SFU SIMON FRASER UNIVERSITY
ENGAGING THE WORLD

CMPT 479/980: Systems and Network Security
Spring 2020

Automatic Detection of DDoS Attacks Using Machine Learning Techniques

Omar Mossad
Parham Yassini

Motivation

- In DDoS, remotely controlled distributed devices are used to attack the victim

- A constantly increasing threat to the availability of any internet-based service

- Example of recent attacks targeting *Github* (February 2018), *Dyn DNS provider* (October 2016), and etc.

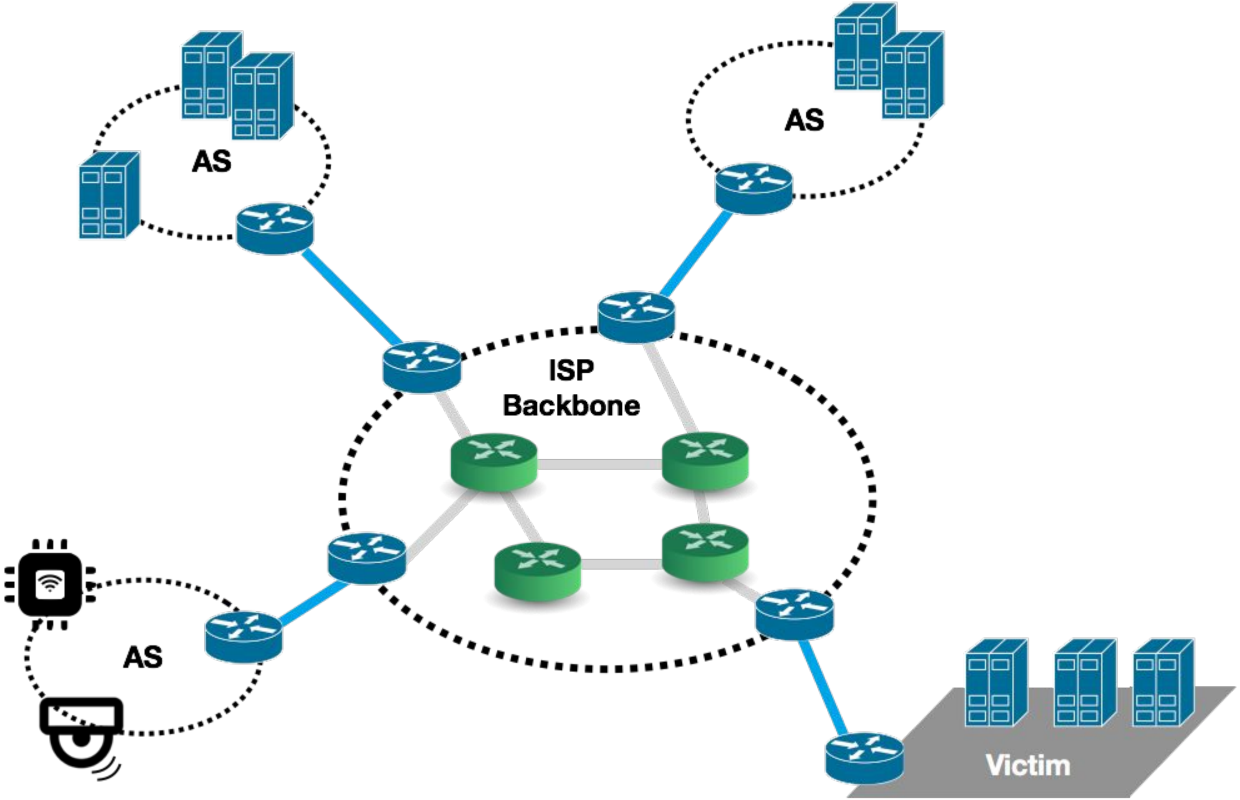
Motivation

Traditional signatures-based methods are unable to adopt to variation of normal flows or emergence of new attack patterns

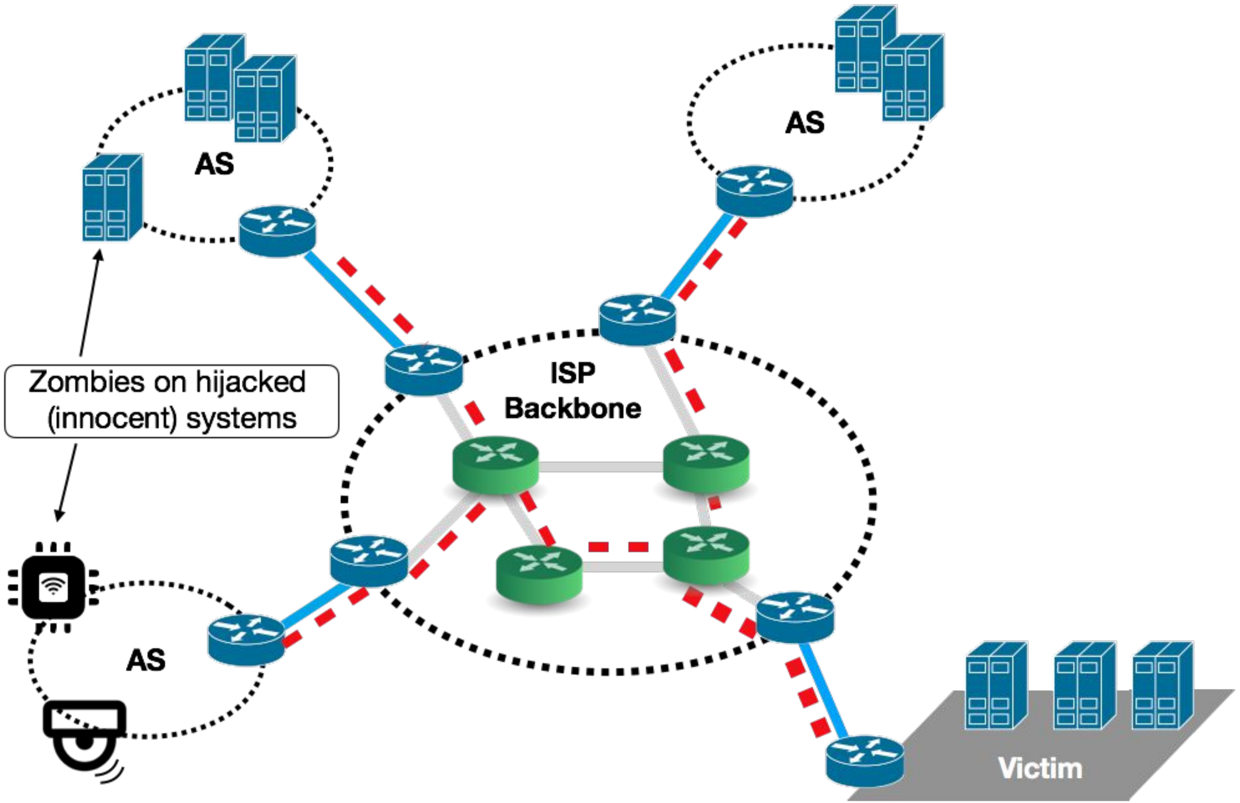
Learning-based methods are capable of automatically finding correlation in the data

$\longrightarrow$ Portable for different scenarios

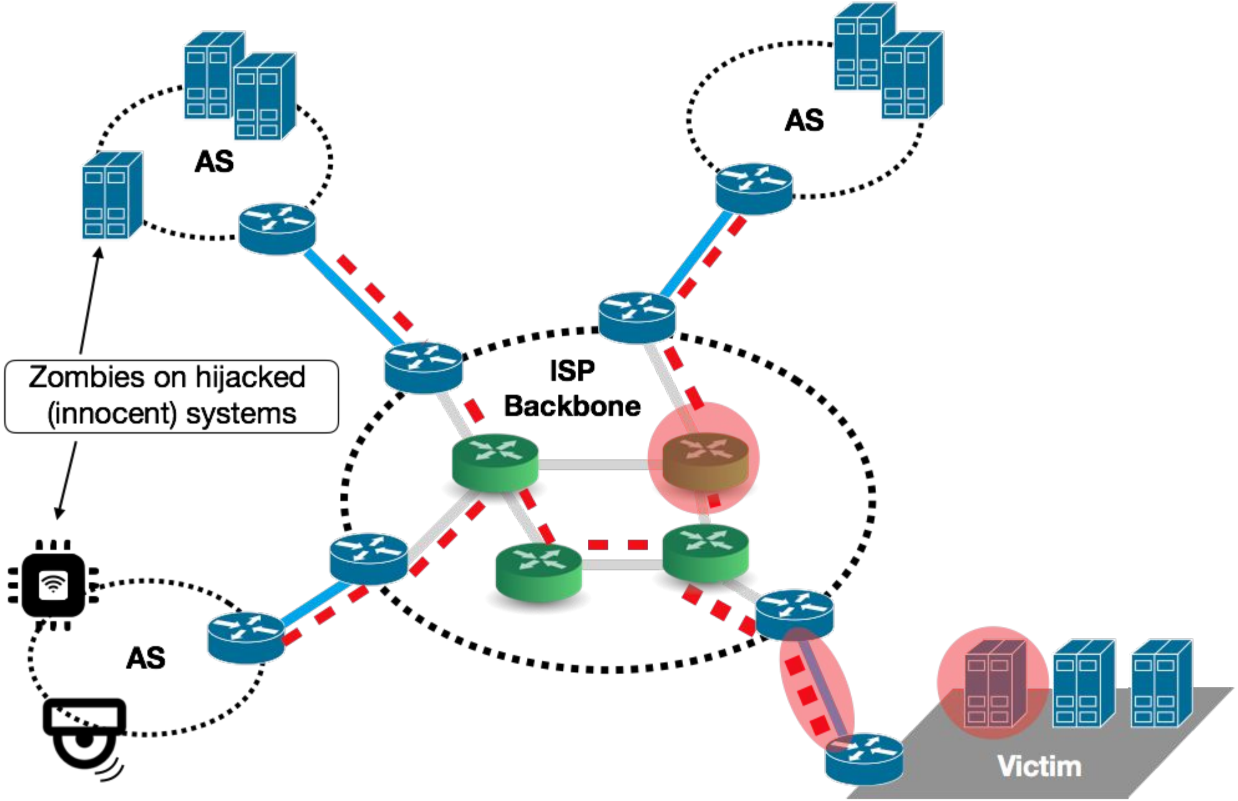
DDoS Attack Model



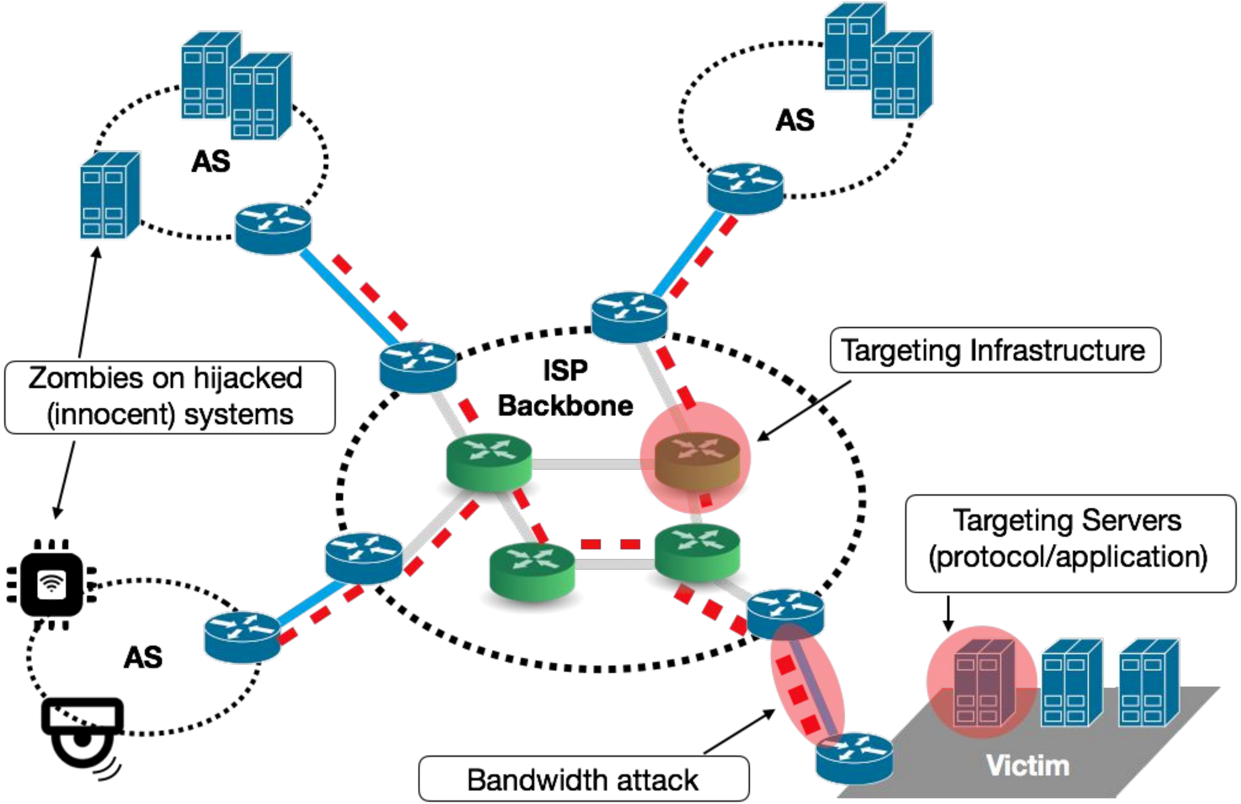
DDoS Attack Model



DDoS Attack Model



DDoS Attack Model



Problem

- Given statistical features for the traffic flow on the victim network, determine whether this flow is ***Malicious*** or ***Benign***.

- Features include *flow duration*, *number of packets*, *protocol*, *packet length*, and etc.

- We extend the main idea and try to ***classify*** the type of attacks (LDAP, SYN Flood, NTP, etc ..)

Challenges

- How to differentiate between different classes of attacks:
    - Survey on research papers with similar objectives and datasets
    - *Feature exploration* using statistics for each class: mean, std, etc..

- How to reduce the number of input variables (~80 features) in order to reduce processing overheads without affecting the classification performance
    - Selecting most distinctive features only.

Challenges

- Huge data size (~14 files each with ~10M entry)

  - We used *cedar.computecanada* to handle memory and computational requirements.

- Inconsistent values (Port no [22-10546], Packet Rate [0-*Inf*], Flow duration [0 - 0.05] , etc..)

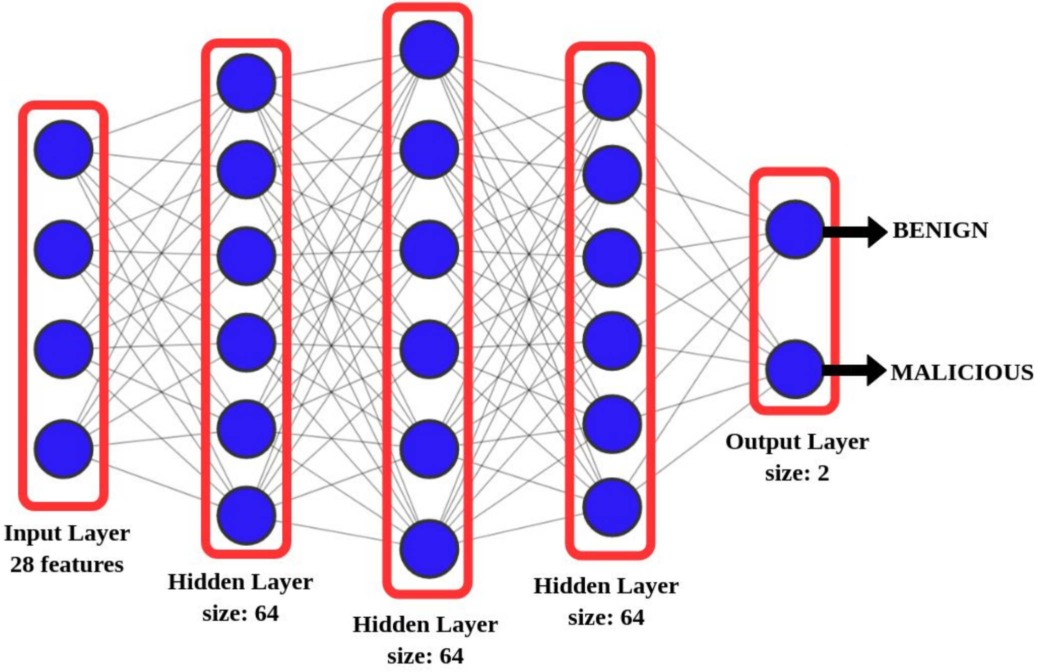
  - Replaced *Inf* with a large integer value ~ 99999
  - Used *Quantile transformer* to normalize the data

Solution

- The reference paper relied on *conventional classification* methods (Decision Tree, Random Forest, Naive Bayes, etc ..) and the results were promising.
- However, they considered distinct features for each type of attack which is not reliable in real life scenarios.
- Therefore, we developed a *deep neural network (DNN)* with 3 hidden layers.
- The main idea is to rely on the network to identify the best weights for each feature.
- We restricted ourselves to the features used in the reference.

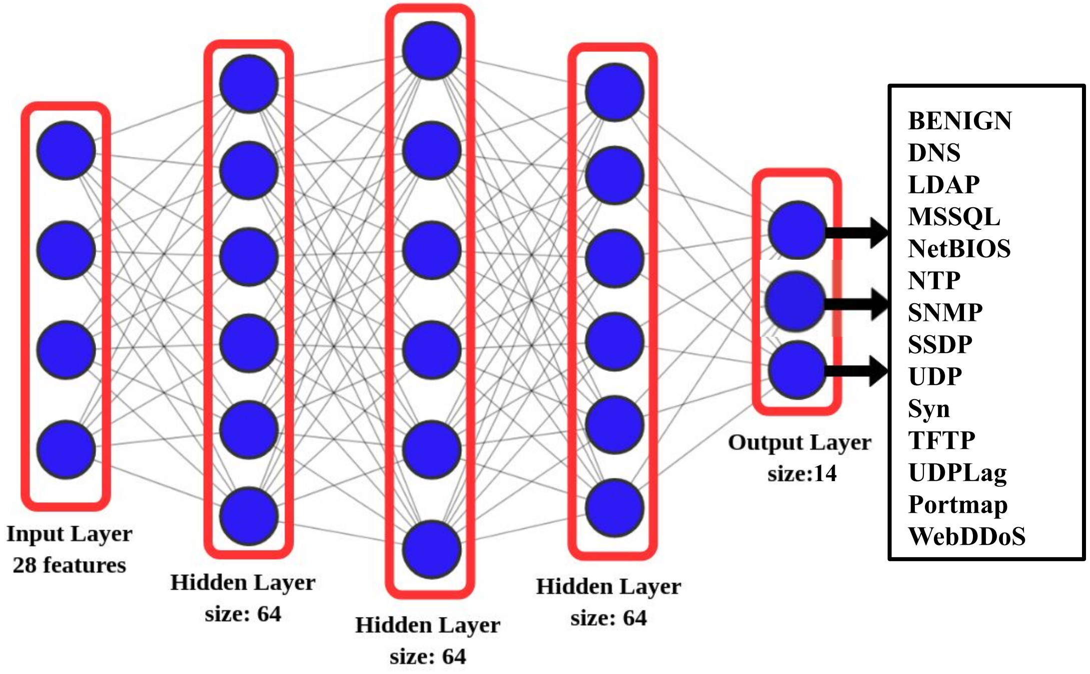
Solution

Network Architecture For Binary Classification



Solution

Network Architecture For Categorical Classification



Results

- We evaluate our model’s precision, recall and F1-Score compared to the reference paper.
- We have replicated the original work with different features but had to restrict it to 1M sample per file.

Algorithm	**Precision**	**Recall**	**F1-Score**
ID3 (Decision Tree)	0.71 / 0.78*	0.17 / **0.65***	0.27 / **0.69***
RF (Random Forest)	0.85 / 0.77*	0.12 / 0.56*	0.20 / 0.62*
Naive Bayes	0.97 / 0.41*	0.06 / 0.11*	0.12 / 0.05*
Logistic Regression	0.49 / 0.25*	0.94 / 0.02*	0.64 / 0.04*
DNN (Ours)	**0.84**	0.33	0.47

* As mentioned in reference paper

Results

- A detailed analysis for the binary classifier

Predicted Class	Actual Class		
		BENIGN	MALICIOUS
	BENIGN	20,209,901 (TN)	8970 (FP)
	MALICIOUS	97,659 (FN)	47,995 (TP)

Results

CMPT 479/980: Systems and Network Security

Spring 2020

- We also evaluate the categorical classification accuracy = 62.26%

Accuracy: 62.26%

Output Class \ Target Class	BENIGN	DNS	LDAP	MSSQL	NetBIOS	NTP	SNMP	SSDP	UDP	Syn	TFTP	UDPLag	Portmap	WebDDoS
BENIGN	NaN% 0	0.0% 65	0.0% 39	0.4% 32982	0.0% 83	0.0% 7	NaN% 0	NaN% 0	NaN% 0	0.0% 13	0.0% 765	0.0% 8	0.0% 0	NaN% 0
DNS	NaN% 0	59.4% 749875	0.0% 0	6.1% 496830	0.0% 0	98.7% 271032	NaN% 0	NaN% 0	NaN% 0	0.0% 0	0.0% 478	0.0% 0	0.0% 0	NaN% 0
LDAP	NaN% 0	36.7% 464005	95.9% 639722	1.4% 110428	0.0% 0	0.0% 0	NaN% 0	NaN% 0	NaN% 0	0.0% 0	0.2% 12353	0.0% 0	0.0% 0	NaN% 0
MSSQL	NaN% 0	0.0% 0	0.0% 0	38.0% 3078677	0.0% 0	0.0% 0	NaN% 0	NaN% 0	NaN% 0	0.0% 0	0.2% 13968	0.0% 0	0.0% 0	NaN% 0
NetBIOS	NaN% 0	0.4% 5676	4.1% 27296	0.1% 11807	56.0% 153733	1.3% 3440	NaN% 0	NaN% 0	NaN% 0	0.0% 0	0.0% 167	19.9% 158677	0.0% 0	NaN% 0
NTP	NaN% 0	3.4% 43264	0.0% 3	28.2% 2279665	0.0% 0	0.0% 0	NaN% 0	NaN% 0	NaN% 0	0.0% 0	0.0% 3573	0.0% 0	0.0% 0	NaN% 0
SNMP	NaN% 0	0.0% 0	0.0% 0	0.7% 55991	0.0% 0	0.0% 0	NaN% 0	NaN% 0	NaN% 0	0.0% 0	0.0% 48	0.0% 0	0.0% 0	NaN% 0
SSDP	NaN% 0	0.0% 0	0.0% 0	19.1% 1547768	0.0% 0	0.0% 0	NaN% 0	NaN% 0	NaN% 0	0.0% 0	0.0% 923	0.0% 0	0.0% 0	NaN% 0
UDP	NaN% 0	0.0% 0	0.0% 0	1.1% 85746	0.0% 0	0.0% 0	NaN% 0	NaN% 0	NaN% 0	0.0% 0	8.9% 698219	0.0% 0	0.0% 0	NaN% 0
Syn	NaN% 0	0.0% 0	0.0% 0	0.8% 67459	0.0% 0	0.0% 0	NaN% 0	NaN% 0	NaN% 0	98.7% 1874407	0.0% 175	0.0% 0	66.7% 2	NaN% 0
TFTP	NaN% 0	0.0% 0	0.0% 0	0.1% 7006	0.0% 0	0.0% 0	NaN% 0	NaN% 0	NaN% 0	0.0% 0	76.6% 6015678	0.0% 0	0.0% 0	NaN% 0
UDPLag	NaN% 0	0.0% 128	0.0% 71	3.8% 306684	43.9% 120543	0.0% 3	NaN% 0	NaN% 0	NaN% 0	0.0% 8	13.2% 1034034	80.1% 640465	0.0% 0	NaN% 0
Portmap	NaN% 0	0.0% 0	0.0% 0	0.2% 13351	0.0% 0	0.0% 0	NaN% 0	NaN% 0	NaN% 0	1.3% 24128	0.9% 72688	0.0% 2	33.3% 1	NaN% 0
WebDDoS	NaN% 0	0.0% 0	0.0% 0	0.0% 133	0.0% 0	0.0% 0	NaN% 0	NaN% 0	NaN% 0	0.0% 0	0.0% 0	0.0% 0	0.0% 0	NaN% 0

Learned Lessons

- In conclusion, we are able to build a powerful network analyzer that can filter DDoS attacks from benign traffic.

- The model is not entirely passive: Once a malicious behaviour is detected, we can block the incoming traffic from the suspicious address.

- **For the final milestone:** Need more insights about the expected traffic features for each type of DDoS attack.

References

Abhishta Abhishta, Roland van Rijswijk-Deij, and Lambert J. M. Nieuwenhuis. 2019. Measuring the impact of a successful DDoS attack on the customer behaviour of managed DNS service providers. SIGCOMM Comput. Commun. Rev. 48, 5 (January 2019), 70–76. DOI:https://doi.org/10.1145/3310165.3310175

Felter, Blair. 5 Of the Most Famous Recent DDoS Attacks. May 2019, www.vxchnge.com/blog/recent-ddos-attacks-on-companies

Sharafaldin, Iman, et al. "Developing Realistic Distributed Denial of Service (DDoS) Attack Dataset and Taxonomy." 2019 International Carnahan Conference on Security Technology (ICCST). IEEE, 2019.