GOVCERT.lu

Weber Jean-Paul

FIRST/TF-CSIRT 25-27 January 2016

TLP: GREEN

- Searching for the best methodology/practices
- Reached a blocking point

- Why not ask here?
  - Skills
  - Experience

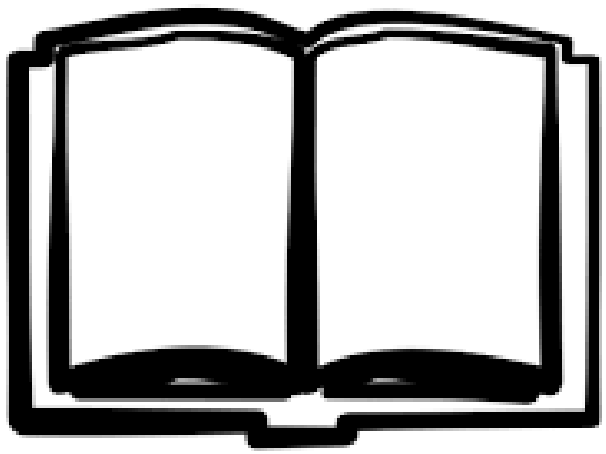
If questions or suggestions ask at any time

- Threat awareness
- Understanding of the threat
- Faster reaction times
- ...

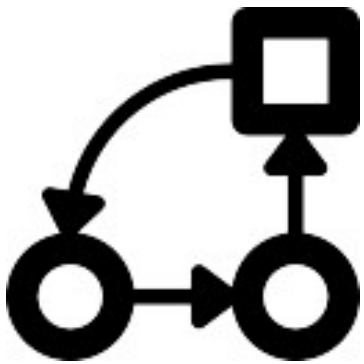
- Targeted audience
- Terminology
- Groupings
- Work-flow

- Consumer
  - IOC based
  - Mitigation Strategies
- Incident Responder (extends Consumer)
  - Capabilities
  - Technical insights
- Analyst (extends Incident Responder)
  - Correlation
  - Prevention

- Incident
  - Internal details
  - Event trace
- Threat
  - Malicious activity
  - Technical insights
- IOCs
  - Domains
  - IPs
  - etc
- Context?



- Domain
  - IP/IPs
  - Whois



- Problems/ideas
  - Representation
  - Store/Share
  - Groupings/Links

GOVCERT.lu | CERT gouvernemental Luxembourg

Flat

Hash: 19dc4.....

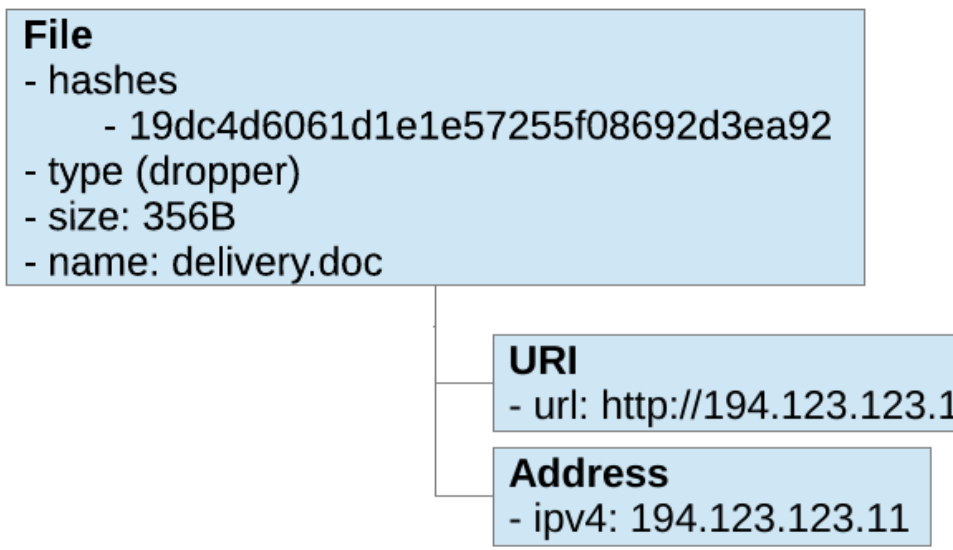
size: 356B

name: delivery.doc

IP: 192.123.123.11

url: http://194.123.123.11/f.zip

Grouped



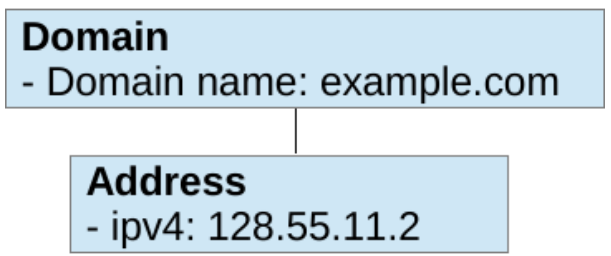
GOVCERT.lu | CERT gouvernemental Luxembourg

Flat

Domain: example.com

IP: 192.123.123.11

Grouped

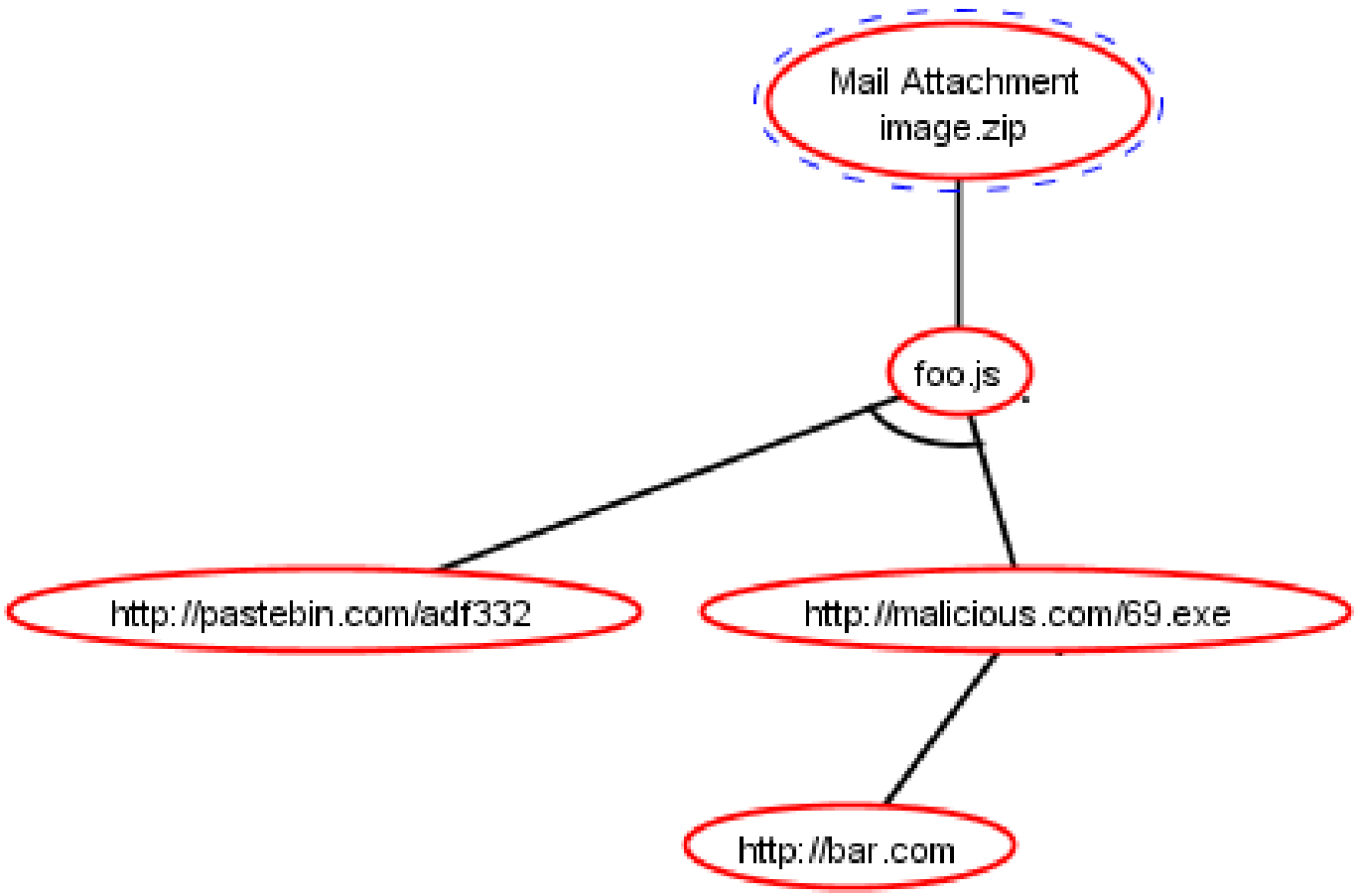


- Report
  - Details
  - IOCs
    - Drawback: Takes time
- Sandbox
  - Fast
    - Drawback: May contain FPs
- Graphs (idea)
  - Easy to Understand
  - Can be flattened
    - Drawback: Hard to create

Flat

FileName:	image.zip
FileName:	foo.js
FileName:	69.exe
Domain:	malicious.com
Domain:	pastebin.com
url:	http://malicious.com/69.exe
url:	http://pastebin.com/adf332
url:	http://bar.com/
IP:	192.123.123.11

Structured


Mail Attachment
image.zip
foo.js
http://pastebin.com/adf332
http://malicious.com/69.exe
http://bar.com

What do you think?
First step

Approach?

- Groupings
- Graph
  - ADTrees?
    - IOCs
    - CoA

Any one had similar ideas

Thank You
Thank you for your attendance

Any comments or Questions?