[External] - Working with Advanced Malware Protection (AMP) False Detections, Outbreaks, and Incident Response

Contents

Introduction

We always strive to improve and expand the threat intelligence for our Advanced Malware Protection (AMP) technology, however if your AMP solution did not trigger an alert or triggered an alert erroneously, you can take some actions to prevent any further impact to your environment. This document provides a guideline on those action items.

Description

Immediate Actions

If you believe that your AMP solution did not protect your network from a threat, take the following actions immediately:

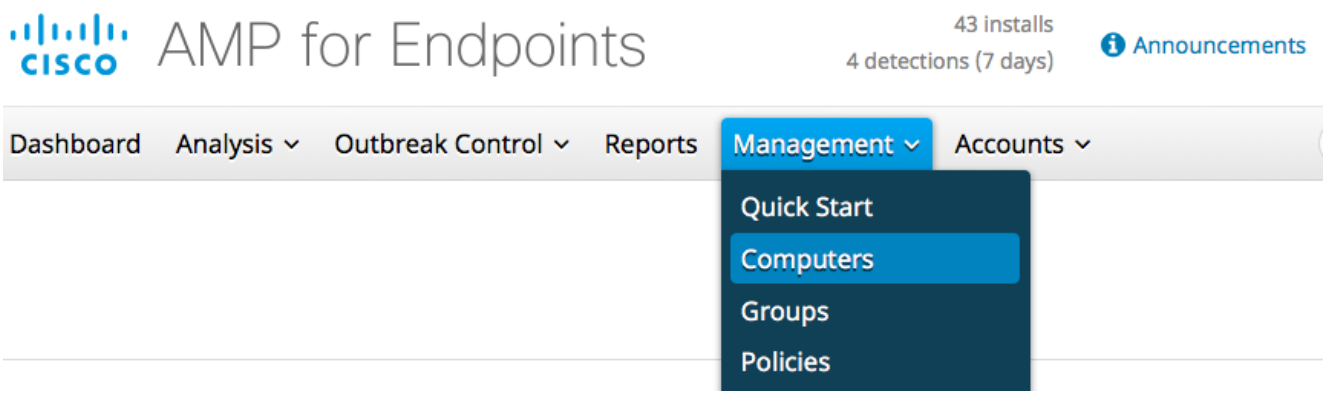
1. Isolate the suspicious machines from the rest of the network. This could include turning the machine off, or disconnecting it from the network physically.
2. Write down the important information about the infection, such as, the time when the machine might be infected, the user activities on the suspicious machines, etc.

Warning: Do not wipe out or reimage the machine. It eliminates the chances of finding the offending software or files during forensic investigation or troubleshooting process.

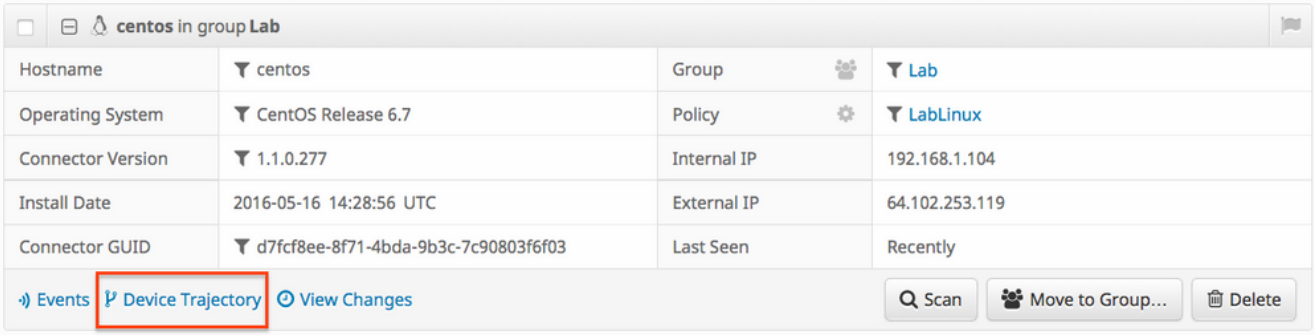
Analysis

1. Use the **Device Trajectory** feature to begin your own investigation. Device Trajectory is capable of storing approximately the 9 million most recent file events. The AMP for Endpoints device trajectory is very useful for tracking down files or processes that led to an infection.

   In the dashboard, navigate to **Management > Computers**.



Find the suspicious machine and expand the record for that machine. Click on **Device Trajectory**
option.



2. If you find any suspicious file or hash, add it to your custom detection lists. AMP for Endpoints can use a custom detection list to treat a file or hash as malicious. This is a great way to provide stop-gap coverage to prevent further impact.

Analysis by Cisco

1. Submit any suspicious samples for dynamic analysis. You can manually submit them from **Analysis > File Analysis** in the dashboard. AMP for Endpoints includes dynamic analysis functionality that generates a report of the behavior of the file from Threat Grid. This also has the benefit of providing the file to Cisco in the event that additional analysis by our research team is required.

2. If you suspect any *false positive* or *false negative* detections in your network, we advise that you leverage custom black list or white list functionality for your AMP products. When you contact Cisco Technical Assistance Center (TAC), provide the following information for analysis:The SHA256 hash of the file.A copy of the file if possible.Information about the file such as where it came from and why it needs to be in the environment.Explain why do you believe this to be a false positive or false negative.
3. If you need assistance mitigating a threat or performing triage of your environment, you will need to engage the Cisco Talos Incident Response (CTIR) team who specialize in creating action plans, researching infected machines, and leveraging advanced tools or features to mitigate an active outbreak.
   Note: The Cisco Technical Assistance Center (TAC) does not provide assistance with this type of engagement.CTIR can be contacted here. This is a paid service starting at $60,000 unless your organization has a retainer for incident response services from Cisco. Once engaged they will provide additional information about their services and open a case for

your incident. We also recommend following up with your Cisco account manager so that they can provide additional guidance on the process.

Related Articles

- Collection of Diagnostic Data from a FireAMP Connector Running on Windows
- File Types That are Scanned by FireAMP Connector