LEVITATION and the FFU Hypothesis
What is LEVITATION?

- A behaviour-based target discovery project
- Multi-disciplinary team
- Prototyping and delivering advances in:
  - Behavioural tradecraft
  - Hypothesis tradecraft
  - Tradecraft automation
Current Hypotheses

Active
- FFU
- Sequential numbers
- Obvious selector names
- Web search terms

In Development
- GPS waypoints
- Devices close to places
- Telephony gaps
- Targets of foreign SIGINT agencies
- Missed calls
FFU Hypothesis

Extremists use Free File Upload (FFU) sites differently than the general public.

Al-Qaida uses FFU sites to distribute Jihadist propaganda

Extremists use FFU sites to distribute training materials
What do we need?

A list of suspect documents
A list of FFU URLs referring to those documents
A list of IPs downloading those URLs

New documents are found by CWOC (CSEC Web Operations Centre) retrieval from URLs, so that’s the easy part.
New URLs

CSEC's web forums team
2nd Party reports & alerts
Machine Learning
  Learning the textual context for the URLs in web forums
HTTP Referrers
  Follow URL referrers back to the originating site

Previous Correlations analysis
Using tech techniques to figure out what else that user was up to at the same time
  e.g. Google analytics cookies
FFU Events Collection

ATOMIC BANJO (Special Source) is collecting HTTP metadata for 102 known FFU sites.

We see about 10-15 million FFU events per day
All the FFU Events are available thru OLYMPIA
Looking for a few good documents

We only care about the 2,200 URLs that point to documents of interest.

E.g. How to make a gas bomb

www.sendspace.com/file/

Every day we sort through the 10–15M events for the interesting ones.

We’re finding about 350 interesting download events per month.
Documents vary

Chloroform in a Lowes bucket

Bajadin Explosives Manual

And lots of pictures of cars on fire
Filtering out Glee Episodes
Resulting events
Start analysis with event info

FFU hit from selector [REDACTED] on 7/03/2012 7:46:51 geolocated to Kenya, accessing The Explosives Course through FFU site sendspace.com with HTTP user agent Mozilla/5.0 (Ubuntu; X11; Linux x86_64; rv:9.0.1) Gecko/20100101 Firefox/9.0.1
Correlating other selectors with the IP

FFU hit from selector [REDACTED] on 7/03/2012 7:46:51 geolocated to Kenya, accessing The Explosives Course through FFU site sendspace.com with HTTP user agent Mozilla/5.0 (Ubuntu; X11; Linux x86_64; rv:9.0.1) Gecko/20100101 Firefox/9.0.1

Can we correlate any other selectors with this IP address?

Mutant Broth query on IP [REDACTED] for 5 hours on either side of 7/03/2012 7:46:51

682 events including 77 with an exact match of the user agent above yielding a Facebook ID [REDACTED], a Google Prefid Cookie [REDACTED], an M_AdNxs Uuid2 Cookie [REDACTED], an M_Quantserve Mc Cookie [REDACTED], and a Google Prefid Cookie [REDACTED]

Correlating Facebook cookie

FFU hit from selector [redacted] on 7/03/2012 7:46:51 geolocated to Kenya, accessing The Explosives Course through FFU site sendspace.com with HTTP user agent Mozilla/5.0 (Ubuntu; X11; Linux x86_64; rv:9.0.1) Gecko/20100101 Firefox/9.0.1

Open Source research indicates that the user of Facebook ID [redacted] is based in Dubai, United Arab Emirates.

Marina Profile Query on Facebook User Cookie [redacted] observed in Mutant Broth Query above

Lots of events including registration email address [redacted]@gmail.com and Facebook name [redacted].

Mutant Broth Sub-Query on Facebook User Cookie [redacted] observed in Mutant Broth Query above

946 events with 893 matching exactly the user agent above

Can we correlate any other selectors with this Facebook ID Cookie?
IP Correlation
Automated analysis documentation

Analytic Process for FFU Hypothesis Hits

FFU hit from selector [REDACTED] on 201201200008480000GMT geolocated to SA, accessing Inexhaustible weapons part 2 through FFU site GET /download/sela7_la_yndb_02/part24.mp4 HTTP/1.1 with HTTP user agent Mozilla/5.0 (SymbianOS/9.3; U; Series60/3.2 NokiaN79-1/11.049; Profile/MIDP-2.1 Configuration/CLDC-1.1 ) AppleWebKit/413 (KHTML, like Gecko) Safari/413

? Can we correlate any other selectors with this IP address?

Mutant Broth query on IP [REDACTED] for 5 hours on either side of 201201200008480000GMT

(MUTANTBROTH_EVENT_COUNT) events with only (MUTANTBROTH_MATCHING_EVENT_COUNT) matching exactly the us agent above.

Marina Activity query on IP [REDACTED] for 5 hours on either side of 201201200008480000GMT

(MARINA_ACTIVITY_EVENT_COUNT) events with possible correlation (MARINA_ACTIVITY_POSSIBLE_CORRELATIONS)
What happens then?

Compare control and experimental groups to show statistical differences

Analyze experimental group to determine statistical power of the hypothesis

Assemble selectors across all hypotheses

Rank selectors according to the number and power of the hypothesis behaviors they show

Deliver an ordered list of suspects to OCT
# Scoreboard

<table>
<thead>
<tr>
<th>Personae</th>
<th>FFU</th>
<th>0.6</th>
<th>0.55</th>
<th>0.52</th>
<th>0.48</th>
<th>Totals</th>
</tr>
</thead>
<tbody>
<tr>
<td>P1</td>
<td>4</td>
<td>2</td>
<td>0</td>
<td>4</td>
<td></td>
<td>5.42</td>
</tr>
<tr>
<td>P2</td>
<td>4</td>
<td>4</td>
<td>0</td>
<td>1</td>
<td></td>
<td>5.08</td>
</tr>
<tr>
<td>P3</td>
<td>4</td>
<td>1</td>
<td>0</td>
<td>4</td>
<td></td>
<td>4.87</td>
</tr>
<tr>
<td>P4</td>
<td>3</td>
<td>4</td>
<td>4</td>
<td>0</td>
<td></td>
<td>3.14</td>
</tr>
</tbody>
</table>

## Hypotheses

<table>
<thead>
<tr>
<th>Weights</th>
<th>FFU</th>
<th>0.6</th>
<th>0.55</th>
<th>0.52</th>
<th>0.48</th>
<th>Totals</th>
</tr>
</thead>
<tbody>
<tr>
<td>0.6</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>0.55</td>
<td>2</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>0.52</td>
<td>1</td>
<td></td>
<td></td>
<td>4</td>
<td></td>
<td>4.87</td>
</tr>
<tr>
<td>0.48</td>
<td>0</td>
<td>4</td>
<td></td>
<td></td>
<td></td>
<td>4.87</td>
</tr>
</tbody>
</table>

**Known** | **New**

TOP SECRET//SI//REL CAN, AUS, GBR, NZL, USA
Successes

An HTTP-referred URL gave us a German hostage video from a previously unknown target.

An FFU upload event gave us an AQIM’s hostage strategy. The resulting report was disseminated widely including by the CIA to their counterparts overseas.
The End

Team Lead: @cse-cst.gc.ca

Tech Lead: @cse-cst.gc.ca

Me: @cse-cst.gc.ca