Beacon Analysis

Problem Space

- 2017 saw 1,579 public data breaches
  - Identity Theft Resource Center 2017 report
- Out of 1,200 orgs surveyed, 71% breached
  - 451 Group 2018 Global Threat Report
- On average, 191 days to ID a breach & 66 days to contain it
  - Ponemon Institute 2017 study
- Average cost of recovery is $3.62 million
  - Ponemon Institute 2017 study

What is Threat Hunting?

- Search for evidence of compromise
  - Assumes the bad guys are already inside
  - Watch the network for suspect traffic
  - Watch logs for suspect entries
  - Incident response for suspicious systems
- Identifies when other layers have failed
- Needs to be tightly defined

https://www.activecountermeasures.com/tightly-defining-cyber-threat-hunting/

Why Threat Hunt The Network?

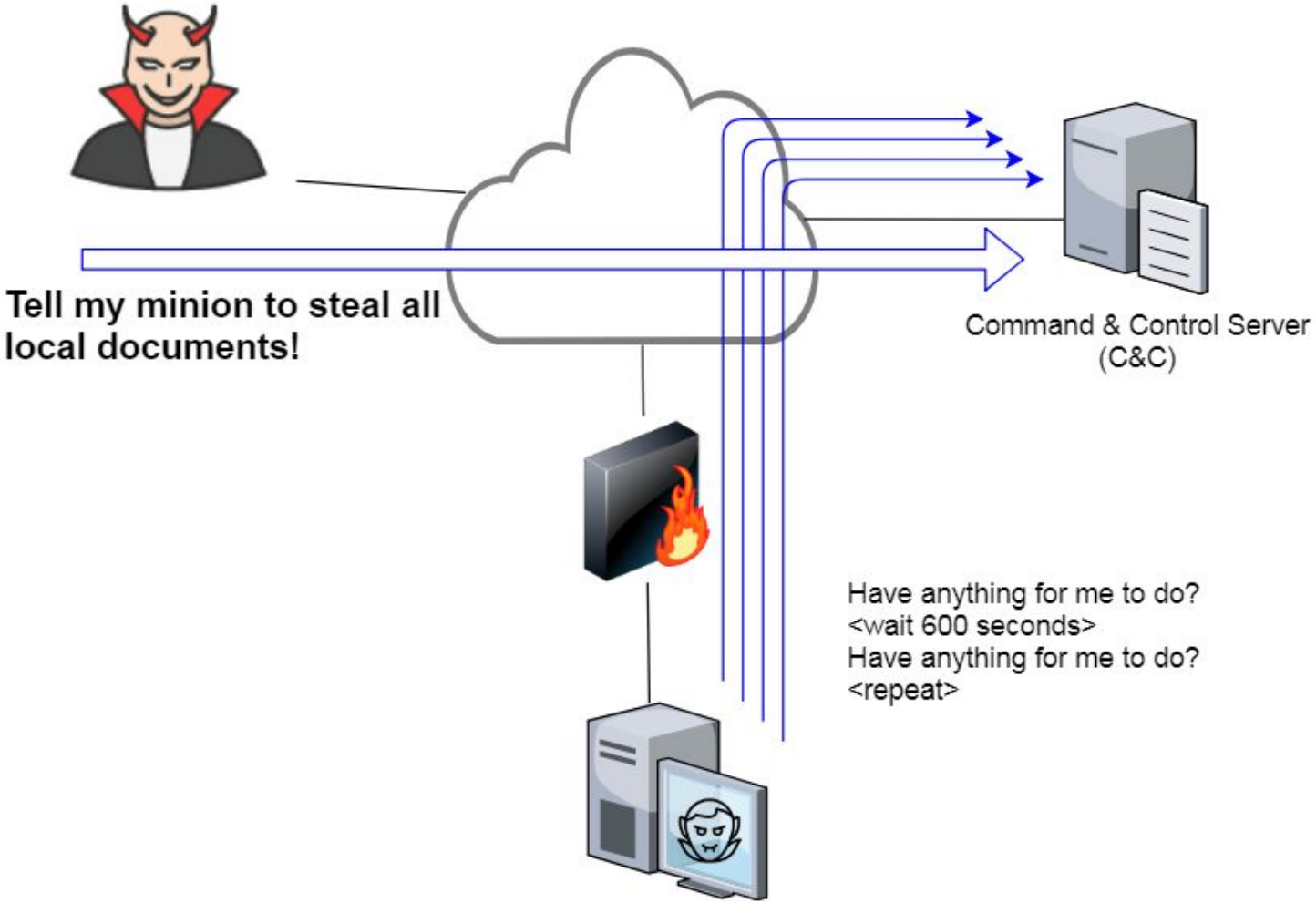
- Because reading system logs is hard
  - Full of stuff we don't care about
  - Log details vary between platforms and apps
  - Can be hard to find a decoder ring
- Are you logging everything?
  - Are you sure? All devices and critical apps?
  - What about BYOD? IoT?
- Attackers focus on hiding their footprint
- The network levels the playing field

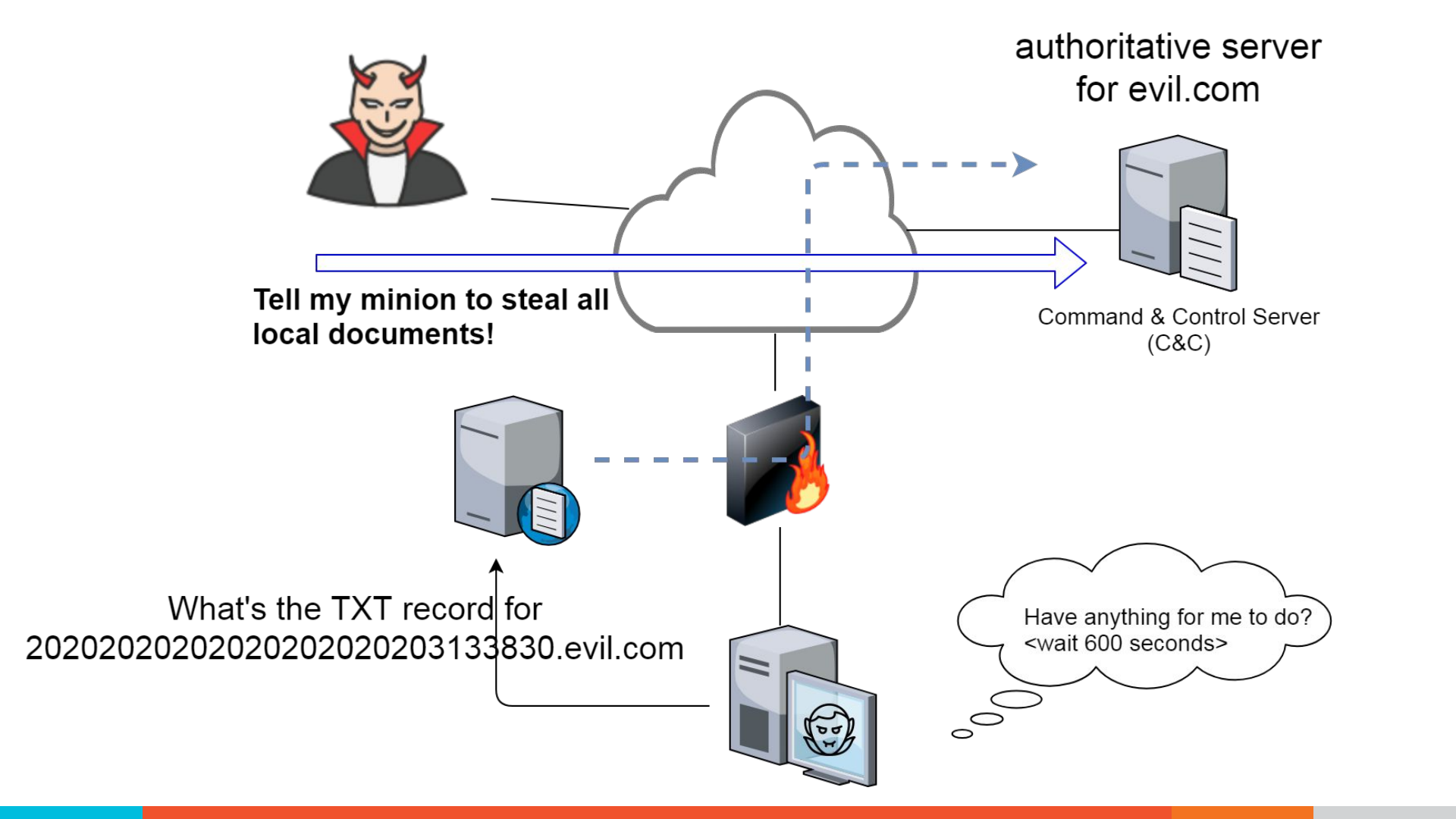
Why Beacon Analysis?

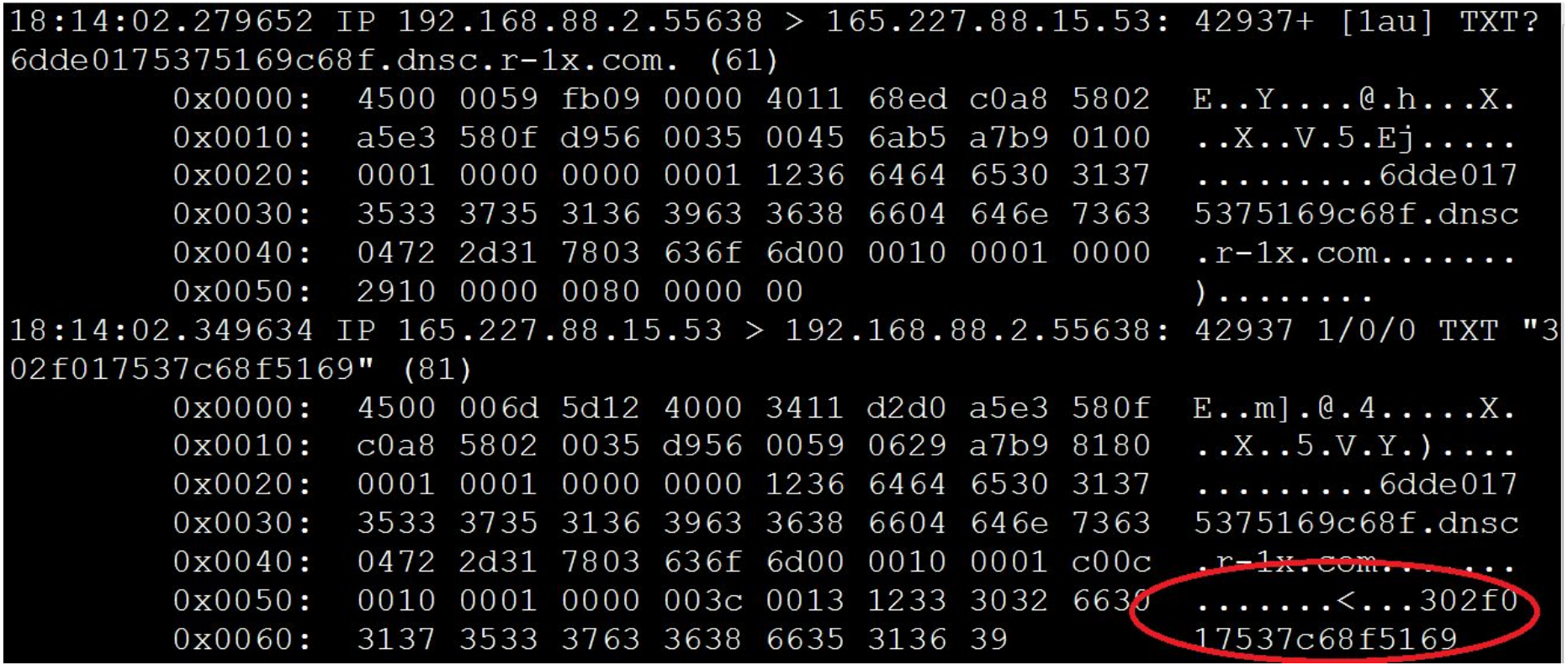
- Malware has to call home to be useful
  - Channel needed to issue commands
  - Internet link is choke point for these comms
  - If they are using MiFi, you have bigger problems
- Communications must be IP complaint
  - You can bend the rules, but not break them
  - Example: Obfuscated data over TCP/443 (HTTPS)
- Persistent connections don’t scale
  - 100,000 bots can’t hold open a connection

Beaconing Rules

- Must work over the Internet
- Must facilitate the attacker's objective
- Must be a functional backdoor
- You can vary timing, but only so much
- You can add padding but only so much
- Solve problems instead of hating


Tell my minion to steal all local documents!
Command & Control Server (C&C)
Have anything for me to do?
<wait 600 seconds>
Have anything for me to do?
<repeat>


authoritative server
for evil.com
Tell my minion to steal all
local documents!
Command & Control Server
(C&C)
What's the TXT record for
20202020202020202020203133830.evil.com
Have anything for me to do?
<wait 600 seconds>

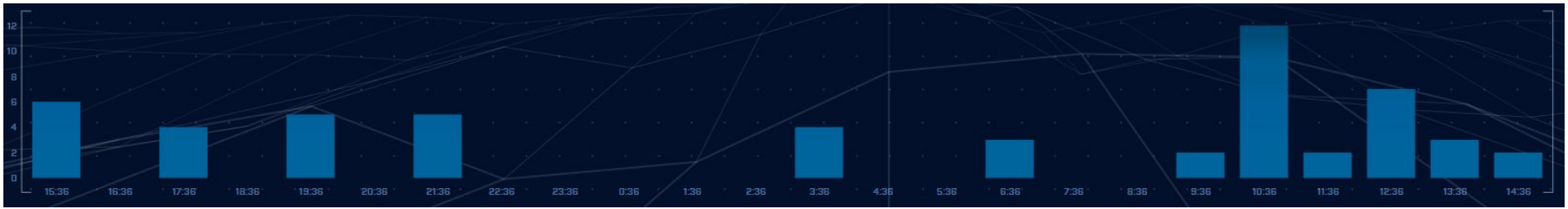

18:14:02.279652 IP 192.168.88.2.55638 > 165.227.88.15.53: 42937+ [1au] TXT?
6dde0175375169c68f.dnsc.r-1x.com. (61)
0x0000: 4500 0059 fb09 0000 4011 68ed c0a8 5802 E..Y....@.h...X.
0x0010: a5e3 580f d956 0035 0045 6ab5 a7b9 0100 ..X..V.5.Ej.....
0x0020: 0001 0000 0000 0001 1236 6464 6530 3137 ....6dde017
0x0030: 3533 3735 3136 3963 3638 6604 646e 7363 5375169c68f.dnsc
0x0040: 0472 2d31 7803 636f 6d00 0010 0001 0000 .r-1x.com.......
0x0050: 2910 0000 0080 0000 00)........
18:14:02.349634 IP 165.227.88.15.53 > 192.168.88.2.55638: 42937 1/0/0 TXT "3
02f017537c68f5169" (81)
0x0000: 4500 006d 5d12 4000 3411 d2d0 a5e3 580f E..m].@.4.....X.
0x0010: c0a8 5802 0035 d956 0059 0629 a7b9 8180 ..X..5.V.Y.)....
0x0020: 0001 0001 0000 0000 1236 6464 6530 3137 ....6dde017
0x0030: 3533 3735 3136 3963 3638 6604 646e 7363 5375169c68f.dnsc
0x0040: 0472 2d31 7803 636f 6d00 0010 0001 c00c .r-1x.com.......
0x0050: 0010 0001 0000 003c 0013 1233 3032 6630 ....<...302f0
0x0060: 3137 3533 3763 3638 6635 3136 39 17537c68f5169

Finding Beacons in Packet Captures

- The more data, the better (24 hours)
- Break out traffic into IP pairs
- Identify first packet timing for each session
- Identify data transfer quantity per session
  - Breaking out send/receive is helpful
- Standard deviation analysis
- Time bucket analysis (1-2 hours)

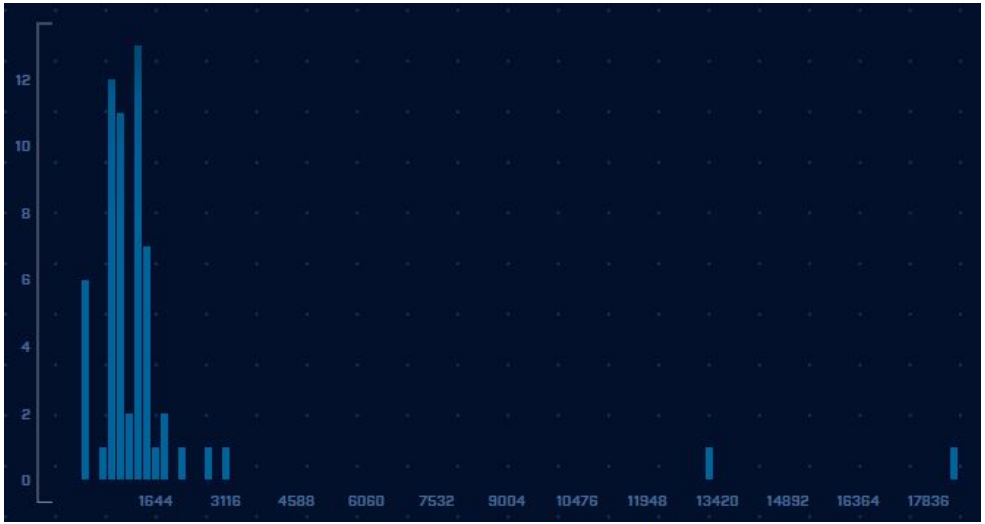
https://www.activecountermeasures.com/blog-tshark-examples-for-extracting-ip-fields/

Not a Beacon

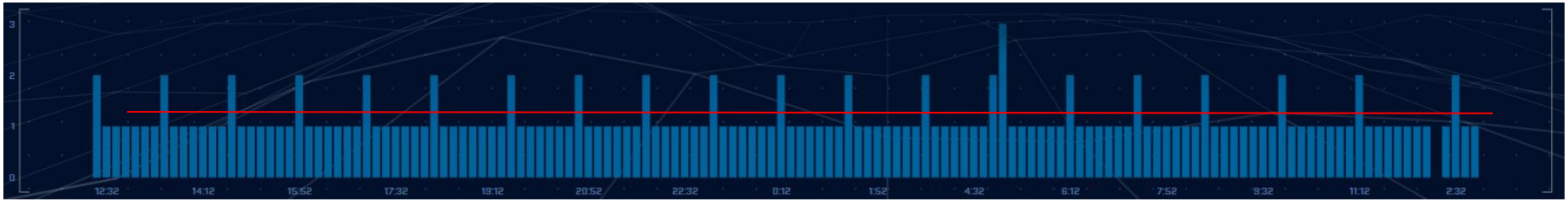


Variations in timing

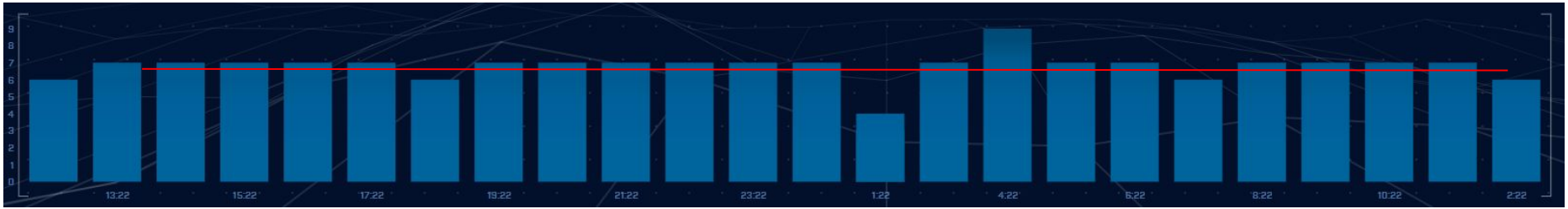
Variations in session size



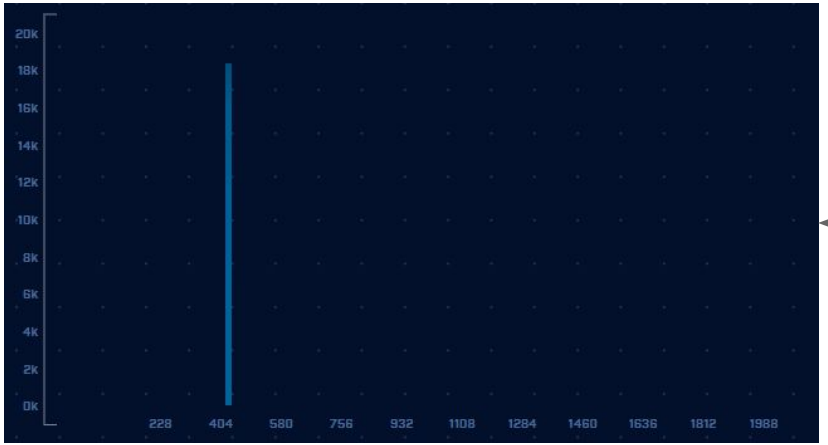
10 Minute Beacon Timing Analysis



60 Minute Beacon Timing Analysis

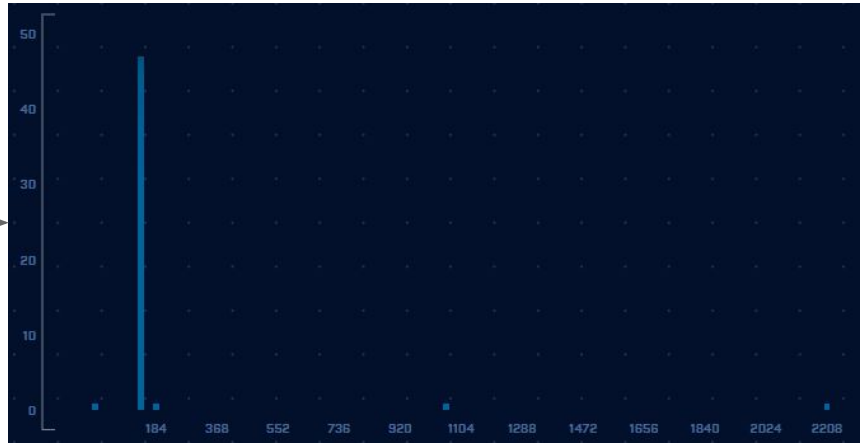


Was The Backdoor Activated?



No

Maybe?



RITA

```
COMMANDS:
     analyze                 Analyze imported databases
     delete-database         Delete an imported database
     import                  Import bro logs into a target database
     html-report             Create an html report for an analyzed database
     reset-analysis          Reset analysis of a database
     show-beacons            Print hosts which show signs of C2 software
     show-bl-hostnames       Print blacklisted hostnames which recieved connections
     show-bl-source-ips      Print blacklisted IPs which initiated connections
     show-bl-dest-ips        Print blacklisted IPs which recieved connections
     show-bl-urls            Print blacklisted URLs which were visited
     show-databases          Print the databases currently stored
     show-exploded-dns       Print dns analysis. Exposes covert dns channels
     show-long-connections   Print long connections and relevant information
     show-scans              Print scanning information
     show-long-urls          Print the longest urls
     show-most-visited-urls  Print the most visited urls
     show-user-agents        Print user agent information
     test-config             Check the configuration file for validity
     help, h                 Shows a list of commands or help for one command
```

https://github.com/activecm/rita

```
ubuntu@ip-172-31-26-215:~/working/beacon$ rita show-beacons beacon | head -10
Score,Source,Destination,Connections,Avg Bytes,TS Range,DS Range,TS Mode,DS Mode,TS Mode Count,
DS Mode Count,TS Skew,DS Skew,TS Dispersion,DS Dispersion,TS Duration
0.999774,192.168.88.2,165.227.88.15,108858,199.578,980,201,1,89,53341,108319,0,0,0,0,1
0.99182,192.168.88.2,13.107.3.1,57,190.07,5902,3,3154,73,9,35,0,0,1,0,0.98537
0.99182,192.168.88.2,13.107.3.2,60,193.833,7576,3,3154,73,10,43,0,0,1,0,0.98537
0.958989,192.168.88.2,205.233.73.201,163,152,31,0,542,76,11,163,0,0,7,0,0.988426
0.955013,192.168.88.2,216.229.4.69,164,148.756,32,0,519,76,9,164,0,0,8,0,0.997905
0.949074,192.168.88.2,216.218.220.101,164,152,32,0,518,76,12,164,0,0,9,0,0.995602
0.939216,192.168.88.2,66.228.58.20,164,151.537,31,0,519,76,11,164,-0.0588235,0,9,0,0.995278
0.93308,192.168.88.2,108.61.56.35,163,152,31,0,543,76,11,163,-0.125,0,8,0,0.991308
0.92634,192.168.88.2,45.33.48.4,164,152,31,0,514,76,12,164,-0.2,0,7,0,0.992535
ubuntu@ip-172-31-26-215:~/working/beacon$ _
```

```
Domain,Unique Subdomains,Times Looked Up
com,65284,209046
r-1x.com,63332,109227
dnsc.r-1x.com,63330,108911
net,1827,99440
org,368,3427
akadns.net,237,13907
edgekey.net,233,7110
akamaiedge.net,173,27381
com.edgekey.net,165,6075
amazonaws.com,114,13297
com.akadns.net,110,8405
elb.amazonaws.com,101,13259
microsoft.com,87,1687
dynect.net,79,129
us-east-1.elb.amazonaws.com,55,6971
uk,54,199
nsatc.net,49,1455
parsely.com,48,889
:_
```

```
202030363a323720504d20202020202020202020203839302c3638362037.7a313730312d6
57787472612e377a0d0a3039.dnsc.r-1x.com,3,1
20202e6f7261636c655f6a72655f75736167650d0a30392f32382f323031.37202031313a3
13220414d202020203c4449.dnsc.r-1x.com,3,1
20202034204b0d0a737663686f73742e6578652020202020202020202020.2020202020202
020313236342053657276696365732020202020202020.2020202020202020202030202020
2020203130.dnsc.r-1x.com,3,2
20202034204b0d0a61746965636c78782e6578652020202020202020202020.2020202020202
020353032342043f6e736f6c652020202020202020.2020202020202020202031202020
2020202020.dnsc.r-1x.com,3,2
2020202e0d0a30312f32352f323031382020303133a333620504d20202020.3c4449523e202
020202020202020202e2e0d.dnsc.r-1x.com,3,1
202020204d757369630d0a30312f33302f323031382020313032a32372041.4d202020203c4
449523e2020202020202020.dnsc.r-1x.com,3,1
2020202035204469722873292020333738 2c3438382c3033372c33373620.627974657320667265650d0a0d0a433a5c55.dnsc.r-1x.com,3,1
20202020343 52c333732204b0d0a72756e646c6c33322e65786520202020.2020202020202
020202020202034343936.dnsc.r-1x.com,3,1
20202020342c3833332c37393220756e6574626f6f74696e2d77696e646f.77732d3635352
:
```

Wrap Up

- Thanks for attending!
- What threat hunting training is helpful?
  - More on tools
  - More on techniques
  - Go down the math rabbit hole
- Drop a note and let us know
  - chris@activecountermeasures.com
  - @ActiveCmeasures