Soliton®

Soliton Dataset 2018

2018年5月30日

株式会社ソリトンシステムズ

Soliton Dataset 2018について

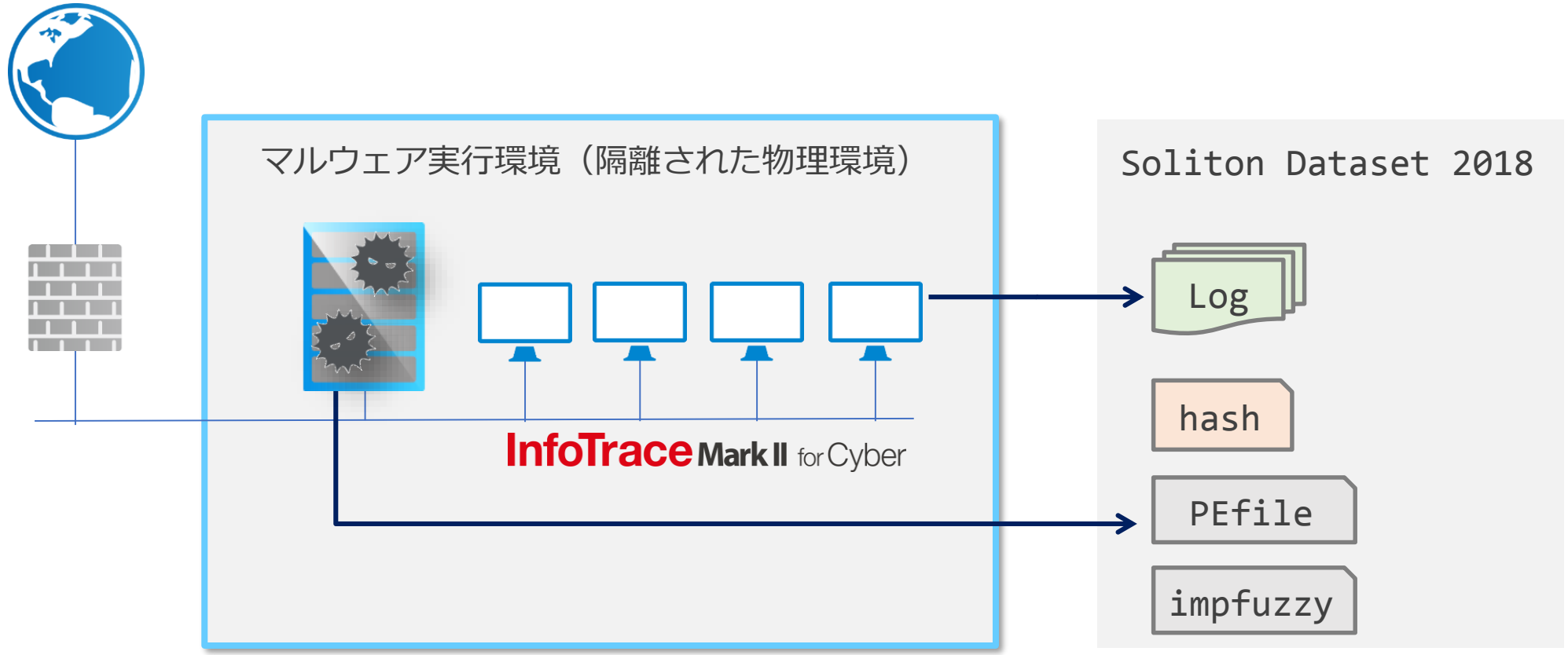
- エンタープライズ向けEDR製品であるInfoTrace Mark II for Cyber（以下Mark II）は、内部不正対策としても利用できるログ取得を行っています。
- この特性は、実際のフォレンジック現場で目にするデータに近いものとしてマルウェア対策研究に役立つと考え、マルウェアをMark II導入環境で動作させた際のログをデータセットとして提供します。

データ取得方針

- 2017年1月～2018年2月に話題になったマルウェア
- セキュリティベンダーから解析結果が公開されたもの
- ファイルタイプにこだわらず収集
- マルウェア実行環境でプロセスとして起動したもの
  - 具体的な侵害活動に至らずとも、起動できたものは提供物に含めています

→計 117 検体となりました

専用のマルウェア実行・ログ取得環境



マルウェア実行環境の詳細はポストミーティングでのご紹介資料をご参照ください：
https://www.iwsec.org/mws/2017/20171201/MWS_Soliton_20181201_Rev2.pdf

提供物一覧（README.txtに記載）

SolitonDataset2018	
├─── 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
├─── MK2Log/	
│　　├─── 30m/	通常出力30分（当初はこちらのみ提供予定でした）
│　　├─── Verbose/	詳細出力30分（参考情報）
│　　├─── Normal/	正常環境（マルウェア投入無し）の30分ログ
│　　├─── OlympicDestroyer/	2時間実行、破壊系
│　　├─── Petya/	横展開、破壊系
│　　├─── StoneDrill/	破壊系
│　　└─── WannaCry/	横展開
├─── 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
├─── Reports/	ログ解析サンプル（おまけ）
├─── Sysinfo/	各マルウェア実行時の環境情報
└─── Tools/	便利ツール（Python）

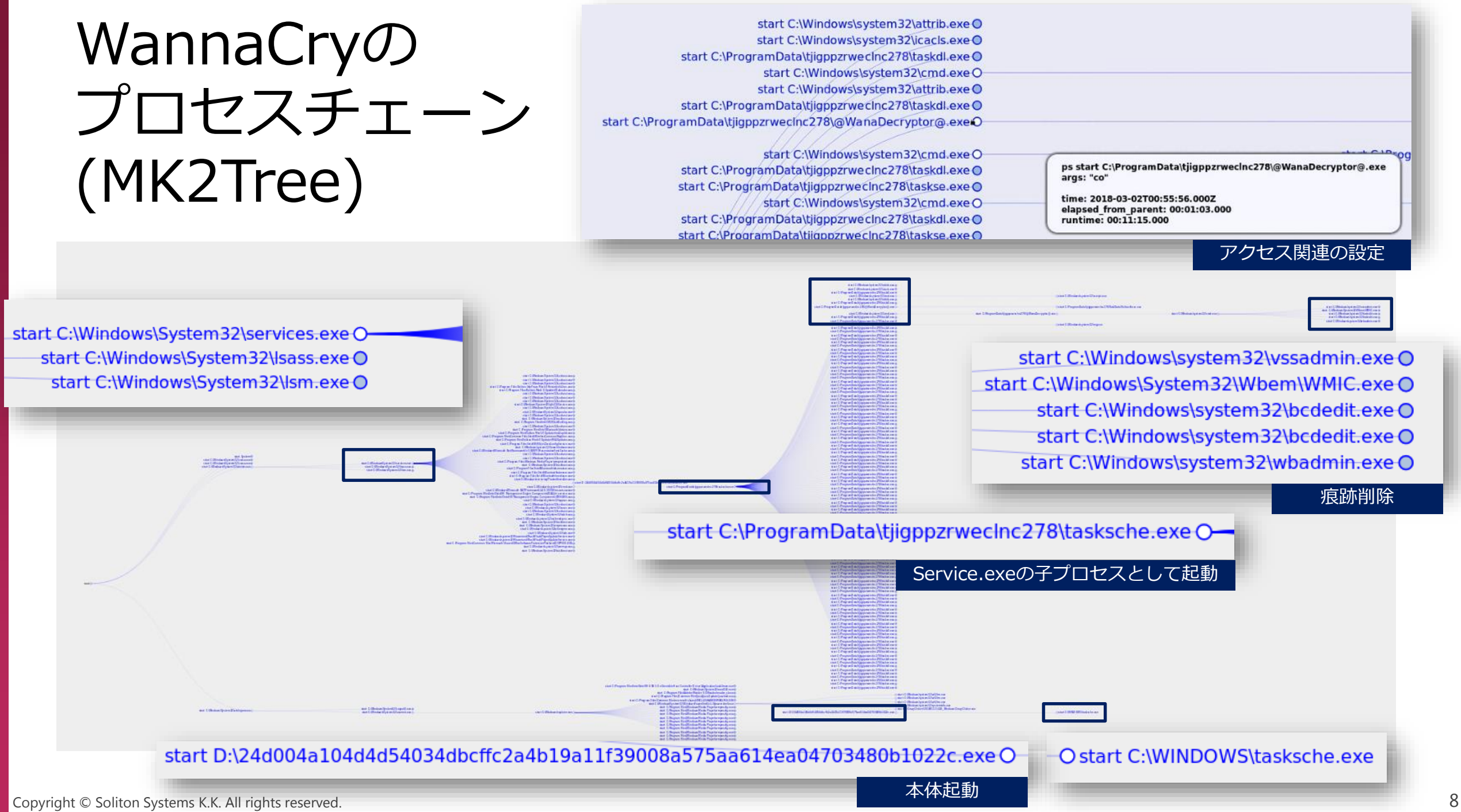
提供物①

- README.txt
  - 注意事項などを記載しています
- ENV.txt
  - 一般的な環境、横展開系の環境など
- List.xlsx
  - マルウェア一覧
  - 拡張子、ウイルス対策ベンダーのラベル、参照URL、Verboseログ有無、レポート有無
- InfoTrace Mark II for Cyberセキュリティログ（MK2Log)
  - 通常出力（30m）
  - 詳細出力（Verbose）
  - 正常環境（Normal）
    - Malware.batという名前の無害バッチ実行のみ
  - 特殊マルウェア：
    - WannaCry：横展開
    - Petya：横展開、破壊系
    - StoneDrill：破壊系
    - Olympic Destroyer：2時間、破壊系

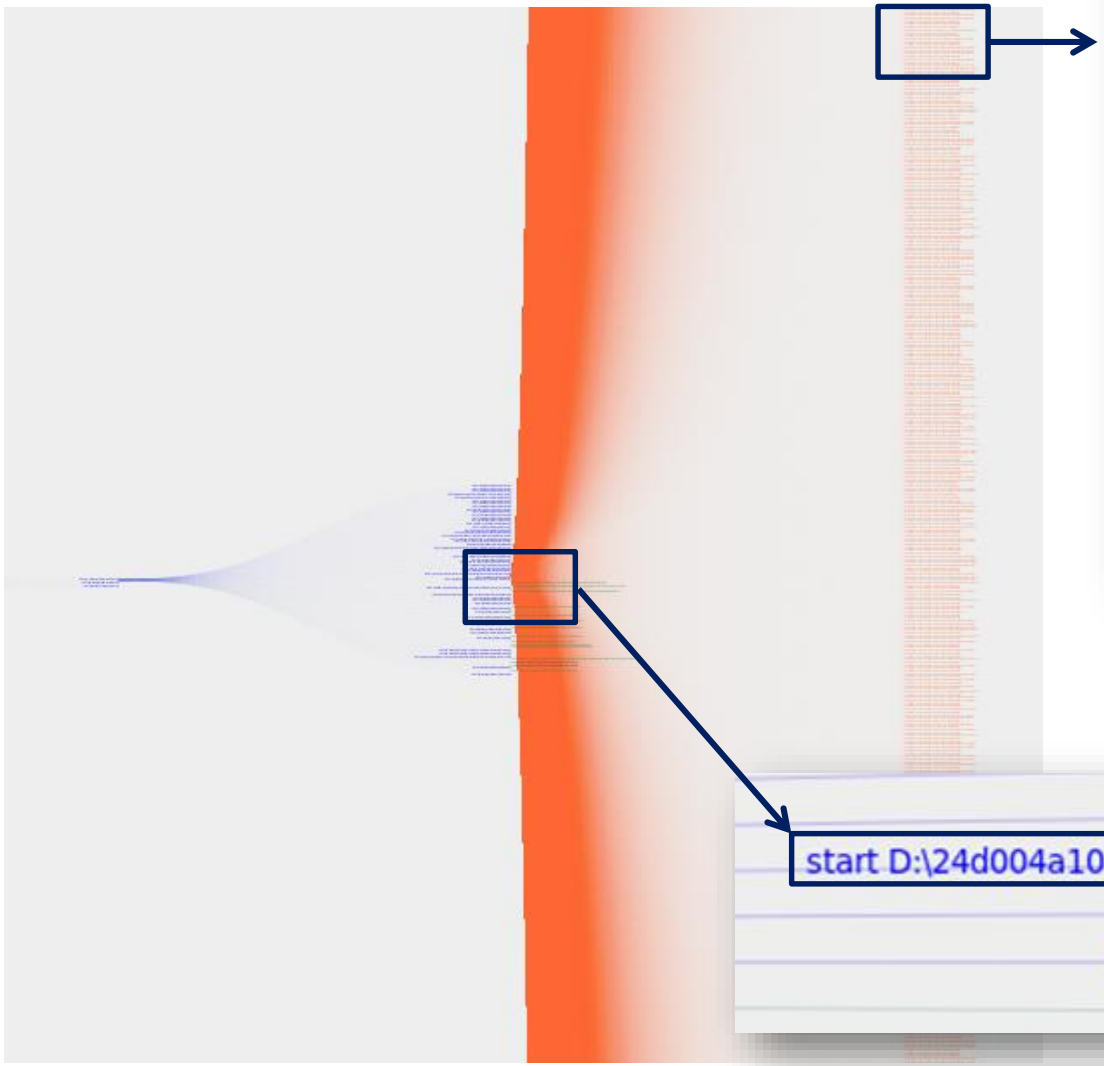
提供物②

- sysinfo
  - 各マルウェア実行時の環境情報
    - w32tm.exeの時刻同期結果とsysteminfo.exe の結果
    - マルウェアに妨害され0byteとなっているものがあります
- impfuzzy、PEfile
  - 各マルウェア検体ごとの結果
    - PEファイル以外はファイルサイズ0となっています
- Tools
  - mk2log
    - Mark IIログをJSON化するPythonツール
  - mk2tree
    - JSON化されたMark IIログをツリー表示するPythonツール
- Format
  - Mark IIのログフォーマットのマニュアル
- Reports(おまけ)
  - いくつかのマルウェアの動作をピックアップしたログ解析サンプル

WannaCryのプロセスチェーン(MK2Tree)



WannaCryの横展開 (MK2Tree)



dcon from 172.24.1.1:49835 to 172.24.1.2:microsoft-ds rcv=292 snd=4,376
dcon from 172.24.1.1:49837 to 172.24.1.2:microsoft-ds rcv=252 snd=4,356
dcon from 172.24.1.1:49839 to 172.24.1.2:microsoft-ds rcv=252 snd=4,356
dcon from 172.24.1.1:49840 to 172.24.1.2:microsoft-ds rcv=252 snd=4,356
dcon from 172.24.1.1:49841 to 172.24.1.2:microsoft-ds rcv=252 snd=4,356
dcon from 172.24.1.1:49845 to 172.24.1.2:microsoft-ds rcv=292 snd=4,376
dcon from 172.24.1.1:49846 to 172.24.1.2:microsoft-ds rcv=252 snd=4,376
dcon from 172.24.1.1:49847 to 172.24.1.2:microsoft-ds rcv=292 snd=4,376
dcon from 172.24.1.1:49850 to 172.24.1.2:microsoft-ds rcv=252 snd=4,356
dcon from 172.24.1.1:49849 to 172.24.1.2:microsoft-ds rcv=252 snd=4,356
dcon from 172.24.1.1:49767 to 172.24.1.2:microsoft-ds rcv=2,064 snd=69,423
con from 172.24.1.1:50257 to 172.24.1.2:microsoft-ds
dcon from 172.24.1.1:50257 to 172.24.1.2:microsoft-ds rcv=705 snd=607
con from 172.24.1.1:50355 to 172.24.1.2:microsoft-ds
dcon from 172.24.1.1:50355 to 172.24.1.2:microsoft-ds rcv=705 snd=607
con from 172.24.1.1:50356 to 172.24.1.2:microsoft-ds
dcon from 172.24.1.1:50356 to 172.24.1.2:microsoft-ds rcv=153,937 snd=5,455,791

脆弱性（MS07-010）を利用した横展開の様子

start C:\Windows\servicing\TrustedInstaller.exe
start D:\24d004a104d4d54034dbcffc2a4b19a11f39008a575aa614ea04703480b1022c.exe
start C:\Windows\system32\cmd.exe
start C:\Windows\Microsoft.NET\Framework\v4.0.30319\mscorsvw.exe
close C:\

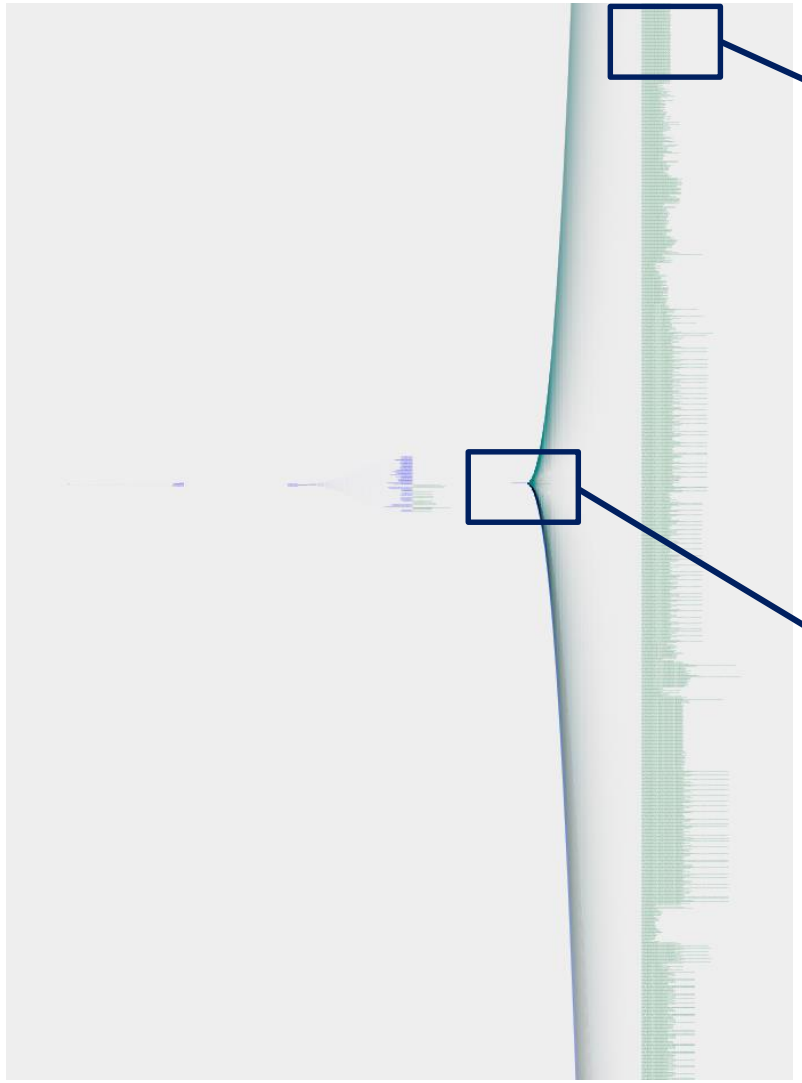
サービス起動したマルウェア本体が横展開を実施

WannaCryの横展開(Log)

```
03/01/2018 19:55:17.836 +0900 sn=4028 evt=net subEvt=con com="PC1" psGUID={BECF254A-5C79-4931-9CDF-143505F33B16} psPath="D:¥24d004a104d4d54034dbcffc2a4b19a11f39008a575aa614ea04703480b1022c.exe" srcIP=172.24.1.1 srcPort=49624 dstIP=172.24.1.2 dstPort=445
03/01/2018 19:55:17.836 +0900 sn=4029 evt=net subEvt=dcon com="PC1" psGUID={BECF254A-5C79-4931-9CDF-143505F33B16} psPath="D:¥24d004a104d4d54034dbcffc2a4b19a11f39008a575aa614ea04703480b1022c.exe" srcIP=172.24.1.1 srcPort=49624 dstIP=172.24.1.2 dstPort=445 recv=132 send=72
03/01/2018 19:55:17.836 +0900 sn=4030 evt=net subEvt=con com="PC1"  psGUID={BECF254A-5C79-4931-9CDF-143505F33B16} psPath="D:¥24d004a104d4d54034dbcffc2a4b19a11f39008a575aa614ea04703480b1022c.exe" srcIP=172.24.1.1 srcPort=49625 dstIP=172.24.1.2 dstPort=445
03/01/2018 19:55:17.976 +0900 sn=4041 evt=net subEvt=dcon com="PC1"  psGUID={BECF254A-5C79-4931-9CDF-143505F33B16} psPath="D:¥24d004a104d4d54034dbcffc2a4b19a11f39008a575aa614ea04703480b1022c.exe" srcIP=172.24.1.1 srcPort=49625 dstIP=172.24.1.2 dstPort=445 recv=637 send=516
```

サービス起動されたプロセス（psGUID={BECF254A-5C79-4931-9CDF-143505F33B16}）が
感染先PC（172.24.1.2）に対して通信を行っていることが確認できます

WannaCryによるファイル暗号化(MK2Tree)



close D:\transcript.txt sz=7,112 rd=7,120 wr=0
create D:\~SD9DCD.tmp
close C:\ProgramData\tjigppzrweclnc278\@Please_Read_Me@.txt sz=933 rd=933 wr=0
create D:\@Please_Read_Me@.txt
rename from D:\transcript.txt.WNCRYT to D:\transcript.txt.WNCRY
del D:\~SD9DCD.tmp
create D:\transcript.txt.WNCRYT
close D:\transcript.txt.WNCRYT sz=7,400 rd=0 wr=7,400
copy from C:\ProgramData\tjigppzrweclnc278\@Please_Read_Me@.txt to D:\@Please_Read_Me@.txt
close D:\@Please_Read_Me@.txt sz=933 rd=0 wr=933
create D:\@WanaDecryptor@.exe

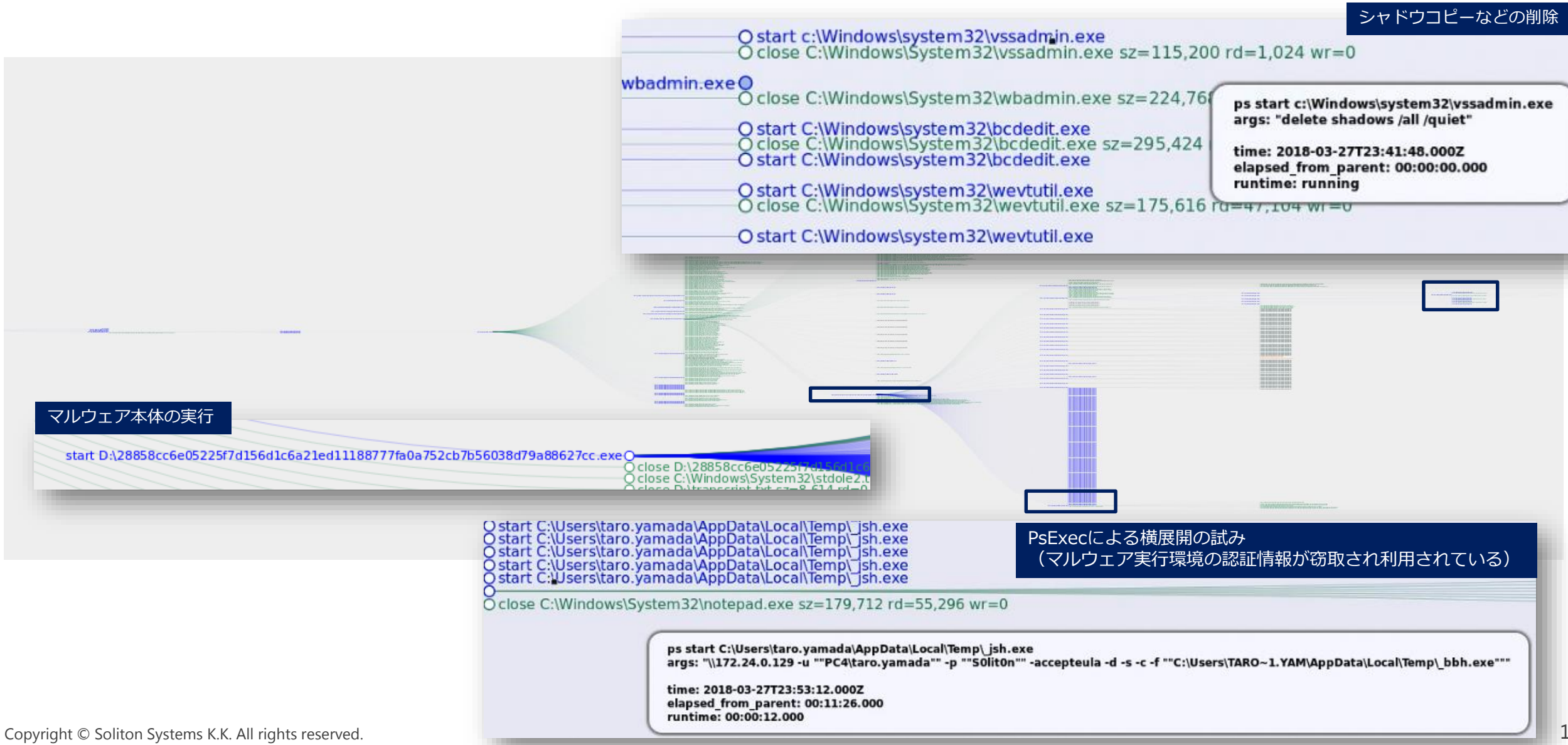
start C:\ProgramData\tjigppzrweclnc278\tasksche.exe
close

WannaCryによるファイル暗号化(Log)

```
03/01/2018 19:54:57.196 +0900 sn=602 evt=file subEvt=close com="PC1" psGUID={4F58F9E3-FD37-4FBD-BC44-80AC0E0D1CEB}
psPath="C:¥ProgramData¥tjigppzrweclnc278¥tasksche.exe" path="D:¥transcript.txt" drvType=HDD read=7120 write=0
sha256=983ff9ae6a57ba30abb4faa94be6da24567f6a46ed6e2370d82e6c9d64806c8d sTime="03/01/2018 19:54:57.196" crTime="03/01/2018 19:53:27.820"
acTime="03/01/2018 00:00:00.000" moTime="03/01/2018 19:54:10.000" size=7112
03/01/2018 19:54:57.196 +0900 sn=603 evt=file subEvt=create com="PC1" psGUID={4F58F9E3-FD37-4FBD-BC44-80AC0E0D1CEB}
psPath="C:¥ProgramData¥tjigppzrweclnc278¥tasksche.exe" path="D:¥~SD9DCD.tmp" drvType=HDD
03/01/2018 19:54:57.196 +0900 sn=606 evt=file subEvt=rename com="PC1" psGUID={4F58F9E3-FD37-4FBD-BC44-80AC0E0D1CEB}
psPath="C:¥ProgramData¥tjigppzrweclnc278¥tasksche.exe" path="D:¥transcript.txt.WNCRYT" drvType=HDD dstPath="D:¥transcript.txt.WNCRY"
dstDrv=HDD sha256=264ff86387c5b15bb76749af1595e275a0dc49dcf52fd04b94c8693180ae71a0 crTime="03/01/2018 19:53:27.820" acTime="03/01/2018
00:00:00.000" moTime="03/01/2018 19:54:10.000" size=7400
03/01/2018 19:54:57.196 +0900 sn=607 evt=file subEvt=del com="PC1" psGUID={4F58F9E3-FD37-4FBD-BC44-80AC0E0D1CEB}
psPath="C:¥ProgramData¥tjigppzrweclnc278¥tasksche.exe" path="D:¥~SD9DCD.tmp" drvType=HDD crTime="03/01/2018 19:54:57.190"
acTime="03/01/2018 00:00:00.000" moTime="03/01/2018 19:54:58.000" size=0 hide=1
03/01/2018 19:54:57.196 +0900 sn=608 evt=file subEvt=create com="PC1" psGUID={4F58F9E3-FD37-4FBD-BC44-80AC0E0D1CEB}
psPath="C:¥ProgramData¥tjigppzrweclnc278¥tasksche.exe" path="D:¥transcript.txt.WNCRYT" drvType=HDD
03/01/2018 19:54:57.196 +0900 sn=609 evt=file subEvt=close com="PC1" psGUID={4F58F9E3-FD37-4FBD-BC44-80AC0E0D1CEB}
psPath="C:¥ProgramData¥tjigppzrweclnc278¥tasksche.exe" path="D:¥transcript.txt.WNCRYT" drvType=HDD read=0 write=7400 sTime="03/01/2018
19:54:57.196" crTime="03/01/2018 19:53:27.820" acTime="03/01/2018 00:00:00.000" moTime="03/01/2018 19:54:10.000" size=7400
03/01/2018 19:55:57.913 +0900 sn=6834 evt=file subEvt=del com="PC1" psGUID={4F58F9E3-FD37-4FBD-BC44-80AC0E0D1CEB}
psPath="C:¥ProgramData¥tjigppzrweclnc278¥tasksche.exe" path="D:¥transcript.txt" drvType=HDD
sha256=983ff9ae6a57ba30abb4faa94be6da24567f6a46ed6e2370d82e6c9d64806c8d crTime="03/01/2018 19:53:27.820" acTime="03/01/2018 00:00:00.000"
moTime="03/01/2018 19:54:10.000" size=7112
```

一部の処理が前後して出力されていますが、元ファイル（サイズ7120byte)が読み込まれ、”D:¥transcript.txt.WNCRYT”というファイル名で7400byteで書き込まれ、ファイル名が”D:¥transcript.txt.WNCRY”というファイル名に変更されたのち、元ファイルが削除されていることが分かります。

Olympic Destroyerのプロセスチェイン(MK2Tree)



Olympic Destroyerの感染活動(Log)

```
03/27/2018 19:44:53.926 sn=1818 evt=ps subEvt=start
psPath="C:¥Users¥taro.yamada¥AppData¥Local¥Temp¥_jsh.exe" cmd="¥¥172.24.0.1 -u
""PC4¥taro.yamada"" -p ""S0lit0n"" -accepteula -d -s -c -f
""C:¥Users¥TARO~1.YAM¥AppData¥Local¥Temp¥_bbh.exe""""
parentPath="D:¥28858cc6e05225f7d156d1c6a21ed11188777fa0a752cb7b56038d79a88627cc.exe"
sha256=3337e3875b05e0bfba69ab926532e3f179e8cfbf162ebb60ce58a0281437a7ef
company="Sysinternals - www.sysinternals.com" copyright="Copyright (C) 2001-2016 Mark
Russinovich" fileDesc="Execute processes remotely" fileVer="2.2" product="Sysinternals
PsExec" productVer="2.2" crTime="03/27/2018 19:41:47.879" acTime="03/27/2018
19:41:47.879" moTime="03/27/2018 19:41:47.879" size=339096 sig=Valid signer="Microsoft
Corporation" issuer="Microsoft Code Signing PCA 2011" cerSN="33 00 00 00 64 47 84 94
86 db 41 19 38 00 00 00 00 00 64" validFrom="10/29/2015 05:31:46.000"
validTo="01/29/2017 05:31:46.000"
```

ファイル名：_jsh.exe
会社：Sysinternals - www.sysinternals.com
著作権：Copyright (C) 2001-2016 Mark Russinovich
ファイルの説明：Execute processes remotely
製品名：Sysinternals PsExec
署名者名：Microsoft Corporation

子プロセスの中に、Windowsの署名のされたPsExecがあります(_jsh.exe）。
コマンドラインに事前に入手していた認証情報や、マルウェア実行環境から取得した認証情報などが確認できます。

Soliton Dataset 2018の利用例

- 動的解析に関する研究や対策開発に
  - 話題となったWell-analyzedなマルウェアの動作ログで マルウェア挙動の概要を学ぶことができます。
  - 物理環境でのマルウェア動作や、スクリプト・マクロ型マル ウェアの動作、マルウェアの横展開を確認できます。
  - 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。
    - ますます潜伏化する攻撃への対抗としてログ取得が注目されますが、 パフォーマンスやログ活用観点から、たくさん記録すればよいわけ ではないということを実感いただけるかも知れません。