Introduction
Not a normal presentation

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

- Why not ask here?
  - Skills
  - Experience

If questions or suggestions ask at any time

TLP: GREEN
J. Weber
Introduction

Benefits

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

TLP: GREEN
Introduction

Issues

- Targeted audience
- Terminology
- Groupings
- Work-flow
Audience
Main requirements

- Consumer
  - IOC based
  - Mitigation Strategies

- Incident Responder (extends Consumer)
  - Capabilities
  - Technical insights

- Analyst (extends Incident Responder)
  - Correlation
  - Prevention
Terminology
Terms/Connotations

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

TLP: GREEN
Issues
First step - Enhancing Data

- Domain
  - IP/IPs
  - Whois

- Problems/ideas
  - Representation
  - Store/Share
  - Groupings/Links
Structures
First step - Example ideas

Flat
Hash: 19dc4......
size: 356B
name: delivery.doc
IP: 192.123.123.11
url: http://194.123.123.11/f.zip

Grouped

File
- hashes
  - 19dc4d6061d1e1e57255f08692d3ea92
- type (dropper)
- size: 356B
- name: delivery.doc

URI
- url: http://194.123.123.11/f.zip

Address
- ipv4: 194.123.123.11
Structures
First step - Example ideas

**Flat**
- Domain: example.com
- IP: 192.123.123.11

**Grouped**
- Domain name: example.com
  - Address: ipv4: 128.55.11.2
Fork-flow - Report vs Sandbox vs Graphs

- Report
  - Details
  - IOCs
    - Drawback: Takes time

- Sandbox
  - Fast
    - Drawback: May contain FPs

- Graphs (idea)
  - Easy to Understand
  - Can be flattened
    - Drawback: Hard to create

TLP: GREEN
J. Weber
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
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?