\Orchestrating a brighter world NEC

Hardening Designers Conference 2023
「濃厚なサイバーセキュリティ最前線:攻撃手法の解析とAnsibleによる堅牢化の自動化」

# インシデント対応から学ぶログ解析テクニック

2023年5月20日

NEC　サイバーセキュリティ戦略統括部　セキュリティ技術センター
リスクハンティング・アナリシスグループ

# \Orchestrating a brighter world

NECは、安全・安心・公平・効率という社会価値を創造し、
誰もが人間性を十分に発揮できる持続可能な社会の実現を目指します。

# Hardening競技会とインシデント対応

◆ Hardening競技会ではkuromame 6による苛烈な攻撃に耐えつつ、
システムを守り、ビジネスを継続させる必要がある


**Kuromame 6からの攻撃を全て防ぐのは難しい**
**≒**
**インシデント対応は必ず発生する**

# NECが行うインシデント対応

## ファストフォレンジック†を基本とした対応を実施

†早急な原因究明、侵入経路や不正な挙動を把握するため、必要最低限のデータを抽出及びコピーし、解析すること[1]

### Windows端末で解析するデータの例

イベントログ
ジャーナル
レジストリ
プリフェッチ
etc

### Linux端末で解析する対象の例

ログ(SSH、HTTP等)
cron
サービスの設定ファイル
etc

[1]デジタル・フォレンジック研究会| 証拠保全ガイドライン第8版
https://digitalforensic.jp/wp-content/uploads/2021/05/gl8-20210520.pdf

# なぜファストフォレンジックなのか？

# ファストフォレンジックの重要性

- ビジネスを継続する→原因追求も行いつつ、ビジネスの復旧を優先するために、完璧なフォレンジックではなく早く適切なフォレンジックが求められる

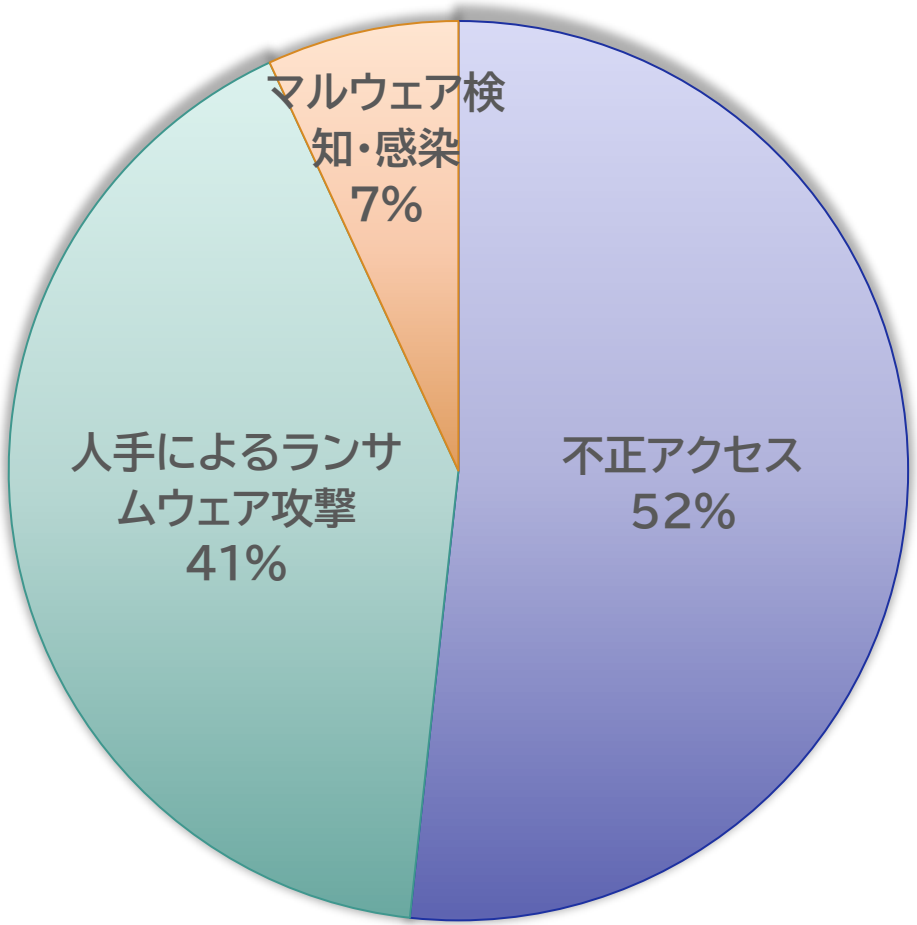
- ファストフォレンジックで見ていくところ
  - 侵入経路/侵害範囲の特定
  - 悪性ファイルの検出・バックドアの有無
  - 情報漏えいの範囲特定

このようなインシデント対応を行っている我々が経験したインシデントについて
全体感からどのように効率化しているかを説明していきます。

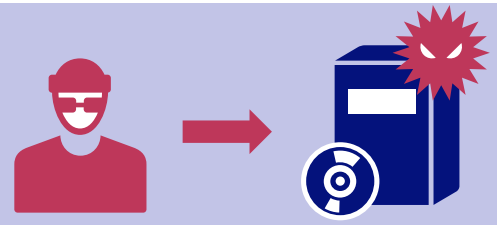
# インシデント対応の全体感

# インシデントの種別

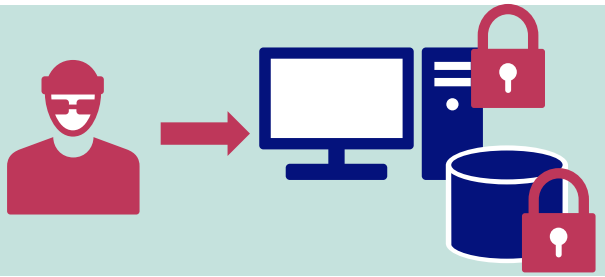
私のチームで対応した攻撃者が明確に存在するインシデントについて
大まかな分類とその割合を紹介



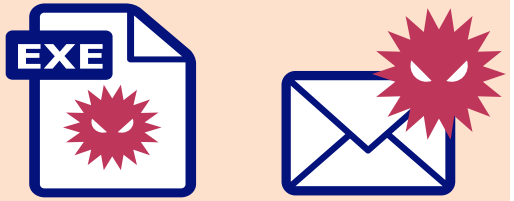

**不正アクセス**
既知の脆弱性や自作したアプリケーションの脆弱性を悪用された事案



**人手によるランサムウェア攻撃**
組織内ネットワーク(NW)に侵入し、ランサムウェアを実行された事案



**マルウェア検知・感染**
メールに添付されていたマルウェアを開いた/セキュリティソフトにより、マルウェアを検知した事案



# 組織内NWへの侵入手口[Tactic:Initial Access]

組織内ネットワーク(NW)への侵入時に使われた手口を記載
1件で複数の手口が使われることもあるため、使用された割合を表示

**正規のアカウントの悪用[Valid Account T1078] ー 55%**

組織で使用されている正規のアカウント(デフォルトのアカウント含む)のクレデンシャル情報を取得し、組織内NWへ侵入

**脆弱性の悪用[Exploit Public-Facing Application T1190] ー 23%**

外部へ公開しているサービス・アプリケーションの脆弱性を悪用し、組織内NWへ侵入

**ドライブバイダウンロード攻撃[Drive-by Compromise T1189] - 5%**

従業員等が使用しているブラウザに脆弱性があり、攻撃者が用意しているサイトへアクセスしたことで、組織内NWへ侵入された。

原因不明:18%

# 正規のアカウントの悪用[Valid Account T1078]

## 組織で使用されている正規のアカウント(デフォルトのアカウント含む)のクレデンシャル情報の取得方法[Tactic: Credential Access]

- Brute Force[T1110]
  パスワードが不明な場合やパスワードハッシュを入手したときに行う総当たり攻撃による手法
- インシデントで確認した手口
  オープンポート(SSHやRDP等)に対して、
  ランダムなユーザ名とパスワードによるブルートフォース攻撃

- Exploitation for Credential Access[T1212](Acquire Access?[T1650])
  クレデンシャル情報取得のためにソフトウェアの脆弱性を悪用する手法
- インシデントで確認した手口
  - FortiGateやSonicWall等のVPN製品の脆弱性を悪用した攻撃でクレデンシャル情報を入手

# 脆弱性の悪用[Exploit Public-Facing Application T1190]

## 既知の脆弱性・自作アプリケーションのプログラムの脆弱性の割合

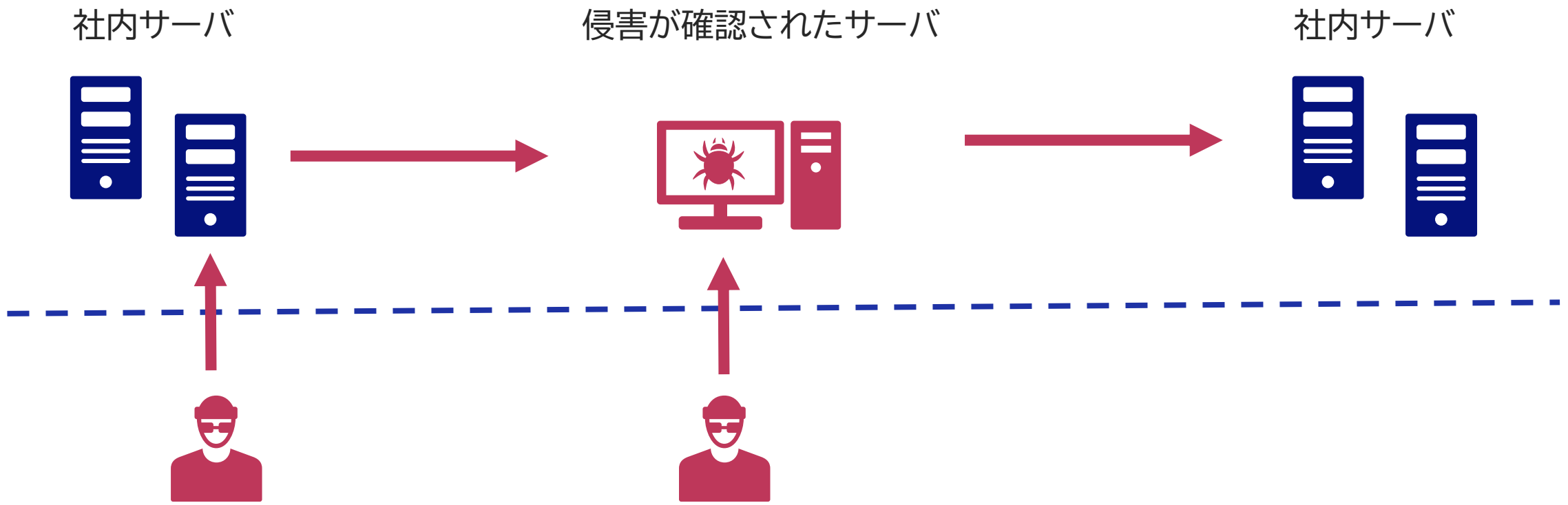
- 既知の脆弱性を狙った攻撃と侵害 - 60%
  - CVEが採番されている攻撃に対する攻撃
  - 攻撃時点で、ゼロデイではなくすでにパッチ公開済み
- 自作のアプリケーション部分に対する攻撃 - 40%
  - SQLインジェクションや認証バイパス等の作成したアプリケーションに脆弱な点がある内容
  - セキュア開発が重要

# 効率的なログ解析

これまでに確認してきた攻撃、使われたテクニックからどういう
部分を見ていくのかを紹介

# 侵入されたサーバ・端末の特定

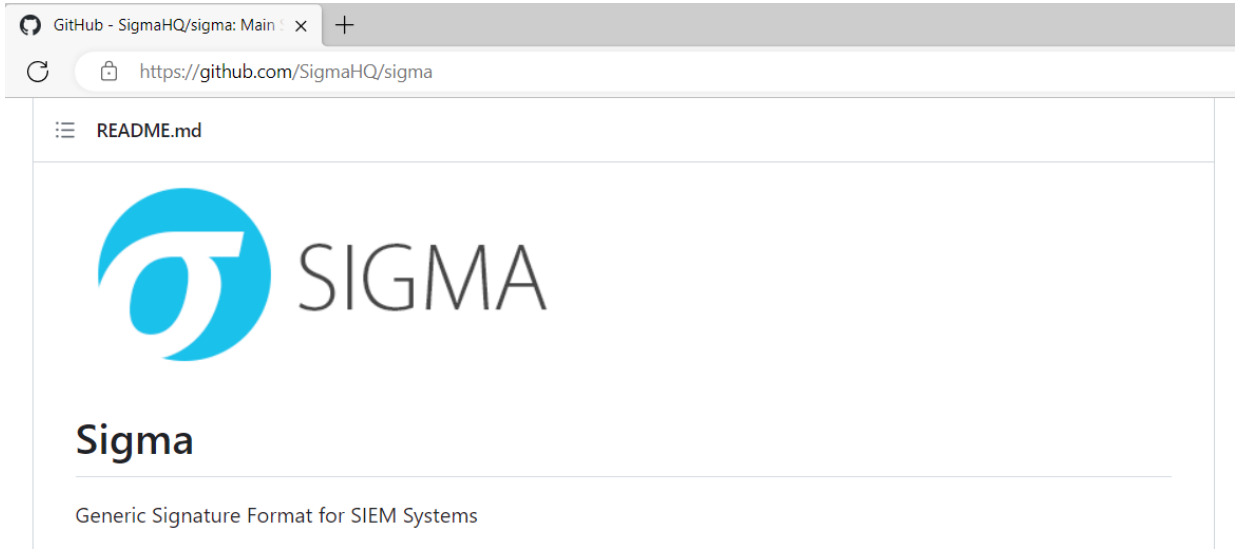
インシデントが発覚し、組織内NWに侵害された恐れがある場合、
どこまで影響範囲が及んでいるか素早く特定する必要がある。



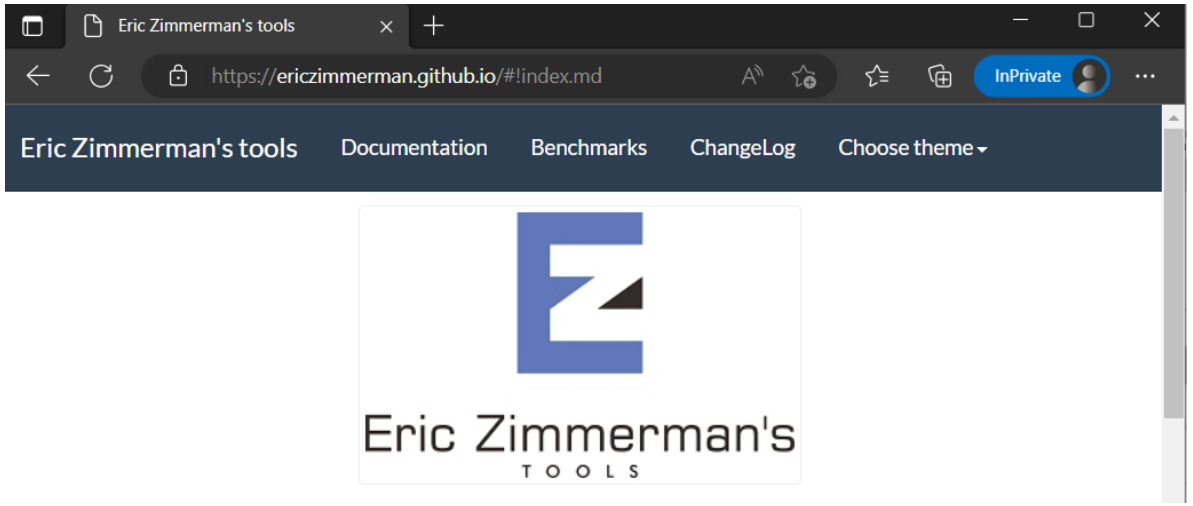

侵害が行われたサーバと侵害が行われていないサーバを切り分けることで優先順位をつけることができる。
起点はどこからかを特定すると探索範囲が絞れる（2023/1/12に侵害の痕跡があれば、1/11以前のログの確認の優先度が下がる）

# HAYABUSA & SIGMA & EZtools


https://github.com/Yamato-Security/hayabusa




https://github.com/SigmaHQ/sigma




https://ericzimmerman.github.io/#!index.md

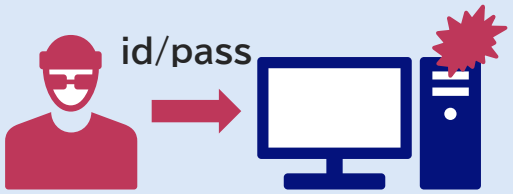
# ツールを使いこなしていく

Hayabusa、Sigma、EZtoolsはとても便利なツール
まずはHayabusaやSigmaを使って、大まかな攻撃の流れを把握するのがよい


理想的な流れ

インシデント対応時に、何を確認し説明できるようにするのか
ツールの使い方や着目点の一部を説明していきます。

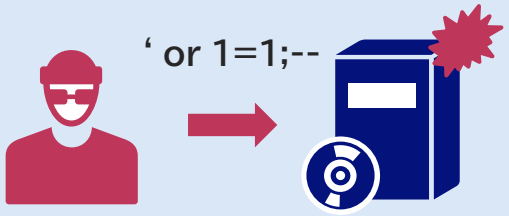
# 初期侵入で見る点




## 不審なログインの有無

- ブルートフォース攻撃
  ⇒多数のログイン試行がないか調査
- 漏えいしたVPN接続情報による攻撃
  ⇒VPN装置のバージョンが最新か確認

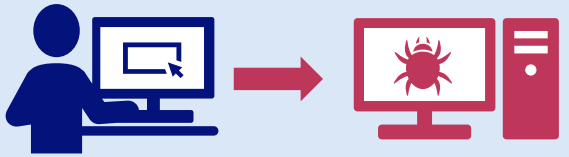
ログイン試行は統一的な調査が可能




## 脆弱性による攻撃

- 既知の脆弱性
  ⇒検出方法を確認して調査
- 未知の脆弱性
  ⇒通常と異なるログがないか調査

製品や調査能力に依存

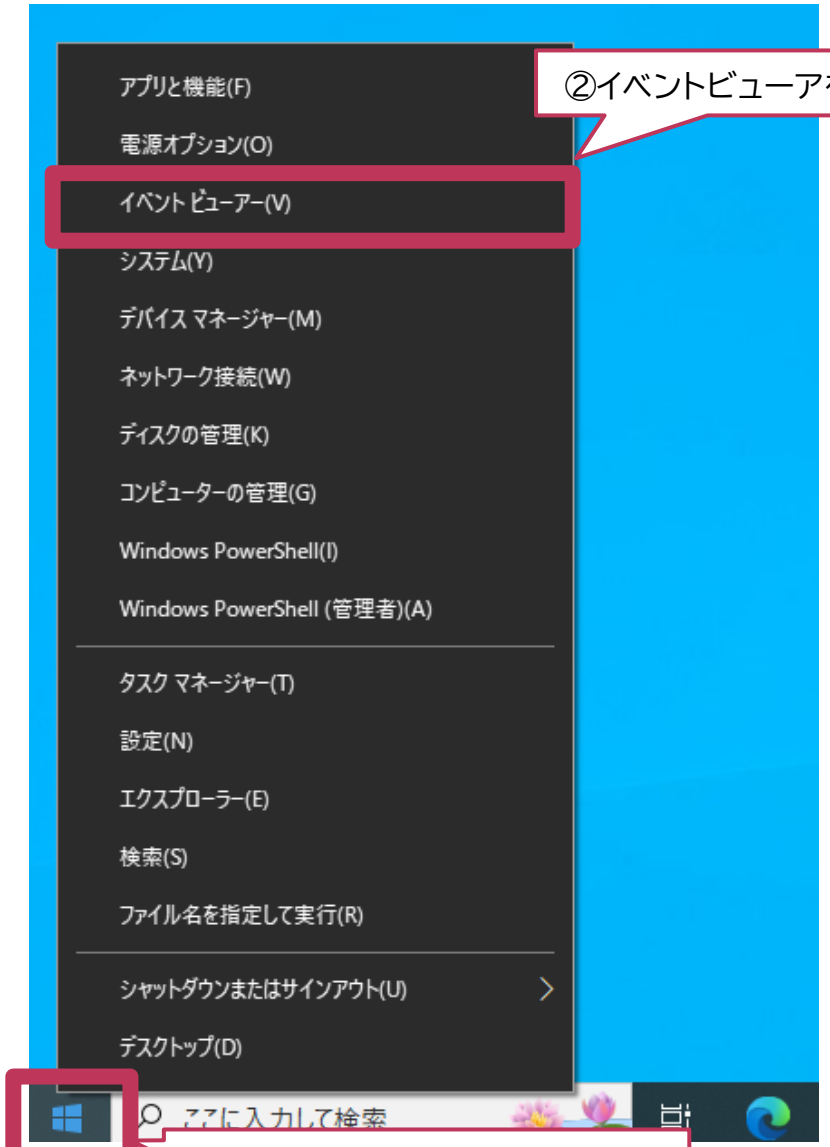


## ユーザ操作による感染

- 攻撃者が用意したサイトへのアクセス
  ⇒不審なドメインの調査
- メールの添付ファイル
  ⇒検体の確保・調査

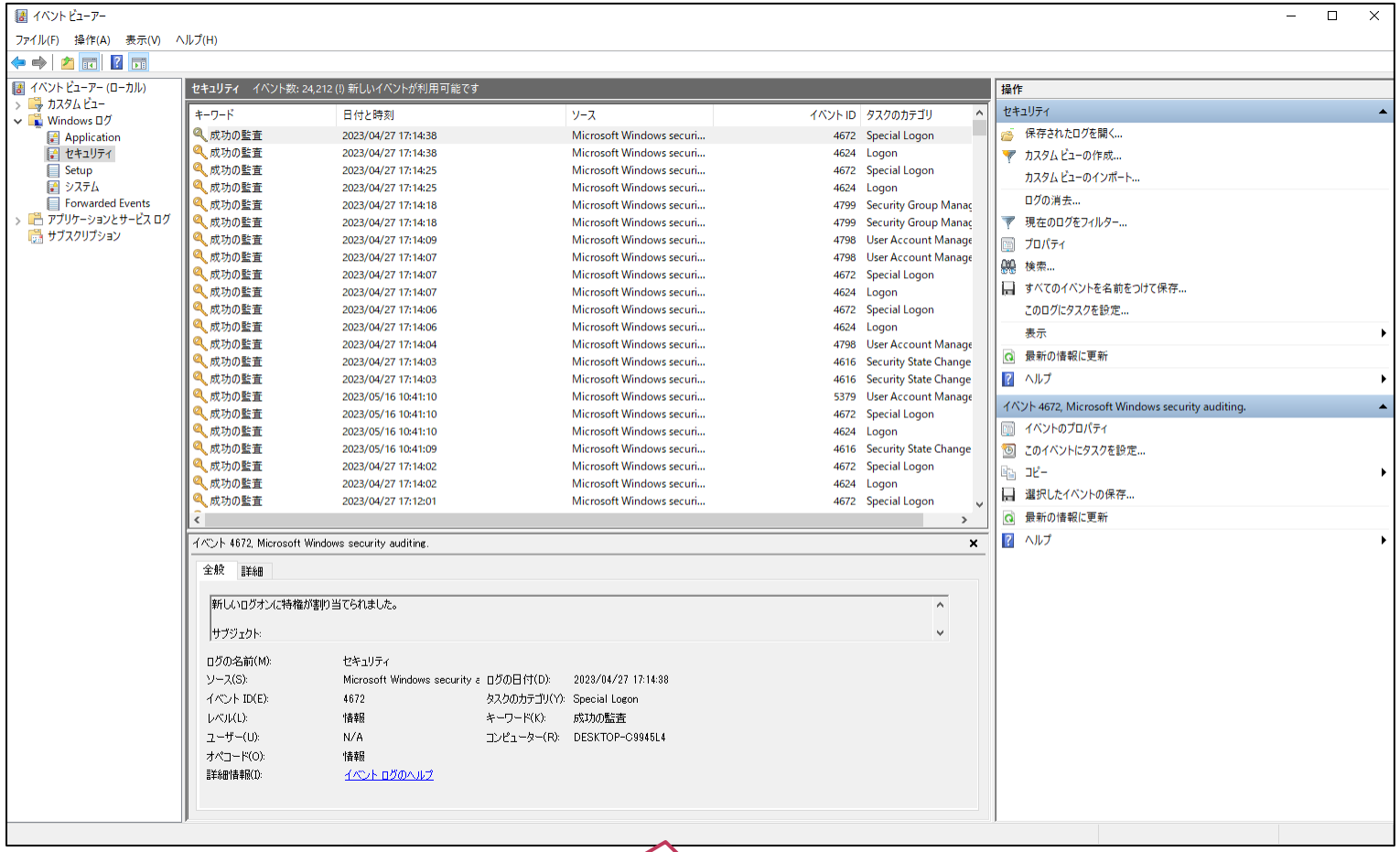
ヒアリング・Proxy等の調査

# Windowsイベントログの確認方法




②イベントビューアを選択

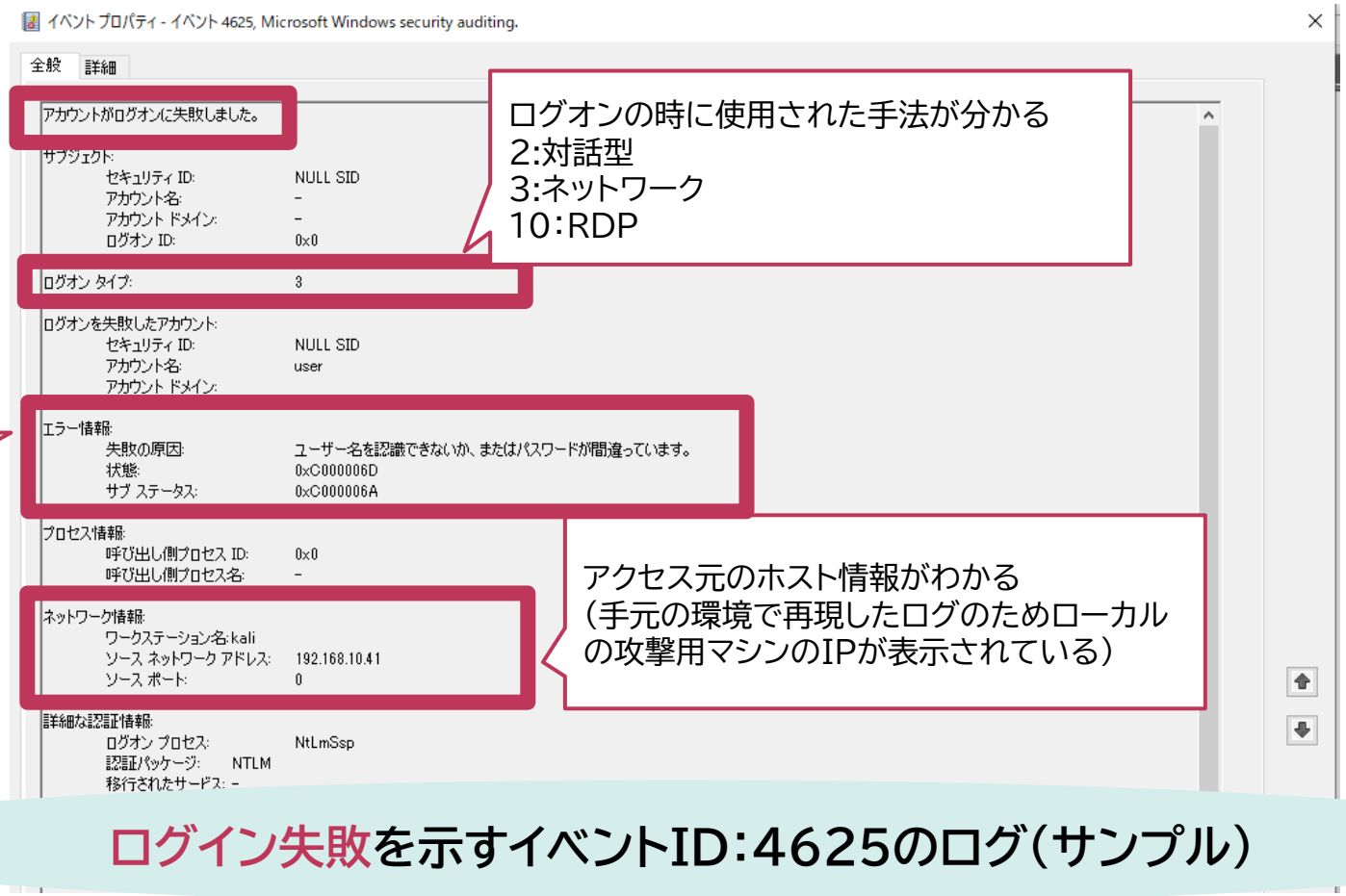
①Windowsのボタンを右クリック




③イベントログを確認可能になる

# ブルートフォース攻撃の調査 – Windowsイベントログ(1/2)

- Securityイベントログのイベント ID:4624と4625を確認
  - 特定のIPからのログオン失敗の試行(イベントID:4625)が複数確認された後のログイン成功(イベントID:4624)はブルートフォースと推測可能




ログオンの失敗が記載

ログオンの時に使用された手法が分かる
2:対話型
3:ネットワーク
10:RDP

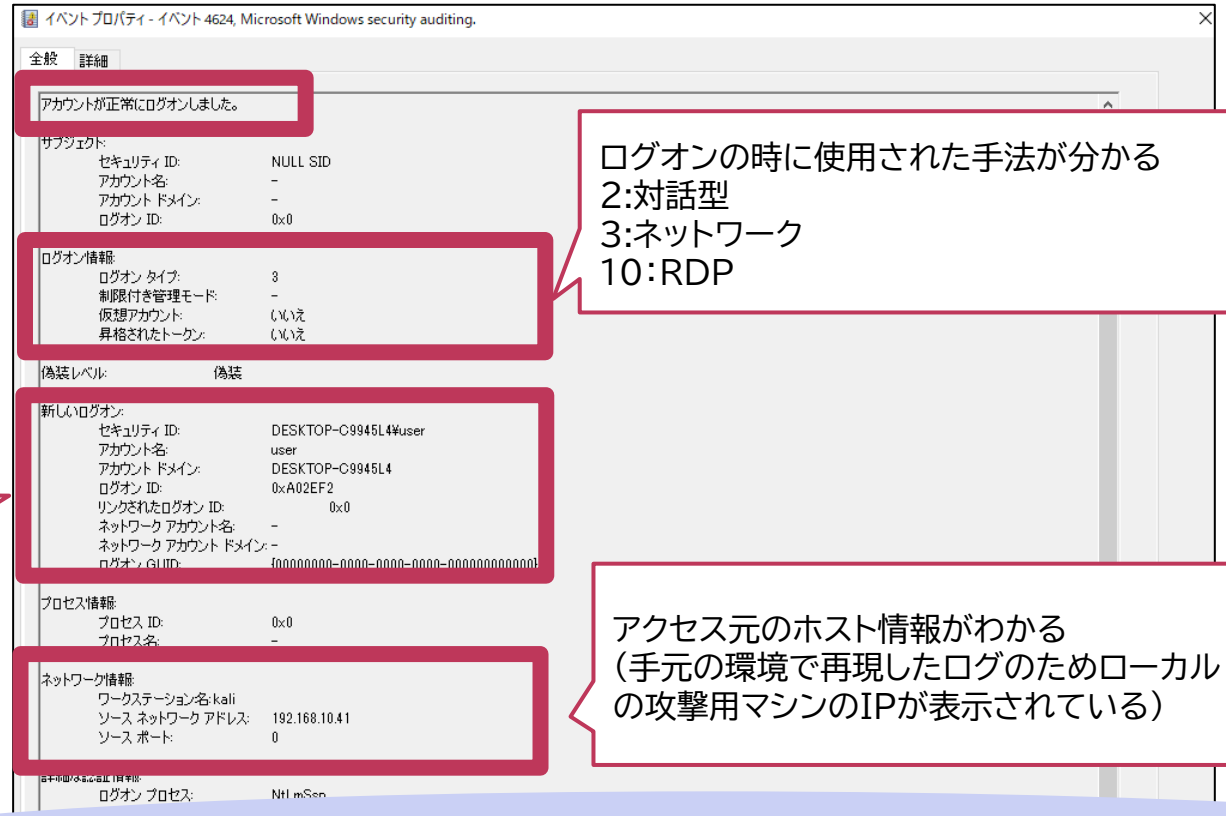
失敗の理由が記載されている

アクセス元のホスト情報がわかる
(手元の環境で再現したログのためローカルの攻撃用マシンのIPが表示されている)

ログイン失敗を示すイベントID:4625のログ(サンプル)

# ブルートフォース攻撃の調査 – Windowsイベントログ(2/2)

- Securityイベントログのイベント ID:4624と4625を確認
  - 特定のIPからのログオン失敗の試行(イベントID:4625)が複数確認された後のログイン成功(イベントID:4624)はブルートフォースと推測可能




**ログオンの成功**が記載

ログオンの時に使用された手法が分かる
2:対話型
3:ネットワーク
10:RDP

ログインしたアカウントの情報

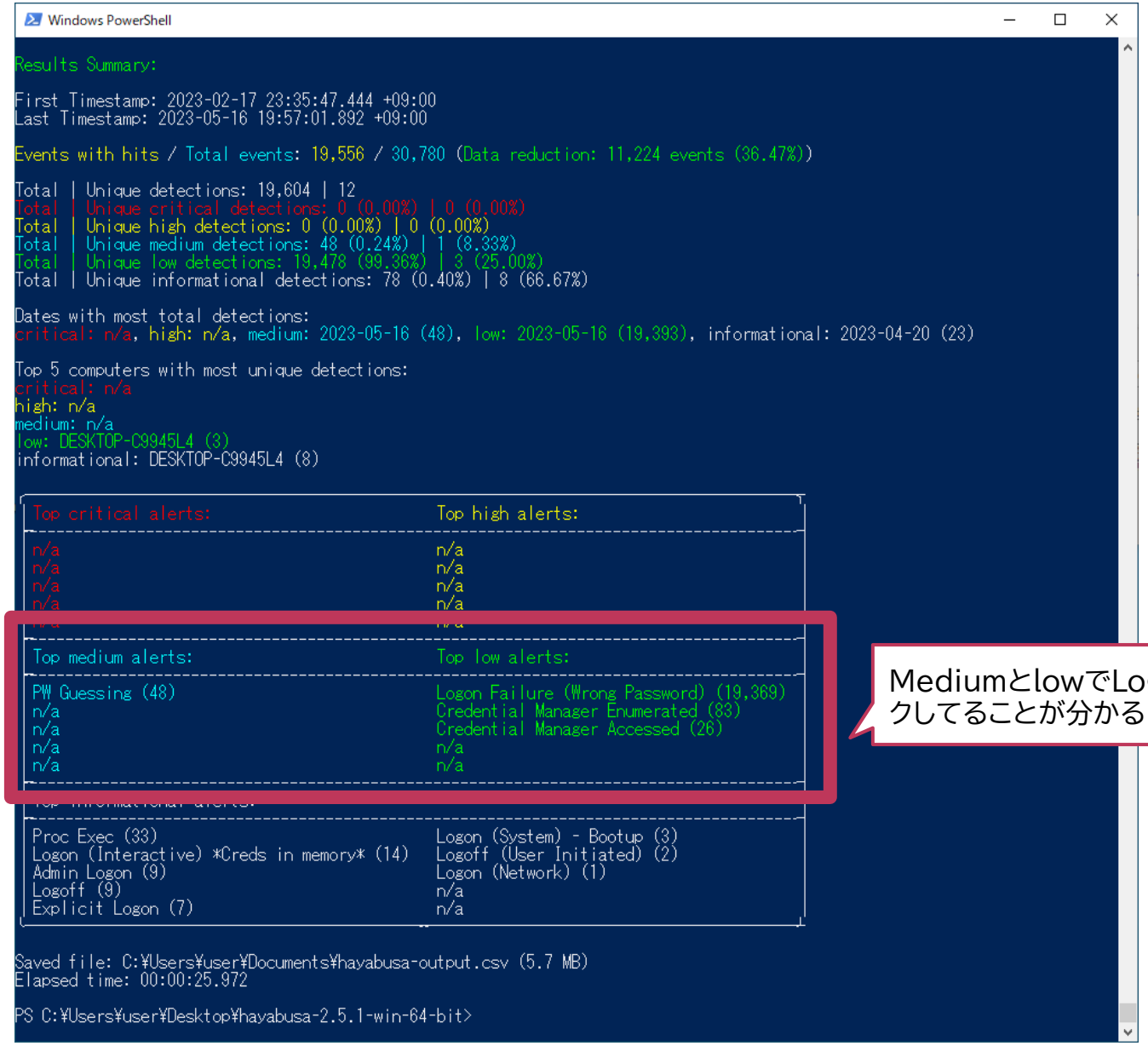
アクセス元のホスト情報がわかる
(手元の環境で再現したログのためローカルの攻撃用マシンのIPが表示されている)

**ログイン成功**を示すイベントID:4624のログ(サンプル)

セキュリティ　イベント数: 29,814 (!) 新しいイベントが利用可能です

| キーワード | 日付と時刻 | ソース | イベント ID | タスクのカテゴリ |
|---|---|---|---|---|
| 失敗の監査 | 2023/05/16 12:41:48 | Microsoft Windows securi... | 4625 | Logon |
| 失敗の監査 | 2023/05/16 12:41:48 | Microsoft Windows securi... | 4625 | Logon |
| 失敗の監査 | 2023/05/16 12:41:47 | Microsoft Windows securi... | 4625 | Logon |
| 失敗の監査 | 2023/05/16 12:41:46 | Microsoft Windows securi... | 4625 | Logon |
| 失敗の監査 | 2023/05/16 12:41:46 | Microsoft Windows securi... | 4625 | Logon |
| 失敗の監査 | 2023/05/16 12:41:45 | Microsoft Windows securi... | 4625 | Logon |
| 失敗の監査 | 2023/05/16 12:41:44 | Microsoft Windows securi... | 4625 | Logon |
| 失敗の監査 | 2023/05/16 12:41:44 | Microsoft Windows securi... | 4625 | Logon |
| 失敗の監査 | 2023/05/16 12:41:43 | Microsoft Windows securi... | 4625 | Logon |
| 失敗の監査 | 2023/05/16 12:41:42 | Microsoft Windows securi... | 4625 | Logon |
| 失敗の監査 | 2023/05/16 12:41:41 | Microsoft Windows securi... | 4625 | Logon |
| 失敗の監査 | 2023/05/16 12:41:41 | Microsoft Windows securi... | 4625 | Logon |
| 失敗の監査 | 2023/05/16 12:41:40 | Microsoft Windows securi... | 4625 | Logon |
| 失敗の監査 | 2023/05/16 12:41:39 | Microsoft Windows securi... | 4625 | Logon |
| 失敗の監査 | 2023/05/16 12:41:39 | Microsoft Windows securi... | 4625 | Logon |
| 失敗の監査 | 2023/05/16 12:41:38 | Microsoft Windows securi... | 4625 | Logon |
| 失敗の監査 | 2023/05/16 12:41:37 | Microsoft Windows securi... | 4625 | Logon |
| 失敗の監査 | 2023/05/16 12:41:37 | Microsoft Windows securi... | 4625 | Logon |
| 失敗の監査 | 2023/05/16 12:41:36 | Microsoft Windows securi... | 4625 | Logon |
| 失敗の監査 | 2023/05/16 12:41:35 | Microsoft Windows securi... | 4625 | Logon |
| 失敗の監査 | 2023/05/16 12:41:35 | Microsoft Windows securi... | 4625 | Logon |
| 失敗の監査 | 2023/05/16 12:41:34 | Microsoft Windows securi... | 4625 | Logon |
| 失敗の監査 | 2023/05/16 12:41:33 | Microsoft Windows securi... | 4625 | Logon |
| 失敗の監査 | 2023/05/16 12:41:33 | Microsoft Windows securi... | 4625 | Logon |
| 失敗の監査 | 2023/05/16 12:41:32 | Microsoft Windows securi... | 4625 | Logon |
| 失敗の監査 | 2023/05/16 12:41:31 | Microsoft Windows securi... | 4625 | Logon |
| 失敗の監査 | 2023/05/16 12:41:30 | Microsoft Windows securi... | 4625 | Logon |
| 失敗の監査 | 2023/05/16 12:41:30 | Microsoft Windows securi... | 4625 | Logon |
| 失敗の監査 | 2023/05/16 12:41:29 | Microsoft Windows securi... | 4625 | Logon |
| 失敗の監査 | 2023/05/16 12:41:28 | Microsoft Windows securi... | 4625 | Logon |
| 失敗の監査 | 2023/05/16 12:41:28 | Microsoft Windows securi... | 4625 | Logon |
| 失敗の監査 | 2023/05/16 12:41:27 | Microsoft Windows securi... | 4625 | Logon |

# Hayabusaで確認(1/2)




MediumとlowでLogon Failureをチェックしてることが分かる

# Hayabusaで確認(2/2)

## ◆ Hayabusaが出力するCSVファイルでの確認

| | | |
|---|---|---|
| Logon Failure (Wrong Password) | Type: 3 ¦ TgtUser: user ¦ SrcComp: kali ¦ SrcIP: 192.168.10.41 ¦ AuthPkg: NTLM ¦ Proc: - | Sec_4625_Low_LogonFail_WrongPW.yml |
| Logon Failure (Wrong Password) | Type: 3 ¦ TgtUser: user ¦ SrcComp: kali ¦ SrcIP: 192.168.10.41 ¦ AuthPkg: NTLM ¦ Proc: - | Sec_4625_Low_LogonFail_WrongPW.yml |
| Logon Failure (Wrong Password) | Type: 3 ¦ TgtUser: user ¦ SrcComp: kali ¦ SrcIP: 192.168.10.41 ¦ AuthPkg: NTLM ¦ Proc: - | Sec_4625_Low_LogonFail_WrongPW.yml |
| Logon Failure (Wrong Password) | Type: 3 ¦ TgtUser: user ¦ SrcComp: kali ¦ SrcIP: 192.168.10.41 ¦ AuthPkg: NTLM ¦ Proc: - | Sec_4625_Low_LogonFail_WrongPW.yml |
| Logon Failure (Wrong Password) | Type: 3 ¦ TgtUser: user ¦ SrcComp: kali ¦ SrcIP: 192.168.10.41 ¦ AuthPkg: NTLM ¦ Proc: - | Sec_4625_Low_LogonFail_WrongPW.yml |

イベントログのログオンタイプと接続元を見やすく表示してくれる

このログを検知したルールを表示可能
（Profile verbose以上を選択）

## ◆ 検知したルールの確認 以下二つのものをチェックしていることが分かる

① セキュリティイベントログの4625のイベントID

② SubStatusが0xc000006a

```
author: Zach Mathis
date: 2020/11/08
modified: 2022/12/16

title: Logon Failure (Wrong Password)
description: Prints logon information.

id: e87bd730-df45-4ae9-85de-6c75369c5d29
level: low
status: stable
logsource:
    product: windows
    service: security
detection:
    selection_basic:
        Channel: Security
        EventID: 4625
    selection_wrong_password:
        SubStatus: "0xc000006a" #Wrong password
    condition: selection_basic and selection_wrong_password
falsepositives:
    - user mistypes password
tags:
references:
ruletype: Hayabusa
```

# EZToolsで確認

## ◆ EvtxECmd.exeを使用する

- EvtxECmdはWindowsイベントログをcsvやjsonの形式で全て書き出してくれる。
- フィルタも可能で特定のイベントIDのみを抜き出すといったことも可能。

```
EvtxECmd.exe –f <イベントログ名> --inc <フィルタしたいイベントID> --exc <除外したいイベントID>
--csvf <出力先のcsvファイル名>
```

| s Id | Computer | Map Description | User Name | Remote Host | Payload Data1 | Payload Data2 | Payload Data3 | Payload Data4 |
|---|---|---|---|---|---|---|---|---|
| 660 | DESKTOP-C9945L4 | Failed logon | -\- | kali (192.168.10.41) | Target: \user | LogonType 3 | FailureReason1: the cause is either a ba… | FailureReason2: user name is correct but the password is wrong |
| 660 | DESKTOP-C9945L4 | Failed logon | -\- | kali (192.168.10.41) | Target: \user | LogonType 3 | FailureReason1: the cause is either a ba… | FailureReason2: user name is correct but the password is wrong |
| 660 | DESKTOP-C9945L4 | Failed logon | -\- | kali (192.168.10.41) | Target: \user | LogonType 3 | FailureReason1: the cause is either a ba… | FailureReason2: user name is correct but the password is wrong |
| 660 | DESKTOP-C9945L4 | Failed logon | -\- | kali (192.168.10.41) | Target: \user | LogonType 3 | FailureReason1: the cause is either a ba… | FailureReason2: user name is correct but the password is wrong |
| 660 | DESKTOP-C9945L4 | Failed logon | -\- | kali (192.168.10.41) | Target: \user | LogonType 3 | FailureReason1: the cause is either a ba… | FailureReason2: user name is correct but the password is wrong |
| 660 | DESKTOP-C9945L4 | Failed logon | -\- | kali (192.168.10.41) | Target: \user | LogonType 3 | FailureReason1: the cause is either a ba… | FailureReason2: user name is correct but the password is wrong |
| 660 | DESKTOP-C9945L4 | Failed logon | -\- | kali (192.168.10.41) | Target: \user | LogonType 3 | FailureReason1: the cause is either a ba… | FailureReason2: user name is correct but the password is wrong |
| 660 | DESKTOP-C9945L4 | Failed logon | -\- | kali (192.168.10.41) | Target: \user | LogonType 3 | FailureReason1: the cause is either a ba… | FailureReason2: user name is correct but the password is wrong |
| 660 | DESKTOP-C9945L4 | Failed logon | -\- | kali (192.168.10.41) | Target: \user | LogonType 3 | FailureReason1: the cause is either a ba… | FailureReason2: user name is correct but the password is wrong |
| 660 | DESKTOP-C9945L4 | Failed logon | -\- | kali (192.168.10.41) | Target: \user | LogonType 3 | FailureReason1: the cause is either a ba… | FailureReason2: user name is correct but the password is wrong |
| 660 | DESKTOP-C9945L4 | Failed logon | -\- | kali (192.168.10.41) | Target: \user | LogonType 3 | FailureReason1: the cause is either a ba… | FailureReason2: user name is correct but the password is wrong |
| 660 | DESKTOP-C9945L4 | Failed logon | -\- | kali (192.168.10.41) | Target: \user | LogonType 3 | FailureReason1: the cause is either a ba… | FailureReason2: user name is correct but the password is wrong |
| 660 | DESKTOP-C9945L4 | Failed logon | -\- | kali (192.168.10.41) | Target: \user | LogonType 3 | FailureReason1: the cause is either a ba… | FailureReason2: user name is correct but the password is wrong |
| 660 | DESKTOP-C9945L4 | Failed logon | -\- | kali (192.168.10.41) | Target: \user | LogonType 3 | FailureReason1: the cause is either a ba… | FailureReason2: user name is correct but the password is wrong |

# Hayabusa vs EvtxCmd

| Hayabusa | | EvtxCmd |
|---|---|---|
| ルールによって削減可能 | ノイズ | フィルタによる削減のみ |
| ルールを把握していなくても利用でき怪しい挙動を抽出可能 | 使いやすさ | 自分で確認をしたいイベントログやファイル等を理解しておく必要がある |
| どのルールによって出力されたログかを把握するのは、慣れが必要 | 出力されたものに対する理解度 | 目的にあったものを出力するため、確実に理解している |

**どちらがより優れているという話ではなく、目的に応じて使い分けましょう**

| | |
|---|---|
| 時間が少ない中で大まかな状態を把握したい（Hardening、フォレンジック初期） | Hayabusa |
| ログの見落としなく、証拠として残して置けるようにしたい | EvtxCmd |

# Linuxのログイン調査

| | |
|---|---|
| /var/log/wtmp | システムに対する成功したログイン試行が記録される<br>確認方法:last コマンド |
| /var/log/btmp | システムに対する失敗したログイン情報が記録される<br>確認方法:lastb コマンド |
| /var/log/lastlog | システムに登録されているユーザの最終ログイン時刻が記録される<br>確認方法:lastlog コマンド |
| /var/log/faillog | システムに登録されているユーザのログイン失敗回数が記録される<br>確認方法:faillog コマンド |
| /var/log/tallylog | システムに登録されているユーザのログイン失敗回数が記録される<br>pam_tally2モジュール利用時に記録<br>確認方法:pam_tally2 コマンド |

# 実行履歴・横展開の特定

## セキュリティソフトの検知履歴・状態確認

マルウェア実行時にセキュリティソフトが検知していないか、
攻撃者がマルウェア実行を妨げないために無効化していないかを確認する

## プログラムの実行履歴の確認

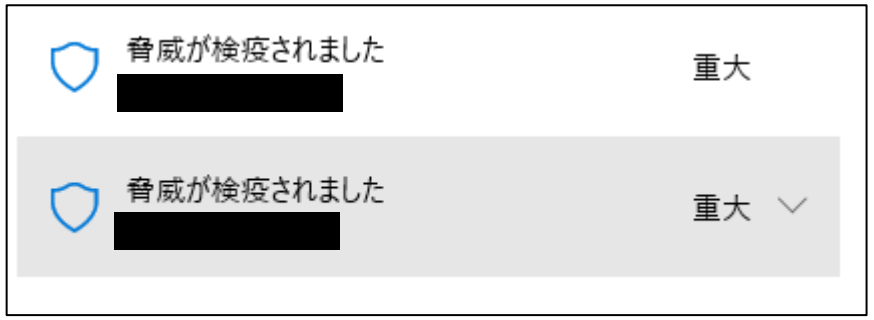
攻撃者はマルウェアだけでなく正規ツールも実行する（例：LOLBIN）
不審なプログラムが実行されていないか、実行履歴を確認する

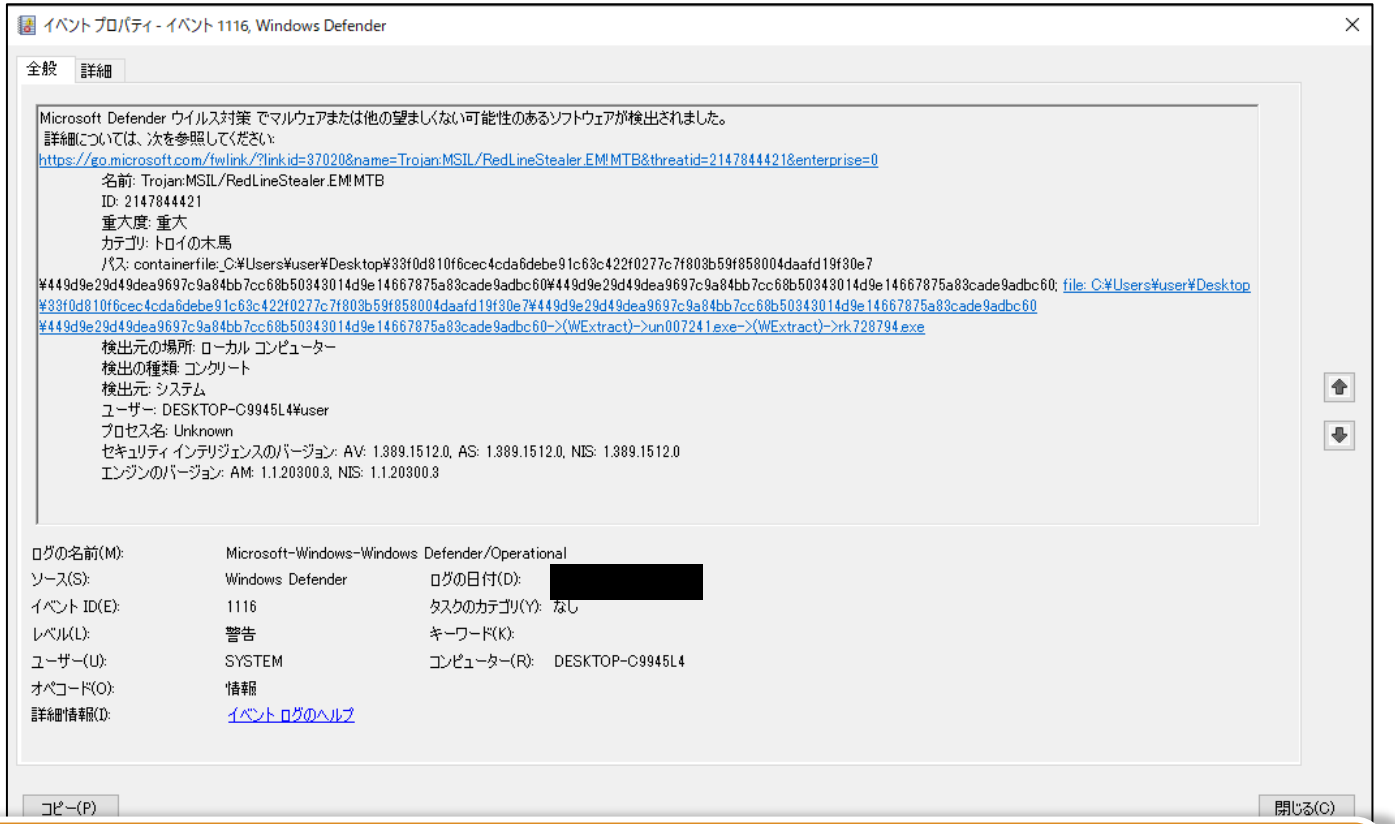
## 横展開の特定

攻撃者は目的を達成するために、別の端末へログイン試行をしている可能性がある
別の端末でも初期侵入の手口が使われていないか、侵害された端末から拡大する動きがないか確認する

# WindowsDefenderの検知履歴（Hayabusaでの検知可能）

◆ Windows Defenderがウイルスを検知した際にもイベントログに痕跡が残る。




**Defenderの検知は「Microsoft-Windows-windows Defender/Operational.evtx」の1116に記録される**

# WindowsDefenderの状態変化(Hayabusaでの検知可能)

- 攻撃者はマルウェア実行前にセキュリティ機能を無効化することがある
  ⇒これもイベントログに記録される。


5001:リアルタイム保護の無効化
5010:アンチスパイウェアの無効化
5012:ウイルススキャンの無効化
5101:マルウェア対策プラットフォームの期限切れ

Microsoft Defender ウイルス対策ソフトウェアの問題をトラブルシューティングするため、イベント ログとエラー コードをレビューする
https://learn.microsoft.com/ja-jp/microsoft-365/security/defender-endpoint/troubleshoot-microsoft-defender-antivirus?view=o365-worldwide

**Defenderの無効化は「Microsoft-Windows-windows Defender/Operational.evtx」の5001,5010,5012,5101に記録される**

# Shimcache/Amcache(Windows)

## Shimcache

どのようなプログラムが実行されたか確認

- ファイルのフルパス
- ファイルサイズ
- ファイルの最終更新日時
- プロセスの実行フラグ

## Amcache

実行されたプログラムの情報が記録

- ファイルのフルパス
- ファイルサイズ
- ファイルの初回実行日時
- ファイルのSHA-1

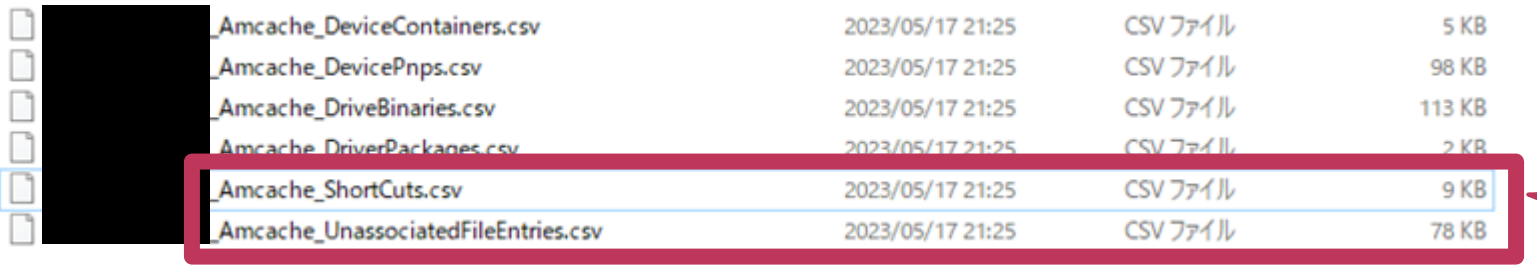
実行フラグの確認、ファイルのハッシュ値の違いで使い分け

# Shimcache Parser & Amcache Parser(EZtools)

- AppCompatCacheParser(Shimcache parser)
  - SYSTEMレジストリのエントリであるShimcacheをパースしてくれる

| Executed | Last Modified Time UTC | Path |
|---|---|---|
| No | 2022-09-09 07:30:23 | C:\Users\user\AppData\Local\Temp\31E29570-B8E7-4669-8A30-D311150A8004\dismhost.exe |
| No | 2022-09-09 07:30:23 | C:\Users\user\AppData\Local\Temp\6CF06492-F898-4B1C-AC29-7C607AE46DE3\dismhost.exe |
| No | 2023-04-26 23:44:30 | C:\Windows\SoftwareDistribution\Download\Install\AM_Delta_Patch_1.387.2106.0.exe |
| No | 2022-09-09 07:29:58 | C:\Windows\system32\DllHost.exe |
| No | 2023-04-25 05:06:27 | C:\Program Files\WindowsApps\Microsoft.YourPhone_1.23032.186.0_x64__8wekyb3d8bbwe\PhoneExperienceHost.exe |
| Yes | 2023-04-26 23:31:04 | C:\Users\user\Desktop\[redacted].exe |

- AmcacheParser
  - C:¥Windows¥AppCompat¥Programs¥Amcache.hveをパース



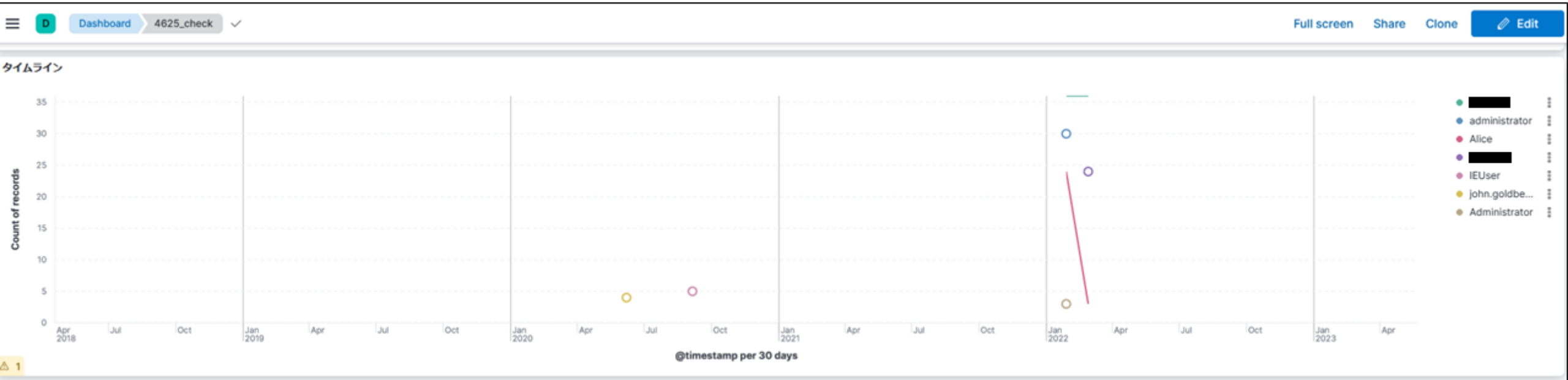

ShortCuts.csvや
UnassociatedFileEntries.csvを見ていく

| Key Name | Lnk Name |
|---|---|
| 7-zip file manag\|1cfcc57bd05e0f1c | C:\ProgramData\Microsoft\Windows\Start Menu\Programs\7-Zip\7-Zip File Manager.lnk |
| 7-zip help.lnk\|b530b9ae32462b97 | C:\ProgramData\Microsoft\Windows\Start Menu\Programs\7-Zip\7-Zip Help.lnk |
| administrative t\|b56430fa90eb27f3 | c:\users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\System Tools\Administrative Tools.lnk |

# 実行されているプログラムの確認(Linux)

| | |
|---|---|
| プロセスファイルシステムの確認 | /proc/PID/　配下に保存されてる情報を確認する<br>プロセスのカレントディレクトリ:/proc/PID/cwd<br>プロセスの実行ファイル:/proc/PID/exe<br>プロセス起動時のコマンドライン:/proc/PID/cmdline |
| プロセス状態の確認 | 実行されているプロセスの状態を確認<br>リソースの大量消費を確認:topコマンド<br>実行されているプロセスを確認:psコマンド |
| ネットワーク接続状態 | 実行されているプログラムとネットワーク接続がないか確認する<br>接続待ち/確立しているプロセスを確認:netstatコマンド |
| auditdのログ確認 | Linuxの監査システムAuditで、実行されるプログラムをログに出力するように設定している場合、出力されたログを確認する |

# さらなる効率化




統計情報

| TargetUserName | LogonType | IpAddress | Count of records | Minimum of @timestamp | Maximum of @timestamp |
|---|---|---|---|---|---|
| [redacted] | 11 | ::1 | 51 | 2022/02/07 13:52:10.573 | 2022/03/27 19:34:55.264 |
| [redacted] | 2 | ::1 | 21 | 2022/02/07 13:52:10.577 | 2022/03/27 19:34:55.280 |
| administrator | 2 | ::1 | 30 | 2022/02/13 22:35:04.356 | 2022/02/13 22:38:34.542 |
| Alice | 2 | 127.0.0.1 | 27 | 2022/01/29 21:22:25.941 | 2022/03/27 19:27:19.113 |
| [redacted] | 11 | ::1 | 12 | 2022/03/27 19:30:55.994 | 2022/03/27 19:31:16.551 |
| [redacted] | 2 | ::1 | 12 | 2022/03/27 19:30:55.997 | 2022/03/27 19:31:16.552 |
| IEUser | 2 | - | 5 | 2020/09/09 22:18:23.627 | 2020/09/09 22:18:23.627 |
| john.goldberg | 2 | 127.0.0.1 | 4 | 2020/06/21 03:59:20.253 | 2020/06/21 03:59:20.253 |
| Administrator | 11 | ::1 | 3 | 2022/02/01 21:42:57.876 | 2022/02/01 21:42:57.876 |

# インシデント対応時に遭遇したトラブル

# インシデント対応時のトラブル

◆ 効率的にログ解析をする中で、我々が遭遇したトラブルを最後に紹介

ログの不足
ログのローテート

システム時刻の
改ざん

Defenderの
検知ログ見落とし

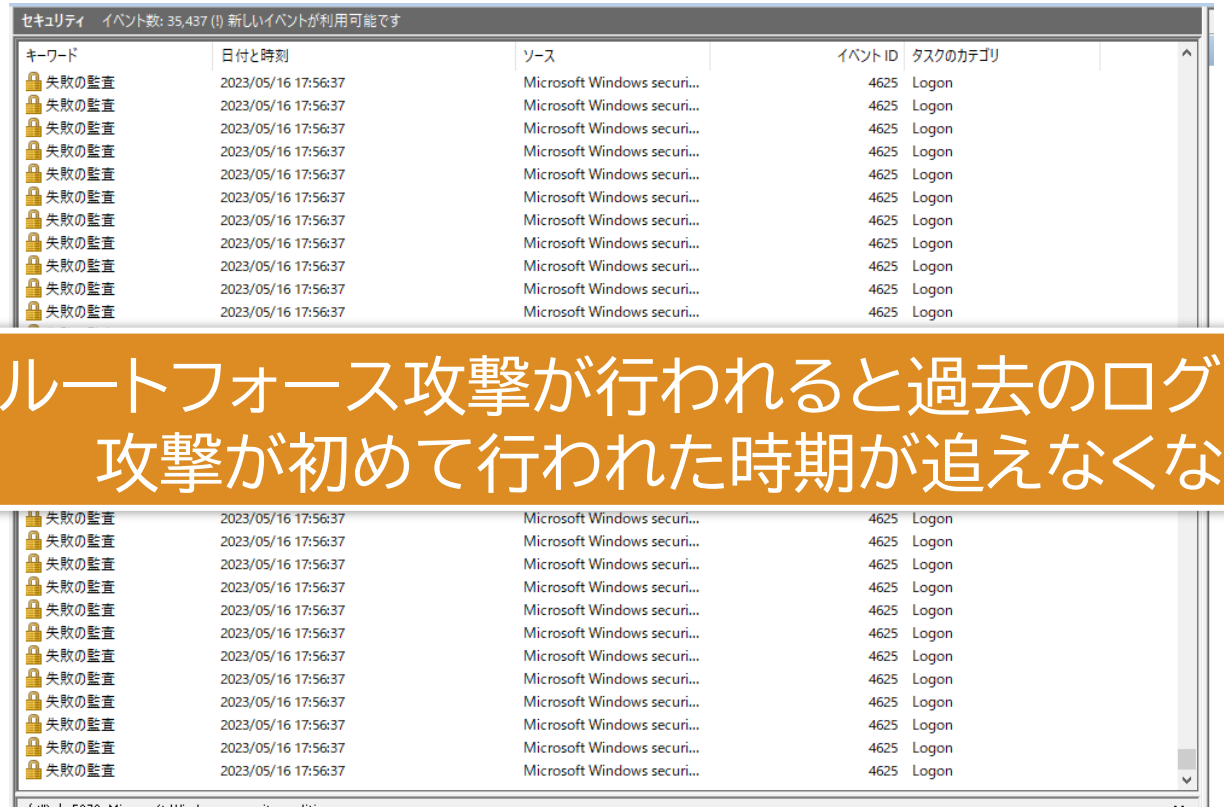
# ログの不足

- ログを取得する設定ではない、
  ログがローテートされてしまい、特定に役立つログを取得する設定がない
  などによる原因特定に至らない事案がある

- 機器のデフォルトの設定でログを取得するようにしていなかった
- ブルートフォース攻撃が行われてしまい、過去のログが消えてしまった。

# ログのローテート

◆ Windowsイベントログのデフォルトサイズ→約20MB(20,489KB)




ブルートフォース攻撃が行われると過去のログが消え、
攻撃が初めて行われた時期が追えなくなる

rockyou.txt(有名なパスワードリスト,1400万ワード)を使ったブルートフォースで20MB以上になる
(所要時間:単一スレッドのブルートフォース実行で6時間ほど)

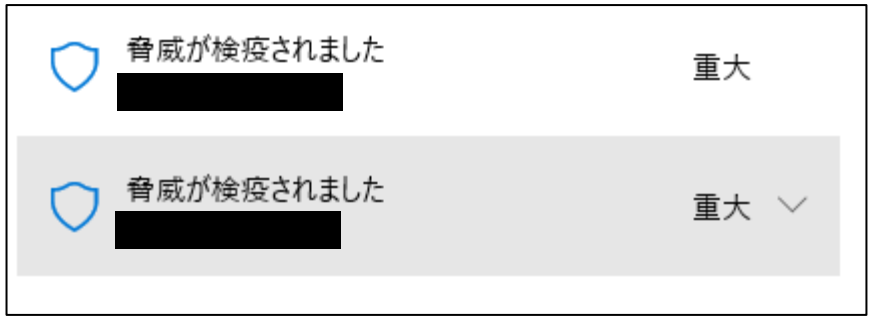
# 時刻の改ざん

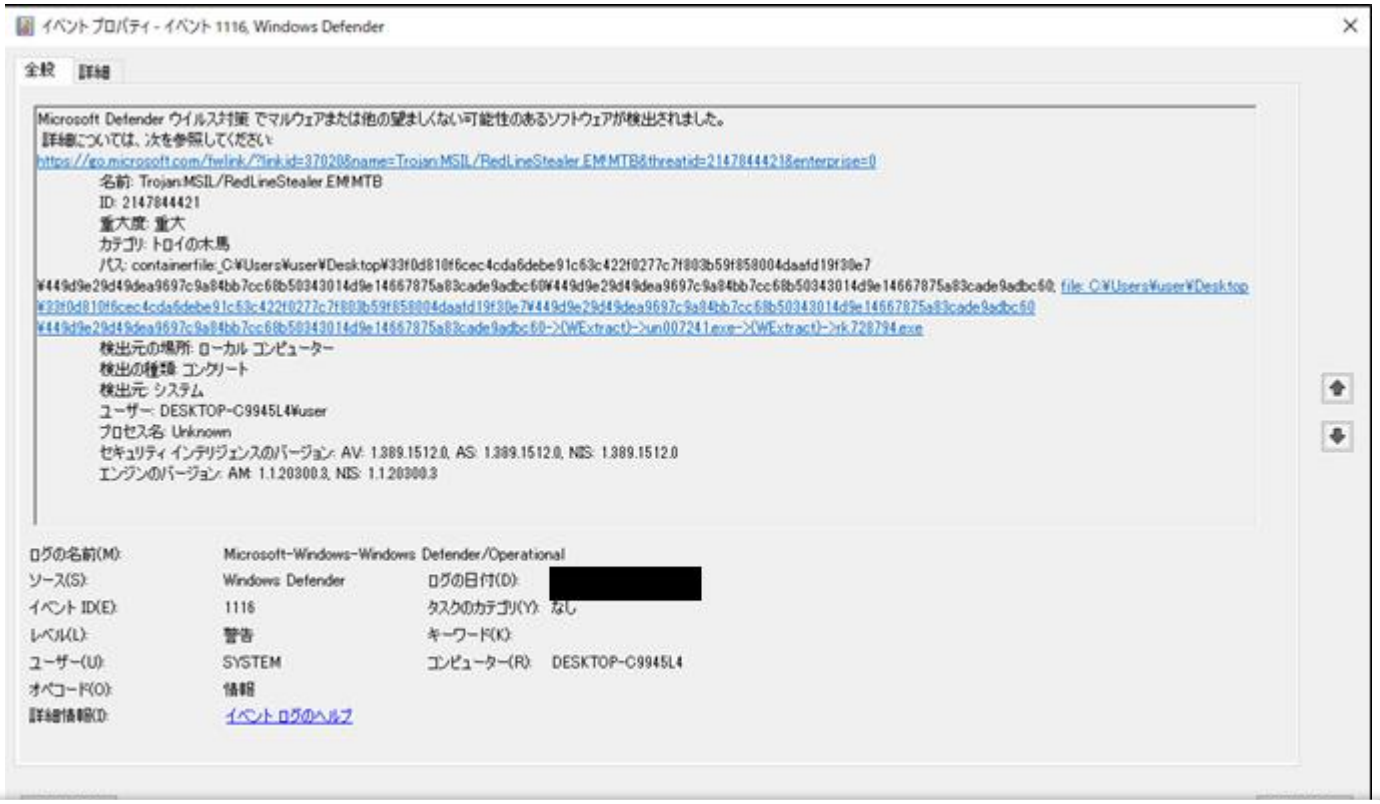
- 攻撃者が侵入後にWindowsのシステム設定日時を変更(数万回の時刻変更の試み)
  例:20yy/mm/dd ⇒ 20yy/01/01に変更
  - 時刻変更前と時刻変更後のタイムラインがずれるため、考慮したうえで調査を行う必要があった

- Windowsの日時変更の検出
  - イベントログ System.evtxのイベントID1、もしくはSecurity.evtxのイベントID4616を確認する

# Defenderの検知ログの見落とし(1/2)

- Windows Defenderのマルウェア検知のイベントログがHayabusaで検知されなかった(2023/3/27時点で解決済み)




**Defenderの検知は「Microsoft-Windows-windows Defender/Operational.evtx」の1116に記録される**

# Defenderの検知ログの見落とし(2/2)

◆インシデント対応時のHayabusa検知ルールは以下のようになっていた

```
id: 810bfd3a-9fb3-44e0-9016-8cdf785fddbf
level: critical
status: test
logsource:
    product: windows
    service: windefend
detection:
    selection:
        Channel: Microsoft-Win  ws-W
        EventID: 1116
        SeverityName: "critical"
falsepositives:
    - bad signature
```

日本語環境だと「重大」となるので抽出されなかった。

```
id: 810bfd3a-9fb3-44e0-9016-8cdf785fddbf
level: critical
status: test
logsource:
    product: windows
    service: windefend
detection:
    selection:
        Channel: Microsoft-Windows-Windows Defender/Operational
        EventID: 1116
        SeverityID: 5 # Severe
falsepositives:
    - bad signature
```

3/27のアップデートでSeverityIDでチェックするようになり、検知可能に

# おわりに

- 今回紹介できたテクニックやインシデント対応時のトラブルは一部現実やHardeningでは想像してないことも起きる

  インシデント対応の事前の準備はしっかりとしておくのも重要だが、セキュアな開発・要塞化も欠かせない

- 「真剣勝負で堅牢化を鍛え上げましょう」


Orchestrating a brighter world
NEC