Endpoints Threat Feeds False Positives and You

Ryan Holeman

ziften

black hat USA 2015

Ziften

- Ziften is not a Threat Feed Provider
- Continuous endpoint visibility that allows you to rapidly view, inspect, and respond to risks and attacks
- Network data is mined at the endpoint for rich application association

Who am I

- **Director of Security R&D @ Ziften**
- **Manage threat feed integration @ Ziften**
- **Frequent conference speaker**
  - BlackHat, DEF CON, Shmoocon, etc
- **Masters degree, skateboarder, kid wrangler, python freak, analytics junky**

Talk Overview

- **Threat feed basics**
- **Feed validation**
- **False Positive Reduction**
  - Feed Enhancements
- **Exercises**

Threat Feed Types

- **Feed consumption**
  - Bulk lists
  - API lookups
- **Feed flavors**
  - Network
  - Binary
  - Vulnerability
  - User

Feed Shopping

- **How do they obtain their feeds?**
  - Sensors, aggregators, crawling, etc
  - Ask for a meeting with a technical lead
- **How often are they updated?**
- **Is there any validation?**
- **Do they provide ample documentation?**
- **Shop around. Not every feed is right for you!**

Feed Management Tools

- Proprietary Solutions
- SIEMS (Splunk, ELK, etc)
- IDS (Bro, Snort, etc)
- Combine (Alex Pinto & Kyle Maxwell)
- CRITS, MANTIS, MISP
- CIF (REN-ISAC)

Threat Feed Validation

- The following are techniques that can be used for threat feed comparison and validation

Quick Analytics

- Run some awk, grep, sort, uniq & comm
- See how many categories
- Check volume for each category
- Check dates!!!
- Look for duplicates in your threat feeds

Check Feeds Agains Traffic Samples

```
ripper@eth0:~$ comm -12 \
> <(awk -F',' '{print $1}' network_sample.csv |sort) \
> <(awk -F',' '{print $1}' feed.csv |sort) \
> |wc -l
     318
ripper@eth0:~$
```

- If you get over N hits, the feed is FP prone
- If you get no hits, the feed is really good or really bad

ziften

Manual Investigation

- What lives at those IPs?
- Are domains still active?
- Spin up a VM and poke around

Overlap Test

- comm is your best friend

```
ripper@eth0:bh2015$ comm -12 \
> <(awk -F',' '{print $1}' exercise_1_feed_1.csv |sort) \
> <(awk -F',' '{print $1}' exercise_1_feed_2.csv |sort) \
> |wc -l
     982
ripper@eth0:bh2015$
```

ziften

black hat USA 2015

False Positive Reduction

- After the fact investigation
- More detailed correlations

Ingress/Egress Correlation

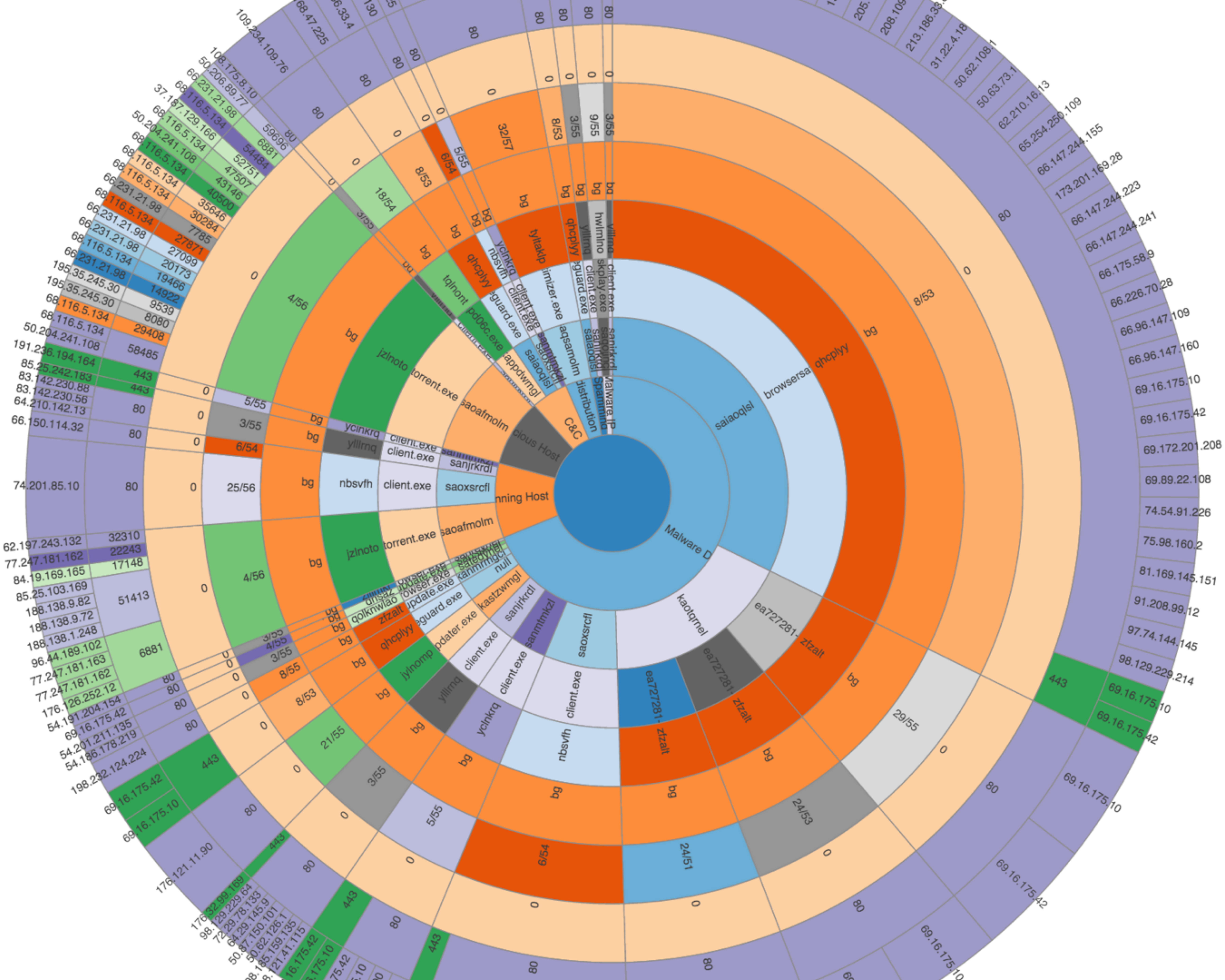
- **Classify your source and feed data into ingress & egress buckets**
  - Combine does a great job at this
  - Typically based on the type of threat
- **All feeds need to do this by default**

Application Association

- **System logs**
  - WFP for Windows
  - ptrace for OSX
  - strace for *nix
- **Watch for hits against**
  - System level processes
  - Process in memory but not on disk

Alert Association

- **IDS alerts**
- **UPNP or no firewall traffic correlation**
- **User activity alerts**
- **Binary alert correlation**
  - Application name or preferably md5/sha hash
  - Source & Destination IP



Malware D
Spamming
Malware IP
distribution
C&C
nning Host
cious Host
saiaoqlsl
browsersa
kaotqmel
ea727281-
zfzalt
qhcplyy
bg
saoxsrcfl
client.exe
nbsvfh
jzlnoto
torrent.exe
saoafmolm
sanjrkrdl
ycinkrq
yllirnq
tqlnont
tyltaklp
appdwmgl
aqsamolm
pdater.exe
kastzwmgl
null
8/53
32/57
29/55
24/53
24/51
6/54
5/55
3/55
21/55
4/56
25/56
18/54
9/55
80
443
0
74.201.85.10
69.16.175.10
69.16.175.42
69.172.201.208
69.89.22.108
74.54.91.226
75.98.160.2
81.169.145.151
91.208.99.12
97.74.144.145
98.129.229.214
62.197.243.132
77.247.181.162
84.19.169.165
66.150.114.32
109.234.109.76
176.121.11.90
198.232.124.224

DNS & URL Associations

- Provides a more accurate network to feed correlation
- Harder to find and typically smaller feed sources

Typical IP & DNS Lookups

- **host**
  - Check if domains still resolve
- **dig**
  - Do DNS lookup or rev IP lookip
- **whois**
  - Check domain or IP for hosting services, parking services, DDoS services, etc

Forward & Passive DNS

- Gives you an idea of how many domains are hosted at an IP address
- Shows you other domains hosted at an IP address
- Providers
  - Rapid7's project Sonar, OTX, VT, Bing ip search, and paid services

Alexa Ranking

- Check your hits against Alexa to see how high they rank
- Check your feed against Alexa to see how many entities rank in Alexa's top 100/1000/10000 domains
- You may have to do some bulk IP resolution and forward DNS lookups
- Some frameworks (CIF) will allow you to whitelist

Exercises

- **Workshop exercises**
  - https://github.com/hackgnar/bh2015
- **Contact info**
  - email: ryan.holeman@ziften.com
  - twitter: @hackgnar