Reconnaissance

User Agents:

Hypothesis:
User Agent Strings may provide insight into an adversary that they may not have intended to show.

Here are some questions to think about that may help as we conduct our hunt:

- What data sources (sourcetypes) are needed to view user agent strings?
- When were specific user agent strings seen?
- What IP addresses where user agent strings seen from?
- Are any of the user agent strings anomalous? That is are there any that are excessively short or long or from systems that would be unexpected?
- Focus your hunt in the month of August 2017

- We can start by searching the stream:http sourcetype, which is our web data captured off the wire, and look for all web traffic where the site referenced is our corporate web site www.froth.ly. We can then use the stats command and generate a count grouped by http_user_agent, the field name for user agent strings, and sort that output by count from largest to smallest.

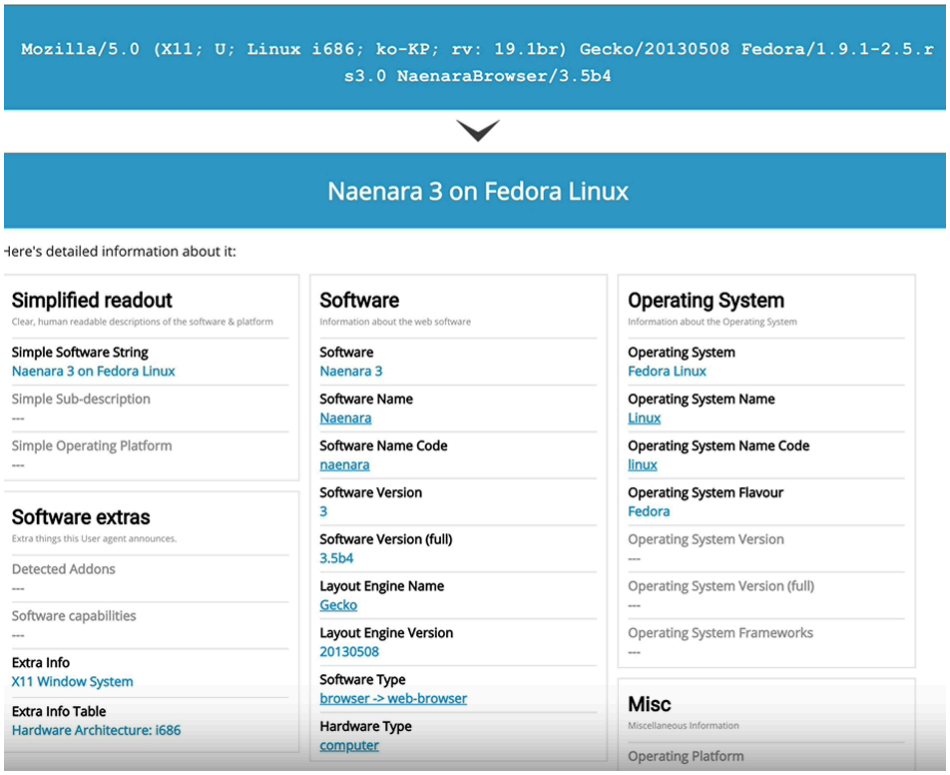
```
index=botsv2 sourcetype=stream:http site=www.froth.ly
| stats count by http_user_agent
| sort - count
```

- After inspecting the results, we can find one result that seems foreign or unknown to us.

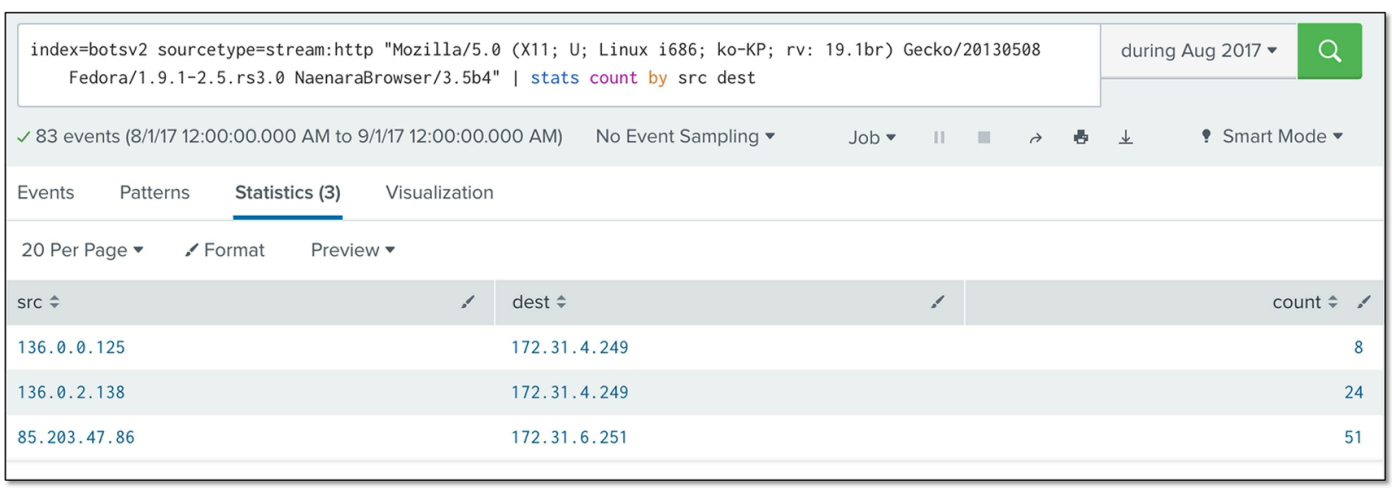
```
Mozilla/5.0 (X11; U; Linux i686; ko-KP; rv: 19.1br) Gecko/20130508 Fedora/1.9.1-2.5.rs3.0 NaenaraBrowser/3.5b4
```

- Upon further invegtigating about the User Agent, we find some non-Western European characters, a code of ko-KP and a browser we are not familiar with.

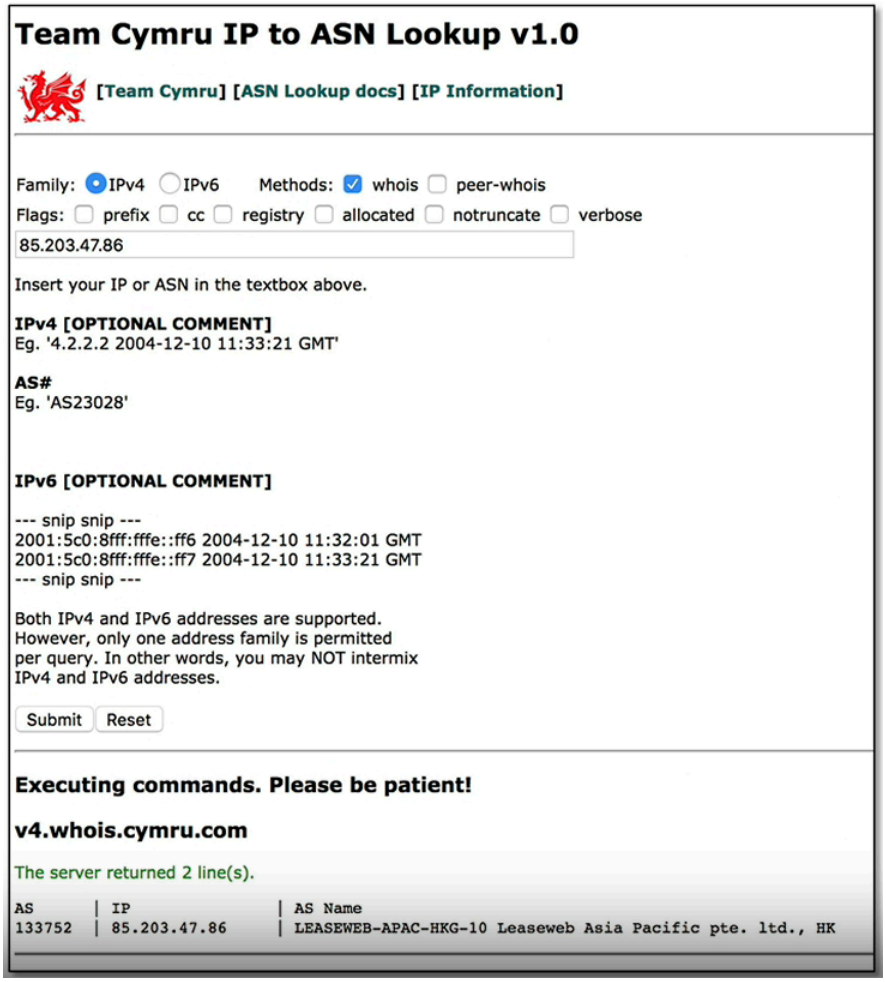
- If we search some of these less familiar values in the user agent string, we can find out that ko-KP is the browser language code for North Korea and when we search for NaenaraBrowser, we can see that it is a North Korean web browser.



- Now that we have identified a suspicious user agent, we can use the stats command and look for source and destination pairs that are referencing this string. We see three external IPs using this user agent string targeting two distinct systems at Frothly.



- Upon researching the Asset Center, we can confirm that 172.31.4.249 is a DNS server called *'gacrux'.*
- Using OSINT tools to dig deeper, we find that this server is hosted using RIPE.NET which is a European Coordination Center for handing out IP addresses. Now using Cymru, we can find the ASN connected with RIPE.NET.



What Have we Learned?

1. User Agent String of North Korean origin visited www.froth.ly
    - Mozilla/5.0 (X11; U; Linux i686; ko-KP; rv: 19.1br) Gecko/20130508 Fedora/1.9.1-2.5.rs3.0 NaenaraBrowser/3.5b4
2. IP address of browser : 85.203.47.86
3. ASN : 133752
4. Visitor used Express VPN in HongKong to connect www.froth.ly.
5. Two additional IP addresses used the same user agent to connect to the site.
   136.0.0.125 and 136.0.2.138

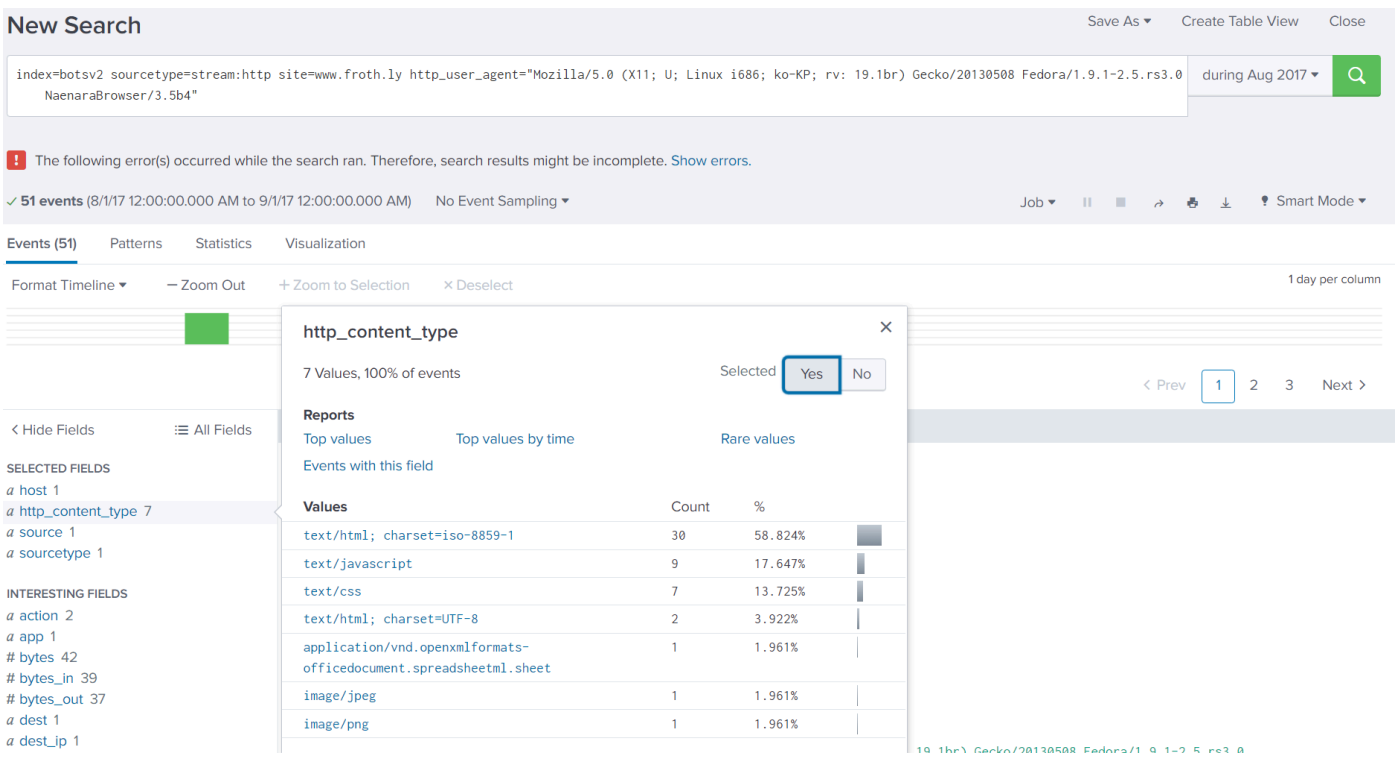
Public Web Visibility

Hypothesis:
PRE- Search Open Websites/Domains
Can we identify Publicly available company information that an adversary may be accessing

Here are some questions to think about that may help as we conduct our hunt:

- From an adversary perspective, where can we find information about our target?
- Did specific user agent strings access company content?
  Mozilla/5.0 (X11; U; Linux i686; ko-KP; rv: 19.1br) Gecko/20130508 Fedora/1.9.1-2.5.rs3.0 NaenaraBrowser/3.5b4
- What IP addresses accessed company content?
- What kinds of company information is available from our website and other places to understand more about us?

- If we start to explore our http data, we can pivot to any number of interesting fields that were extracted at search time. One of those fields is http_content_type. This field is used to indicate the mime type in the event.



- We can see that, one of the MIME types is a office document. Spreadsheet. Upon clicking that, we can see that company_contacts.xlsx file has been downloaded on August 5th

```
timestamp: 2017-08-05T08:15:48.785770Z
transport: tcp
uri_path: /files/company_contacts.xlsx
```

What Have we Learned?

1. company_contacts.xlsx was downloaded.
2. It was downloaded on 8/5/17 1:15:49.707 AM.