Previously seen command line argument

You might want to create a baseline of the earliest and latest times a command-line argument appeared in your dataset when doing the following:

- Detecting techniques in the Orangeworm attack group
- Monitoring command line interface actions

Prerequisites

Content developed by the Splunk Security Research team requires the use of consistent, normalized data provided by the Common Information Model (CIM). This search requires the Endpoint data model. For information on installing and using the CIM, see the Common Information Model documentation.

Example

New command line processes indicate new programs that might or might not be legitimate. You want to create a lookup file of known processes that you can use to check against new ones found in command line arguments to decide if further investigation is necessary.

To optimize the search shown below, you should specify an index and a time range.

1. Ensure that your deployment is ingesting records process activity from your hosts to populate the Endpoint data model in the Processes node. You must be ingesting logs with both the process name and command line from your endpoints. The complete process name with command-line arguments are mapped to the "process" field in the Endpoint data model.

2. Run the following search:

```splunk
|tstats summariesonly=true allow_old_summaries=true min(_time) AS firstTime max(_time) AS lastTime FROM datamodel=Endpoint.Processes WHERE Processes.process_name=cmd.exe AND Processes.process="* /c *" BY Processes.process |rename "Processes.*" as "***"
```

Search explanation

The table provides an explanation of what each part of this search achieves. You can adjust this query based on the specifics of your environment.
### Splunk Search

```
|tstats summariesonly=true allow_old_summaries=true min(_time) AS firstTime max(_time) AS lastTime FROM datamodel=Endpoint.Processes WHERE Processes.process_name=cmd.exe AND Processes.process="* /c *" BY Processes.process
```

### Explanation

Query the Endpoint.Processes data model object for the process name "cmd.exe" and a process that includes /c, which runs a command. Return the first and last time that each matching command line argument was seen.

### Rename

```
|rename "Processes.*" as "***"
```

Rename the data model object for better readability.

---

**Result**

After you create this baseline, you can look for new command line arguments that might indicate a threat.

For additional information about this search, such as its applicability to common frameworks and standards, see this project on GitHub.