POORTEGO

Mike Geide

Zscaler, Inc.

Session ID: BR-303

Session Classification: Intermediate

RSACONFERENCE
EUROPE 2012

Threat Intelligence for the 99%

https://github.com/mgeide/poortego

Disclaimer

- The project is in its infancy
- Presentation contains demos
  - Demos like to FAIL
- Presentation mentions vendors
  - Not intended to plug or knock
- Hollywood imagery used for your attention
  - No Hollywood stars have actually endorsed this project
- No kittens were harmed in the making of this…

Whois

I am a dataholic –

and it's not just enough to have the data…

I want to organize it, understand it, and act on it!

Whois

I am a dataholic –

and it's not just enough to have the data…

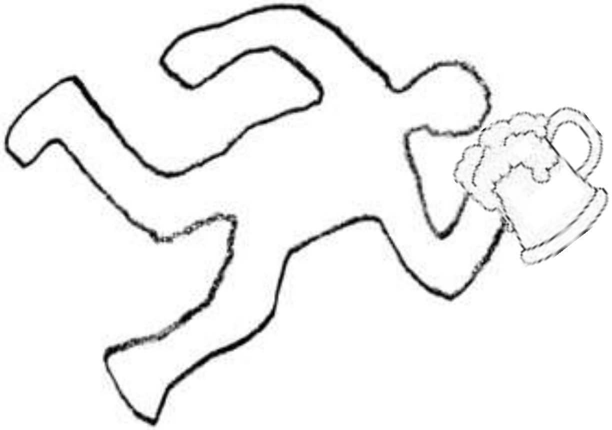
I want to organize it, understand it, and act on it!

"Are you employed sir?"

- Researcher @ Zscaler, Inc.
  - >4 billion transaction / week
- Various Gov't SOC / CERT
  - US-CERT USG netflow

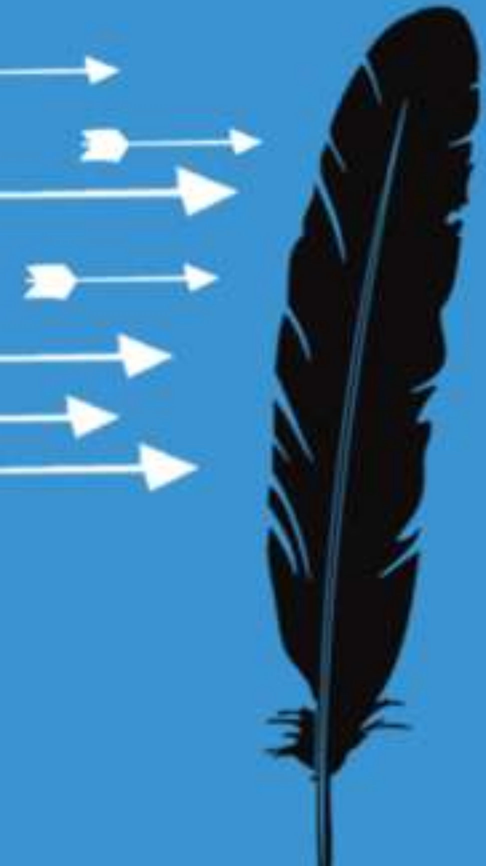
Outline

- Threat Intelligence / OSINT Concepts
- Current State of Tools
- Introducing “Poortego”
- Future Work



Threat Intelligence &

OSINT Concepts



Cyber Threat Intelligence

"…*information directly pertaining to a vulnerability of, or threat to, a system or network, including information pertaining to the protection of a system or network from: (1) efforts to degrade, disrupt, or destroy such systems or network; or (2) theft or misappropriation of information, intellectual property, or personally identifiable information*."

Cyber Intelligence Sharing Protection Act

http://www.gop.gov/bill/112/2/hr3523

Cyber Threat Intelligence

~~*"…information directly pertaining to a vulnerability of, or threat to, a system or network, including information pertaining to the protection of a system or network from: (1) efforts to degrade, disrupt, or destroy such systems or network; or (2) theft or misappropriation of information, intellectual property, or personally identifiable information."*~~

Wha??
No legal speak brah…

Threat Intelligence *(informally)*

- Information about "bad stuff" (threats)
  - Actors, Vulnerabilities, Exploits, Malware/Tools, etc. ("TTPs" & "IOCs")

Threat Intelligence *(informally)*

- That provides actionable info related to the protection / defense of "good stuff"
  - Cyber assets, Intellectual property, PII, etc.

Open-Source Intelligence (OSINT)

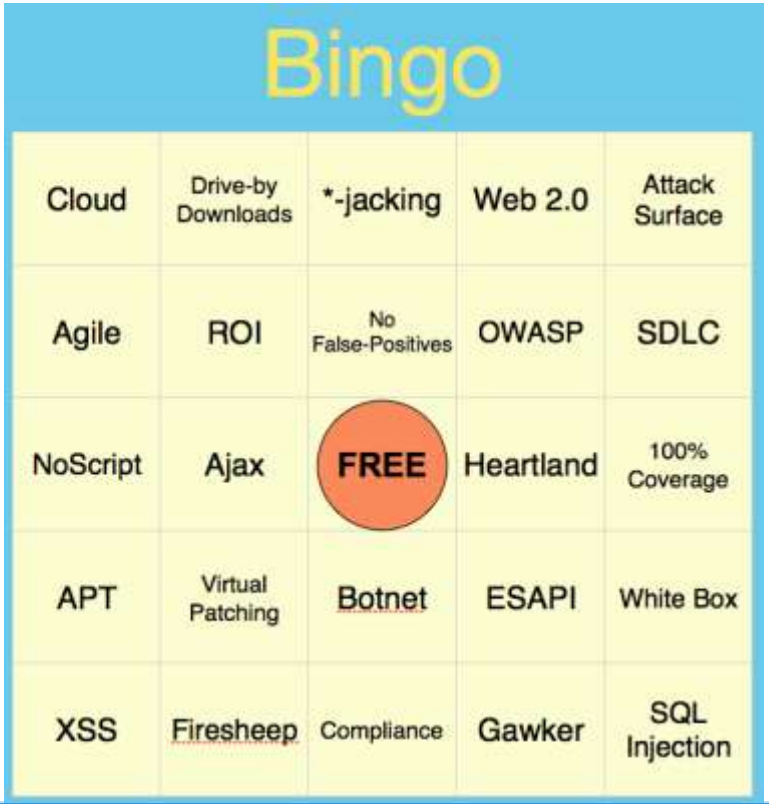
- Use of publicly available information / sources

- Examples, related to cyber threat intelligence:
  - Security blog posts, news stories, advisories, etc.
  - Zeus/SpyEye Tracker, Malware Domains List, Dshield, VirusTotal, Anubis/Wepawet, ThreatExpert, Zscaler's Zulu, etc.

Why Intelligence?

- You don’t know what you don’t know
- You can’t act on what you don’t know
- I’m sure there are Sun Tzu references ☺
  - or OODA-loop if you prefer…
- Helps with threat id
  - “APT” vs. opportunistic

The “why”
Best Illustrated Through Application



Bingo

Cloud	Drive-by Downloads	*-jacking	Web 2.0	Attack Surface
Agile	ROI	No False-Positives	OWASP	SDLC
NoScript	Ajax	FREE	Heartland	100% Coverage
APT	Virtual Patching	Botnet	ESAPI	White Box
XSS	Firesheep	Compliance	Gawker	SQL Injection

Applied Ex.#1

Taken From:
Zscaler “1.PHP”
Incident Whitepaper

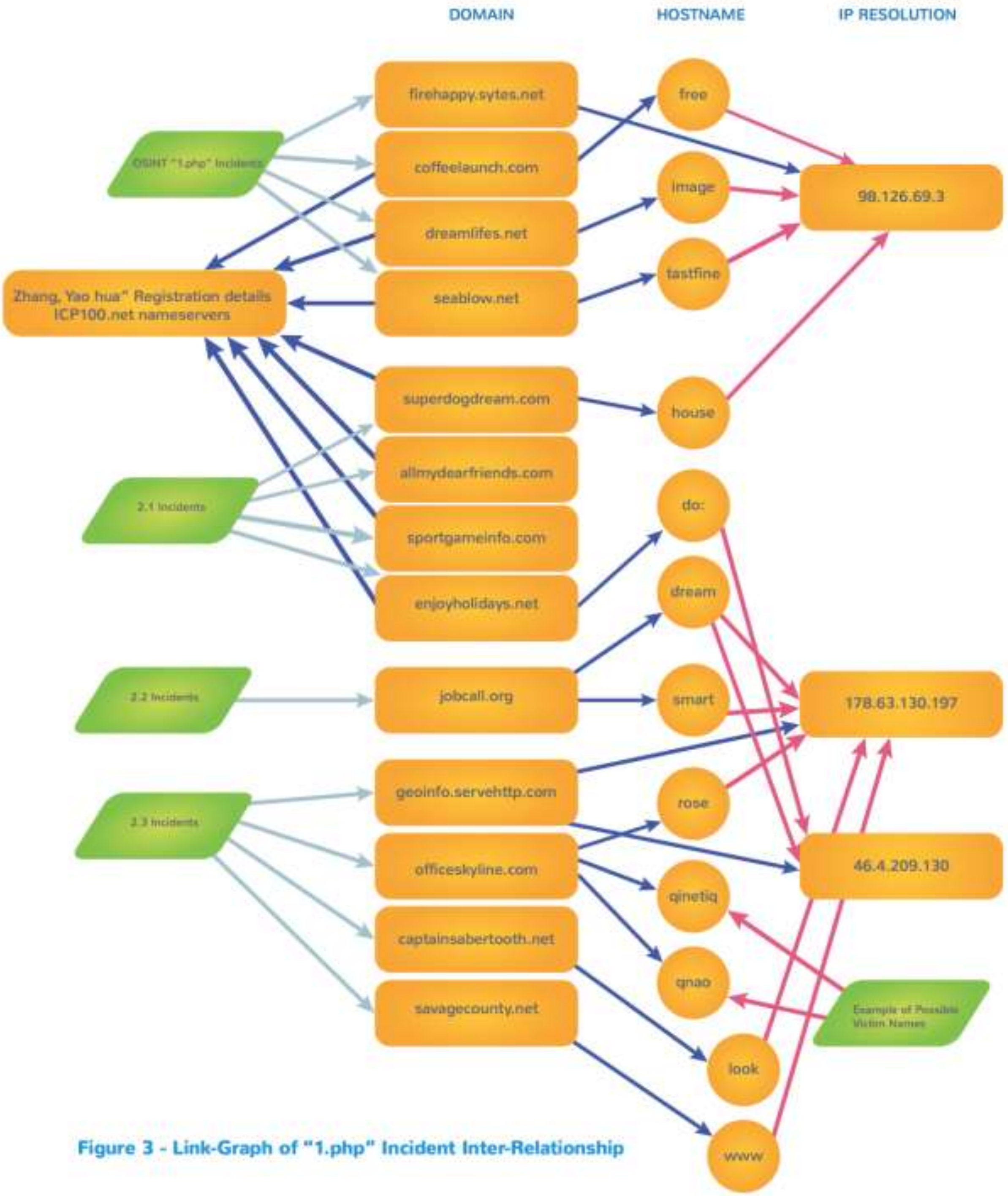
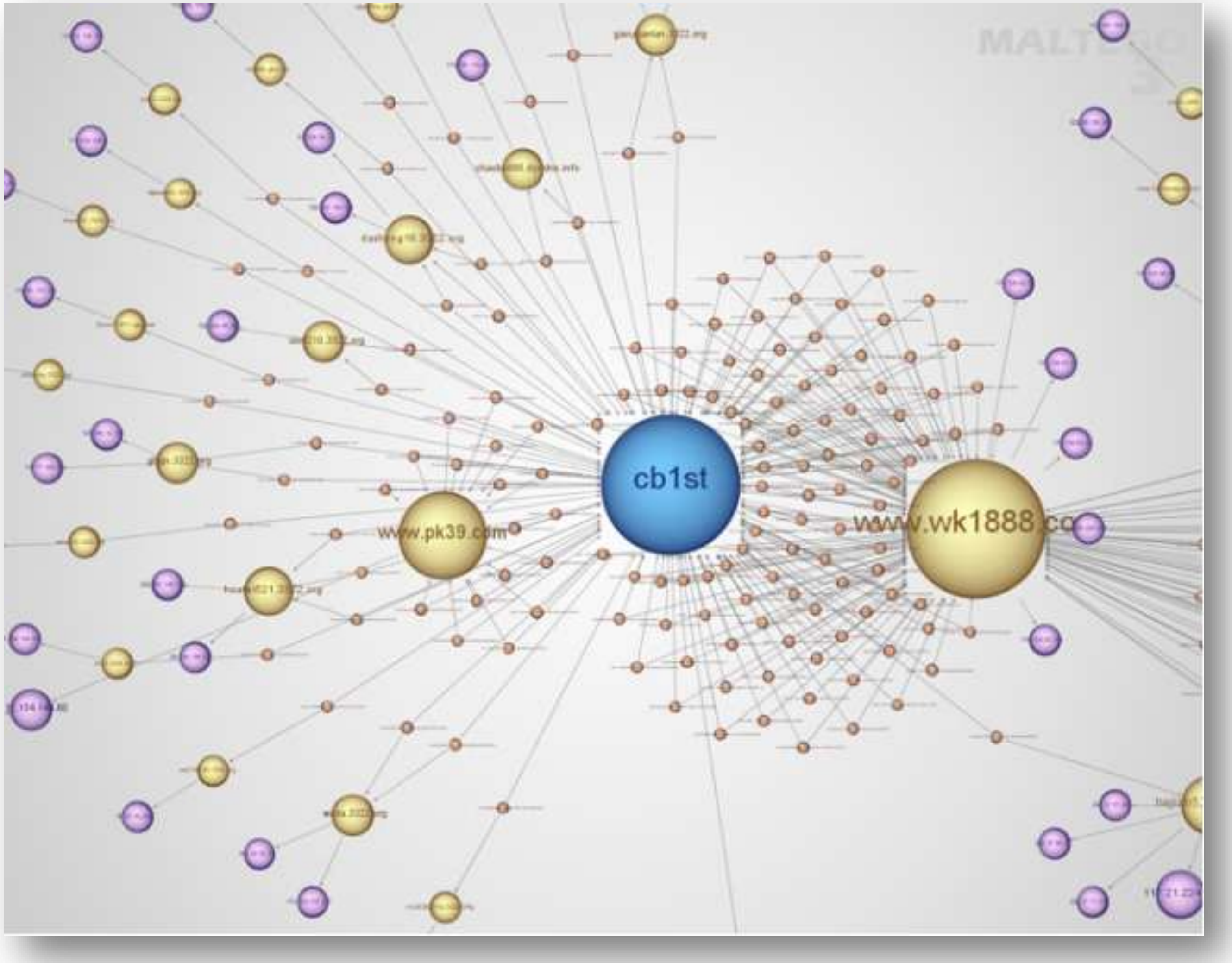


Figure 3 - Link-Graph of "1.php" Incident Inter-Relationship

Applied Ex.#2

Norman (Aug 29, 2012)
“The Many Faces of Gh0st Rat”

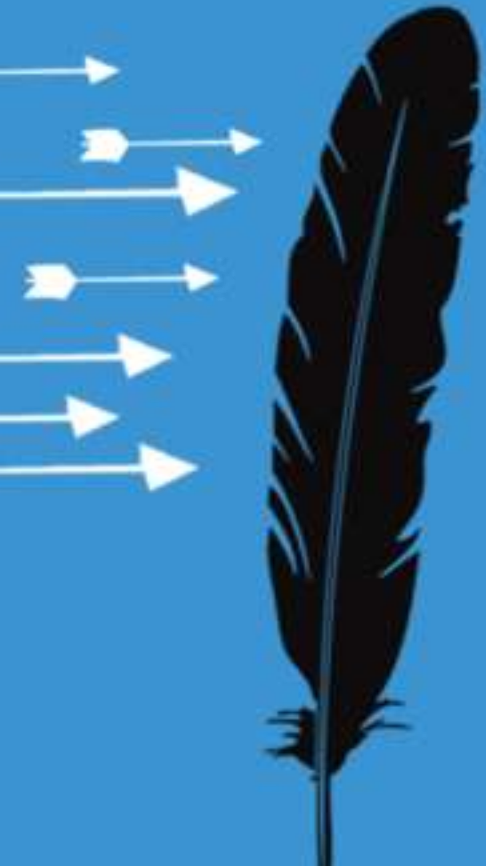


>1200 samples
49 variants
=>
8 super clusters

Basic Intelligence Operations

- Data collection / aggregation
  - Often includes parsing, normalization, storage
- Data correlation
  - Building relationships and meta-data across data
- Identification of “new” and “important” information (extrapolate)
  - Search/filter and rules/alerting
- Apply “meaning” to information
  - Analytic reasoning / logic
  - Analyst reporting / visualization

Transforms

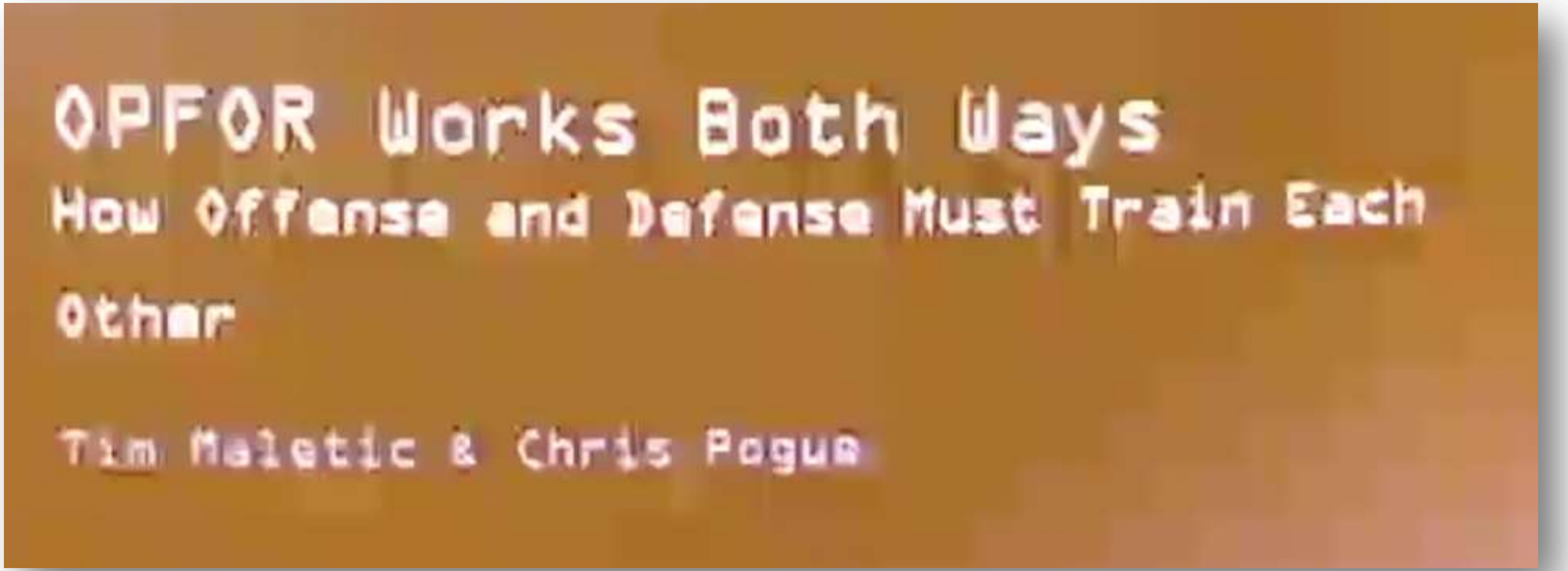


Attack v Defense

SideBar

(If time allows)

Attack ⬄ Defense



OPFOR Works Both Ways

How Offense and Defense Must Train Each Other

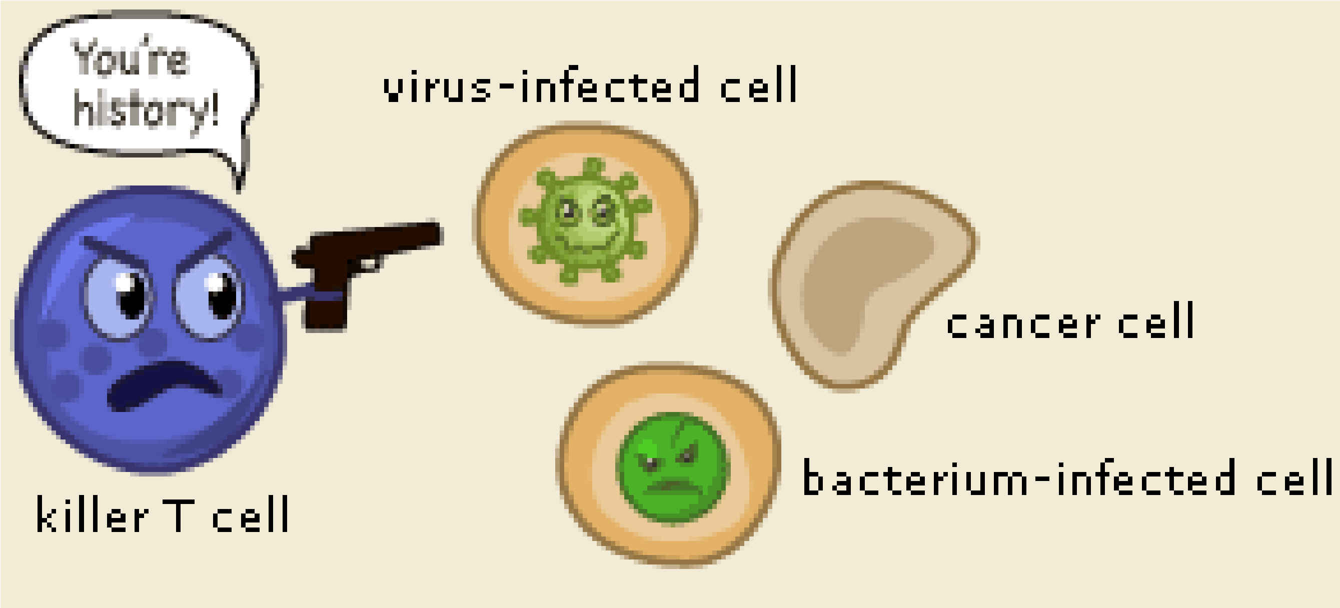
Tim Maletic & Chris Pogue

ShmooCon 2012

(OPFOR: Opposing Forces)

Attack ⇔ Defense

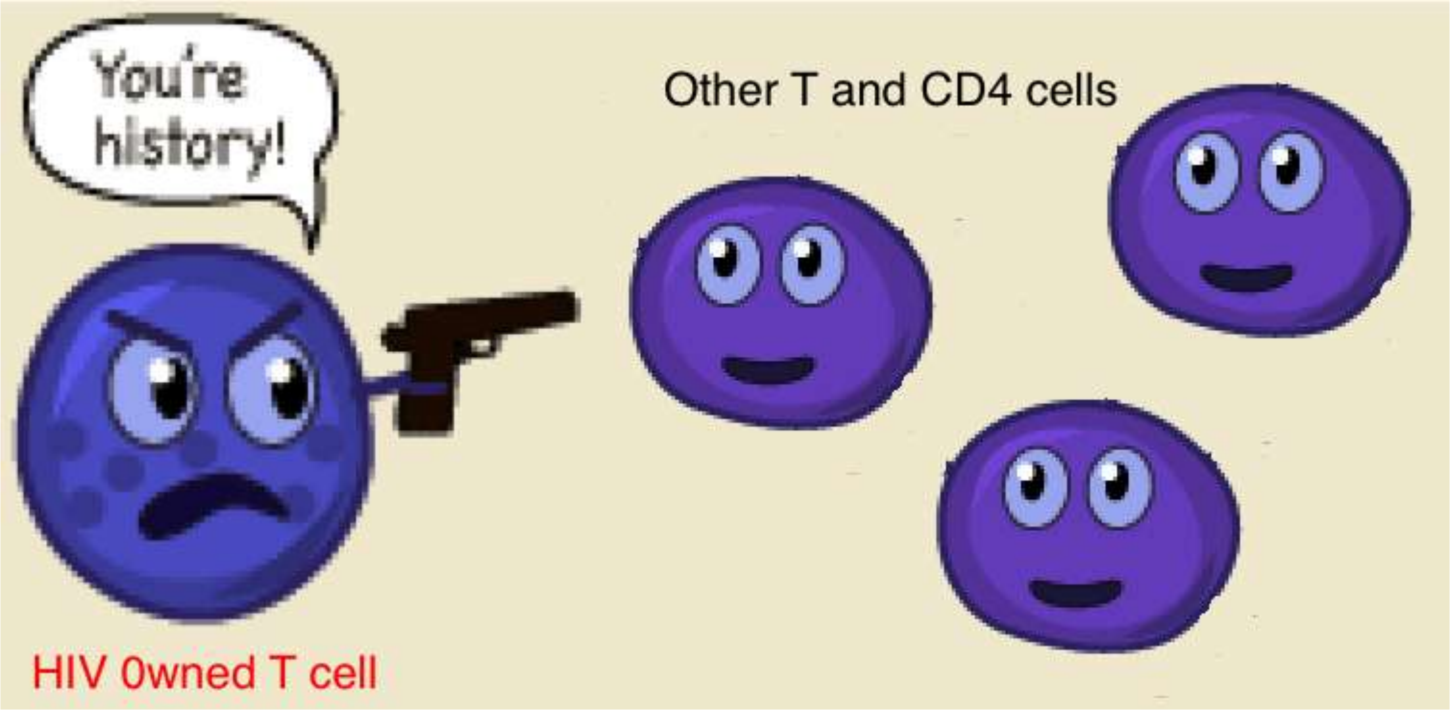
- Similar requirements, such as intelligence, just different perspectives…



The killer T cells terminate cancer cells and cells infected by a virus or bacterium.

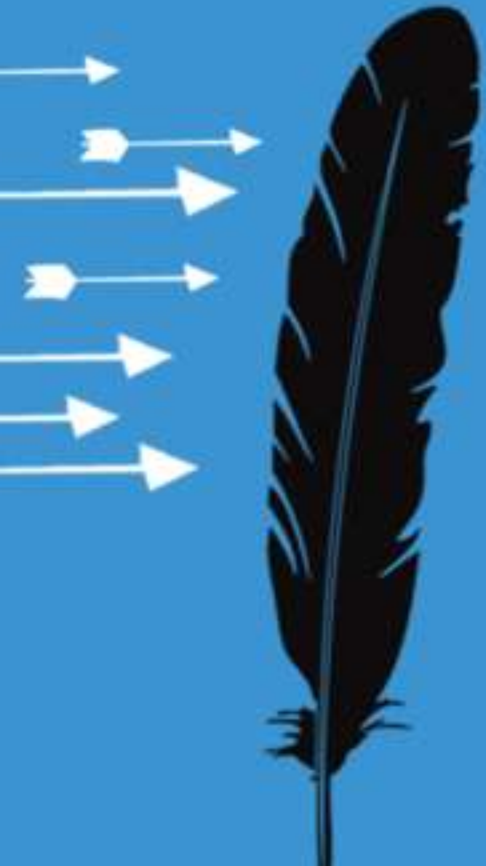
Attack ⬄ Defense

- Similar requirements, such as intelligence, just different perspectives…



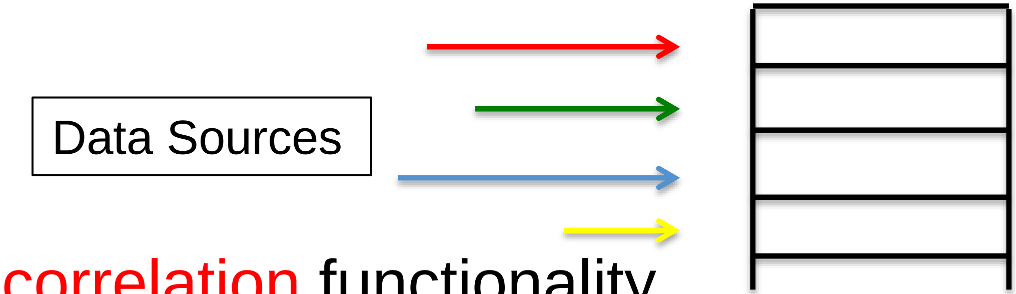
Current State

# of Tools



RSACONFERENCE EUROPE 2012

Aggregation Tools


Data Sources

- Often have some have correlation functionality
- SIEM and log management tools and products
  - **Pros:** mature product space, lots of options / features
  - **Cons:** tied to specific data types / purpose, can be expensive, difficult to deploy and manage
- "Collective Intelligence Framework" (CIF) Project
  - collectiveintel.net (FOSS)
  - CIF-Lite customization (github.com/mgeide/cif-lite)

DEMO 1

CIF

“Intelligence” Tools

- Considered a “niche” space
- Commercial tools are few and very $$$$
  - Popular ex.: Palantir and Analyst Notebook
- GOTS and private solutions
  - Extensive development needs, limited support / deployment…

“Other” FOSS Tools

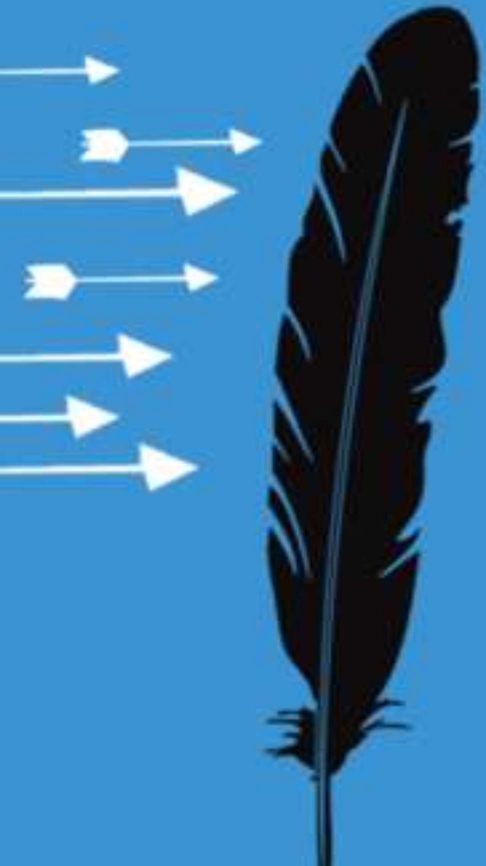
- They don’t satisfy full intel. requirements
- Often fall into other buckets
- ..but are great projects
- Examples:
  - Parse / normalization (e.g., Google Refine)
  - Visualization tools (e.g., Gephi)
  - Data search (e.g., Sphinx)
  - Data mining (e.g., Weka)
  - Stats / machine learning (e.g., R)

Outlier Intelligence Tool

- Maltego (and its little brother CaseFile)
  - Commercial, closed-source
  - License ~$650/yr
  - Private server ~$30K/yr
  - Free, but limited version for private use
  - Rapidly becoming a “standard” tool

DEMO 2

Maltego



It does have limitations…

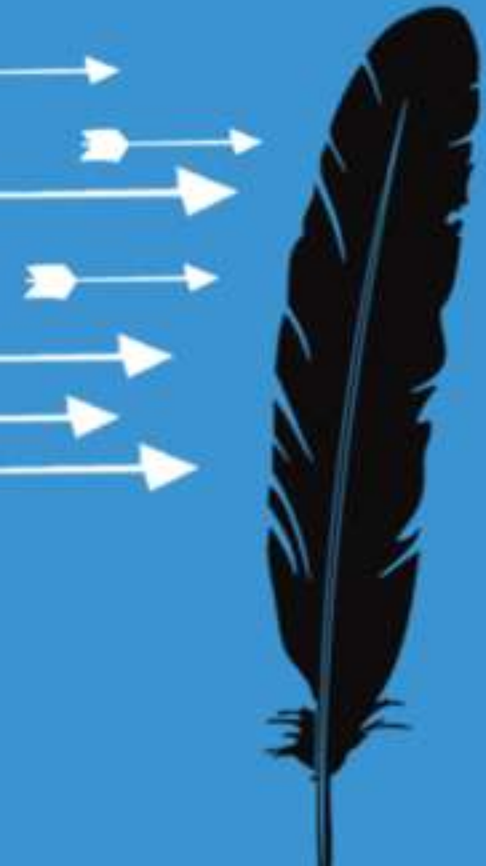
MALTEGO

- CE transform limitations
- Cost is still there
- Does not have open-source flexibility
  - Back / front-end integration with “other” projects
- Transform input tied to one entity
- Data shared with Paterva’s servers *
- Limited export (.mtgx) format **

* Unless private server purchased or local/CaseFile
** Zipped GraphML format

“Other” FOSS Tool Mentions

- FOCA
  - OSINT pen-testing tool
  - Written in .Net (Spanish)
- Sploitego (DefCon 2012)
  - Python Maltego framework, focus on pen-testing
- Dradis
  - Framework for sharing security assessment data
- Netglub
  - Maltego clone, not maintained
- EAR



Introducing

“Poortego”

https://github.com/mgeide/poortego

Goals

- A completely FOSS OSINT / Threat Intel. tool
- FLEXIBLE!
  - Use regardless of perspective (attack, defense, etc.)
  - Support any backend/storage import/export needs
  - Support data rules / transform functionality (Maltego)
  - Easy integration with other tools and platforms
- Start an OSINT community tool
  - Other analysts have noted a gap in this space

Development Influence 1

HD Moore on WarVOX2 at B-Sides Vegas 2011

Revitalize interesting/dead projects (e.g., war-dialing utils) by integrating them into a popular/standard framework (Metasploit) … now people care to use and maintain the project.

Development Influence 2

Wes Young on Collective Intel. Framework (CIF)

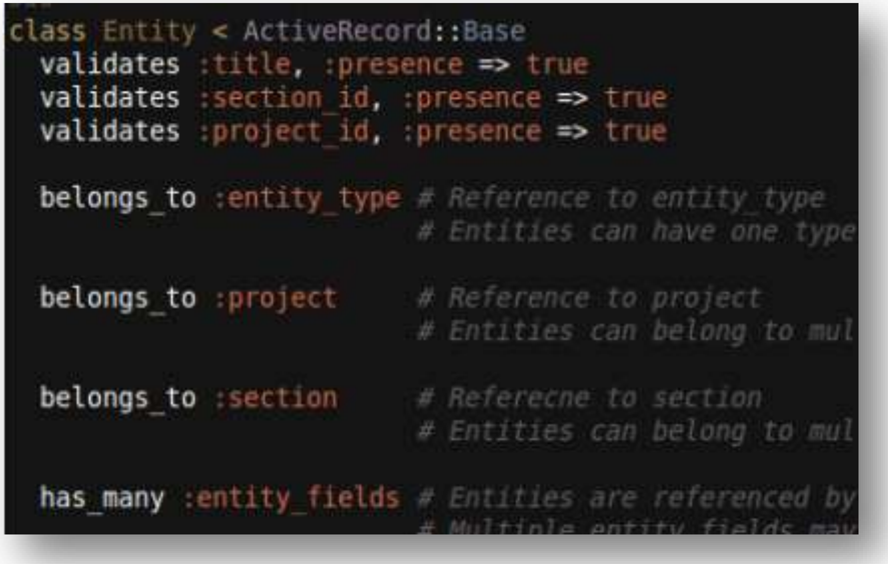
“embrace the suck, it’s better than having no code at all, sometimes that’s the difference between sharing data and not”

Development Architecture

- Ruby
  - ActiveRecords
  - Rex::UI
- Stand-alone CLI
- Metasploit plugin
- Stand-alone transforms
  - Maltego support
- Import / Export plugins

ActiveRecords

- Abstracts data store/retrieve layer
- Support for a multitude of storage sys:
  - Local/file (sqlite)
  - RDBMSs (MySQL/Postgres)
  - NoSQL (MongoDB)
  - In mem. key/value (Redis)
  - Distrib. (Hadoop)
- Constraints done in code versus DB



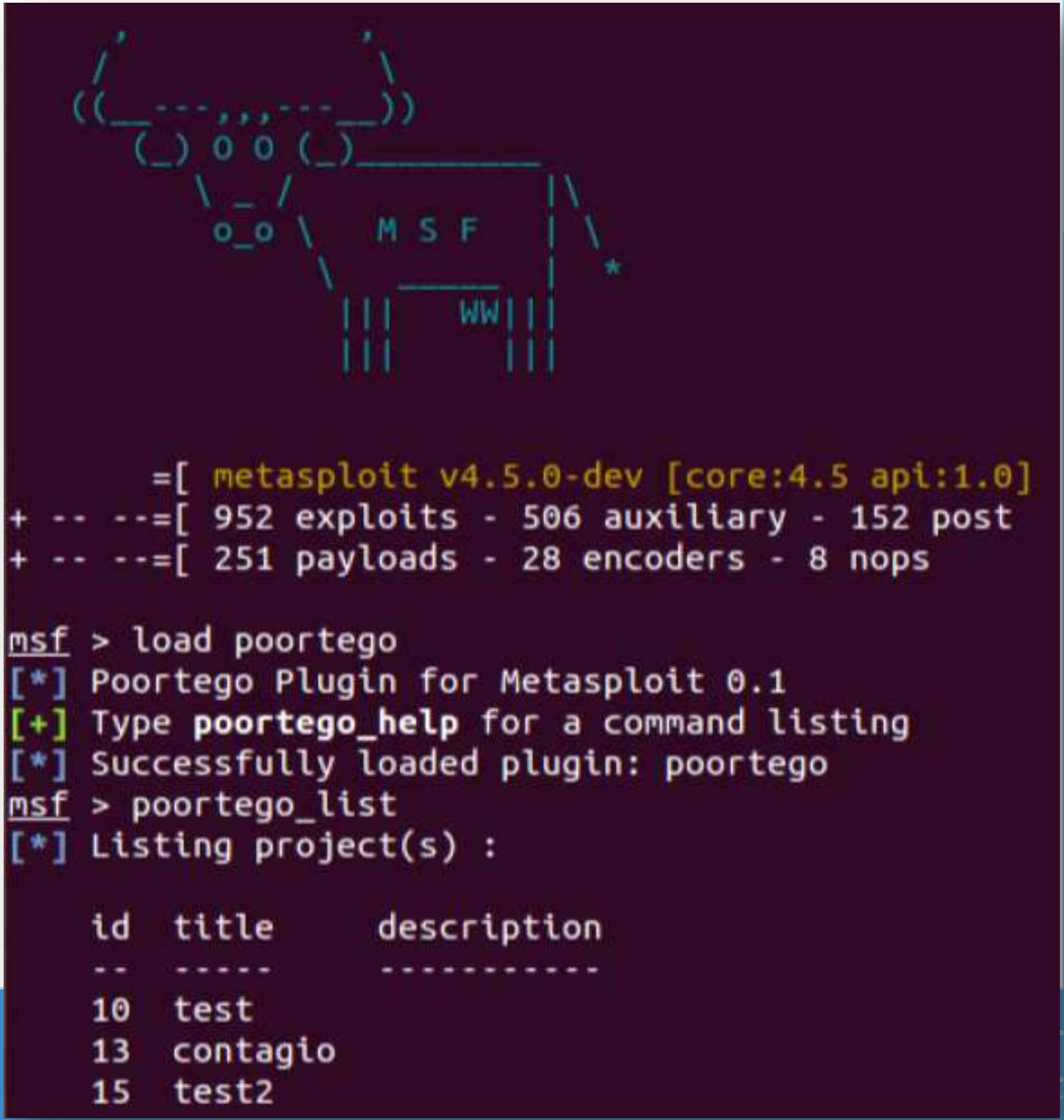
```
class Entity < ActiveRecord::Base
  validates :title, :presence => true
  validates :section_id, :presence => true
  validates :project_id, :presence => true

  belongs_to :entity_type # Reference to entity_type
                          # Entities can have one type

  belongs_to :project     # Reference to project
                          # Entities can belong to mul

  belongs_to :section     # Referecne to section
                          # Entities can belong to mul

  has_many :entity_fields # Entities are referenced by
                          # Multiple entity fields may
```

Rex::UI CLI / Metasploit Plugin

msfconsole

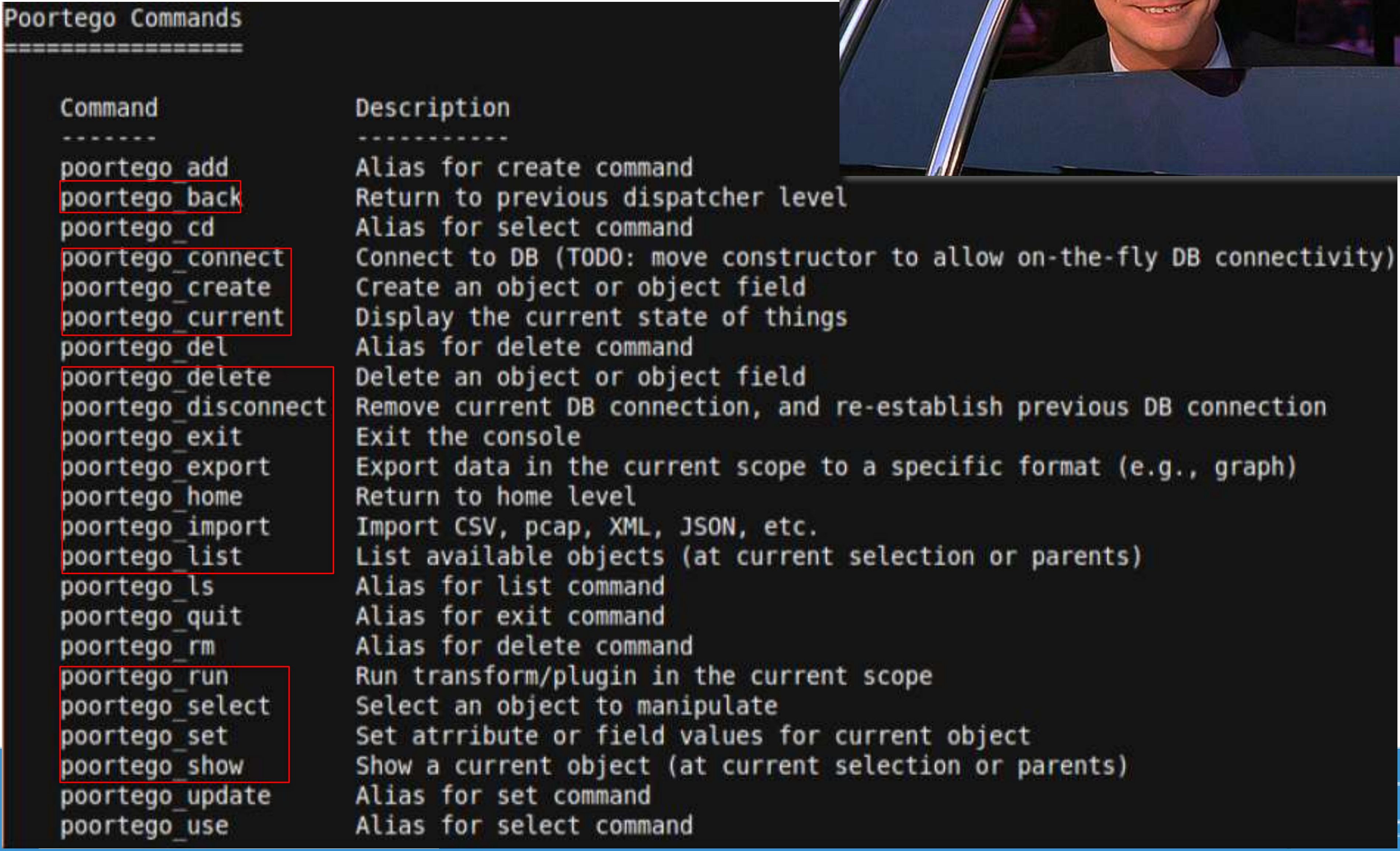
load plugin

Poortego
commands,
projects, data



```
     ,           ,
    /             \
   ((__---,,,---__))
      (_) O O (_)_________
         \ _ /            |\
          o_o \   M S F   | \
               \   _____  |  *
                |||   WW|||
                |||     |||


       =[ metasploit v4.5.0-dev [core:4.5 api:1.0]
+ -- --=[ 952 exploits - 506 auxiliary - 152 post
+ -- --=[ 251 payloads - 28 encoders - 8 nops

msf > load poortego
[*] Poortego Plugin for Metasploit 0.1
[+] Type poortego_help for a command listing
[*] Successfully loaded plugin: poortego
msf > poortego_list
[*] Listing project(s) :

    id  title     description
    --  -----     -----------
    10  test
    13  contagio
    15  test2
```

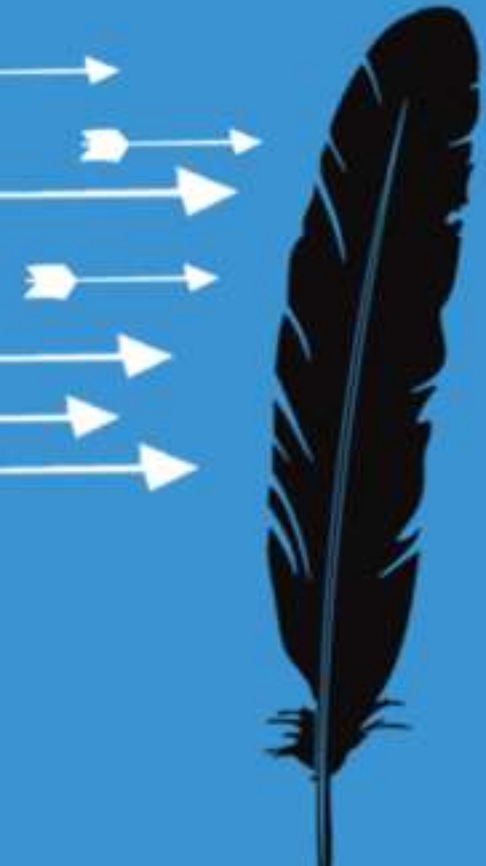
Simple Commands



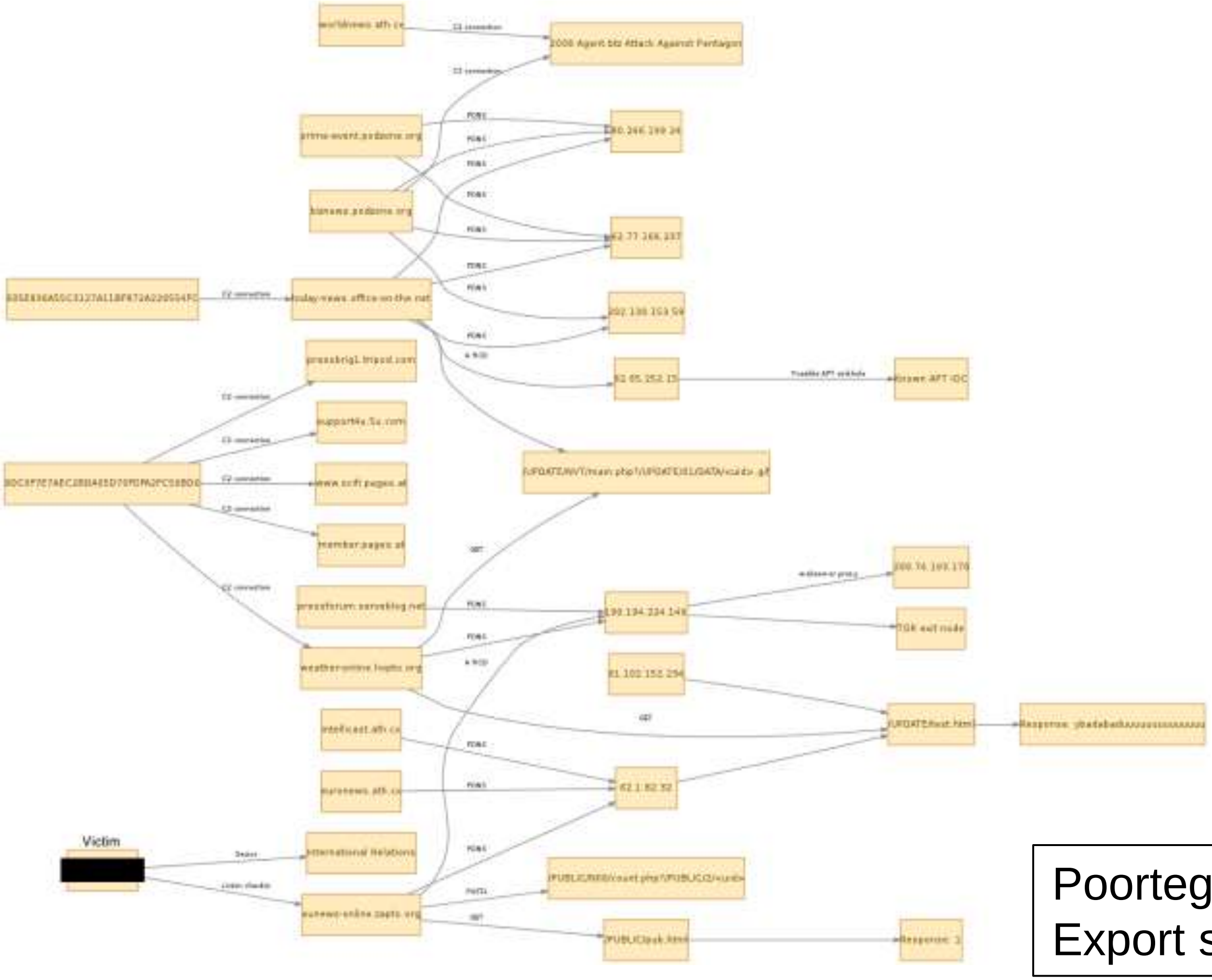
```
Poortego Commands
=================

    Command              Description
    -------              -----------
    poortego_add         Alias for create command
    poortego_back        Return to previous dispatcher level
    poortego_cd          Alias for select command
    poortego_connect     Connect to DB (TODO: move constructor to allow on-the-fly DB connectivity)
    poortego_create      Create an object or object field
    poortego_current     Display the current state of things
    poortego_del         Alias for delete command
    poortego_delete      Delete an object or object field
    poortego_disconnect  Remove current DB connection, and re-establish previous DB connection
    poortego_exit        Exit the console
    poortego_export      Export data in the current scope to a specific format (e.g., graph)
    poortego_home        Return to home level
    poortego_import      Import CSV, pcap, XML, JSON, etc.
    poortego_list        List available objects (at current selection or parents)
    poortego_ls          Alias for list command
    poortego_quit        Alias for exit command
    poortego_rm          Alias for delete command
    poortego_run         Run transform/plugin in the current scope
    poortego_select      Select an object to manipulate
    poortego_set         Set atrribute or field values for current object
    poortego_show        Show a current object (at current selection or parents)
    poortego_update      Alias for set command
    poortego_use         Alias for select command
```

DEMO 3

Poortego

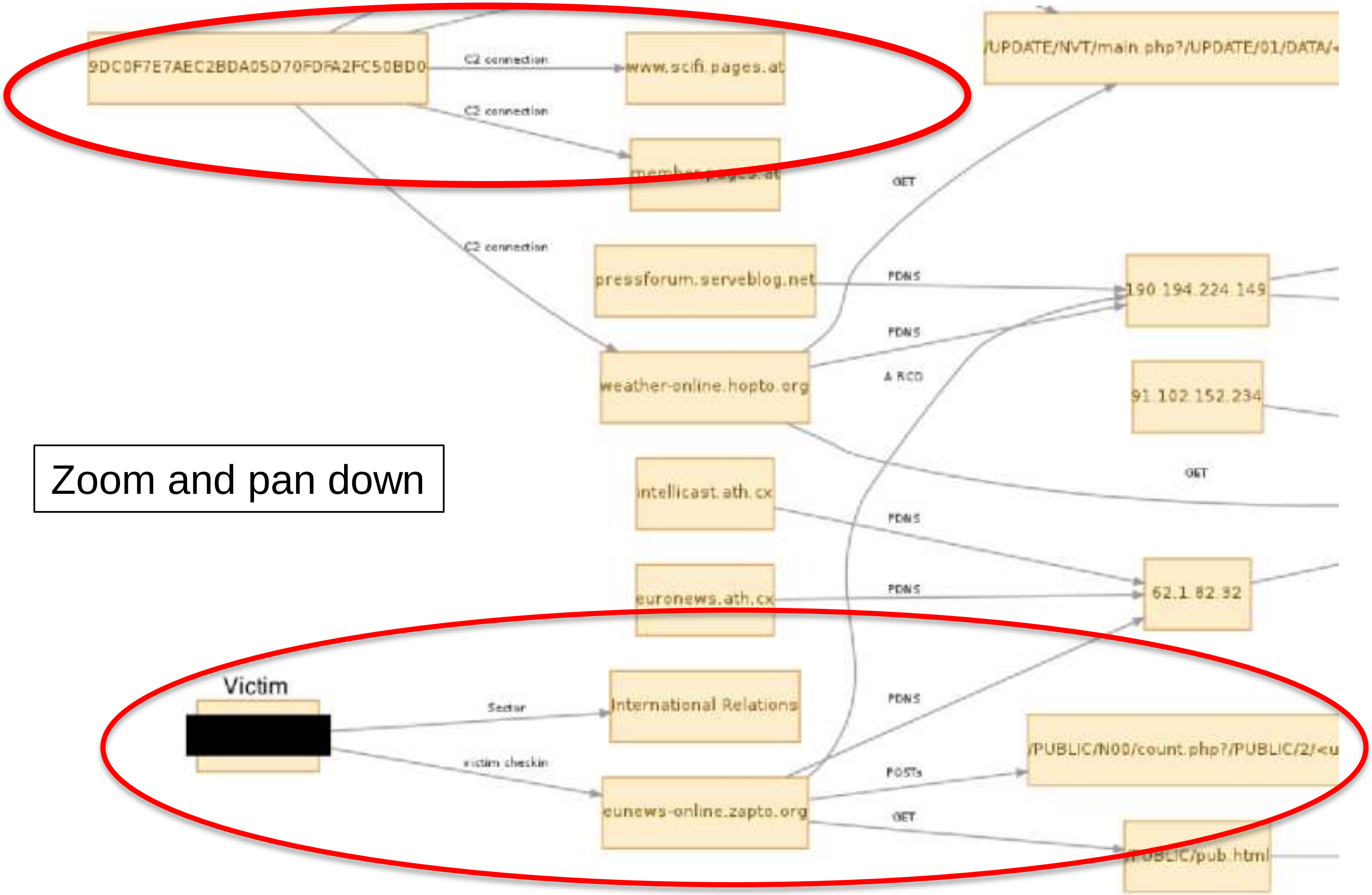


Poortego Case Study



Poortego Graphviz
Export screenshot

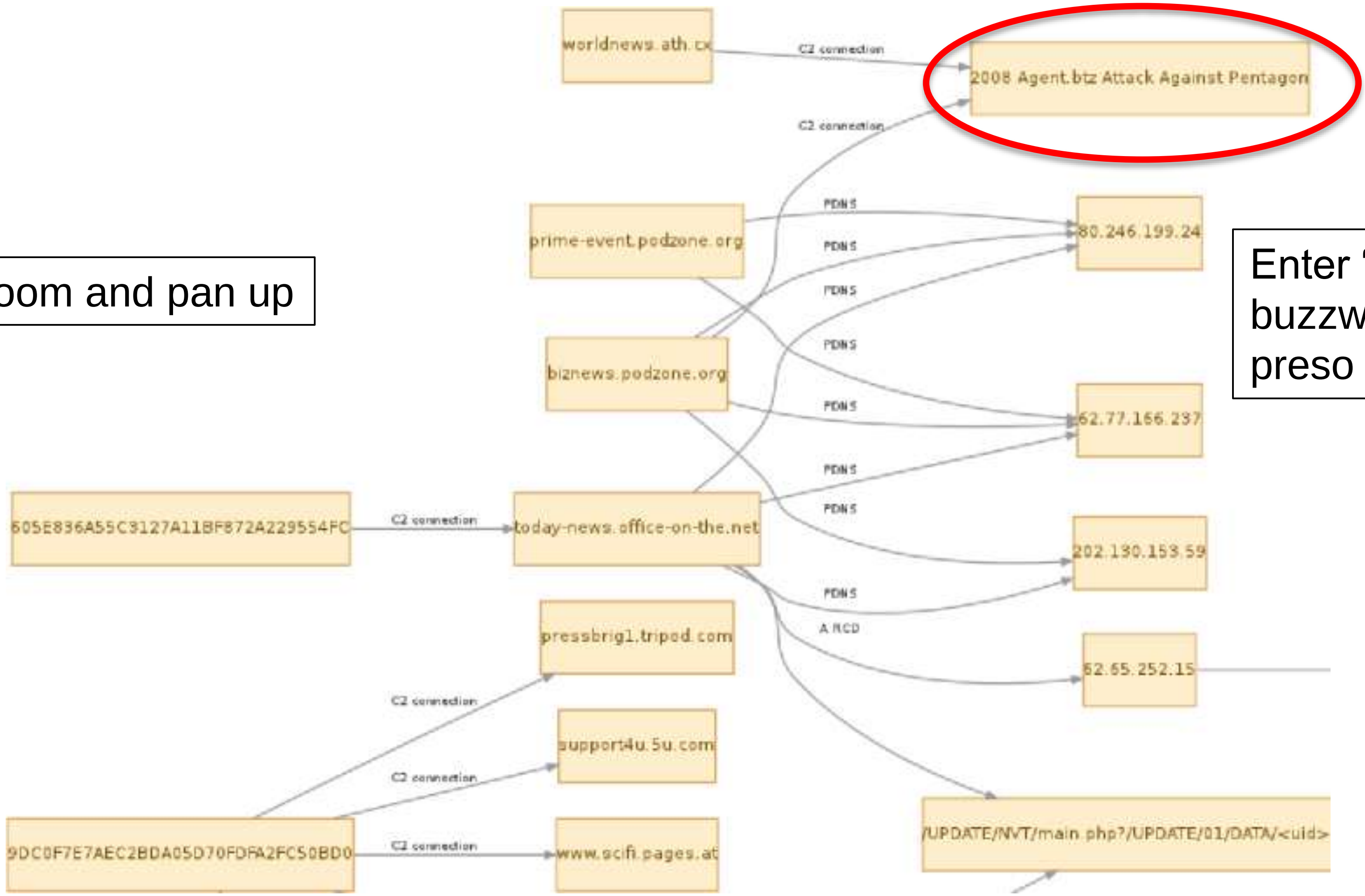
Poortego Case Study (Zoom)



Zoom and pan down

Poortego Case Study

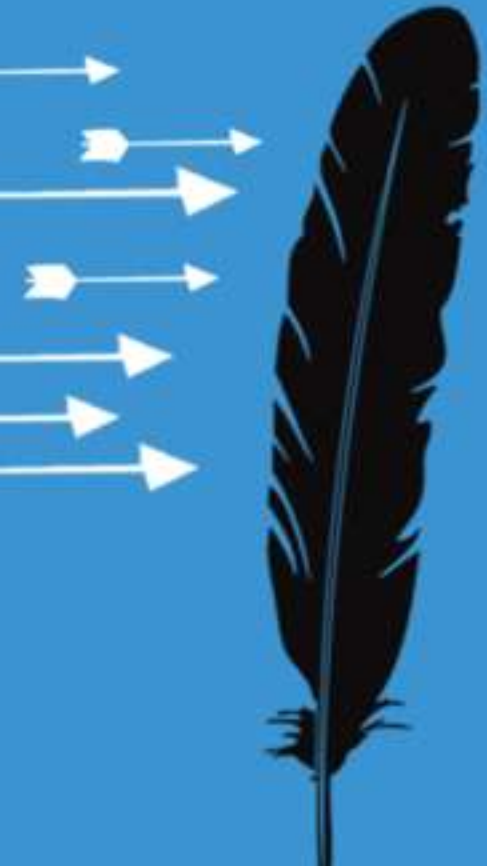
Zoom and pan up



Enter "APT" buzzword in preso here…

Future Work

And Application



Future Work

- GUI work (web / RESTful API)
- What’s up doc.? (documentation)
- Build more importers / exporters / transforms
  - Numerous formats people use (e.g., OpenIOC)
- Wider Community Support
  - Blogpost / notify community
  - Add to Metasploit Git Repository?
  - Contact me if interested in participating

Apply This Presentation

- Leverage OSINT in your “attack” / “defense”
  - Select tools that are appropriate for your need and budget
- Check out Poortego / add the plugin to your Metasploit environment
- Spread the word about the project
- Offer feedback and code if you can

Apply Online Now!

Questions

Community driven threat intel. tool

Let's be awesome together

Thanks for Listening

https://github.com/mgeide/poortego

MIKE GEIDE

MGEIDE
(zscaler.com, gmail.com)