Getting to know your Anti-Virus: Cisco AMP

Summary

Cisco Advanced Malware Protection (AMP) is an advanced endpoint protection software which is supported and monitored by a central console. AMP is an application that monitors the machine on which it is installed, searching for suspicious activity. Endpoints with AMP clients installed will report back to IT administrators where they can view events, set up alerts, and get an overview of the volume of suspicious activity occurring on their network. Finally, AMP also provides traditional Anti-Virus scanning through Tetra (Windows) and Clam AV (Mac & Linux).

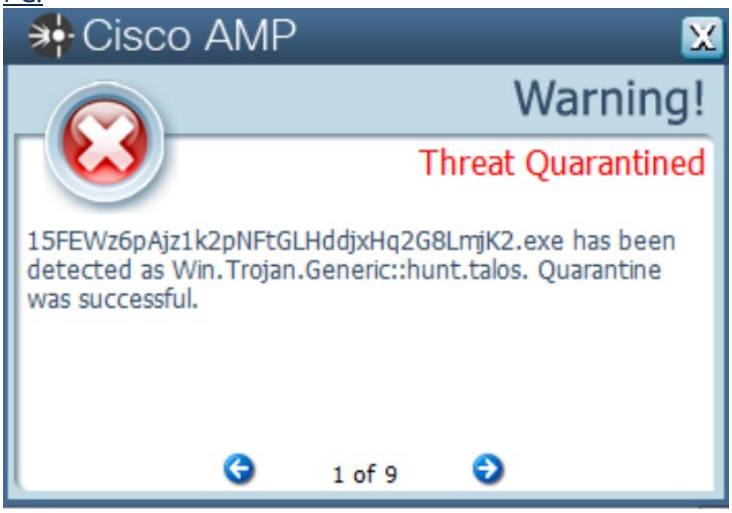
Event Types Monitored:

- Threats (rootkits, malicious activity, suspicious system activity, etc.)
- Indications of compromise (multiple infected files, dropper infection, suspicious download, ransomware, Cloud IOCs, etc.)
- Quarantine status
- Endpoint status
- Miscellaneous events (vulnerable application detected, application installed, application uninstalled)

Why Does It Matter To Me?

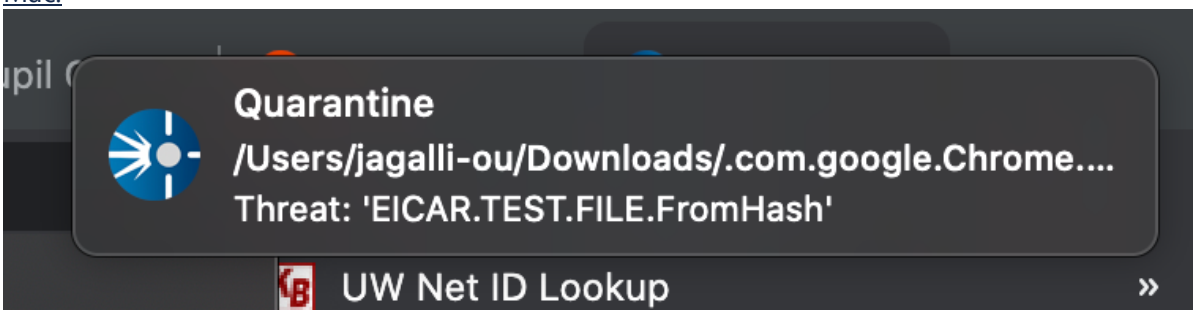
- Cisco AMP will alert you if it finds suspicious activity or a suspicious program and will block that program from being downloaded or used. In this event, it is important to follow up with a scan if the listed program is unknown, or to alert SMPH IT if it is a legitimate program that is being falsely recognized as malicious.
- This is an example of what a block alert will look like on your computer:

PC:



k

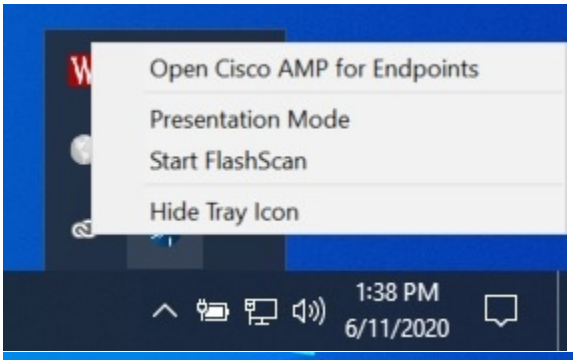
Mac:

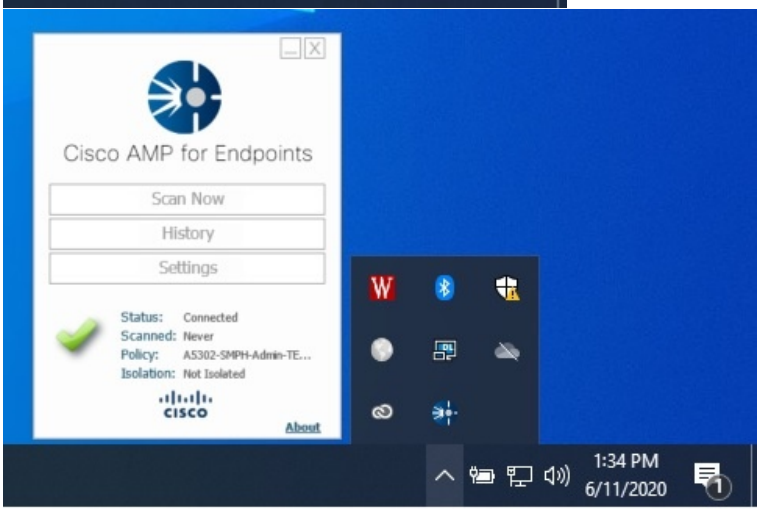


Remediation:

PC:

- Click the chevron symbol in your Windows taskbar and locate the Cisco AMP icon on your taskbar (a blue circle with a white flashlight symbol inside). Click to open AMP for Endpoints. You can perform a Quick Scan under the Scan Now button which takes about 10 minutes.



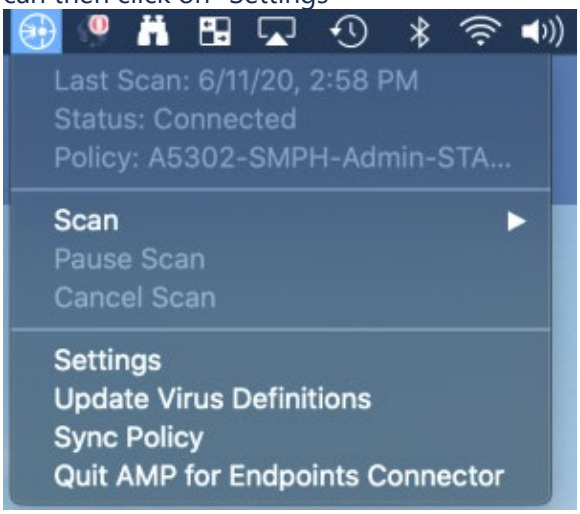


- After the scan is completed, you will see a summary of the scan including: Threats Detected and Threats Removed
- If you have finished a scan and AMP continues to report the same threat, there may be a deeper infection on the computer. You can instead run a Full Scan which scans through the entire file system of the computer and any external data stores.

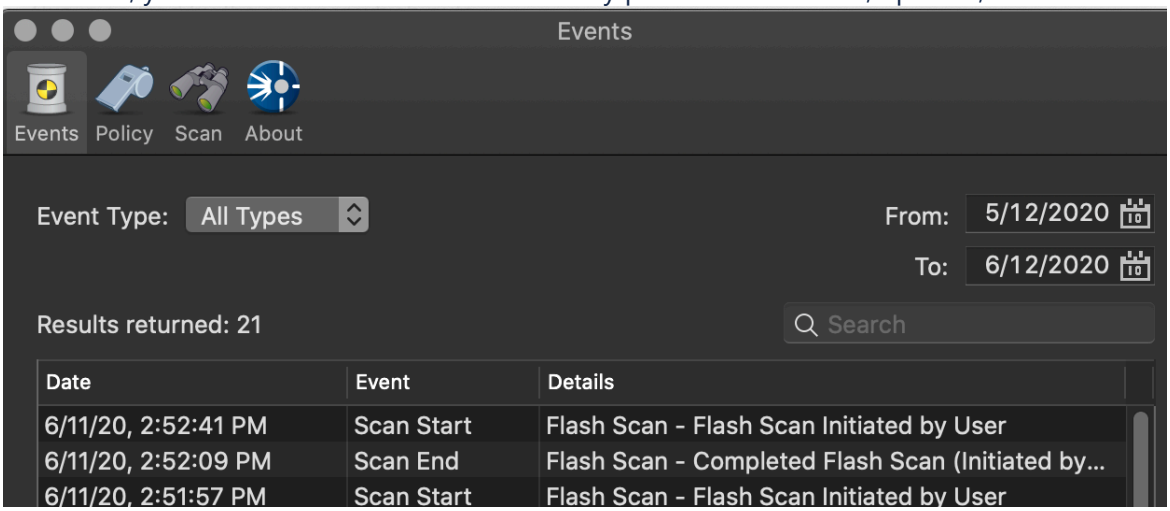
- From there, if you are still being alerted of any sort of peculiar or suspect issues on your PC, please contact SMPH IT support for further followup.

  Mac:

- If you click on the Cisco AMP icon on your taskbar (a white circle with a flashlight symbol inside), you can then click on "Settings"

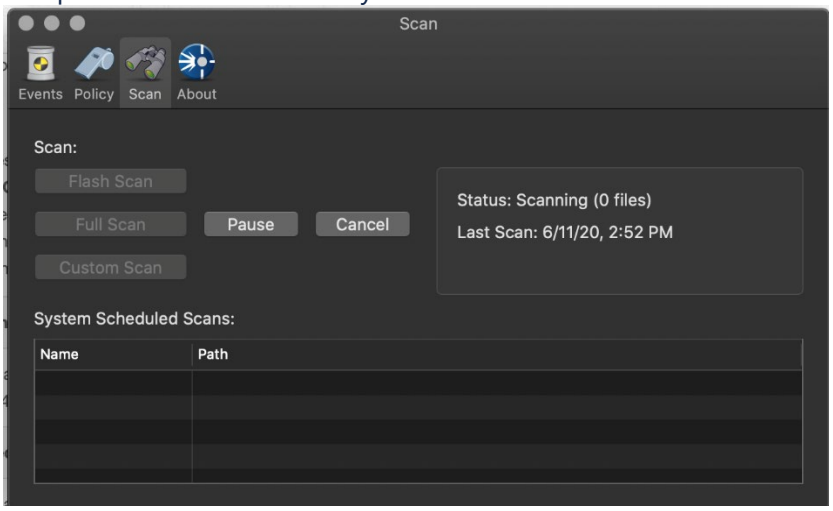


- From here, you should see a window that lists any previous detections, updates, or events



- Click on the icon for "Scan" and then click "Flash Scan". A scan will begin, which on most machines takes between 5 to 15 minutes depending on the number of files. It will tell you the status of the scan in that window. Once it has changed from "Scanning" to "Connected" the scan will have

completed and should list any detections it finds. If it does not find any, the box will remain blank.



- If you receive repeated notifications for the same or similar detection, we recommend performing a full scan from this same menu. This scan takes much longer, but it is capable of picking up threats in locations that the flash scan may have missed.
- Lastly, if either of these methods fails to remediate the issue, please contact SMPH IT for additional follow up.