Содержание

Введение

Мы всегда стремимся улучшить и развернуть интеллект угрозы для нашей технологии Усовершенствованной вредоносной защиты (AMP). Если ваш продукт AMP не инициировал предупреждение в реальное время, можно принять некоторые меры для предотвращения дальнейшего влияния к среде. Этот документ предоставляет рекомендацию по тем вопросам для принятия решения.

Описание

Немедленные действия

Если вы полагаете, что ваше решение для AMP не защищало вашу сеть от угрозы, примите следующие меры сразу:

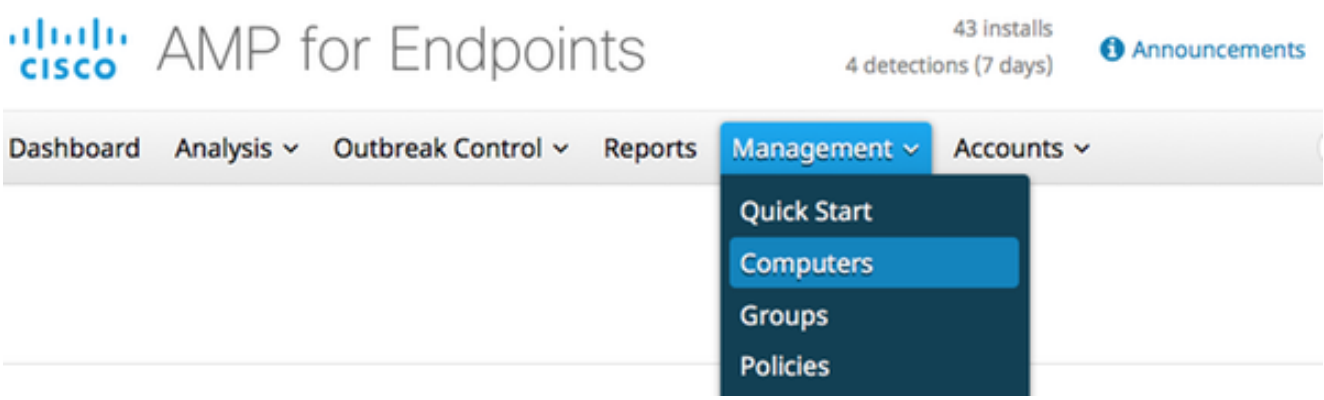
1. Изолируйте подозрительные машины от остатка сети. Это могло включать выключение машины или разъединение его от сети физически.
2. Запишите важную информацию о заражении, такой как, время, когда машина могла бы быть заражена, пользовательские действия на подозрительных машинах, и т.д.

   % Warning: Не вытирайте или повторно захватывайте образ машину. Это устраняет возможности обнаружения незаконного программного обеспечения или файлов во время судебного расследования или процесса устранения проблем.

Анализ

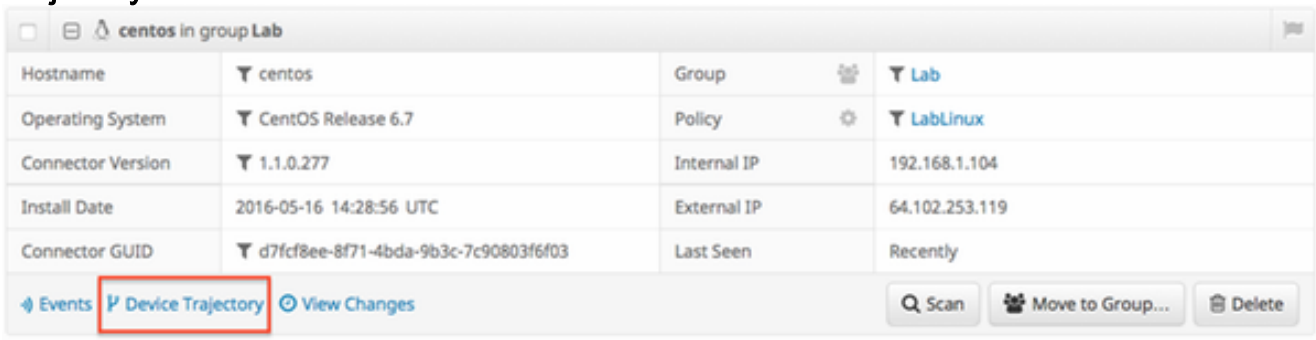
1. Используйте функцию **Траектории Устройства** для начинания собственного расследования. Траектория устройства способна к хранению приблизительно 9 миллионов новых событий файла. AMP для траектории устройства Оконечных точек очень полезен для разыскивания файлов или процессов, которые привели к заражению.

   В информационной панели перейдите к **менеджменту> Компьютеры**.



?

Найдите подозрительную машину и разверните запись для той машины. Щелкните по опции **Device Trajectory**.



?

2. При обнаружении какого-либо подозрительного файла или хэша добавьте его к пользовательским спискам обнаружения. AMP для Оконечных точек может использовать пользовательский список обнаружения для обработки файла или хэша как злонамеренных. Это - отличный способ предоставить временную страховую защиту для предотвращения дальнейшего влияния.

Анализ Cisco

1. Отправьте любые подозрительные выборки для динамического анализа. Можно вручную отправить их от **Анализа> Анализ Файла** в информационной панели. AMP для Оконечных точек включает функциональность динамического анализа, которая генерирует отчёт поведения файла от Сетки Угрозы. Это также обладает преимуществом обеспечения файла к Cisco, если требуется дополнительный анализ нашей исследовательской группой.

2. Если вы подозреваете какой-либо *ошибочный допуск* или обнаружения *ложного отрицательного* в вашей сети, мы советуем усилить пользовательский черный список или функциональность белого списка для продуктов AMP. При контакте с Центром технической поддержки Cisco (TAC) предоставьте следующую информацию для анализа:Хэш SHA256 файла.Копия файла, если это возможно.Информация о файле такой как, куда это прибыло из и почему это должно быть в среде.Объясните, почему делают вы полагаете, что это ошибочный допуск или ложный отрицательный.
3. При необходимости в помощи, смягчающей угрозу или выполняющей медицинскую сортировку среды необходимо будет нанять Команду Экстренного ответа Cisco

(CSIRT), кто специализируется на создании планов действий, исследовании компьютеров пораженный вирусом и усилении усовершенствованных программных средств или функций для решения вспышки.
Примечание: Центр технической поддержки Cisco (TAC) не предоставляет помощи с этим типом обязательства.Команда CSIRT может быть enagaged путем вызова этого номера телефона: +1-844-831-7715. Они предоставляют дополнительные сведения о своих сервисах и открывают случай для вашего инцидента. Добейтесь своего Cisco Account Manager так, чтобы они могли предоставить дополнительное разъяснение на процессе.

Похожие статьи

- Набор диагностических данных от разъёма FireAMP, работающего на Windows
- Типы файла, Которые Просмотрены Разъёмом FireAMP