目录

简介

我们总是努力改进和展开我们先进的恶意软件保护(安培)技术的威胁智力。如果您的安培产品没有触发在实时的一警报，您能采取一些行动防止其中任一促进影响到您的环境。本文在那些操作项提供一个指南。

说明

即时动作

如果相信您的安培解决方案没有保护您的从威胁的网络，请立即采取以下行动：

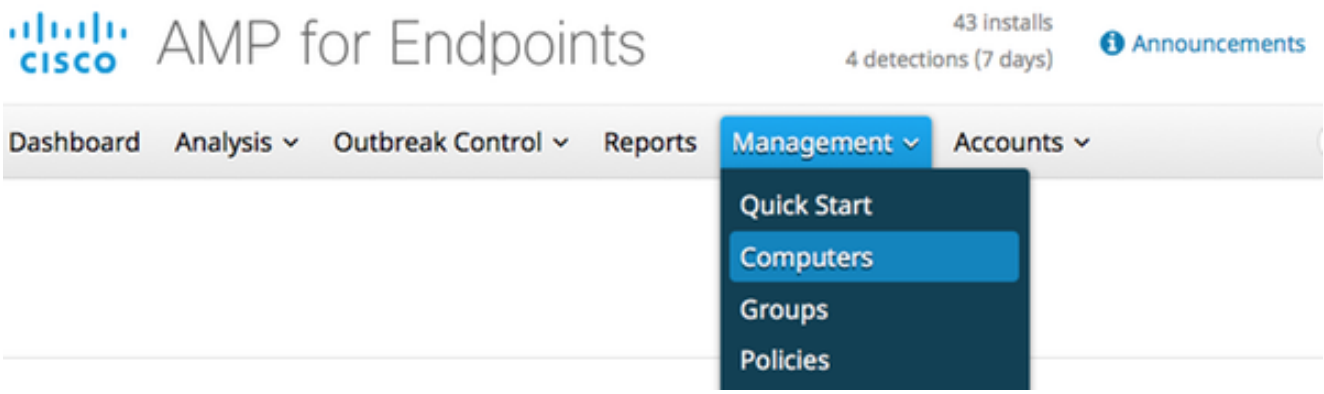
1. 从网络的其余隔离可疑机器。这能包括关闭计算机或者物理的断开它从网络。
2. 写下关于传染，例如，时候，当计算机也许被传染，用户活动在可疑机器等等的重要信息。

   警告： 请勿消除也请勿再镜像计算机。它在法庭调查或故障排除流程中排除查找触犯的软件或文件的机会。

分析

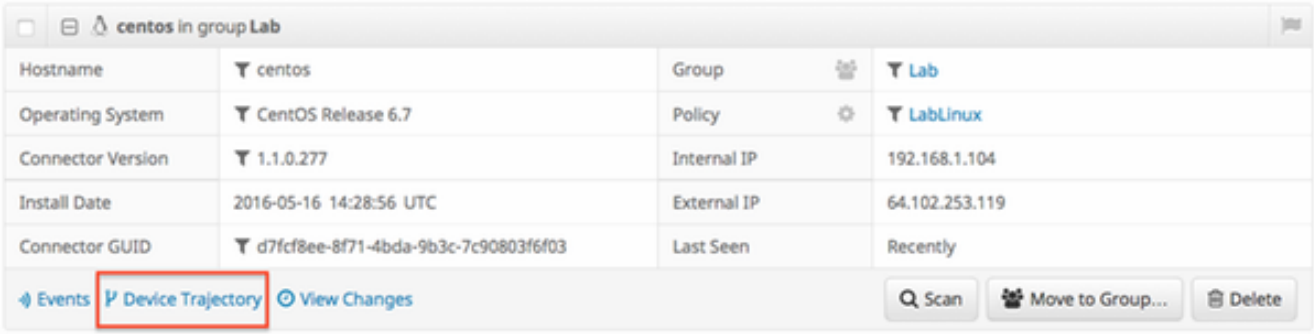
1. 请使用**设备弹道**功能开始您自己的调查。设备弹道能够近似存储9百万个多数最近文件事件。终点设备弹道的安培为搜寻文件是非常有用的或那导致传染的进程。

   在控制板，请导航到**Management>计算机**。



   ??

   查找可疑计算机并且展开该计算机的记录。点击**设备弹道**选项。



??

2. 如果查找任何可疑文件或哈希，请添加它到您的自定义检测列表。终端的安培能使用一自定义检测列表对待文件或切细如有恶意。这是一个巨大方式提供临时的覆盖防止进一步影响。

分析用思科

1. 提交动态分析的所有可疑示例。 您能从**分析>**在控制板的**文件分析**手工提交他们。终端的安培包括生成文件行为报告从威胁网格的动态分析功能。在我们的研究小组的另外的分析要求情况下，这也有提供文件的好处给思科。

2. 如果怀疑在您的网络的任何*错误肯定*或*假攻击*检测，我们建议您利用自定义黑色列表或白色列表功能您的安培产品的。当您与Cisco技术支持中心(TAC)联系时，为分析请提供以下信息：文件的SHA256哈希。文件的若可能复制。关于文件的信息例如来自的地方，并且为什么需要在环境。解释您为什么认为此是错误肯定或假攻击。
3. 如果需要援助缓和专门化创建行动方案您的环境的威胁或执行的会审，您将需要从事思科紧急响应团队(CSIRT)，研究受感染的机器和利用先进的工具或功能的解决爆发。
   注意：Cisco技术支持中心(TAC)不提供援助此种订婚。CSIRT团队可以通过呼叫此电话号码enagaged ：+1-844-831-7715. 他们提供关于他们的服务的其他信息，并且开您的事件的一个Case。进一步进行您的Cisco Account管理器，以便他们在进程能提供另外的指导。

相关条款

- FireAMPWindows
- FireAMP