OWASP

Open Web Application Security Project

The Benefits of Python & Open Source

Simplifying the Life of an Incident Responder

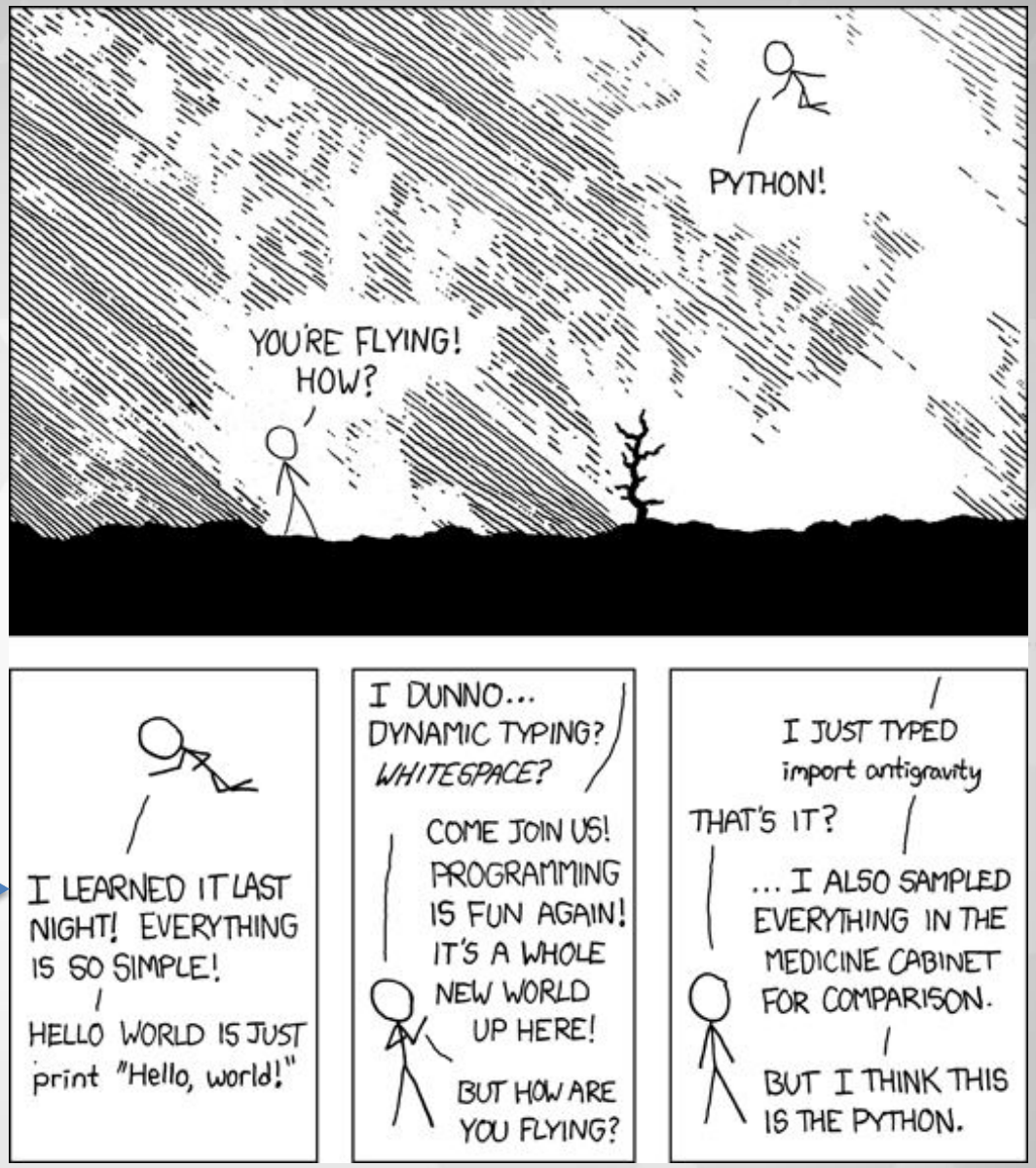
Introduction

- Why Python?
  - How can it assist with IR and Forensics?
- A Practical Example
- Live Demo

Why Python?

I'll let the pros explain

http://xkcd.com/353/



Why Python?

- Beautiful syntax
- Easy to learn and teach
- And:

Python + Incident Response + Open Source == A Good Time

Example

Volatility – Open Source Memory Forensics

Let's Simplify Incident Response

- A reactive security measure through which most proactive security measures are built

- Key Step: Lessons Learned

How Python Can Help

- Time is your enemy when handling an incident
- We need to eradicate the problem quickly
- Python can be leveraged for automation
- Many security tools are written in Python
  - Cuckoo Sandbox [Malware Analysis]
  - GRR Rapid Response [IR Framework]
  - Volatility [Memory Forensics Framework]

A Practical Example

- Assumptions:
  - You're being targeted by a group that uses PlugX
    - APT! They're probably based out of CN… just saying.
  - You need to identify the extent of the compromise
  - You need details now!
    - TTPs, IOCs, <insert buzzword>, etc.

A Practical Example

- What do we do?
  - We first turn to OSINT
    - Gather a list of Indicators to search for on our network
- What do we find?
  - A fantastic article published here
  - It has a lot of good information about PlugX

Read the article and copy/paste the IOCs!

A Practical Example

- A Decent Solution:
  - Use Python to automate the gathering of IOCs

```
usage: intel.py [-h] -i INPUT PATH [INPUT PATH ...] [-o OUTPUT FILE] [-e] [-v]

Used for Extracting and Vetting Intel.

optional arguments:
  -h, --help                                                show this help message and exit
  -i INPUT PATH [INPUT PATH ...], --input INPUT PATH [INPUT PATH ...]  one or more paths to input file or URL.
  -o OUTPUT FILE, --output OUTPUT FILE                      optional path to output file.
  -e, --extract                                             extract intel from input data.
  -v, --vet                                                 vet intel from input data.
```

```
python intel.py -e -i "http://www.bluecoat.com/security-blog/2013-11-25/plugx-used-against-mongolian-targets"
```

A Practical Example

Output:

```
606a3279d855f122ea3b34b0eb40c33f
d0d2079e1ab0e93c68da9c293918a376
6ab333c2bf6809b7bdc37c1484c771c5
73b6df33cf24889a03ecd75cf5a699b3
576aa3655294516fac3c55a364dd21d8
198fd054105ad89a93e401d8f59320d1
021babf0f0b8e5df2e5dbd7b379bd3b1
cc7b091b94c4f0641b180417b017fec2
cc1a806d25982acdb35dd196ab8171bc
yahoomesseges.com
yahoo.com
centralasia.regionfocus.com
Yahoomesseges.com
mseupdate.strangled.net
bodologetee.com
ppt.bodologetee.com
ssupdate.regionfocus.com
peaceful.swordwind.net
peaceful003.linkpc.net
peaceful.linkpc.net
mongolia.regionfocus.com
usa.regionfocus.com
```

A Practical Example

- A Decent Solution:
  - Use Python to automate the creation of IOCs

```
usage: ioc_creator.py [-h] -i FILE PATH [-or] [-n IOC NAME] [-o DIRECTORY PATH]

Generate OpenIOC 1.1 File From Input Data.

optional arguments:
  -h, --help                                show this help message and exit
  -i FILE PATH, --input FILE PATH           Full Path to Input File.
  -or, --or_only                            Optionally, Write the IOC Using 'OR' Logic Only.
  -n IOC NAME, --name IOC NAME              Optionally, Select a Different IOC Name (Default is UUID).
  -o DIRECTORY PATH, --output_dir DIRECTORY PATH  Optionally, specify output directory (Default is CWD).
```

```
python ioc_creator.py -i "/Users/Johnny/Desktop/osint_intel.txt" -o "/Users/Johnny/Desktop/"
```

A Practical Example

```
<?xml version='1.0' encoding='UTF-8'?>
<OpenIOC xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance" xmlns:xsd="http://www.w3.org/2001/XMLSchema" xmlns="http://openioc.org/schemas/OpenIOC_1.1" id="af612e36-3b69-4364
-date="0001-01-01T00:00:00">
  <metadata>
    <short_description>b71d2c41-d14a-4fc5-96f5-5c187139eb3c</short_description>
    <description>Automatically generated IOC</description>
    <keywords/>
    <authored_by>IOC_api</authored_by>
    <authored_date>2014-11-20T02:15:15</authored_date>
    <links/>
  </metadata>
  <criteria>
    <Indicator id="22753384-a4b5-4d02-8bd6-d9e6dd4e731b" operator="OR">
      <IndicatorItem id="5d77f99b-a400-4927-8868-b7d20cd291a9" condition="is" preserve-case="false" negate="false">
        <Context document="FileItem" search="FileItem/Md5sum" type="mir"/>
        <Content type="md5">606a3279d855f122ea3b34b0eb40c33f</Content>
      </IndicatorItem>
      <IndicatorItem id="9bb9ee97-6584-455a-b76d-53714933c26f" condition="is" preserve-case="false" negate="false">
        <Context document="FileItem" search="FileItem/Md5sum" type="mir"/>
        <Content type="md5">d0d2079e1ab0e93c68da9c293918a376</Content>
      </IndicatorItem>
      <IndicatorItem id="e6c222c2-0f1c-4d2e-b4a3-a09196e1b5e4" condition="is" preserve-case="false" negate="false">
        <Context document="FileItem" search="FileItem/Md5sum" type="mir"/>
        <Content type="md5">6ab333c2bf6809b7bdc37c1484c771c5</Content>
      </IndicatorItem>
      <IndicatorItem id="d4a006fe-cef6-4833-86de-be383b6ca214" condition="is" preserve-case="false" negate="false">
        <Context document="FileItem" search="FileItem/Md5sum" type="mir"/>
        <Content type="md5">73b6df33cf24889a03ecd75cf5a699b3</Content>
      </IndicatorItem>
      <IndicatorItem id="b3f23979-2dc5-466b-ab05-e8951fa5b6a8" condition="is" preserve-case="false" negate="false">
        <Context document="FileItem" search="FileItem/Md5sum" type="mir"/>
        <Content type="md5">576aa3655294516fac3c55a364dd21d8</Content>
      </IndicatorItem>
      <IndicatorItem id="8fd784af-cb38-4547-a1b5-c1f112ce6cb1" condition="is" preserve-case="false" negate="false">
        <Context document="FileItem" search="FileItem/Md5sum" type="mir"/>
        <Content type="md5">198fd054105ad89a93e401d8f59320d1</Content>
      </IndicatorItem>
      <IndicatorItem id="bd7f46e0-98ff-45cf-bdcd-fc763a1271d4" condition="is" preserve-case="false" negate="false">
        <Context document="FileItem" search="FileItem/Md5sum" type="mir"/>
        <Content type="md5">021babf0f0b8e5df2e5dbd7b379bd3b1</Content>
      </IndicatorItem>
      <IndicatorItem id="1da50e11-2e9a-4569-a11e-f769a480399a" condition="is" preserve-case="false" negate="false">
        <Context document="FileItem" search="FileItem/Md5sum" type="mir"/>
        <Content type="md5">cc7b091b94c4f0641b180417b017fec2</Content>
      </IndicatorItem>
```

OpenIOC File

Live Demo...