# Cisco Secure Endpointフォレンジックスナップショット情報

## 内容



## 概要

このドキュメントでは、フォレンジックスナップショットがエンドポイントから収集できる特権情報について説明します。

著者：Ciscoソフトウェアエンジニア、Pedro Medina

## 前提条件

- シスコの「セキュアエンドポイント」コンソール
- シスコ「Orbital」

### 要件

- AdminまたはNon-Adminユーザによる「セキュアエンドポイント」へのアクセス
- シスコの「Orbital」へのアクセス

**注：ユーザが管理者以外のユーザである場合は、TACサポートチームから「管理者以外のフォレンジックスナップショット」機能を有効にするようリクエストする必要があります。**

## 一般情報

フォレンジックスナップショットが要求されると、この説明表に基づいて必要な情報を見つけることができる、必要な情報に基づく表形式で情報が表示されます。

| [名前(Name)] | 意味 | プライバシーの問題 |
| --- | --- | --- |
| Autoexec項目 | コンピューターの起動時に実行される項目 | なし |
| Bitlocker暗号化の監視 | マウントされたすべてのドライブの暗号化ステータス | 暗号化されていないバージョンのファに対する一部の可視性 |
| DNSキャッシュテーブルモニタリング | 最近検索したドメイン | 最近のブラウザ履歴。 |

| | | |
|---|---|---|
| ホストファイルデータ | hostsファイルの項目 | なし |
| ホストにインストールされたプログラム | インストール済みアプリケーション | なし |
| リスニングポート | ネットワークリスナーを開くプログラムを一覧表示します | なし |
| ロードされたモジュールハッシュ | 実行中のダイナミックリンクライブラリ(DLL)ファイルのハッシュ値 | なし |
| ロードされたモジュールプロセス | 実行中のプロセスの名前、パス、および PID | なし |
| ロードされたモジュールとプロセス | ロードされたモジュールからプロセス表のPIDへのモジュールIDのマッピング | なし |
| ログオンセッション | システムユーザを含むログインユーザ | なし |
| マップされたドライブ | ローカルおよびリモートのマウントポイント、ファイル・システム・タイプ、ブート・パーティション情報、暗号化情報。 | なし |
| ネットワーク接続 – プロセス | 送受信ネットワーク接続を特定のPIDにマッピングし、プロセスを開始したスタートアップコマンドラインを表示します。 | 特定のアプリケーションのネットワー続が露呈する可能性があり、プライベである可能性があります。 |
| ネットワーク インターフェイス | デバイス上のすべての物理および仮想ネットワークインターフェイスのリスト | なし |
| ネットワークプロファイルレジストリ | マシンが接続しているネットワークのリスト。 | WIFI SSIDの潜在的な露出。 |
| OSバージョン | オペレーティングシステムのバージョン | なし |
| Powershell履歴 | デバイス上で実行され、システムに保存されているすべてのPowershellコマンドの一覧。 | パスワード、秘密のAPIキー、およびスプトにコード化されたその他の機密データを公開する可能性があります。 |
| プリフェッチディレクトリ | メモリ管理機能：OSは、頻繁にロードされる実行可能ファイルをプリロードして、起動時間を節約しようとします。 | ユーザの習慣の露出。 |
| 最近のファイルデータ | 最近使用/アクセスしたファイル | ユーザの習慣とプライベートなファイの公開。 |
| ファイルハッシュの実行 | 名前、パス、コマンドライン、PID、実行中のすべての実行可能ファイルの所有者。 | なし |
| サービスモニタリングの実行 | 実行中のすべてのサービスの名前、サービスタイプ、PID、およびスタートアップの種類 | なし |
| スケジュールされたタスク | システムで定期的に実行するように設定されたすべての自動タスクの一覧 | なし |
| 共有リソース | システムでsharesoを開きます | なし |
| スタートアップ項目 | マシンの起動時に実行される項目 – これらはレジストリキーに格納されるという点で | なし |

| | | |
|---|---|---|
| | autoexecとは異なります | |
| システムネットワーク状態の監視 | ネットワーク統計情報 | なし |
| 一時ディレクトリファイルデータ | プロセスによって作成された一時ファイル | ユーザの閲覧履歴が漏えいする可能性<br>ります。 |
| 信頼できるルート証明書 | 信頼されたルート証明書ストアのデータダンプ | なし |
| UBSTORレジストリキー | プラグインされたUSBデバイスの履歴 | デバイスのシリアル番号の露出。 |
| ユーザグループ | コンピューター上のローカルグループ | なし |
| UserAssistモニタリング | 最近実行したファイルを表示します | 暗号化やワイピングツールの実行など<br>れた動作が発生する可能性があります |
| ユーザ | デバイス上のローカルユーザ | なし |
| ユーザ – ログイン済み | 現在デバイスにログインしているローカルユーザ | なし |
| WMIイベントフィルタモニタリング | 特定の項目のイベントログを監視します | なし |
| Windows AV製品の監視 | システムにアンチウイルスがインストールされている場合 | なし |
| Windows BAMエントリの監視 | ファイルの実行の証拠を提供 | 動作を公開する可能性がある |
| Windows環境変数 | パス情報、システム変数などを表示します。 | なし |
| Windowsホットフィックス | インストールされているすべてのパッチのリスト | なし |
| Windows NTドメインの検索 | マシンが認証できるドメインのリスト | なし |
| Windows ShellBags監視 | フォルダに対するユーザのアクセス権や、そのフォルダを表示するための設定などに関する情報を提供します。 | ユーザの習慣の露出。 |
| Windows ShimCacheの監視 | 実行可能ファイルとの互換性を追跡 | ユーザの行動の露出。 |
| Chrome拡張機能の監視 | Chrome拡張機能を一覧表示します | ユーザの行動の露出。 |
| Windows Office MRU | 各Officeアプリケーションで最近使用したファイルを一覧表示します | 機密ファイル名の公開、ユーザの動作 |