Detecting recurring malware on a host

Applicability

- Product: Splunk Enterprise or Splunk Cloud
- Feature: Search
- Function: Malware monitoring

To optimize the search shown below, you should specify an index. In addition, this sample search uses Symantec Endpoint Protection data. You can replace this source with any other malware data used in your organization.

Problem

You want to search antivirus logs to find systems on your network that are experiencing multiple infiltrations so that you can mitigate the issue.
Solution

Media, iframe, embed and object tags are not supported inside of a PDF.

Additional resources

For more great content from the Splunk Education and Training team, check out Splunk How-To on YouTube or sign up for a course. In addition, these Splunk resources might help you understand and implement this search:

- Data Descriptor: Antivirus data
- Splunk Add-On: Symantec Endpoint Protection