

エンドポイント用AMPまたはFireAMPによるエンドポイントIOCスキュンの実行

内容

[概要](#)

[前提条件](#)

[要件](#)

[使用するコンポーネント](#)

[背景説明](#)

[IOC シグニチャ ファイル](#)

[IOC シグニチャ ファイルでのスキュンの実行](#)

[IOC シグニチャ ファイルの作成](#)

[IOC シグニチャ ファイルのアップロード](#)

[スキュンの開始](#)

概要

このドキュメントでは、Mandiant IOC エディタで侵入の痕跡 (IOC) 署名ファイルを作成する方法、Cisco FireAMP ダッシュボードにこのファイルをアップロードする方法、およびエンドポイント IOC スキュンを開始する方法について説明します。

前提条件

要件

エンドポイント IOC スキュンを実行する前に、ドライブに 1 ギガバイト以上の空き容量があることを確認することを推奨します。

使用するコンポーネント

このドキュメントの情報は、Cisco FireAMP Windows Connector バージョン 4.0.2 以降で利用可能なエンドポイント IOC スキュナに基づいています。

このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されました。このドキュメントで使用するすべてのデバイスは、初期 (デフォルト) 設定の状態から起動しています。対象のネットワークが実稼働中である場合には、どのようなコマンドについても、その潜在的な影響について確実に理解しておく必要があります。

背景説明

エンドポイント IOC スキャナ機能は、複数のコンピュータにわたり、セキュリティ侵害後のインジケータをスキャンするために使用する、強力なインシデント対応ツールです。

注：FireAMP では Mandiant 言語で IOC をサポートしていますが、Mandiant IOC エディタ自体はシスコにより開発されたものではなく、シスコではサポートしていません。シスコサポートでは、ユーザが作成した IOC またはサードパーティ製 IOS のトラブルシューティングは行いません。

IOC シグニチャ ファイル

IOC シグニチャ ファイルは、既知の脅威、攻撃者の攻撃手法、またはその他の侵害の証拠を特定する技術特性を説明する、拡張可能な XML スキーマです。

エンドポイント IOC は、OpenIOC ベースのファイルからコンソール経由でインポートされます。このファイルは、名前、サイズ、ハッシュなどのファイル プロパティと、プロセス情報、実行中のサービス、Microsoft Windows レジストリ エントリなどのシステム プロパティをトリガーとして使用するように作成されています。IOC 構文は、インシデント対応者が特定のアーティファクトを検索したり、マルウェア ファミリの洗練された相関検出を作成するロジックを使用したりするために使用できます。

IOC シグニチャ ファイルでのスキャンの実行

IOC シグニチャ ファイルでスキャンを実行するには、以下の 3 つのステップを完了する必要があります。

1. IOC シグニチャ ファイルを作成します。
2. IOC シグニチャ ファイルをアップロードします。
3. スキャンを開始します。

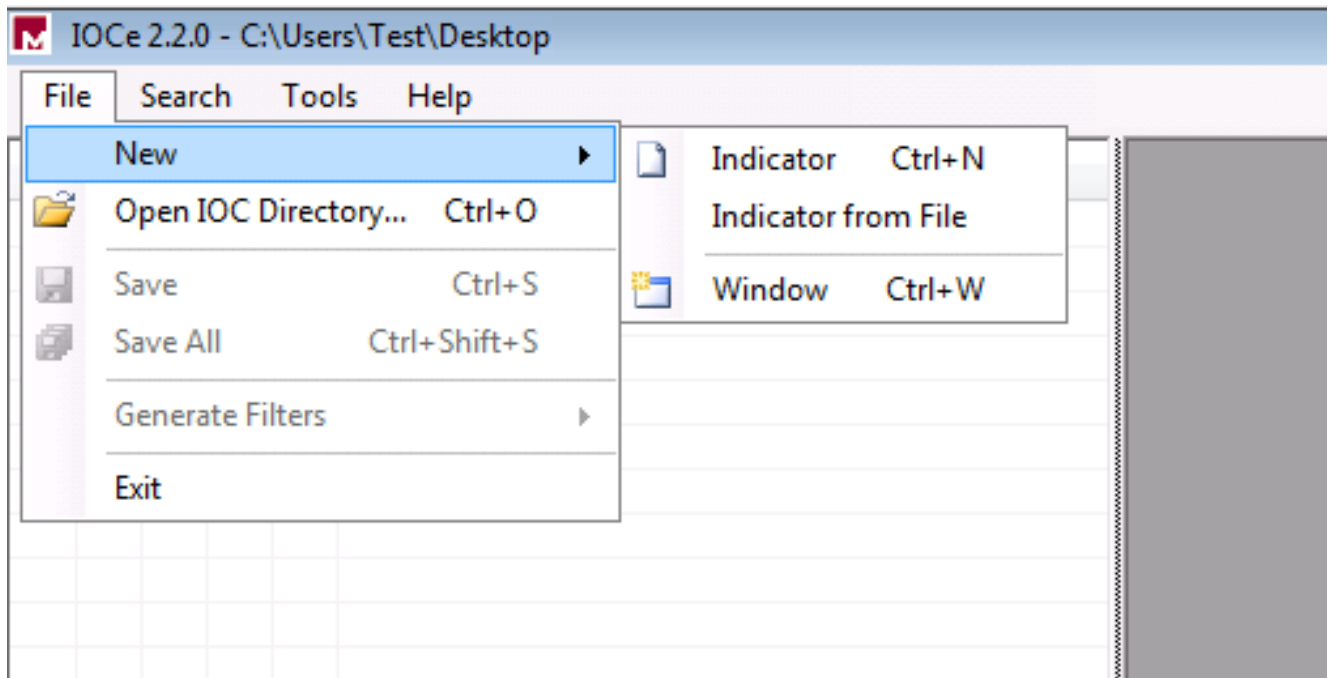
以降のセクションで、これらのステップについて説明します。

IOC シグニチャ ファイルの作成

注：この例では、Mandiant IOC エディタを使用して、`test.txt` という名前のテキスト エディタの IOC シグニチャ ファイルを作成します。

IOC シグニチャ ファイルを作成するには、次の手順を実行します。

1. [IOCe]を開き、[File] > [New] > [Indicator] に移動します。ブランクのワークスペースが表示されます。ここで、IOC の作成を開始できます。



注：特定の目的に応じた IOS を作成する場合は、該当するプロパティを備えたバイナリ ロジックを使用します。初期演算子は OR です。この最も単純な演算子をベースに、作業を開始できます。これにより IOC の初期機能が有効になるので、演算子を変更する必要はありません。スキャンで IOS シグニチャ ファイルを使用するには、少なくとも 2 つのプロパティまたは条件がファイルに設定されている必要があります。

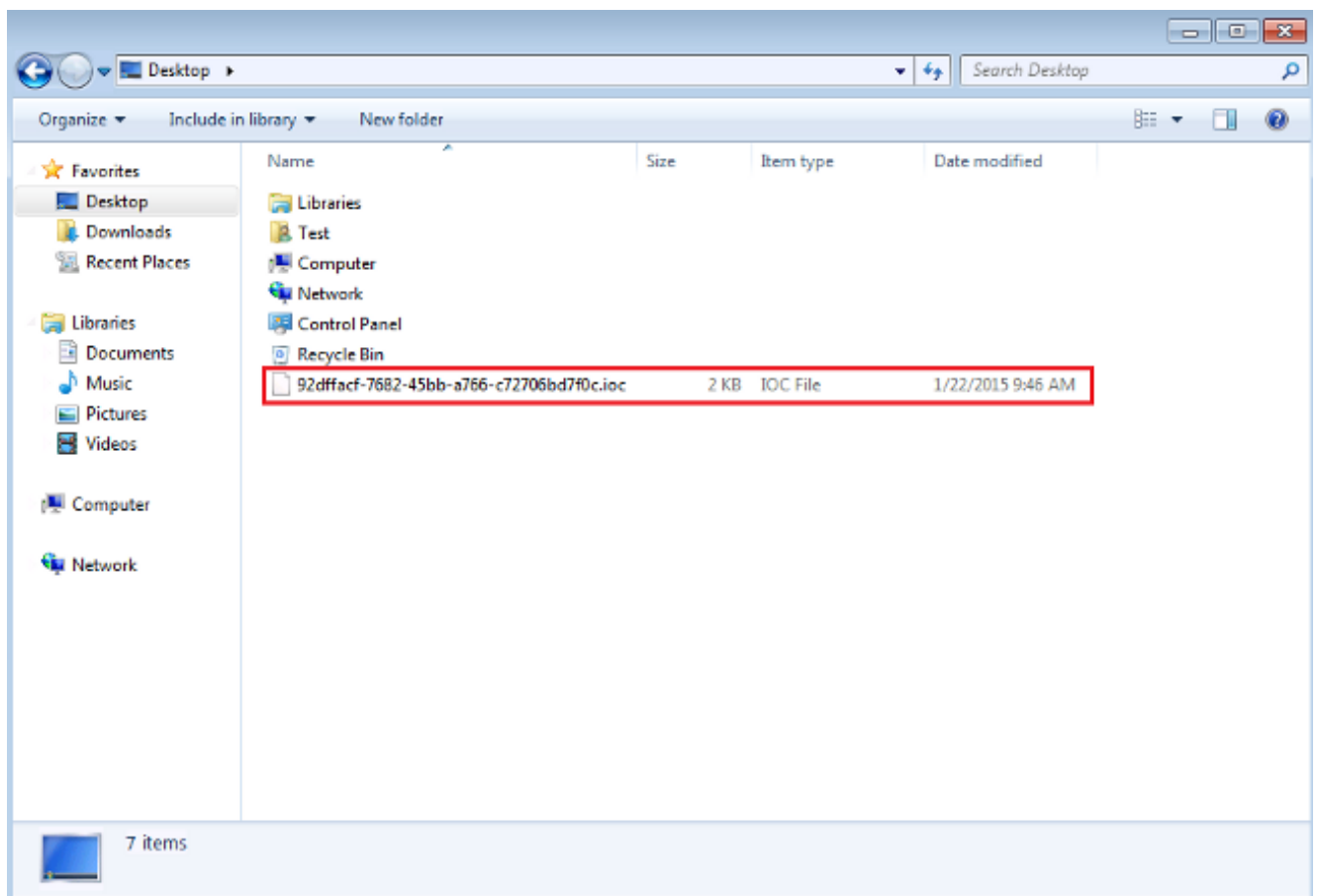
2. 演算子を追加するために、[Items] ドロップダウン メニューをクリックします。追加する必要がある最初のプロパティは、[File Extension contains] です。[Items] ツリー メニュー内でこのプロパティを見つけてクリックします。
3. プロパティを追加した後、画面右端にある小さいアイコンをクリックして [Configuration] ペインを開きます。このペイン内の [Content] フィールドを使用して、照合するファイル拡張子を追加します。たとえば、**test.txt** ファイルを照合するには、**[txt]** を追加します。



4. 次は、論理演算子を追加する必要があります。この例では、[test] テキスト ファイルと一致させるので、[AND] 演算子を使用して、次のプロパティを追加します。[Items] ツリー メニュー内でファイル名を見つけて選択します。[Properties] ペインで、検索対象のファイルの名前を追加します。たとえば、[Content] フィールドに [test] を追加します。



5. この単純な IOC には、他に追加しなければならないプロパティはないので、この時点でファイルを保存できます。[File] > [Save]の順にクリックします。これで、.ioc 拡張子が付いたシグニチャファイルがシステムに保存されます。



IOC シグニチャ ファイルのアップロード

スキャンを実行するには、IOC ファイルを FireAMP ダッシュボードにアップロードする必要があります。IOC シグニチャ ファイル、XML ファイル、あるいは複数の IOC ファイルが含まれる zip アーカイブを使用できます。ダッシュボードによって圧縮解除されて、IOC シグニチャを含むファイルが解析されます。構文エラーがある場合や、サポートされていないプロパティが使用されている場合は、通知されます。

ヒント：アップロードできるファイルのサイズは、最大 5 メガバイトです。

以下の手順に従って、IOC シグニチャ ファイルを FireAMP ダッシュボードにアップロードします。

1. FireAMP クラウド コンソールにログインし、[Outbreak Control] > [Installed Endpoint IOC]に移動します。
2. [Upload]をクリックします。これにより、[Upload Endpoint IOCs] ウィンドウが表示されます。

Upload Endpoint IOCs ×

You can upload a single Endpoint IOC XML file, or a .zip file containing multiple Endpoint IOC documents

There is a 5 megabyte file upload limit

No file selected Browse

Close Upload

IOC シグニチャ ファイルのアップロードが正常に完了すると、シグニチャがリストに表示されます。

Endpoint IOC - Installed Endpoint IOCs ^{beta}

Categories + Groups + Keywords +

Search Showing ? Actions ▾ □

Upload

<input type="checkbox"/> Test 59c4cc2d-e1e7-489f-93fd-30596fda0052.ioc	Uploaded: 9:20 AM Eastern Standard Time, 1/22/2015	Active	View Edit 🗑️ 📄
---	---	--------	--

3. シグニチャの実際の XML データを表示するには、[View]をクリックします。

Endpoint IOC beta

File name: 59c4cc2d-e1e7-489f-93fd-30596fda0052.ioc

View All

View

Edit

Active

Short Description:

Test

Description

No description given

Categories

No Categories to display

IOC Groups

No IOC Groups to display

Keywords

No Keywords to display

Source [Download]

```
1 <?xml version="1.0" encoding="us-ascii"?>
2 <ioc xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance" xmlns:xsd="http://www.w3.org/2001/XMLSchema"
3 id="59c4cc2d-e1e7-489f-93fd-30596fda0052" last-modified="2015-01-22T14:16:48" xmlns="http://schemas.mandiant.co
4 /2010/ioc">
5   <short_description>Test</short_description>
6   <authored_by>Test Author</authored_by>
7   <authored_date>2015-01-22T14:16:35</authored_date>
8   <links />
9   <definition>
10    <Indicator operator="OR" id="325adeacd-d75e-4fae-9cf4-cf8dcae84a36">
11      <IndicatorItem id="5311e18c-0e6a-4491-bb1a-a63331a463a2" condition="contains">
12        <Context document="FileItem" search="FileItem/FileExtension" type="mir" />
13        <Content type="string">txt</Content>
14      </IndicatorItem>
15      <Indicator operator="AND" id="017fc010-f0ea-4ede-b252-885bb85cfcf3">
16        <IndicatorItem id="6ac73c61-9e9f-43da-9317-38d09990c337" condition="contains">
17          <Context document="FileItem" search="FileItem/FileName" type="mir" />
18          <Content type="string">test</Content>
19        </IndicatorItem>
20      </Indicator>
21    </Indicator>
22  </definition>
23 </ioc>
```

スキヤンの開始

シグニチャ ファイルをアップロードした後、フル スキヤンを実行します。最初のスキヤンは、コンピュータ全体のメタデータのカタログを作成する必要があるため、フルスキヤンである必要があります。これは、1 ~ 2時間かかる可能性があります。フル スキヤンによってシステムのカタログが構築された後は、フラッシュ スキヤンを実行できます。

注：フル スキヤンは CPU を駆使します。PC の使用中にはフル スキヤンを実行しないようにしてください。このスキヤン機能を定期的使用する予定の場合は、カタログを再構築するために毎月 1 回フル スキヤンを実行できます。

IOC スキヤンを実行するには、2 つの方法を使用できます。1 つは、イベントまたはダッシュボードから即時スキヤンを実行するという方法です。このスキヤンは、次回 PC がクラウドにハートビートを送信するとトリガーされます。

注：初めてフル スキヤンを実行する場合は、[Re-catalog before scan]オプションをオンにする必要はありません。

Run Scan on win7



Windows 7, SP 1.0 Device in
IOC Test using IOC Test

1 Endpoint IOC active.

Scan Engine:

File

Endpoint IOC

Scan Depth:

Flash

Full

Re-catalog before scan

Running a full scan is **time consuming and resource intensive**. On endpoints with a large number of files a full scan can take multiple days to run. You should only run a full scan during non-business hours otherwise consider running a flash scan.

Close

Start Scan

もう一つの方法は、ダッシュボードの [Outbreak Control]メニューから、スケジュールされたエンドポイント IOC スキャンを作成することです。オフピーク中にスキャンを実行したい場合は、このオプションが最適です。スケジュールされたタスクを作成し、[Log on as Batch] グループ ポリシー アクセス権限を許可するには、対象のコンピュータへのアクセス権限が割り当てられたアカウントのクレデンシャルを入力する必要があります。

Endpoint IOC - Initiate Scan ^{beta}

Policy:

IOC Test

Scheduled Scan User Name:

Test

Scheduled Scan Password:

••••••••

Run Scan On:

2015-01-22

09

:

30

Flash scan

Full scan

Re-catalog before scan

Schedule Scan

1 Active Endpoint IOC

1 group using IOC Test with 1 Endpoint IOC capable connector out of 1 total connector

- ioc test with 1 Endpoint IOC capable connector out of 1 total connector

エンドポイント IOC スキャンをスケジュールする際に、以下の警告メッセージが表示されます。

Warning



Running a full scan is **time consuming and resource intensive**. On endpoints with a large number of files a full scan can take multiple days to run. You should only run a full scan during non-business hours otherwise consider running a flash scan.

You have selected to re-catalog before a full scan, which can take longer to complete. You may not need to re-catalog if you recently ran a full scan with re-catalog.

Are you sure you want to schedule a full scan ?

Close

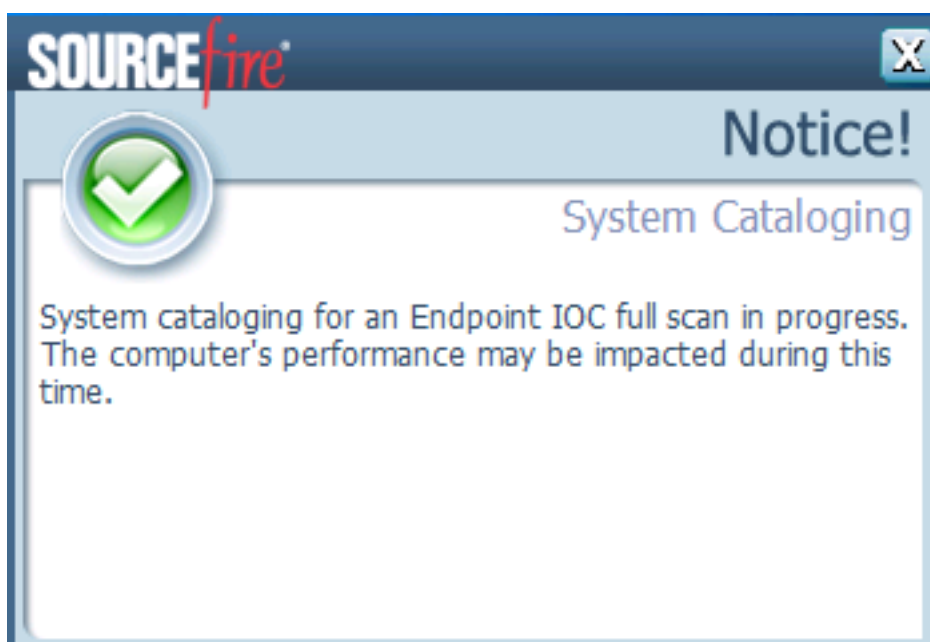
Schedule

入力したクレデンシャルが有効であれば、次回 PC がハートビートを送信するときに以下のようなジョブが Windows タスク スケジューラに表示されます。

Name	Status	Triggers	Next Run Time
Immunet Scan 1421937278	Ready	At 9:40 AM on 1/22/2015	1/22/2015 9:40:00 AM

スキャンが開始すると、以下のメッセージが表示されます。

注：非表示になるように GUI が設定されている場合、[System Cataloging]メッセージは表示されません。



スキャンが完了した後、[Endpoint IOC Scan Detection Summary]を表示できます。以下の例に、test.txt IOC シグニチャ ファイルの一致結果を示します。

Win7 Scanned 16713078 objects. Found 655 matching objects and 0 malicious detections. 11:55 AM Eastern Standard Time, 1/22/2015

Connector Info: Computer: win7, Connector GUID: a0881bab-af05-402c-a7c8-0bf0824a6638, Current User: [redacted]

Run Scan | Launch Device Trajectory

Win7 Endpoint IOC Scan Detection Summary (matched 1 of 1 IOCs). 11:55 AM Eastern Standard Time, 1/22/2015

Endpoint IOC Summary: Matching Endpoint IOCs: Test [Filename: 59c4cc2d-e1e7-489f-93fd-305968da0052.ioc]

View All