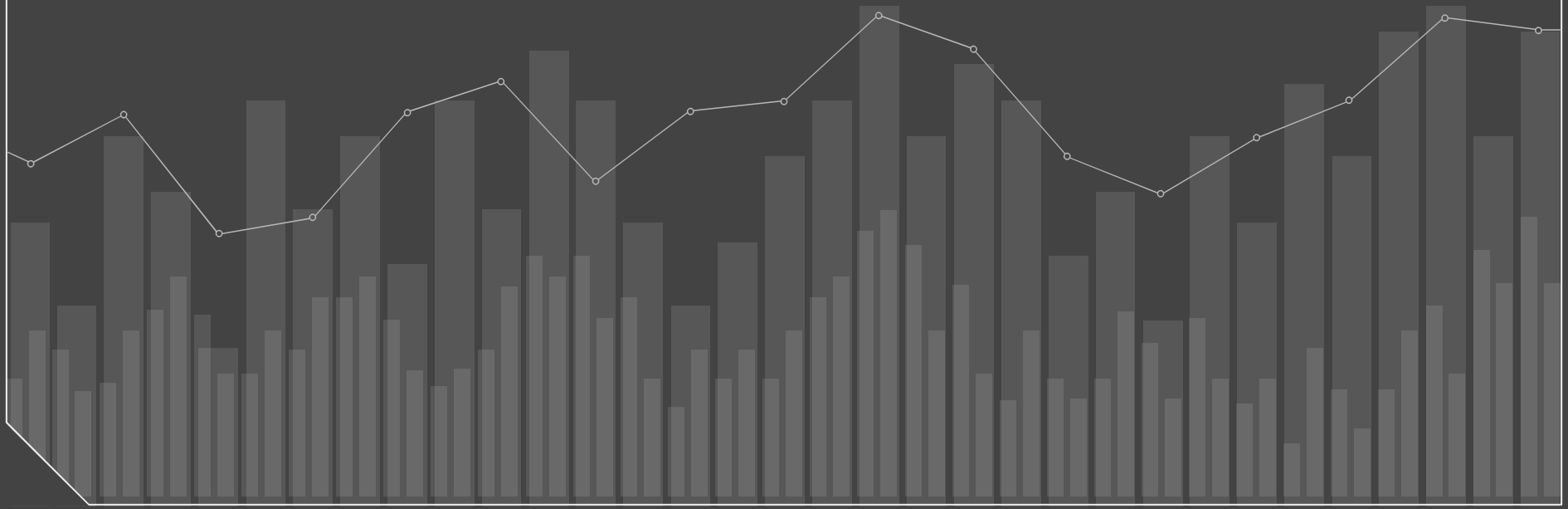
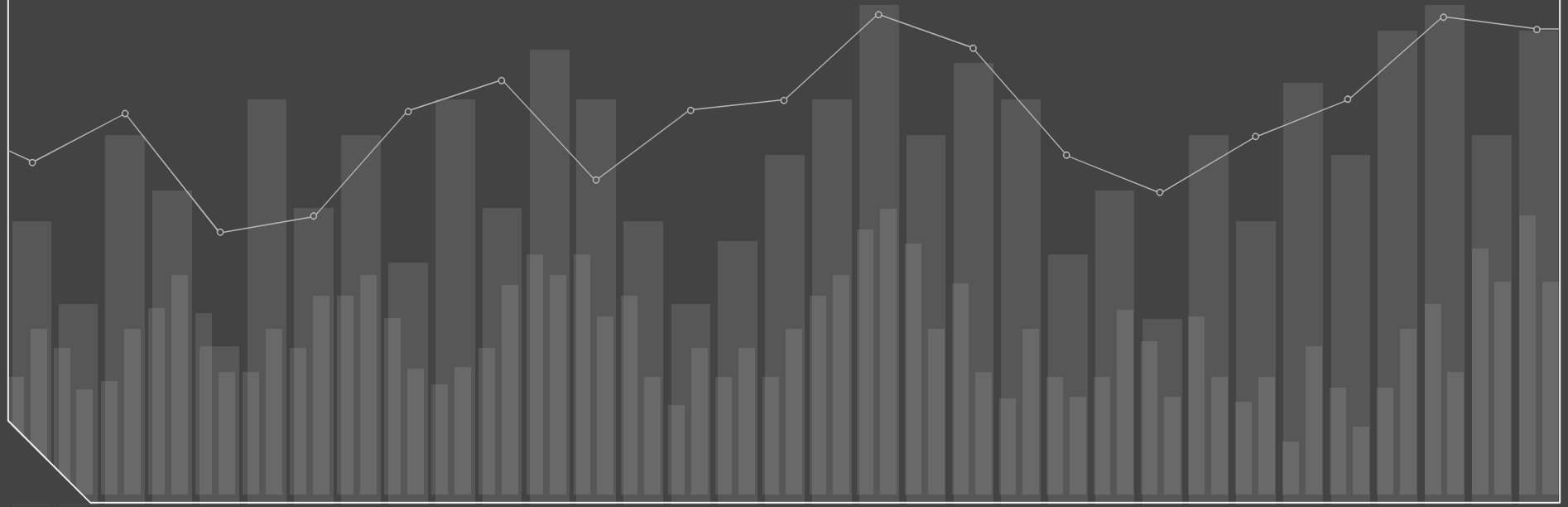
# Red Mirror:
# Bringing Telemetry to Red Teaming



# # whoami

- Red Team, Pen Testing, & Vulnerability Management Lead @ Fortune 100
- Wisconsin CCDC Red Team
- ELK n00b
- Twitter: @ztgrace

# Origin Story



https://github.com/ztgrace/pwnboard

# Wisconsin CCDC

## PWNboard

| Hosts | Team 1 | Team 2 | Team 3 | Team 4 | Team 5 | Team 6 | Team 7 | Team 8 | Team 9 | Team 10 |
|---|---|---|---|---|---|---|---|---|---|---|
| 2012 | 172.25.21.3 host: RT5, session: XXBVWG1P, type: empire last seen: 5m | 172.25.22.3 host: RT2, session: P2X6KHBS, type: empire last seen: 4m | 172.25.23.3 host: RT4, session: ATLJNMFS, type: empire last seen: 1m | 172.25.24.3 host: RT4, session: W1LXZQG0, type: empire last seen: 4m | 172.25.25.3 host: RT3, session: X7D2LY2Z, type: empire last seen: 4m | 172.25.26.3 | 172.25.27.3 host: RT5, session: 86, type: meterpreter last seen: 0m | 172.25.28.3 host: RT1, session: 51, type: meterpreter last seen: 0m | 172.25.29.3 | 172.25.30.3 |
| FILESERVER1 | 172.25.21.9 host: RT1, session: 90, type: meterpreter last seen: 0m | 172.25.22.9 host: RT1, session: WWON03Q7, type: empire last seen: 6m | 172.25.23.9 host: RT1, session: root, type: backdoor last seen: 9m | 172.25.24.9 host: RT4, session: 90, type: meterpreter last seen: 0m | 172.25.25.9 host: RT5, session: 69, type: meterpreter last seen: 0m | 172.25.26.9 host: RT5, session: OL6OWPDU, type: empire last seen: 8m | 172.25.27.9 | 172.25.28.9 host: RT3, session: 50, type: meterpreter last seen: 0m | 172.25.29.9 host: RT2, session: OM29GKPH, type: empire last seen: 2m | 172.25.30.9 host: RT4, session: adminnobody, type: backdoor last seen: 2m |
| e-comm | 172.25.21.11 host: RT1, session: root, type: backdoor last seen: 3m | 172.25.22.11 host: RT4, session: EOBKRYBO, type: empire last seen: 8m | 172.25.23.11 host: RT4, session: 39, type: meterpreter last seen: 0m | 172.25.24.11 | 172.25.25.11 | 172.25.26.11 | 172.25.27.11 host: RT1, session: 18, type: meterpreter last seen: 0m | 172.25.28.11 host: RT4, session: adminnobody, type: backdoor last seen: 6m | 172.25.29.11 host: RT3, session: TZE70I5P, type: empire last seen: 7m | 172.25.30.11 host: RT5, session: 51, type: meterpreter last seen: 0m |
| Ubuntu DNS | 172.25.21.23 host: RT5, session: BMAN1WSF, type: empire last seen: 10m | 172.25.22.23 host: RT2, session: root, type: backdoor last seen: 2m | 172.25.23.23 host: RT2, session: 77, type: meterpreter last seen: 0m | 172.25.24.23 host: RT4, session: QZ9XFDJZ, type: empire last seen: 3m | 172.25.25.23 | 172.25.26.23 host: RT3, session: OXHGRHDU, type: empire last seen: 3m | 172.25.27.23 host: RT1, session: XBDXR71G, type: empire last seen: 7m | 172.25.28.23 host: RT4, session: adminnobody, type: backdoor last seen: 6m | 172.25.29.23 host: RT1, session: adminnobody, type: backdoor last seen: 1m | 172.25.30.23 host: RT1, session: root, type: backdoor last seen: 10m |
| DC | 172.25.21.27 host: RT5, session: JU8TZ6RC, type: empire last seen: 5m | 172.25.22.27 host: RT2, session: 87, type: meterpreter last seen: 0m | 172.25.23.27 host: RT1, session: QESSQS18, type: empire last seen: 3m | 172.25.24.27 | 172.25.25.27 host: RT5, session: root, type: backdoor last seen: 3m | 172.25.26.27 host: RT3, session: GX4WJZYS, type: empire last seen: 8m | 172.25.27.27 host: RT1, session: adminnobody, type: backdoor last seen: 10m | 172.25.28.27 host: RT1, session: root, type: backdoor last seen: 2m | 172.25.29.27 host: RT3, session: root, type: backdoor last seen: 9m | 172.25.30.27 |
| mail | 172.25.21.39 host: RT5, session: E2S2V34B, type: empire last seen: 2m | 172.25.22.39 host: RT5, session: adminnobody, type: backdoor last seen: 7m | 172.25.23.39 host: RT1, session: 67, type: meterpreter last seen: 0m | 172.25.24.39 host: RT5, session: adminnobody, type: backdoor last seen: 6m | 172.25.25.39 host: RT2, session: 12, type: meterpreter last seen: 0m | 172.25.26.39 | 172.25.27.39 host: RT1, session: adminnobody, type: backdoor last seen: 6m | 172.25.28.39 host: RT5, session: root, type: backdoor last seen: 10m | 172.25.29.39 | 172.25.30.39 host: RT2, session: 74, type: meterpreter last seen: 0m |
| PAN | 172.25.21.100 | 172.25.22.100 | 172.25.23.100 | 172.25.24.100 | 172.25.25.100 | 172.25.26.100 | 172.25.27.100 | 172.25.28.100 | 172.25.29.100 | 172.25.30.100 |

Vyrus
@vyrus001

Allready modified both your changes to talk to elasticsearch and work with my kibana dash, thanks!!!

Mar 4

Sweet, np

Mar 5

Is your ELK for an operational dashboard? Or reporting of activity to teams?

Mar 5

yes

all the data goes in, [redacted] data from the "beats" [redacted] and then a bunch of kibana dashboards on the front end

# beats/libbeat

- Lightweight data collection and shipping
- Small, fast and no external dependencies (thanks  )
- https://www.elastic.co/products/beats
- https://www.elastic.co/guide/en/beats/libbeat/current/community-beats.html
- https://github.com/elastic/beats
- Community Beats ~70

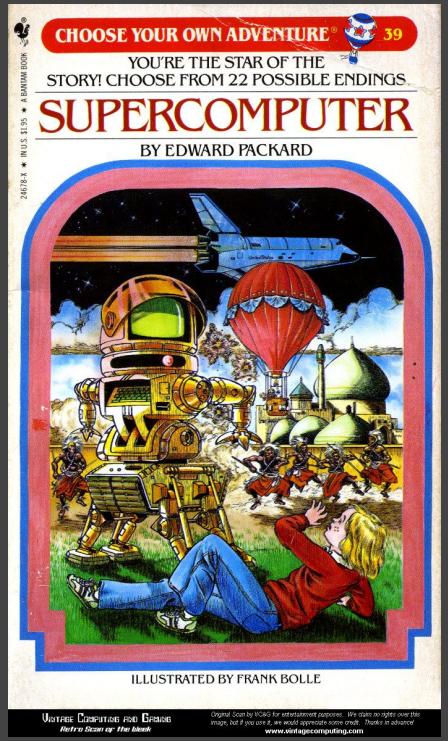
# Why Telemetry?

The goal of the red team should be to make the blue team:

# What this talk’s not:

~~apt-get install redteam-telemetry~~

# More like:



# Prior Art

https://vincentyiu.co.uk/cobaltsplunk/

**Vincent Yiu**

SYON (斯圆安全)

## CobaltSplunk

24th Aug 2018 on Attack Infrastructure

TLDR; use Splunk as a central log database and analysis system for offensive infrastructure logs. In many engagements, you will want accurate logging across multiple RAT systems, phishing web servers, mail systems, and more. Currently only supports Cobalt Strike, but will be looking at supporting Empire, Pupy, Metasploit, Apache, Nginx, and more!

# ...and as of ~4 hours ago


https://github.com/outflanknl/RedELK

# Typical Session Logging

bash->script

msfconsole -> spool

```
echo “spool /root/.msf4/msfconsole.log” >> ~/.msf4/msfconsole.rc
```

Empire - agents.log

Cobalt Strike - beacon logs

# Network Logging

tcpdump -ni eth0 -w hax.pcap

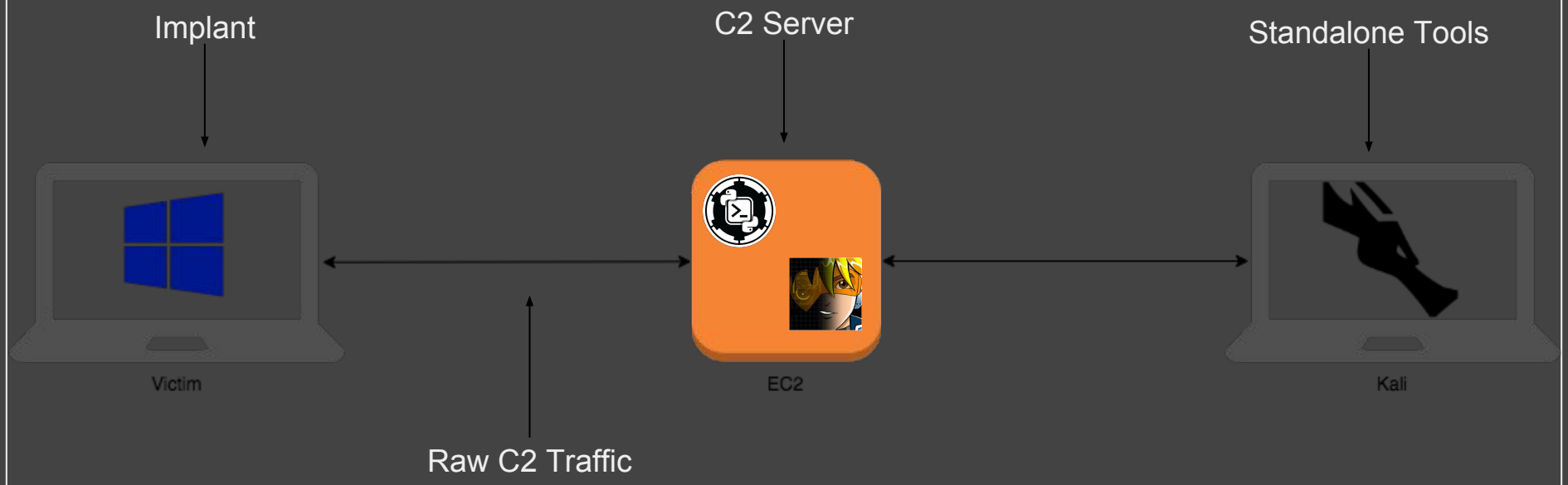
# What Could Go Wrong?

You forgot to  start the loggers...

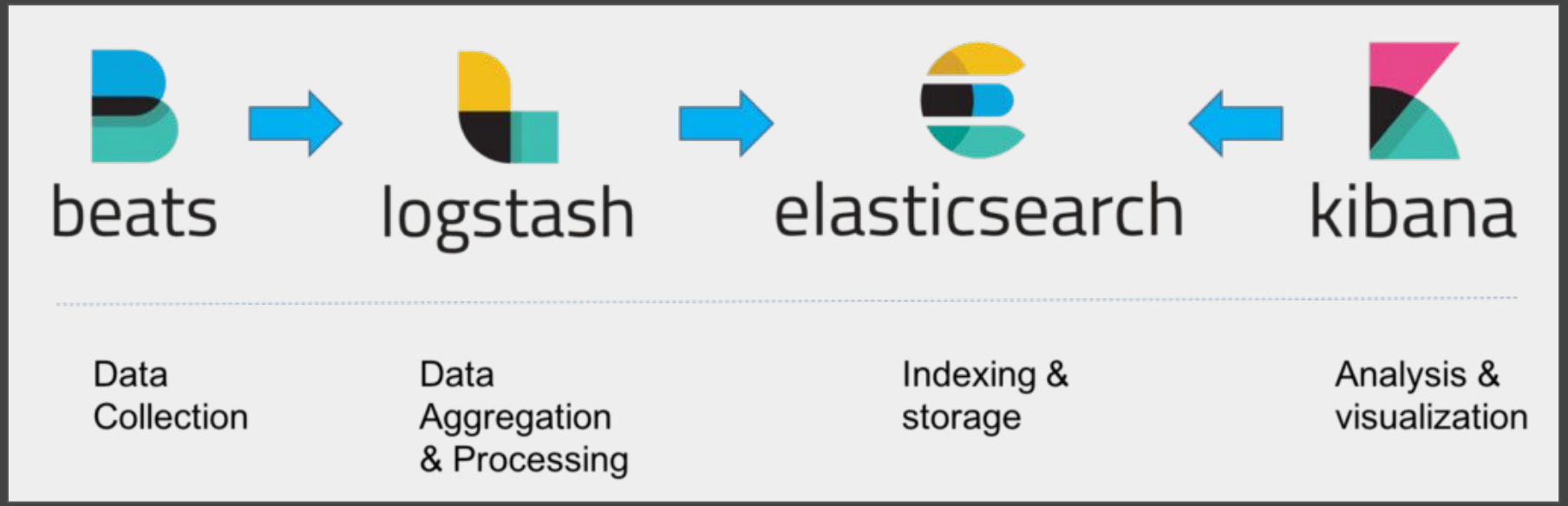
# What’s Missing?

- Real-Time monitoring
- Easily construct timelines across all infrastructure
- Sane querying for events instead of grepping script log files
- Data-driven prioritization
- Mean Time to X

# What Data to Collect?



# ELK Stack

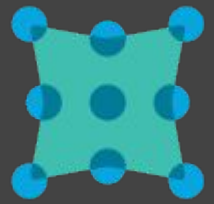

beats
logstash
elasticsearch
kibana
Data Collection
Data Aggregation & Processing
Indexing & storage
Analysis & visualization

# What beats are useful for RTT?

- Packetbeat
- Filebeat
- Connbeat
- Metricbeat

# Packetbeat

- Decodes and stores common network protocols (DNS, HTTP, MySQL)
- Can capture flows
- Use cases:
  - Great match for C2 infrastructure
- Limitations:
  - Only supported protocols are logged



https://www.elastic.co/products/beats/packetbeat

# Packetbeat Config

```
packetbeat.interfaces.device: eth0
packetbeat.flows:
  enabled: false
  timeout: 30s
  period: 10s
packetbeat.protocols:
- type: dns
  enabled: true
  ports: [53]
  include_authorities: true
  include_additionals: true
  send_request:  true
  send_response: true
  transaction_timeout: 10s
- type: http
  enabled: true
  ports: [80]
  send_headers: true
  send_all_headers: true
  include_body_for: ["text/plain", "text/xml", "audio/mp4"]
  send_request: true
  send_response: true
```

# Connbeat

- Can monitor all TCP connections vs Packetbeat's specific protocols
- Use a Logstash mutate filter to clean up sensitive data
- Can capture CLI
- Limitations
  - Only *full* TCP connections are logged
  - No UDP


```
"local_ip": "192.168.2.139",
"local_port": 44432,
"local_process": {
  "binary": "",
  "cmdline": "nmap -A -sT -T4 -n -v 192.168.1.0/24",
  "environ": [
    "SSH_CONNECTION=192.168.2.1 55386 192.168.2.139 22",
    "LESSCLOSE=/usr/bin/lesspipe %s %s",
    "LANG=en_US.UTF-8",
    "AWS_SECRET_ACCESS_KEY=wJalrXUtnFEMI/K7MDENG/bPxRfiCYzEXAMPLEKEY",
    "JAVA_HOME=/usr/lib/jvm/java-8-oracle",
    "J2SDKDIR=/usr/lib/jvm/java-8-oracle",
    "XDG_SESSION_ID=2",
    "DERBY_HOME=/usr/lib/jvm/java-8-oracle/db",
    "USER=root",
    "LSCOLORS=gxBxhxDxfxhxhxhxhxcxcx",
    "PWD=/root",
    "HOME=/root",
    "J2REDIR=/usr/lib/jvm/java-8-oracle/jre",
    "SSH_CLIENT=192.168.2.1 55386 22",
    "TMUX=/tmp//tmux-0/default,697,0",
    "SSH_TTY=/dev/pts/0",
    "MAIL=/var/mail/root",
    "TERM=screen-256color",
    "SHELL=/bin/bash",
    "TMUX_PANE=%3",
    "AWS_ACCESS_KEY_ID=AKIAIOSFODNN7EXAMPLE",
    "SHLVL=2",
    "LOGNAME=root",
    "DBUS_SESSION_BUS_ADDRESS=unix:path=/run/user/0/bus",
    "XDG_RUNTIME_DIR=/run/user/0",
    "PATH=/usr/local/sbin:/usr/local/bin:/usr/sbin:/usr/bin:/sbin:/bin:/
    "LESSOPEN=| /usr/bin/lesspipe %s",
    "_=/usr/bin/nmap"
  ],
  "pid": 63966
},
"remote_ip": "192.168.1.17",
"remote_port": 5900,
"type": "connbeat"
```


https://github.com/raboof/connbeat

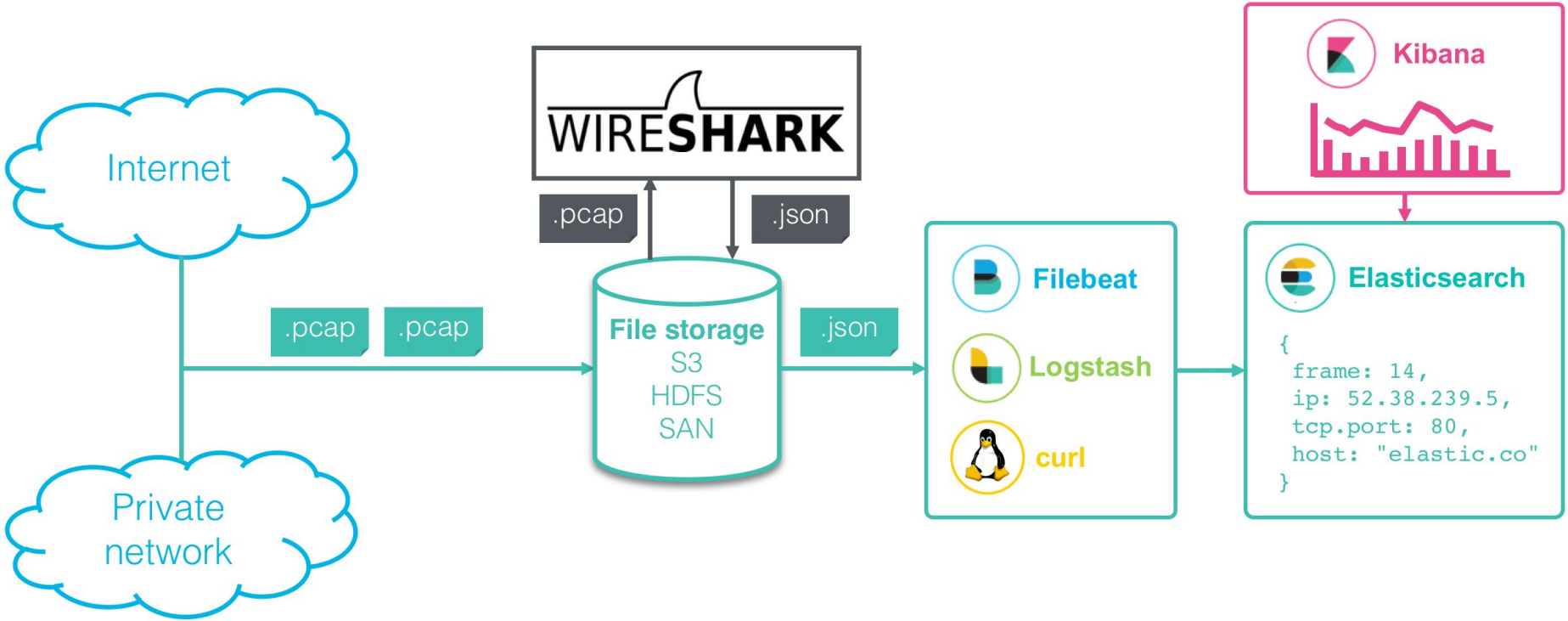
# Metricbeat

- Monitors system/app health
- Logs network data using socket module
- Only monitors full TCP connections
- Use cases:
  - TCP socket C2 monitoring (Metasploit)
  - Monitoring anything TCP
  - Network I/O

Table JSON

| | | |
|---|---|---|
| @timestamp | | October 1st 2018, 21:47:06.636 |
| t | _id | q-SsMmYB3TPggOS6BjPd |
| t | _index | metricbeat-6.4.1-2018.10.01 |
| # | _score | - |
| t | _type | doc |
| t | beat.hostname | kali |
| t | beat.name | kali |
| t | beat.version | 6.4.1 |
| t | host.name | kali |
| t | metricset.module | system |
| t | metricset.name | socket |
| # | metricset.rtt | 28,431 |
| t | system.socket.direction | outgoing |
| t | system.socket.family | ipv4 |
| | system.socket.local.ip | 192.168.2.139 |
| # | system.socket.local.port | 38,168 |
| t | system.socket.process.cmdline | nmap -A -sT -T4 -n -v 192.168.1.0/24 |
| t | system.socket.process.command | nmap |
| t | system.socket.process.exe | /usr/bin/nmap |
| # | system.socket.process.pid | 107,557 |
| | system.socket.remote.ip | 192.168.1.62 |
| # | system.socket.remote.port | 2,105 |
| # | system.socket.user.id | 0 |
| t | system.socket.user.name | root |

# tshark + filebeat



# Direct tshark->json setup

```
cat /etc/supervisor/conf.d/tshark.conf
[program:tshark]
directory=/var/log/pcaps/
command=tshark -i eth0 -f 'not (port 9200 and host 127.0.0.1)' -T ek -x > tshark-$(date +"%Y-%m-%d").json
autostart=true
autorestart=true
```

*Warning: Very memory intensive*

# tcpdump->tshark->json

```
tcpdump -ni eth0 -w $(date +"%Y-%m-%d") -G not host elasticsearch
```

Or

```
tshark -a filesize:10000 -i eth0 -w $(date +"%Y-%m-%d") -f 'not host elasticsearch'
```

then:

```
for i in $(ls); do tshark -r $i -T ek -x > "${i}.json"; done
```

Or

Use the `-z postrotate` command in tcpdump

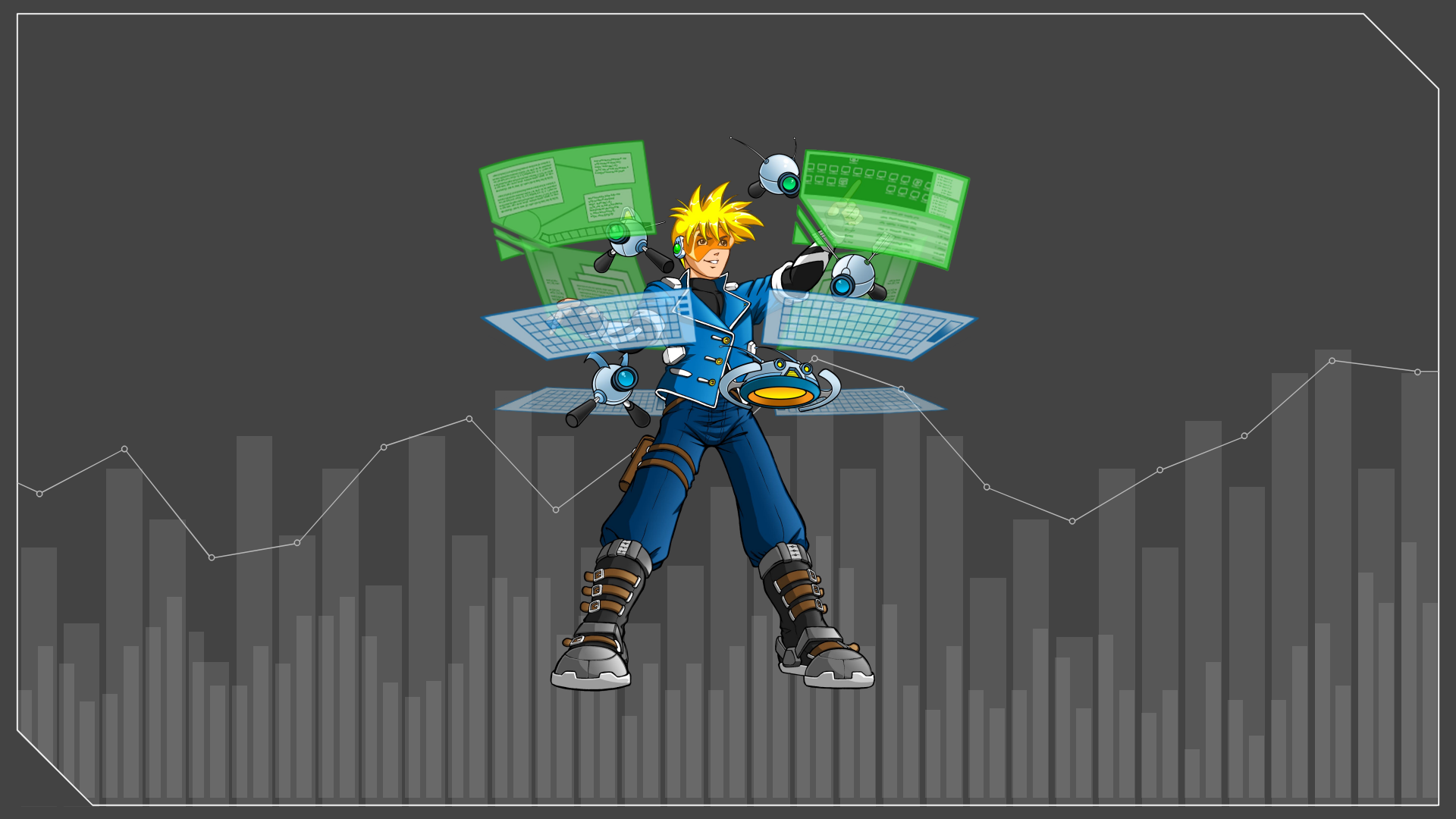
# tshark+Filebeat setup

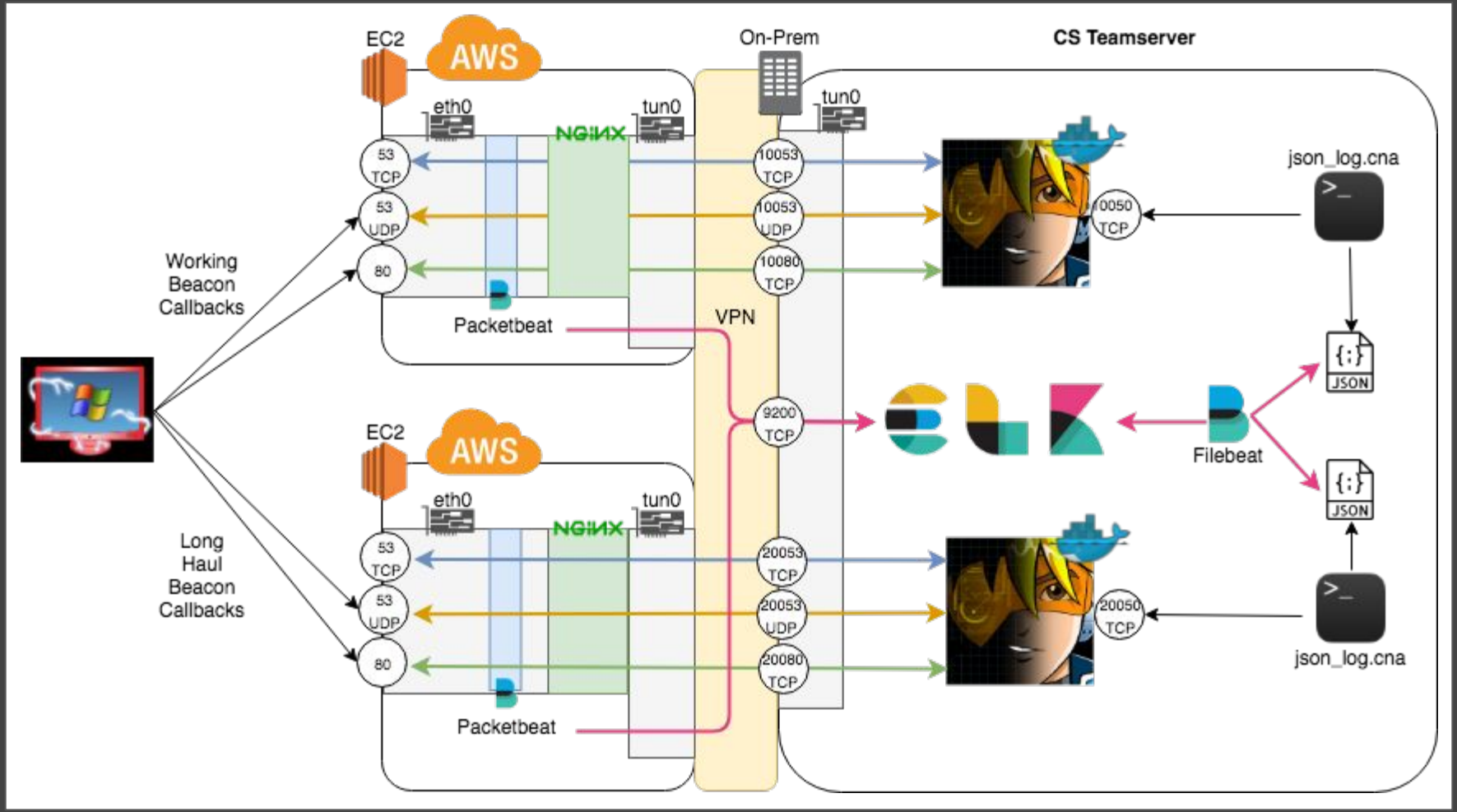
```
# cat /etc/filebeat/filebeat.yml
filebeat.prospectors:
- input_type: log
  paths:
    - "/var/log/pcaps/packets*.json"
  document_type: "pcap_file"
  json.keys_under_root: true

processors:
 - drop_event:
     when:
       equals:
         index._type: "pcap_file"

output.elasticsearch:
  hosts: ["192.168.2.140:9200"]
  template.enabled: false
```

# tshark + filebeat

- Advantages
  - Can use filters to ignore traffic
- Warning: *Exclude Elasticsearch/Logstash traffic from your capture!*
- Limitations:
  - Can’t tie traffic to commands/progs

https://www.elastic.co/blog/analyzing-network-packets-with-wireshark-elasticsearch-and-kibana






https://zachgrace.com/posts/cobalt_strike_redirectors/

# Cobalt Strike

Logs are broken down by day, host and type

```
/opt/cobaltstrike
# tree logs/180605
logs/180605
├── 172.25.108.158
│   ├── beacon_15824.log
│   └── beacon_20341.log
├── 172.31.45.243
│   ├── beacon_59349.log
│   └── beacon_9559.log
├── events.log
├── unknown
│   ├── beacon_15824.log
│   ├── beacon_20341.log
│   ├── beacon_59349.log
│   └── beacon_9559.log
└── weblog.log

3 directories, 10 files
```

# Missing Artifact Data

- Artifact data is used to generate the TTP report
- Not logged?

# CS Structured Logging a.k.a. JSON Logging

- Log desired events as single-line JSON
- Import data with Filebeat and custom field mapping
- Add additional metadata


LIVE DEMO!
WHAT COULD GO WRONG?

# Logging Empire

- Can use packetbeat the same way as CS
- Unstructured logs in `Empire/downloads/<agent>/agent.log`

```
2018-09-24 02:25:21 :
Tasked agent to run shell command whoami

2018-09-24 02:25:23 :
redlab\redadmin
^M..Command execution completed.

2018-09-24 02:29:55 :
Tasked agent to run module powershell/collection/screenshot

2018-09-24 02:29:58 :
Output saved to ./downloads/9LD4ST7U/screenshot/DC1_2018-09-24_02-29-58.png

2018-09-24 02:30:55 :
Tasked agent to run shell command ipconfig

2018-09-24 02:31:00 :
Windows IP Configuration


Ethernet adapter Local Area Connection:

   Connection-specific DNS Suffix  . : localdomain
   Link-local IPv6 Address . . . . . : fe80::c82:e391:3cfe:78e9%11
   IPv4 Address. . . . . . . . . . . : 192.168.2.137
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . : 192.168.2.2

Tunnel adapter isatap.localdomain:

   Media State . . . . . . . . . . . : Media disconnected
   Connection-specific DNS Suffix  . : localdomain

^M..Command execution completed.

2018-09-24 02:48:28 :
```

# Parsing agent.log with Logstash

Define a grok pattern for the timestamp:

EMPIRETS %{YEAR}-%{MONTHNUM}-%{MONTHDAY} %{HOUR}:%{MINUTE}:%{SECOND}

Match the pattern and grab all data until next timestamp:

```
multiline {
   pattern => "^EMPIRETS"
   negate => true
   what => "next"
 }
```

**2018-09-24 02:23:45 : [*] Agent info: nonce 4670631711105946 jitter 0.0 servers None internal_ip 192.168.2.137 working_hours session_key R@P$9x^K[_tHdB65mrn7w(qjc:;s&F>1 children None checkin_time 2018-09-24 02:23:44 hostname DC1 id 1 delay 5 username REDLAB\redadmin kill_date parent None process_name powershell listener http process_id 1892 profile /admin/get.php,/news.php,/login/process.php|Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko os_details Microsoft Windows Server 2008 R2 Standard lost_limit 60 taskings None name 9LD4ST7U language powershell external_ip 70.92.244.223 session_id 9LD4ST7U lastseen_time 2018-09-24 02:23:44 language_version 2 high_integrity 1 [+] Agent 9LD4ST7U now active:**

**MATCHED**

| | |
|---|---|
| after match: | [*] Agent info: nonce 4670631711105946 jitter 0.0 servers None internal_ip 192.168.2.137 working_hours session_key R@P$9x^K[_tHdB65mrn7w(qjc:;s&F>1 children None checkin_time 2018-09-24 02:23:44 hostname DC1 id 1 delay 5 username REDLAB\redadmin kill_date parent None process_name powershell listener http process_id 1892 profile /admin/get.php,/news.php,/login/process.php\|Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko os_details Microsoft Windows Server 2008 R2 Standard lost_limit 60 taskings None name 9LD4ST7U language powershell external_ip 70.92.244.223 session_id 9LD4ST7U lastseen_time 2018-09-24 02:23:44 language_version 2 high_integrity 1 [+] Agent 9LD4ST7U now active: |

**2018-09-24 02:25:21 : Tasked agent to run shell command whoami**

**MATCHED**

| | |
|---|---|
| after match: | Tasked agent to run shell command whoami |

**2018-09-24 02:25:23 : redlab\redadmin ^M..Command execution completed.**

**MATCHED**

| | |
|---|---|
| after match: | redlab\redadmin ^M..Command execution completed. |

**2018-09-24 02:29:55 : Tasked agent to run module powershell/collection/screenshot**

**MATCHED**

| | |
|---|---|
| after match: | Tasked agent to run module powershell/collection/screenshot |

**2018-09-24 02:29:58 : Output saved to ./downloads/9LD4ST7U/screenshot/DC1_2018-09-24_02-29-58.png**

**MATCHED**

| | |
|---|---|
| after match: | Output saved to ./downloads/9LD4ST7U/screenshot/DC1_2018-09-24_02-29-58.png |

**2018-09-24 02:30:55 : Tasked agent to run shell command ipconfig**

**MATCHED**

| | |
|---|---|
| after match: | Tasked agent to run shell command ipconfig |

# Adding MITRE ATT&CK Data

attck_empire by Daniel Stepanic - https://github.com/dstepanic/attck_empire

- Maps empire module execution to Tactic IDs
- Outputs data as a json file for MITRE ATT&CK Navigator
- Could be converted to a LS plugin or HTTP server for enrichment

# Approach

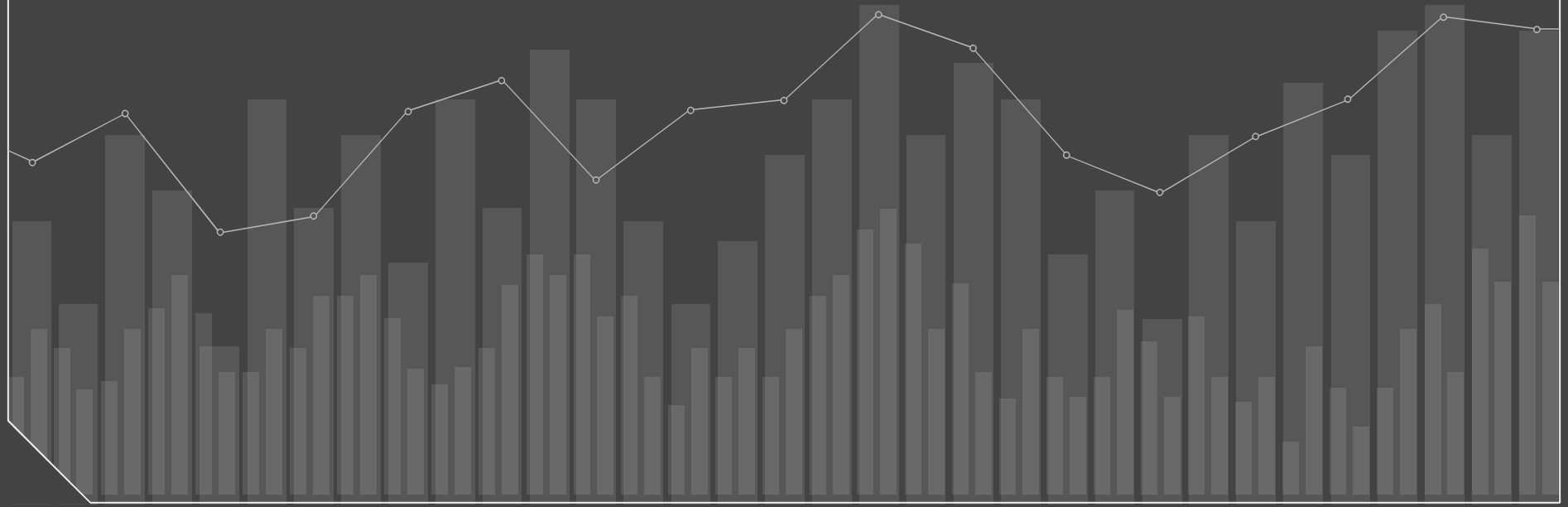
- Parse ~/.msf4 logs with Logstash
- Build a custom structured logger like my CS json_log.cna using the on_* events

# Web/BurpSuite

Web Audit Search Engine (WASE) by Thomas Patzke (@blubbfiction)

- https://github.com/thomaspatzke/WASE

# Outcomes



# Infrastructure Troubleshooting

# Operational Security

- Monitor who’s talking to your infrastructure
- Figure out where zombie beacons are coming from

Dashboard / OPSEC

Full screen | Share | Clone | Edit | Auto-refresh | April 1st 2018, 00:00:00.000 to June 1st 2018, 23:59:59.999

Search... (e.g. status:200 AND extension:PHP) Options

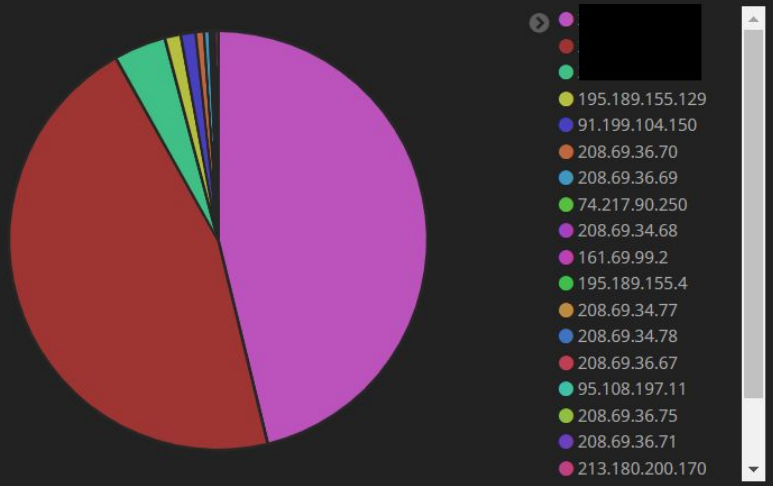
Add a filter +

Beacons Table

Legit C2

| client_ip: Descending | | Count |
|---|---|---|
| [redacted] | | 22,338 |
| [redacted] | | 22,075 |
| [redacted] | | 1,950 |
| 195.189.155.129 | BitDefender | 605 |
| 91.199.104.150 | BitDefender | 557 |
| 208.69.36.70 | OpenDNS | 309 |
| 208.69.36.69 | OpenDNS | 213 |
| 74.217.90.250 | Palo Alto | 96 |
| 208.69.34.68 | OpenDNS | 16 |

DNS Beacon Pie Chart




I'M
WATCHING YOU

# Monitor OPSEC

OPSEC Monitoring | 44 hits | New | Save | Open | Share | Reporting | Auto-refresh | October 1st 2018, 05:15:58.184 to October 6th 2018, 07:26:02.757

type:dns [redacted] | Options

Add a filter +

packetbeat*

Selected Fields

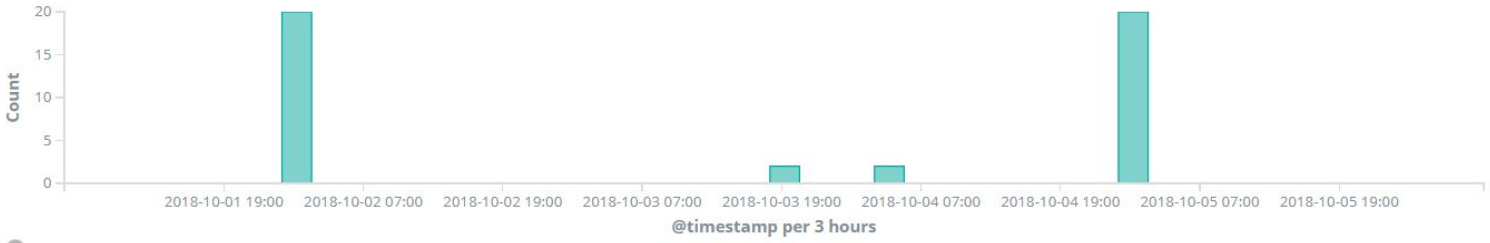
- t client_ip
- t dns.response_code

Available Fields

Popular

- t _type
- client_geoip.location
- t dns.op_code
- t dns.question.name
- t dns.question.type

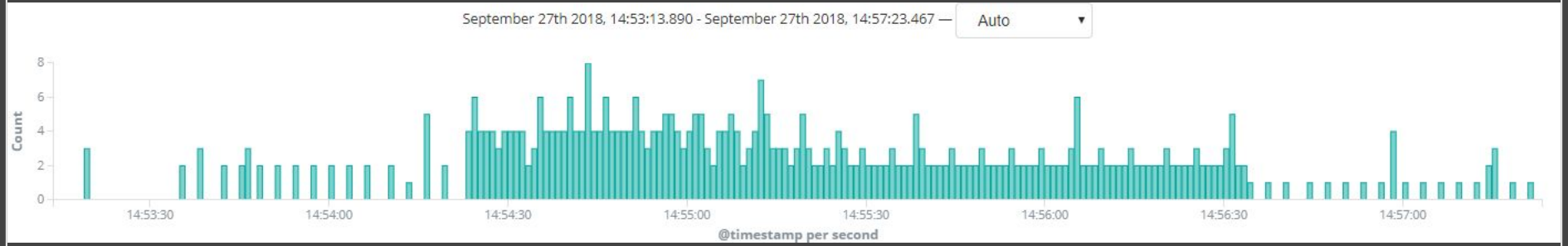
October 1st 2018, 05:15:58.184 - October 6th 2018, 07:26:02.757 — Auto



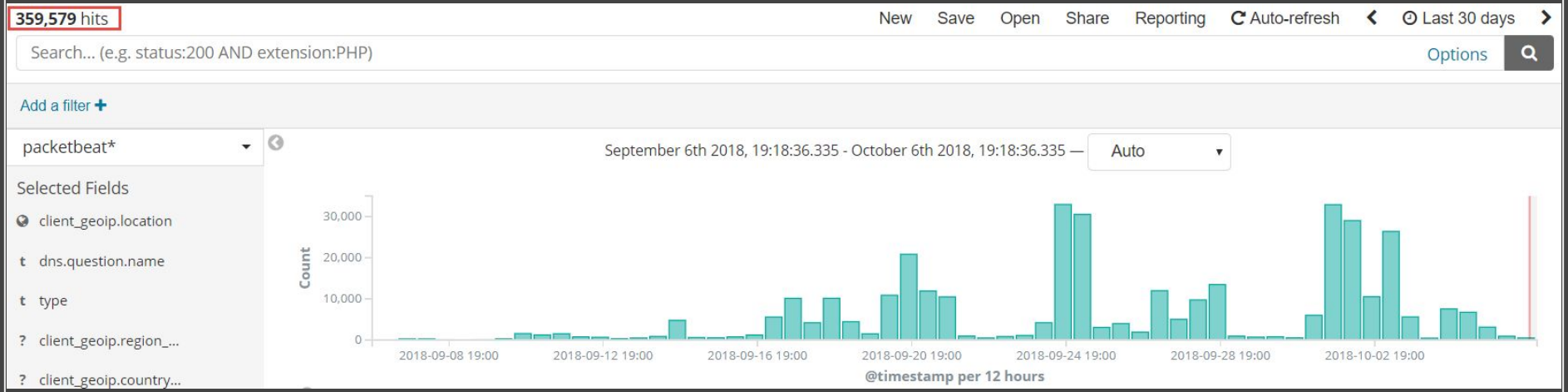

| Time | dns.response_code | client_ip |
|---|---|---|
| October 2nd 2018, 02:28:42.079 | [redacted] | [redacted] |
| October 2nd 2018, 02:28:39.637 | | |

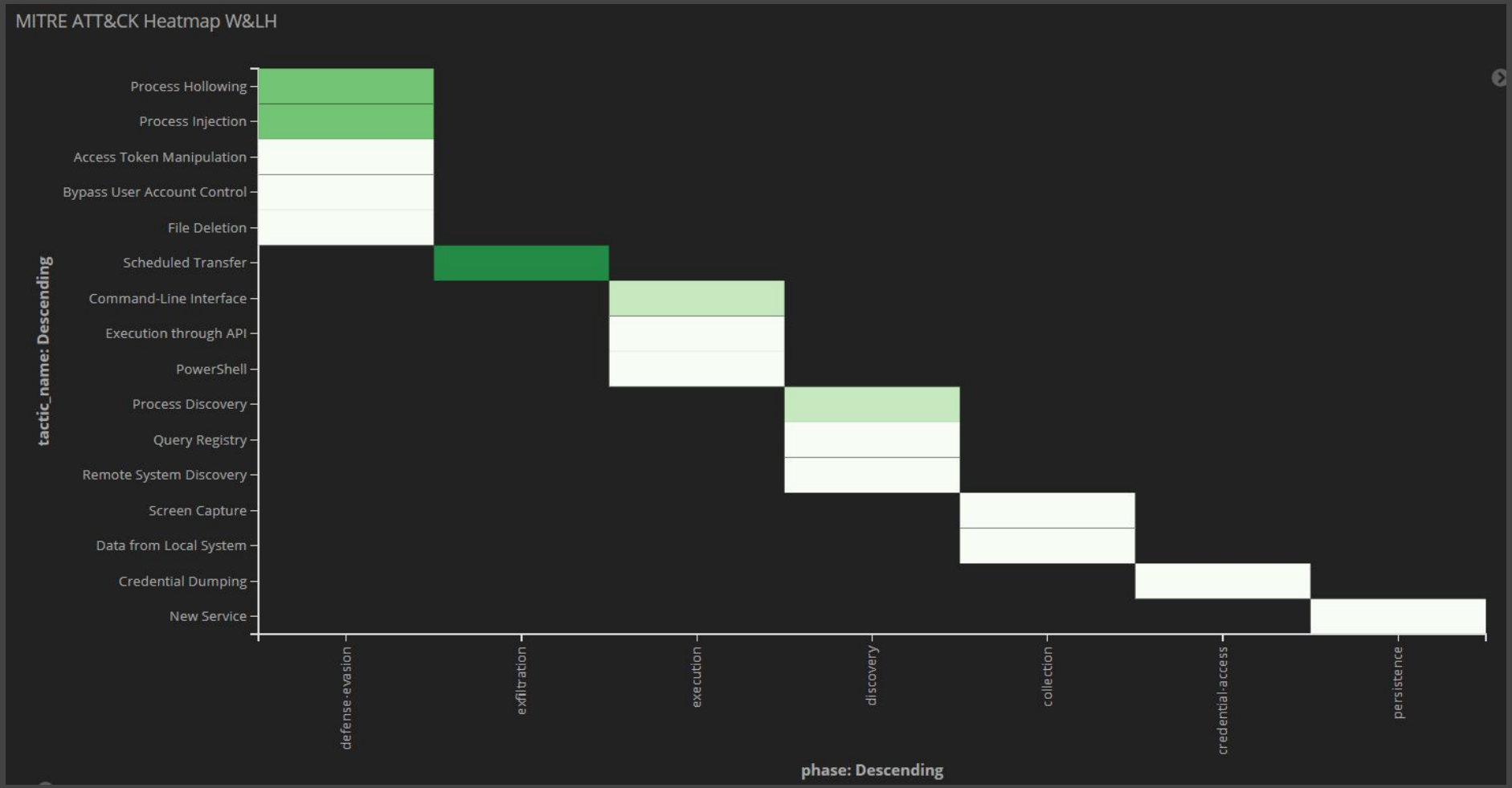
Inspired by curi0usJack: https://gist.github.com/curi0usJack/971385e8334e189d93a6cb4671238b10

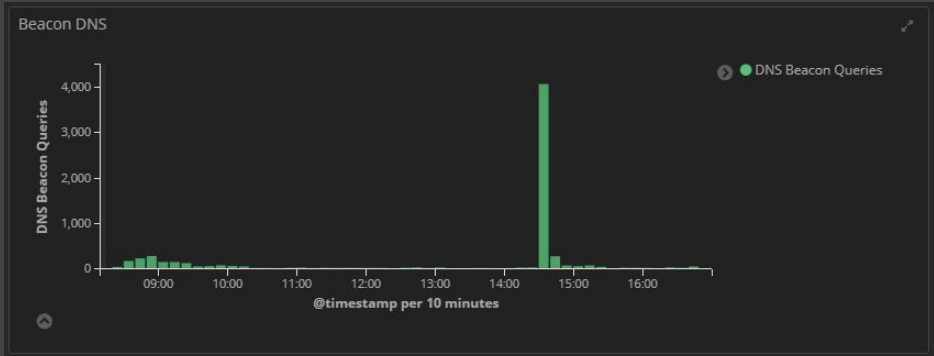
# Spot The DNS Exfil

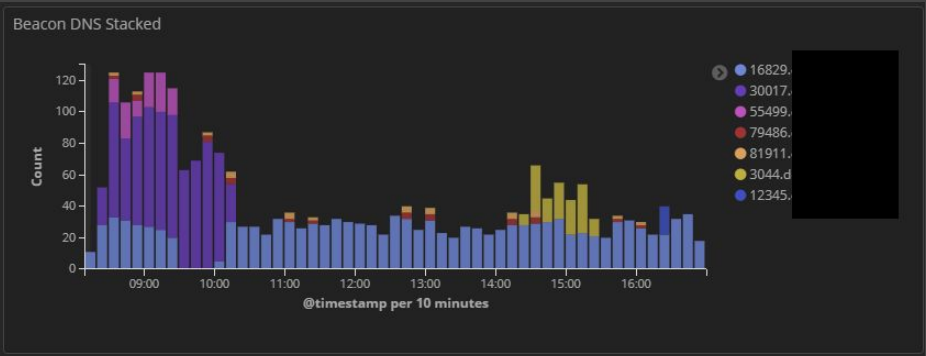


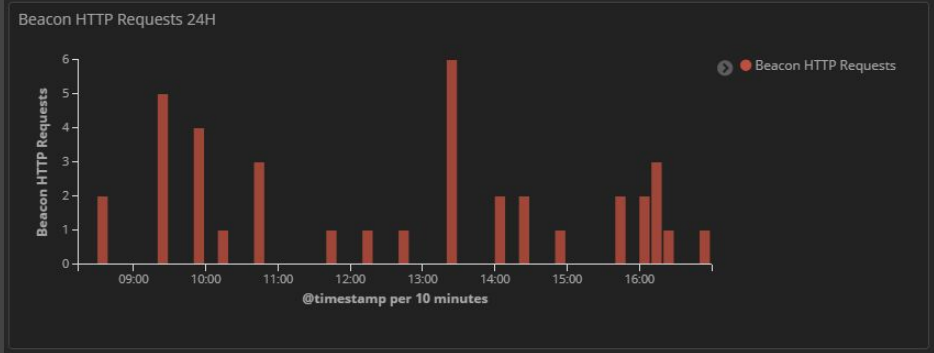
# Stealth Mode?

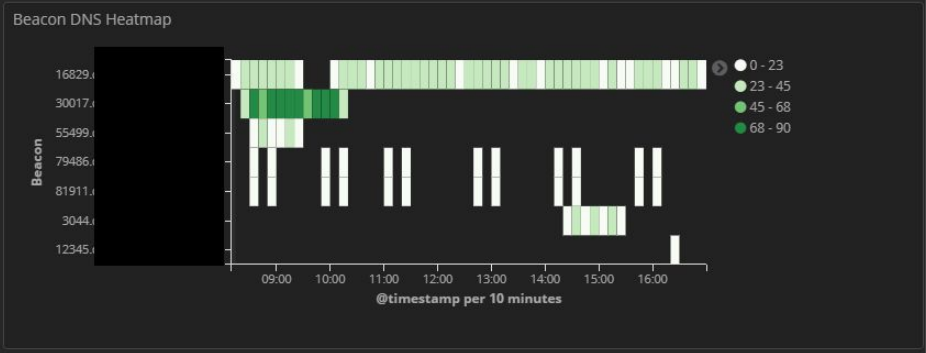


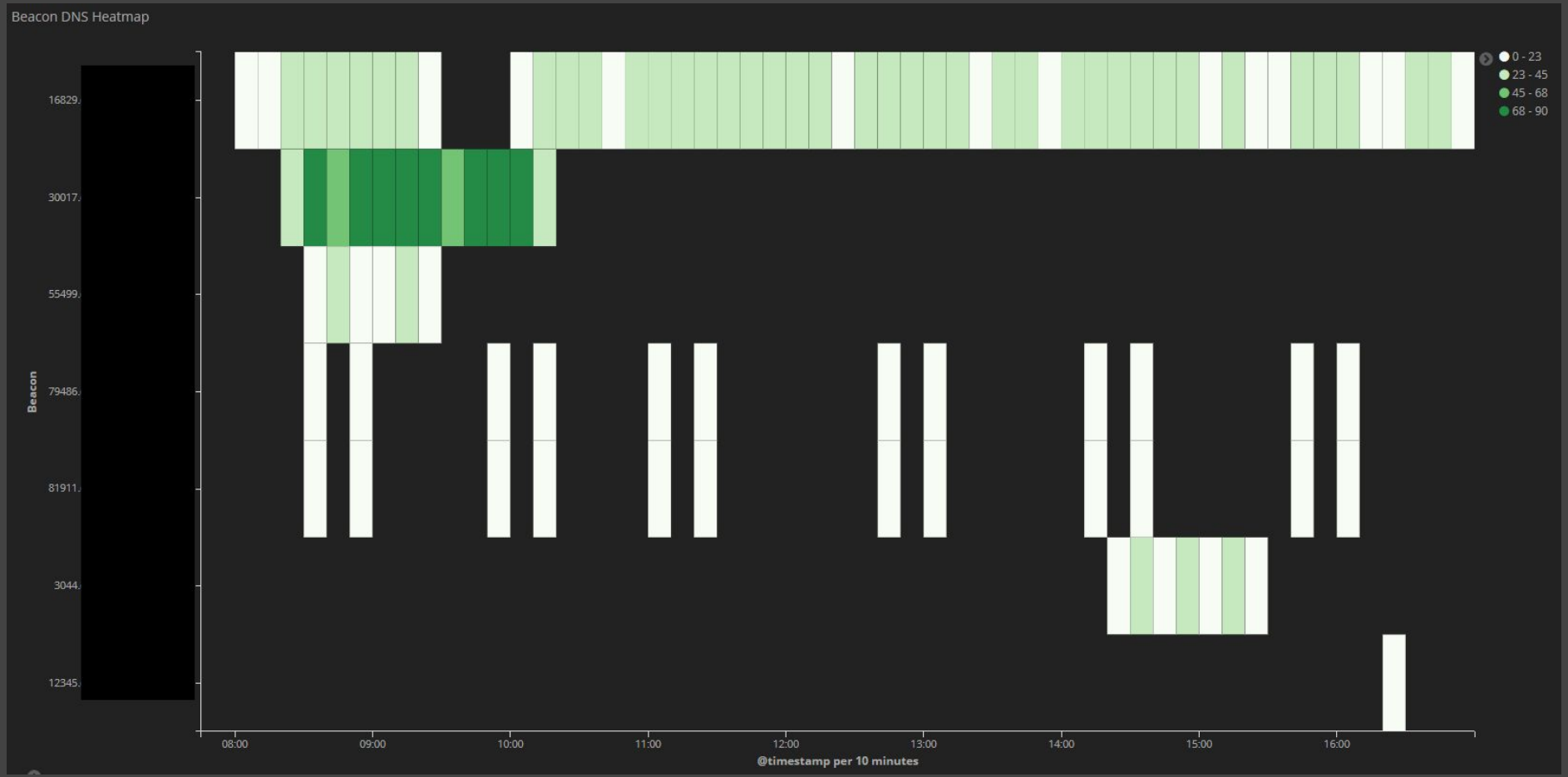

MITRE ATT&CK Heatmap W&LH
Process Hollowing
Process Injection
Access Token Manipulation
Bypass User Account Control
File Deletion
Scheduled Transfer
Command-Line Interface
Execution through API
PowerShell
Process Discovery
Query Registry
Remote System Discovery
Screen Capture
Data from Local System
Credential Dumping
New Service
tactic_name: Descending
defense-evasion
exfiltration
execution
discovery
collection
credential-access
persistence
phase: Descending

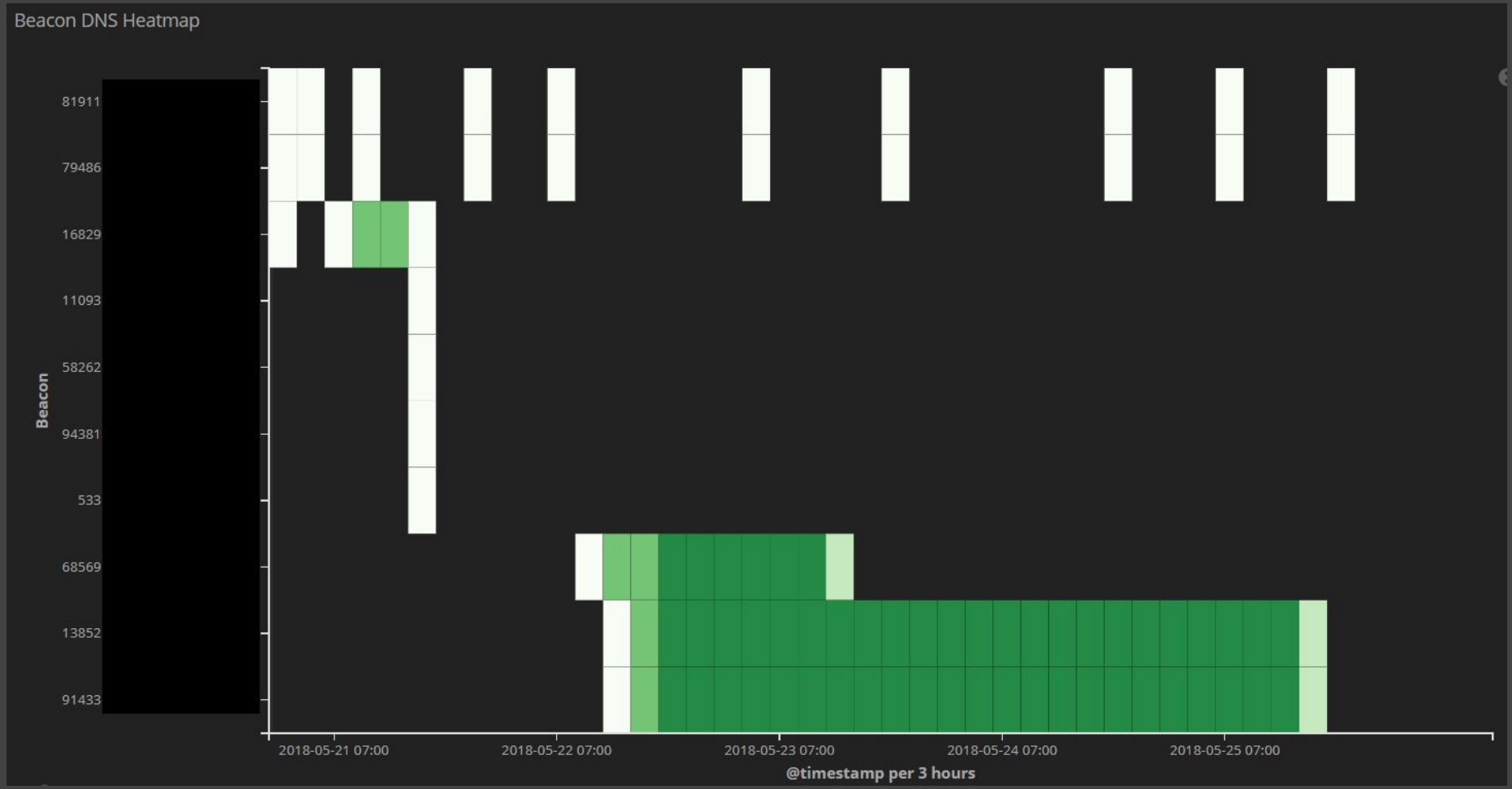

Beacon DNS
DNS Beacon Queries
DNS Beacon Queries
4,000
3,000
2,000
1,000
0
09:00
10:00
11:00
12:00
13:00
14:00
15:00
16:00
@timestamp per 10 minutes


Beacon DNS Stacked
Count
120
100
80
60
40
20
0
09:00
10:00
11:00
12:00
13:00
14:00
15:00
16:00
@timestamp per 10 minutes
16829.
30017.
55499.
79486.
81911.
3044.d
12345.


Beacon HTTP Requests 24H
Beacon HTTP Requests
Beacon HTTP Requests
6
5
4
3
2
1
0
09:00
10:00
11:00
12:00
13:00
14:00
15:00
16:00
@timestamp per 10 minutes


Beacon DNS Heatmap
Beacon
16829.
30017.
55499.
79486.
81911.
3044.
12345.
09:00
10:00
11:00
12:00
13:00
14:00
15:00
16:00
@timestamp per 10 minutes
0 - 23
23 - 45
45 - 68
68 - 90


Beacon DNS Heatmap
0 - 23
23 - 45
45 - 68
68 - 90
Beacon
16829.
30017.
55499.
79486.
81911.
3044.
12345.
08:00
09:00
10:00
11:00
12:00
13:00
14:00
15:00
16:00
@timestamp per 10 minutes


Beacon DNS Heatmap
Beacon
81911
79486
16829
11093
58262
94381
533
68569
13852
91433
2018-05-21 07:00
2018-05-22 07:00
2018-05-23 07:00
2018-05-24 07:00
2018-05-25 07:00
@timestamp per 3 hours

# Simple Automation (Reporting)

```
 1 #!/usr/bin/env python
 2
 3 from elasticsearch import Elasticsearch
 4 from datetime import datetime
 5 from pprint import pprint
 6
 7 size = 1000
 8 es = Elasticsearch()
 9 res = es.search(index="filebeat*",
10                 body={"query": {"match": {'event':'event_beacon_initial'}}}, size=size)
11
12 pprint(res)
13
14 for hit in res['hits']['hits']:
15
16     data = hit['_source']
17     #pprint(data)
18     if data.get('role', None):
19         data = hit['_source']
20         print("%s - beaconid: %s %s" % (data['role'], data['hostname'], data['user']))
```

# Gaps

- Attacking from Windows systems
- Cross-index correlation (no subselect statements like SQL)
- Needs Moar RAMs

# Dear Toolmakers

- Please use ISO 8601 or Unix timestamps
- Add structured logging or sane log formats to your tools

# What’s Next?

- Add similar telemetry to windows systems for easier correlations
- Feed to machine learning, build attacker behavioral models
- Frequency between commands/better callback frequency

# References and Resources

- Code from the talk: https://github.com/ztgrace/red_team_telemetry
- Red Team Telmetry Blog Post - https://zachgrace.com/posts/red-team-telemetry-part-1/
- PCAP->ELK - https://www.elastic.co/blog/analyzing-network-packets-with-wireshark-elasticsearch-and-kibana
- Packetbeat - https://www.elastic.co/products/beats/packetbeat
- Connbeat - https://github.com/raboof/connbeat
- Cobalt Strike infrastructure - https://blog.cobaltstrike.com/2014/01/14/cloud-based-redirectors-for-distributed-hacking/
- Cobal Strike infrastrucutre detail - https://zachgrace.com/posts/cobalt_strike_redirectors/
- curi0usJack .htaccess redirection - https://gist.github.com/curi0usJack/971385e8334e189d93a6cb4671238b10
- RedELK - https://github.com/outflanknl/RedELK