FFRI Dataset 2016のご紹介

株式会社ＦＦＲＩ
http://www.ffri.jp

Ver 2.00.01

Agenda

- FFRI Dataset 2016概要
- Cuckoo Sandbox
  - 具体的なデータ項目
- データの利用例

FFRI Dataset 2016の概要

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

- ＋FFRI Dataset 2013, 2014, 2015
  - 2013: Cuckoo ログファイル約2600検体分
  - 2014: Cukcoo 及びFFR yarai analyzer professionalログファイル3000検体分
  - 2015: Cuckoo ログファイル3000検体分

（補足）FFRIの検体収集の取り組み

- 独自のWeb Crawlingによる収集
  - Web感染型、Web上で配布されているマルウェア等
- 他ベンダとの検体交換

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
  - Windows 8.1(x64)
  - Windows 10(x64)

- 1検体（解析対象） 1ログファイル
  - ログファイルは、json形式
  - 一検体90秒実行

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",
   "version"=>"2.0-dev",
   "package"=>"",
   "started"=>1461437853.0,
   "route"=>"none",
   "custom"=>"",
   "machine"=>
    {"status"=>"stopped",
     "name"=>"mws2016_81",
     "started_on"=>"2016-04-23 18:57:33",
     "manager"=>"VirtualBox",
     "label"=>"mws2016_81",
     "shutdown_on"=>"2016-04-23 18:57:54"},
```

具体的なデータ項目(virustotal)


```
"virustotal"=>
 {"scan_id"=>
   "00e0777f2b82263f93f28756f81eb1fdcc1eb00558d4a61458047105",
  "sha1"=>"3d0dba16ef66f026229477308b4b42593e36c4f1",
  "resource"=>"e53a0e6ae338ec4e8d7b2ab6642c1bd4",
  "verbose_msg"=>"Scan finished, information embedded",
  "response_code"=>1,
  "scan_date"=>"2016-03-15 13:05:05",
  "permalink"=>
   "https://www.virustotal.com/file/00e0777f2b82263f93
  "summary"=>
   {"positives"=>37,
    "permalink"=>      "https://www.virustotal.com/file/00e0777f2b82263f
    "scan_date"=>"2016-03-15 13:05:05"},
```

具体的なデータ項目(virustotal)

```
"scans"=>
  {"Bkav"=>
    {"detected"=>false,
     "version"=>"1.3.0.7744",
     "update"=>"20160312",
     "result"=>nil,
     "normalized"=>[]},
   "TotalDefense"=>
    {"detected"=>false,
     "version"=>"37.1.62.1",
     "update"=>"20160315",
     "result"=>nil,
     "normalized"=>[]},
```

具体的なデータ項目(static)


```
{"pdb_path"=>nil,
  "pe_imports"=>
   [{"imports"=>
      [{"name"=>nil, "address"=>"0x403018"},
…
     "dll"=>"MFC42.DLL"},
{"imports"=>
      [{"name"=>"__getmainargs", "address"=>"0x4031c8"},
       {"name"=>"_initterm", "address"=>"0x4031cc"},
…
 "peid_signatures"=>["Armadillo v1.71"],
  "keys"=>[],
  "imported_dll_count"=>4,
  "pe_timestamp"=>"2016-02-08 13:08:14",
  "pe_exports"=>[],
  "signature"=>[],
  "pe_imphash"=>"0e9ca07c574ad39fb99fb3033c1192fd",
```

具体的なデータ項目(static)


```
"pe_sections"=>
   [{"size_of_data"=>"0x00002000",
     "virtual_address"=>"0x00001000",
     "entropy"=>4.52906442766945,
     "name"=>".text",
"virtual_size"=>"0x00001495"},
    {"size_of_data"=>"0x00001000",
     "virtual_address"=>"0x00003000",
     "entropy"=>4.200849088316575,
     "name"=>".rdata",
     "virtual_size"=>"0x00000cb2"},
```

具体的なデータ項目(dropped)


```
"dropped"=>
 [{"yara"=>[],
   "sha1"=>"a24a6280eb25c8217631eb223c40f5ccaff783bd",
   "name"=>"c8ef05d267dfabd2_9ZzgFDcw9M",
   "sha512"=>
    "e19f56462a43ac9b144935d339f154b24746e3b8472f28894319dfb6fe3b80e2f342cca33789
   "urls"=>[],
   "crc32"=>"6BDB80EF",
   "path"=>
    "/home/cuckoo/cuckoo/storage/analyses/6703/files/c8ef05d267dfabd2_9ZzgFDcw9M",
   "ssdeep"=>
    "49152:Pq3pd94XRYVfHQK5rCO/puBMlsUDiVFxMT9SC0Mv/AMb2jrP65pAB3i3ZXb7Pe/G:
   "sha256"=>
    "c8ef05d267dfabd24bcb892466cbeb08750fd0e8087cf9e64927b71939512d2c",
   "type"=>"data",
   "md5"=>"2ddc28719b953f3ebc5e6a7453ab2455",
   "size"=>3188224},
```

具体的なデータ項目(behavior)

```
 "behavior"=>
  {"generic"=>
    [{"ppid"=>2480,
      "first_seen"=>1461637335.231775,

"process_name"=>"E73996EE0CA1B81E97517B492EA9DE73D1.exe",
      "pid"=>1096,
      "summary"=>
       {"file_created"=>
         ["C:¥¥Users¥¥rihoko¥¥AppData¥¥Local¥¥Temp¥¥132390",
          "C:¥¥Users¥¥rihoko¥¥AppData¥¥Local¥¥Temp¥¥51997",
…
       },
 // file_recreated, regkey_written, dll_loaded, file_opened, etc.
```

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"}},
```

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(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"=>
  {"tls"=>
    [{"server_random"=>

"ce575bf410e9638abdde89fa3369d896626c6db100a678e8d2121c87f3445a34",
       "session_id"=>""}],
   "udp"=>
    [{"src"=>"192.168.0.3",
      "dst"=>"192.168.0.255",
      "offset"=>1554044,
      "time"=>3.311015129089355 5,
      "dport"=>137,
      "sport"=>137},
```

具体的なデータ項目(network)


```
"http"=>
   [{"count"=>1,
     "body"=>"",
     "uri"=>
      "http://ctldl.windowsupdate.com/msdownload/updat…",
     "user-agent"=>"Microsoft-CryptoAPI/6.3",
     "port"=>80,
     "host"=>"ctldl.windowsupdate.com",
     "version"=>"1.1",
     "path"=>
      "/msdownload/update/v3/sta…",
     "data"=>
      "GET
/msdownload/update/v3/static/trustedr/en/disallowedcertstl.cab?761e54e3dd3e5c11
HTTP/1.1¥r¥nConnection: Keep-Alive¥r¥nAccept: */*¥r¥nUser-Agent: Microsoft-Cry
     "method"=>"GET"},
```

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
- 悪性通信の検出
  - 識別情報の外部送信検知(hostname, username, GUI等)
- 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
- 動作プラットフォームにおける振る舞いの差異