FFRI Dataset 2017のご紹介

株式会社ＦＦＲＩ
http://www.ffri.jp

Ver 2.00.01

Agenda

- FFRI Dataset 2017概要
- Cuckoo Sandbox
  - 具体的なデータ項目
- データの利用例

FFRI Dataset 2017の概要

- FFRIで収集したマルウェアの動的解析ログ
  - 2017/3～2017/4に収集された検体、計6,251件
  - PE形式かつ実行可能なもの
  - 15ベンダー以上でマルウェア判定を受けているもの

- ＋FFRI Dataset 2013, 2014, 2015, 2016
  - 2013: Cuckoo ログファイル約2600検体分
  - 2014: Cukcoo、FFR yarai analyzer professionalログファイル約3000検体分
  - 2015: Cuckoo ログファイル約3000検体分
  - 2016: Cuckoo ログファイル約8000検体分

（補足）FFRIの検体収集の取り組み

- VirusTotalを用いた収集
- 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 7 x86
- 1検体（解析対象） 1ログファイル
  - ログファイルは、json形式
  - 一検体最大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
signatures	ユーザー定義シグニチャとの照合結果
virustotal	VirusTotalから得られる情報
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、動作概要等）
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": {
    "route": "none",
    "package": "",
    "ended": 1493813568.183504,
    "version": "2.0.1",
    "custom": "",
    "machine": {
        "status": "stopped",
        "manager": "VirtualBox",
        "started_on": "2017-05-03 12:10:59",
        "name": "cuckoo1",
        "label": "guest",
        "shutdown_on": "2017-05-03 12:12:47"
    },
    "added": 1493811716.636417,
    "category": "file",
    "score": 7.4,
```

具体的なデータ項目(virustotal)


```
"virustotal": {
    "scan_id": "0381289278306e3c27238d525e44c13166c8d7bcd706890…
    "tags": [
        "nsis",
        "peexe",
        "overlay"
    ],
    "resource": "0381289278306e3c27238d525e44c13166c8d7bcd70689…
    "ssdeep": "6144:un/L+D97+9OlOrv2ZJnI+pjOu/Smp5LBfdjB3XUx0Xz…
    "additional_info": {
        "trid": "NSIS - Nullsoft Scriptable Install System (94.…
        "f-prot-unpacker": "NSIS",
        "imports": {
        "USER32": [
            "CharPrevA",
            "GetMessagePos",
            "EndPaint",
```

具体的なデータ項目(virustotal)


```
"scans": {
    "Tencent": {
        "version": "1.0.0.1",
        "detected": true,
        "result": "Win32.Trojan.Zerber.Anfq",
        "update": "20170215"
    },
    "AVware": {
        "version": "1.5.0.42",
        "detected": true,
        "result": "Trojan.Win32.Generic!BT",
        "update": "20170215"
    },
    "Emsisoft": {
        "version": "4.0.0.834",
        "detected": true,
        "result": "Trojan.GenericKD.4308690 (B)",
```

具体的なデータ項目(static)


```
"static": {
    "keys": [],
    "pe_resources": [
        {
            "offset": "0x0002e238",
            "filetype": "data",
            "language": "LANG_ENGLISH",
            "name": "RT_BITMAP",
            "size": "0x00000368",
            "sublanguage": "SUBLANG_ENGLISH_US"
        },
        {
            "offset": "0x0002e5a0",
            "filetype": "data",
            "language": "LANG_ENGLISH",
            "name": "RT_ICON",
            "size": "0x000002e8",
```

具体的なデータ項目(static)


```
"pe_sections": [
    {
        "virtual_size": "0x000061c2",
        "name": ".text",
        "virtual_address": "0x00001000",
        "entropy": 6.433093603961752,
        "size_of_data": "0x00006200"
    },
    {
        "virtual_size": "0x0000121e",
        "name": ".rdata",
        "virtual_address": "0x00008000",
        "entropy": 4.986436199642432,
        "size_of_data": "0x00001400"
    },
    {
        "virtual_size": "0x0001bc38",
```

具体的なデータ項目(dropped)


```
"dropped": [
    {
        "sha1": "c9d10f6bc29c5138eb4497b085a45b22cc05eea5",
        "sha256": "cf6efc2b7989f2868c223d6b63b578f16341633f418c…
        "sha512": "fed807c147f7c73a0fc791604907d26d5cafa35a49e5…
        "name": "cf6efc2b7989f286_zcbrmqmkks.9212",
        "size": 17873,
        "filepath": "c:¥¥tmp8t2cjf¥¥lib¥¥api¥¥zcbrmqmkks.9212",
        "path": "/home/john/.cuckoo/storage/analyses/103/files/…
        "crc32": "C893B883",
        "yara": [],
        "urls": [
            "http://www.cuckoosandbox.org"
        ],
        "type": "data",
        "md5": "716100f52756526fc0cf15db1085f9aa",
        "ssdeep": null,
```

具体的なデータ項目(behavior)


```
"behavior": {
    "apistats": {
        "3540": {
            "RegQueryValueExA": 1,
            "GetNativeSystemInfo": 1,
            "NtClose": 197,
            "GetFileSizeEx": 12,
            "NtGetContextThread": 1,
            "LoadStringW": 1,
            "CoUninitialize": 16,
            "GetFileSize": 2,
            "NtQueryValueKey": 7,
            "NtOpenKey": 28,
            "SetFileTime": 2,
            "FindResourceExW": 2,
            "CreateDirectoryW": 12,
            "RtlDecompressBuffer": 1,
```

具体的なデータ項目(behavior)


```
"processtree": [
    {
        "children": [],
        "process_name": "lsass.exe",
        "command_line": "C:¥¥Windows¥¥system32¥¥lsass.exe",
        "track": false,
        "pid": 492,
        "ppid": 376,
        "first_seen": 1493811724.752586
    },
    {
        "children": [
            {
                "children": [
                    {
                        "children": [],
                        "process_name": "mshta.exe",
```

具体的なデータ項目(behavior)


```
"summary": {
    "regkey_deleted": [
        "HKEY_CURRENT_USER¥¥Software¥¥Microsoft¥¥Windows¥¥C…
        "HKEY_LOCAL_MACHINE¥¥SOFTWARE¥¥Microsoft¥¥Windows¥¥…
        "HKEY_LOCAL_MACHINE¥¥SOFTWARE¥¥Microsoft¥¥Windows¥¥…
        "HKEY_CURRENT_USER¥¥Software¥¥Microsoft¥¥Windows¥¥C…
    ],
    "file_opened": [
        "C:¥¥Users¥¥Smith¥¥AppData¥¥Local¥¥Microsoft¥¥Windo…
        "c:¥¥tmp8t2cjf¥¥lib¥¥core¥¥",
        "c:¥¥Users¥¥Public¥¥documents¥¥",
        "c:¥¥tmp8t2cjf¥¥modules¥¥packages¥¥pub.py",
        "C:¥¥Users¥¥Smith¥¥AppData¥¥Roaming¥¥Microsoft¥¥Win…
        "C:¥¥",
        "C:¥¥Users¥¥Smith¥¥AppData¥¥Roaming¥¥Microsoft¥¥Win…
        "c:¥¥PerfLogs¥¥",
        "c:¥¥Users¥¥Smith¥¥Desktop¥¥gndikchadqgjpza.ppt",
```

具体的なデータ項目(behavior)


```
"calls": [
    {
        "tid": 3544,
        "status": 1,
        "time": 1493811728.057385,
        "return_value": 32775,
        "category": "system",
        "stacktrace": [],
        "arguments": {
            "mode": 32769
        },
        "flags": {
            "mode": "SEM_FAILCRITICALERRORS|SEM_NOOPENFILEE…
        },
        "api": "SetErrorMode"
    },
    {
```

具体的なデータ項目(target)


```
"target": {
    "file": {
    "sha1": "27f6b7c6ef8c1aefe3eb9e0792e3008d5d535c30",
    "ssdeep": null,
    "sha512": "04813bb0d21b82ff0f92b9e013aa4e61c1f6c408591be43e…
    "name": "0381289278306e3c27238d525e44c13166c8d7bcd706890c44…
    "size": 296373,
    "sha256": "0381289278306e3c27238d525e44c13166c8d7bcd706890c…
    "path": "/home/john/.cuckoo/storage/binaries/0381289278306e…
    "crc32": "512B0DAF",
    "yara": [],
    "urls": [
        "http://nsis.sf.net/NSIS_Error"
    ],
        "md5": "ec96d9fea732cec91dfd9beabeab3bd9",
        "type": "PE32 executable (GUI) Intel 80386, for MS Wind…
    },
```

具体的なデータ項目(strings)

```
"strings": [
    "!This program cannot be run in DOS mode.",
    "iRichu",
    "`.rdata",
    "@.data",
    ".ndata",
    " s495l[B",
    "Instu`",
    "softuW",
    "NulluN",
    "j@Vh`[B",
    "D$,SPS",
    "D$$+D$",
    "D$,+D$$P",
    "PPPPPP",
    "@PWSh(",
    "<¥u001fv¥"PhX",
```

具体的なデータ項目(strings)


```
"network": {
    "smtp": [],
    "http": [],
    "icmp": [
        {
            "dst": "192.168.56.111",
            "type": 3,
            "src": "149.202.255.113",
            "data": ""
        },
        {
            "dst": "192.168.56.111",
            "type": 3,
            "src": "149.202.255.19",
            "data": ""
        },
       {
```

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