



MWS Cup 課題3

株式会社 F F R I
<http://www.ffri.jp>



課題作成者

- NTTセキュアプラットフォーム研究所
- NTTセキュリティ・ジャパン株式会社
- 株式会社FFRI

大月勇人

森下知哉

村上純一



Agenda

- 課題3
 - 概要及び狙い
 - FFRI Dataset概要
 - 課題3-1
 - 課題3-2

課題3 / 概要及び狙い

■ 概要

FFRI Datasetを題材としたマルウェア動的解析ログの分析

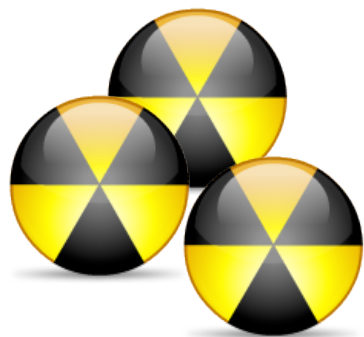
■ 狙い

(課題3-1)マルウェア動的解析ログの構造理解、目視・手動分析

(課題3-2)構造理解した上での大量データの自動処理

課題3 / FFRI Dataset 概要

- FFRIで収集したマルウェアの動的解析ログ
 - 2016/1-3に収集された検体、計8,243 x 2(Win8.1/10)
 - PE形式かつ実行可能なもの
 - 10ベンダー以上でマルウェア判定を受けているもの



FFRI保有検体



Cuckoo Sandbox

動的解析



解析ログ

(参考) 具体的なデータ項目

項目 (大見出し)	内容
info	解析の開始、終了時刻、id等 (idは1から順に採番)
signatures	ユーザー定義シグニチャとの照合結果 (今回は使用無)
virustotal	VirusTotalの検査履歴との照合結果 (検体のMD5値に基づく)
static	検体のファイル情報 (インポートAPI、セクション構造等)
dropped	検体の実行時に生成したファイル
behavior	検体実行時のAPIログ (PID、TID、API名、引数、返回值等)
processtree	検体実行時のプロセスツリー (親子関係)
summary	検体の実行時にアクセスしたファイル、レジストリ等の概要情報
target	解析対象検体のファイル情報 (ハッシュ値等)
debug	検体解析時のCuckoo Sandboxのデバッグログ
strings	検体中に含まれる文字列情報
network	検体の実行時に行った通信の概要情報

(参考) 具体的なデータ項目(behavior)

```
{ "category" => "process",  
  "status" => 1,  
  "stacktrace" => [],  
  "api" => "NtAllocateVirtualMemory",  
  "return_value" => 0,  
  "arguments" =>  
    { "base_address" => "0x02ed0000",  
      "region_size" => 4096,  
      "process_handle" => "0xffffffff",  
      "protection" => 4,  
      "allocation_type" => 4096 },  
  "time" => 1461637335.935775,  
  "tid" => 3000,  
  "flags" =>  
    { "protection" => "PAGE_READWRITE",  
      "allocation_type" => "MEM_COMMIT" } },
```

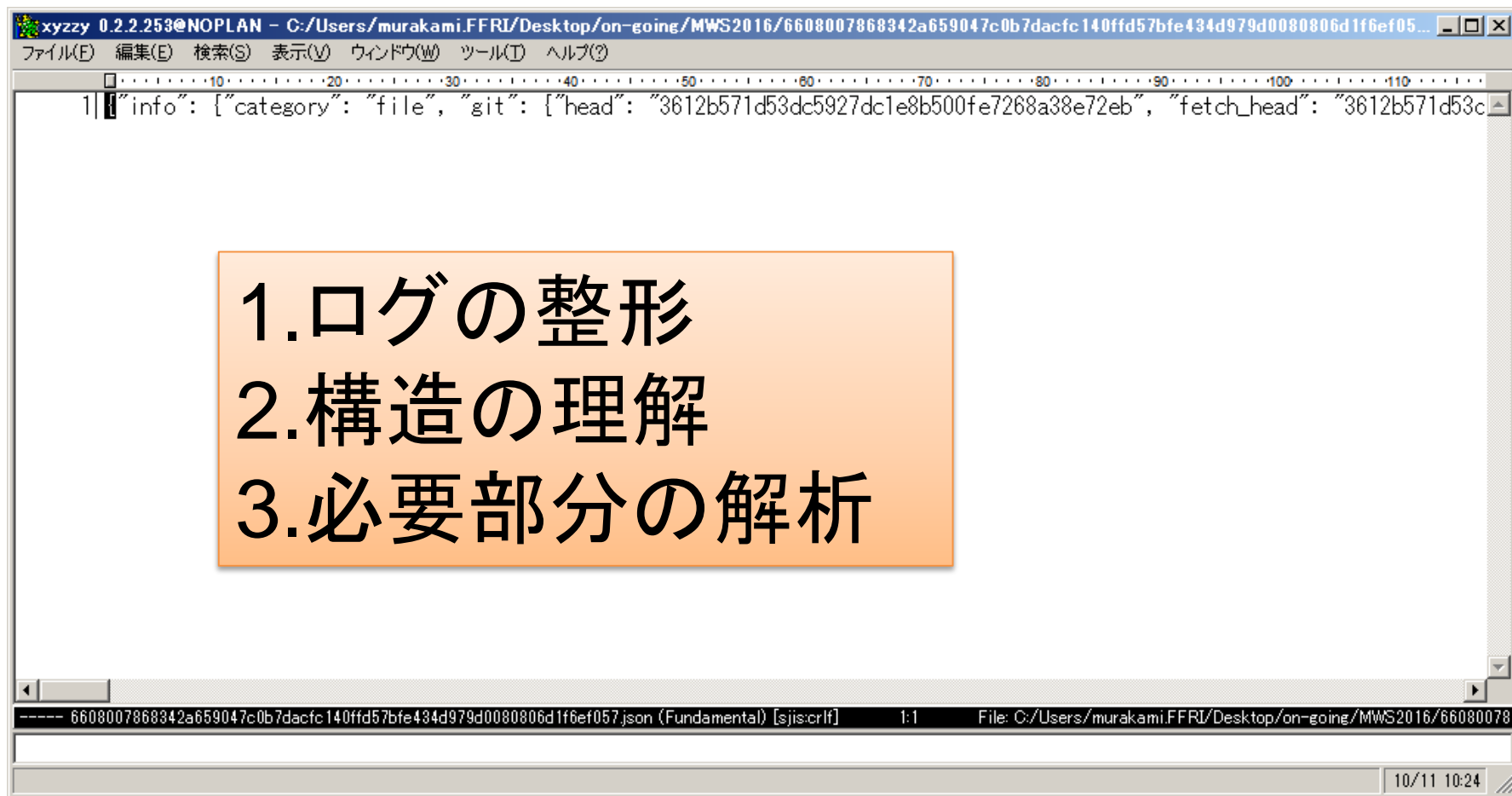
課題3 / 課題3-1

- FFRI Dataset中の指定した3つの検体ログに関して他プロセスへのコードインジェクションと考えられる挙動を解析

(1) bd2953e64396acb23d9d484a58ccb9a95d12b5d897a399448a39fb170fa34ad8
(2) 5096dda2bf508cd6932484e862325fc67802985e6c8b0af22ea6a4d49fd3b820
(3) 15d65de0fd47a3deb5fb390050283d81b56235b2a77ac9ae97d71714cff7f76

- 当該挙動について以下を明らかにする
 - コード挿入元プロセス情報 (PID、プロセス名)
 - コード挿入先プロセス情報 (PID、プロセス名)
 - コードの挿入方法
 - 挿入コードの実行開始方法

実際のFFRI Dataset(json形式)

A screenshot of a terminal window. The title bar reads "xyzyy 0.2.2.253@NOPLAN - C:/Users/murakami.FFRI/Desktop/on-going/MWS2016/6608007868342a659047c0b7dacfc140ffd57bfe434d979d0080806d1f6ef05...". The menu bar includes "ファイル(F)", "編集(E)", "検索(S)", "表示(V)", "ウインドウ(W)", "ツール(T)", and "ヘルプ(?)". The main area shows a single line of JSON data:

```
1|{"info": [{"category": "file", "git": [{"head": "3612b571d53dc5927dc1e8b500fe7268a38e72eb", "fetch_head": "3612b571d53c
```

1. ログの整形
2. 構造の理解
3. 必要部分の解析

課題3 / 課題3-2

- 2つの検体ログを新たに提供（FFRI Dataset未収録）
- 上記の亜種と考えられる検体をDataset中の指定した50件の検体ログから見つけ出し、根拠とともに回答する
- APIコールログを共通性判断の材料とする
（回答例）
 - ハッシュ値：84799a9a……
 - 根拠：XXX APIが XXX に XXX をしている

ハッシュ値、根拠ともに全て回答すること（部分点あり）