-1] マルウェア動的解析ログからコードインジェクションを行う API コールを分析せよ

・分析対象ログは FFRI Dataset 2017 に含まれている
・コードインジェクションに失敗したことがわかるケースは対象外とすること
・API 名はログに含まれる名称で答えること

分析対象ログ：
[Log1] 7e6e2813ca9fa8dbd79f9dd61f7061daccdec96302a5ad31dcb968ffcdd7c70a.json
[Q3-1-1] コードインジェクション元とインジェクション先の PID およびプロセス名を答えよ
[Q3-1-2] コードインジェクションのためにメモリ確保やコードの書き込みを行う API コールを特定し、動作の概要を説明せよ
[Q3-1-3] コードインジェクションでインジェクトしたコードを実行する API コールを特定し、コード実行方式の概要を説明せよ

[Log2] 7140e68ebe1b3a376560d689b860ec4cd6d5f3a411af2be8d3e8401e873bb937.json
[Log3] cda34f6e5a38e87359569861659ec2a6d843180008498d66bb3f9f4b50b719a3.json
※Log1 と同様に解答すること

■回答例
[3-1-1]
インジェクション元: pid=1234, name=malware.exe
インジェクション先: pid=1238, name=svchost.exe

[3-1-2]
1. NtAllocateVirtualMemory により, pid=1238, name=svchost.exe の 0x40000～0x70000 の領域を確保.
2. WriteProcessMemory により上記領域に書き込み.
3. NtProtectVirtualMemory により上記領域のアクセス権を PAGE_EXECUTE_READ に変更し，実行権限を付与.

[3-1-3]

1. コード挿入後に pid=1238, name=svchost.exe に対し，上記のコード挿入領域内である 0x41280 をエントリポイントとする新規スレッドを CreateRemoteThread により作成. tid は 1240.
2. NtResumeThread により上記スレッドの実行を開始.

[Q3-2] FFRI Dataset 2017 に含まれるマルウェア動的解析ログを分析し、Sandbox Fingerprinting と考えられる API コールを列挙せよ

Sandbox Fingerprinting と考えられる挙動について次の情報を答えよ
・挙動の概要説明（例: Cuckoo Sandbox 固有の .py のファイルの存在確認）
・当該 API コールを含むログファイル名
・当該 API コールを含む PID, プロセス名
・API コール（Cuckoo Sandbox の signature 化を想定し、API コールの流れやパラメータを具体的に記載すること）

ただし、下記の点を考慮すること
・分析対象ログは FFRI Dataset 2017 全てとする
・Cuckoo Sandbox の signature として実装済みのパターンは対象外とする
・挙動は 3 パターンまでとする。概要・API コールが同じ挙動を複数回答しても無効
・API 名 はログに含まれる名称で答えること

[Q3-3] 実践的な研究をするためにはどんなデータセットが必要か？

解答

以下の URL にアクセスし、11:55 までに Google フォームから解答を提出すること。
https://goo.gl/forms/z5pTKc2OFtUQUGPu2

解答の提出には Google へのログインが必要です。
提出(Google フォームの送信)は基本的に一度で行うようにすること。
同一アカウントからの複数回の回答提出は不可です(編集は可能)