Phishing Detection on Tor Hidden Services

By:
Martin Steinebach

From the proceedings of

The Digital Forensic Research Conference

DFRWS EU 2021

March 29 - April 1, 2021

PHISHING DETECTION ON TOR HIDDEN SERVICES

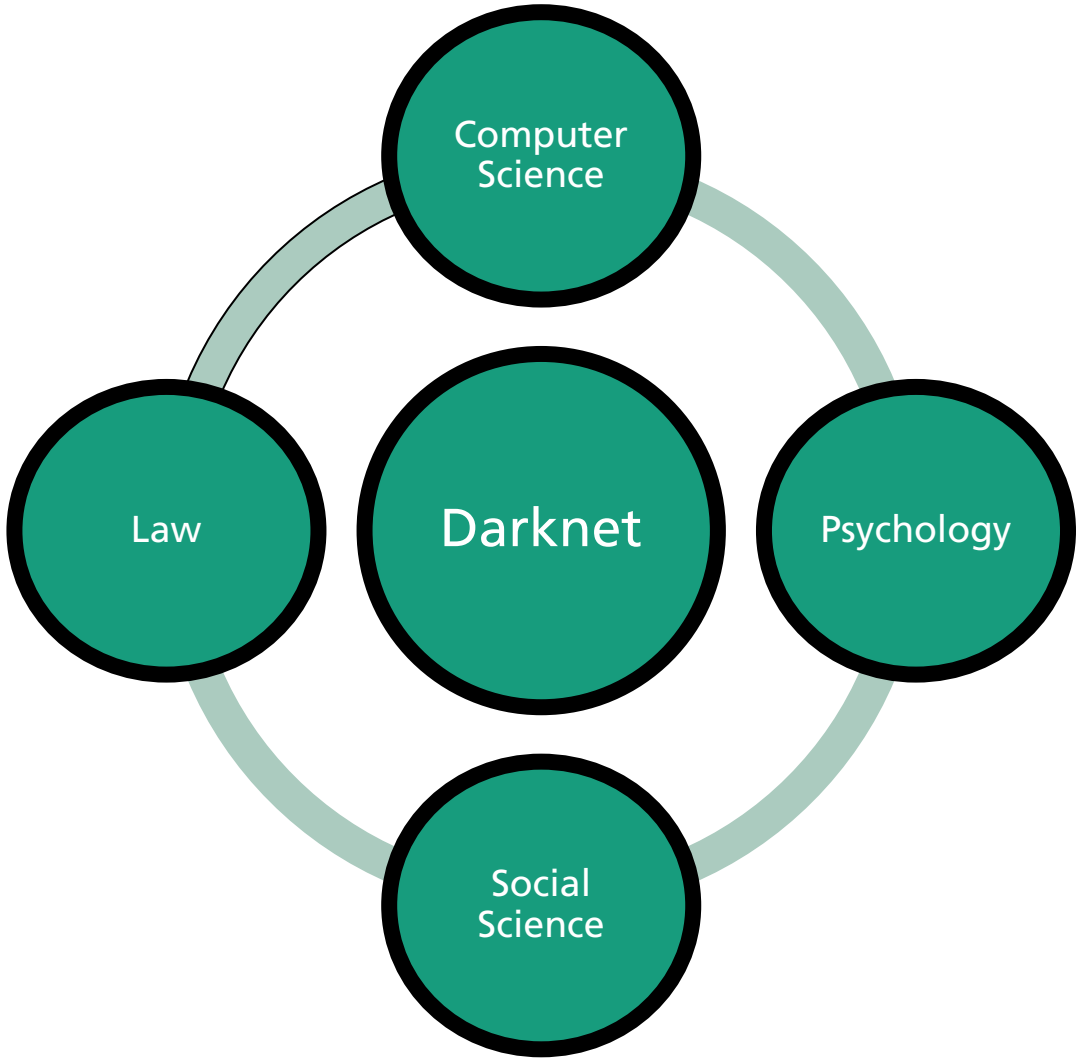
Martin Steinebach, Sascha Zenglein, Katharina Brandl

Gefördert durch
Bundesministerium
für Bildung
und Forschung

SIFO.de

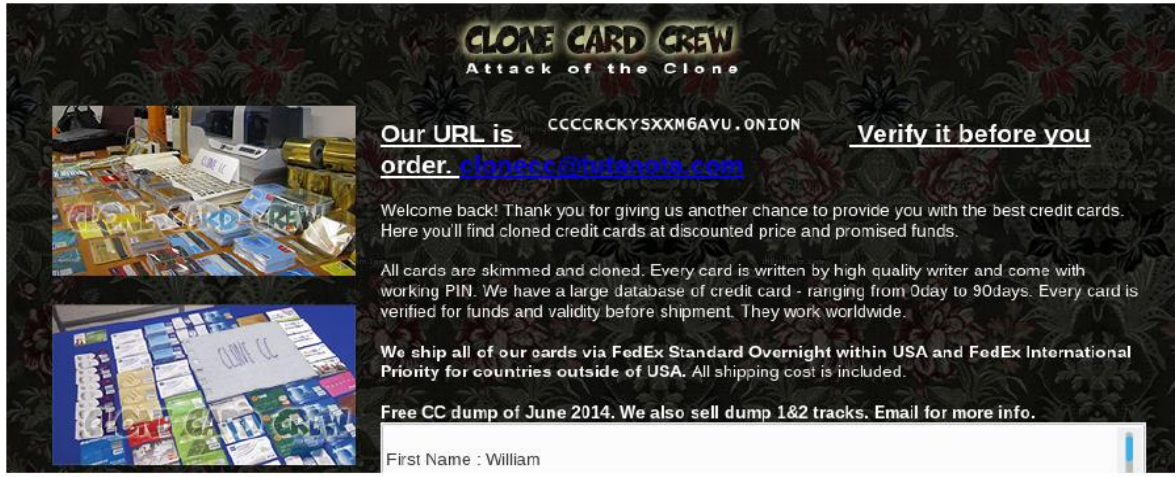
BACKGROUND

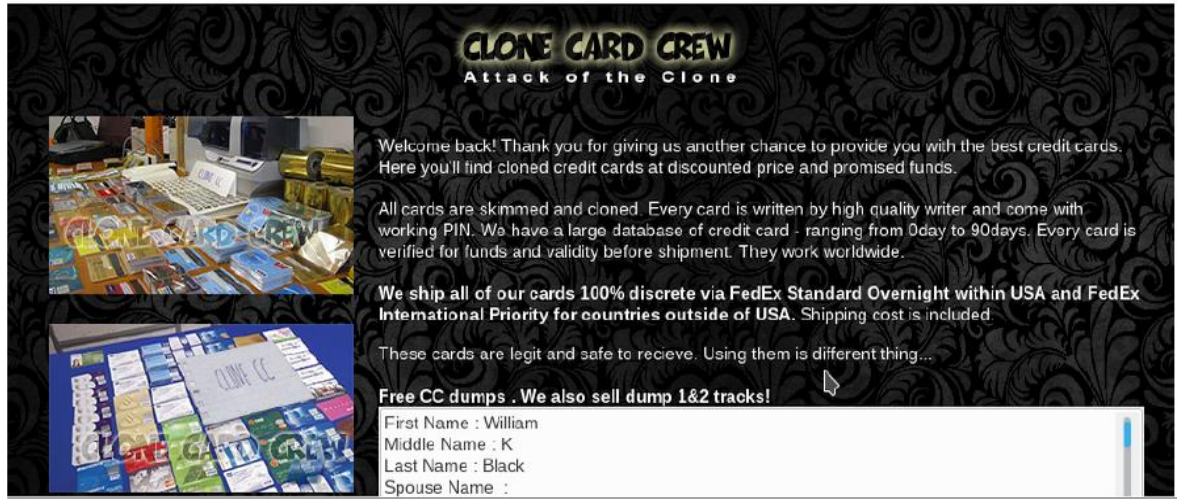
- PANDA
  - Interdisciplinary research project
  - Running until mid 2022
  - Risks and chances of darknets



MOTIVATION

- Phishing in Tor most often means cloning
- Goal: Cheating users in paying for (illegal) things without receiving them
- Many darknet studies claim vast amount of illegal offerings
  - How many are genuine?
- How big is the risk from fake legal offerings?
  - Fake whistleblower site





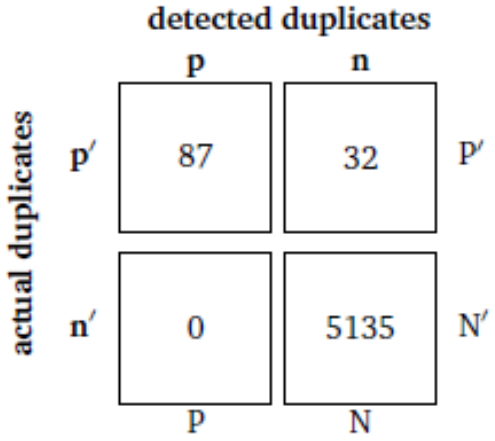
APPROACH

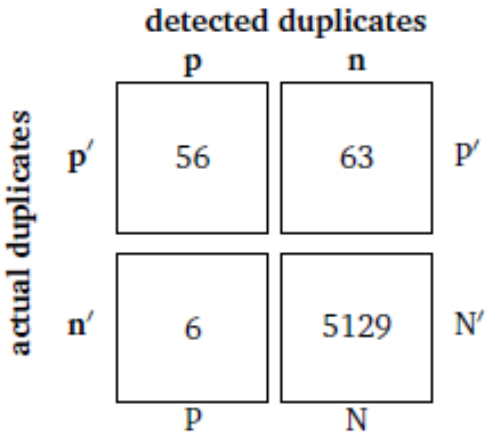
- Crawling of onion pages
- Implementation of comparison techniques
  - Addresses
  - Embedded images
  - Textual content
- Finding suitable similarity measures
  - Edit distances
  - Crypto Hashes, Robust Hahses
  - NLP methods

DETECTOR CONFUSION MATRICES

Testing phase; 103 onion services, 5,254 comparisons

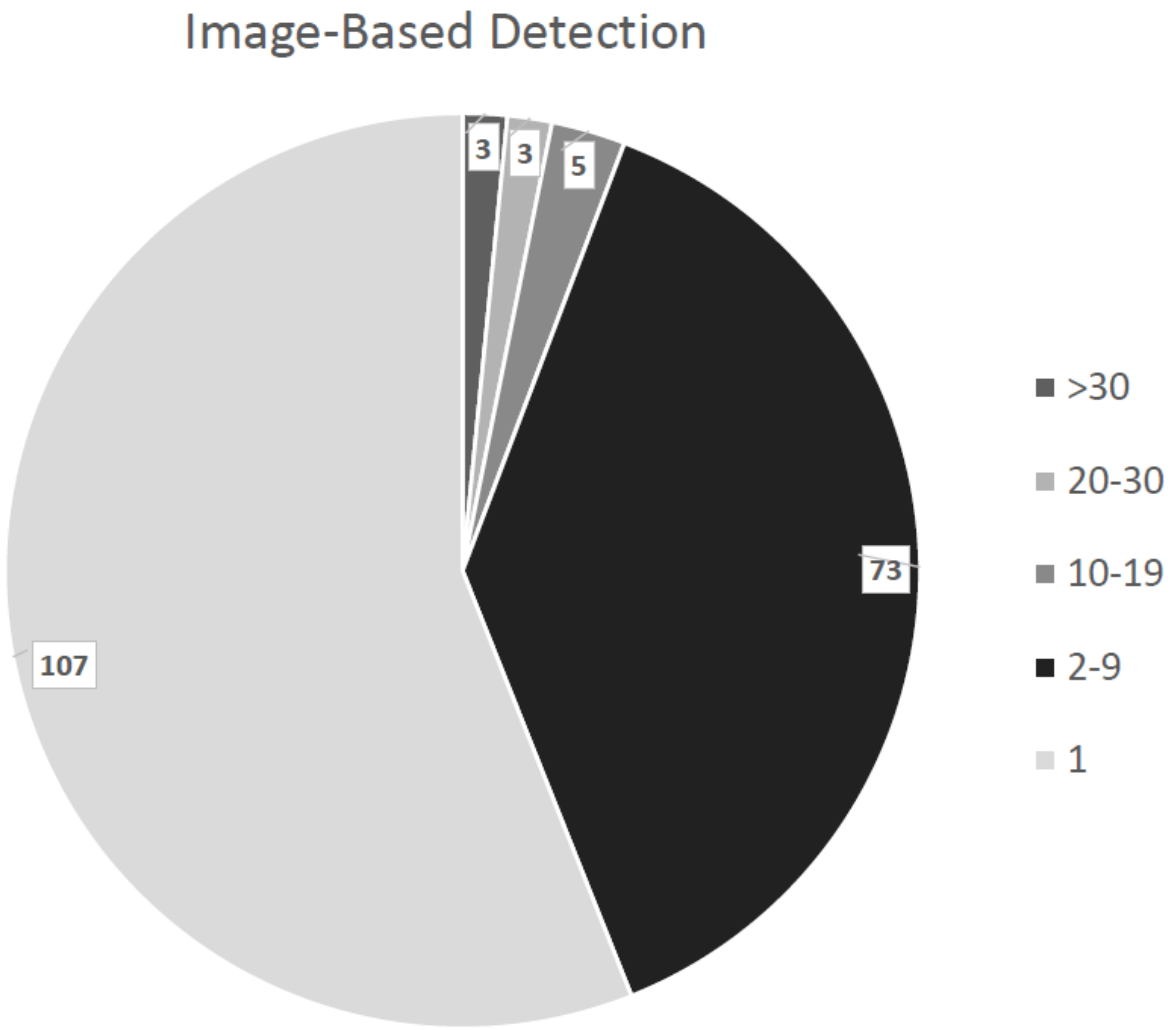
image	address





FINDINGS

- Phishing sites can be found with simple tools
- Most sites seem to be created automatically
- Image-based detection performs best
  - Results for 4,210 services
- Most pages with clones have Bitcoin context



THANK YOU.