[外部] — 使用高级恶意软件防护(AMP)进行误检、病毒爆发和事件响应

目录

[简介](#)

[描述](#)

- [即时动作](#)
- [分析](#)
- [思科分析](#)

[相关文章](#)

简介

我们始终致力于改进和扩展高级恶意软件防护(AMP)技术的威胁情报，但是，如果您的AMP解决方案没有触发警报或错误触发警报，您可以采取一些措施防止对您的环境造成任何进一步的影响。本文档对这些措施项提供了指南。

描述

即时动作

如果您认为您的AMP解决方案无法保护您的网络免受威胁，请立即采取以下措施：

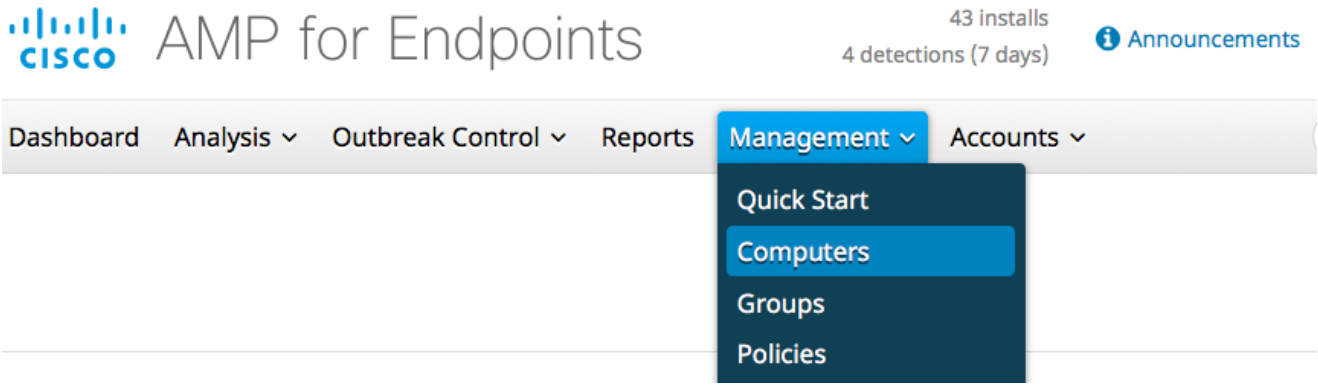
1. 将可疑计算机与网络的其余部分隔离。这可能包括关闭计算机，或者从物理上断开计算机与网络的连接。
2. 写下感染的重要信息，例如计算机受到感染的时间，可疑计算机上的用户活动等。

警告：不要擦除或重新映像计算机。它可避免在取证调查或故障排除过程中发现恶意软件或文件的机会。

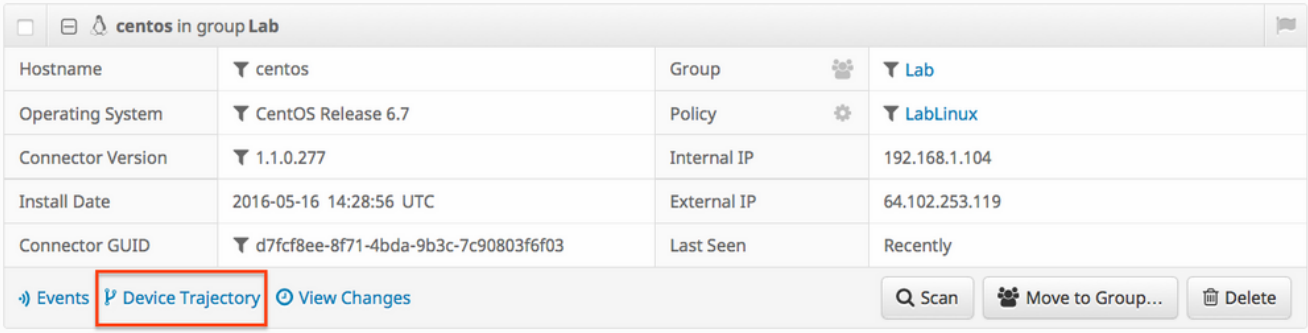
分析

1. 使用设备轨迹功能开始您自己的调查。设备轨迹能够存储大约900万个最新的文件事件。面向终端的AMP设备轨迹对于跟踪导致感染的文件或进程非常有用。

   在控制面板中，导航到管理>计算机。



找到可疑的计算机，并展开该计算机的记录。单击Device Trajectory选项。



2. 如果发现任何可疑文件或散列，请将其添加到自定义检测列表。面向终端的AMP可以使用自定义检测列表将文件或散列视为恶意文件。这是提供停止间隔覆盖以防止进一步影响的好方法。

思科分析

1. 提交任何可疑示例以进行动态分析。您可以从控制面板中的分析>文件分析中手动提交这些示例。面向终端的AMP包含动态分析功能，可生成来自Threat Grid的文件行为报告。如果我们的研究团队需要进行其他分析，这样做还有好处可将该文件提供给思科。

2. 如果您怀疑您的网络中存在误报或误报检测，我们建议您对AMP产品使用自定义黑名单或白名单功能。当您联系思科技术支持中心(TAC)时，请提供以下信息以供分析：

   - 文件的SHA256散列。
   - 如果可能，提供文件的副本。
   - 有关文件的信息，例如文件来自何处以及为何需要将其置于环境中。
   - 解释为什么您认为此错误是正面还是负面。

3. 如果您需要缓解威胁或执行环境分类方面的帮助，您需要与思科Talos事件响应(CTIR)团队接洽，该团队专门制定行动计划、研究受感染的计算机并利用高级工具或功能来缓解活动病毒爆发。

注意：思科技术支持中心(TAC)不提供此类活动的协助。

此处可联系CTIR。这是一项收费服务，起价为60,000美元，除非您的组织有思科的突发事件

响应服务预付款。参与后，他们将提供有关其服务的其他信息，并为您的事件创建案例。我们还建议跟进您的思科客户经理，以便他们能够提供有关此流程的其他指导。

相关文章

- 从Windows上运行的FireAMP连接器收集诊断数据
- FireAMP连接器扫描的文件类型

关于此翻译
思科采用人工翻译与机器翻译相结合的方式将此文档翻译成不同语言，希望全球的用户都能通过各自的语言得到支持性的内容。

请注意：即使是最好的机器翻译，其准确度也不及专业翻译人员的水平。

Cisco Systems, Inc. 对于翻译的准确性不承担任何责任，并建议您总是参考英文原始文档（已提供链接）。

关于此翻译
思科采用人工翻译与机器翻译相结合的方式将此文档翻译成不同语言，希望全球的用户都能通过各自的语言得到支持性的内容。

请注意：即使是最好的机器翻译，其准确度也不及专业翻译人员的水平。

Cisco Systems, Inc. 对于翻译的准确性不承担任何责任，并建议您总是参考英文原始文档（已提供链接）。