Detecting TOR traffic

Applicability

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

Problem

The TOR anonymity network is the perfect place to hide command-and-control, exfiltration, or ransomware payment through bitcoin. You would like to use firewall data to find TOR traffic on your network.
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:

- Splunk App: Stream
- Data Descriptor: Firewall data
- Splunk Answers: How to detect TOR traffic