

ADVERSARIAL PHISHING ATTACKS & DEFENCES



Prepared by : Archana Sreekumar
Mentored by : Dr Krishnasree Achutan
Collaborator : Gilad Gressel

PAPERS

1) “Cracking Classifiers for Evasion: A Case Study on the Google’s Phishing Pages Filter “

- Authors: Bin Liang, Miaoqiang Su, Wei You, Wenchang Shi, Gang Yang
- ACM 978-1-4503-4143-1/16/04, 2016

2) “Wild Patterns: Ten Years After the Rise of Adversarial Machine Learning”

- Authors: Battista Biggio, Fabio Roli
- Pattern Recognition(Journal), 2017

3) “Adversarial Examples for Malware Detection”

- Authors: Kathrin Grosse, Nicolas Papernot, Praveen Manoharan, Michael Backes
- Computer Security – ESORICS 2017

PAPERS

4) “Defense Against the Dark Arts: An overview of adversarial example security research and future research directions”

- Authors: Ian Goodfellow
- IEEE workshop on Security and Privacy, 2018

5) “Adversarial Sampling Attacks Against Phishing Detection”

- Authors: Hossein Shirazi, Bruhadeshwar Bezawada, Indrakshi Ray, Charles Anderson
- IFIP Annual Conference on Data and Applications Security and Privacy, 2019

Thank You