# SOURCE*fire*®

# TRALSE POSITIVE

Simple Methods for Confirming IDS/IPS Alerts

# Introduction

- Geoffrey Serrao

- Currently Employed at Sourcefire, Inc.
  - ‣ Tier I Technical Support Engineer

- Typical work day for a Tier 1
  - ‣ Hardware questions
  - ‣ Configuration questions
  - ‣ False positive analysis

**SOURCE***fire*®
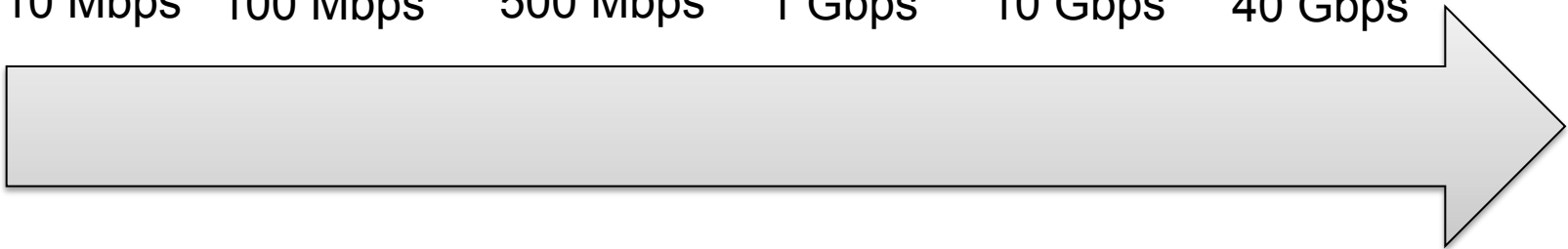
# IDS/IPS Alerts

- Big Three
  - Snort
  - Suricata
  - Bro IDS

- IDS/IPS systems generate alerts based on:
  - ‣ Signatures
  - ‣ Network Anomalies

- We will be dealing mostly with signature based events today

**SOURCE**fire®

# A Trend

- More data is being analyzed
- More events are being generated
- What do we do with all of these events?

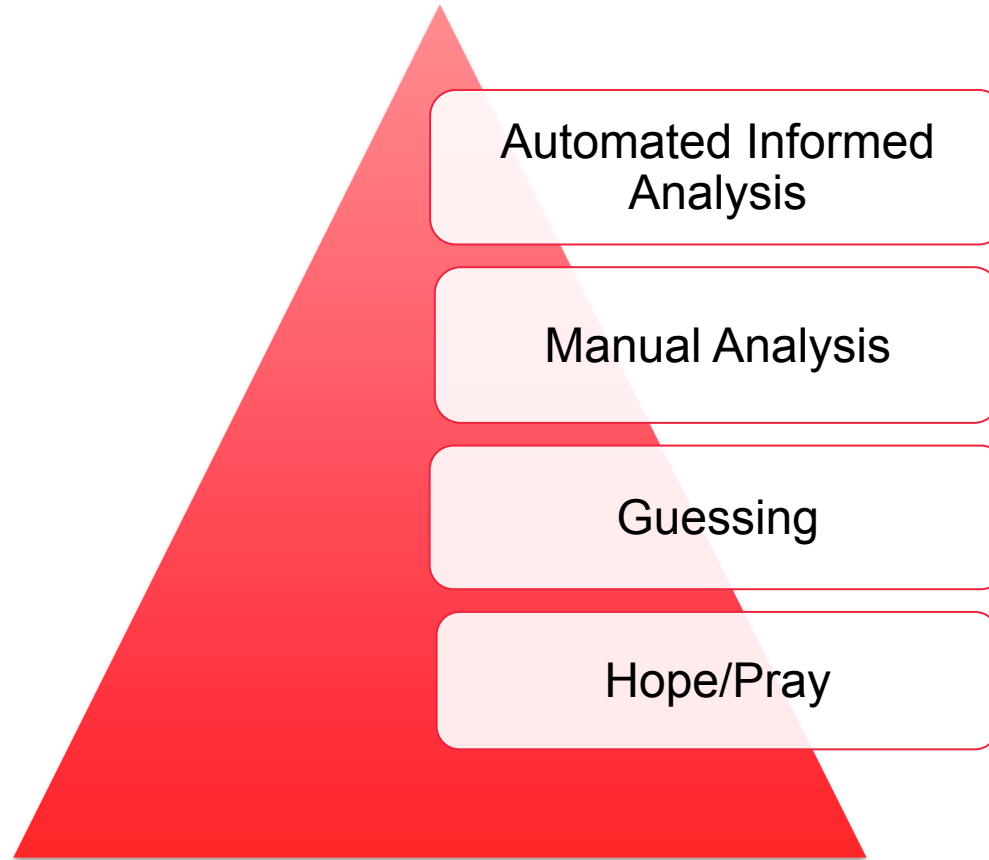| 10 Mbps | 100 Mbps | 500 Mbps | 1 Gbps | 10 Gbps | 40 Gbps |

**SOURCE**fire®

# Current Incident Handling Process

- Preparation

- Detection and Notification

- Investigation And Qualification  ⬅

- Communication

- Containment and Recovery

- Lessons Learned

**SOURCE**fire®

# Existing Techniques

Best

Automated Informed Analysis

Manual Analysis

Guessing

Hope/Pray

Worst

SOURCE*fire*®

# The Current Method

- Step 1: Verify Rule Context
  - ▸ Rule Header
  - ▸ Content Matches
- Step 2: Verify Endpoints
  - ▸ Who's talking
- Step 3: Verify Conversation
  - ▸ What's being said – gets technical
- Step 4: Verify Operational Context
  - ▸ How does this type of attack affect my network deployment? – also gets technical

**SOURCE**fire®

# A Happy Example

# Drawbacks of the Current Method

- Limited by the amount of information available to the analyst at the time

- Time intensive

- Tedious

- Reactive approach

**SOURCE**fire®

# Real World Example

# How to Improve

- Let's take a more proactive approach

- Increase the amount of information available to the analyst

- Increase the quality of the dissected payload

- Use automation tools

- The best methods are the most informed methods

- We need a bigger source of information

**SOURCE**fire®

# What I'd Like to See

| IP's | rDNS | Verdict |
|---|---|---|
| … | | |
| 54.243.156.140 | sourcefire.com | Clean |
| 64.214.53.2 | sf-nat.sourcefire.com | Clean |
| 205.178.189.131 | flocon.org | Clean |
| 167.216.129.13 | immunet.com | Clean |
| 23.23.170.170 | snort.org | Clean |
| 69.43.161.180 | antivirus-online21.com | +Investigate |
| 192.88.209.252 | cert.org | Clean |
| 10.20.57.16 | <none> | RFC 1918 |
| … | | |

http://dns-bh.sagadc.org/domains.txt

# Information Sources

**SOURCE**fire®

# Information Sources, Cont.

- Common
  - ▸ http://www.malwaredomains.com
  - ▸ www.mxtoolbox.com
  - ▸ https://www.dnsstuff.com/
  - ▸ http://www.siteadvisor.com/
  - ▸ https://www.phishtank.com/
- Not so common
  - ▸ Pastebin.com
  - ▸ Twitter.com

SOURCE*fire*®

# Favorite Information Source

- [http://support.clean-mx.de/clean-mx/viruses](http://support.clean-mx.de/clean-mx/viruses)

- They've been really tolerating my automated testing

- Easily encoded POST http requests for
  - IP
  - Domain

# Python!



https://xkcd.com/353/

SOURCE*fire*®
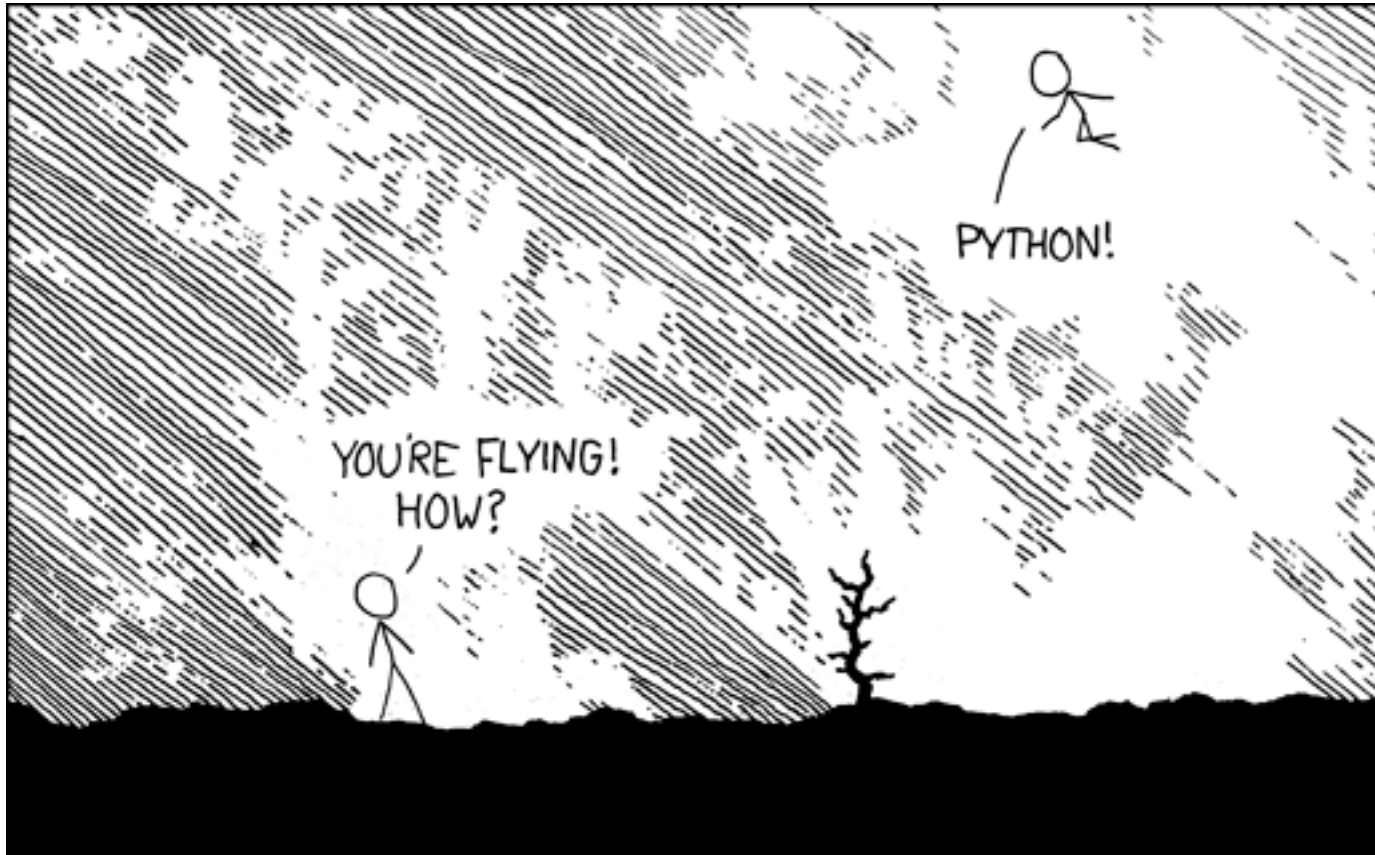
# The Code 1 of 3

```
from scapy.all import *
from scapy.utils import *
…
print "Reading PCAP(s):"
for x in range(num_pcaps):
    try:
        pkts.extend(rdpcap(caps[x]))
    except Exception, e: print e

print "Collecting IPs.."
for pkt in pkts:
    if pkt.haslayer(IP):
        if not pkt[IP].src in ip_list:
            ip_list.append(pkt[IP].src)
        if not pkt[IP].dst in ip_list:
            ip_list.append(pkt[IP].dst)
print len(ip_list), " unique IPs collected from pcap(s)"
…
```

**SOURCE***fire*®

# The Code 2 of 3

```
for i in ip_list:
    if check_country:
        try:
            location = str(GEOIP.lookup(i)).split('country')[1].strip('[] \n' )
        except Exception, e:
            print "country lookup failure.", e

    if check_hostname:
        try:
            hostname = socket.getfqdn(i)
        except Exception, e:
            hostname = "Couldn't find hostname", e
```

**SOURCE**fire®

# The Code 3 of 3

```
response = urlopen('http://support.clean-mx.de/clean-mx/viruses.php')
forms = ParseResponse(response, backwards_compat=False)
form = forms[0]

try:
            br = mechanize.Browser()
            …
            form['ip'] = i
            response = urlopen(form.click()).read()

            if not response.find('<br><br><div align="center"><b>For this
query is nothing recorded in our database.</b><br>') > -1:
                        reputation = "- Investigate"
            else:
                        reputation = "+ Clean"
```

# Finished Output

```
-=Open proxy analysis=-
Got  248690  dangerous IPs.
Dangerous IPs matched: None

-=Full Analysis=-
6  IPs to check.
    169.10.11.239      US                              169.10.11.239        + Clean t:0.85781
     72.21.81.253      US                               72.21.81.253      - Investigate t:0.86674
 174.143.121.210      US                          www.stylebistro.com        + Clean t:0.53773
    169.14.238.54      US                              169.14.238.54        + Clean t:0.87787
    169.10.22.247      US                              169.10.22.247        + Clean t:0.48822
 178.255.240.230      IT                             www.witcom.com      - Investigate t:13.33818
```

SOURCE*fire*®

# Caveats and Pitfalls

- Customers with secure networks and tight data retention policies may not be able to take full advantage

- Working with encryption

- Tuning for accuracy

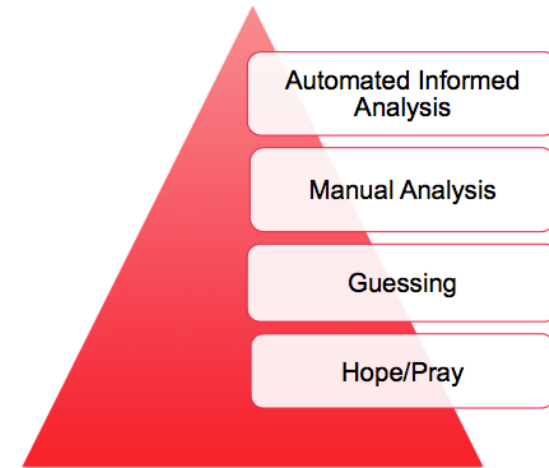**SOURCE***fire*®

# Future Development

- PCAPalyze
    - PHP web application (HTTPS) interface
    - Flask + Python back end
        - SCAPY used for extrapolating PCAP data

- Uses more sources of data

- Available for the public to use

- Works with more protocols

**SOURCE**fire®

# In Summation

| IP's | rDNS | Verdict |
|------|------|---------|
| ... | | |
| 54.243.156.140 | sourcefire.com | Clean |
| 64.214.53.2 | sf-nat.sourcefire.com | Clean |
| 205.178.189.131 | flocon.org | Clean |
| 167.216.129.13 | immunet.com | Clean |
| 23.23.170.170 | snort.org | Clean |
| 69.43.161.180 | antivirus-online21.com | +Investigate |
| 192.88.209.252 | cert.org | Clean |
| 10.20.57.16 | <none> | RFC 1918 |
| ... | | http://dns-bh.sagadc.org/domains.txt |

Pyramid (top to bottom):
- Automated Informed Analysis
- Manual Analysis
- Guessing
- Hope/Pray

```
-=Open proxy analysis=-
Got  248690  dangerous IPs.
Dangerous IPs matched: None

-=Full Analysis=-
6  IPs to check.
   169.10.11.239     US                           169.10.11.239      + Clean t:0.85781
    72.21.81.253     US                            72.21.81.253  - Investigate t:0.86674
  174.143.121.210    US           www.stylebistro.com             + Clean t:0.53773
   169.14.238.54     US                           169.14.238.54     + Clean t:0.87787
   169.10.22.247     US                           169.10.22.247     + Clean t:0.48822
  178.255.240.230    IT               www.witcom.com         - Investigate t:13.33818
```

SOURCEfire®

# Questions

**SOURCE**fire®