Soliton®

Soliton Dataset 2022

2022年7月12日

株式会社ソリトンシステムズ

Soliton Dataset 2022 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。

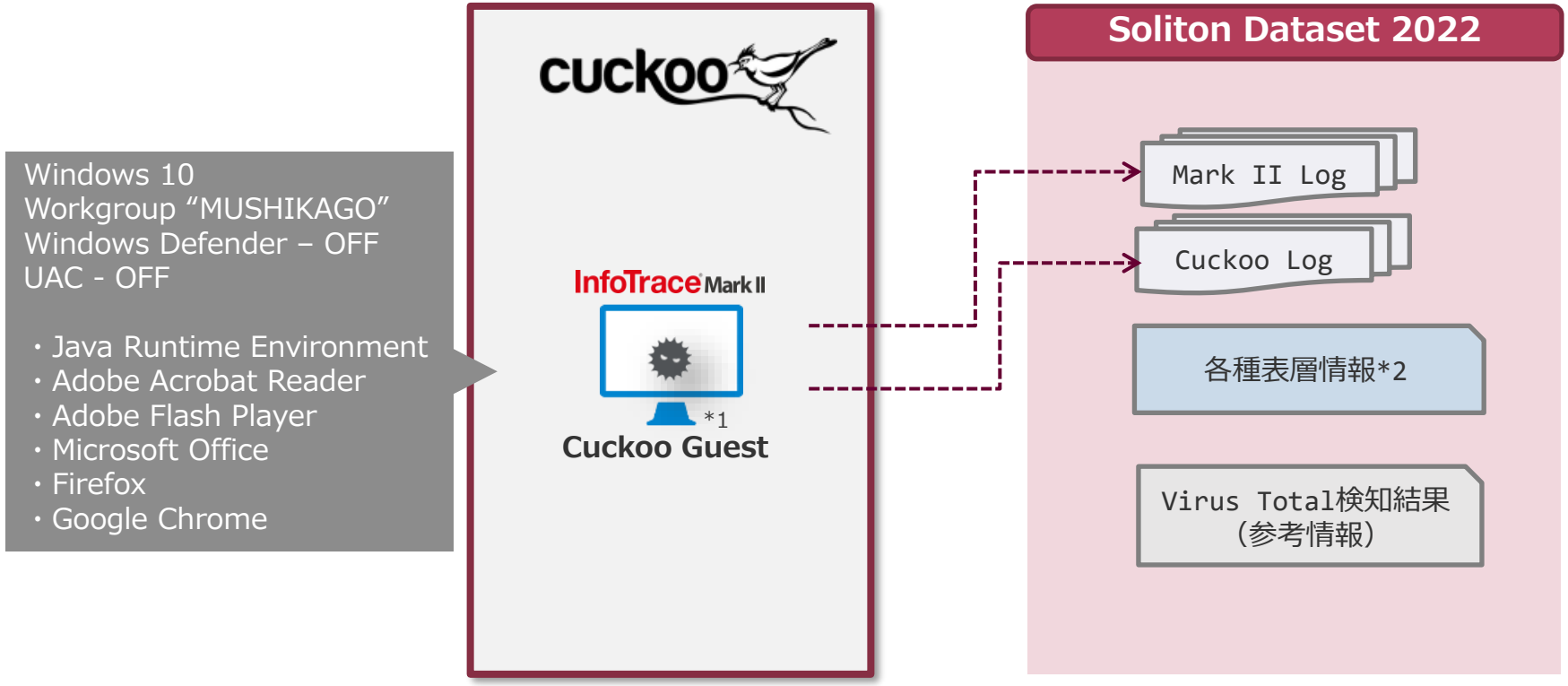
- マルウェア対策研究においては様々な観点での調査を行うため、複数種類のデータが提供されていることが望ましいと考えました。

- 動的解析システム Cuckoo Sandbox上にWindows 10 Enterpriseベースで Mark IIを導入したKVM環境とAWS(EC2)環境をそれぞれ構築し、 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

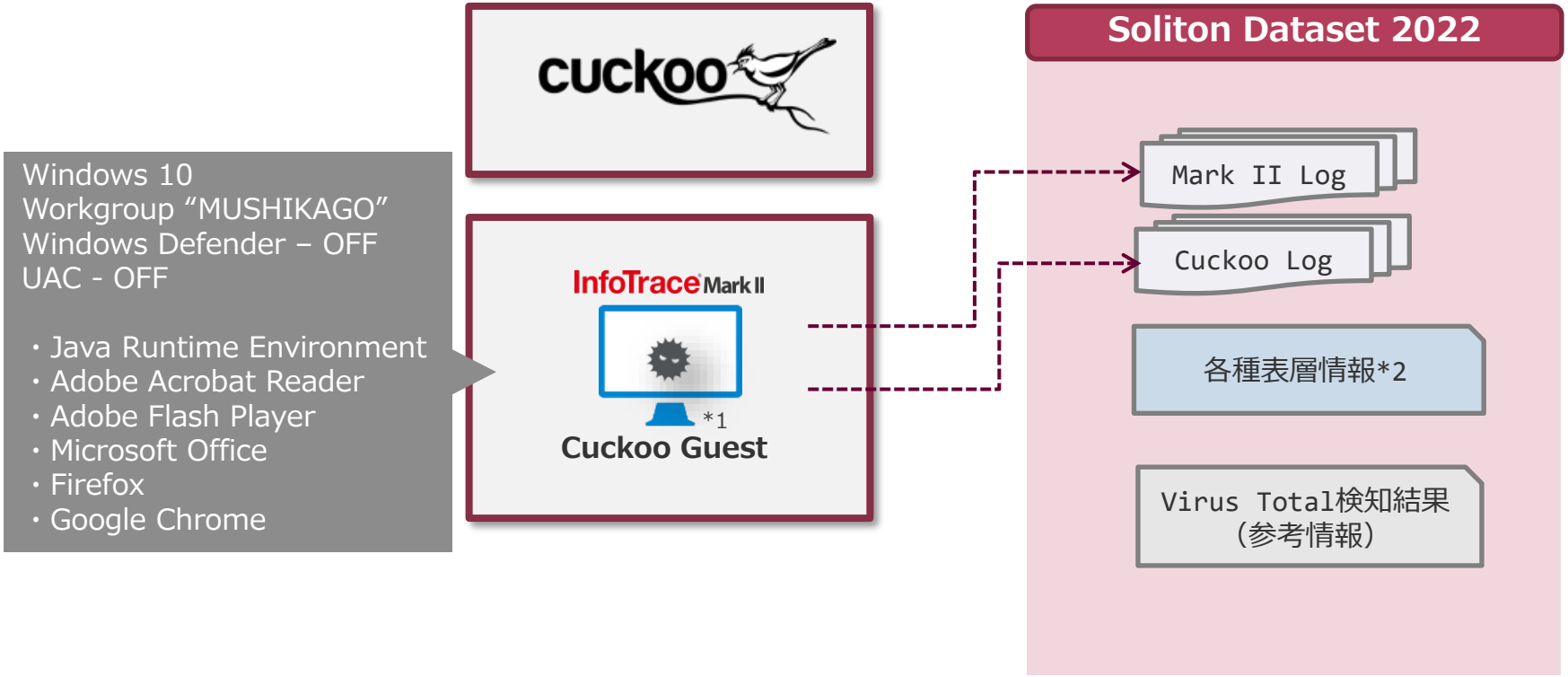
- 2021年4月～2022年3月に話題になったマルウェア 445検体
- 調査会社などから解析結果が公開されているものを中心にVirusTotalより収集しました
- ファイル形式にこだわらずに収集しているため、PEファイルだけではなく、スクリプトやマクロ型マルウェアなども含まれます 238検体
  - DLL型のマルウェアの実行パラメータは当該マルウェアのMark IIログをご参照ください。

マルウェア実行・ログ取得環境(KVM)



*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 2022のREADME等をご参照ください。

マルウェア実行・ログ取得環境(AWS)



*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 2022のREADME等をご参照ください。

提供物一覧

```
SolitonDataset2022
├─── README.txt
├─── ENV.txt（環境情報）
├─── Sysinfo/（ログ取得端末のシステム情報）
├─── MalwareList.csv（検体リスト）
├─── Data/
│      └─── <マルウェアファミリ名>/
│             └─── <マルウェアハッシュ値>/
│                    ├─── aws_mk2.log（AWS(EC2)におけるMark IIログ）
│                    ├─── aws_mk2.json（aws_mk2.logをJSONにしたログ）
│                    ├─── kvm_mk2.log（KVMにおけるMark IIログ）
│                    ├─── kvm_mk2.json（kvm_mk2.logをJSONにしたログ）
│                    ├─── aws_cuckoo.json（AWS(EC2)におけるCuckooログ）
│                    ├─── kvm_cuckoo.json（KVMにおけるCuckooログ）
│                    └─── vt_report.json（VirusTotal検知結果）
├─── Surface/ （各マルウェアの表層情報）
├─── Format/ （MarkIIログ項目一覧）
└─── Tools/ （便利ツール）
```

検体リスト（MalwareList.csv）

SHA256	MD5	SHA-1	マルウェア	KVM実行時	AWS実行時	VirusTotalにおけ	検知したア	スキャンに	AWS-Mark	AWS-Mark	AWS-Cuck	KVM-Mark	KVM-Mark	KVM-Cuc	参考ページ	参考ページURL
0c6f444c6	bb266486	11203786	ALPHV	PE32 exec	.exe	2022/4/29 17:59	51	68	1365806	1741218	226158	78064	97732	258832	ALPHV (B	https://www.va
13828b39(	c6901bc67	783b2b05	ALPHV	PE32 exec	.exe	2022/4/29 18:04	51	69	822592	1053418	250227	162898	207199	261547	ALPHV (B	https://www.va
15b57c1b(	c1dd3d5a	89060eff6	ALPHV	PE32 exec	.exe	2022/4/29 18:06	51	69	1428689	1819296	250458	163175	207448	264595	ALPHV (B	https://www.va
1af1ca666	518264085	ce5540c0c	ALPHV	PE32 exec	.exe	2022/5/5 17:39	50	68	1324568	1688895	265445	48707	59860	280996	ALPHV (B	https://www.va
2587001d(	4168465b8	77413cb3f	ALPHV	PE32 exec	.exe	2022/4/6 9:08	52	68	275003	347899	265401	127247	161113	260998	ALPHV (B	https://www.va
28d7e6fe3	0b6ef1e65	5c6ca5581	ALPHV	PE32 exec	.exe	2022/4/8 19:48	54	69	479396	619596	247840	39213	47918	275416	ALPHV (B	https://www.va
2cf54942e	ed075c471	f466b4d68	ALPHV	PE32 exec	.exe	2022/2/14 6:14	51	68	1321420	1682856	241066	151107	192177	228591	ALPHV (B	https://www.va
38834b79(	9c54d3b2a	da1e4a09a	ALPHV	PE32 exec	.exe	2022/2/3 18:49	48	67	1361441	1733511	267199	163269	207898	261944	ALPHV (B	https://www.va
3d7cf20ca	aea5d3cce	087497940	ALPHV	PE32 exec	.exe	2022/2/25 18:24	52	70	1363628	1737283	235104	46559	57201	235954	ALPHV (B	https://www.va
4e18f9293	70b8bc741	655c2567(	ALPHV	PE32 exec	.exe	2022/3/3 16:27	54	70	1393342	1774250	264177	155416	197880	263338	ALPHV (B	https://www.va
59868f4b3	fe16fa500	e2243638(	ALPHV	PE32 exec	.exe	2022/2/14 17:44	57	69	1332655	1697105	267008	154149	196183	265389	ALPHV (B	https://www.va

- 検体ハッシュ値(SHA256，SHA-1，MD5)
- マルウェアファミリ
- KVM実行時のファイルタイプ(Cuckoo判定)
- AWS実行時の拡張子(VirusTotal判定)
- VirusTotalスキャン日時
- 検知したアンチウイルスエンジン数(VTより)
- 使用したアンチウイルスエンジン数(VTより)
- AWS-Mark IIログファイルサイズ(.log)
- KVM-Mark IIログファイルサイズ(.log)
- AWS-Mark IIログファイルサイズ(.json)
- KVM-Mark IIログファイルサイズ(.json)
- Cuckooログファイルサイズ(AWS，KVM)
- 参考ページタイトル・コメント
- 参考ページURL

例）LockBit2.0の起動（Mark IIログ）

04/07/2022 11:59:16.023 +0900 loc=ja-JP type=ITM2 sn=207 lv=6 rs=2 trs=6 rf=C16:C8:L8:R8 **evt=ps subEvt=start** os=Win com="mws" domain="MUSHIKAGO" profile="mws" tmid=203cbdd9-250d-50cf-9e5c-9aa6c0ade4dd csid=S-1-5-21-1134204224-2411533656-1793949185 ip=172.24.7.101,fe80::70e6:25ab:67c9:141c mac=52:54:00:ca:68:ad usr="mws" usrDomain="MWS" sessionID=1 psGUID={BCF63BE3-59F9-45B3-8EE9-4A8758DCC2BA} psPath="C:¥Users¥mws¥AppData¥Local¥Temp¥**3cbdd9250d50cf9e5c9aa6c0ade4dde2995e1319e96a160ba6730e063e86f5bc**.exe" **psID=3360** parentGUID={78E1499D-26C6-4CD5-A74C-113D6B3F3AE4} parentPath="C:¥tmpwutom2¥bin¥inject-x86.exe" psUser="mws" psDomain="MWS" arc=x86 sha256=**3cbdd9250d50cf9e5c9aa6c0ade4dde2995e1319e96a160ba6730e063e86f5bc** sha1=f535b56f029c5c42c3915e1546912d7e49fe9f38 md5=30e9d7d5ba0b230866ce5b0c932b2a50 crTime="03/08/2021 23:43:29.724" acTime="04/07/2022 11:59:15.930" moTime="03/08/2021 23:43:29.771" size=982528 sig=None

例）LockBit2.0の起動（Cuckooログ）


```
"behavior": {
        "generic": [
            {
                "process_path":
"C:¥¥Users¥¥mws¥¥AppData¥¥Local¥¥Temp¥¥3cbdd9250d50cf9e5c9aa6c0ade4dde2995e1319e96a160
ba6730e063e86f5bc.exe",
                "process_name": "3cbdd9250d50cf9e5c9aa6c0ade4dde2995e1319e96a160ba6730e063e86f5bc.exe",
                "pid": 3360,
                "summary": {
                    "file_created": [
 (省略)
:
:
                "first_seen": 1649332756.289423,
                "ppid": 7700
            },
:
:
```

例）LockBit2.0によるファイル暗号化（Mark IIログ）

- 04/07/2022 11:59:19.695 +0900 loc=ja-JP type=ITM2 sn=299 lv=7 rs=12 trs=44 rf=C16:C8:L8:R8:C10:L10:R10 **evt=file subEvt=close** os=Win com="mws" domain="MUSHIKAGO" profile="mws" tmid=203cbdd9-250d-50cf-9e5c-9aa6c0ade4dd csid=S-1-5-21-1134204224-2411533656-1793949185 ip=172.24.7.101,fe80::70e6:25ab:67c9:141c mac=52:54:00:ca:68:ad usr="mws" usrDomain="MWS" sessionID=1 psGUID={BCF63BE3-59F9-45B3-8EE9-4A8758DCC2BA} psPath="C:¥Users¥mws¥AppData¥Local¥Temp¥3cbdd9250d50cf9e5c9aa6c0ade4dde2995e1319e96a160ba6730e063e86f5bc.exe" **path="C:¥Program Files¥Java¥jre1.8.0_271¥bin¥server¥classes.jsa"** drvType=HDD **read=4096 write=4608** sha256=bd46ff0d5af076712b0d06b1acf9f7e71dd2e5746ed0ac5737bcf1ec2fe35813 sTime="04/07/2022 11:59:19.664" crTime="01/07/2021 16:21:35.894" acTime="04/07/2022 11:59:19.680" moTime="04/07/2022 11:59:19.680" **size=18809344** new=0

- 04/07/2022 11:59:19.695 +0900 loc=ja-JP type=ITM2 sn=303 lv=7 rs=12 trs=46 rf=C16:C8:L8:R8:C10:L10:R10 **evt=file subEvt=rename** os=Win com="mws" domain="MUSHIKAGO" profile="mws" tmid=203cbdd9-250d-50cf-9e5c-9aa6c0ade4dd csid=S-1-5-21-1134204224-2411533656-1793949185 ip=172.24.7.101,fe80::70e6:25ab:67c9:141c mac=52:54:00:ca:68:ad usr="mws" usrDomain="MWS" sessionID=1 psGUID={BCF63BE3-59F9-45B3-8EE9-4A8758DCC2BA} psPath="C:¥Users¥mws¥AppData¥Local¥Temp¥3cbdd9250d50cf9e5c9aa6c0ade4dde2995e1319e96a160ba6730e063e86f5bc.exe" **path="C:¥Program Files¥Java¥jre1.8.0_271¥bin¥server¥classes.jsa"** drvType=HDD **dstPath="C:¥Program Files¥Java¥jre1.8.0_271¥bin¥server¥classes.jsa.lockbit"** dstDrv=HDD sha256=bd46ff0d5af076712b0d06b1acf9f7e71dd2e5746ed0ac5737bcf1ec2fe35813 crTime="01/07/2021 16:21:35.894" acTime="04/07/2022 11:59:19.680" moTime="04/07/2022 11:59:19.680" **size=18809344**

例）LockBit2.0によるファイル暗号化（Cuckooログ）


```
{
                "category": "file",
                "status": 1,
                "stacktrace": [],
                "api": "NtWriteFile",
                "return_value": 259,
                "arguments": {
                    "file_handle": "0x00000480",
                    "filepath": "C:¥¥Program Files¥¥Java¥¥jre1.8.0_271¥¥bin¥¥server¥¥classes.jsa",
                    "buffer":
"¥u0097H¥u008aY¥u0088/¥nLb¥u0095¥u00cd{¥u00b1¥f¥u00f3¥u00d4¥u00c3¥u001e¥u00a0¥u0099¥u00a9¥u0
08b¥u00c0$Z¥u00b0j¥u00e3¥u00db¥u00d7¥u00d0&H%¥u0091¥u0086¥u00dcd:¥u00daFo¥u00d2¥u00c1¥u00ea
¥u00ab¥u00e0¥u00ce¥"¥u00c2<¥u00f3¥u0010¥u00d2?¥u00b9V¥u001ae)H?¥u00fe¥u0089¥u0003FtJH
:
¥u00ae¥u00f4;¥u009fL,¥u0005h¥u00a1¥u00d0¥u001d1?o$c¥u0087Z¥u009ei^P¥u00cdp¥u000e¥u001b¥u00e0¥
u0016oe¥u00fe",
                    "offset": 18808832
                },
                "time": 1649332759.680423,
                "tid": 1728,
                "flags": {}
            },
```

注意点①

- 注意点について
  - 今回はAWSを使用したマルウェア実行環境も構築しました。AWSをサポートしていないCuckooを動かすことや、AWSにおけるマルウェア実行時の安全管理措置についての調整等に手間取ったこともあり、次ページに記載した注意点が生じています。
  - 本資料では主な注意点のみを記載しています。詳細はREADMEでご確認ください。
  - データセットとしては至らない点もございますが、注意点を踏まえてご活用いただければ幸いです。

注意点②

- AWS(EC2)環境では、もともとAWSで使用されているプロセスのログも記録されています。監視除外しておらず、KVM環境よりもログ量が増えています。

- AWS(EC2)ではPDF実行環境設定に問題があり、PDFマルウェアが実行できなかったため、AWS環境でのPDFマルウェアのログは収録していません。

- マルウェアを実行する際のファイルタイプ判定が異なります。
  - KVMではCuckooの判定結果
  - AWSではVirusTotalの判定結果

Soliton Dataset 2022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（238件/445件）
  - AWS(EC2)とKVMにおけるログが確認できます
  - 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 #mws2022-pre
チャンネルまでお気軽にどうぞ！