Uncommon top level domains

You might want to be able to extract uncommon top level domains from your data when doing the following:

- Monitoring employee network traffic

Prerequisites

In order to execute this procedure in your environment, the following data, services, or apps are required:

- Splunk Enterprise or Splunk Cloud Platform
- Firewall data
- URL Toolbox

Example

You recently started work as a Security Analyst for a company whose users often access websites that don't use the Latin alphabet. You need to be able to accurately extract all URLs from your data.

To optimize the search shown below, you should specify an index and a time range. In addition, this sample search uses Palo Alto Networks data. You can replace this source with any other firewall data used in your organization.

1. Run the following search:

```
sourcetype=pan:threat | stats count BY url | urlparser field=url listname="mozilla" mode=extended
```

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.

<table>
<thead>
<tr>
<th>Splunk Search</th>
<th>Explanation</th>
</tr>
</thead>
<tbody>
<tr>
<td>sourcetype=pan:threat</td>
<td>Search only threat events from Palo Alto Networks data.</td>
</tr>
</tbody>
</table>
### Splunk Search

| stats count BY url |

**Explanation**

Show the event count for each value in the `url` field.

| urlparser field=url listname="mozilla" mode=extended |

**Explanation**

Use the URLParser app to extract domains from the Mozilla catalog.

These are the default settings for the URLParser. Searching `| urlparser` will yield the same results as specifying the parameters shown here.

---

### Result

The results show the URLs visited by your users, but it doesn't separate the legitimate ones from the suspicious ones. Use your own lookup tables to help sort through the results, or use the analytic functions of the URL Toolbox app, like [Shannon Entropy](#), to find URLs that you need to investigate.