Soliton Dataset 2018について

2017年12月1日
株式会社ソリトンシステムズ

※本資料に記載の内容は、2017年12月1日時点の予定であり、今後変更の可能性があるものです、あらかじめご了承ください。

Soliton Dataset 2018

- 目的
  - エンタープライズ向けセキュリティログ取得製品を利用し
    様々なマルウェア動作ログを提供することで、マルウェア対策
    の研究・開発の促進に寄与することを目指します
- 特長
  - Windows上でのマルウェア動作ログ
  - 横展開やMBR書き換え系マルウェアも
    可能な範囲で記録を取る方針

提供内容

- InfoTrace Mark II for Cyberのセキュリティログ
- VirusTotalにクエリした結果も付与
- 検体実行に関する補足情報
  - マルウェアを動作させるために特別な何かを実施した場合にはその情報も付与
    - DLLの実行引数など

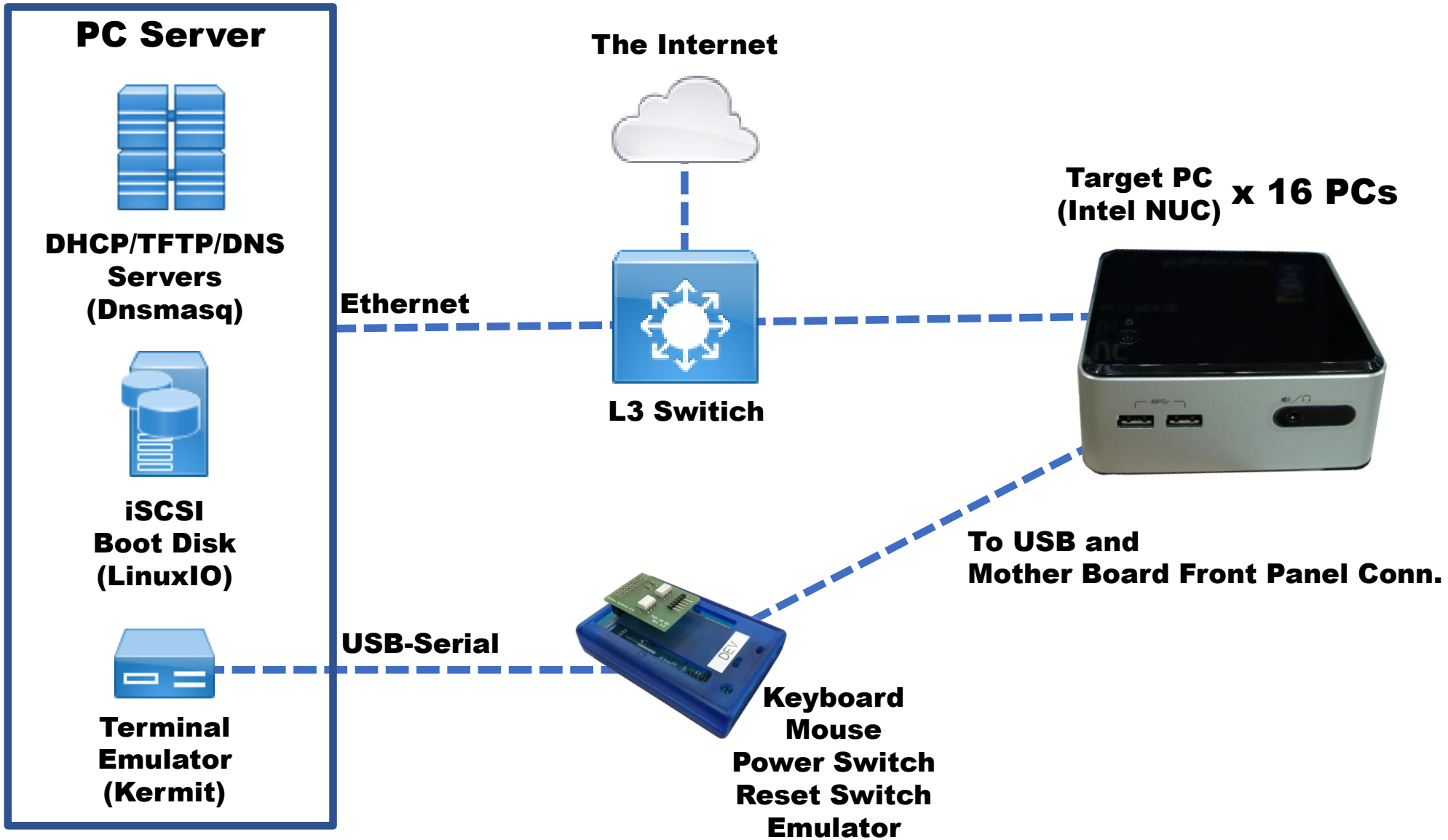
利用するマルウェア

- 収集元
  - VirusTotalを中心に独自に収集
- 収集方針
  - 影響が大きく、調査が必要と思われたマルウェアを対象に収集
  - 1年以内に話題になったもの・出来るだけ新しいものにフォーカス
- ファイルタイプ
  - PEだけではなく、スクリプトや、Officeマクロタイプも対象
    （動作するマルウェアであれば種類は問わない）
- 検体数
  - 量よりも質を重視しつつ、100検体分以上を目指す

ログ取得方針

- 1検体1ログファイル
  - ログはKey=Value形式
  - 1検体最大15分実行
    - 15分以上必要となることが分かった場合は延長するケースもあり
- 検体特性理解のために必要な情報は出来る限り取得
  - 横展開するマルウェアは複数端末にて実行
  - MBR書き換えを行うものも記録可能な範囲で取得
- マルウェア実行環境
  - Windows 7 32bit
  - 詳細は次ページ以降ご参照

マルウェア実行環境概要（コードネーム：Tsurutus）



マルウェア実行 PC

マルウェア実行環境の特長

- ButtonClicker 改め、CrazyClicker

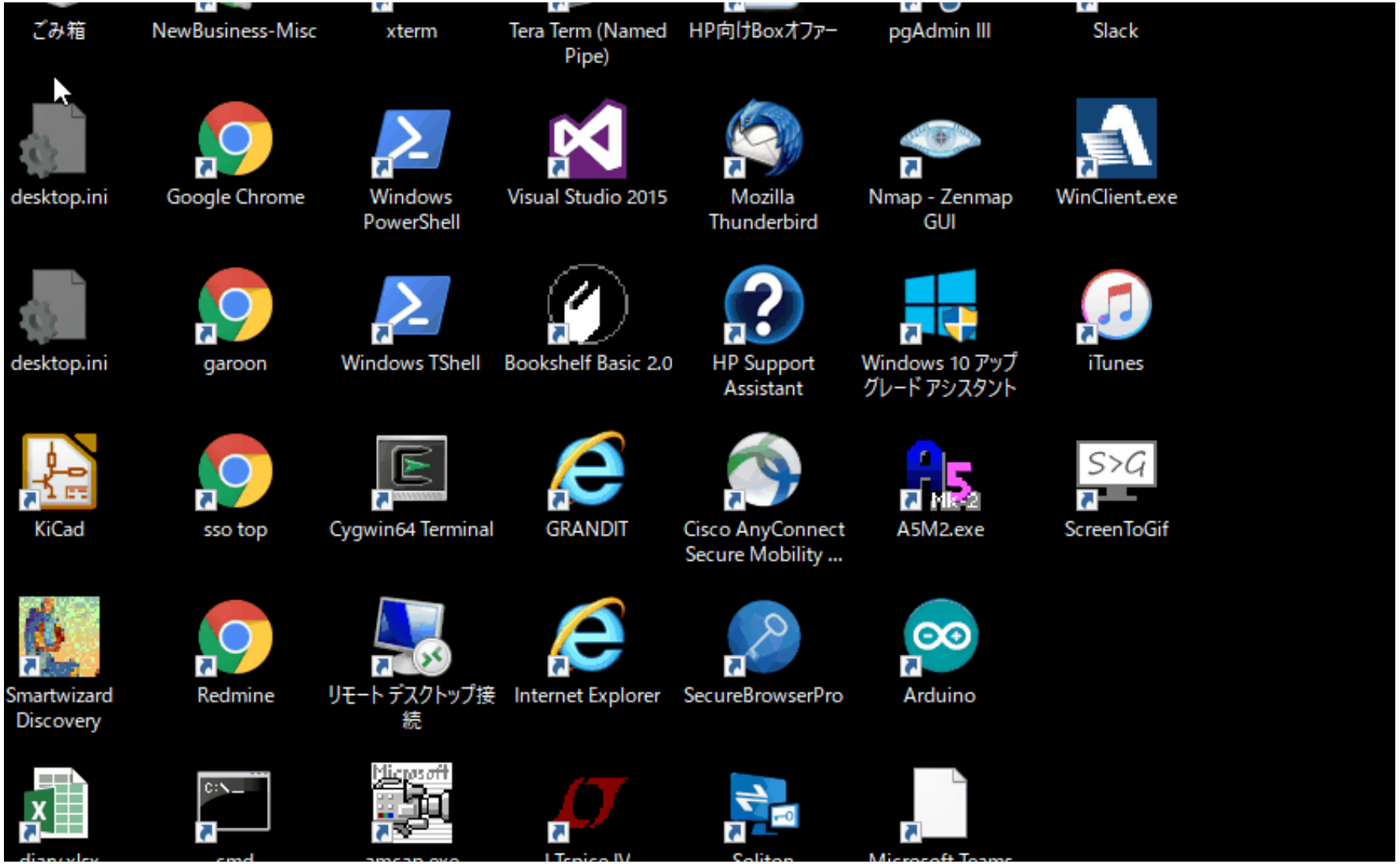
  マルウェアの活性化をアシストすべく、画面に現れる実行警告ダイアログ等のボタンを自動で認識し、クリックしていくプログラム。

- ディスクのロールバック

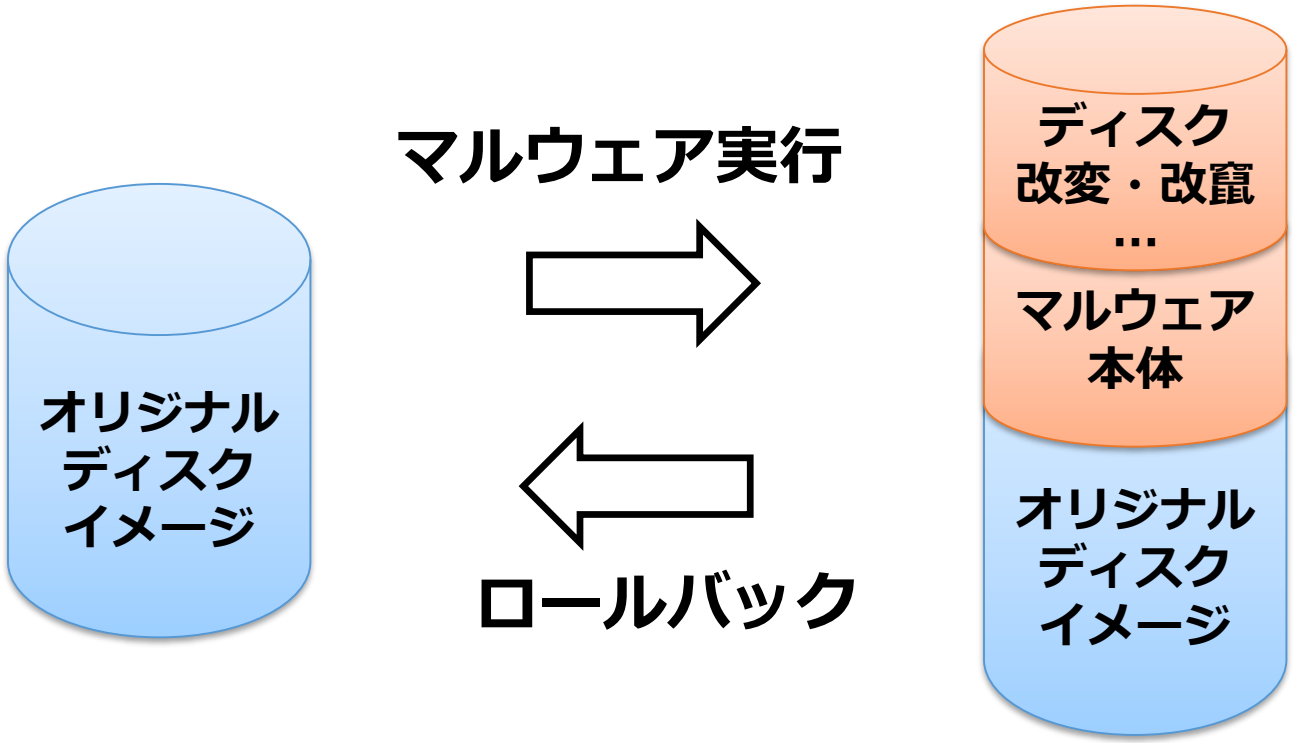
  バッキングストアに dm-thin を使ったブロックデバイスを利用

  – ファイルシステムの余計な処理が無い

ボタン出現自動認識＆自動クリック CrazyClicker



Device-Mapper (dm-thin) を使った ブロックデバイス層でのディスクのロールバック



例) /dev/mapper/boot/win7-x86-pc1

このブロックデバイス を iSCSI ターゲットの
バッキングストアとして使用

InfoTrace Mark II for Cyber（以下Mark II）

- 国産EDR
  - セキュリティログ、アプリ・通信制御などを実装

- セキュリティログ機能
  - プロセスチェーンを追えるように独自IDを付与
  - ファイルハッシュ値を記録（MD5/SHA1/SHA256）
  - プロセス・ファイル・レジストリ・ネットワークはカーネルレベルで監視
  - データセットでは、監視除外フィルタを外した状態で記録

Mark II ログ例 ①

06/30/2017 13:13:13.890 +0900 loc=ja-JP type=ITM2 sn=20612 evt=ps subEvt=start com="MWC01" domain="WORKGROUP"
profile="MWCtest" tmid=e4009d1d-9311-4249-9487-a373cde7192 3463664321-2923530833-3546627382
ip=172.31.48.118,fe80::5992:af4e:8c90:5591 mac=06:4d:00:f9:a6:d5 usr="admin1"
psGUID={4EEBA2F1-FB65-42BF-A258-4121E64FB1D7} psPath="C:¥Windows¥System32¥rundll32.exe" cmd="027cc.dll #1"
4E94-92FB-974428120B84} parentPath="C:¥Windows¥System32¥cmd.exe"
psUser="admin1" psDomain="MWC01" arc=x86 sha256=3fa4912eb43fc304652d7b01f118589259861e 3e54d5f987670
sha1=892503b20247b341cfd20dda5fdacfa41527a087 md5=c648901695e275c8f2ad04b687a68ce2 company="Microsoft Corporation"
copyright="c Microsoft Corporation. All rights reserved." fileDesc="Windows ホスト プロセス (Rundll32)" fileVer="6.1.7600.16385
(win7_rtm.090713-1255)" product="MicrosoftR WindowsR Operating System" productVer="6.1.7600.16385" crTime="06/30/2017
12:50:51.609" acTime="06/30/2017 12:50:51.609" moTime="03/30/2017 23:58:17.736" size=45056 sig=Valid signer="Microsoft
Windows" issuer="Microsoft Windows Verification PCA" cerSN="33 00 00 00 4c 80 d5 f9 98 50 76 b0 9c 00 01 00 00 00 4c"
validFrom="03/02/2017 03:46:04.000" validTo="05/10/2018 03:46:04.000"

プロセスがスタート

実行プロセスのパス（psPath）とコマンド引数

psGUIDは、プロセスごとに付与するソリトン独自ID

親プロセスのパス

06/30/2017 13:13:14.415 +0900 loc=ja-JP type=ITM2 sn=20626 evt=file subEvt=close com="MWC01" domain="WORKGROUP"
profile="MWCtest" tmid=e4009d1d-9311-4249-9487-a373cde7192c 463664321-2923530833-3546627382
ip=172.31.48.118,fe80::5992:af4e:8c90:5591 mac=06:4d:00:f9:a6:d5 usr="admin1" usrDomain="MWC01" sessionID=2
psGUID={4EEBA2F1-FB65-42BF-A258-4121E64FB1D7} psPath="C:¥Windows¥System32¥rundll32.exe"
path="C:¥Windows¥dllhost.dat" drvType=HDD read=0 write=381816 pe=1 arc=x86
sha256=f8 0c277ce49c60e35c029ff29 1f3fb02670d5
sha1=cd23b7c9e0edef184930bc8e0ca2264f0608bcb3 md5=aeee996fd3484f28e5cd85fe26b6bdcd company="Sysinternals -
www.sysinternals.com" copyright="Copyright (C) 2001-2010 Mark Russinovich" fileDesc="Execute processes remotely" fileVer="1.98"
product="Sysinternals PsExec" productVer="1.98" crTime="06/30/2017 13:13:14.414" acTime="06/30/2017 13:13:14.414"
moTime="06/30/2017 13:13:14.414" size=381816 sig=Valid signer="Microsoft Corporation" issuer="Microsoft Code Signing PCA"
cerSN="61 01 cf 3e 00 00 00 00 00 0f" validFrom="12/0 " validTo="03/08/2011 07:40:29.000"

ファイルをクローズ

実行プロセスのパス

対象ファイルのパス

書き込みバイト数

プロダクト名はPsExec

Microsoftの正規署名付き

Mark II ログ例 ②

06/30/2017 13:18:34.449 +0900 loc=ja-JP type=ITM2 sn=22085 evt=file subEvt=create com="MWC01" domain="WORKGROUP" profile="MWCtest"
tmid=e4009d1d-9311-4249-9487-a373cde7192c csid=S-1-5-21-3 33-3546627382 ip=172.31.48.118,fe80::5992:af4e:8c90:5591
mac=06:4d:00:f9:a6:d5 usr="admin1" usrDomain="MWC01" sessionID=2 psGUID={4EEBA2F1-FB65-42BF-A258-4121E64FB1D7}
psPath="C:¥Windows¥System32¥rundll32.exe" mntFld="¥¥172.31.48.79¥admin$" path="¥¥172.31.48.79¥admin$¥027cc.dll" drvType=Net

ファイルをクリエイト

06/30/2017 13:18:34.459 +0900 loc=ja-JP type=ITM2 sn=22087 evt=file subEvt=copy co st"
tmid=e4009d1d-9311-4249-9487-a373cde7192c csid=S-1-5-21-346 33-3546627382 ip=172.31.48.118,fe80::5992:af4e:8c90:5591
mac=06:4d:00:f9:a6:d5 usr="admin1" usrDomain="MWC01" sessionID=2 psGUID={4EEBA2F1-FB65-42BF-A258-4121E64FB1D7}
psPath="C:¥Windows¥System32¥rundll32.exe" path="C:¥Users¥admin1¥Desktop¥027cc.dll" drvType=HDD dstMntFld="¥¥172.31.48.79¥admin$"
dstPath="¥¥172.31.48.79¥admin$¥027cc.dll" dstDrv=Net sha256=027cc450ef
sha1=34f917aaba5684fbe56d3c57d48ef2a1aa7cf06d md5=71b6a493388e7d0
acTime="06/30/2017 13:18:34.078" moTime="06/30/2017 13:18:34.078" size=362360

rundll32.exeが管理共有経由で別端末に027cc.dllを生成

ファイルをコピー

rundll32.exeが、ローカルの027cc.dllを、別端末の027cc.dllにコピー

06/30/2017 13:18:34.459 +0900 loc=ja-JP type=ITM2 sn=22088 evt=file subEvt=close com="MWC01" domain="WORKGROUP" profile="MWCtest"
tmid=e4009d1d-9311-4249-9487-a373cde7192c csid=S-1-5-21-34 33-3546627382 ip=172.31.48.118,fe80::5992:af4e:8c90:5591
mac=06:4d:00:f9:a6:d5 usr="admin1" usrDomain="MWC01" sessionID=2 psGUID={4EEBA2F1-FB65-42BF-A258-4121E64FB1D7}
psPath="C:¥Windows¥System32¥rundll32.exe" mntFld="¥¥172.31.48.79¥admin$" path="¥¥172.31.48.79¥admin$¥027cc.dll" drvType=Net read=0
write=362360 pe=1 arc=x86 crTime="06/30/2017 13:18:34.078" acTime="06/30 7 13:18:34.078"
size=362360 sig=Invalid signer="Microsoft Corporation" issuer="Microsoft Code Signing PCA" cerSN="61 01 cf 3e 00 00 00 00 0f"
validFrom="12/08/2009 07:40:29.000" validTo="03/08/2011 07:40:29.000"

ファイルをクローズ

別端末の027cc.dllに、362360byte書き込み

Microsoftを騙っているが、正規署名ではない

06/30/2017 13:18:34.460 +0900 loc=ja-JP type=ITM2 sn=22086 lv=5 evt=ps subEvt=start com="MWC01" domain="WORKGROUP" profile="MWCtest"
tmid=e4009d1d-9311-4249-9487-a373cde7192c csid=S-1-5-21-346 33-3546627382 ip=172.31.48.118,fe80::5992:af4e:8c90:5591
mac=06:4d:00:f9:a6:d5 usr="admin1" usrDomain="MWC01" sessionID=2 psGUID={5FE60
psPath="C:¥Windows¥dllhost.dat" cmd="¥¥172.31.48.79 -accepteula -s -d C:¥Windows¥System32¥rundll32.exe ""C:¥Windows¥027cc.dll"",#1 55"
psID=4032 parentGUID={4EEBA2F1-FB65-42BF-A258-4121E64FB1D7} parentPath="C:¥Windows¥System32¥rundll32.exe" psUser="admin1"
psDomain="
sha1=cd23b eee996fd3484f28e5cd85fe26b6bdcd company="Sysinternals - www.sysinternals.com"
copyright="Copyright (C) 2001-2010 Mark Russinovich" fileDesc="Execute processes remotely" fileVer="1.98" product="Sysinternals PsExec"
productVer="1.98" crTime="06/30/2017 13:13:14.414" acTime="06/30/2017 13:13:14.414" moTime="06/30/2017 13:13:14.414" size=381816
sig=Valid signer="Microsoft Corporation" issuer="Microsoft Code Signing PCA" cerSN="61 01 cf 3e 00 00 00 00 0f" validFrom="12/08/2009
07:40:29.000" validTo="03/08/2011 07:40:29.000"

実行プロセスは、dllhost.dat

プロセスがスタート

管理共有経由で、PsExec(dllhost.dat)が、別端末の027cc.dllを実行

親プロセスのGUIDより、これまで仕事をしてきた
rundll32.exeが親であることが分かる

親プロセスは、rundll32.exe

Soliton Datasetの利用例

- 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。
    - 仮想環境では動作しないマルウェアや、スクリプト・マクロ型マルウェアの動作を確認できます。
    - 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。

- マルウェア実行環境（Tsurutus）
  - Mark IIログ取得用環境です、ご興味ある方はお声がけください。