TRALSE POSITIVE

Simple Methods for Confirming IDS/IPS Alerts

Introduction

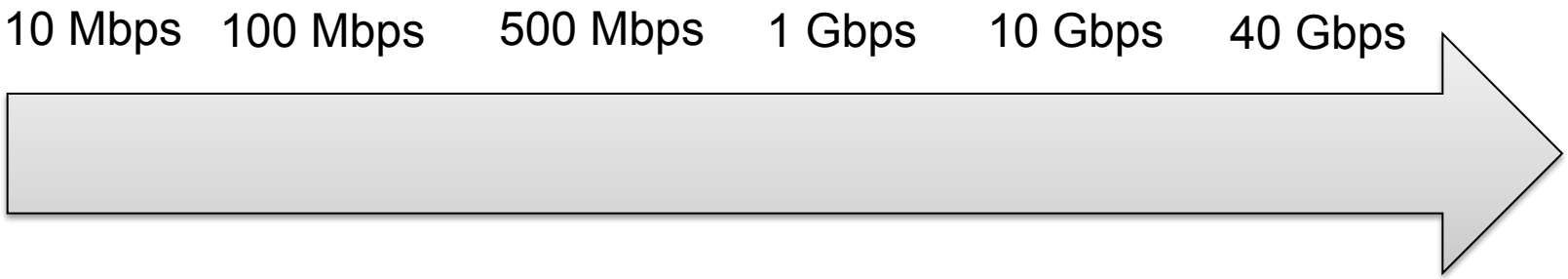
- Geoffrey Serrao
- Currently Employed at Sourcefire, Inc.
  - Tier I Technical Support Engineer
- Typical work day for a Tier 1
  - Hardware questions
  - Configuration questions
  - False positive analysis

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

A Trend

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



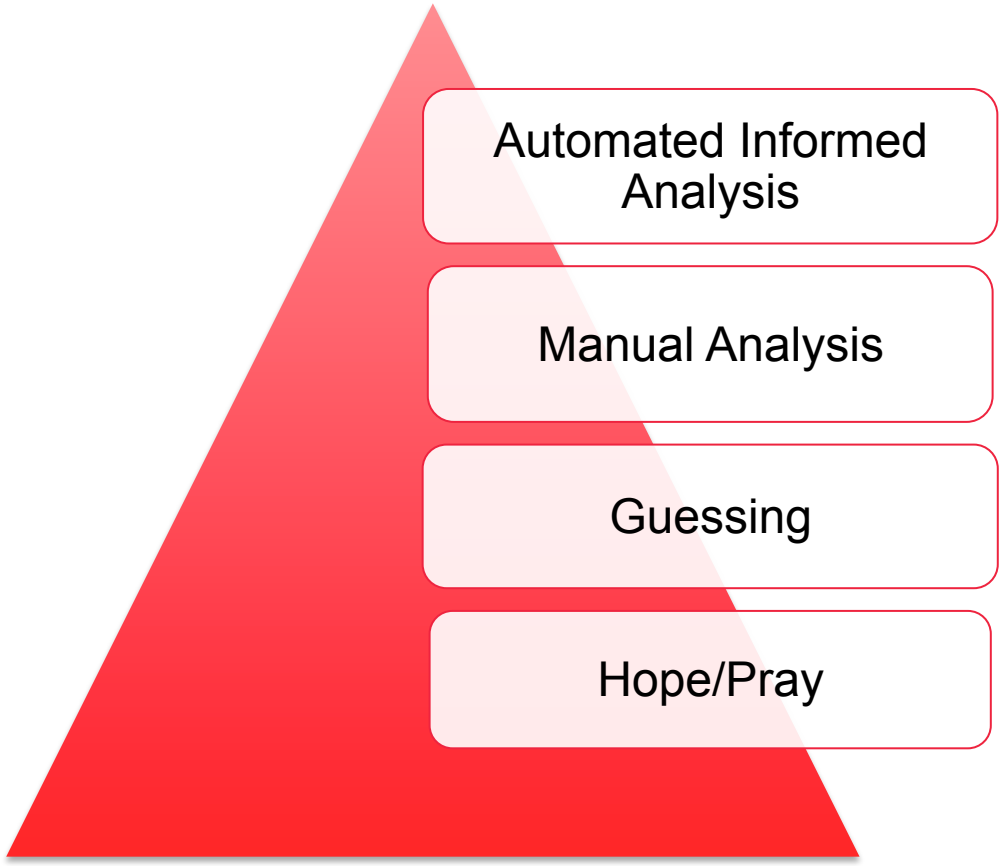
SOURCEfire®

Current Incident Handling Process

- Preparation
- Detection and Notification
- Investigation And Qualification
- Communication
- Containment and Recovery
- Lessons Learned

Existing Techniques

Best



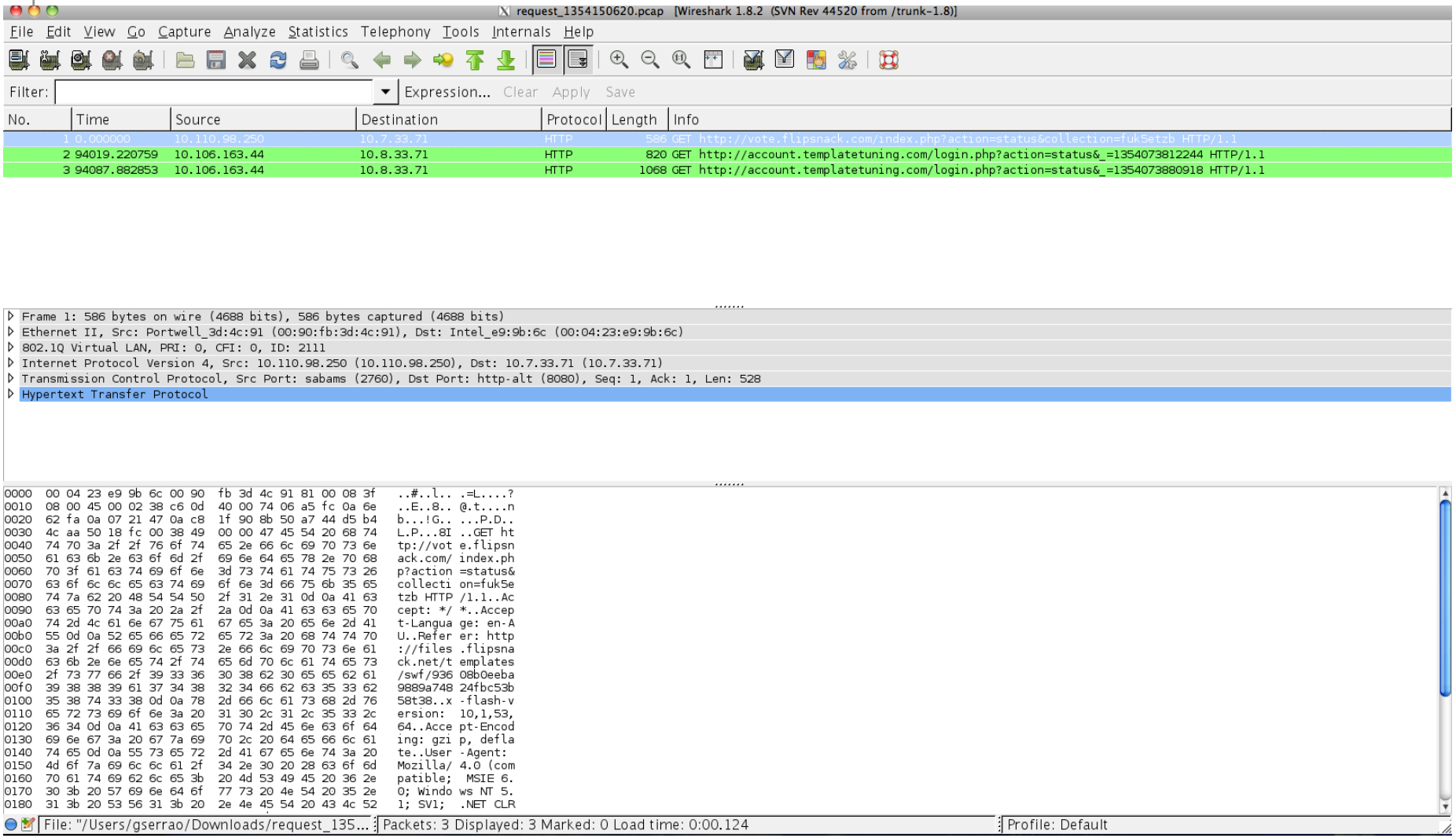
Worst

SOURCEfire®

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

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

Real World Example

traffic.pcap [Wireshark 1.8.2 (SVN Rev 44520 from /trunk-1.8)]

File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help

Filter: Expression... Clear Apply Save

No.	Time	Source	Destination	Protocol	Length	Info
607	35.484069	72.21.195.15	10.8.0.4	TCP	1514	[TCP segment of a reassembled PDU]
608	35.484072	72.21.195.15	10.8.0.4	TCP	294	[TCP segment of a reassembled PDU]
609	35.484087	10.8.0.4	72.21.195.15	TCP	54	50489 > http [ACK] Seq=853 Ack=117693 Win=523896 Len=0
610	35.484185	72.21.195.15	10.8.0.4	TCP	1514	[TCP segment of a reassembled PDU]
611	35.484280	72.21.195.15	10.8.0.4	TCP	1514	[TCP segment of a reassembled PDU]
612	35.484306	10.8.0.4	72.21.195.15	TCP	54	50489 > http [ACK] Seq=853 Ack=120613 Win=524280 Len=0
613	35.484376	72.21.195.15	10.8.0.4	TCP	1514	[TCP segment of a reassembled PDU]
614	35.484494	72.21.195.15	10.8.0.4	TCP	1514	[TCP segment of a reassembled PDU]
615	35.484518	10.8.0.4	72.21.195.15	TCP	54	50489 > http [ACK] Seq=853 Ack=123533 Win=524280 Len=0
616	35.484576	72.21.195.15	10.8.0.4	TCP	1514	[TCP segment of a reassembled PDU]
617	35.484682	72.21.195.15	10.8.0.4	TCP	1514	[TCP segment of a reassembled PDU]
618	35.484684	72.21.195.15	10.8.0.4	TCP	294	[TCP segment of a reassembled PDU]
619	35.484695	10.8.0.4	72.21.195.15	TCP	54	50489 > http [ACK] Seq=853 Ack=126693 Win=523896 Len=0
620	35.484794	72.21.195.15	10.8.0.4	TCP	1514	[TCP segment of a reassembled PDU]
621	35.484899	72.21.195.15	10.8.0.4	TCP	1514	[TCP segment of a reassembled PDU]
622	35.484900	72.21.195.15	10.8.0.4	HTTP	343	HTTP/1.1 200 OK (JPEG JFIF image)
623	35.484913	10.8.0.4	72.21.195.15	TCP	54	50489 > http [ACK] Seq=853 Ack=129902 Win=523848 Len=0
624	35.509065	10.8.0.4	10.8.0.187	TCP	78	50490 > netbios-ssn [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=8 TSval=425440370 TSecr=0 SACK_PERM=1
625	35.512143	10.8.0.187	10.8.0.4	TCP	74	netbios-ssn > 50490 [SYN, ACK] Seq=0 Ack=1 Win=8192 Len=0 MSS=1460 WS=256 SACK_PERM=1 TSval=11948705 TSecr=4254
626	35.512168	10.8.0.4	10.8.0.187	TCP	66	50490 > netbios-ssn [ACK] Seq=1 Ack=1 Win=524280 Len=0 TSval=425440370 TSecr=11948705
627	35.519204	10.8.0.4	10.8.0.187	NBSS	138	Session request, to 10.8.0.187<20> from GSERRAO_MAC<00>
628	35.520890	10.8.0.187	10.8.0.4	NBSS	71	Negative session response, Called name not present
629	35.520924	10.8.0.4	10.8.0.187	TCP	66	50490 > netbios-ssn [ACK] Seq=73 Ack=7 Win=524280 Len=0 TSval=425440370 TSecr=11948706
630	35.520999	10.8.0.4	10.8.0.187	TCP	66	50490 > netbios-ssn [FIN, ACK] Seq=73 Ack=7 Win=524280 Len=0 TSval=425440370 TSecr=11948706
631	35.521062	10.8.0.4	10.8.0.187	TCP	78	50491 > netbios-ssn [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=8 TSval=425440370 TSecr=0 SACK_PERM=1
632	35.522402	10.8.0.187	10.8.0.4	TCP	66	netbios-ssn > 50490 [ACK] Seq=7 Ack=74 Win=66560 Len=0 TSval=11948706 TSecr=425440370
633	35.522752	10.8.0.187	10.8.0.4	TCP	74	netbios-ssn > 50491 [SYN, ACK] Seq=0 Ack=1 Win=8192 Len=0 MSS=1460 WS=256 SACK_PERM=1 TSval=11948706 TSecr=4254
634	35.522765	10.8.0.4	10.8.0.187	TCP	66	50491 > netbios-ssn [ACK] Seq=1 Ack=1 Win=524280 Len=0 TSval=425440370 TSecr=11948706
635	35.531185	10.8.0.4	10.8.0.187	NBSS	138	Session request, to 10<20> from GSERRAO_MAC<00>
636	35.532248	10.8.0.187	10.8.0.4	NBSS	71	Negative session response, Called name not present
637	35.532348	10.8.0.4	10.8.0.187	TCP	66	50491 > netbios-ssn [ACK] Seq=73 Ack=7 Win=524280 Len=0 TSval=425440370 TSecr=11948707
638	35.532463	10.8.0.4	10.8.0.187	TCP	66	50491 > netbios-ssn [FIN, ACK] Seq=73 Ack=7 Win=524280 Len=0 TSval=425440370 TSecr=11948707
639	35.532577	10.8.0.4	10.8.0.187	TCP	78	50492 > netbios-ssn [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=8 TSval=425440370 TSecr=0 SACK_PERM=1
640	35.535807	10.8.0.187	10.8.0.4	TCP	66	netbios-ssn > 50491 [ACK] Seq=7 Ack=74 Win=66560 Len=0 TSval=11948708 TSecr=425440370
641	35.536057	10.8.0.187	10.8.0.4	TCP	74	netbios-ssn > 50492 [SYN, ACK] Seq=0 Ack=1 Win=8192 Len=0 MSS=1460 WS=256 SACK_PERM=1 TSval=11948708 TSecr=4254
642	35.536101	10.8.0.4	10.8.0.187	TCP	66	50492 > netbios-ssn [ACK] Seq=1 Ack=1 Win=524280 Len=0 TSval=425440370 TSecr=11948708
643	35.542716	10.8.0.4	10.8.0.187	NBSS	138	Session request, to *SMBSERVER<20> from GSERRAO_MAC<00>
644	35.543786	10.8.0.187	10.8.0.4	NBSS	71	Negative session response, Called name not present
645	35.543865	10.8.0.4	10.8.0.187	TCP	66	50492 > netbios-ssn [ACK] Seq=73 Ack=7 Win=524280 Len=0 TSval=425440370 TSecr=11948708

```
0000  00 7f 28 b8 55 78 b8 8d  12 30 5d 16 08 00 45 00   ..(.Ux.. .0]...E.
0010  00 3d 8e 7c 00 00 ff 11  19 1f 0a 08 00 04 0a 08   .=.|.... ........
0020  00 01 ed e9 00 35 00 29  a3 30 19 bd 01 00 00 01   .....5.) .0......
0030  00 00 00 00 00 00 03 77  77 77 07 6d 6f 7a 69 6c   .......w ww.mozil
```

File: "/Users/gserrao/Dropbox/pcapalyze/traf... | Packets: 3613 Displayed: 3613 Marked: 0 Load time: 0:00.584 | Profile: Default

SOURCEfire®

How to Improve

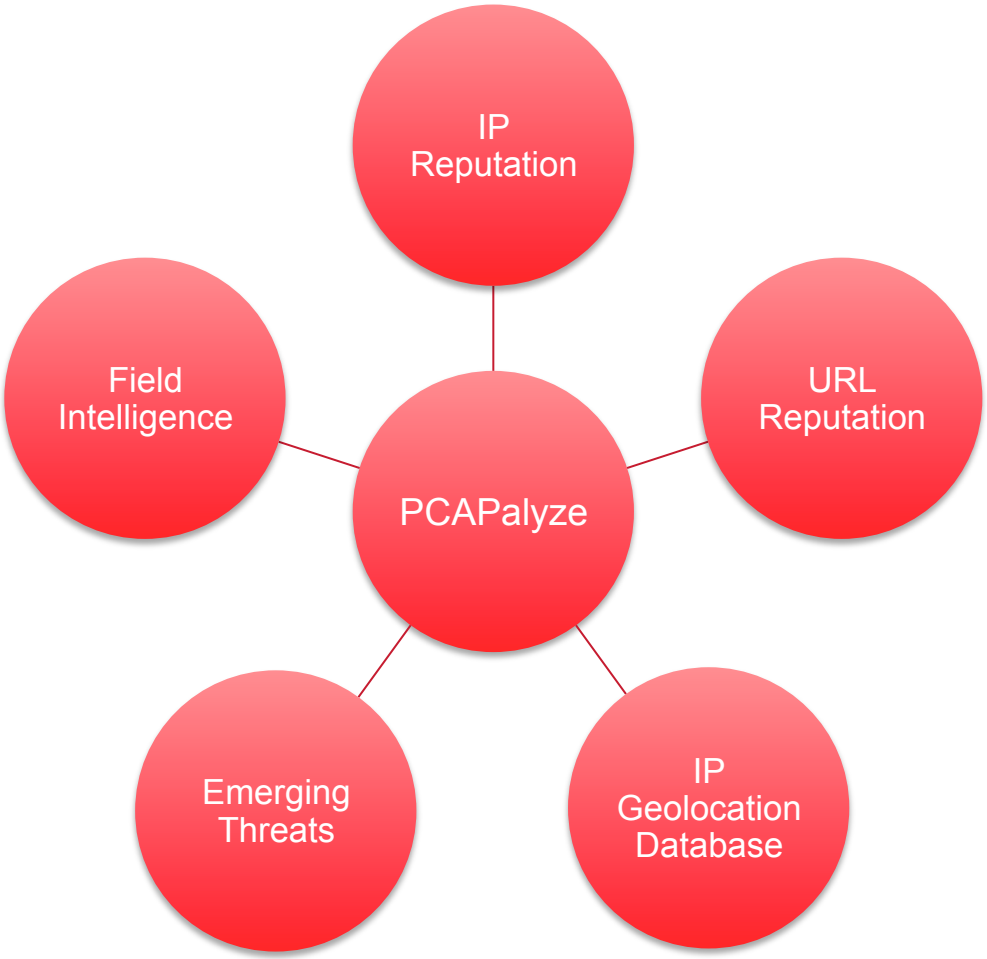
- Let's take a more proactive approach
- Increase the amount of information available to the analyst
- Increase the quality of the dissected payload
- Use automation tools
- The best methods are the most informed methods
- We need a bigger source of information

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



Information Sources, Cont.

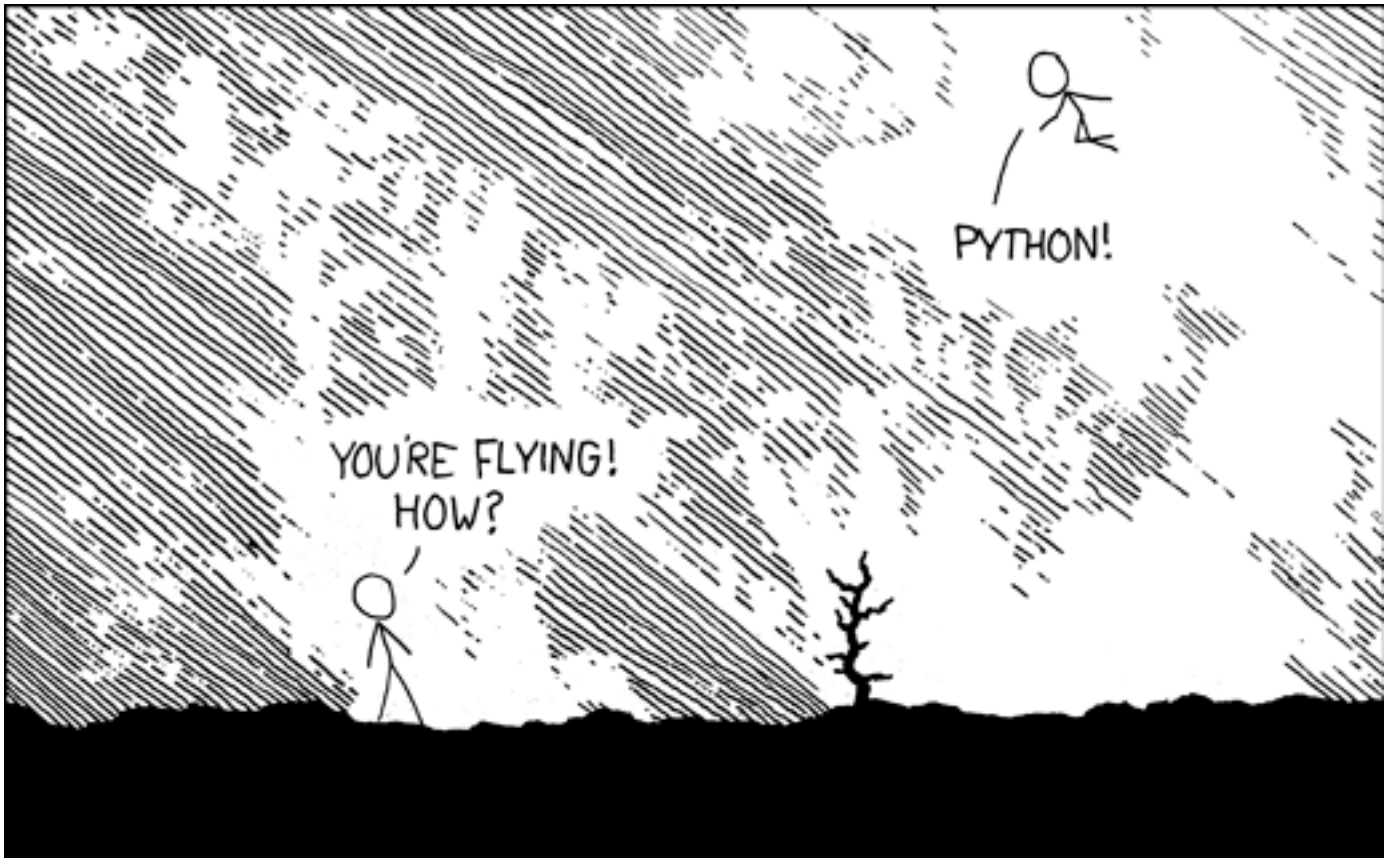
- Common
  - http://www.malwaredomains.com
  - www.mxtoolbox.com
  - https://www.dnsstuff.com/
  - http://www.siteadvisor.com/
  - https://www.phishtank.com/
- Not so common
  - Pastebin.com
  - Twitter.com

Favorite Information Source

- 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/

SOURCEfire®

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)”
…
```

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
```

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
```

SOURCEfire®

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

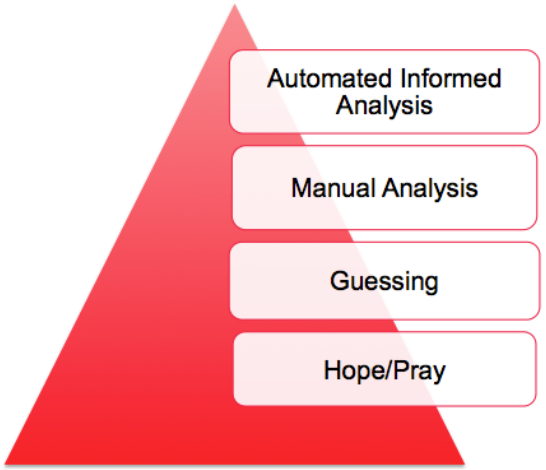
Future Development

- 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

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




```
-=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

SOURCEfire®