



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

DFRWS is dedicated to the sharing of knowledge and ideas about digital forensics research. Ever since it organized the first open workshop devoted to digital forensics in 2001, DFRWS continues to bring academics and practitioners together in an informal environment.

As a non-profit, volunteer organization, DFRWS sponsors technical working groups, annual conferences and challenges to help drive the direction of research and development.

<https://dfrws.org>

PHISHING DETECTION ON TOR HIDDEN SERVICES

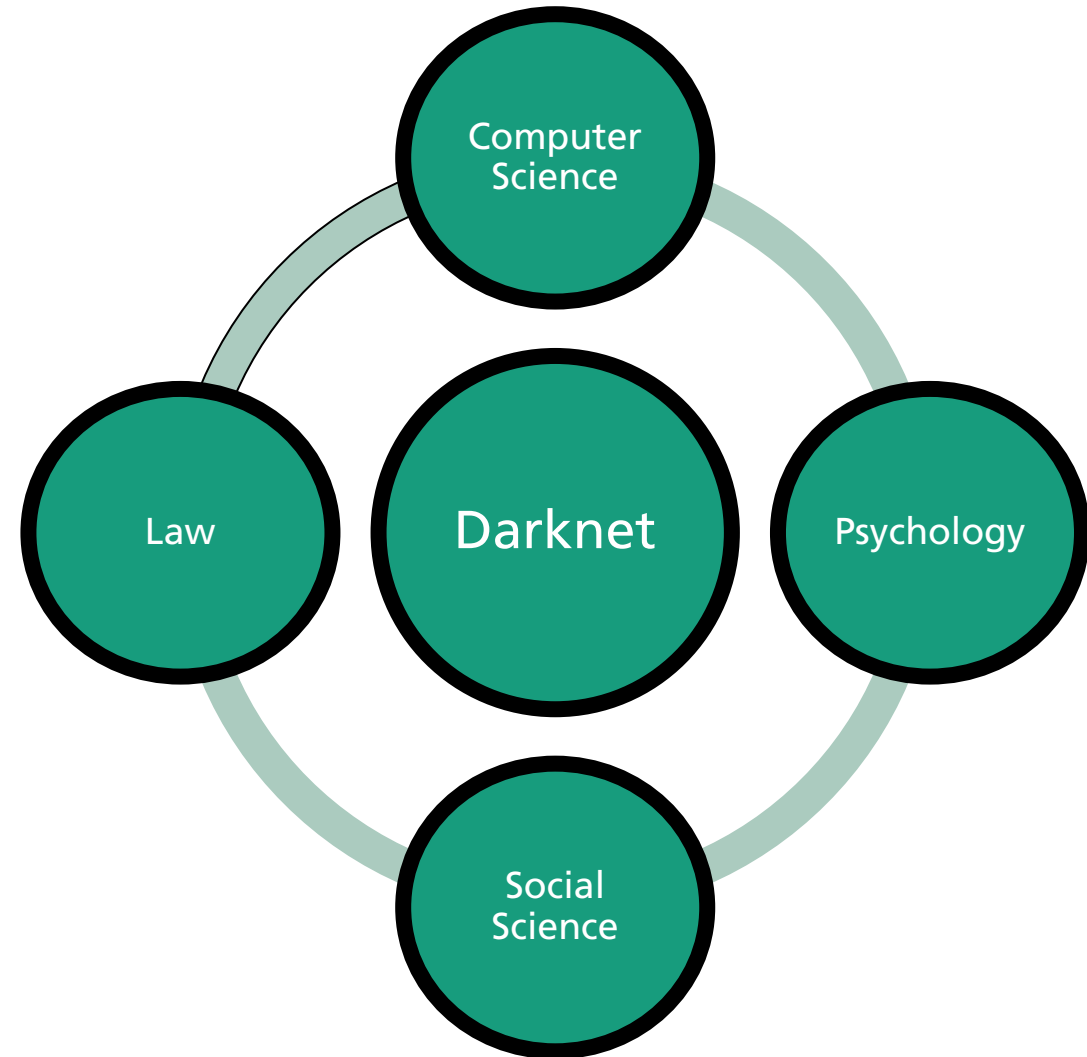
Martin Steinebach, Sascha Zenglein, Katharina Brandl



SIFO.de

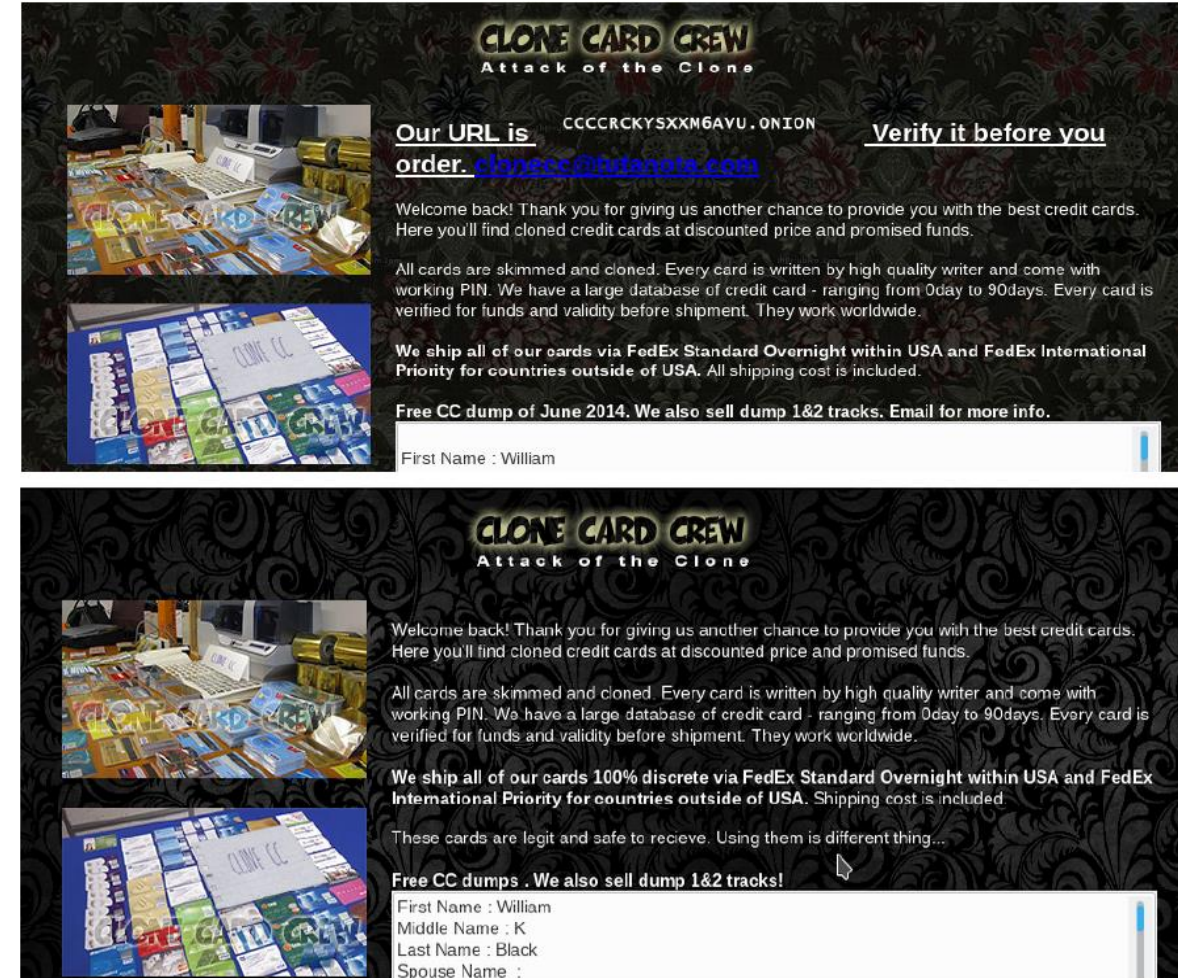
BACKGROUND

- 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 Hashes
 - NLP methods

```
</style></head><body><a class="fhgruttzhghg" href="http://visitorfifjwl377.onion  
<p class="btc">This site runs without sponsors at the moment.... Please donate to  
--><div style="text-align: center;"><a href="http://sgkvfgvtxjzvbadm.onion/"><div  
&ensp;
```

```
<a href="http://un62d2ywi33bho53.onion/"><div style="display: inline-block;  
&ensp;
```

```
<a href="http://bitblendzdkrdkvf.onion/?r=37985"><div style="display: inline
```

visitorfifjwl377.onion

```
</style></head><body><a class="fhgruttzhghg" href="http://visitorfi5kl7q7i.onio  
<p class="btc">This site runs without sponsors at the moment.... Please donate t  
--><div style="text-align: center;"><a href="http://sgkvfgvtxjzvbadm.onion/"><di  
&ensp;
```

```
<a href="http://un62d2ywi33bho53.onion/"><div style="display: inline-block  
&ensp;
```

```
<a href="http://bitblendervrfkzr.onion/?r=37985"><div style="display: inli
```

visitorfi5kl7q7i.onion

DETECTOR CONFUSION MATRICES

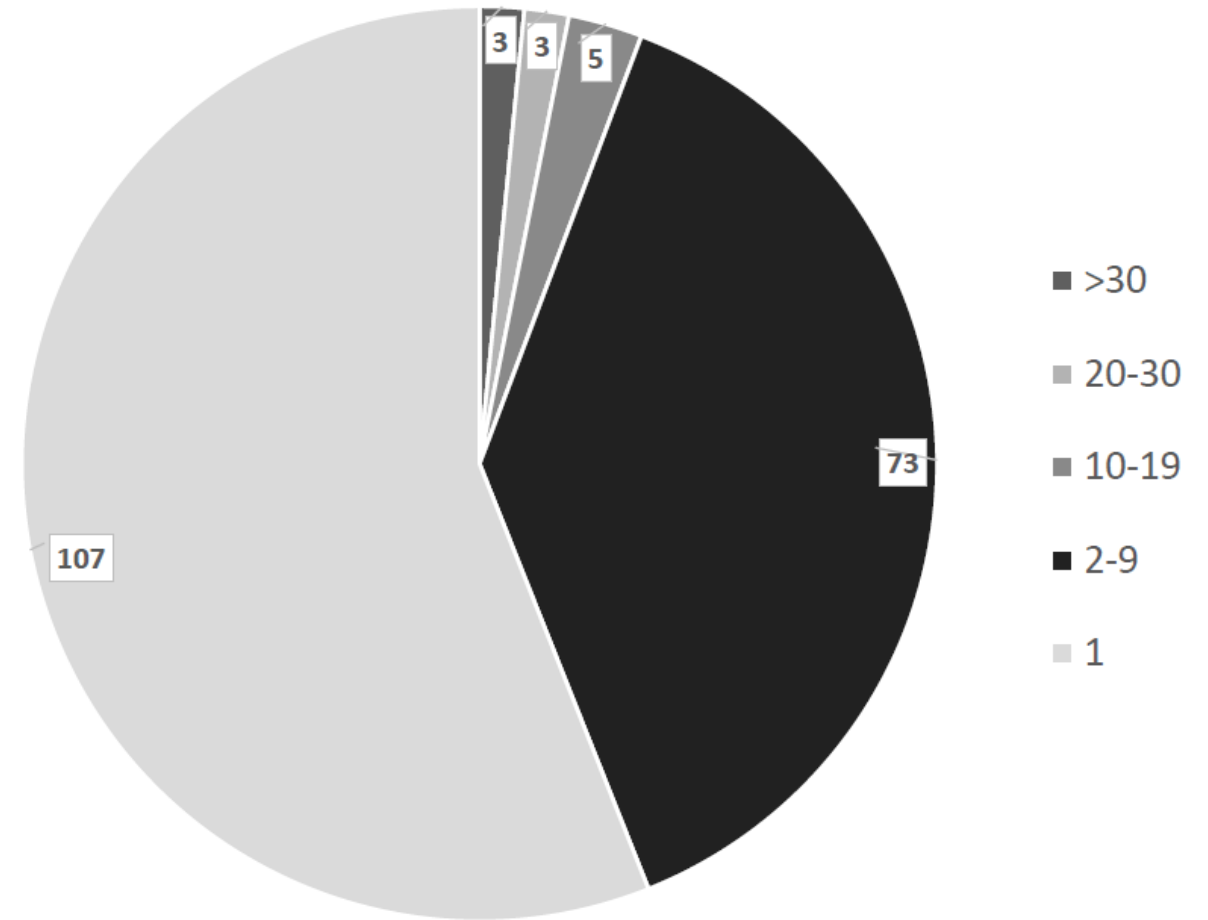
Testing phase; 103 onion services, 5,254 comparisons

image				address			
detected duplicates				detected duplicates			
p				p			
actual duplicates	p'	87	p'	actual duplicates	p'	56	p'
	n'	0	N'		n'	6	N'
p				p			
n				n			

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

Image-Based Detection



THANK YOU.

