An Analysis of Recurrent Neural Networks forBotnet Detection Behavior

Kyle McClintick
Dept. of Electrical & Computer Engineering, Worcester Polytechnic Institute,
Worcester, MA 01609 USA

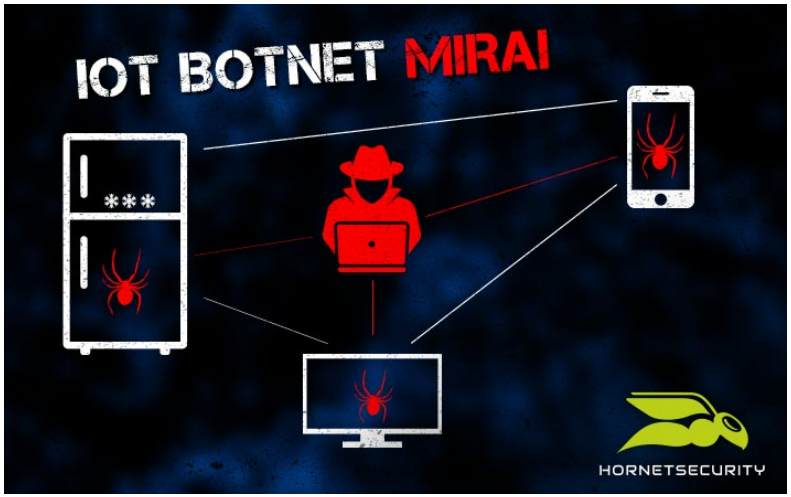
Wireless Innovation Laboratory

WPI

April 29th, 2020

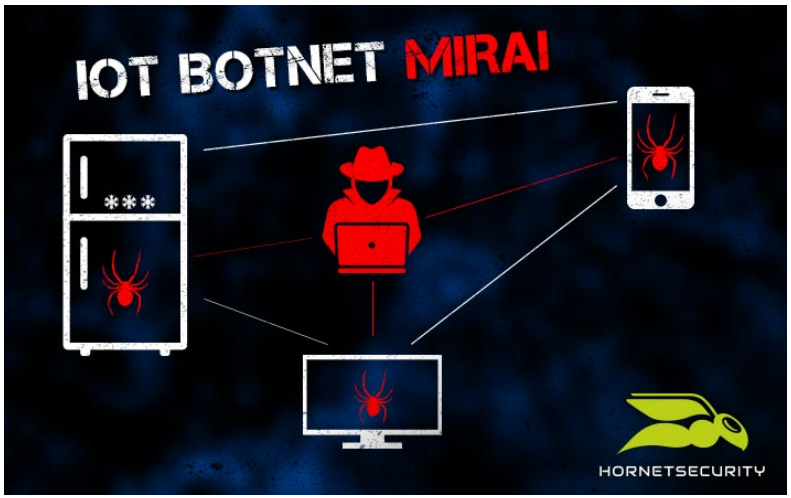
Brief History

- 2014: DDoS attacks on competing Minecraft servers under the pseudonym lelddos
- 2016: French hosting company OVH suffered a DDoS attack with a total capacity of up to 1.5 terabits per second
- Co-developer published the source code under the name Anna-Senpai. Many hackers copied and developed the code.
- Largest DDoS attack ever launched, targeting the DNS provider Dyn. Amazon, Netflix and Spotify, were unavailable for a long time



Brief History

- FBI involved, three Alaskans pleaded guilty and avoided jail time by manditory employment with the FBI to counter botnet of things attacks
- 2019: bot net of things attacks have returned with 11 new exploits (27 total now) spreads primarily through presentation systems, smart TVs, routers and IP cameras

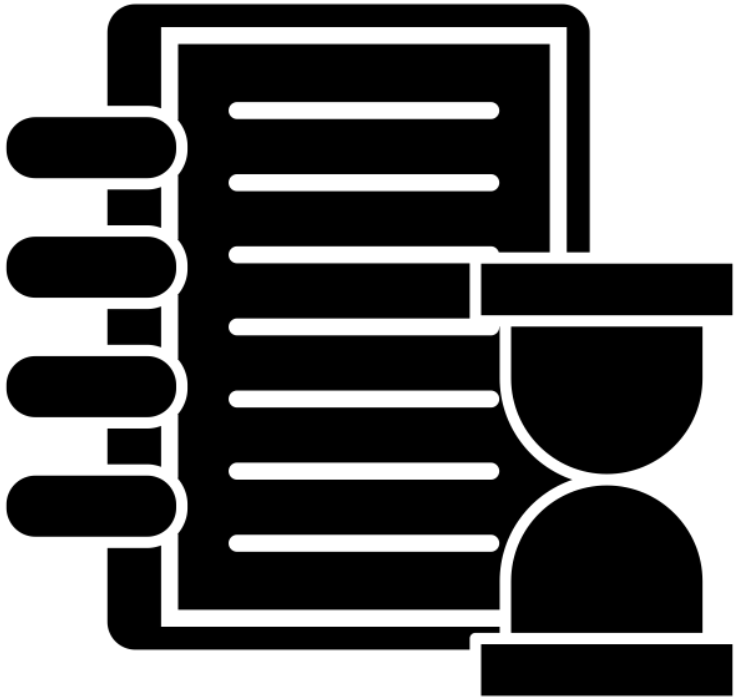


Personal Interest

DARPAs Open Programmable Secure 5G (OPS-5G) program will create open source software and systems enabling secure 5G and follow-on mobile networks. OPS-5G creates capabilities to address feature velocity in open source software, a trillion-node Botnet of Things (BoT), network slicing on suspect gear and adaptive adversaries operating at scale. The long-term objective is a US-friendly ecosystem.

Agenda

- Abstract
- Key Contributions
- State of the Art
- Novel Method
- Results
- Conclusion



Abstract

Figure: A Botnet can be conceived as a group of compromised computers which can be controlled remotely to execute coordinated attacks or commit fraudulent acts. The fact that Botnets continuously evolve means that traditional detection approaches are always one step behind.

Abstract

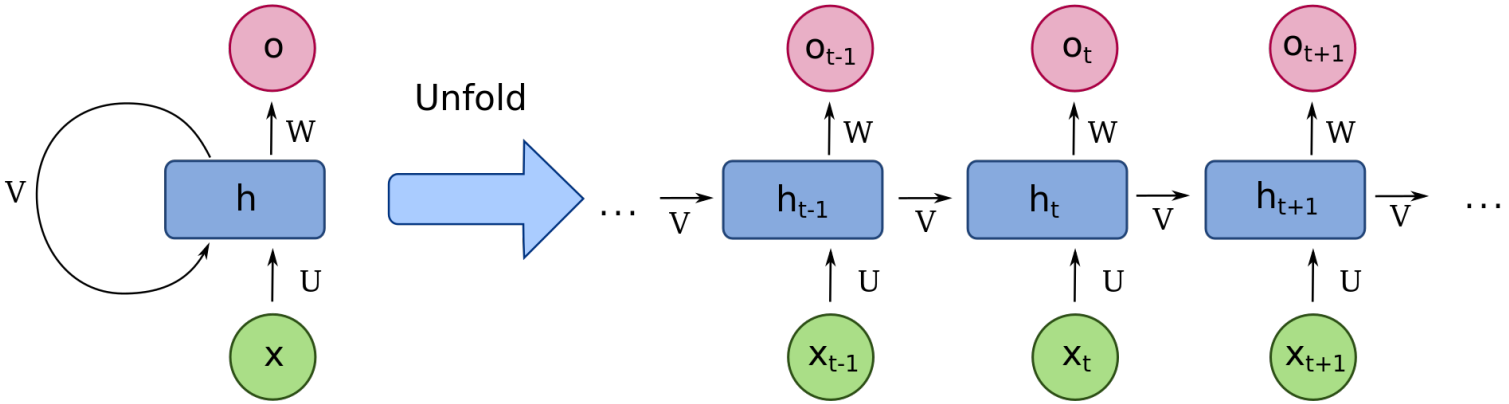
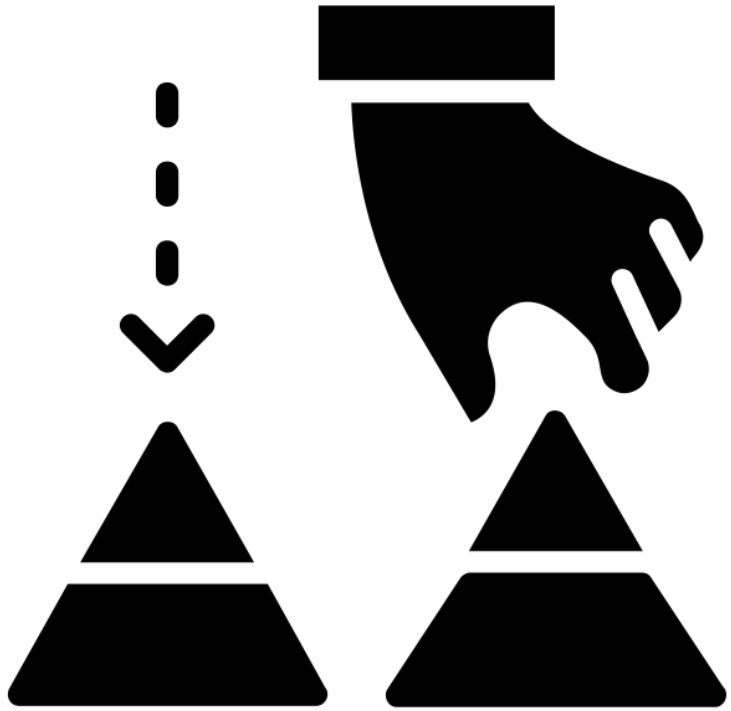


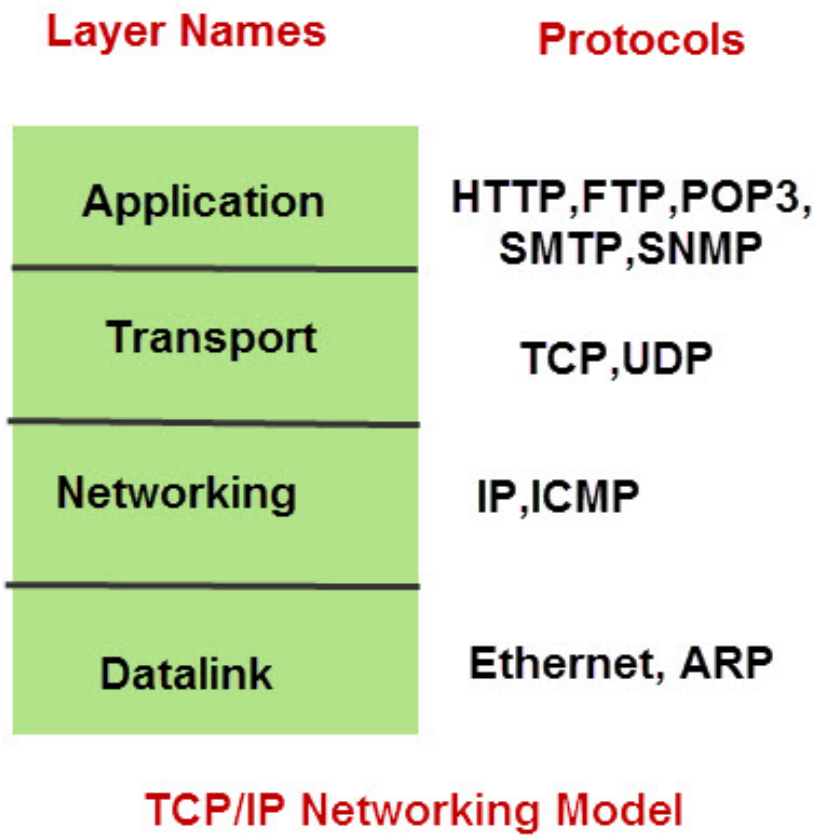
Figure: Temporal analysis of network behavior, specifically duration and load of network traffic from different nodes, can be used to infer if a node is part of a botnet attack. Using Recurrent Neural Networks, preliminary are good. However, experiments exposed that experimental data is too similar to classify accurately.

Key Contributions

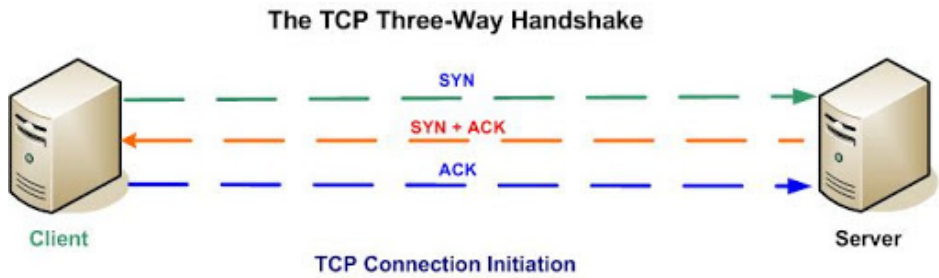
- A better model: state of the Art is the Strastosphere Intrusion Prevention System (IPS) project, a first order Markov Model, which struggles to sample large state spaces, and only makes predictions using the pervious state
- All bots must receive instructions from the bot master at some point, can this sparse, long-sequence behavior be recognized?



State of The Art



TCP/IP Networking Model



State of The Art

TCP segment header

Offsets	Octet	0								1								2								3							
Octet	Bit	7	6	5	4	3	2	1	0	7	6	5	4	3	2	1	0	7	6	5	4	3	2	1	0	7	6	5	4	3	2	1	0
0	0	Source port																Destination port															
4	32	Sequence number																															
8	64	Acknowledgment number (if ACK set)																															
12	96	Data offset				Reserved **0 0 0**				NS	CWR	ECE	URG	ACK	PSH	RST	SYN	FIN	Window Size														
16	128	Checksum																	Urgent pointer (if URG set)														
20 ...	160 ...	Options (if *data offset* > 5. Padded at the end with "0" bytes if necessary.) ...																															

State of The Art

TABLE I
SYMBOL ASSIGNMENT STRATEGY FOR BUILDING BEHAVIORAL MODEL ACCORDING TO THE STRATOSPHERE PROJECT.

	Size Small			Size Medium			Size Large		
	Dur. Short	Dur. Med	Dur. Long	Dur. Short	Dur. Med	Dur. Long	Dur. Short	Dur. Med	Dur. Long
Strong Per	a	b	c	d	e	f	g	h	i
Weak Per.	A	B	C	D	E	F	G	H	I
Weak Non-Per.	r	s	t	u	v	w	x	y	z
Strong Non-Per	R	S	T	U	V	W	X	Y	Z
No Data	1	2	3	4	5	6	7	8	9

Symbols for time difference	
Between 0 and 5 seconds:	.
Between 5 and 60 seconds:	,
Between 60 and 5 mins:	+
Between 5 mins and 1 hour	*
Timeout of 1 hour:	0

2.4.R*R.R.R*a*b*a*a*b*b*a*R.R*R.R*a*a*b*a*a*a*a*

Fig. 1. An example of the behavioral model of connection from IP address 10.0.2.103 to destination port 53 at IP address 8.8.8.8 port 53 using protocol UDP.

Novel Method: Data Representation

- Data: 50 different possible states, each state is grouped into a length n sequence $X_{n,t} \in \{0,1\}^{50}$. A connection can have any number of sequences.
- Labels: Binary classification, normal or botnet. $Y_t \in \{0,1\}$
- Collection: TCP/IP connections between computers at Czech technical university in Prague.

TABLE II
GENERAL INFORMATION ABOUT DATASETS

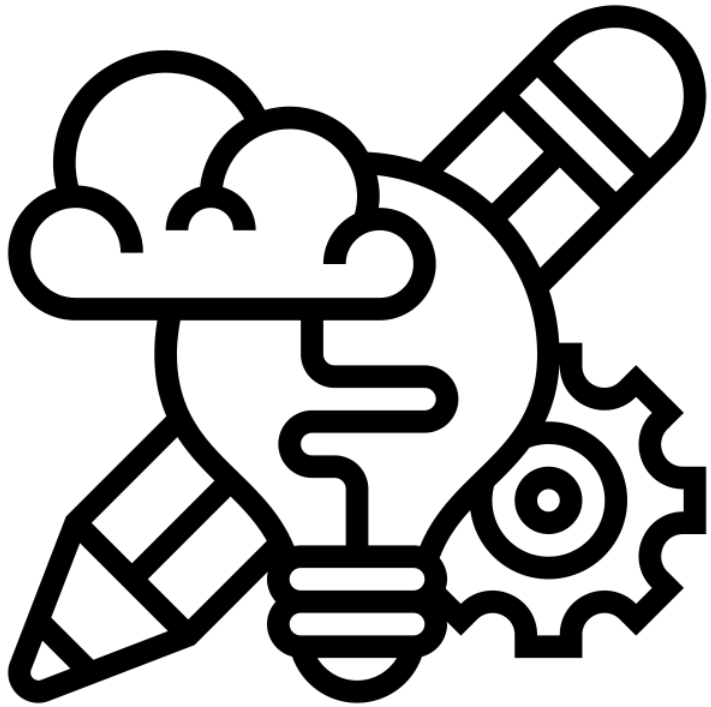
ID	Desc.	Botnet Conn.	Normal Conn.	MCFP IDs
A	Bonet Neris	2101	713	CTU13-42
B	Bonet DonBot	188	300	CTU13-47

Novel Method: Challenges

- Architecture: while LSTM has the capability to classify outcomes using states from millions of time steps ago, there is no generative approach to implement this
- Class imbalance: many more normal states than botnet for DonBot, many more botnet states than normal for Neris
- State space design: choosing how many states go in a connection may have significant effects on pattern recognition

Novel Method: Architecture

- RMSprop weight updates, 30 epochs
- 128 neurons, 1 layer. Dropout of $p = 0.1$



Novel Method: Class Imbalance

TABLE III
AVERAGE AND STANDARD DEVIATION VALUES FOR ADR AND FAR AFTER 50 EXECUTIONS FOR DIFFERENT SAMPLING STRATEGIES

	ADR		FAR	
	Avg.	*Sd.*	*Avg.*	*Sd.*
No Sampling	0.9796	0.0106	0.0372	0.0227
Under Sampling	0.9680	0.0197	0.0195	0.0179
Over Sampling	0.9601	0.0132	0.0111	0.0068

Figure: Attack Detection Ratio and False Alarm Rate on test data when random samples are removed from the dataset (under sampling) and when random samples are duplicated in the dataset (over sampling) to balance the number of samples in each class. Undersampling is used due to increasing training speed.

Novel Method: State Space Design

2.4.R*R.R.R*a*b*a*a*b*b*a*R.R*R.R*a*a*b*a*a*a*a*

Fig. 1. An example of the behavioral model of connection from IP address 10.0.2.103 to destination port 53 at IP address 8.8.8.8 port 53 using protocol UDP.

TABLE IV
AVERAGE AND STANDARD DEVIATION VALUES FOR ADR AND FAR AFTER 100 EXECUTION CONSIDERING DIFFERENT NUMBER OF STATE CONNECTIONS

Number of States		4	5	6	10	25	50	100
ADR	***Avg***	0.953	0.955	0.962	**0.968**	**0.970**	0.968	0.969
	sd	0.024	0.025	0.022	0.022	0.019	0.021	0.021
FAR	***Avg***	0.023	0.021	0.020	**0.019**	**0.018**	0.016	0.020
	sd	0.017	0.018	0.018	0.017	0.016	0.014	0.039

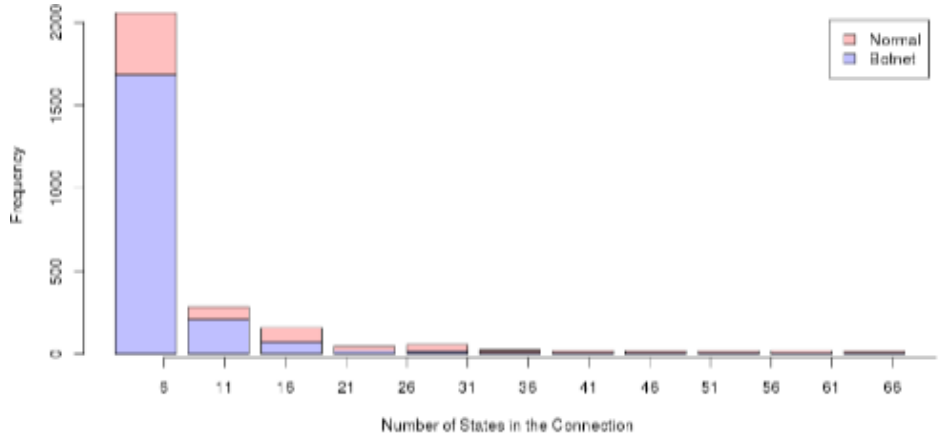


Fig. 2. Frequency histogram of the number of states per connection

Results

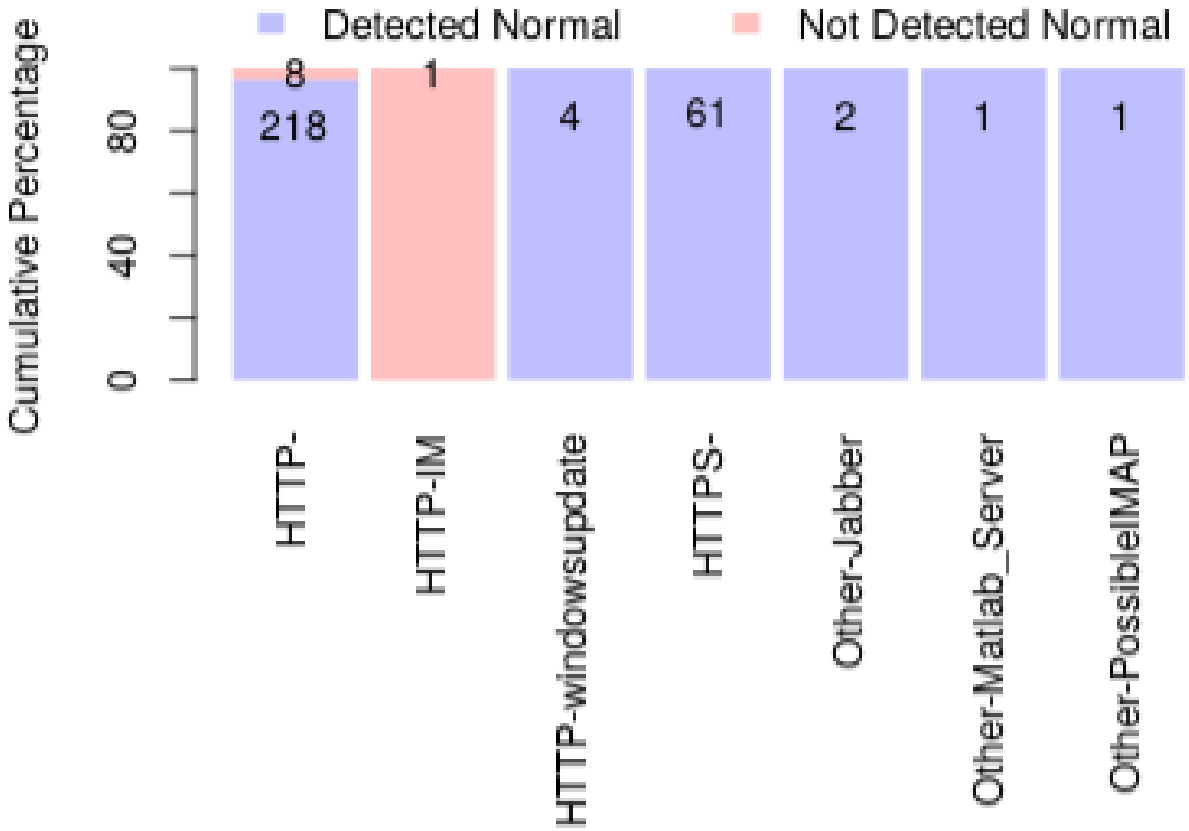


Fig. 4. Discriminative analysis of connections labeled as Normal.

Results

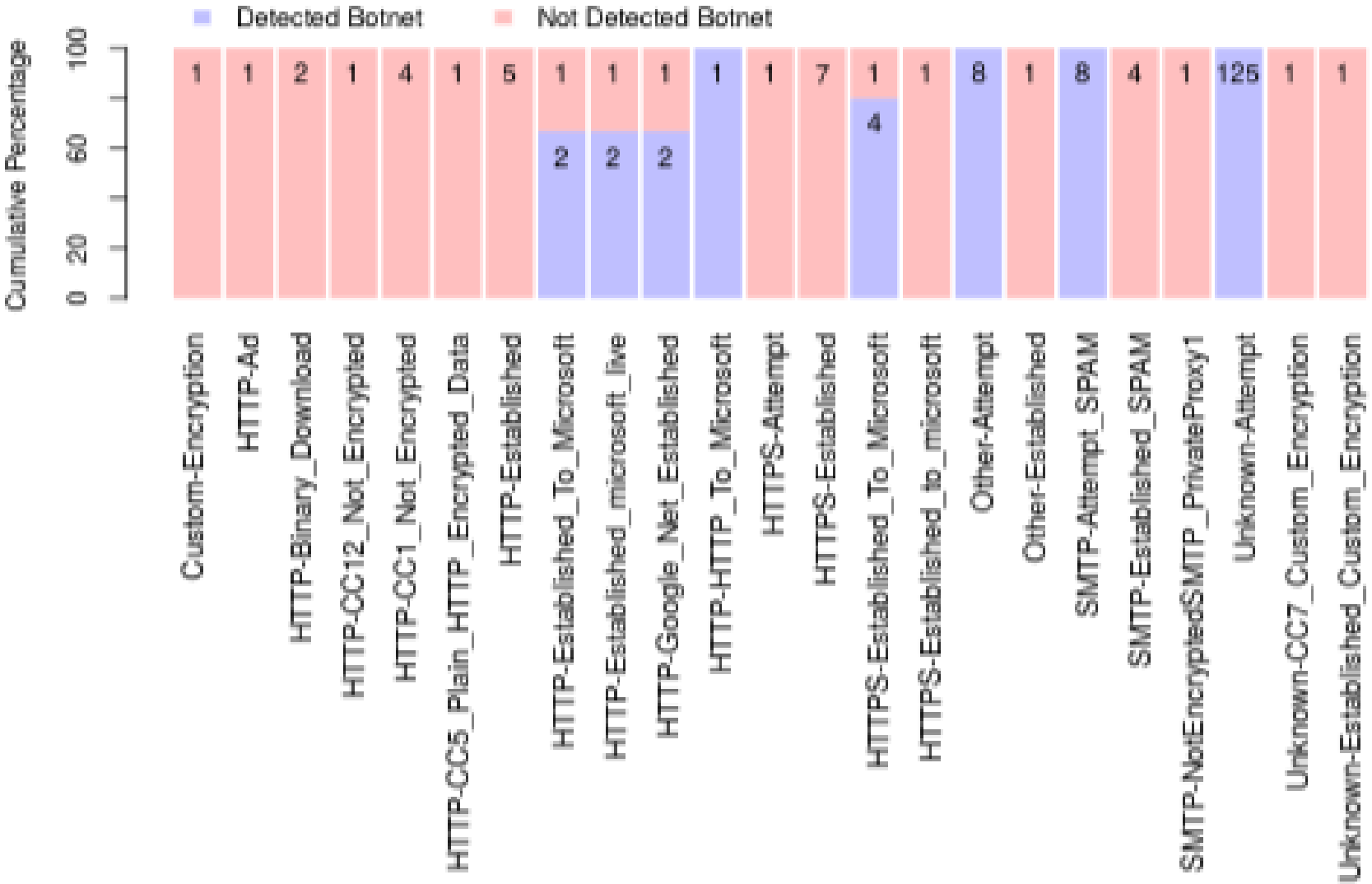


Fig. 3. Discriminative analysis of connections labeled as Botnet

Conclusion

- Most all port 80 HTTP- service connections where normal
- Most all ports with no listed service connections were botnet
- Data size, periodicity, and duration of TCP connections were not correlated to labels
- How good was the data set? Can other botnet datasets be classified just off of TCP source port? Seems too simple...