

変更点

2.3.0 [2023/12/23] - SECCON Christmas Release

新機能:

- ATT&CK Navigatorで可視化するために、TTPを抽出してJSONファイルを作成する `ttp-visualize` コマンドを追加した。 (#76) (@fukusuket)
- コンピュータ毎に検知されたTTPsの要約を出力する `ttp-summary` コマンドを追加した。 (#78) (@fukusuket)

バグ修正:

- `timeline-partition-diagnostic` コマンドの文字化けを修正した。 (#74) (@fukusuket)

2.2.0 [2023/12/03] - Nasi Lemak Release

新機能:

- Windows10の `Microsoft-Windows-Partition%4Diagnostic.evtx` を解析し、接続されたすべてのデバイスおよびそれらのボリュームシリアル番号に関する情報を出力する `timeline-partition-diagnostic` コマンドを追加した。現在および過去に接続されたデバイスに関する情報を出力する。(処理は <https://github.com/theAtropos4n6/Partition-4DiagnosticParser> を参考に作成された) (#70) (@fukusuket)

改善:

- `vt-lookup` コマンドのプログレスバーの表示を改善した。 (#68) (@fukusuket)

バグ修正:

- キーが存在しない場合の未処理の例外のバグを修正した。 (#65) (@fukusuket)
- JSON入力の場合、`extract-scriptblocks` コマンドで改行処理が正しく行われていなかった。 (#71) (@fukusuket)

2.1.0 [2023/10/31] - Halloween Release

新機能:

- PowerShell EID 4104のScriptBlockログを元に戻す `extract-scriptblocks` コマンドを追加した。 (#47) (@fukusuket)

改善:

- TakajoがNim 2.0.0でコンパイルできるようになった。 (#31) (@fukusuket)
- 依存関係を減らすため、HTTPクライアントをPuppyに置き換えた。 (#33) (@fukusuket)
- パフォーマンス向上のため、VirusTotalクエリをマルチスレッドにした。 (#33) (@fukusuket)
- タイムラインを指定する際のファイル存在チェックを追加した。 (@fukusuket)
- タイムラインがJSONL形式でない場合の警告を追加した。 (#43) (@fukusuket)
- `sysmon-process-tree` コマンドでルートプロセス情報も出力する。プロセスがタイムスタンプ順にソートされるようになった。 (#54) (@fukusuket)

バグ修正:*

- Hayabusa 2.8.0以上の結果で `timeline-suspicious-processes` を実行した際のクラッシュを修正した。 (#35) (@fukusuket)

- 無効なAPIキーが指定された場合に、VirusTotalの検索でJSONパースエラーが発生する問題を修正した。 (@fukusuket)
- `sysmon-process-tree` コマンドでプロセス情報が2回出力されることがあるバグを修正した。(#52) (@fukusuket)
- `timeline-suspicious-processes` が `ParentPGUID` フィールドを正しく出力していなかったので修正した。また、PIDの10進数変換を改善した。(#50) (@fukusuket)
- 指定された `PGUID` が無効であるか、JSONL タイムラインに存在しない場合にエラーが発生する問題を修正した。(#53) (@fukusuket)

2.0.0 [2022/08/03] - [SANS DFIR Summit 2023 Release](#)

新機能:

- `list-domains` : `vt-domain-lookup` コマンドで使用する、重複のないドメインのリストを作成する。 (@YamatoSecurity)
- `list-hashes` : `vt-hash-lookup` で使用するプロセスのハッシュ値のリストを作成する。 (@YamatoSecurity)
- `list-ip-addresses` : `vt-ip-lookup` コマンドで使用する、重複のない送信元/送信先のIPリストを作成する。 (@YamatoSecurity)
- `split-csv-timeline` : コンピューター名に基づき、大きなCSVタイムラインを小さなCSVタイムラインに分割する。 (@YamatoSecurity)
- `split-json-timeline` : コンピューター名に基づき、大きなJSONLタイムラインを小さなJSONLタイムラインに分割する。 (@fukusuket)
- `stack-logons` : ユーザー名、コンピューター名、送信元IPアドレス、送信元コンピューター名など、項目ごとの上位ログオンを出力する。 (@YamatoSecurity)
- `sysmon-process-tree` : プロセスツリーを出力する。 (@hitenkoku)
- `timeline-logon` : ログオンイベントのCSVタイムラインを作成する。 (@YamatoSecurity)
- `timeline-suspicious-processes` : 不審なプロセスのCSVタイムラインを作成する。 (@YamatoSecurity)
- `vt-domain-lookup` : VirusTotalでドメインのリストを検索し、悪意のあるドメインをレポートする。 (@YamatoSecurity)
- `vt-hash-lookup` : VirusTotalでハッシュのリストを検索し、悪意のあるハッシュ値をレポートする。 (@YamatoSecurity)
- `vt-ip-lookup` : VirusTotalでIPアドレスのリストを検索し、悪意のあるIPアドレスをレポートする。 (@YamatoSecurity)

v1.0.0 [2022/10/28] - [Code Blue 2022 Bluebox Release](#)

新機能:

- `list-undetected-evt-x-files` : 検知しなかったルールファイルの一覧を表示する機能を追加した。(#4) (@hitenkoku)
- `list-unused-rules` : 検知しなかったevtxファイルの一覧を表示する機能を追加した。(#4) (@hitenkoku)
- ログを追加。 `-q`, `--quiet` で表示しないようにできる。(#12) (@YamatoSecurity @hitenkoku)
- `-o`, `--output` オプションの追加。結果を別ファイルにtxt形式で出力する機能を追加した。(#11) (@hitenkoku)