Soliton®

Soliton Dataset 2019

2019年6月4日

株式会社ソリトンシステムズ

Soliton Dataset 2019 について

- エンタープライズ向けEDR製品であるInfoTrace Mark II for Cyber（以下Mark II）は、内部不正対策としても利用できるログ取得を行っています。
- この特性は、実際のフォレンジック現場で目にするデータに近いものとしてマルウェア対策研究に役立つと考え、マルウェアをMark II導入環境で動作させた際のログをデータセットとして提供します。

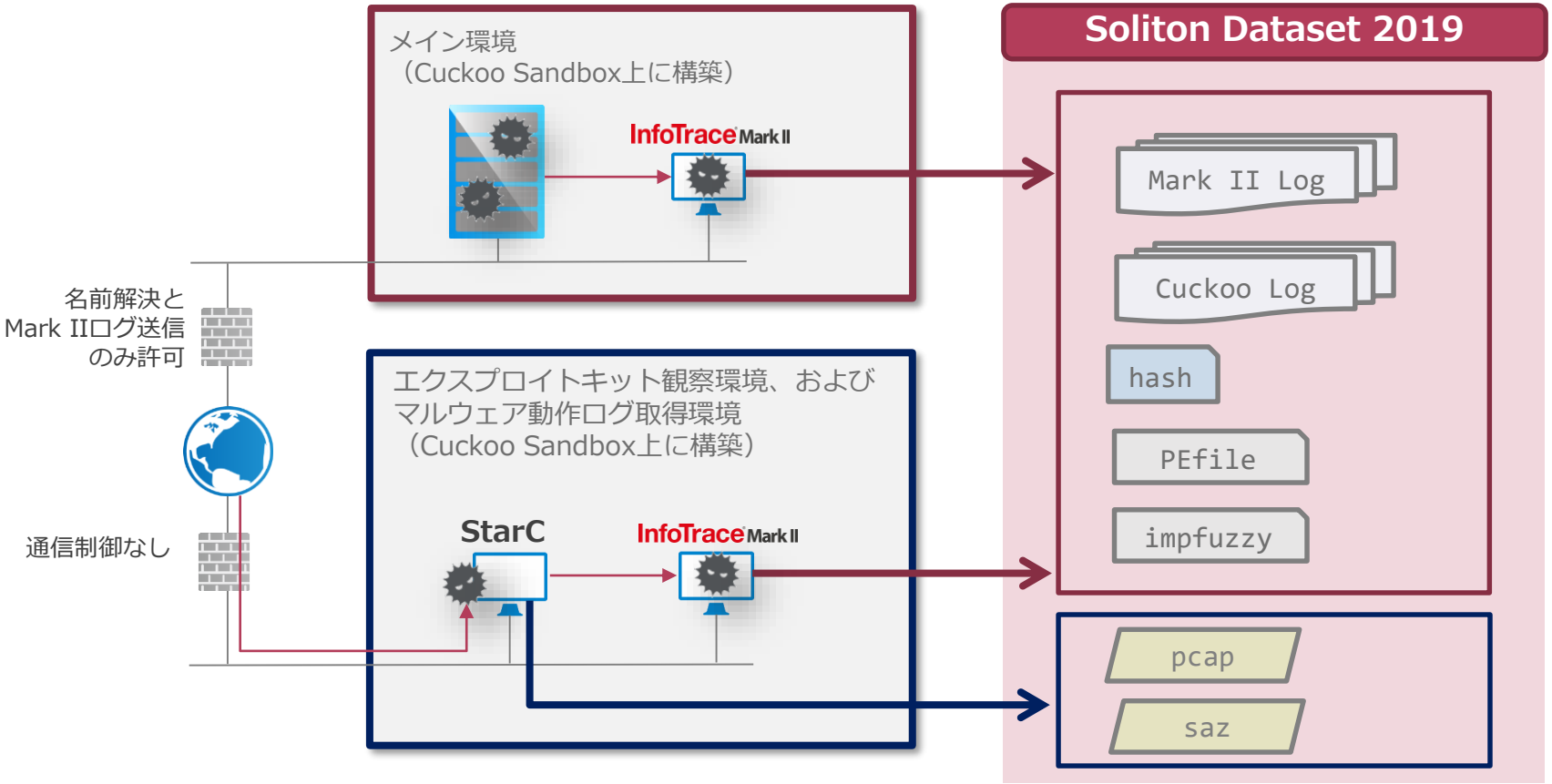
- マルウェア対策研究においては様々な観点での調査を行うため、複数種類のデータが提供されていることが望ましいと考えました。
- 動的解析システム Cuckoo Sandbox上に
  Windows 7 ProベースでMark IIを導入したゲスト環境を構築し
  Mark IIログとCuckooログの両方をデータセットとして提供します。

データ取得方針

- メイン環境
  - 2018年1月～2019年3月のマルウェア 485検体
  - VirusTotalより次のマルウェアを収集
    - マルウェア名（Emotet，Dreambot，Trickbot，ZACOM，TAIDOOR，IXESHE，DASERF，RedLeaves，CHCHES，ANEL，PLUGX，sorebrect，Oni，gandcrab）でサーチされた検体
    - 10以上のアンチウイルスエンジンでマルウェアと判定されている検体

- エクスプロイトキット観測環境および
マルウェア動作ログ取得環境
  - 2019年3月～5月にStarCなどでエクスプロイトキットを観測
  - 観測で得られた検体を実行してMark II/Cuckooログを取得
  - StarCで観測できたトラフィックデータ（fiddlerとtsharkで取得）も提供
    - 取り扱いはご注意ください。

マルウェア実行・ログ取得環境



提供物一覧（README.txtに記載）

SolitonDataset2019	
├─── README.txt	データセットの説明、注意事項など
├─── ENV.txt	実行環境の説明
├─── List.xlsx	マルウェア一覧
├─── Main/	
│ ├─── MK2Log/	Mark IIログ
│ └─── Cuckoo/	Cuckoo Sandboxログ
├─── EK/	
│ ├─── MK2Log/	Mark IIログ
│ ├─── Cuckoo/	Cuckoo Sandboxログ
│ ├─── pcap/	tsharkデータ
│ └─── saz/	fiddlerデータ
├─── Format/	ログフォーマットマニュアル
├─── impfuzzy/	各マルウェアのimpfuzzy結果
├─── PEfile/	各マルウェアのPEfile結果
├─── Sysinfo/	各マルウェア実行時の環境情報
└─── Tools/	便利ツール（Python）

例）ANELの起動（Mark IIログ）

03/27/2019 09:15:12.359 +0900 loc=ja-JP sn=7948 evt=ps subEvt=start os=Win com="JOHN-PC" domain="WORKGROUP" profile="3adf9e3e44fd106dd97b1d5cefff821d0b7ef583" tmid=Soliton3adf9e3e44fd106dd97b1d5cefff821d0b7ef583 ip=172.24.2.1,fe80::2dfc:c872:ad07:1bcc mac=52:54:00:d7:70:23 usr="John" usrDomain="John-PC" sessionID=1 psGUID={2DE1CF23-2F6C-4CB5-80F8-B2CE8BCC7F99} psPath="C:¥Users¥John¥AppData¥Local¥Temp¥af64311e861906c7b7e74be69f2be68cdcbf918508a55f1b1be83b36d6c3f27e.exe" psID=3692 parentGUID={51E129AD-CD2D-4162-9ABE-21F4BD7834DC} parentPath="C:¥tmpsdzytj¥bin¥inject-x86.exe" psUser="John" psDomain="John-PC" arc=x86 sha256=af64311e861906c7b7e74be69f2be68cdcbf918508a55f1b1be83b36d6c3f27e sha1=3adf9e3e44fd106dd97b1d5cefff821d0b7ef583 md5=0bb944e26cce95f8803fdd9c47ef3249 company="1" fileVer="1.00" product="工程1" productVer="1.00" crTime="03/25/2019 15:57:12.180" acTime="03/25/2019 15:57:12.180" moTime="03/25/2019 15:57:12.196" size=348160 sig=None

※今回はSHA-1をProfile名、TMID名として利用しました。
SHA256/SHA-1/MD5およびVirusTotalで得られた各ベンダーの検知名等の一覧を「List.xlsx」として提供します。

例）ANELの起動（Cuckooログ）


```
"behavior": {
      "generic": [
         {
            "process_path":"C:¥¥Users¥¥John¥¥AppData¥¥Local¥¥Temp¥¥af64311e861906c7b7e74be69f2be68c
dcbf918508a55f1b1be83b36d6c3f27e.exe",
            "process_name": "af64311e861906c7b7e74be69f2be68cdcbf918508a55f1b1be83b36d6c3f27e.exe",
            "pid": 3692,
（省略）
            "first_seen": 1553678112.609375,
            "ppid": 3604
},

:
:
```

例）GetCryptによるシャドウコピー削除（Mark IIログ）

05/22/2019 06:14:51.078 +0900 loc=ja-JP sn=124290 evt=ps subEvt=start os=Win
com="N4O-PC" domain="WORKGROUP"
profile="75aa1e3404aaab3a11ee7cb2f7e3682145fa6324"
tmid=75aa1e3404aaab3a11ee7cb2f7e3682145fa6324 ip=192.168.124.103
mac=52:54:00:b8:9e:17 usr="n4o" usrDomain="n4o-PC" sessionID=1
psGUID={745BFA83-D13C-4514-BCFD-CF9FBAA598F0}
psPath="C:¥Windows¥System32¥vssadmin.exe" cmd="delete shadows /all /quiet"
psID=2328 parentGUID={51D484A4-A6B0-4D51-AADD-BA64FEBEBDF0}
parentPath="C:¥Users¥n4o¥AppData¥Local¥Temp¥75aa1e3404aaab3a11ee7cb2f7e3682145
fa6324.exe" psUser="n4o" psDomain="n4o-PC" arc=x86
sha256=e09bf4d27555ec7567a598ba89ccc33667252cef1fb0b604315ea7562d18ad10
sha1=b1b1e773a7a6ba38302b345a908bb52b0f7e6394
md5=6e248a3d528ede43994457cf417bd665 company="Microsoft Corporation"
copyright="c Microsoft Corporation. All rights reserved." fileDesc="Command Line Interface
for MicrosoftR Volume Shadow Copy Service " fileVer="6.1.7600.16385 (win7_rtm.090713-
1255)" product="MicrosoftR WindowsR Operating System" productVer="6.1.7600.16385"
size=115200 sig=Valid signer="Microsoft Windows" issuer="Microsoft Windows Verification
PCA"

例）GetCryptによるシャドウコピー削除（Cuckooログ）


```
"behavior": {
"generic": [
  {
    "process_path":
"C:¥¥Users¥¥n4o¥¥AppData¥¥Local¥¥Temp¥¥75aa1e3404aaab3a11ee7cb2f7e3682145fa6324.exe",
    "process_name": "75aa1e3404aaab3a11ee7cb2f7e3682145fa6324.exe",
    "pid": 3780,
    "summary": {
 (省略)
    "command_line": [
            "¥"C:¥¥Windows¥¥System32¥¥vssadmin.exe¥"  delete shadows /all /quiet",
            "vssadmin.exe  delete shadows /all /quiet“
     ]
 (省略)
     },
   "first_seen": 1558505670.578125,
   "ppid": 3752
 }
],
}
```

Soliton Dataset 2019の利用例

- 動的解析の研究・学習に
  - Mark IIログとCuckooログの両方を確認できます
    - Mark IIで動作の流れを把握、Cuckooで詳細把握など
  - PEファイル以外の検体も含まれます
  - 起動できなかったマルウェアも含まれます
    - データクレンジングはしておりませんのでご注意ください
  - エンタープライズの実環境に近い、OS標準ソフトウェアなどの動作も含まれたログのため、実環境でマルウェア挙動を見出す研究の参考としてお使いいただけます。