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


Used for Extracting and Vetting Intel.

optional arguments:
  -h, --help
  -i INPUT PATH [INPUT PATH ...], --input INPUT PATH [INPUT PATH ...]
  -o OUTPUT FILE, --output OUTPUT FILE
  -e, --extract
  -v, --vet

A Practical Example

Output:

Remove a few things...
A Practical Example

• A Decent Solution:
  – Use Python to automate the creation of IOCs
A Practical Example