

Advanced Malware Protection (アンペア) 偽検出、発生およびインシデント レスポンスを操作する場合

目次

[はじめに](#)

[説明](#)

[即時の処置](#)

[分析](#)

[Cisco による分析](#)

[関連記事](#)

概要

Advanced Malware Protection (アンペア) テクノロジーのための脅威知性を改善し、拡張するように常に努力しますがアンペア ソリューションがアラートを誘発しなかったし、またはアラートを間違っ​​て引き起こさなかったら、環境にそれ以上の影響を防ぐいくつかの処置をとることができます。この資料はそれらのやるべきことでガイドラインを提供したものです。

説明

即時の処置

アンペア ソリューションは脅威からネットワークを保護しなかったことを信じたら、次の処置をすぐにとって下さい:

1. ネットワークの他からの疑わしい マシンを隔離して下さい。これはマシンを消すか、またはネットワークから物理的に切り離すことを含む可能性があります。
2. マシンが感染するかもしれませんときに疑わしい マシンで感染、のような、時間ユーザー操作、先祖などについての重要な情報を書いて下さい

警告: 一掃しませんでしたり、またはマシンをイメージ変更しないで下さい。それは法廷調査かトラブルシューティング プロセスの間におこるソフトウェアかファイルを見つける可能性を除去します。

分析

1. あなた自身の調査を始めるのにデバイス トラジェクトリ機能を使用して下さい。デバイス トラジェクトリは 9,000,000 のほとんどの最近のファイル イベントをおよそ保存することができます。エンド ポイント デバイス トラジェクトリのためのアンペアはファイルを見つけ出すために非常に役立ちますまたはそれが感染に導いたプロセス。

ダッシュボードでは、**管理 > コンピュータへのナビゲート**。

Quick Start

Computers

Groups

Policies

疑わしいマシンを探し、そのマシンのためのレコードを拡張して下さい。トラジェクトリオプションを『Device』をクリックして下さい。

| centos in group Lab | | | |
|---------------------|--------------------------------------|-------------|----------------|
| Hostname | centos | Group | Lab |
| Operating System | CentOS Release 6.7 | Policy | LabLinux |
| Connector Version | 1.1.0.277 | Internal IP | 192.168.1.104 |
| Install Date | 2016-05-16 14:28:56 UTC | External IP | 64.102.253.119 |
| Connector GUID | d7fcf8ee-8f71-4bda-9b3c-7c90803f6f03 | Last Seen | Recently |

[Events](#)
[Device Trajectory](#)
[View Changes](#)
Q Scan
Move to Group...
Delete

- 疑わしいファイルを見つけるか、またはハッシュする場合、カスタム検出リストにそれを追加して下さい。エンドポイントのためのアンペアはファイルを扱うか、または悪意のあるようにハッシュするのにカスタム検出リストを使用できます。これはそれ以上の影響を防ぐために応急力バレッジを提供する大きい方法です。

Cisco による分析

- 動的解析のために疑わしいサンプルを入れて下さい。ダッシュボードで分析 > ファイル分析から手動でそれらを入れることができます。エンドポイントのためのアンペアは[脅威グリッド](#)からのファイルの動作のレポートを生成する動的解析機能性が含まれています。調査チームによる追加分析が必要となればこれにまた Cisco へファイルを提供することの利点があります。
- ネットワークの *false positive* または偽陰性検出を疑う場合、アンペア製品ののためのカスタム黒いリストまたは白リスト機能性を利用することを助言します。Cisco Technical Assistance Center (TAC) に連絡するとき、分析に次の情報を提供して下さい: ファイルの SHA256 ハッシュ。ファイルのコピーもし可能なら。どこにどのような来た、そしてなぜから環境にある必要があるかファイルについての情報。false positive または偽陰性であるとこれがなぜ信じるか説明して下さい。
- 脅威を軽減するか、またはアクションプランを作成し、アクティブな発生を軽減するために感染したマシンを研究し、高度ツールが機能を利用していることを専門にする環境のトリアージを行っていればアシスタンスを必要とする場合 Cisco セキュリティ インシデント レスポンス サービス (CSIRS) チームを実行する必要があります。

注: Cisco Technical Assistance Center (TAC) は約束のこの型を支援に与えません。

CSIRS チームはこの電話番号を呼出すことによって engaged できます: +1-844-831-7715。これは組織に Cisco からのインシデント レスポンス サービスのための保持板がなければ \$60,000 で開始する支払済サービスです。実行されてそれらがサービスについてのそ

の他の情報を提供し、事件のためのケースをオープンすれば。それらがプロセスで追加指導を提供できるようにまた Cisco Account Manager によって追うことを推奨します。

関連記事

- [Windows FireAMP](#)
- [FireAMP](#)