进行妥协(IOC)扫瞄的终端征兆与终端或FireAMP的安培

目录

简介

本文描述如何通过Mandiant IOC编辑器创建妥协(IOC)签名文件的征兆，如何上传它到思科FireAMP控制板和如何启动终端IOC扫描。

先决条件

要求

思科建议您有自由推进空间至少一千兆字节，在您尝试运行终端IOC扫瞄前。

使用的组件

本文档中的信息根据终端IOC扫描仪，是可用的在Cisco FireAMP Windows连接器版本4.0.2和以上。

本文档中的信息都是基于特定实验室环境中的设备编写的。本文档中使用的所有设备最初均采用原始（默认）配置。如果您使用的是真实网络，请确保您已经了解所有命令的潜在影响。

背景信息

终端IOC扫描仪功能是使用为了扫描在多台计算机间的POST妥协指示器的一个强大的事件响应工具。

> **注意**：虽然FireAMP支持与Mandiant语言的IOC，没有开发也思科不支持Mandiant IOC编辑器软件。Cisco支持不排除故障用户建立或第三方IOC。

IOC签名文件

IOC签名文件是识别已知威胁、攻击者方法，或者妥协其他证据技术特征的说明的一可扩展XML模式。

您能通过控制台导入终端IOC从在文件特性写入为了触发例如名称、大小和哈希的基于OpenIOC的文件，以及其他属性和系统属性例如进程信息，运行服务和Microsoft Windows注册表条目。IOC语法可以由事件响应方用于为了查找特定人工制品或为了使用逻辑创建恶意软件家族的复杂，关联的检测。

运行在IOC签名文件的扫描

有您必须完成为了运行在IOC签名文件的一扫描的三个步骤：

1. 创建IOC签名文件。
2. 上传IOC签名文件。
3. 启动扫描。

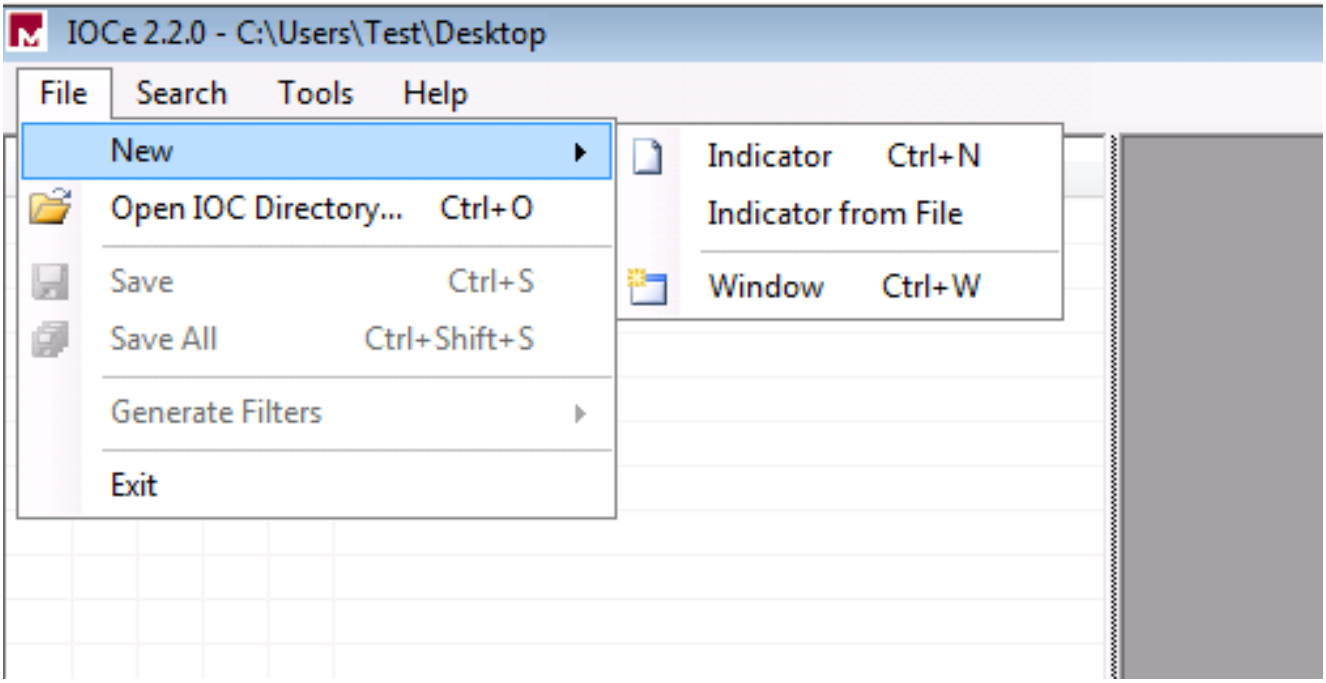
这些步骤在跟随的部分被扩展。

创建IOC签名文件

> **注意**：在本例中， Mandiant IOC编辑器用于为了创建名为**test.txt的**文本文件的IOC签名文件。

完成这些步骤为了创建IOC签名文件：

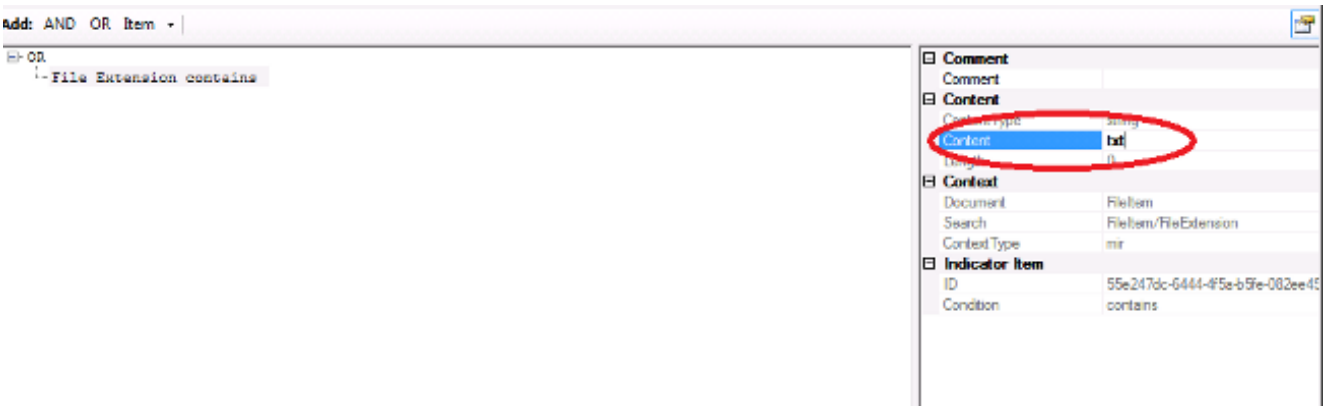
1. 打开**IOCe**并且导航到**File > New >指示器**。这提供一个空白的工作区，以便您能开始构件IOC。



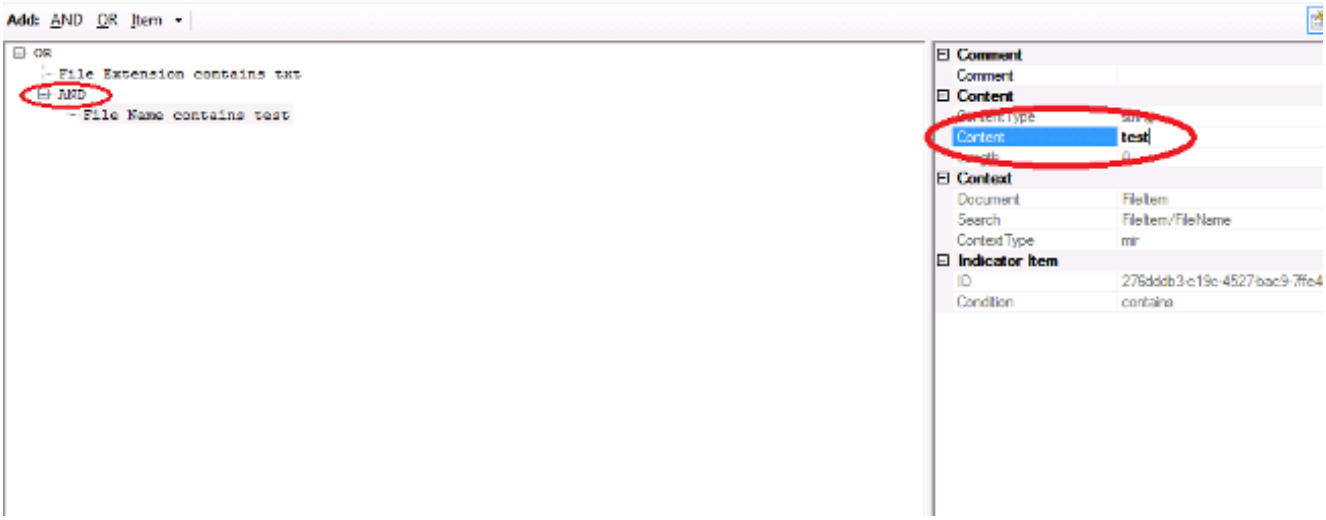
注意：为了创建特定的事的IOC，请以属性使用二进制逻辑。最初的操作员是或，是工作的最简单的基础。这允许IOC的初始函数工作，因此您没有要求更改它。要求IOC签名文件在扫描有至少两个属性或情况为了顺利地使用它。

2. 点击**项目**下拉菜单为了添加操作员。您应该添加的第一个属性是**文件扩展包含**。查找在**项目**树菜单的属性并且点击它。

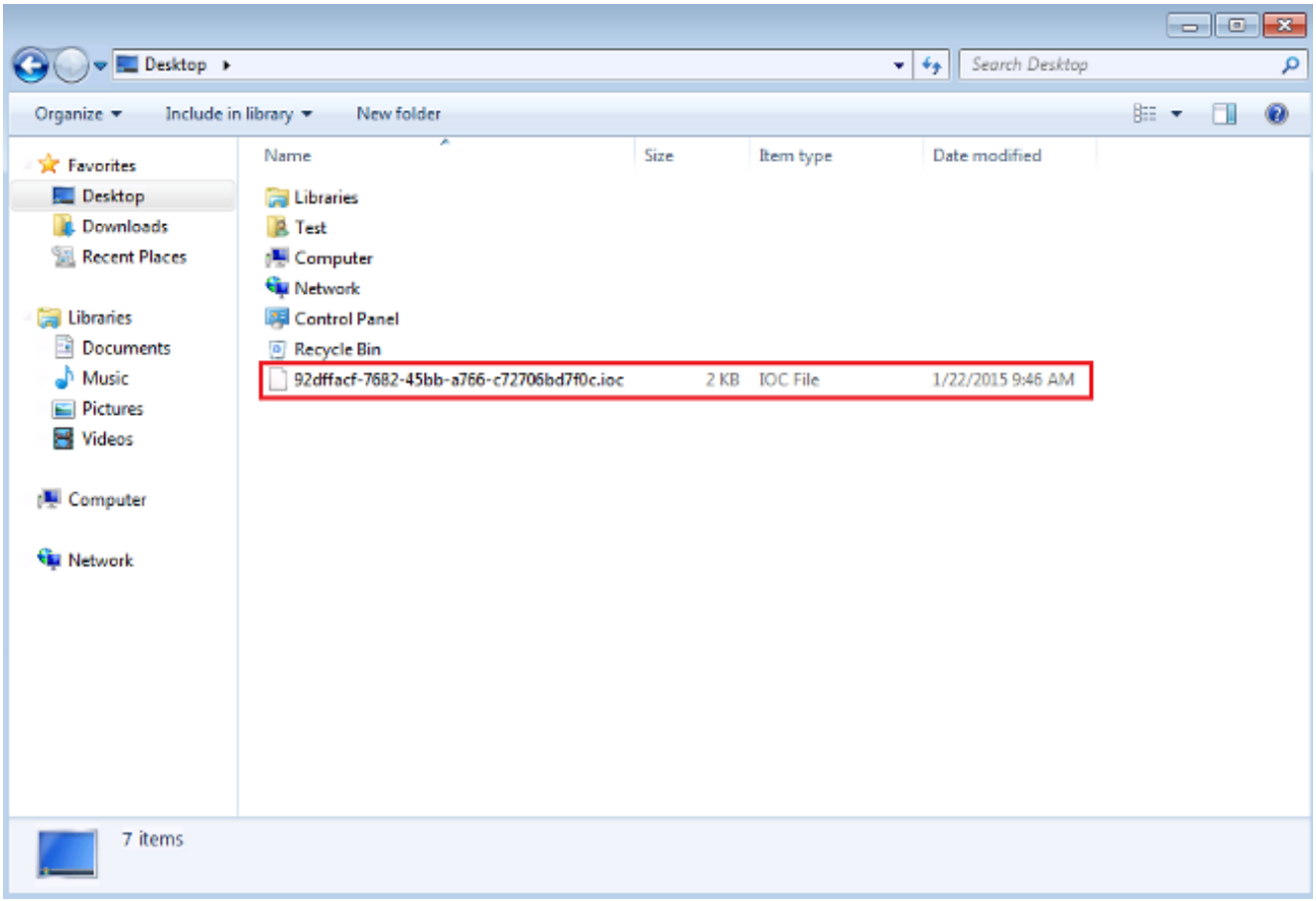
3. 在您添加一属性后，请点击在屏幕的最右端的小图标为了打开配置窗格。在此窗格内，请使用**内容**字段为了匹配文件扩展。例如，请添加**txt**为了匹配**test.txt**文本文件：



4. 您必须当前添加逻辑操作员。在本例中，您将匹配**测试正文**文件。为了匹配此，请使用*和*操作员并且添加下属性。找出文件名并且从**项目**树菜单选择它。在属性窗格中，请添加您要查找文件的名称。例如，请在内容字段添加**测验**：



5. 因为另外的属性为此简单IOC不是必要的，您能当前保存文件。点击**File > Save**，并且有**.ioc**分机的一个签名文件在system:保存



上传IOC签名文件

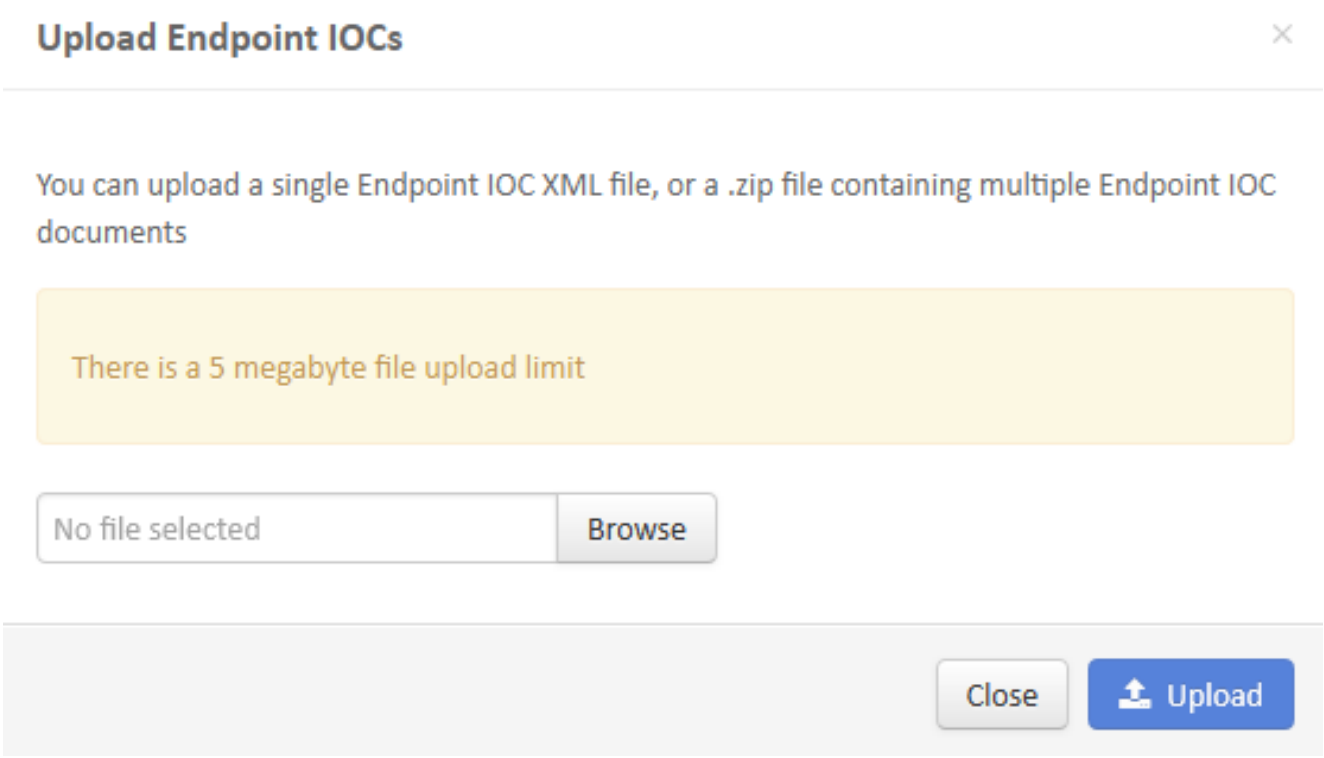
为了执行扫描，您必须上传IOC文件到FireAMP控制板。您能使用IOC签名文件、XML文件或者包含多个IOC文件的邮政编码存档。控制板解压并且解析有IOC签名的文件。如果使用，您通知不正确的语法或一不支持的属性。

提示：您能上传在大小上是五兆字节的文件。

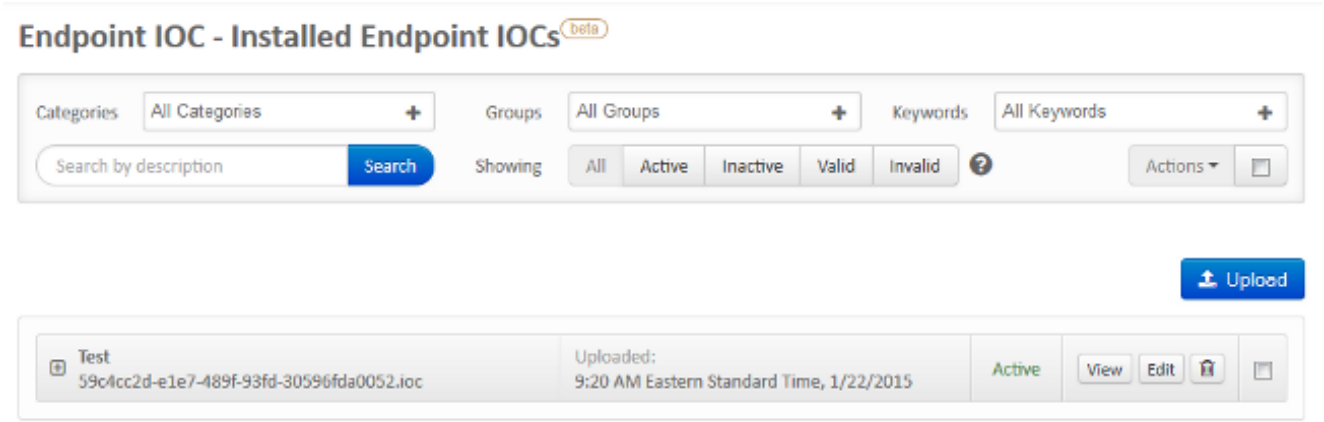
完成这些步骤为了上传IOC签名文件到FireAMP控制板：

1. 登录FireAMP Cloud控制台并且导航到**爆发控制>安装终端IOC**。

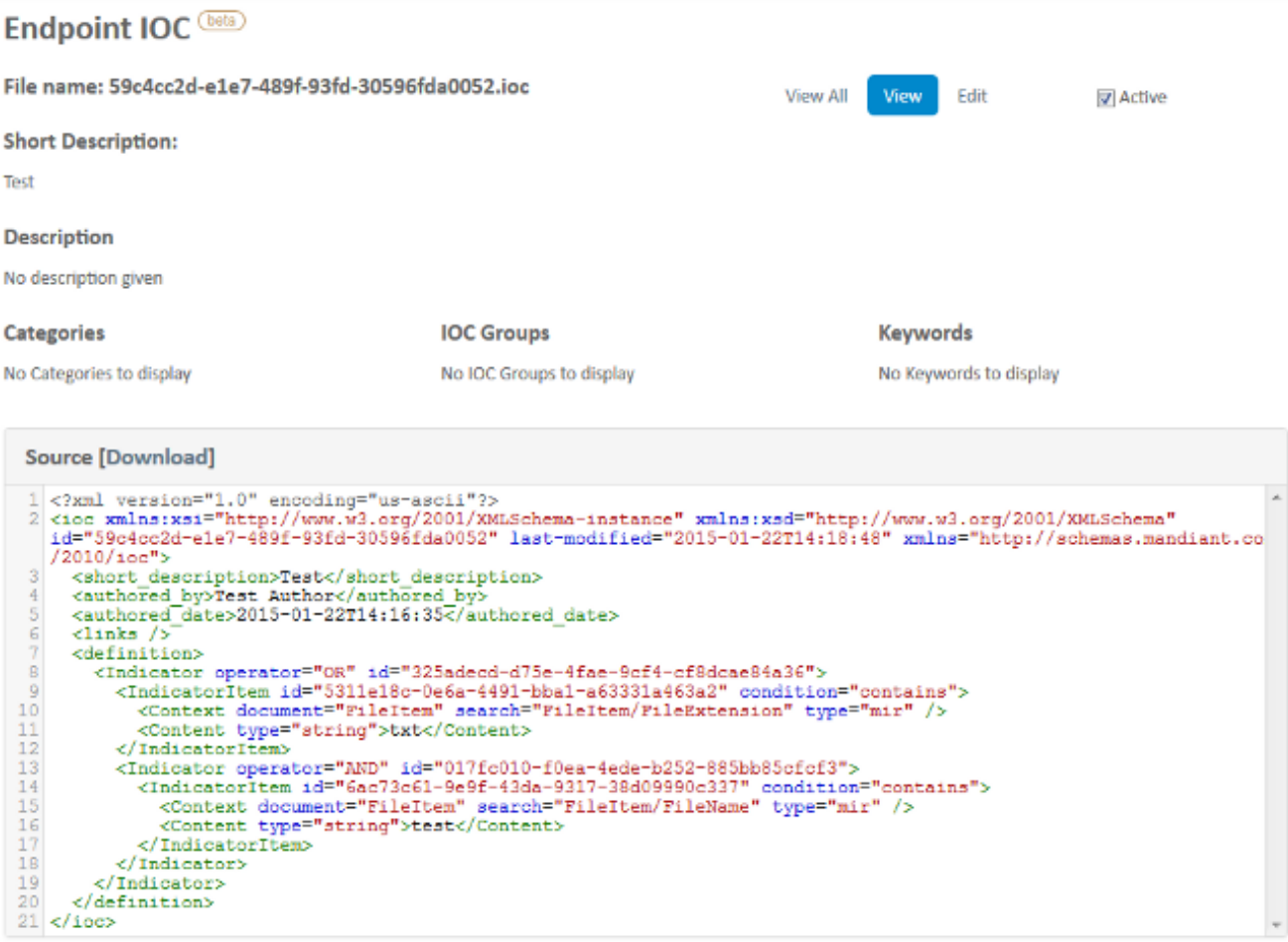
2. 点击**加载**，并且**加载终端IOC**窗口出现：



在IOC签名文件顺利后地上传，签名出现在列表：



3. 点击**视图**为了查看签名的实际XML数据：



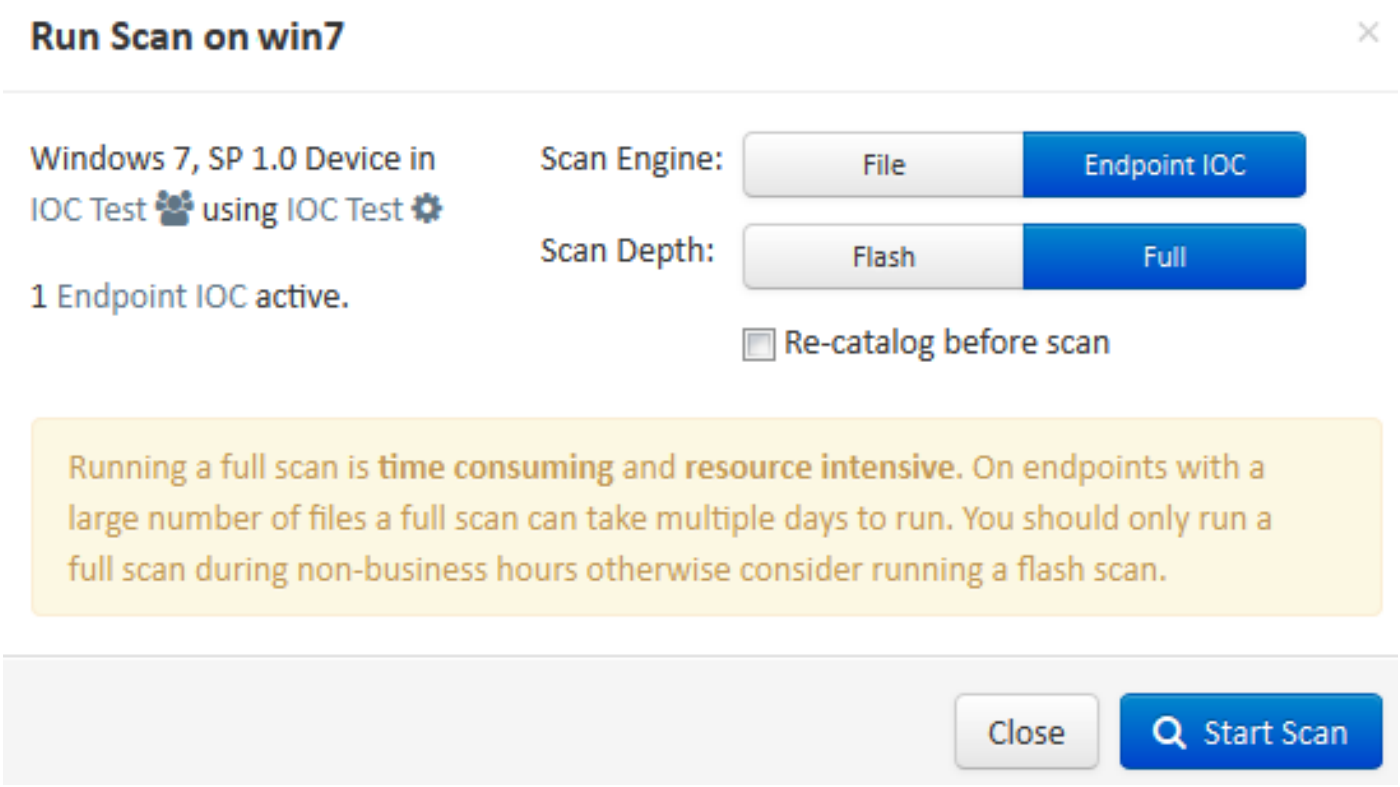
启动扫描

在您上传签名文件后，请执行一全双工扫描。第一扫描必须是一全双工扫描，因为必须构件元数据目录整个计算机的，能耗费1个– 2个小时。在系统通过一全双工扫描后，编目您可执行一*闪存*扫描。

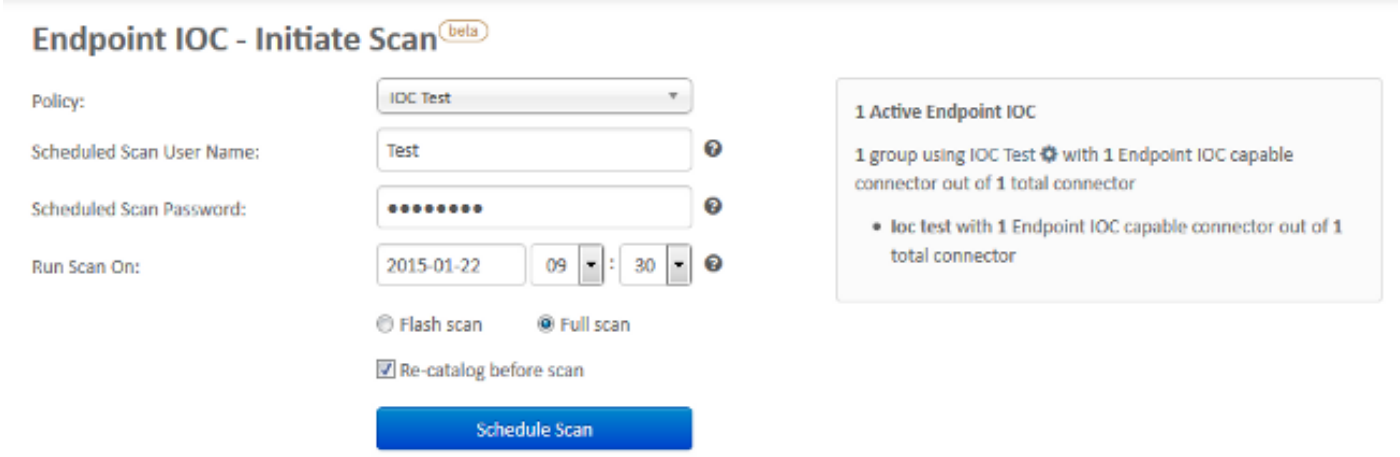
> **注意**：全双工扫描非常强化中央处理。思科建议您不运行在PC的一全双工扫描，当是在使用中的时。如果计划定期使用功能，您可每月一次执行一全双工扫描为了重建目录。

有您能使用为了运行IOC扫描的两不同的说法。第一种方法是执行一立即扫描从事件或从控制板。PC发送检测信号对Cloud的这下次被触发。

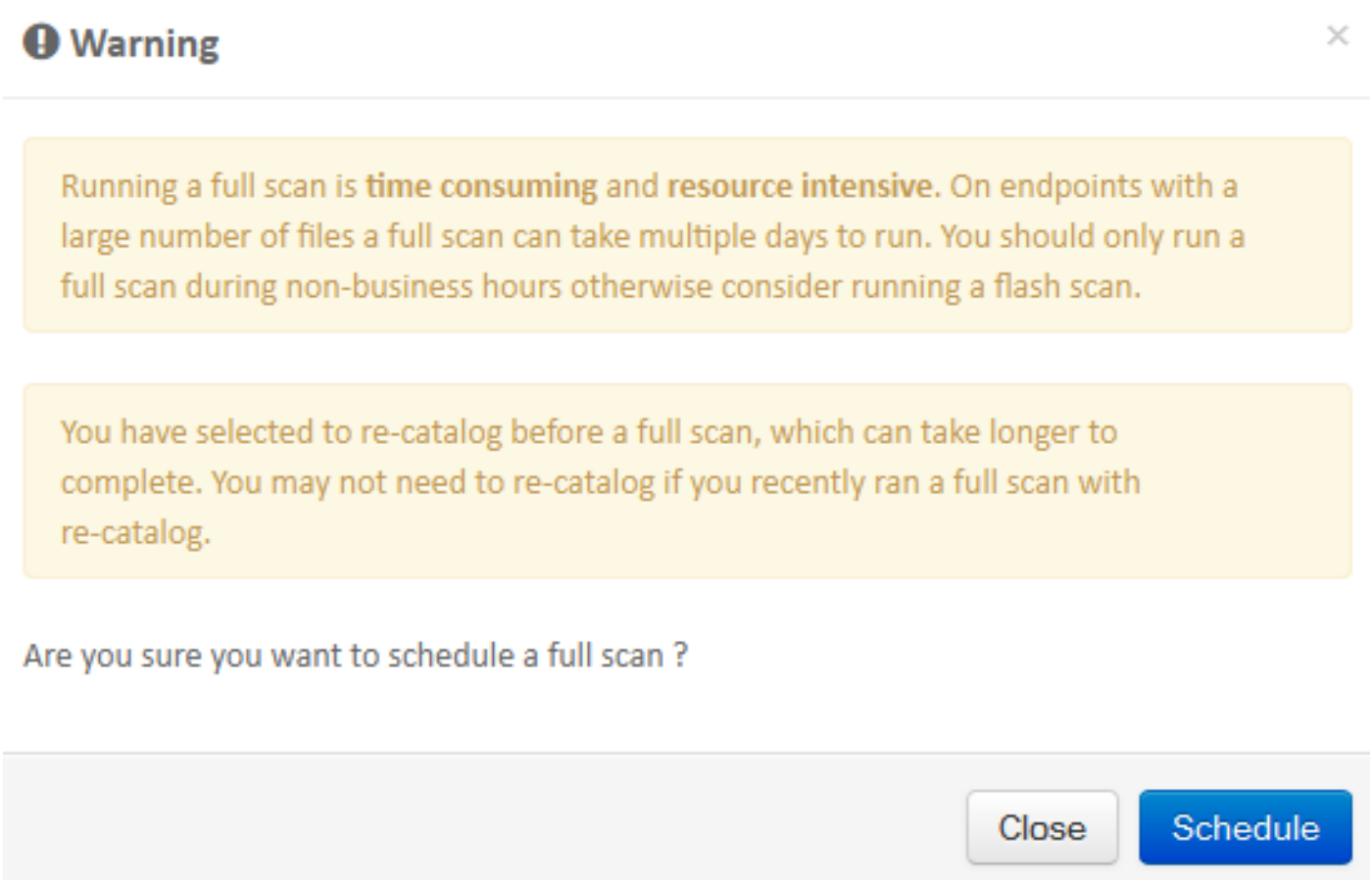
> **注意**：如果这第一次是您运行全双工扫描，您没有要求**在扫描**选项前检查**重新归类**。



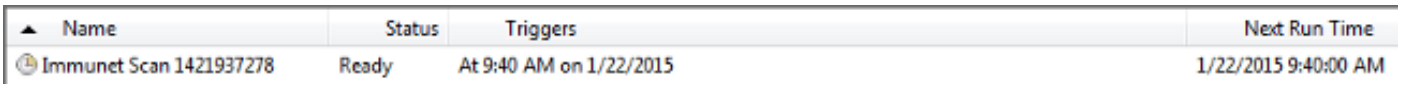
第二种方法是创建从控制板的**爆发控制菜单的**一被安排的终端IOC扫描。在非高峰时间时，当您希望执行扫瞄此选项也许是理想的。您必须提供有在给的计算机的权限为了创建Scheduled Tasks和允许**登录**帐户的凭证，**因为批**组策略权限。



当您安排一终端IOC扫描时，此警告消息出现：

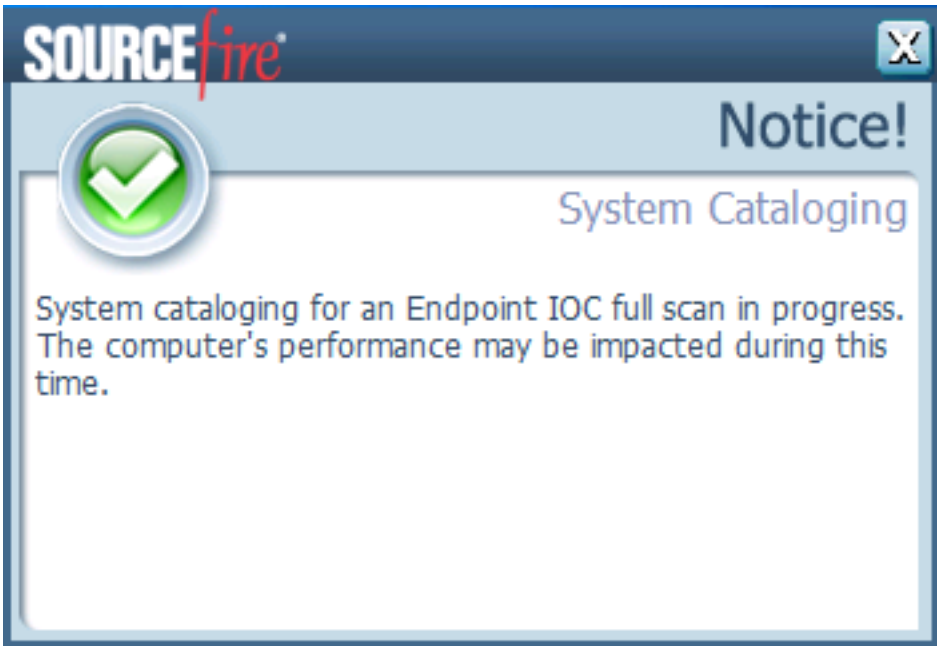


当下次该您的PC发送检测信号，并且，如果您的凭证有效，您应该看到工作类似于此在Windows任务安排器：



当扫描开始时，此消息出现：

注意：如果GUI配置隐藏，则您看不到**系统编目的**公告。



当扫描完成时，您能查看*终端IOC扫描检测摘要*。此示例显示**test.txt** IOC签名文件的一匹配：