課題3

株式会社ＦＦＲＩ
http://www.ffri.jp

Ver 2.00.01

担当及び課題作成協力者

- 課題作成協力者
  - 大月勇人　　立命館大学
  - 市田達也　　（株）リクルートテクノロジーズ
  - 桑原和也　　デジタルアーツ（株）

- 担当
  - 村上純一　　（株）FFRI

※http://www.iwsec.org/mws/2015/committee.html

課題3の狙い

- マルウェアの動的解析データ(FFRI Dataset 2015)を対象としたデータ、データ群の分析

- 課題解決を通して人手での分析ではなくデータを処理するプログラム等の仕組み、技術の確立を促す

課題３　マルウェア動的解析　設問1　（問題文）

FFRI Dataset 2015中に含まれる
ハッシュ値(1)～(8)の検体に関して，

APIログに基づいて，プロセスを生成しうる挙動を解析せよ.

生成されたプロセスのうち，
processtree に現れていないものを列挙し，

それぞれ下記の3点について説明せよ.

1. だれが　2. どのように　3. なにを起動したか

ただし，下記の点を考慮すること.

- プロセスとして動作するサービスについても対象とすること.
- スクリプトを実行する挙動が含まれる場合，
  スクリプト内で実行される見込みのプログラム(外部コマンド)，
  DOSコマンド等の内部コマンドについてもそれぞれ記載すること.
- 確実に失敗したことがわかる挙動は除外すること.

processtree の例


```
"processtree": [
        {
            "parent_id": 1884,
            "pid": 3172,
            "children": [
                {
                    "parent_id": 3172,
                    "pid": 3552,
                    "children": [
                        {
                            "parent_id": 3552,
                            "pid": 3808,
                            "children": [],
                            "name": "svchost.exe"
                        }
                    ],
                    "name": "explorer.exe"
                }
            ],
            "name": "0E644D290D01866EA2DA95BF373EC0B2B30DE491"
        }
    ],
```

APIログの例

```
"processes": [
  {
    "parent_id": 1884,
    "process_name": "0E644D290D01866EA2DA95BF373EC0B2B30DE491",
    "process_id": 3172,
    "first_seen": "2015-05-21 08:53:59,781",
    "calls": [
      (略)
      {
        "category": "process",
        "status": true,
        "return": "0x00000001",
        "timestamp": "2015-05-21 08:54:00,093",
        "thread_id": "3176",
        "repeated": 0,
        "api": "CreateProcessInternalW",
        "arguments": [
          {
            "name": "ApplicationName",
            "value": "C:\\Windows\\syswow64\\explorer.exe"
          },
          (略)
```

1. だれが

成功

2. どのように

3. なにを起動したか

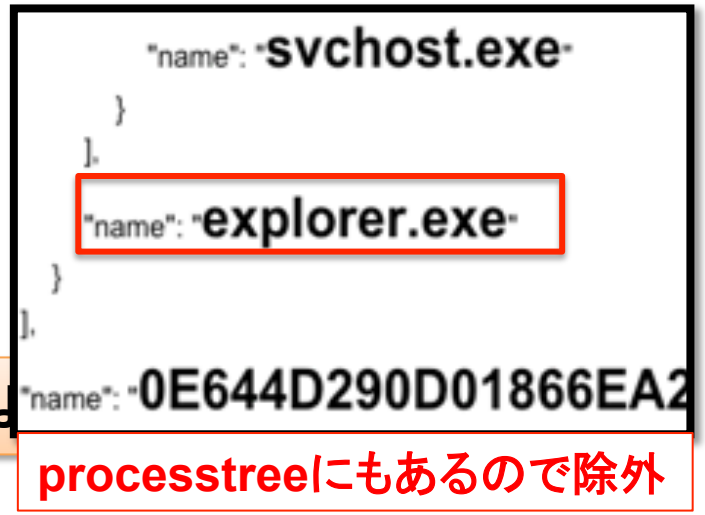
APIログの例

```
"processes": [
  {
    "parent_id": 1884,
    "process_name": "0E644D290D01866EA2DA95BF373EC0B2B30DE491",
    "process_id": 3172,
    "first_seen": "2015-05-21 08:53:59,781",
    "calls": [
      (略)
      {
        "category": "process",
        "status": true,
        "return": "0x00000001",
        "timestamp": "2015-05-21 08:54:00,093",
        "thread_id": "3176",
        "repeated": 0,
        "api": "CreateProcessInternalW",
        "arguments": [
          {
            "name": "ApplicationName",
            "value": "C:\\Windows\\syswow64\\explorer.exe"
          },
          (略)
```

1. だれが

成功

2. どのよ



processstreeにもあるので除外

3. なにを起動したか

課題３　マルウェア動的解析　設問1　（問題文）

FFRI Dataset 2015中に含まれる
ハッシュ値(1)～(8)の検体に関して，

APIログに基づいて，プロセスを生成しうる挙動を解析せよ.

生成されたプロセスのうち，
processtree に現れていないものを列挙し，

それぞれ下記の3点について説明せよ.

1. だれが　2. どのように　3. なにを起動したか

ただし，下記の点を考慮すること.

- プロセスとして動作するサービスについても対象とすること.
- スクリプトを実行する挙動が含まれる場合，
  スクリプト内で**実行される見込み**のプログラム(外部コマンド)，
  DOSコマンド等の内部コマンドについてもそれぞれ記載すること.
- 確実に失敗したことがわかる挙動は除外すること.

課題３　マルウェア動的解析　設問２　（問題文）

FFRI Dataset 2015中に含まれる以下のファイル名を保有する**50**検体に関してその解析ログに基づき、当該マルウェアが実行できた機能を「機能一覧」から全て抽出し、該当する場合は「1（半角イチ）」、該当しない場合は「0（半角ゼロ）」にて

添付の表「submit_answer.csv」にフラグをつけて提出してください。

なお、分析中における下の通信については分析対象外とします（存在しない通信として扱う）。
・宛先IPアドレスが111.22.34.0/24の通信
・マルウェアが通信したのではない、Windows 8.1のデフォルト通信

課題３　マルウェア動的解析　設問２　（機能一覧）

【機能一覧】

A.検体自身の削除

B.端末情報の取得

C.他プロセスへのコード/DLL注入

D.取得した情報の外部送信

E.レジストリを利用した自動起動登録

F.タスクスケジューラを利用した自動起動登録

G.サービスを利用した自動起動登録

H.DoS攻撃の実行

I.P2Pによる外部ホストとの通信

J.レジストリを利用したInternet Explorerにおけるホームページ、スタートページの変更

K.他ファイルのドロップ（マルウェアファイル名の検体自身を除く）

L.外部へのメール送信

M.IRCによる外部ホストとの通信

N.レジストリを利用したInternet ExplorerにおけるProxy設定の変更

O.アンチウイルスソフトの停止または起動妨害

P.インストール済みアプリケーション一覧の取得

Q.Windows Update自動更新の停止

R.Windows Firewallの設定確認および変更の試み

S.キーロギングの実行

T.画面キャプチャの実行(プライマリモニタにおけるキャプチャ画面指定とデバイスコンテキストの取得までを対象)

U.HTTPによる外部ホストとの通信(OSデフォルト通信は除き、マルウェアが意図して通信したと考えられるものを対象)

V.hostsファイルの書き換え

W.自ファイルのコピー作成

X.ファイルの探索

Y.Explorerの設定確認および変更の試み

A~Zまでの全２６機能

課題３　マルウェア動的解析　設問２　（目的と着眼点）

目的

マルウェアの有する悪意のある機能の全体を理解することで、動的解析時の幅広い基礎を身に着ける。

50検体という人力では難しい分量に対しツールによる自動化に挑戦させる

着眼点

オープンソースのCuckooサンドボックスのログ構造を理解し、適切なログを抽出

問題文・各機能の意味を正確に理解し、ログが表現する範囲を考慮する

ヒント１：ログのどの部分に注目するべきか考えよう！

- virustotal、static、**behavior、dropped、network、behavior、・・・**
- 判定には１プロセスのみで良い、それともスレッドを追うべきか

ヒント２：実際にマルウェアが実行している挙動とは何かを考えよう！

- レジストリは**「呼び出し」**だけで良い？
- API実行時の状態は
- その他、何を持って実行していると判断できる

ヒント３：26の挙動は全て判定できるものか考えよう

- **「API」、「レジストリ」**以外に判定出来る要素はあるのか
- 閾値や独自の定義を利用した場合は本当にそれが正しいといえるのか