

Hardening Designers Conference 2024 Day2

Kibanaダッシュボードを活用した Windowsフォレンジックの効率化

2024年7月5日(金)

NEC サイバーセキュリティ戦略統括部

リスクハンティング・システムグループ

\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。

NECが実施するインシデント対応

ファストフォレンジックを実施して、お客さまのインシデント対応を支援

ファストフォレンジックとは… 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

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9版」

<https://digitalforensic.jp/wp-content/uploads/2023/02/shokohoznGL9.pdf>

なぜファストフォレンジックを採用？

- 早急な実態解明/ビジネスの早期復旧を目的とする事案への対応が求められるため、必要最低限のデータを解析するファストフォレンジックを実施



調査対象は？

- **Windows OS**に対するフォレンジックが**最多**
その他は、Linux OS、NW機器、ミドルウェア、クラウド等



Windowsフォレンジックの難しいポイント

ポイント



テキスト形式でないアーティファクトが多く、解析のためにはツールを使った成形が必要

ポイント



アーティファクトに関する知識が必要

例



MFT

MFTをcatコマンドで覗いてみても何も分からない

```
Windows PowerShell
PS C:\Users\...> cat '.\C:$MFT'
FILE07nPB... \H-s... リ-s... リ-s... リ-s... リ0hJ-s... リ-s... リ-s... リ-s... リ-s... リ@s$MFTH0?|@tト2@|
-H@@!JM+++++-----P@I++
I&... +++ FILE008X... \H-s... リ-s... リ-s... リ-s... リ0pR-s... リ-s... リ-s... $MFTMirrH@
s... リ-s... リ-s... リ-s... リ0pR-s... リ-s... リ-s... $LogFileH@?@2@-
++++ H@?@2@-
++++ FILE0互
```

例



レジストリ

- 調査に必要なレジストリキーに関する知識が必要
- 以下のようなレジストリハイブが存在し、これらの中には多数のレジストリキーが存在する

SYSTEM SOFTWARE SAM NTUSER.DAT

※しかし、多数あるレジストリキーの中で、調査に活用できるレジストリキーは限られている

スピードを求められるフォレンジックにおいて

複数のアーティファクトを一つ一つ成形している時間はない

スピードを求められるフォレンジックにおいて

調査に活用できるポイントを都度調べる時間はない

調査メンバーが画一的かつ効率的に調査を実施できる基盤を構築したい

Windowsフォレンジック標準化に向けた取り組み(1/2)

スクリプトで以下のような成形を一括で実行

各アーティファクトにツールを実行してCSVファイルに成形

- Eric Zimmerman's Tools(<https://ericzimmerman.github.io>)を使用してCSVファイルに成形(例:MFTはMFTECmdを使用)

ある程度の理解が必要なアーティファクトは、調査しやすいように出力される情報を選択

- 例:レジストリはRECcmd(<https://github.com/EricZimmerman/RECcmd>)というツールで成形
この際、調査に必要なレジストリキーを記載したバッチファイルを指定することで、調査に活用できるレジストリキーのみ、CSVファイルに出力することができる

```
Description: UserAssist(Executables)
HiveType: NtUser
Category: Program Execution
KeyPath: Software\Microsoft\Windows\CurrentVersion\Explorer\UserAssist\{CEBFF5CD-ACE2-4F4F-9178-9926F41749EA}\Count
Recursive: false
Comment: "GUI-based programs launched by the executables file"
```

↑ 実行されたプログラムの調査に活用できるレジストリキー「UserAssist」を抽出するバッチファイル

▶ 調査開始



Windowsフォレンジック標準化に向けた取り組み(2/2)

◆ CSVファイルを解析する調査項目を整備

■ フィルタリング条件まで指定することで作業レベルで標準化可能

4-(2)	MFT/USNJournal	ファイル参照の痕跡を調査。	mftecmd.csv	<p>【調査対象】 Extension=.lnk</p> <p>【確認項目】 ParentPath=パス FileName=ファイル名 Created0x10=ファイル生成時刻 (UTC) LastAccess0x10=最終ファイルアクセス時刻 (UTC)</p> <p>【説明】 MFTに記録されているファイル参照履歴(lnkファイルの生成)を調査する。</p>
4-(3)	MFT/USNJournal	ファイル参照の痕跡を調査。		<p>【調査対象】 FileName=*.lnk</p> <p>【確認項目】 Path: lnkファイルのパス FileName: lnkファイル名 Reason: USNレコード生成理由 TimeStamp(+00:00): 時刻 (UTC)</p> <p>【説明】 USNJournalに記録されているファイル参照履歴(lnkファイルの生成)を調査する。</p>

【調査対象】 → フィルタリング条件
 Extension=.lnk

【確認項目】 → 確認するフィールド
 ParentPath=パス
 FileName=ファイル名
 Created0x10=ファイル生成時刻 (UTC)
 LastAccess0x10=最終ファイルアクセス時刻 (UTC)

さらなる効率化に向けて

◆ 標準化後の課題

フィルタリングを毎回実施する必要がある

- 以下の拡張子をOR条件で検索するという複雑なクエリも存在



exe



dll



src



com



job



vbs



ps1



psm1



scr



bat

複数のアーティファクトを1つのファイルで解析できない

- 複数のファイルを開いて行き来しながら解析する必要がある



MFTの
成形結果



レジストリの
成形結果

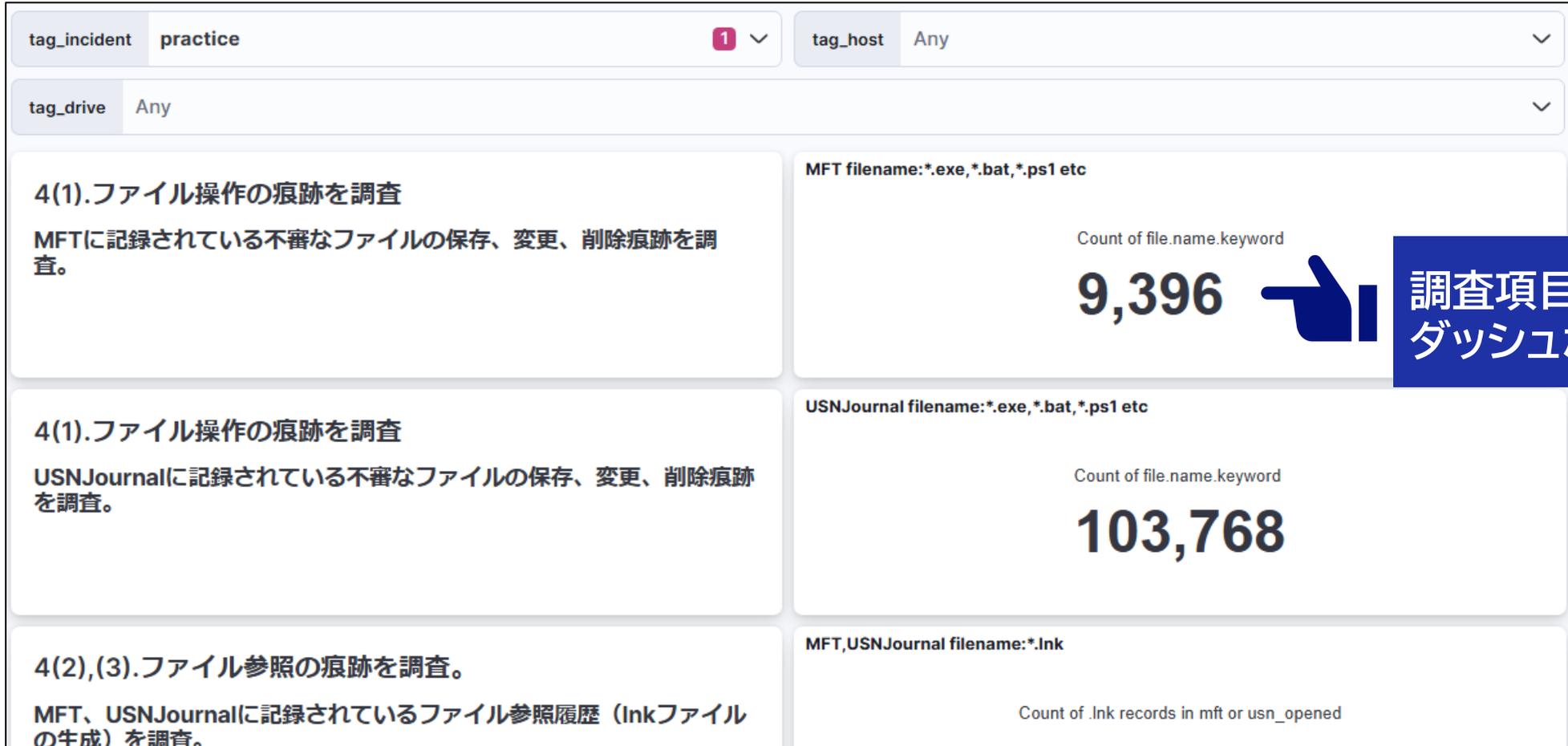


イベントログの
成形結果

これらの課題を解決するために、Kibanaダッシュボードの作成に取り組んだ

作成したKibanaダッシュボード(1/2)

◆ 調査項目ごとに対応するダッシュボードを作成



作成したKibanaダッシュボード(2/2)

tag: mft × file.extension: is one of exe, dll, src, com, job, vbs, ps1, psm1, scr, bat ×

tag_incident Any

◀ ▶

4-(1) MFTの不審なファイル操作の痕跡を調査。

【確認項目】

- file.path : パス
- file.name : ファイル名
- file.zone_id_contents : ダウンロード元を確認
- file.mtime.si : 最終ファイル修正時刻 (SI)
- file.accessed.si : 最終ファイルアクセス時刻 (SI)
- file.ctime.si : 最終MFTレコード修正時刻 (SI)
- file.created.si : ファイル生成時刻 (SI)

① file.extension: is one of exe, dll, src, com, job, vbs, ps1, psm1, scr, bat ×

②

【3つの工夫】

- ①ダッシュボードに遷移した時点でフィルタリングが完了
- ②確認すべきフィールドについて説明を記載
- ③確認すべきフィールドのみ表示

mft_timeline_base 9396 documents

Columns 1 field sorted

	@timestamp	tag_host	tag_drive	file.directory	file.name	file.zone_id_contents	file.mtime.si	file.accessed.si	file.ctime.si	file.created.si
✓	2022/03/01 15:58:06.857	KY1011	C	.\Windows\assembly\NativeImages_v4.0.30319_64\Microsoft.CSharp\badb4d0607cbbbd10c6b33a07635c05b	Microsoft.CSharp.ni.dll	(empty)	2022/03/01 15:58:06.873	2022/03/01 15:58:06.873	2022/03/01 15:58:06.904	2022/03/01 15:58:06.857
✓	2022/03/01 15:57:59.214	KY1011	C	.\Users\Alice\AppData\Local\Temp	__PSScriptPolicyTest_rrygnwn2.zvz.ps1	(empty)	2022/03/01 15:57:59.214	2022/03/01 15:57:59.214	2022/03/01 15:57:59.214	2022/03/01 15:57:59.214
✓	2022/03/01 15:57:59.214	KY1011	C	.\Users\Alice\AppData\Local\Temp	__PSScriptPolicyTest_onfp1ty1.01b.psm1	(empty)	2022/03/01 15:57:59.214	2022/03/01 15:57:59.214	2022/03/01 15:57:59.214	2022/03/01 15:57:59.214
✓	2022/02/13 23:42:01.448	KY1011	C	.\Windows\assembly\NativeImages_v4.0.30319_32\Microsoft.M870d558a#\db92e5434c588054bb630c44d0205559	Microsoft.Management.Infrastructure.Native.ni.dll	(empty)	2022/02/13 23:42:01.448	2022/02/13 23:42:01.448	2022/02/13 23:42:01.448	2022/02/13 23:42:01.448
✓	2022/02/13 23:42:01.040	KY1011	C	.\Windows\assembly\NativeImages_v4.0.30319_32\Microsoft.Kd58820a5#\13f90ca204868a15fec3c0fe64b95239	Microsoft.KeyDistributionService.Cmdlets.ni.dll	(empty)	2022/02/13 23:42:01.040	2022/02/13 23:42:01.040	2022/02/13 23:42:01.057	2022/02/13 23:42:01.040

実対応を通じたダッシュボードの改善

「侵害の原因」と「情報漏洩の有無」の観点はインシデント対応時に見解を求められることが多いため、ダッシュボードの改善を重点的に実施

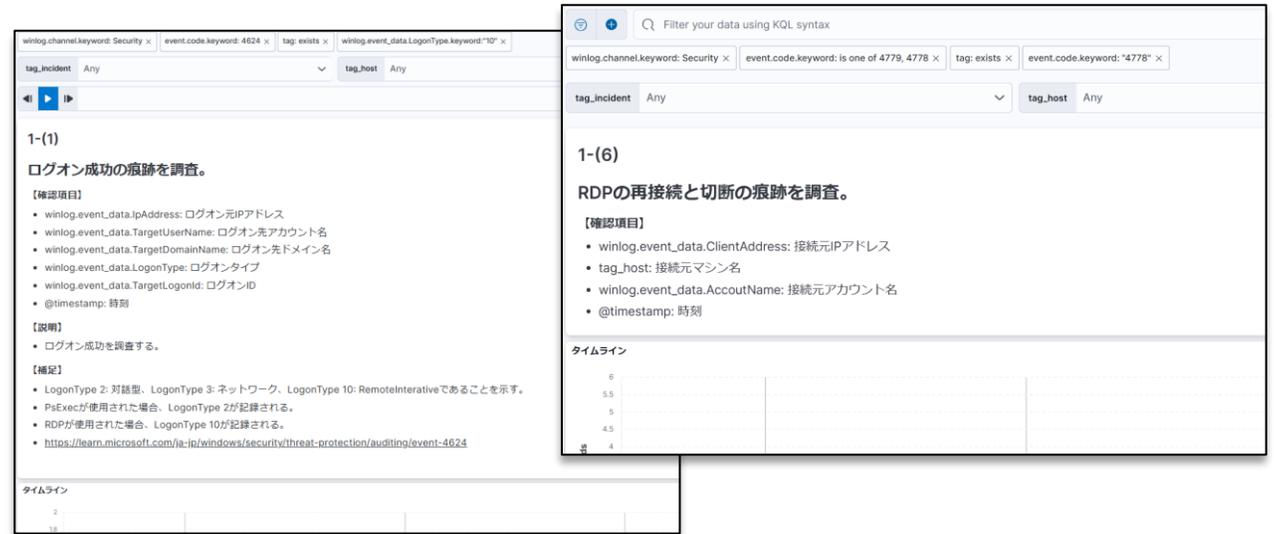
◆ 実対応時に感じたこと

■ 侵害の原因

- 1つの侵害方法に関連する調査項目は1つの画面で確認したい
- RDPであればイベントログ(Security)のイベントID4624、4778、4779等を確認するが、別々のダッシュボードになっている

■ 情報漏洩の有無

- Window OSからネットワーク通信が発生しているネットワークインターフェースの名前を特定したい



bytes.sent	network.interface_luid
4,615,938	1,689,399,632,855,040

- SRUMというアーティファクトで、特定のプロセスの1時間当たりの送信バイトを特定できる
- 紐づくInterfaceLuidは特定できるが、ネットワークインターフェースの名前までは分からない

侵害の原因

- ◆ 調査項目を横断した、攻撃者の侵害方法毎の調査ダッシュボードを作成
 - 画像はRDPのものだが、SMB、PSExec、WMI、PSRemotingでも同様に作成

The screenshot displays a security dashboard with two main panels. The top panel, titled '1-(1) Channel:Security, EventID:4624, LogonType:10', shows RDP login events. The bottom panel, titled '1-(6) Channel:Security, EventID: 4778 · 4779', shows session management events.

1-(1) Channel:Security, EventID:4624, LogonType:10
RDPでログオン成功した際に記録される。

確認項目

- winlog.event_data.IpAddress: ログオン元IPアドレス
- winlog.event_data.TargetUserName: ログオン先アカウント名
- winlog.event_data.TargetDomainName: ログオン先ドメイン名
- winlog.event_data.LogonType: ログオンタイプ
- winlog.event_data.TargetLogonId: ログオンID
- @timestamp: ログオン成功の時刻 (JST)

@timestamp	winlog.event_data.IpAddress	winlog.event_data.TargetD...	winlog.event_data.TargetU...	winlog.event_data.LogonT...	winlog.event_data.TargetL...
2023/09/06 14:34:21.096	0.0.0.0	[REDACTED]	[REDACTED]	10	0x781fb
2023/09/06 14:34:00.171	0.0.0.0	[REDACTED]	[REDACTED]	10	0x5d072
2023/09/06 12:36:51.393	0.0.0.0	[REDACTED]	[REDACTED]	10	0x3b3c22
2023/09/06 12:36:05.720	0.0.0.0	[REDACTED]	[REDACTED]	10	0x47aa20
2023/09/06 12:35:06.488	0.0.0.0	[REDACTED]	[REDACTED]	10	0x10a1a7

1-(6) Channel:Security, EventID: 4778 · 4779
セッションの再確立 (4778), セッションの切断 (4779) を確認

確認項目

- winlog.event_data.ClientAddress: 接続元IPアドレス
- winlog.event_data.AccountDomain: 標的ドメイン名
- winlog.event_data.AccountName: 標的アカウント名
- @timestamp: 時刻 (JST)
- winlog.event_data.SessionName: セッション名

@timestamp	tag_host	event.code.keywo...	winlog.event_data.Clien...	winlog.event_data.Acco...	winlog.event_data.Acco...	winlog.event_data.Sessi...
2023/11/22 09:48:47.960	DC	4778	ローカル	RIHT	Administrator	Console
2023/11/20 08:50:04.962	DC	4779	192.168.188.1	RIHT	Administrator	RDP-Tcp#0
2023/11/20 08:33:16.189	DC	4778	192.168.188.1	RIHT	Administrator	RDP-Tcp#0

ネットワークインターフェイス名の特定

◆ InterfaceLuidから、ネットワークインターフェイス名を特定するダッシュボードを作成

- 特定することで、インターネットに繋がるネットワークインターフェイスであるか容易に確認できる
- インターネットに繋がるものであった場合、危険度が高まる

InterfaceLuid ↔ InterfaceGuid				
Top 10000 values of winlog.event_data.IfLuid.keyword	Top 10000 values of winlog.event_data.InterfaceGuid.keyword	Count of records	Minimum of @timestamp	Maximum of @timestamp
1689399632855040	{fc5be0b6-a576-4474-9e2d-62c64723d349}	40	2023/11/15 10:03:41.341	2023/11/27 17:11:32.900

InterfaceGuid ↔ ネットワークインターフェイスの名前(NetworkCardsキー)				
2 documents				
Columns	1 field sorted			
@timestamp	tag_host	registry.value	registry.data.strings1	
2023/11/15 10:03:41.510	WS	ServiceName	{FC5BE0B6-A576-4474-9E2D-62C64723D349}	
2023/11/15 10:03:41.510	WS	Description	Intel(R) 82574L Gigabit Network Connection	

まとめ

- ◆ Windows OSに対するファストフォレンジックには以下のような課題があり、画一的かつ効率的に調査をすることが難しかった
 - テキスト形式でないアーティファクトが多く、解析のためにはツールを使った成形が必要
 - フォレンジック調査に活用できるデータに関する知識が必要
- ◆ スクリプトを使用したアーティファクトの一括成形とKibanaダッシュボード作成によって、上記課題を解決することができた
- ◆ 実対応を通して新たなダッシュボードを作成することで、さらなる効率化をすることができた

\Orchestrating a brighter world

NEC