

サイバーセキュリティシンポジウム道後2023

インシデント発生時のフォレンジックの効率化 に関する取り組み

2023年6月29日 ～ 2023年6月30日

NEC サイバーセキュリティ戦略統括部

\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。

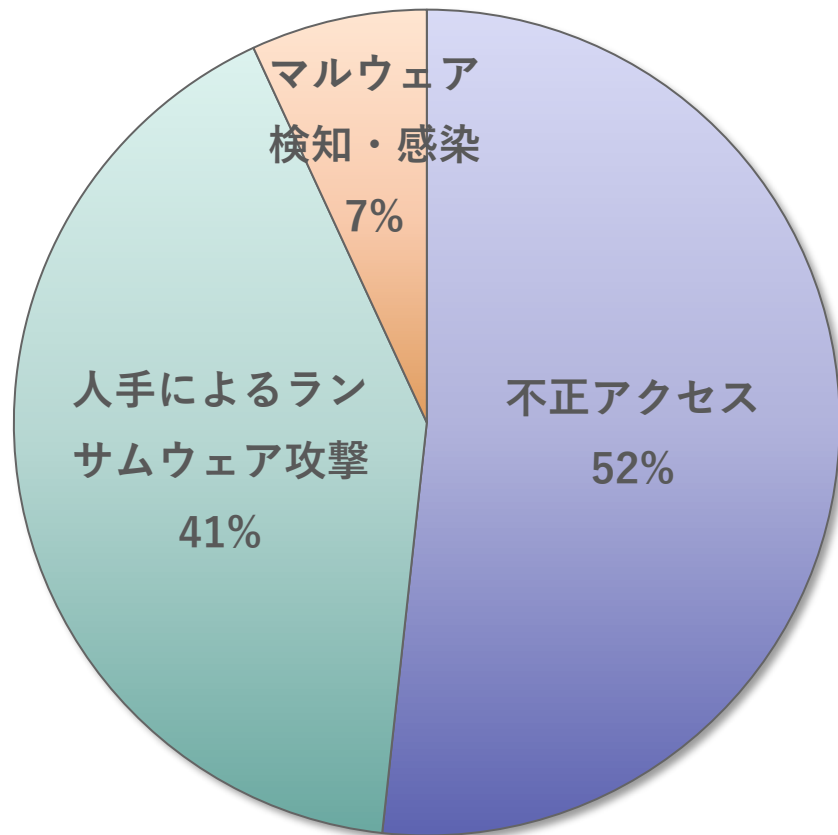
目次

1. インシデント対応の全体感
2. NECにおけるインシデント対応
3. インシデント対応時に遭遇したトラブル

インシデント対応の全体感

インシデントの種別

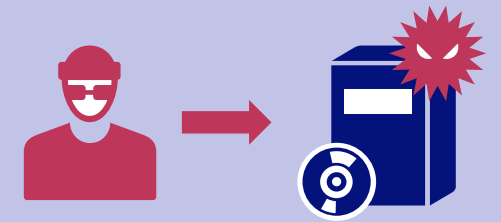
我々のチームで対応した攻撃者が明確に存在するインシデントについて
大まかな分類とその割合を紹介



※当部門にて対応した過去事案の分類結果

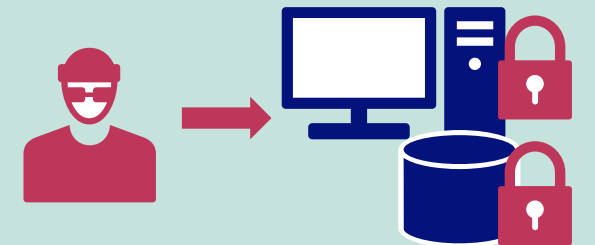
不正アクセス

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] — 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へ侵入された。

脆弱性の悪用 [Exploit Public-Facing Application T1190] — 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へ侵入された。

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]

- ◆ 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

- ◆ 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

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

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

- NTFS管理ファイル
- プリフェッチ
- イベントログ
- レジストリ
- 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

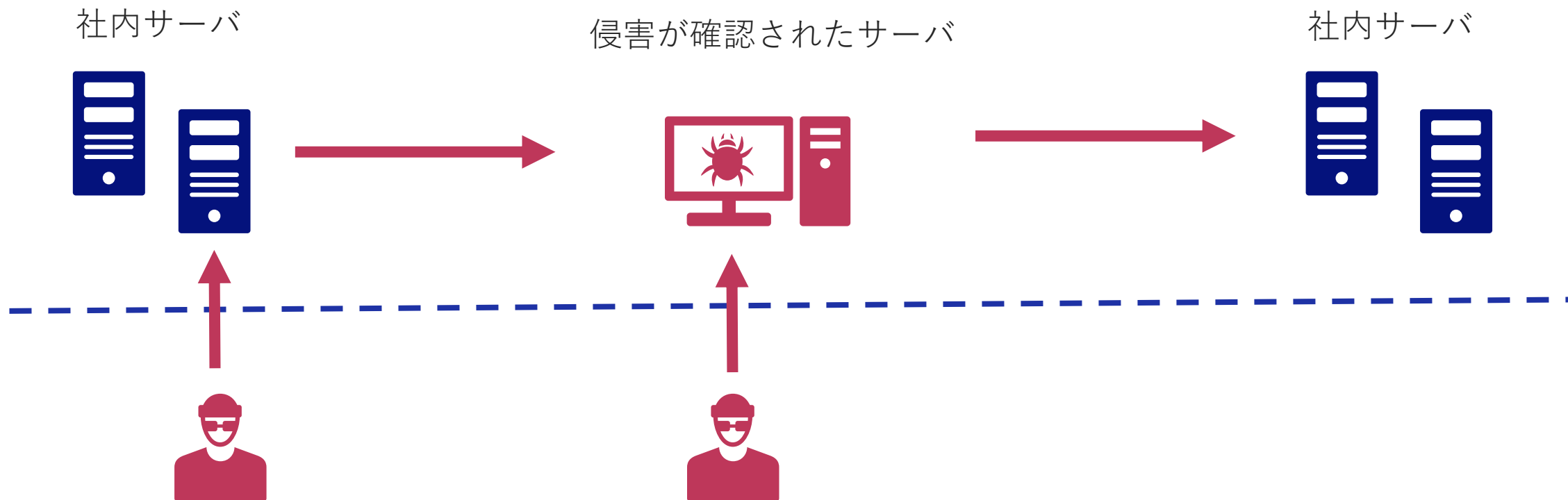
[1] デジタル・フォレンジック研究会 | 証拠保全ガイドライン第8版 <https://digitalforensic.jp/wp-content/uploads/2021/05/gl8-20210520.pdf>

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

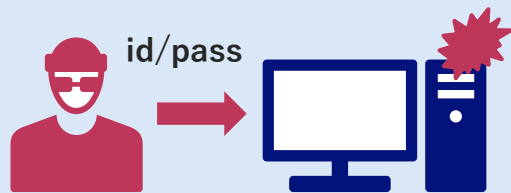
侵入されたサーバ・端末の特定

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）

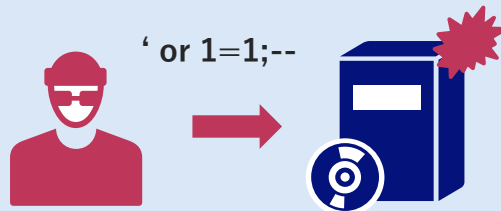
初期侵入で見る点



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

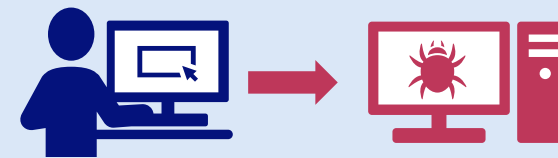
ログイン試行は統一的な調査が可能



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

ログの収集

CDIR-C と Autoruns で初動対応用のログを収集

各ツール実行用のバッチファイルを用意しており、簡単に保全が可能

○ 製品紹介

CDIR-C - データ収集用ツール



CDIR-C (Cyber Defense Institute Incident Response Collector) は、調査対象端末の汚染や業務への影響を最小限に抑えながら安全にデータを収集することができるデータ収集用ツールです。

CDIR-Cで収集したデータは一般的なフォレンジックツールで読み込んで解析することが可能なため、自組織では証拠保全までを実施し、フォレンジック調査を外部のサービスベンダーに依頼することを想定している組織にも有効にご活用頂けます。

- <https://github.com/CyberDefenseInstitute/CDIR>
- <https://www.cyberdefense.jp/products/cdir.html>

[Learn](#) / [Sysinternals](#) / [Downloads](#) /

Autoruns for Windows v14.09

Article • 06/08/2023 • 8 contributors

In this article

- [Introduction](#)
- [Usage](#)
- [Autorunsc Usage](#)
- [Related Links](#)
- [Download](#)

- <https://learn.microsoft.com/ja-jp/sysinternals/downloads/autoruns>

調査観点の事前整理

調査観点を事前に調査し、Excelシートに整理
属人性を排除し、インシデントの調査を分担して行えるように

◆ Windowsの調査観点（6カテゴリ、全72項目）

- 侵害の痕跡
- 不審なプログラムの実行痕跡
- 不審な永続化設定
- 不審な操作の痕跡（内部探索、痕跡削除など）
- 他ホストへの侵害拡大の痕跡
- 情報流出の痕跡

侵害の痕跡の調査観点（抜粋）

ログオン成功とログオン失敗を調査することで、侵害の範囲の絞込みが可能

◆ Security イベント ログの イベントID：4624 の調査

① ログオン成功の痕跡

- Type 2は対話型（PsExecも対象）
- Type 3 はネットワーク
- Type10 は RemoteInteractive（RDPも対象）

② ローカルでの Pass-the-Hash の痕跡

- Type 9 かつ LogonProcessがseclogoの場合、ローカルのPass-the-Hashの痕跡

◆ Security イベント ログの イベントID：4625 の調査

③ ログオン失敗の痕跡

例: ログオン失敗が大量に続いた後、ログオン成功が確認された
(ブルートフォースや辞書攻撃により、ログオンされたと推測可能)

【例】 ログオン痕跡の調査: 手動での解析 (1/4)

◆ イベントログの確認方法

The image shows a Windows Start menu on the left and the Windows Event Viewer application on the right. The Start menu has a red box around the Windows logo at the bottom and another red box around the 'イベントビューアー(V)' (Event Viewer) option. A blue callout bubble with the text '① Windowsのボタンを右クリック' (Right-click the Windows button) points to the first red box. Another blue callout bubble with the text '② イベントビューアーを選択' (Select Event Viewer) points to the second red box. The Event Viewer window shows the 'セキュリティ' (Security) log selected in the left pane. A table of events is displayed in the main pane, with event 4672 (Special Logon) highlighted. A third blue callout bubble with the text '③ イベントビューアーからイベントログが確認できる' (Event log can be confirmed from Event Viewer) points to the Event Viewer window.

① Windowsのボタンを右クリック

② イベントビューアーを選択

③ イベントビューアーからイベントログが確認できる

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
成功の監査	2023/04/27 17:14:38	Microsoft Windows securi...	4672	Special Logon
成功の監査	2023/04/27 17:14:38	Microsoft Windows securi...	4624	Logon
成功の監査	2023/04/27 17:14:25	Microsoft Windows securi...	4672	Special Logon
成功の監査	2023/04/27 17:14:18	Microsoft Windows securi...	4624	Logon
成功の監査	2023/04/27 17:14:18	Microsoft Windows securi...	4799	Security Group Manag...
成功の監査	2023/04/27 17:14:18	Microsoft Windows securi...	4799	Security Group Manag...
成功の監査	2023/04/27 17:14:09	Microsoft Windows securi...	4798	User Account Manage...
成功の監査	2023/04/27 17:14:07	Microsoft Windows securi...	4798	User Account Manage...
成功の監査	2023/04/27 17:14:07	Microsoft Windows securi...	4672	Special Logon
成功の監査	2023/04/27 17:14:07	Microsoft Windows securi...	4624	Logon
成功の監査	2023/04/27 17:14:06	Microsoft Windows securi...	4672	Special Logon
成功の監査	2023/04/27 17:14:06	Microsoft Windows securi...	4624	Logon
成功の監査	2023/04/27 17:14:04	Microsoft Windows securi...	4798	User Account Manage...
成功の監査	2023/04/27 17:14:03	Microsoft Windows securi...	4616	Security State Change
成功の監査	2023/04/27 17:14:03	Microsoft Windows securi...	4616	Security State Change
成功の監査	2023/05/16 10:41:10	Microsoft Windows securi...	5379	User Account Manage...
成功の監査	2023/05/16 10:41:10	Microsoft Windows securi...	4672	Special Logon
成功の監査	2023/05/16 10:41:10	Microsoft Windows securi...	4624	Logon
成功の監査	2023/05/16 10:41:09	Microsoft Windows securi...	4616	Security State Change
成功の監査	2023/04/27 17:14:02	Microsoft Windows securi...	4672	Special Logon
成功の監査	2023/04/27 17:14:02	Microsoft Windows securi...	4624	Logon
成功の監査	2023/04/27 17:12:01	Microsoft Windows securi...	4672	Special Logon

イベント 4672, Microsoft Windows security auditing.

全般 詳細

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:

ログの名前(M): セキュリティ
ソース(S): Microsoft Windows security
イベント ID(E): 4672
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](#)

ログの日付(D): 2023/04/27 17:14:38
タスクのカテゴリ(Y): Special Logon
キーワード(K): 成功の監査
コンピューター(R): DESKTOP-C9945L4

【例】 ログオン痕跡の調査: 手動での解析 (2/4)

◆ Security イベント ログの イベントID : 4624 と 4625 の確認

- 特定のIPアドレス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できる



ログオン失敗 が確認できる

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（今回のログオンタイプ）
- 10: RDP

ログオン失敗の理由が確認できる

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アドレスが表示されている)

ログイン失敗 を示すイベントID：4625のログ（サンプル）

【例】 ログオン痕跡の調査: 手動での解析 (3/4)

◆ Security イベント ログの イベントID : 4624 と 4625 の確認

- 特定のIPアドレス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できる

イベント プロパティ - イベント 4624, Microsoft Windows security auditing.	
全般	詳細
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
ログオン情報:	
ログオン タイプ:	3
制限付き管理モード:	-
仮想アカウント:	いいえ
昇格されたトークン:	いいえ
偽装レベル:	偽装
新しいログオン:	
セキュリティ ID:	DESKTOP-C9945L4\user
アカウント名:	user
アカウント ドメイン:	DESKTOP-C9945L4
ログオン ID:	0xA02EF2
リンクされたログオン ID:	0x0
ネットワーク アカウント名:	-
ネットワーク アカウント ドメイン:	-
ログオン GUID:	{00000000-0000-0000-0000-000000000000}
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:	kali
ソース ネットワーク アドレス:	192.168.10.41
ソース ポート:	0
詳細な認証情報:	
ログオン プロセス:	NtLmSsp
認証パッケージ:	NTLM
移行されたサービス:	-
パッケージ名 (NTLM のみ):	NTLM V2
キーの長さ:	128

ログオンの成功 が確認できる

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（今回のログオンタイプ）
- 10: RDP

ログオンに成功したアカウントの情報が確認できる

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アドレスが表示されている）

ログイン成功 を示す イベントID : 4624 のログ（サンプル）

【例】 ログオン痕跡の調査: 手動での解析 (4/4)

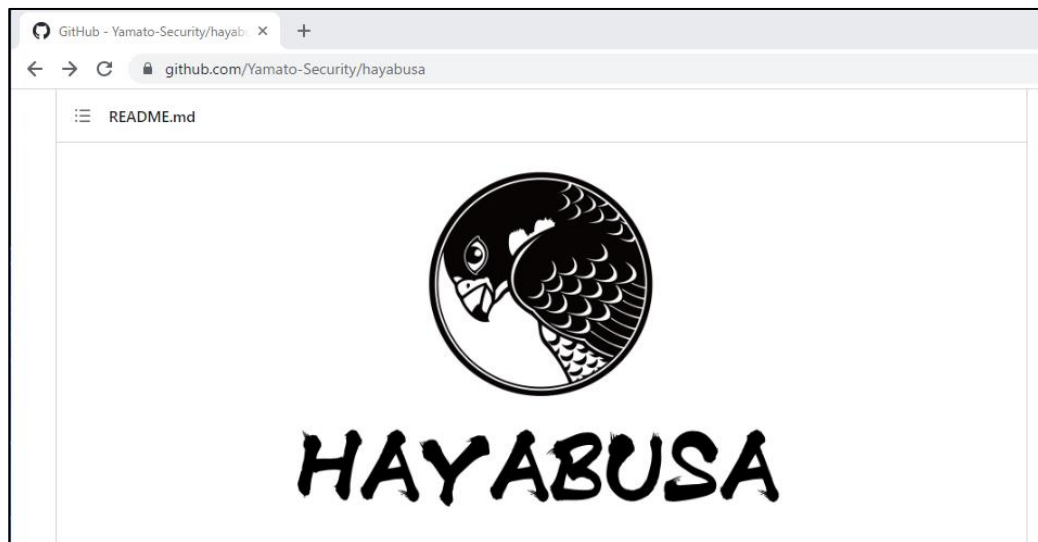
実際に解析する場合、大量のログが記録されているため、手動で一つずつ解析するのは非常に困難

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

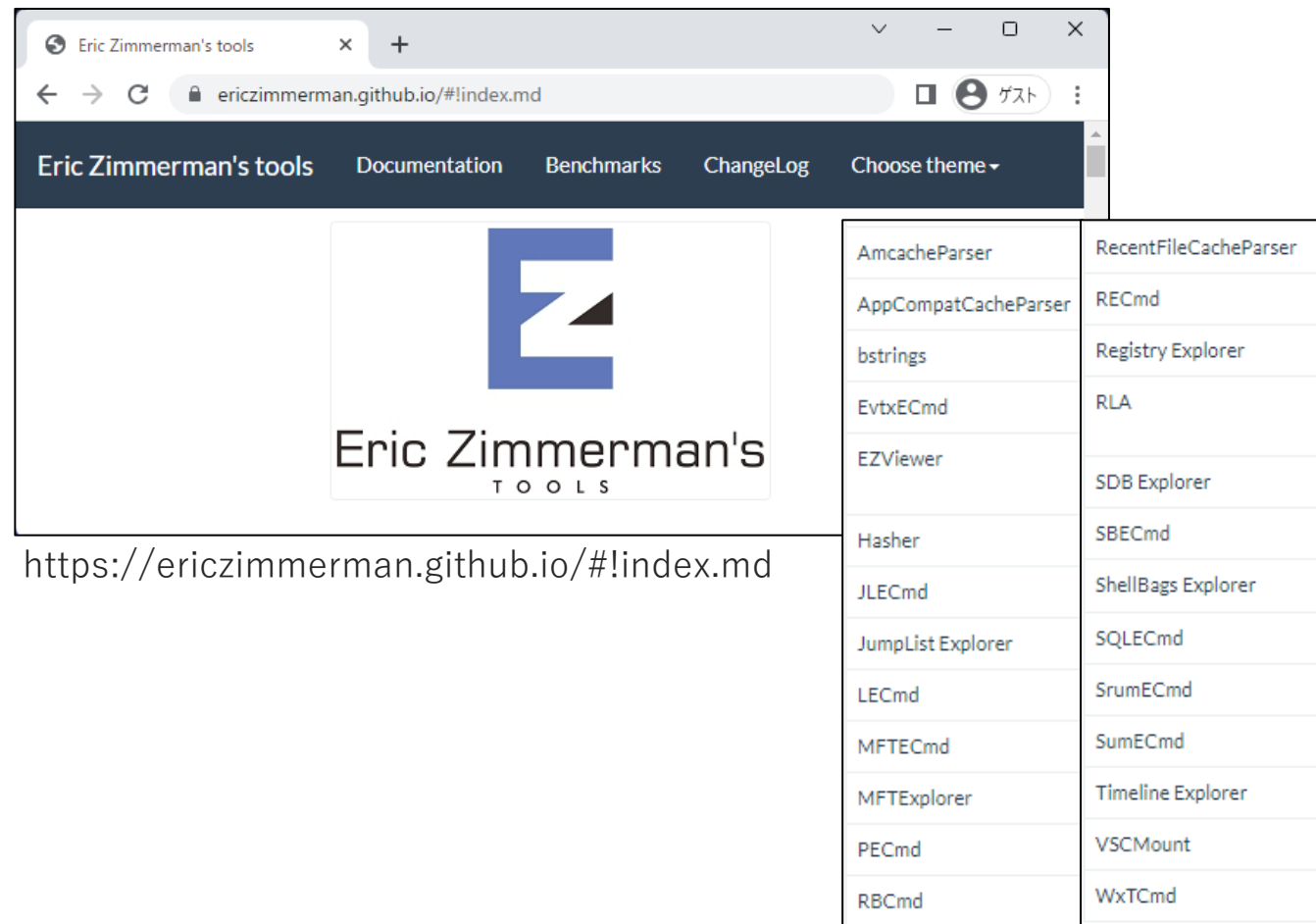
ログ解析用ツールの活用

ログを手動で見っていくのは、非常に大変

Hayabusa や EZ Tools などのツールを活用して効率よくログを解析



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



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

【例】 ログオン痕跡の調査: Hayabusaでの解析 (1/2)

```
Windows PowerShell

Results Summary:
First Timestamp: 2023-02-17 23:35:47.444 +09:00
Last Timestamp: 2023-05-16 19:57:01.892 +09:00

Events with hits / Total events: 19,556 / 30,780 (Data reduction: 11,224 events (36.47%))

Total | Unique detections: 19,604 | 12
Total | Unique critical detections: 0 (0.00%) | 0 (0.00%)
Total | Unique high detections: 0 (0.00%) | 0 (0.00%)
Total | Unique medium detections: 48 (0.24%) | 1 (8.33%)
Total | Unique low detections: 19,478 (99.36%) | 3 (25.00%)
Total | Unique informational detections: 78 (0.40%) | 8 (66.67%)

Dates with most total detections:
critical: n/a, high: n/a, medium: 2023-05-16 (48), low: 2023-05-16 (19,393), informational: 2023-04-2

Top 5 computers with most unique detections:
critical: n/a
high: n/a
medium: n/a
low: DESKTOP-C9945L4 (3)
informational: DESKTOP-C9945L4 (8)

Top critical alerts:
n/a
n/a
n/a
n/a
n/a

Top high alerts:
n/a
n/a
n/a
n/a
n/a

Top medium alerts:
PW Guessing (48)
n/a
n/a
n/a
n/a

Top low alerts:
Logon Failure (Wrong Password) (19,369)
Credential Manager Enumerated (83)
Credential Manager Accessed (26)
n/a
n/a

Top informational alerts:
Proc Exec (33)
Logon (Interactive) *Creds in memory* (14)
Admin Logon (9)
Logoff (9)
Explicit Logon (7)
Logon (System) - Bootup (3)
Logoff (User Initiated) (2)
Logon (Network) (1)
n/a
n/a

Saved file: C:\Users\User\Documents\hayabusa-output.csv (5.7 MB)
Elapsed time: 00:00:25.972

PS C:\Users\User\Desktop\hayabusa-2.5.1-win-64-bit>
```

Top medium alerts:

PW Guessing (48)
n/a
n/a
n/a
n/a

Top low alerts:

Logon Failure (Wrong Password) (19,369)
Credential Manager Enumerated (83)
Credential Manager Accessed (26)
n/a
n/a

mediumとlow で Logon Failure を検出していることが分かる

- PW Guessing
- Logon Failure (Wrong Password)

【例】 ログオン痕跡の調査: Hayabusaでの解析 (2/2)

◆ Hayabusaが出力するCSVファイルの確認

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

以下の2件を検出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

```
1 author: Zach Mathis
2 date: 2020/11/08
3 modified: 2022/12/16
4
5 title: Logon Failure (Wrong Password)
6 description: Prints logon information.
7
8 id: e87bd730-df45-4ae9-85de-6c75369c5d29
9 level: low
10 status: stable
11 logsource:
12   product: windows
13   service: security
14 detection:
15   selection_basic:
16     Channel: Security
17     EventID: 4625
18   selection_wrong_password:
19     SubStatus: "0xc000006a" #Wrong password
20   condition: selection_basic and selection_wrong_password
21 falsepositives:
22   - user mistypes password
23 tags:
24 references:
25 ruletype: Hayabusa
```

【例】 ログオン痕跡の調査: EZ Tools での解析

◆ EZ Tools の1つである EvtxECmd を活用する

- EvtxECmd は Windows イベントログを CSV や JSON 形式で書き出すことができる。
- フィルタ機能を用いることで、特定のイベントIDのみを抜き出すこともできる。

```
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>
```

Event 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
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 EZ Tools (EvtxECmd)

Hayabusa

EZ Tools (EvtxECmd)

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 ファイルなど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 ログかを把握するには、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

時間が少ない中で大まかな状態を把握したい
(インシデント対応の初期など)

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

EvtxECmd (EZ Tools)

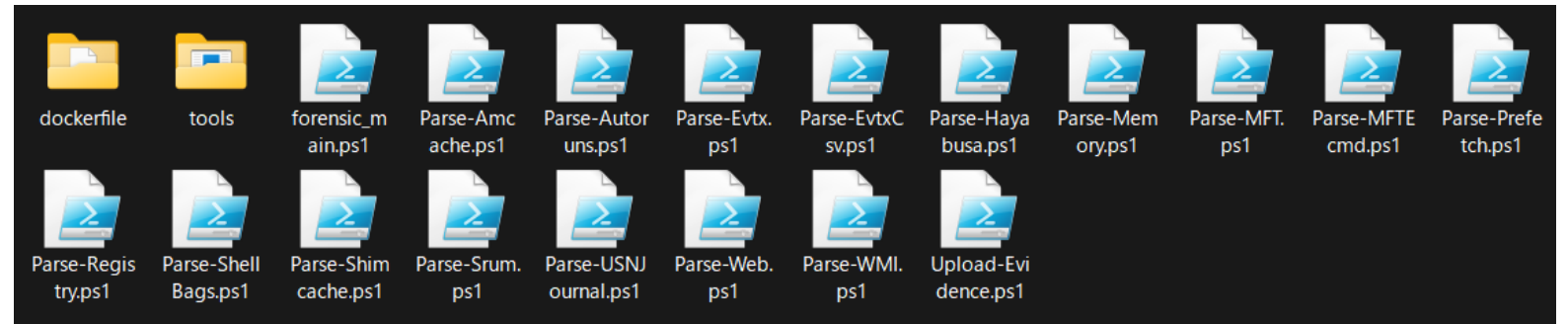
収集したログのパースの自動化

ログの解析に集中できるようにパース作業はすべて自動化

- ◆ CDIR-C、Autorunsで保全したログを指定すると、自動でパースしてCSVの形式で出力するスクリプトを用意し、効率化させている

```
start:
---Fast Forensics Target
MFT:True
USNJJournal:True
Amcache:True
SRUM:True
WMI:True
Autoruns:False
EVTX:True
Prefetch:True
Registry:True
Shellbags:True
Shimcache:True
WebHistory:True
Memory:False

Confirmation
Do you want to continue?
[Y] Yes(Y) [N] No(N) [?] ヘルプ (既定値は "Y"): Y
---parse wmi start:
---parse srum start:
---parse amcache start:
---parse shimcache start:
---parse srum start:
---parse shellbags start:
---parse web start:
---parse evtx(Hayabusa) start:
---parse evtx start:
---parse reg start:
---parse usnjrnl start:
---parse mft start:
---parse mftcmd start:
All Job End
```



さらなる効率化へ（開発中）

Elastic Stack を使ってログの可視化、ログの分析を容易にする試み



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

ログの不足
ログのローテーション

システム時刻の
改ざん

Windows
Defenderの
検知ログ見落とし

トラブル 1: ログの不足

次のことが原因で、インシデント原因の特定に至らない事案があった。

- ◆ そもそもログを取得する設定がない。
 - 機器がデフォルトの設定になっており、ログを取得する設定がなかった。
- ◆ ログがローテートされてしまい、特定に役立つログが確認できない。
 - 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。

トラブル1: ローテーションによる過去のログの消失

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

セキュリティ イベント数: 35,437 (1) 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 17:56:37	Microsoft Windows securi...	4625	Logon
失敗の監査	2023/05/16 17:56:37	Microsoft Windows securi...	4625	Logon
失敗の監査	2023/05/16 17:56:37	Microsoft Windows securi...	4625	Logon
失敗の監査	2023/05/16 17:56:37	Microsoft Windows securi...	4625	Logon
失敗の監査	2023/05/16 17:56:37	Microsoft Windows securi...	4625	Logon
失敗の監査	2023/05/16 17:56:37	Microsoft Windows securi...	4625	Logon
失敗の監査	2023/05/16 17:56:37	Microsoft Windows securi...	4625	Logon
失敗の監査	2023/05/16 17:56:37	Microsoft Windows securi...	4625	Logon
失敗の監査	2023/05/16 17:56:37	Microsoft Windows securi...	4625	Logon
失敗の監査	2023/05/16 17:56:37	Microsoft Windows securi...	4625	Logon
失敗の監査	2023/05/16 17:56:37	Microsoft Windows securi...	4625	Logon

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

失敗の監査	2023/05/16 17:56:37	Microsoft Windows securi...	4625	Logon
失敗の監査	2023/05/16 17:56:37	Microsoft Windows securi...	4625	Logon
失敗の監査	2023/05/16 17:56:37	Microsoft Windows securi...	4625	Logon
失敗の監査	2023/05/16 17:56:37	Microsoft Windows securi...	4625	Logon
失敗の監査	2023/05/16 17:56:37	Microsoft Windows securi...	4625	Logon
失敗の監査	2023/05/16 17:56:37	Microsoft Windows securi...	4625	Logon
失敗の監査	2023/05/16 17:56:37	Microsoft Windows securi...	4625	Logon
失敗の監査	2023/05/16 17:56:37	Microsoft Windows securi...	4625	Logon
失敗の監査	2023/05/16 17:56:37	Microsoft Windows securi...	4625	Logon
失敗の監査	2023/05/16 17:56:37	Microsoft Windows securi...	4625	Logon
失敗の監査	2023/05/16 17:56:37	Microsoft Windows securi...	4625	Logon

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: 単ースレッドのブルートフォース実行で6時間ほど)

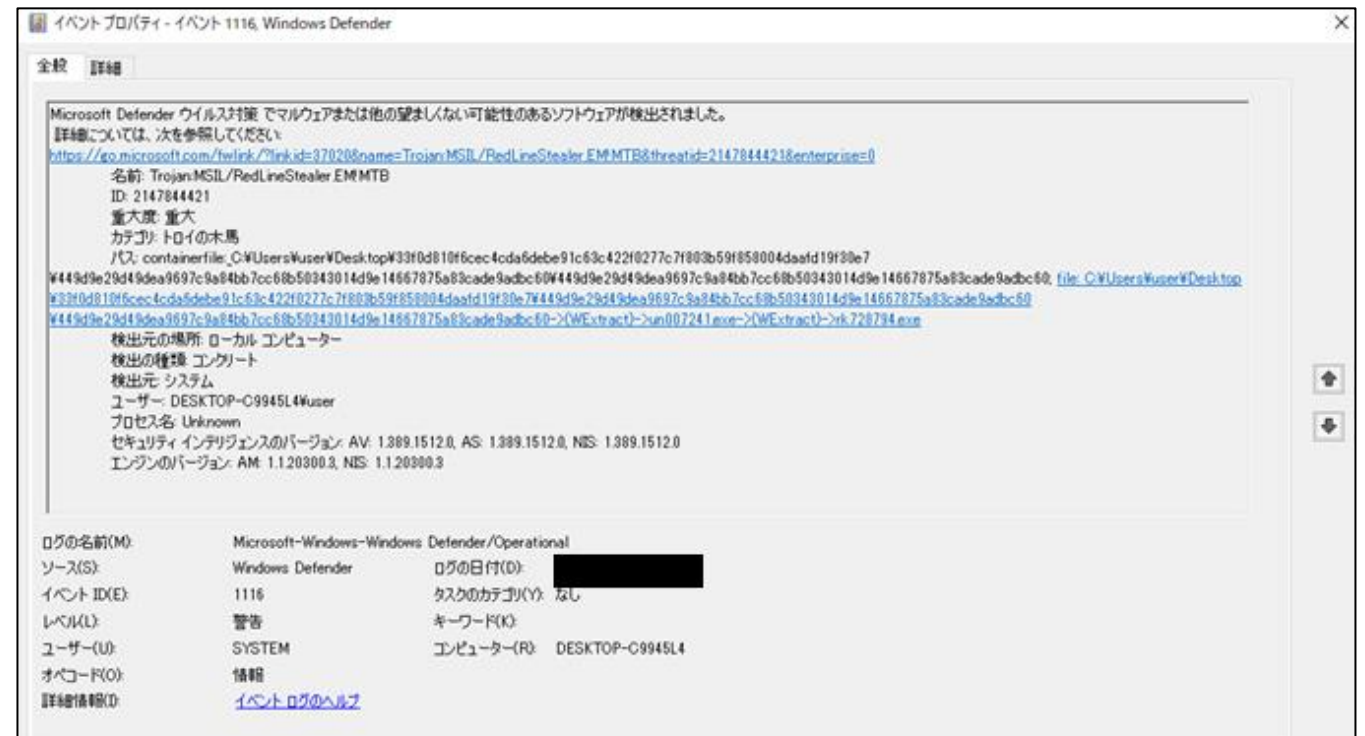
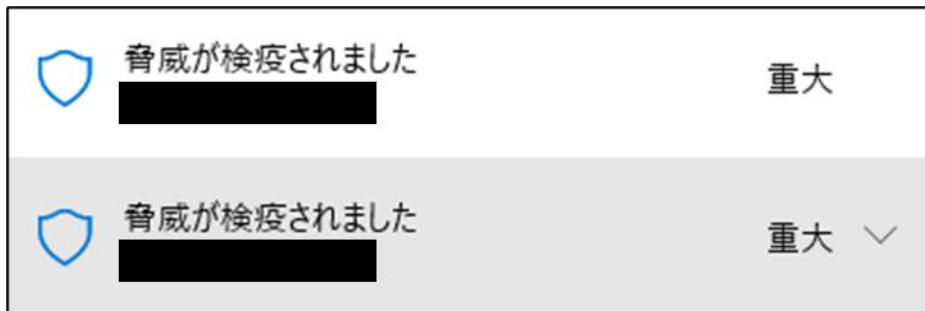
トラブル 2：時刻の改ざん

- ◆ 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、これを考慮した調査が必要であった。

- ◆ Windowsの日時変更の検出には、以下のイベントログを確認する必要がある
 - System.evtx のイベントID 1
 - Security.evtx のイベントID 4616

トラブル 3: Windows 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)



Windows Defenderの検知は「Microsoft-Windows-windows Defender/Operational.evtx」のイベントID 1116に記録される

トラブル 3: Windows 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になっていた

```
8 id: 810bfd3a-9fb3-44e0-9016-8cdf785fddbfc
9 level: critical
10 status: test
11 logsource:
12   product: windows
13   service: windefend
14 detection:
15   selection:
16     Channel: Microsoft-Windows-Windows Defender/Operational
17     EventID: 1116
18     SeverityName: "critical"
19 falsepositives:
20   - bad signature
```

アップデート前

日本語環境だと「重大」となる
ので抽出されなかった。

```
8 id: 810bfd3a-9fb3-44e0-9016-8cdf785fddbfc
9 level: critical
10 status: test
11 logsource:
12   product: windows
13   service: windefend
14 detection:
15   selection:
16     Channel: Microsoft-Windows-Windows Defender/Operational
17     EventID: 1116
18     SeverityID: 5 # Severe
19 falsepositives:
20   - bad signature
```

アップデート後

2023/3/27のアップデートで
SeverityIDで検知できるようになり、
検知可能に

\Orchestrating a brighter world

NEC