FFRI Dataset 2013のご紹介

Fourteenforty Research Institute, Inc.
株式会社 フォティーンフォティ技術研究所
http://www.fourteenforty.jp

Agenda

- FFRI Dataset 2013概要
- Cuckoo Sandbox
- 具体的なデータ項目
- データの利用例

FFRI Dataset 2013の概要

- FFRIで収集したマルウェアの動的解析ログ
  - 2012/9～2013/3に収集された検体
  - PE形式かつ実行可能なもの
  - 約2600検体分（ログファイル計1.7GB)

- 下記の3検体の解析ログを同梱
  - 遠隔操作マルウェア/ MITBマルウェア / 韓国MBR破壊マルウェア

Cuckoo Sandbox - http://www.cuckoosandbox.org

- オープンソース（一部非公開）のマルウェア解析システム
  - 仮想環境内でマルウェアを実行
  - 実行時のふるまいをモニタリング
  - VirusTotal連携、yara連携等
- 社内のマルウェア解析用ネットワークにシステムを設置、実行
  - 1検体当り90秒実行
- 1検体（解析対象） 1ログファイル
  - ログファイルは、json形式

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）
yara	yara(OSSのマルウェア検知・分類エンジン）の標準ルールとの照合結果 - https://code.google.com/p/yara-project/
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	検体が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、返り値等）
processtree	検体実行時のプロセスツリー（親子関係）
summary	検体が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	検体が実行時に行った通信の概要情報

具体的なデータ項目(info)


```
"info": {
        "category": "file",
        "started": "2013-03-05 00:59:26",
        "ended": "2013-03-05 01:00:57",
        "version": "0.5",
        "duration": "90 seconds",
        "id": 1
    },
```

具体的なデータ項目(yara)

```
"yara": [
        {
            "meta": {
                "description": "Matched shellcode byte patterns",
                "author": "nex"
            },
            "name": "shellcode",
            "strings": [
                "{ 8B EC 81 EC }",
                "{ 8B EC E9 }"
            ]
        }
    ],
```

具体的なデータ項目(virustotal)


```
"scans": {
        "MicroWorld-eScan": {
            "detected": true,
            "version": "12.0.250.0",
            "result": "Gen:Variant.Symmi.13832",
            "update": "20130221"
        },
        "nProtect": {
            "detected": false,
            "version": "2013-02-20.01",
            "result": null,
            "update": "20130220"
        },
```

具体的なデータ項目(static)


```
"static": {
        "pe_imports": [
            {
                "imports": [
                    {
                        "name": "CoCreateInstance",
                        "address": "0x1000a280"
                    }
                ],
                "dll": "ole32.dll"
            },
```

具体的なデータ項目(static)


```
"pe_sections": [
        {
            "size_of_data": "0x8a00",
            "virtual_address": "0x1000",
            "entropy": 6.703983306682313,
            "name": ".text",
            "virtual_size": "0x89b3"
        },
```

具体的なデータ項目(dropped)


```
"dropped": [
    {
        "size": 1499136,
        "sha1": "3070831b756bacc31f798c96fc430d3fdd974cfb",
        "name": "shdocvw.dll",
        "type": "PE32 executable (DLL) (GUI) Intel 80386, for
        "crc32": "E511A8A9",
        "ssdeep": null,
        "sha256": "d0ad6ed837de4968f3bf93c5053619f02a88
        "sha512": "393bd0f4d64b5ee927ea3ef7bfca639097c8
        "md5": "796eb88d9546ac489b7fec7795760e0f"
    },
```

具体的なデータ項目(behavior)


```
{
                "category": "system",
                "status": "SUCCESS",
                "return": "0x00000000",
                "timestamp": "2013-03-28 11:05:08,885",
                "thread_id": "1384",
                "repeated": 0,
                "api": "NtClose",
                "arguments": [
                    {
                        "name": "Handle",
                        "value": "0x000000b0"
                    }
                ]
            },
```

具体的なデータ項目(processtree)


```
"processtree": [
        {
            "pid": 1436,
            "name": "CD51605CE8F0CA9A6B536CFAD85CDF3B.bin",
            "children": [
                {
                    "pid": 1296,
                    "name": "rundll32.exe",
                    "children": []
                }
            ]
        }
    ],
```

具体的なデータ項目(summary)


```
"summary": {
        "files": [
            "c:¥¥autoexec.bat",
            "C:¥¥Documents and Settings",
            "C:¥¥Documents and Settings¥¥cuckoo1¥¥Local Settings",
            "C:¥¥Documents and Settings¥¥cuckoo1¥¥Application Data¥¥btacp.dll",
            "C:¥¥Documents and Settings¥¥cuckoo1¥¥Application Data¥¥btacp.dll.123.Manifest",
            "C:¥¥WINDOWS¥¥system32¥¥msctfime.ime",
            "C:¥¥WINDOWS¥¥Registration¥¥R000000000007.clb",
            "C:¥¥WINDOWS¥¥system32¥¥shdocvw.dll",
            "C:¥¥WINDOWS¥¥system32¥¥stdole2.tlb"
        ],
        "keys": [
            "HKEY_LOCAL_MACHINE¥¥Software¥¥Microsoft¥¥Rpc¥¥PagedBuffers",
```

具体的なデータ項目(target)


```
"target": {
      "category": "file",
      "file": {
          "size": 155136,
          "sha1": "387ed6c3690aff95dbeff449c91a3dd9323a530a",
          "name": "CD51605CE8F0CA9A6B536CFAD85CDF3B.bin",
          "type": "PE32 executable (GUI) Intel 80386, for MS Windows",
          "crc32": "FE038869",
          "ssdeep": null,
          "sha256": "21f421c07dd47fc45a7e908abf3e2d9c687ba194af32a
          "sha512": "8053b0d68154b2bd4681abc1509736b480b197030ac
          "md5": "cd51605ce8f0ca9a6b536cfad85cdf3b"
      }
  },
```

具体的なデータ項目(strings)

```
"strings": [
        "!This program cannot be run in DOS mode.",
        "`.rdata",
        "@.data",
        "t@Jt0Jt¥u001fJt",
        "t)9>t%G",
        "Ht5Ht'HHt",
```

具体的なデータ項目(network)


```
"network": {
      "udp": [
         {
            "dport": 53,
            "src": "111.22.33.251",
            "dst": "111.22.33.1",
            "sport": 1054
         },
       "http": [
         {
            "body": "",
            "uri": "http://xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx
            "user-agent": "Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1)",
            "method": "GET",
            "host": “xxxxxxxxxxxxxxxxxxxxxxxxx",
            "version": "1.1",
```

データの利用例

- マルウェア検知・分類
  - ヒューリスティック検知
  - 傾向分析
  - クラスタリング

- ベンチマーク
  - 自身の自動解析システムとの比較、有効性検証