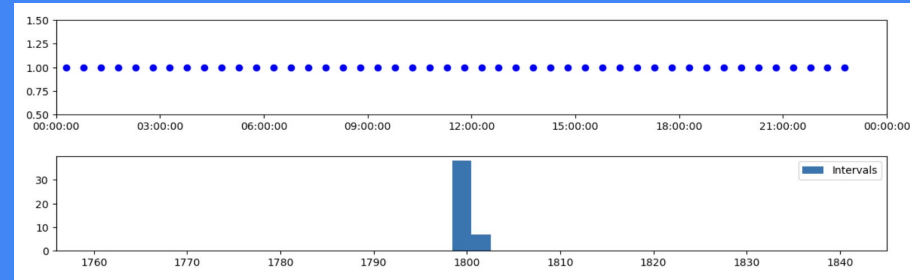


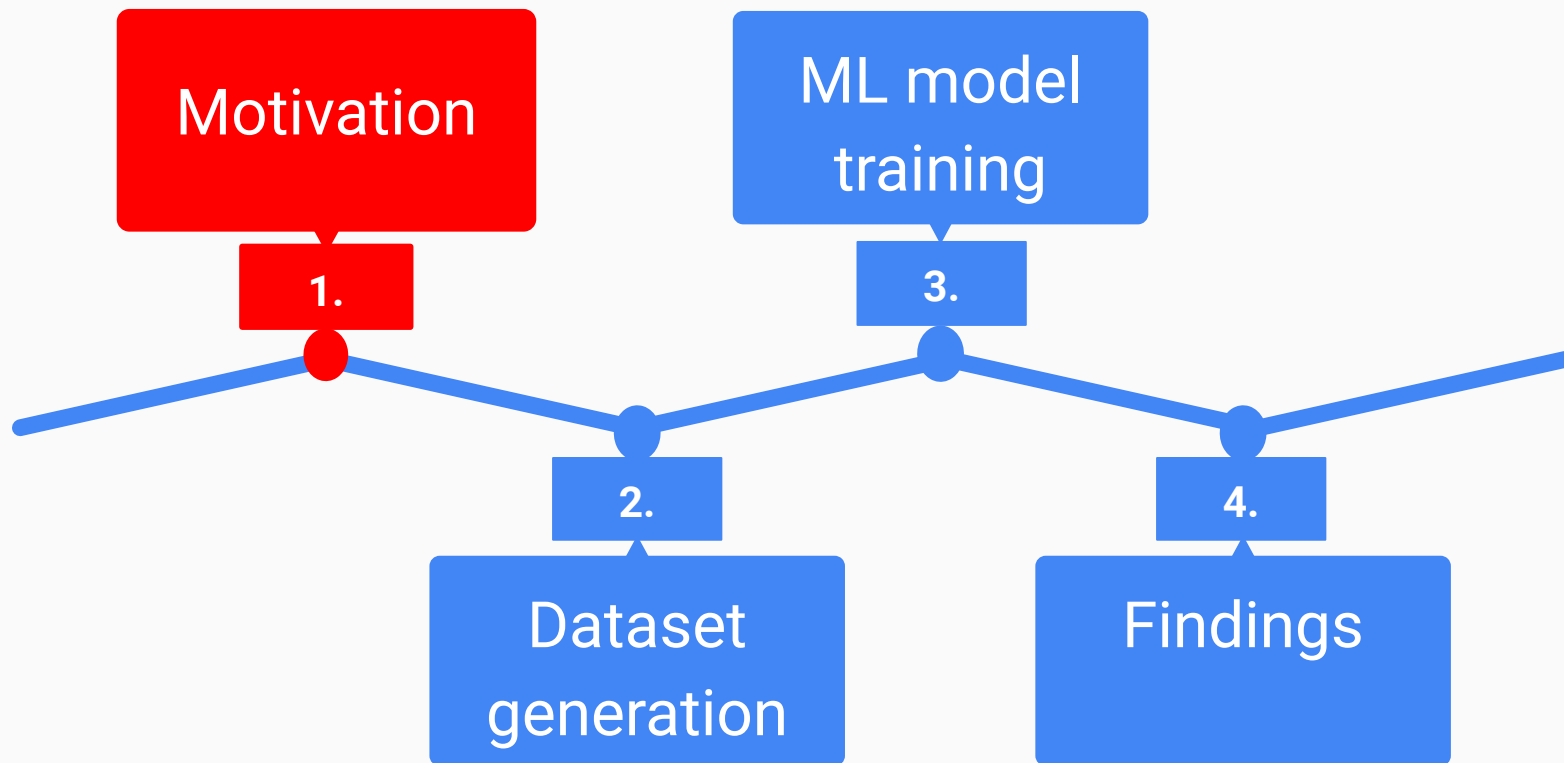
# Detecting Network Beaconing with CNNs and Zeek Logs

Ignacio Arnaldo

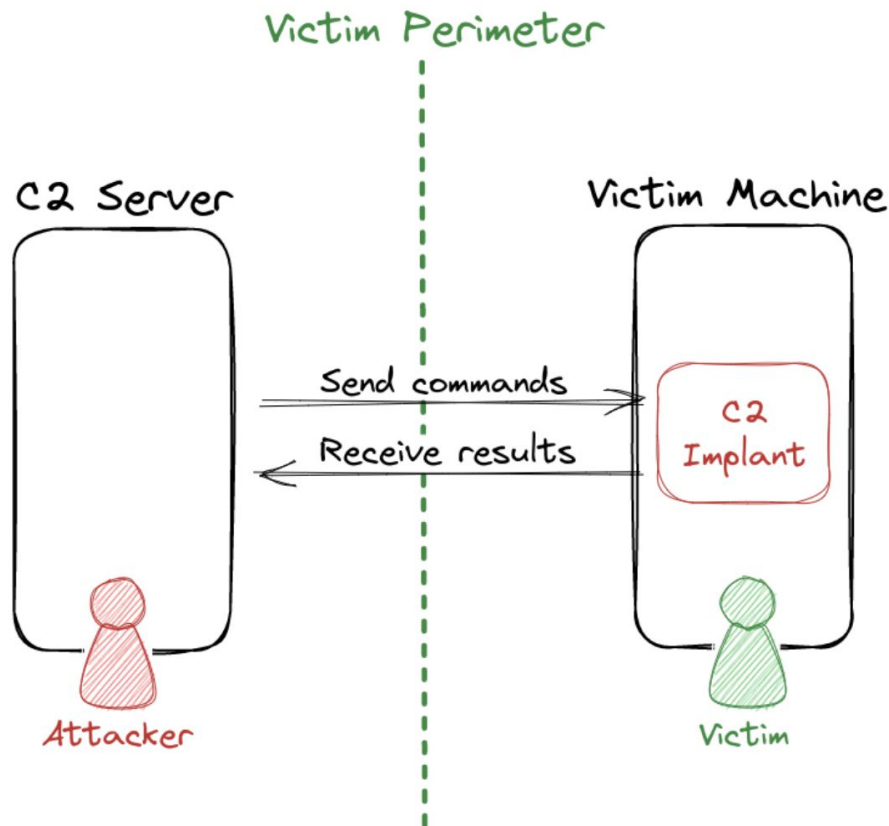


The diagram illustrates the combination of three components: Zeek, K, and TensorFlow. The Zeek logo (a stylized 'Z' with arrows) is followed by a plus sign, then the K logo (a red square with a white 'K'), followed by another plus sign and the TensorFlow logo (an orange 3D 'T' with 'TensorFlow' text). Below this sequence is an equals sign, indicating that these components are combined to form a system for detecting network beaconn.





Listeners (server side)  $\longleftrightarrow$  implants and agents/beacons (client side)



## C2 frameworks

- Caldera
- Metasploit/Meterpreter
- Sliver
- Empire
- Cobalt Strike
- ...

## Useful references:

- [C2Matrix](#) (130+ frameworks)
- [Learning Sliver C2 \(02\) - Beacons and Sessions](#)

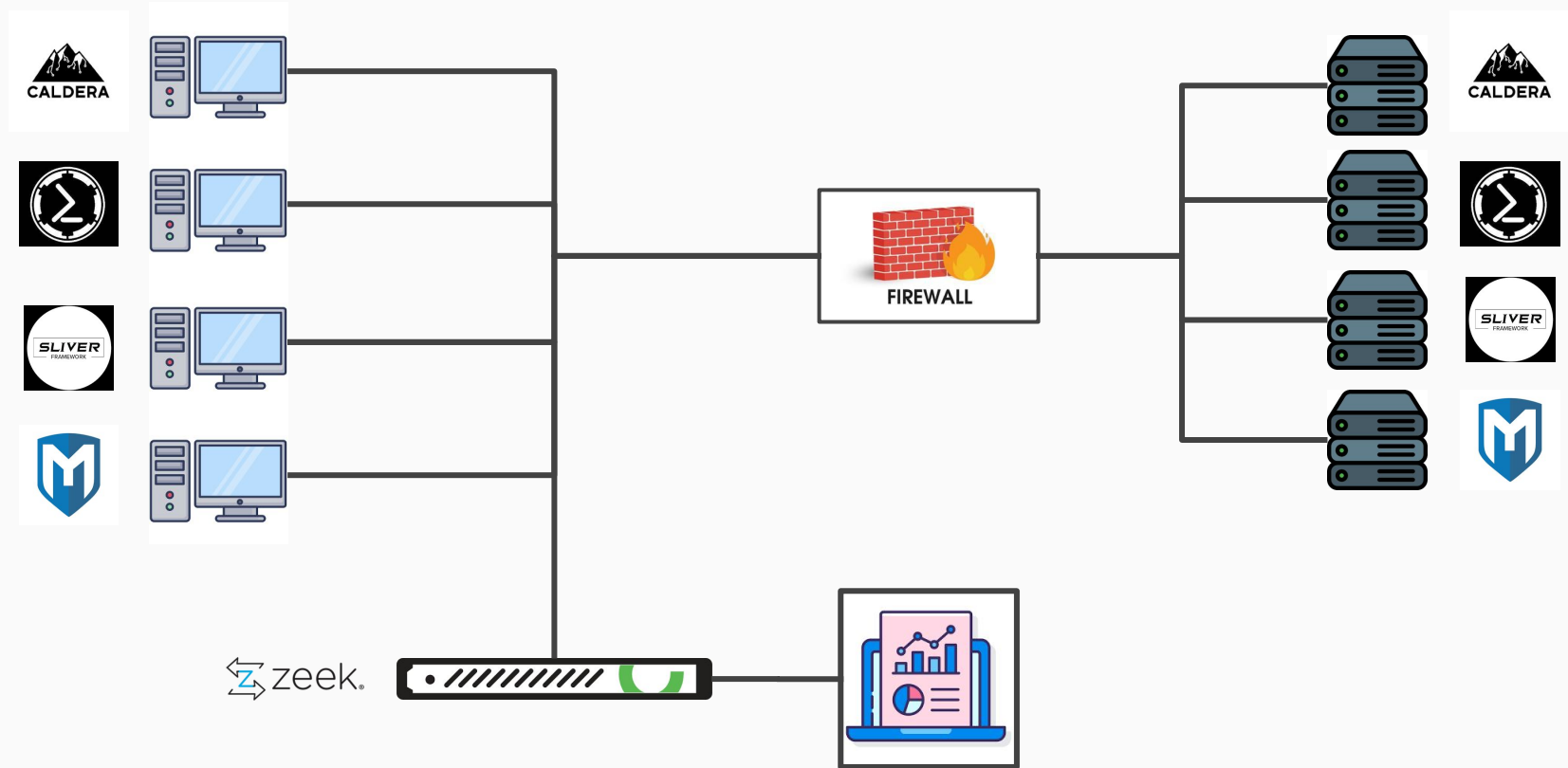
# C2 Matrix - 135 frameworks!!

Link: [C2 Matrix](#)

	A	B	C	D	E	F	G
1		C2 Info					
2	Name	License	Price	GitHub	Site	Twitter	Evaluator
3	AirStrike	NA	NA	<a href="https://github.com/smokemc/airstrike">https://github.com/smokemc/airstrike</a>		@q8fawazo	<a href="#">Contribute</a>
4	Alan	Created Commons	NA	<a href="https://github.com/enkomio/AlanFramework">https://github.com/enkomio/AlanFramework</a>		@s4tan	@s4tan
5	Alchemist	NA	NA		<a href="https://blog.talosintelligence.com/2022/10/alchemist-o">https://blog.talosintelligence.com/2022/10/alchemist-o</a>		@TalosSecurity
6	Arcis	NA	NA	<a href="https://github.com/sweetsoftware/Ares">https://github.com/sweetsoftware/Ares</a>			@nas_bench
7	AsyncRAT-C#	MIT	NA	<a href="https://github.com/NYAN-x-CAT/AsyncRAT-C-Sharp">https://github.com/NYAN-x-CAT/AsyncRAT-C-Sharp</a>			<a href="#">Contribute</a>
8	AtlasC2	MIT	NA	<a href="https://github.com">https://github.com</a> < <a href="https://grimme.at/aslasc-2-ca">https://grimme.at/aslasc-2-ca</a>		@gr1mmie	@Adam_Mashingt
9	BabyShark	NA	NA	<a href="https://github.com/Unkl4b/BabyShark">https://github.com/Unkl4b/BabyShark</a>		@Unkl4b	@nas_bench
10	Badrats	GNU GPL3	NA	<a href="https://github.com/KevinClark/badrats">https://github.com/KevinClark/badrats</a>		@GuhnoPlusLinux	<a href="#">Contribute</a>
11	BlackMamba	MIT	NA	<a href="https://github.com/losevs/BlackMamba">https://github.com/losevs/BlackMamba</a>			<a href="#">Contribute</a>
12	Brute Ratel	Commercial	\$2,500		<a href="https://bruteratel.com/">https://bruteratel.com/</a>	@NinjaParanoid	@NinjaParanoid
13	Bunraku	Apache 2	NA	<a href="https://github.com/theshadowboxers/bunraku">https://github.com/theshadowboxers/bunraku</a>			<a href="#">Contribute</a>
14	C3	BSD3	NA	<a href="https://github.com">https://github.com</a> < <a href="https://labs.f-secure.com/tools">https://labs.f-secure.com/tools</a>		@FSecureLabs	@ajpc500
15	CALDERA	Apache 2	NA	<a href="https://github.com/mitre/caldera">https://github.com/mitre/caldera</a>			@jorgeorchilles
16	Callidus	GNU GPL3	NA	<a href="https://github.com/3xpl0it0d3r/Callidus">https://github.com/3xpl0it0d3r/Callidus</a>		@chiragsavla94	@chiragsavla94
17	CHAOS	BSD3	NA	<a href="https://github.com/vtiagoriampert/CHAOS">https://github.com/vtiagoriampert/CHAOS</a>		@vtiagoriampert	@leekirkpatrick4
18	CloakNDaggerC2	GNU GPL2	NA	<a href="https://github.com/matt-culbert/CloakNDaggerC2">https://github.com/matt-culbert/CloakNDaggerC2</a>			
19	Cobalt Strike	Commercial	\$5,900		<a href="https://www.cobaltstrike.com/">https://www.cobaltstrike.com/</a>		@TimMedin
20	Core Impact	Commercial	\$12,600		<a href="https://www.coresecurity.com/">https://www.coresecurity.com/</a>	@coreadvories	@zurro
21	Covenant	GNU GPL3	NA	<a href="https://github.com">https://github.com</a> < <a href="https://cobbr.io/tags/covenant">https://cobbr.io/tags/covenant</a>		@cobbr_io	@jorgeorchilles
22	DaaC2	NA	NA	<a href="https://github.com/crawl3r/DaaC2">https://github.com/crawl3r/DaaC2</a>			<a href="#">Contribute</a>
23	Dali	MIT	NA	<a href="https://github.com">https://github.com</a> < <a href="https://h0mbre.github.io/imag">https://h0mbre.github.io/imag</a>		@h0mbre_	@jorgeorchilles
24	DarkFinger	MIT	NA	<a href="https://github.com/hvp3rllnx/DarkFinger-C2">https://github.com/hvp3rllnx/DarkFinger-C2</a>		@hvp3rlinx	@nas_bench
25	DBC2	NA	NA	<a href="https://github.com/Arno0x/DBC2">https://github.com/Arno0x/DBC2</a>			<a href="#">Contribute</a>
26	DcRat	MIT	NA	<a href="https://github.com/qwdqanchun/DcRat">https://github.com/qwdqanchun/DcRat</a>		@qwdqanchun	<a href="#">Contribute</a>
27	DCV2C	NA	NA	<a href="https://github.com/3NalInfoSec/DCV2C">https://github.com/3NalInfoSec/DCV2C</a>			
28	DeimosC2	MIT	NA	<a href="https://github.com/DeimosC2/DeimosC2">https://github.com/DeimosC2/DeimosC2</a>		@CharlesDardaman	@jasc22
29	DiscordGo	NA	NA	<a href="https://github.com/emmanuel/discordgo">https://github.com/emmanuel/discordgo</a>			
30	Disctopia	GNU GPL3	NA	<a href="https://github.com/3ct0x/disctopia-c2">https://github.com/3ct0x/disctopia-c2</a>			<a href="#">Contribute</a>
31	Eggshell	GNU GPL2	NA	<a href="https://github.com/neoneggplant/EggShell">https://github.com/neoneggplant/EggShell</a>			<a href="#">Contribute</a>
32	emp3r0r	MIT	NA	<a href="https://github.com/im33-m0/emp3r0r">https://github.com/im33-m0/emp3r0r</a>			<a href="#">Contribute</a>

[illegible]

# Lab setup: analysis of Caldera, Empire, Sliver, and Meterpreter traffic



# Zeek logs: conn, dns, http, ssl

## conn.log | IP, TCP, UDP, ICMP connection details

FIELD	TYPE	DESCRIPTION
ts	time	Timestamp of first packet
uid	string	Unique identifier of connection
id	record conn_id	Connection's 4-tuple of endpoint addresses
proto	enum	Transport layer protocol of connection
service	string	Application protocol ID sent over connection
duration	interval	How long connection lasted
orig_bytes	count	Number of payload bytes originator sent
resp_bytes	count	Number of payload bytes responder sent
conn_state	string	Connection state (see <a href="#">conn.log</a> > <a href="#">conn_state</a> )
local_orig	bool	Value=T if connection originated locally
local_resp	bool	Value=T if connection responded locally
missed_bytes	count	Number of bytes missed (packet loss)
history	string	Connection state history (see <a href="#">conn.log</a> > <a href="#">history</a> )
orig_pkts	count	Number of packets originator sent
orig_ip_bytes	count	Number of originator IP bytes (via IP total_length header field)
resp_pkts	count	Number of packets responder sent
resp_ip_bytes	count	Number of responder IP bytes (via IP total_length header field)

## dns.log | DNS query/response details

FIELD	TYPE	DESCRIPTION
ts	time	Earliest timestamp of DNS protocol message
uid & id		Underlying connection info > See <a href="#">conn.log</a>
proto	enum	Transport layer protocol of connection
trans_id	count	16-bit identifier assigned by program that generated DNS query
rtt	interval	Round trip time for query and response
query	string	Domain name subject of DNS query
qclass	count	QCLASS value specifying query class
qclass_name	string	Descriptive name query class
qtype	count	QTYPE value specifying query type
qtype_name	string	Descriptive name for query type
rcode	count	Response code value in DNS response
rcode_name	string	Descriptive name of response code value
AA	bool	Authoritative Answer bit: responding name server is authority for domain name
TC	bool	Truncation bit: message was truncated
RD	bool	Recursion Desired bit: client wants recursive service for query
RA	bool	Recursion Available bit: name server supports recursive queries
Z	count	Reserved field, usually zero in queries and responses
answers	vector	Set of resource descriptions in query answer
TTLs	vector	Caching intervals of RRs in answers field
rejected	bool	DNS query was rejected by server
auth	table	Authoritative responses for query
addl	table	Additional responses for query

## http.log | HTTP request/reply details

FIELD	TYPE	DESCRIPTION
ts	time	Timestamp for when request happened
uid & id		Underlying connection info > See <a href="#">conn.log</a>
trans_depth	count	Pipelined depth into connection
method	string	Verb used in HTTP request (GET, POST, etc.)
host	string	Value of HOST header
uri	string	URI used in request
referrer	string	Value of referer header
version	string	Value of version portion of request
user_agent	string	Value of User-Agent header from client
origin	string	Value of Origin header from client
request_body_len	count	Uncompressed data size from client
response_body_len	count	Uncompressed data size from server
status_code	count	Status code returned by server
status_msg	string	Status message returned by server

## ssl.log | SSL handshakes

FIELD	TYPE	DESCRIPTION
ts	time	Time when SSL connection first detected
uid & id		Underlying connection info > See <a href="#">conn.log</a>
version	string	SSL/TLS version server chose
cipher	string	SSL/TLS cipher suite server chose
curve	string	Elliptic curve server chose when using ECDH/ECDHE
server_name	string	Value of Server Name Indicator SSL/TLS extension
resumed	bool	Flag that indicates session was resumed
last_alert	string	Last alert seen during connection

<https://zeek.org/>

<https://github.com/corelight/zeek-cheatsheets/>

<https://tryhackme.com/>

<https://try.bro.org/>



# Caldera: beaconing vs. interactions

corelight | INVESTIGATOR Nacho Admin

Event List Queries +01:00 London 2023-06-24 05:49:34 2023-07-11 17:18:24 Live Run

```
1 #path=conn
2 | id.orig_h=10.2.128.46
3 | id.resp_h=34.217.28.127
4
5
```

Interactions

Long conns logged every ~1 day

Results

3 Jun 25 Tue 27 Thu 29 July Mon 03 Wed 05 Fri 07 Jul 09 Tue 11

#path	ts	id.orig_h	id.resp_h	id.res...	pr...	orig_by...	resp_b...	duration
conn	2023-06-23T19:56:05.265660Z	10.2.128.46	34.217.28.127	8888	tcp	578633	293544	54595.98781490326
conn	2023-06-24T11:06:36.504202Z	10.2.128.46	34.217.28.127	8888	tcp	922555	468018	86165.56323504448
conn	2023-06-25T11:03:12.134542Z	10.2.128.46	34.217.28.127	8888	tcp	917765	465588	86411.59540605545
conn	2023-06-26T11:03:57.753312Z	10.2.128.46	34.217.28.127	8888	tcp	925429	469476	86431.94644498825
conn	2023-06-27T11:04:57.499819Z	10.2.128.46	34.217.28.127	8888	tcp	922075	467775	86434.76174807549
conn	2023-06-28T11:06:05.920160Z	10.2.128.46	34.217.28.127	8888	tcp	913933	463644	86264.06125593185
conn	2023-06-29T11:04:40.982214Z	10.2.128.46	34.217.28.127	8888	tcp	917285	465345	86246.77599596977
conn	2023-06-30T11:03:00.758679Z	10.2.128.46	34.217.28.127	8888	tcp	930218	471906	86641.78966617584
conn	2023-07-01T11:07:32.745721Z	10.2.128.46	34.217.28.127	8888	tcp	924950	469233	86119.5669169426
conn	2023-07-02T11:03:27.101587Z	10.2.128.46	34.217.28.127	8888	tcp	914891	464130	86547.97586083412
conn	2023-07-03T11:06:26.441724Z	10.2.128.46	34.217.28.127	8888	tcp	923992	468747	86343.44373989105
conn	2023-07-04T11:06:26.885952Z	10.2.128.46	34.217.28.127	8888	tcp	921117	467289	86142.82350301743

Query status: Done Hits: 21 Speed: 771.39 GB/s EPS: 1.04M Work: 12 Completion: 100%

© 2023 Corelight Privacy Policy



# Empire: http agent configuration

(Empire: agents) > agents

Agents ID	Name	Language	Internal IP	Username	Process	PID	Delay	Last Seen	Listener
7V55CF7T	7V55CF7T	python	10.2.128.198	ubuntu	python3	731189	5/0.0	2023-03-09 06:34:36 UTC (6 months ago)	http
83MWG8HH	83MWG8HH	python	10.2.128.198	ubuntu	python3	563738	5/0.0	2023-09-20 14:34:33 UTC (2 seconds ago)	http
HILV5BKC	HILV5BKC	python	10.2.128.198	ubuntu	python3	838479	5/0.0	2023-08-17 06:13:26 UTC (a month ago)	http

Configurable delay/interval and jitter

Configurable URIs and user agent

(Empire: 83MWG8HH) > info

Agent Options	session_id	83MWG8HH
name	listener	83MWG8HH
listener	host_id	http
host_id	hostname	1
hostname	language	ip-10-2-128-198
language	language_version	python
language_version	delay	3.8
delay	jitter	5
jitter	external_ip	0.0
external_ip	internal_ip	100.21.194.208
internal_ip	username	10.2.128.198
username	high_integrity	ubuntu
high_integrity	process_id	False
process_id	process_name	563738
process_name	os_details	python3
os_details	nonce	Linux,ip-10-2-128-198,5.4.0-1029-aws,#30-Ubuntu SMP Tue Oct 20 10:06:38 UTC 2020,x86_64
nonce	checkin_time	6771358990493704
checkin_time	lastseen_time	2023-09-20T14:30:56+00:00
lastseen_time	parent	2023-09-20T14:39:19+00:00
parent	children	
children	servers	
servers	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
profile	functions	
functions	kill_date	
kill_date	working_hours	
working_hours	lost_limit	60
lost_limit		





# Empire: beaoning every ~5 seconds

corelight | INVESTIGATOR

Event List

Queries

+01:00 London

2023-09-20 15:35:01  
2023-09-20 15:36:01

Live

Run

```
1 #path = http
2 | id.orig_h=10.2.128.198
3 | id.resp_h=35.87.21.43
```

“Profile”

Zero req. bytes  
Constant resp bytes

Show suggestions (^Space)

Language syntax Event List widget

Results

ts	path	id.orig_h	id.resp_h	method	id.resp_p	host	uri	request_body_len	response_body...
2023-09-20T14:35:03.567041Z	ttp	10.2.128.198	35.87.21.43	GET	80	35.87.21.43:80	/news.php	0	1291
2023-09-20T14:35:08.587121Z	ttp	10.2.128.198	35.87.21.43	GET	80	35.87.21.43:80	/admin/get.php	0	1291
2023-09-20T14:35:13.607742Z	ttp	10.2.128.198	35.87.21.43	GET	80	35.87.21.43:80	/login/process.php	0	1291
2023-09-20T14:35:18.627389Z	ttp	10.2.128.198	35.87.21.43	GET	80	35.87.21.43:80	/admin/get.php	0	1291
2023-09-20T14:35:23.648824Z	ttp	10.2.128.198	35.87.21.43	GET	80	35.87.21.43:80	/admin/get.php	0	1291
2023-09-20T14:35:28.668117Z	ttp	10.2.128.198	35.87.21.43	GET	80	35.87.21.43:80	/login/process.php	0	1291
2023-09-20T14:35:33.688928Z	ttp	10.2.128.198	35.87.21.43	GET	80	35.87.21.43:80	/admin/get.php	0	1291
2023-09-20T14:35:38.710277Z	ttp	10.2.128.198	35.87.21.43	GET	80	35.87.21.43:80	/news.php	0	1291
2023-09-20T14:35:43.730060Z	ttp	10.2.128.198	35.87.21.43	GET	80	35.87.21.43:80	/login/process.php	0	1291
2023-09-20T14:35:48.746724Z	ttp	10.2.128.198	35.87.21.43	GET	80	35.87.21.43:80	/news.php	0	1291
2023-09-20T14:35:53.767159Z	ttp	10.2.128.198	35.87.21.43	GET	80	35.87.21.43:80	/admin/get.php	0	1291
2023-09-20T14:35:58.787711Z	ttp	10.2.128.198	35.87.21.43	GET	80	35.87.21.43:80	/login/process.php	0	1291

Query status: Done Hits: 12 Speed: 0.22 GB/s EPS: 77k Work: 0 Completion: 100%

© 2023 Corelight | Privacy Policy



# Empire: shell activity pattern

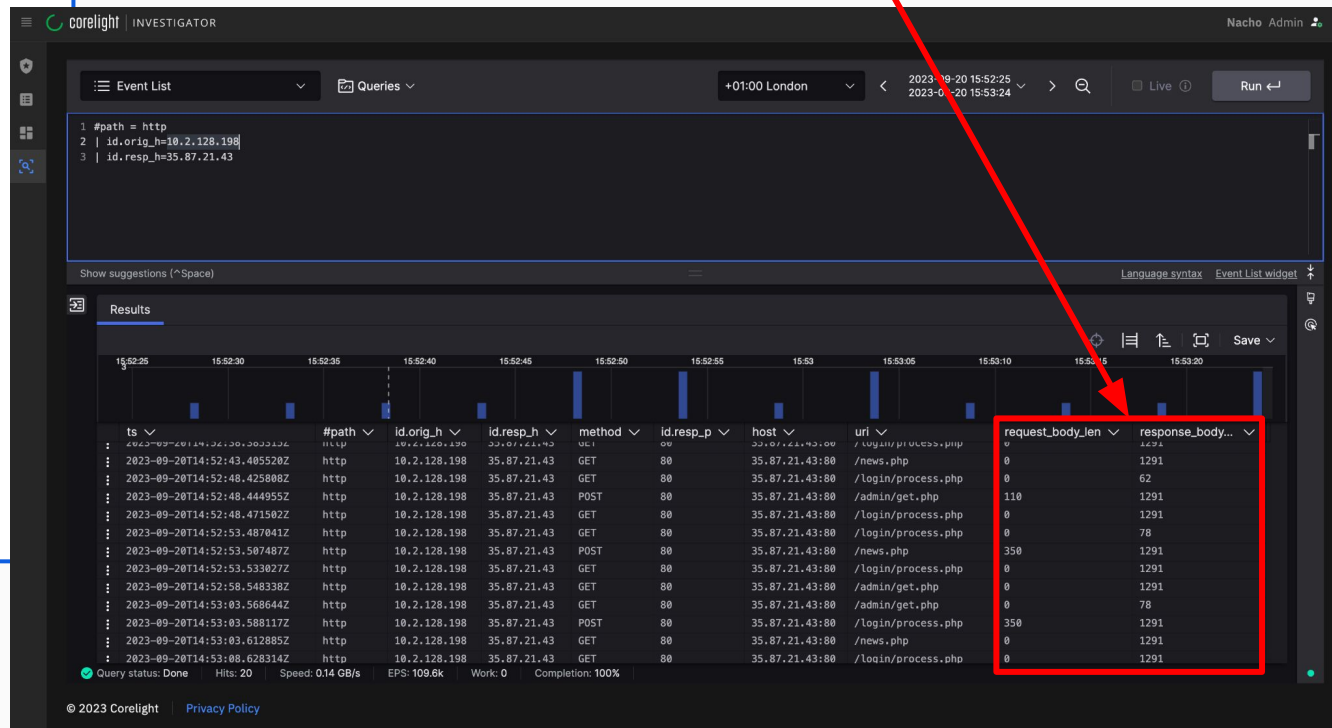
```
(83MwG8HH) /home/ubuntu/apps/empire_client > date
Wed Sep 20 14:52:08 UTC 2023
(83MwG8HH) /home/ubuntu/apps/empire_client > whoami
ubuntu
(83MwG8HH) /home/ubuntu/apps/empire_client > ls /
-rwxr-xr-x root root 06:44:08 03/14/21 0.000000 B sys
-rwxr-xr-x root root 06:44:06 03/14/21 0.000000 B proc
-rwxr-xr-x root root 06:22:30 08/10/23 4.000000 KB lib
-rwxr-xr-x root root 23:25:24 10/26/20 4.000000 KB srv
-rwxr-xr-x root root 14:29:50 09/20/23 1.000000 KB run
-rwxr-xr-x root root 06:10:57 07/29/23 4.000000 KB boot
-rwxr-xr-x root root 14:52:18 09/20/23 4.000000 KB tmp
-rwxr-xr-x root root 23:25:24 10/26/20 4.000000 KB opt
-rwxr-xr-x root root 22:56:37 08/30/23 3.000000 KB dev
-rwxr-xr-x root root 06:01:19 06/20/23 4.000000 KB snap
-rwxr-xr-x root root 23:32:25 10/26/20 16.000000 KB lost+found
-rwxr-xr-x root root 06:50:40 09/14/23 20.000000 KB/sbin
-rwxr-xr-x root root 16:39:57 02/18/21 4.000000 KB root
-rwxr-xr-x root root 23:28:20 10/26/20 4.000000 KB usr
-rwxr-xr-x root root 05:26:05 01/01/21 4.000000 KB home
-rwxr-xr-x root root 06:47:30 09/19/23 4.000000 KB etc
-rwxr-xr-x root root 06:33:46 09/15/23 36.000000 KB bin
-rwxr-xr-x root root 23:30:58 10/26/20 4.000000 KB var
-rwxr-xr-x root root 23:25:24 10/26/20 4.000000 KB mnt
-rwxr-xr-x root root 23:25:24 10/26/20 4.000000 KB media
-rwxr-xr-x root root 06:31:54 03/03/22 4.000000 KB lib64
-rwxr-xr-x root root 23:25:18 10/26/20 4.000000 KB libx32
-rwxr-xr-x root root 23:25:18 10/26/20 4.000000 KB lib32

(83MwG8HH) /home/ubuntu/apps/empire_client >
(83MwG8HH) /home/ubuntu/apps/empire_client > pwd
/home/ubuntu/apps/empire_client
(83MwG8HH) /home/ubuntu/apps/empire_client > ls ../home/
-rwxr-xr-x ubuntu ubuntu 14:52:51 03/03/23 1.000000 KB bash_stager.sh
-rw-rw-r-- ubuntu ubuntu 14:32:32 09/20/23 0.000000 B iwashere_202309
-rw-rw-r-- ubuntu ubuntu 12:22:44 05/15/23 0.000000 B iwashere.txt

(83MwG8HH) /home/ubuntu/apps/empire_client > ls ~/
-rwxr-xr-x ubuntu ubuntu 14:52:51 03/03/23 1.000000 KB bash_stager.sh
-rw-rw-r-- ubuntu ubuntu 14:32:32 09/20/23 0.000000 B iwashere_202309
-rw-rw-r-- ubuntu ubuntu 12:22:44 05/15/23 0.000000 B iwashere.txt

(83MwG8HH) /home/ubuntu/apps/empire_client > ls /home/ubuntu/
-rwxr-xr-x ubuntu ubuntu 14:52:51 03/03/23 1.000000 KB bash_stager.sh
-rw-rw-r-- ubuntu ubuntu 14:32:32 09/20/23 0.000000 B iwashere_202309
-rw-rw-r-- ubuntu ubuntu 12:22:44 05/15/23 0.000000 B iwashere.txt
```

Requests every ~5s with back and forth data





# Sliver: beacon with --seconds 30 --jitter 5

```
[server] sliver > generate beacon --os linux --http 18.236.93.116 --seconds 30 --jitter 5
```

```
[*] Generating new linux/amd64 beacon implant binary (30s)
[*] Symbol obfuscation is enabled
: Compiling, please wait ...
: Compiling, please wait ...
: Compiling, please wait ...
: Compiling, please wait ...
: Compiling, please wait ...
: Compiling, please wait ...
: Compiling, please wait ...
: Compiling, please wait ...
[*] Build completed in 1m22s
[*] Implant saved to /home/ubuntu/apps/sliver_server/ROTTEN_KEY
```

corelight INVESTIGATOR

Event List

1 #path=http  
2 | id.orig\_h=10.2.128.87  
3 | id.res\_h=18.236.93.116

Results

POST and GET

Randomized URIs

#path	ts	id.orig_h	id.res...	me...	status_c...	host	uri
http	2023-09-20T08:42:31.911047Z	10.2.128.87	80	POST	202	18.236.93.116	/rest/v1/admin.php?e=562n94520
http	2023-09-20T08:42:31.913194Z	10.2.128.87	80	GET	200	18.236.93.116	/bundle/umd/umd/bundles/umd/jquery.min.js?_=71895889
http	2023-09-20T08:43:02.788001Z	10.2.128.87	80	POST	202	18.236.93.116	/rest/rest/samples.php?v=633h91974
http	2023-09-20T08:43:02.793074Z	10.2.128.87	80	GET	200	18.236.93.116	/bundle/bundles/bundle/bundle/scripts/js/route.js?v=83752p221
http	2023-09-20T08:43:34.128300Z	10.2.128.87	80	POST	202	18.236.93.116	/login.php?k=14892380
http	2023-09-20T08:43:34.129844Z	10.2.128.87	80	GET	200	18.236.93.116	/js/bundle/jscript/umd/jquery.js?r=8d2344137
http	2023-09-20T08:44:08.601424Z	10.2.128.87	80	POST	202	18.236.93.116	/sign-up.php?x=q6v3913296
http	2023-09-20T08:44:08.603286Z	10.2.128.87	80	GET	200	18.236.93.116	/scripts/assets/bootstrap.js?h=57175o081
http	2023-09-20T08:44:39.854944Z	10.2.128.87	80	POST	202	18.236.93.116	/actions/samples.php?z=u48512167
http	2023-09-20T08:44:39.856788Z	10.2.128.87	80	GET	200	18.236.93.116	/bootstrap.min.js?i=7_30271n7
http	2023-09-20T08:45:12.155601Z	10.2.128.87	80	POST	202	18.236.93.116	/actions/v1/login.php?a=666h892o0
http	2023-09-20T08:45:12.157127Z	10.2.128.87	80	GET	200	18.236.93.116	/jquery.min.js?l=45v916954

Query status: Done Hits: 20 Speed: 0.27 GB/s EPS: 123.5k Work: 0 Completion: 100%

© 2023 Corelight Privacy Policy



# Sliver: beaconing -> session -> shell

corelight | INVESTIGATOR Nacho Admin

Event List Queries -00:00 UTC 2023-09-22 10:15:34 2023-09-22 10:24:00 Live Run

```
1 #path=http
2 | id.orig_h = "10.2.128.87"
3 | id.resp_h = "18.236.93.116"
```

Beaconing Session Shell

Results

ts	#path	id.res...	me...	status_c...	host	request_body...	response_body...	url
2023-09-22T10:23:19.251722Z	http	80	POST	202	18.236.93.116	746	0	/rest/api.php?p=98588656
2023-09-22T10:23:19.253808Z	http	80	POST	202	18.236.93.116	300	0	/actions/login.php?o=3152kk2012
2023-09-22T10:23:19.254485Z	http	80	POST	202	18.236.93.116	242	0	/signin.php?i=77s050063
2023-09-22T10:23:19.252816Z	http	80	GET	204	18.236.93.116	0	0	/email.js?c=72279469
2023-09-22T10:23:20.458614Z	http	80	GET	200	18.236.93.116	0	1141	/umd/scripts/bundles/bundle/email.js?j=1607b1656
2023-09-22T10:23:20.529988Z	http	80	POST	202	18.236.93.116	787	0	/actions/index.php?v=527ay8897
2023-09-22T10:23:20.529882Z	http	80	GET	200	18.236.93.116	0	192	/bundle/js/javascript/jscript/assets/bundles/route.js?j=754p28480
2023-09-22T10:23:21.116373Z	http	80	POST	202	18.236.93.116	151	0	/v1/rest/rpc.php?_k49335n736
2023-09-22T10:23:21.115594Z	http	80	GET	200	18.236.93.116	0	152	/bundles/umd/jquery.min.js?b=16859r741
2023-09-22T10:23:22.089228Z	http	80	POST	202	18.236.93.116	106	0	/rest/rest/signin.php?g=518e76542
2023-09-22T10:23:22.089356Z	http	80	POST	202	18.236.93.116	1194	0	/v1/sign-up.php?n=28864215
2023-09-22T10:23:22.088627Z	http	80	GET	200	18.236.93.116	0	152	/jquery.min.js?l=5776666i0
2023-09-22T10:23:22.265816Z	http	80	POST	202	18.236.93.116	143	0	/v1/sign-up.php?k=5402k9711
2023-09-22T10:23:22.264915Z	http	80	POST	202	18.236.93.116	647	0	/rest/samples.php?i=5064c5081
2023-09-22T10:23:22.263862Z	http	80	GET	200	18.236.93.116	0	1116	/jscript/js/bundle/assets/umd/umd/js/route.js?t=161883595
2023-09-22T10:23:22.600611Z	http	80	POST	202	18.236.93.116	143	0	/v1/actions/rpc.php?p=14291160
2023-09-22T10:23:22.601250Z	http	80	POST	202	18.236.93.116	199	0	/rest/sign-up.php?o=922n63160

Query status: Done Hits: 321 Speed: 0.19 GB/s EPS: 127k Work: 3 Completion: 100%

© 2023 Corelight Privacy Policy



# Metasploit/meterpreter with http listener: beacons every ~10 seconds

corelight INVESTIGATOR

Event List

1 #path=http  
2 | id.orig\_h=10.2.128.138  
3 | id.resp\_h=52.27.49.238

Results

#path	ts	id.orig_h	id.resp_p	method	status_code	host	uri
http	2023-09-20T08:42:56.809688Z	10.2.128.138	8080	GET	200	52.27.49.238:8080	/k9_bwk-T9a85QD9BXfU0ZwuJG80BkZK2BwdgVe58DzKzCP6q5KvD1DbkZ170ceaklWZmDxXjs2n5rXtuIjmc6TEwg-8ZL/
http	2023-09-20T08:43:06.910337Z	10.2.128.138	8080	GET	200	52.27.49.238:8080	/k9_bwk-T9a85QD9BXfU0ZwuJG80BkZK2BwdgVe58DzKzCP6q5KvD1DbkZ170ceaklWZmDxXjs2n5rXtuIjmc6TEwg-8ZL/
http	2023-09-20T08:43:17.011094Z	10.2.128.138	8080	GET	200	52.27.49.238:8080	/k9_bwk-T9a85QD9BXfU0ZwuJG80BkZK2BwdgVe58DzKzCP6q5KvD1DbkZ170ceaklWZmDxXjs2n5rXtuIjmc6TEwg-8ZL/
http	2023-09-20T08:43:27.111928Z	10.2.128.138	8080	GET	200	52.27.49.238:8080	/k9_bwk-T9a85QD9BXfU0ZwuJG80BkZK2BwdgVe58DzKzCP6q5KvD1DbkZ170ceaklWZmDxXjs2n5rXtuIjmc6TEwg-8ZL/
http	2023-09-20T08:43:37.212795Z	10.2.128.138	8080	GET	200	52.27.49.238:8080	/k9_bwk-T9a85QD9BXfU0ZwuJG80BkZK2BwdgVe58DzKzCP6q5KvD1DbkZ170ceaklWZmDxXjs2n5rXtuIjmc6TEwg-8ZL/
http	2023-09-20T08:43:47.313809Z	10.2.128.138	8080	GET	200	52.27.49.238:8080	/k9_bwk-T9a85QD9BXfU0ZwuJG80BkZK2BwdgVe58DzKzCP6q5KvD1DbkZ170ceaklWZmDxXjs2n5rXtuIjmc6TEwg-8ZL/
http	2023-09-20T08:43:57.413967Z	10.2.128.138	8080	GET	200	52.27.49.238:8080	/k9_bwk-T9a85QD9BXfU0ZwuJG80BkZK2BwdgVe58DzKzCP6q5KvD1DbkZ170ceaklWZmDxXjs2n5rXtuIjmc6TEwg-8ZL/
http	2023-09-20T08:44:07.514352Z	10.2.128.138	8080	GET	200	52.27.49.238:8080	/k9_bwk-T9a85QD9BXfU0ZwuJG80BkZK2BwdgVe58DzKzCP6q5KvD1DbkZ170ceaklWZmDxXjs2n5rXtuIjmc6TEwg-8ZL/
http	2023-09-20T08:44:17.614508Z	10.2.128.138	8080	GET	200	52.27.49.238:8080	/k9_bwk-T9a85QD9BXfU0ZwuJG80BkZK2BwdgVe58DzKzCP6q5KvD1DbkZ170ceaklWZmDxXjs2n5rXtuIjmc6TEwg-8ZL/
http	2023-09-20T08:44:27.716013Z	10.2.128.138	8080	GET	200	52.27.49.238:8080	/k9_bwk-T9a85QD9BXfU0ZwuJG80BkZK2BwdgVe58DzKzCP6q5KvD1DbkZ170ceaklWZmDxXjs2n5rXtuIjmc6TEwg-8ZL/
http	2023-09-20T08:44:37.815441Z	10.2.128.138	8080	GET	200	52.27.49.238:8080	/k9_bwk-T9a85QD9BXfU0ZwuJG80BkZK2BwdgVe58DzKzCP6q5KvD1DbkZ170ceaklWZmDxXjs2n5rXtuIjmc6TEwg-8ZL/
http	2023-09-20T08:44:47.916080Z	10.2.128.138	8080	GET	200	52.27.49.238:8080	/k9_bwk-T9a85QD9BXfU0ZwuJG80BkZK2BwdgVe58DzKzCP6q5KvD1DbkZ170ceaklWZmDxXjs2n5rXtuIjmc6TEwg-8ZL/
http	2023-09-20T08:44:58.016874Z	10.2.128.138	8080	GET	200	52.27.49.238:8080	/k9_bwk-T9a85QD9BXfU0ZwuJG80BkZK2BwdgVe58DzKzCP6q5KvD1DbkZ170ceaklWZmDxXjs2n5rXtuIjmc6TEwg-8ZL/
http	2023-09-20T08:45:08.117422Z	10.2.128.138	8080	GET	200	52.27.49.238:8080	/k9_bwk-T9a85QD9BXfU0ZwuJG80BkZK2BwdgVe58DzKzCP6q5KvD1DbkZ170ceaklWZmDxXjs2n5rXtuIjmc6TEwg-8ZL/
http	2023-09-20T08:45:18.218721Z	10.2.128.138	8080	GET	200	52.27.49.238:8080	/k9_bwk-T9a85QD9BXfU0ZwuJG80BkZK2BwdgVe58DzKzCP6q5KvD1DbkZ170ceaklWZmDxXjs2n5rXtuIjmc6TEwg-8ZL/
http	2023-09-20T08:45:28.319530Z	10.2.128.138	8080	GET	200	52.27.49.238:8080	/k9_bwk-T9a85QD9BXfU0ZwuJG80BkZK2BwdgVe58DzKzCP6q5KvD1DbkZ170ceaklWZmDxXjs2n5rXtuIjmc6TEwg-8ZL/
http	2023-09-20T08:45:38.420053Z	10.2.128.138	8080	GET	200	52.27.49.238:8080	/k9_bwk-T9a85QD9BXfU0ZwuJG80BkZK2BwdgVe58DzKzCP6q5KvD1DbkZ170ceaklWZmDxXjs2n5rXtuIjmc6TEwg-8ZL/

Query status: Done Hits: 20 Speed: 0.24 GB/s EPS: 74.8k Work: 0 Completion: 100%

© 2023 Corelight Privacy Policy

## The Application Protocol

Once the Meterpreter connect URL is requested, the actual dispatch loop starts to run. The Meterpreter payload will make repeated requests with a HTTP body consistent of "RCV". Any queued commands will be returned to the payload, which will process them individually, and return the results in a following request. If no commands were returned as a result of a "RCV" request, the payload will double the interval until the next request, with a maximum that is generally about 10 seconds.

Additional details about the configuration of the HTTP transport can be found on the [transport control](#) wiki page.



# Beaconing configurations in C2 Frameworks

## Caldera



### Agents

Groups are collections of agents so hosts can be compromised simultaneously. You must deploy at least 1 agent in order to run an operation.

[Click here to deploy an agent](#)

### GLOBAL TIMERS

Beacon min (seconds)

Beacon max (seconds)

Watchdog (seconds)

Untrusted (seconds)

### STEALTH

plain-text obfuscation

Jitter (min/max) sec

adjust visibility

```
[Empire] Post-Exploitation Framework
=====
[Version] 5.0.0-beta2 | [Web] https://github.com/BC-SECURITY/Empire
[Starkiller] Multi-User GUI | [Web] https://github.com/BC-SECURITY/Starkiller
[Documentation] | [Web] https://bc-security.gitbook.io/empire-wiki/
=====
```

# EMPIRE

412 modules currently loaded  
1 listeners currently active  
1 agents currently active

INFO: Connected to localhost

(Empire) >

```
(Empire) > uselistener http
http
http_com
http_foreign
http_hop
http_malleable
```

```
(Empire) > uselistener http
```

```
id      http
authors Will Schroeder, @harmj0y, https://twitter.com/harmj0y
description Starts a http[s] listener (PowerShell or Python) that uses a GET/POST approach.
category client_server
```

Name	Value	Required	Description
Name	http	True	Name for the listener.
Host	http://172.31.36.104	True	Hostname/IP for staging.
BindIP	0.0.0.0	True	The IP to bind to on the control server.
Port		True	Port for the listener.
Launcher	powershell -noP -sta -w 1 -enc	True	Launcher string.
StagingKey	>+[YSIMR-DA/8.cFb7eu9*2)EIG&IQ	True	Staging key for initial agent negotiation.
DefaultDelay	5	True	Agent delay/reach back interval (in seconds).
DefaultJitter	0.0	True	Jitter in agent reachback interval (0.0-1.0).
DefaultLostLimit	60	True	Number of missed checkins before exiting
DefaultProfile	/admin/get.php,/news.php,/login/process.php Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko	True	Default communication profile for the agent.
CertPath		False	Certificate path for https listeners.
KillDate		False	Date for the listener to exit (MM/dd/yyyy).
WorkingHours		False	Hours for the agent to operate (09:00-17:00).
Headers	Server:Microsoft-IIS/7.5	True	Headers for the control server.
Cookie	nqjWQM0grERg	False	Custom Cookie Name
StagerURI		False	URI for the stager. Must use /download/. Example: /download/stager.php
UserAgent	default	False	User-agent string to use for the staging request (default, none, or other).
Proxy	default	False	Proxy to use for request (default, none, or other).
ProxyCreds	default	False	Proxy credentials ((domain\username:password) to use

## Meterpreter

### The Application Protocol

Once the Meterpreter connect URL is requested, the actual dispatch loop starts to run. The Meterpreter payload will make repeated requests with a HTTP body consistent of "RECV". Any queued commands will be returned to the payload, which will process them individually, and return the results in a following request. If no commands were returned as a result of a "RECV" request, the payload will double the interval until the next request, with a maximum that is generally about 10 seconds.

Additional details about the configuration of the HTTP transport can be found on the [transport control](#) wiki page.


# How about malware?\*



what is the range of frequencies at which malware is programmed to beacon to c2 servers? 

*\*The mandatory ChatGPT slide*

Index	Malware	Beaconing Frequency
1	Mirai	60 seconds
2	XOR DDoS	120 seconds
3	Andromeda/Gamarue	180 seconds
4	Trickbot	180-300 seconds
5	Emotet	15-30 minutes
6	GrandCrab	15-30 minutes
7	Ursnif	5-20 minutes
8	Dridex	30-45 minutes
9	Trickster	45-60 minutes
10	Qbot	60-90 minutes
11	Zeus	60-90 minutes
12	Ursnif/Gozi	90-120 minutes
13	Agent Tesla	120 minutes
14	NanoCore	5-10 hours
15	DarkComet	24 hours
16	Poison Ivy	24 hours
17	Carbanak	3-5 days
18	NetWire	7-14 days
19	njRAT	7-14 days
20	Ryuk	3-5 days
21	LockerGoga	15-30 minutes
22	Sodinokibi	15-30 minutes
23	GandCrab	20 minutes
24	REvil/Sodinokibi	20-30 minutes
25	Maze	30-60 minutes

I hope this updated table is helpful.  Regenerate response

Send a message 

Free Research Preview. ChatGPT may produce inaccurate information about people, places, or facts. [ChatGPT May 24 Version](#)

# Key observations

- C2 frameworks and malware:
  - 130+ frameworks listed in the [C2Matrix](#)
  - “Keep-alive” beacons
  - Periodicity: seconds to days + jitter (optional)
- Different channels/listeners (http, dns, etc.)
- Mixture of “beaconing patterns” and “interaction patterns”
- Network or measurement latencies

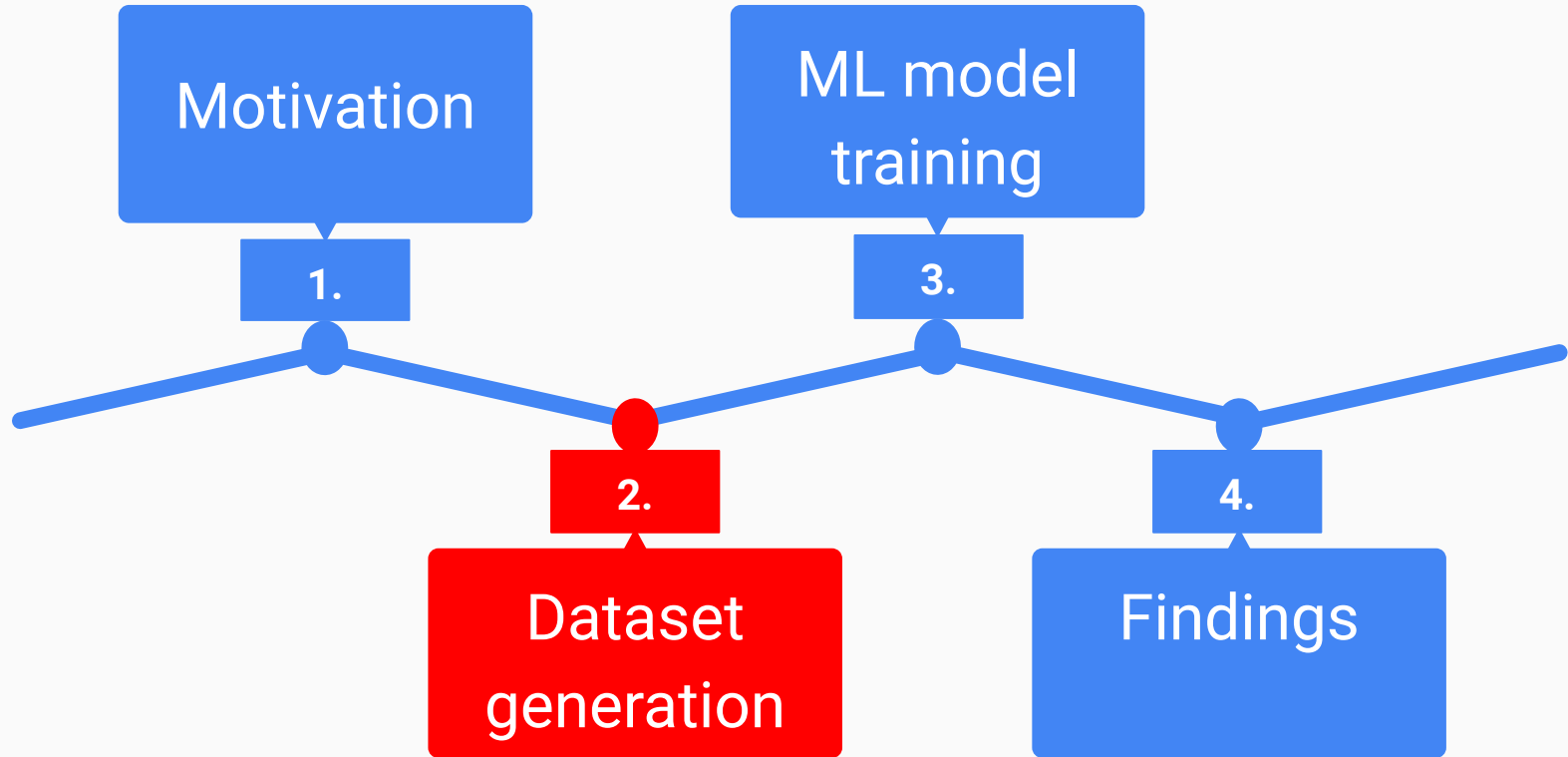


## Key ideas:

1. Focus on timestamp sequences only
2. We can generate synthetic beaconing patterns
3. A ML model should be able to detect *many* beaconing patterns

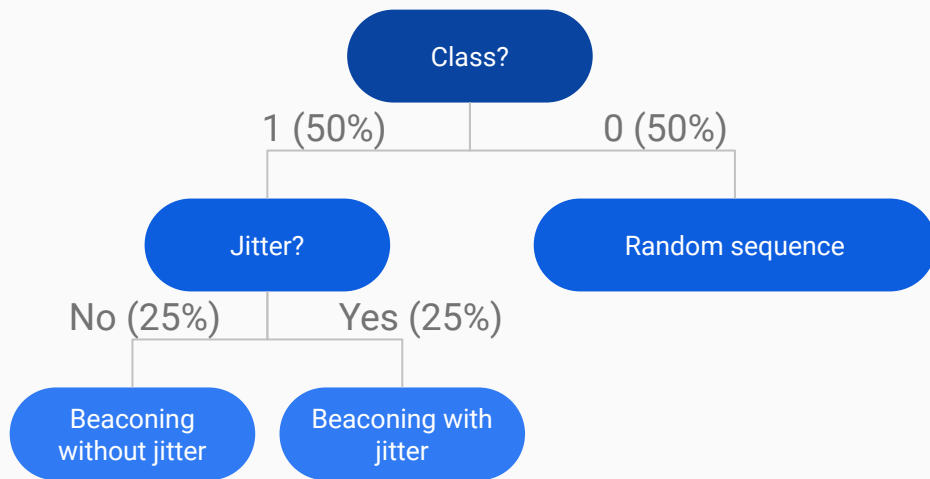


# Outline



# Dataset generation

## Generation strategy

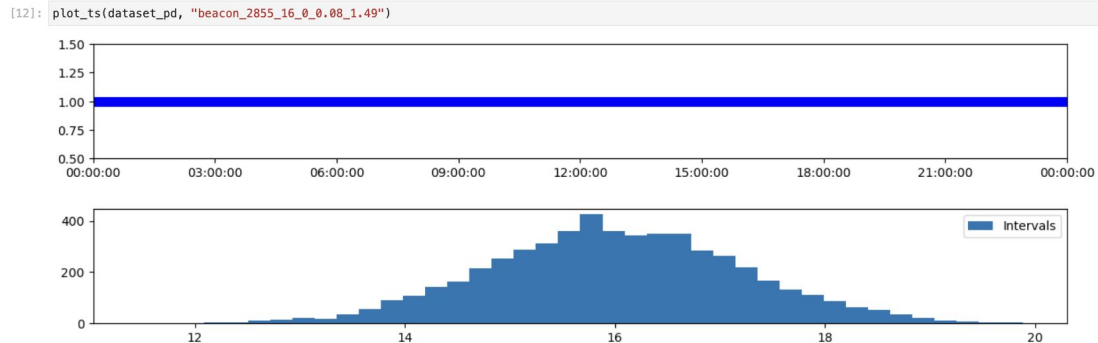


## Sequence parameters

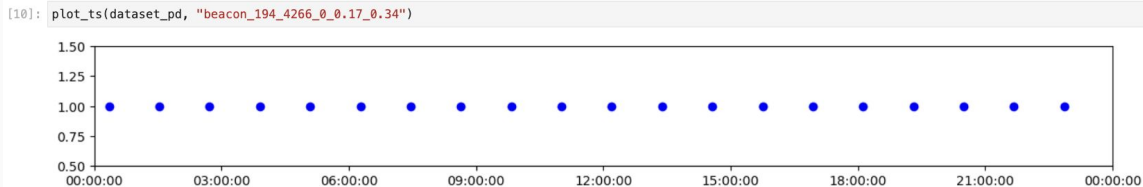
- Max duration: 24 hours
- First event:
  - Min: 0s
  - Max: (86400 - 1) seconds
- Frequency range:
  - min: 10 seconds
  - Max: 14400 seconds (4 hours)
- Jittering range:
  - Min: 1% of period
  - Max: 50% of period
- Network latency:
  - White/gaussian noise
  - min:= 0.0001 seconds
  - max = 2 seconds
- Random sequence: *next\_ts* sampled from a uniform distribution over [*current\_ts*, *end\_ts*]

# Beaconing without jitter (aka “perfect beacons”)

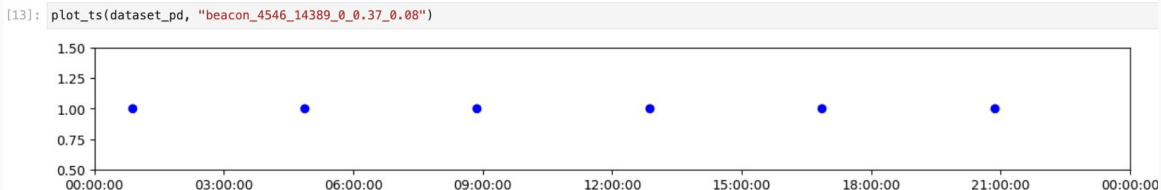
Period: 16 seconds



Period: 4266 seconds



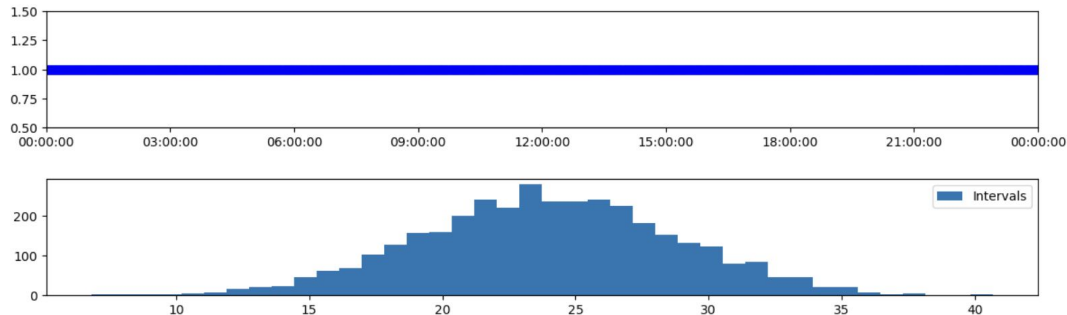
Period: 14389 seconds



# Beaconing with jitter

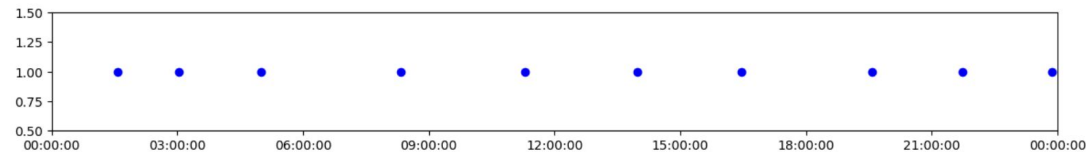
Period: 24 seconds  
Jitter: 19%

```
[16]: plot_ts(dataset_pd, "beacon_365_24_1_0.19_0.92")
```



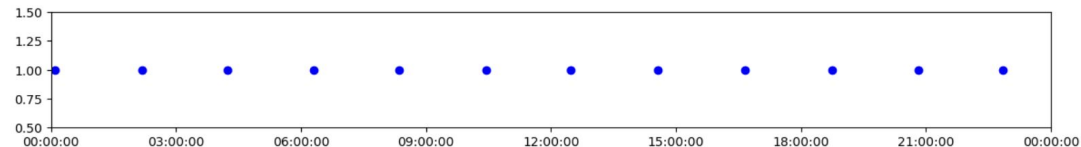
Period: 9618 seconds  
Jitter: 25%

```
[24]: plot_ts(dataset_pd, "beacon_4869_9618_1_0.25_1.96")
```



Period: 7455 seconds  
Jitter: 1%

```
[21]: plot_ts(dataset_pd, "beacon_1350_7455_1_0.01_0.85")
```

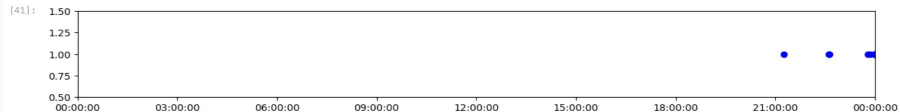


# Random sequences

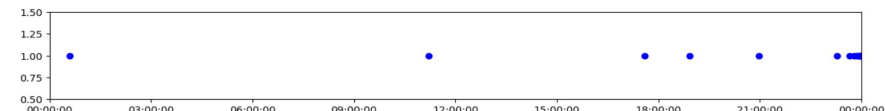
```
[24]: plot_ts(dataset_pd, "random_1454_0.14")
```



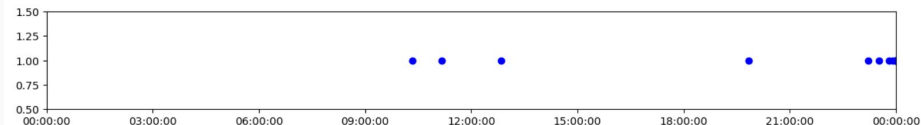
```
[41]: plot_ts(dataset_pd, "random_548_1.01")
```



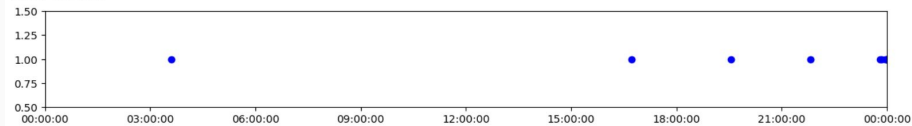
```
[120]: plot_ts(dataset_pd, "random_1255_1.7")
```



random\_2179\_0.82



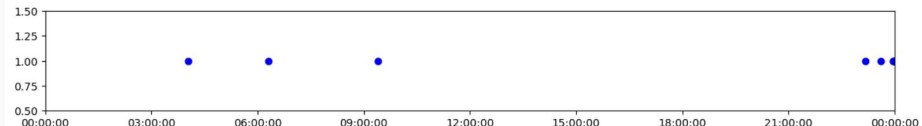
random\_4835\_0.29



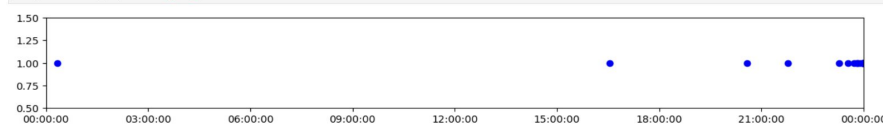
random\_2359\_0.97



random\_4125\_1.16



```
[131]: plot_ts(dataset_pd, "random_160_1.13")
```



# From timestamps to scaled intervals

Period: 4266s

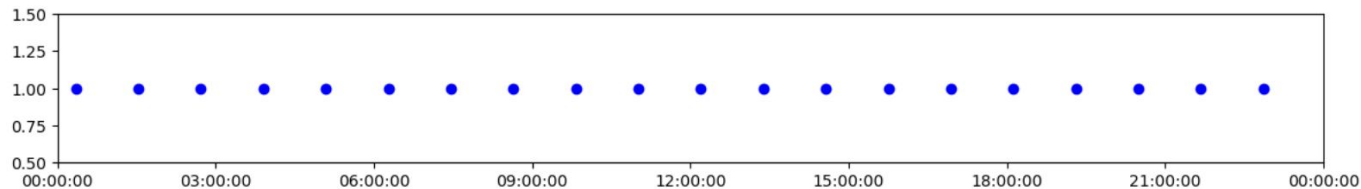


Intervals



Scaled intervals

```
[10]: plot_ts(dataset_pd, "beacon_194_4266_0_0.17_0.34")
```

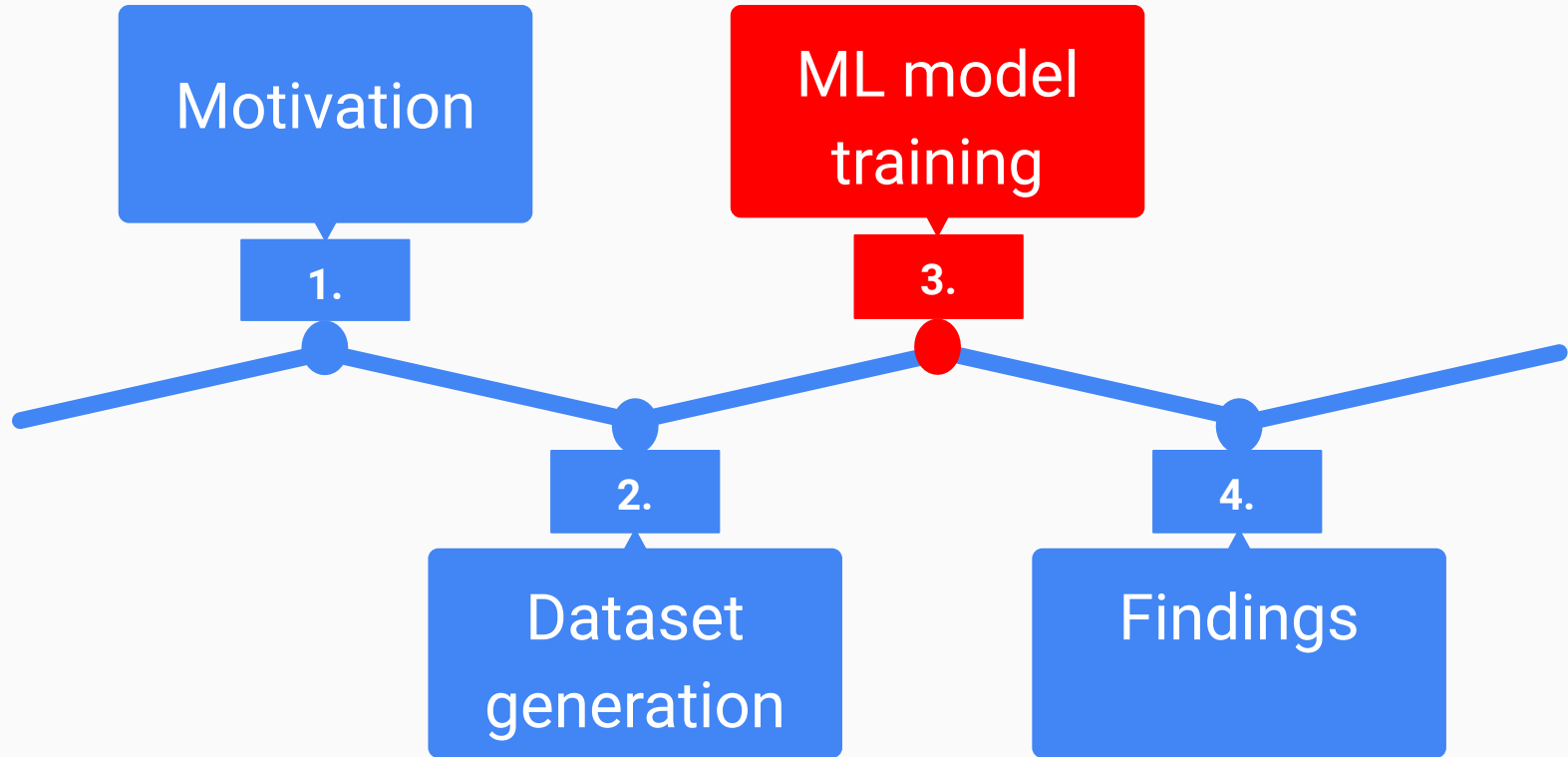


```
[162]: list(dataset_pd.loc[dataset_pd["id"] == "beacon_194_4266_0_0.17_0.34"]["intervals"])[0]
```

```
[162]: array([4265.844, 4266.239, 4265.774, 4266.082, 4265.929, 4266.359, 4265.386, 4266.172, 4266.114, 4266.283, 4266.083, 4265.675,
         4266.381, 4265.706, 4265.624, 4266.303, 4265.807, 4266.506, 4265.75 ])
```

```
[164]: intervals = list(dataset_pd.loc[dataset_pd["id"] == "beacon_194_4266_0_0.17_0.34"]["intervals"])[0]
intervals_mean = 602.487
intervals_var = 2978.388
intervals_std_np = (intervals - intervals_mean) / intervals_var
intervals_std_np
```

```
[164]: array([1.23 , 1.2301, 1.23 , 1.2301, 1.23 , 1.2302, 1.2298, 1.2301, 1.2301, 1.2301, 1.2301, 1.2299, 1.2302, 1.2299, 1.2299,
         1.2301, 1.23 , 1.2302, 1.2299])
```



# 1D Convolutional Neural Networks

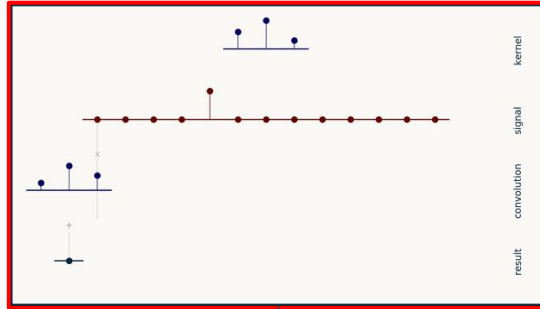
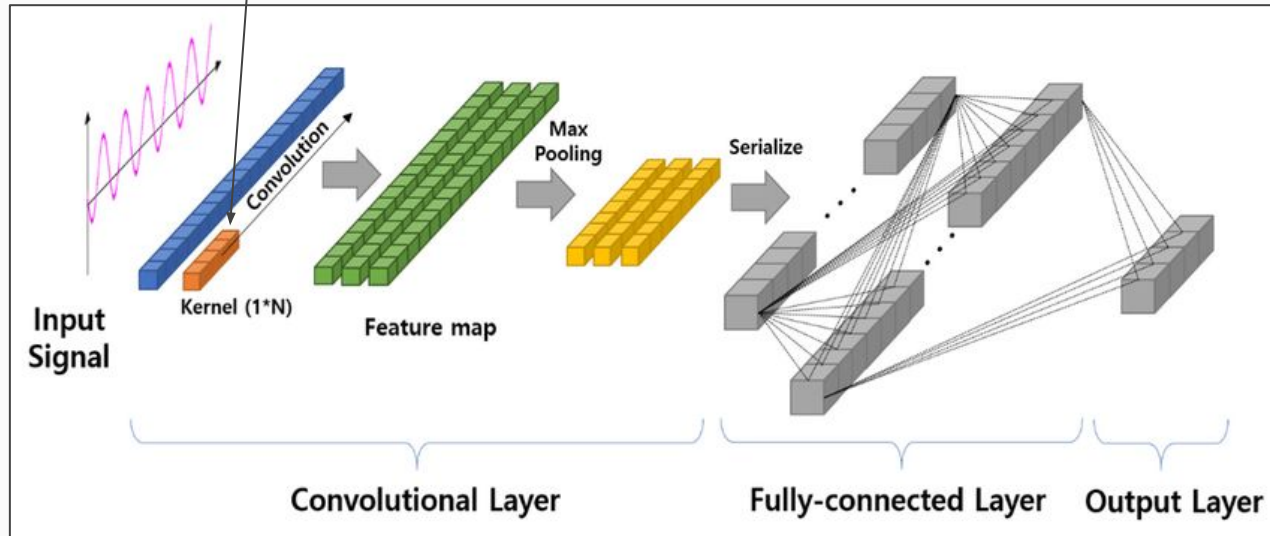


Figure: CNN with:

- 1 1D convolutional layer + 2 fully connected layers
- 3 filters (aka kernels)
- Filter length: 4





# 1D Convolutional Neural Network

## Model specification

```
[43]: u = Input(shape=(max_sequence_length,1))
      v = Conv1D(filters=32, kernel_size=12, strides=4, data_format="channels_last", padding="valid", activation='relu')(u)
      v = MaxPooling1D(2)(v)
      v = Dropout(rate=0.1)(v)
      v = Conv1D(filters=16, kernel_size=6, strides=2, data_format="channels_last", padding="valid", activation='relu')(v)
      v = MaxPooling1D(2)(v)
      v = Dropout(rate=0.1)(v)
      v = Flatten()(v)
      v = Dense(100)(v)
      v = Activation('relu')(v)
      v = Dropout(0.2)(v)
      v = Dense(2)(v)
      v = Activation('sigmoid')(v)

      model = Model(inputs=[u], outputs=v)

      model.compile(
          loss=tf.keras.losses.BinaryCrossentropy(),
          optimizer = 'nadam'
      )

      model.summary()
```

2 conv layers:

- 32 filters of size 12
- 16 filters of size 6

2 dense layers

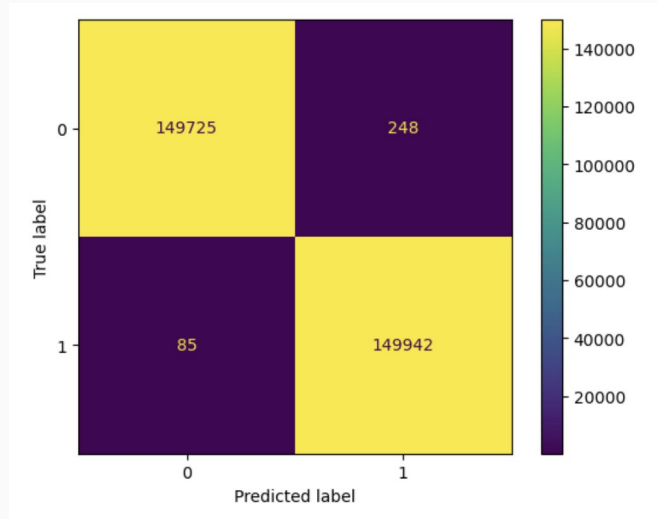
(aka fully connected)

2 outputs

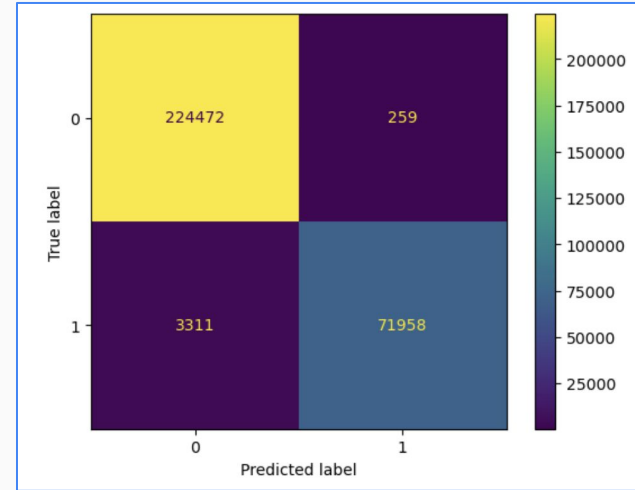
- Inputs: scaled intervals
  - max\_sequence\_length = 100
  - Arrays of shape (100, 1)
- Outputs:
  - Beaconsing probability
  - Jittering probability

# 1M sequences dataset: Test Results (left out data)

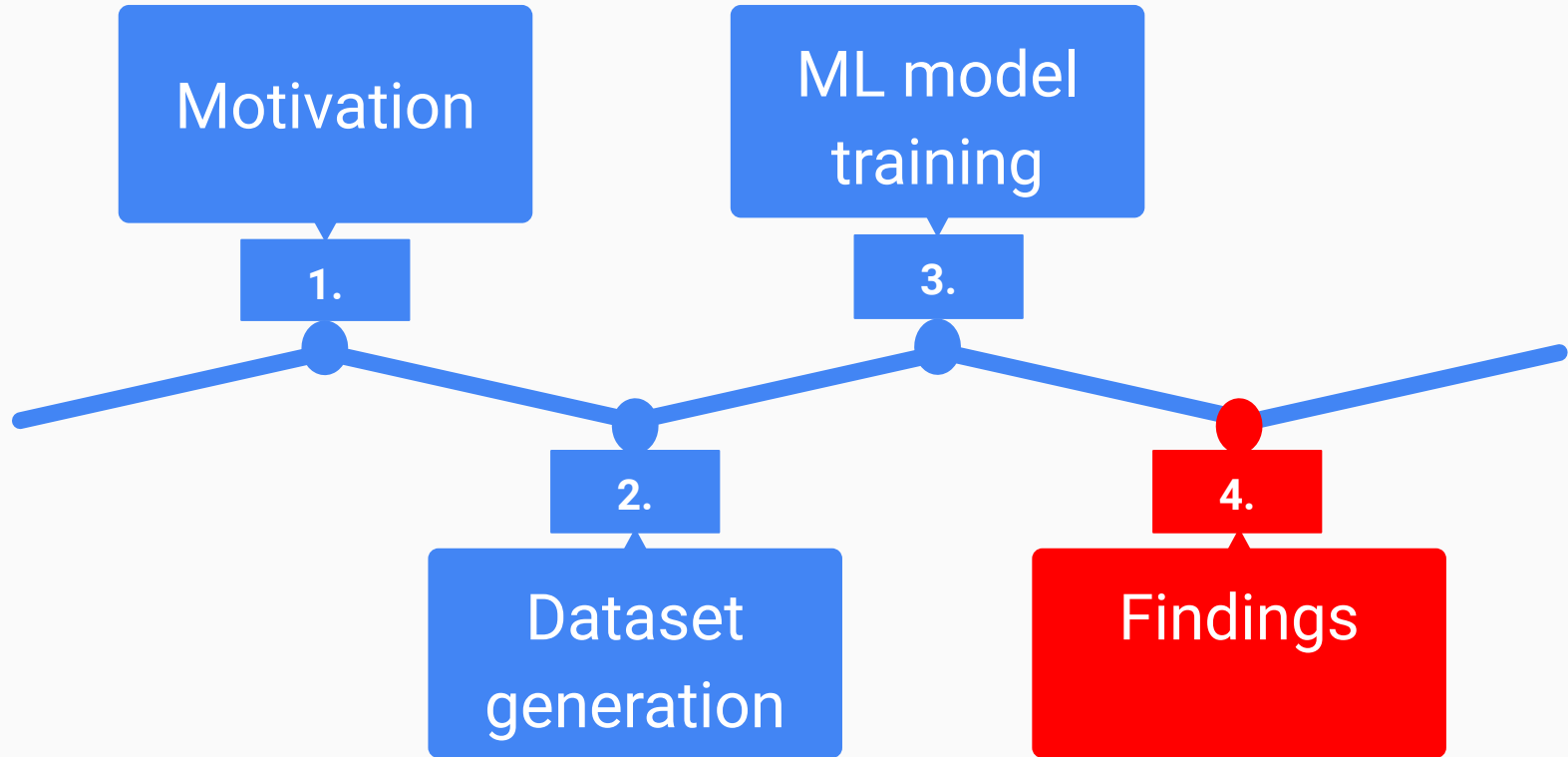
Beaconing output



Jittering output



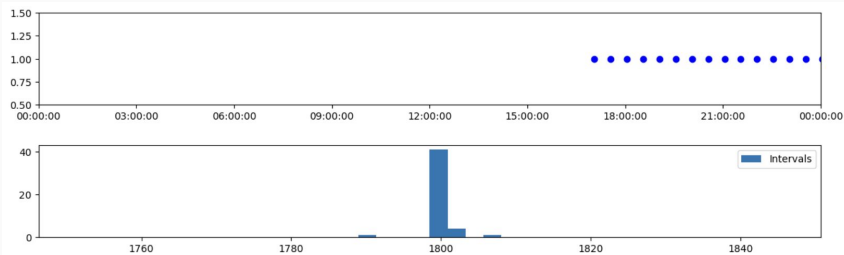
- FPs: random sequences that ~look like beaconing
- FNs:
  - Beaconing sequences with high jitter
  - Sequences with low beaconing frequency periods and high network latency



# Malware PCAP: Zeus 24 hours (link: [Malware of the Day - Zeus - Active Countermeasures](#))

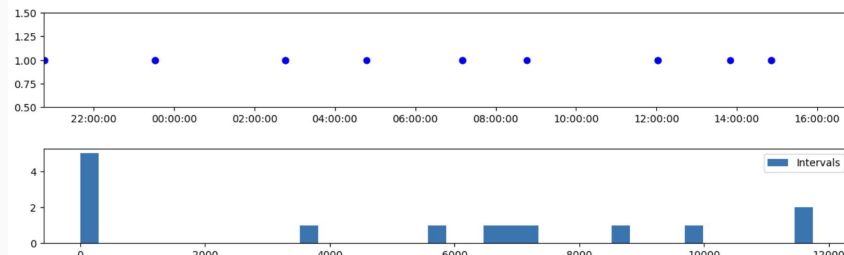
## Beaconing without jitter

192.168.99.53-> tile-service.weather.microsoft.com

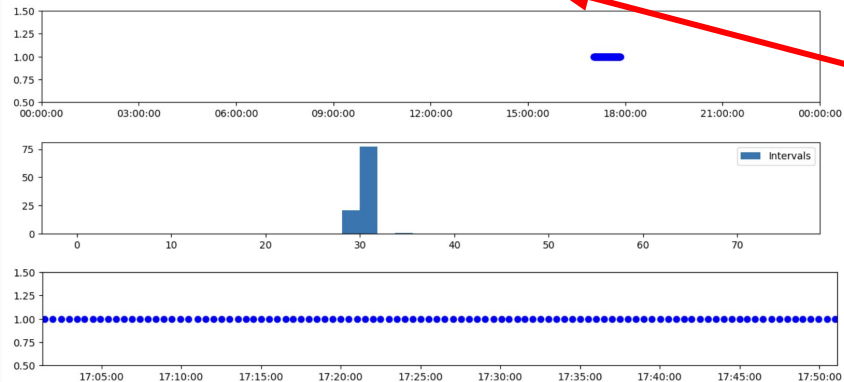


## Beaconing with jitter

192.168.99.53-> ctldl.windowsupdate.com



192.168.99.53-> mahamaya1ifesciences.com



<http://mahamaya1ifesciences.com/>

4

/ 90

4 security vendors flagged this URL as malicious

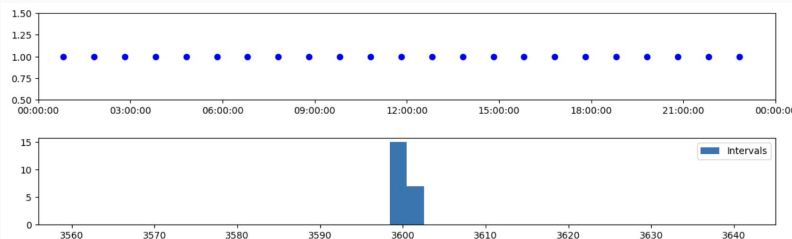
<http://mahamaya1ifesciences.com/>  
[mahamaya1ifesciences.com](http://mahamaya1ifesciences.com/)



Community Score

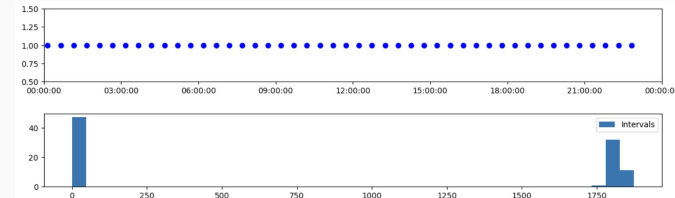
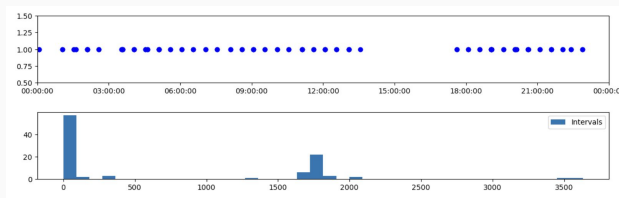
# Home lab: DNS (NOERROR) beaconing on 2023-07-15

192.168.XX.XX -> 0.android.pool.ntp.org



Query	Period
0.android.pool.ntp.org	3600
europa.pool.ntp.org	
time.apple.com	
time.windows.com	
tccprod01.honeywell.com	300
tccprod02.honeywell.com	
tccprod03.honeywell.com	
_mywifiext._tcp.local	60
a.root-servers.net	30

## Findings with jittering

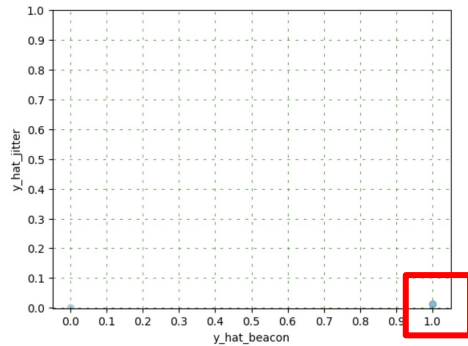


Beaconing with  
jitter

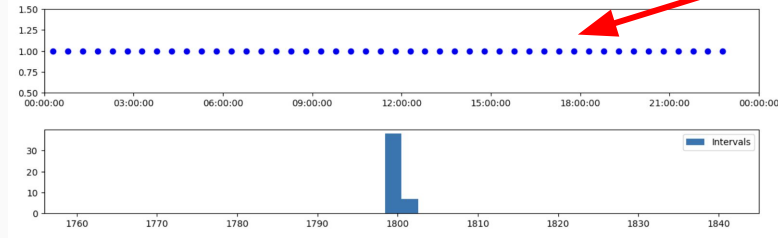
Beaconing  
without jitter

# Home lab: DNS (NXDOMAIN) beaoning on 2023-07-15

- 12 NXDOMAIN queries
- 2 findings without jitter



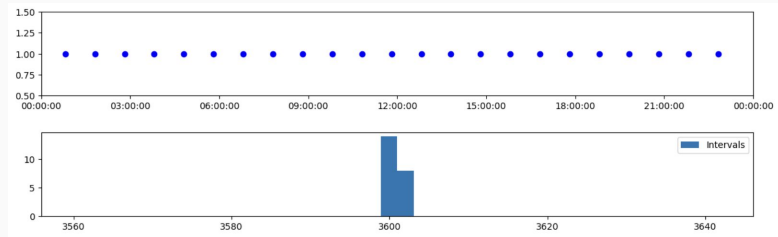
192.168.XX.XX -> dummybeaconflag.ml



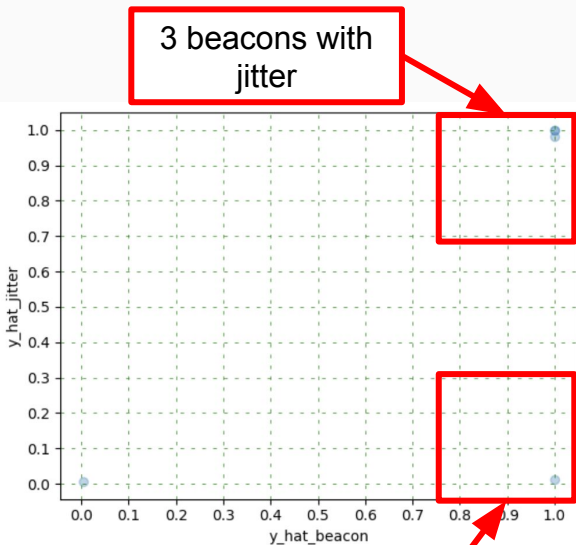
```
#!/bin/bash
```

```
while true  
do  
    nslookup dummybeaconflag.ml  
    sleep 1800  
done
```

192.168.XX.XX-> eu.pool.ntp.org



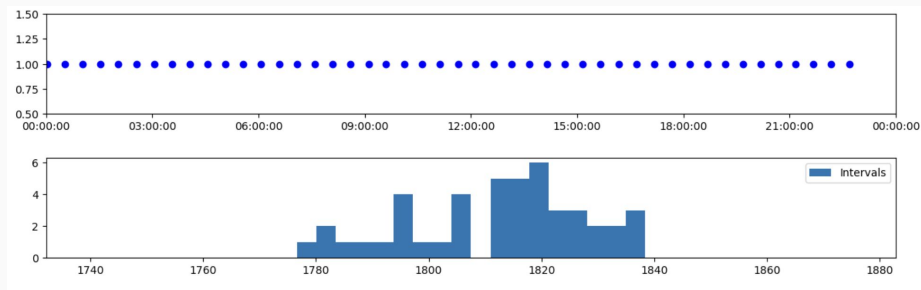
# Home lab: SSL beaconing 2023-07-18



1 beacon without jitter

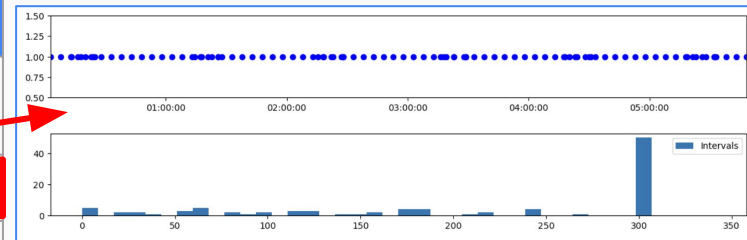
## Beaconing without jitter

192.168.XX.XX -> safebrowsing.googleapis.com



## Beaconing with jitter

server_name	Mean interval	Std
certstream.calidog.io	81.96	22.99
softsensor-telemetry.release.v2.corelight.io	206.09	107.93
cloud.us.humio.com	107.74	86.54



# Evaluation at scale with conn, dns, http, and ssl logs

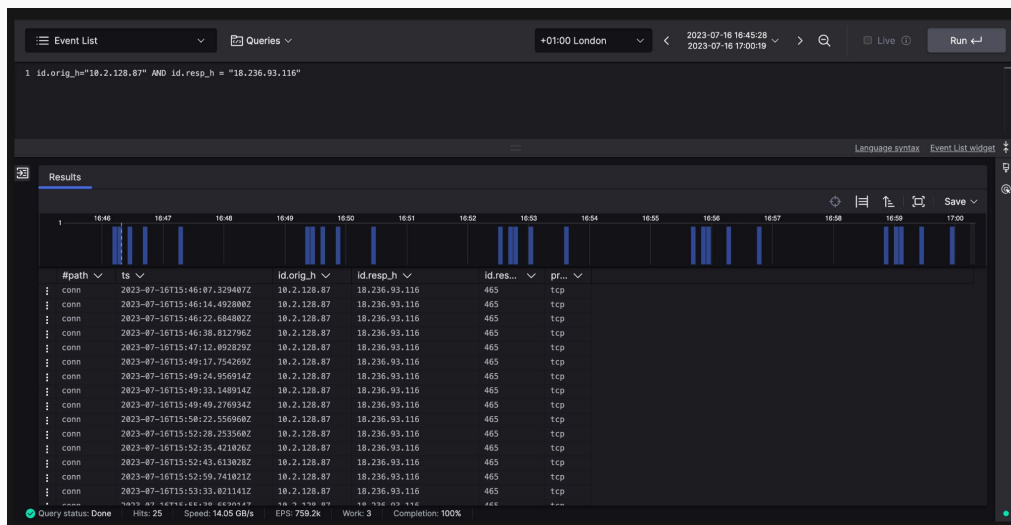
- Source/dest pairs:
  - conn: (source IP, destination IP)
  - dns, http, ssl: (source IP, registrable domain)
- High volume and elevated number of source/dest pairs are a challenge, explored ways to filter down logs:
  - Established connections
  - HTTP requests with request size < 2000 bytes
  - Domains with gTLDs (.xyz, .site, .download etc.)
- High-scored activities seem to be beacons
- Most findings seemed to be legit beacons, and only a handful of suspicious ones
- WIP: combine beaconing with additional features:
  - URI and req/resp sizes for http
  - Domain popularity for dns, http and ssl
  - Query type for dns (TXT, A, AAAA, etc.)
  - ?



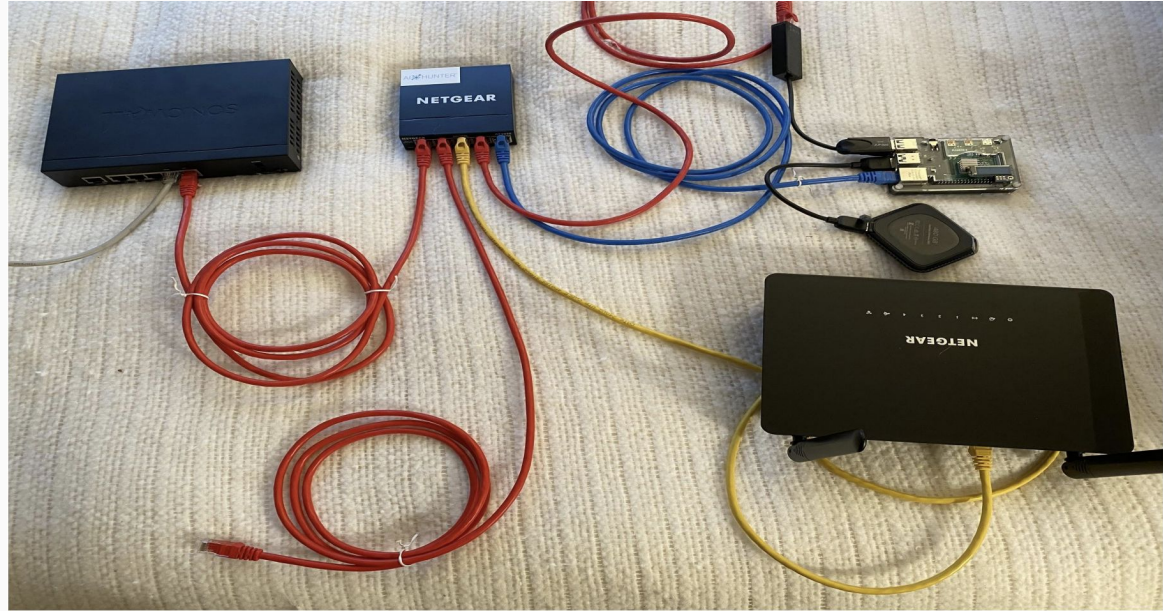
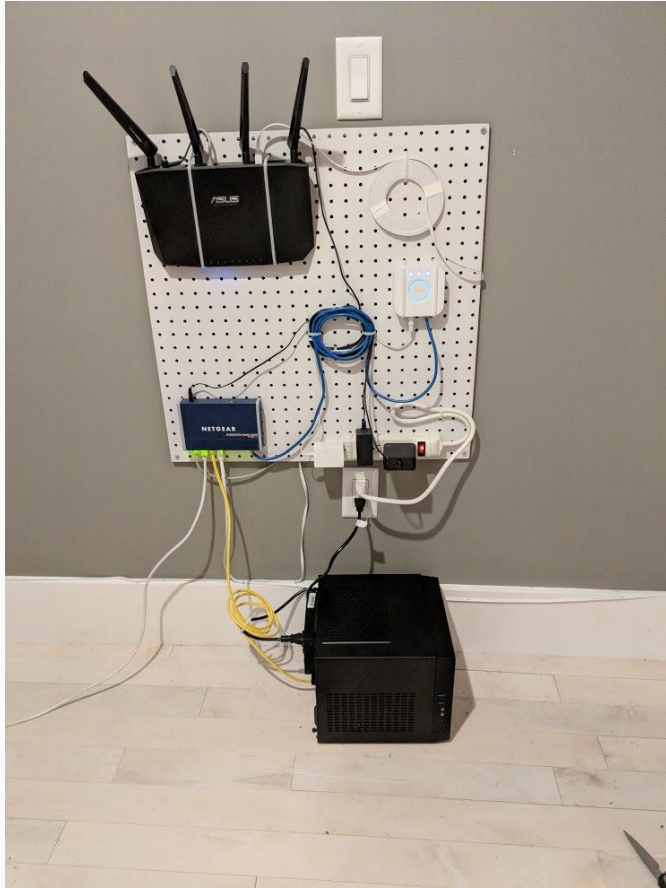
# Key takeaways and Q&A

- Beacons are prevalent in C2 frameworks and in *many* services & applications
- Beacons are messy, looking for “perfect” beacons will miss many interesting activities
- CNNs promising to deal with:
  - Diversity in beaconing patterns
  - Missing beacons
  - Activities with beacons + interactions
- The approach can be adapted to surface other temporal patterns

## Active Sliver session



# Home Labs



[https://www.blackhillsinfosec.com/wp-content/uploads/2020/09/SLIDES\\_HowToBuildHomeLab.pdf](https://www.blackhillsinfosec.com/wp-content/uploads/2020/09/SLIDES_HowToBuildHomeLab.pdf)