

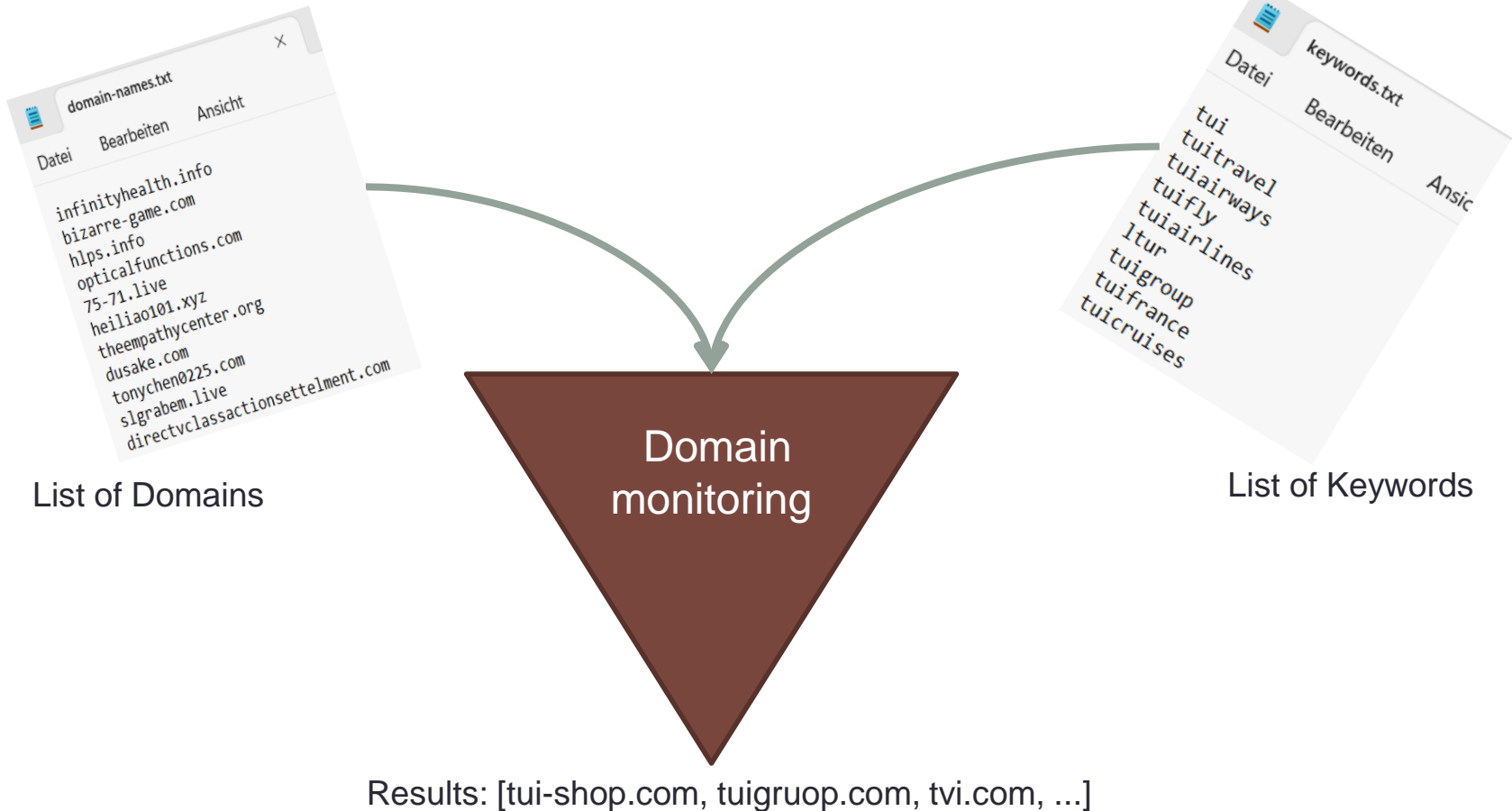
HOW CAN COMPANIES MONITOR FRAUDULENT DOMAINS ON THEIR OWN

Patrick Steinhoff, 16.11.2023

Agenda

- Introduction
- Presentation of open source program for domain monitoring operations
 - Domainthreat
- Collaboration Points to other departments
- Summary

Introduction



Why Domain Monitoring?

Threat Landscape:

- Brand infringements
- Ransomware / Malware channel
- Phishing
- Social Engineering
- ...

➔ Its a matter of collaboration between departments

Example UDRP Cases

Case Number	Domain(s)	Complainant	Respondent	Ruleset	Status
2008257	skyvvaveantennas.com	Skywave Antennas, Inc.	BAROUD RAYMOND	UDRP	TRANSFERRED 13-Sep-2022
<p>domain name to effectuate a phishing scheme Additionally Respondent uses the confusingly similar nature of the domain name to divert users to Respondent's own webpage where the Respondent displays competing hyperlinks ♦ Respondent registered and</p> <p>13-Sep-2022 08:28pm 0 Comments Follow</p>					
2004923	eastman.com	Eastman Chemical Company	Mong Wong / Plastic goba l co.ltd	UDRP	TRANSFERRED 16-Aug-2022
<p>as part of a fraudulent phishing scheme ♦ Respondent lacks both rights to and legitimate interests in the domain name ♦ Respondent provided false contact information when it registered the domain name ♦ Respondent knew of Complainant's rights</p> <p>16-Aug-2022 01:27pm 0 Comments Follow</p>					
1998215	xn--gogle-6dc.com	Google LLC	Steven Ng	UDRP	TRANSFERRED 29-Aug-2022
<p>a PUNYCODE translation of the IDN g ogle.com ♦ Prior UDRP panels have found IDNs and their PUNYCODE translations to be equivalent. ♦ See Google LLC v Christopher Hadnagy FA 1944032 Forum June 17 2021 finding the IDN g gle.com and its PUNYCODE</p> <p>29-Aug-2022 01:31pm 0 Comments Follow</p>					

“vv” → “w”

“rn” → “m”

xn--gogle-6dc.com →
gòogle.com

*Look-a-like Domains are domains that are confusingly similar registered to original company (mailing) domains.



Open Source Repos github



Patrick Steinhoff

PAST2212

Just a small guy with small dreams and a great cat to fight cyber criminals

Popular repositories

Customize your pins

domainthreat

Public

Daily Domain Monitoring to detect phishing and brand impersonation with subdomain enumeration and source code scraping

Python 12 1

zonethreat

Public

Domain Zone File Monitoring for brand names and mailing domain names to detect phishing and brand impersonations

Python 3

certthreat

Public

CERT Transparency Log Monitoring for brand names and mailing domain names to detect phishing and brand impersonations

Python 2

websitewatcher

Public

Detect and send e-mails about changes of observed domains / websites.

Python 1

scamback

Public

send fake credentials to known phishing sites

Python

Domainmonitoring based on daily, newly registered Domains (Version 3.02)

```
with open(f'{desktop}/Newly-Registered-Domains_Calender-Week_{datetime.datetime.now().isocalendar()[1]}_{datetime.datetime.today().year}.csv', mode='a', newline='') as f:
    writer = csv.writer(f, delimiter=',')
    for keyword in list_file_keywords:
        for domain in list_file_domains:
            if keyword in domain and all(black_keyword not in domain for black_keyword in list_file_blacklist_keywords) is True:
                writer.writerow([domain, keyword, today, Topic_Match(), "Full Word Match"])

            elif jaccard(keyword, domain) is not None:
                writer.writerow([domain, keyword, today, Topic_Match(), "Jaccard"])

            elif damerau(keyword, domain) is not None:
                writer.writerow([domain, keyword, today, Topic_Match(), "Damerau-Levenshtein"])

            elif jaro_winkler(keyword, domain) is not None:
                writer.writerow([domain, keyword, today, Topic_Match(), "Jaro-Winkler"])

            elif LCS(keyword, domain, 0.5) is not None:
                writer.writerow([domain, keyword, today, Topic_Match(), "LCS"])


            elif unconfuse(domain) is not domain:
                latin_domain = unicodedata.normalize('NFKD', unconfuse(domain)).encode('latin-1', 'ignore')
                if keyword in latin_domain:
                    writer.writerow([domain, keyword, today, Topic_Match(), "IDN Full Word Match"])
```



You can run it on windows, linux, ...




And its for free

You can use it, modify it, adapt it, ...



<https://github.com/PAST2212/domainthreat>








 **domainthreat** Public

 Pin  Unwatch 1

 main  1 branch  0 tags

Go to file Add file Code

 **PAST2212 Update README.md** 1df0b67 2 weeks ago  201 commits

 User Input	Update keywords.txt	4 months ago
 Changelog	Update Changelog	last month
 LICENSE.md	Create LICENSE.md	6 months ago
 README.md	Update README.md	2 weeks ago
 detectidna.py	Add files via upload	last month
 domainthreat.py	v 3.0	last month
 requirements.txt	Update requirements.txt	last month

Domainmonitoring based on daily, newly registered Domains (Version 3.02)

Detection Scope of domainthreat v 3.02:

- full-word matching (e.g. amazon-shop.com),
- regular typo squatting cases (e.g. ammazon.com),
- typical look-alikes / phishing / so called CEO-Fraud domains (e.g. arnazon.com (rn = m),
- IDN Detection / look-alike Domains based on full word matching (e.g. pay**ρ**al.com - greek letter RHO 'ρ' instead of latin letter 'p'),
- IDN Detection / look-alike Domains based on partial word matching (e.g. pya**ρ**a1.com - greek letter RHO 'ρ' instead of latin letter 'p' AND "ya" instead of "ay" AND Number "1" instead of Letter "l")

Domainmonitoring based on daily, newly registered Domains (Version 3.02)

Example Features of domainthreat v 3.02 :

- check if domain is parked or not (experimental state)
- check if domain is email ready (ready for receiving mails or ready for sending mails)
- keyword detection in source codes of newly registered domains (even if they are in other languages)

==> This is to cover needs of international companies and foreign-speaking markets

- daily CSV / Excel export

A	B	C	D	E	F
Domains	Keyword Fou	Detected by	Subdomains		
bluetiktok.net	tiktok	Full Word Match	('www.bluetiktok.net', 'bluetiktok.net')		
tiktok77.top	tiktok	Full Word Match	('app.tiktok77.top', 'www.tiktok77.top', 'tiktok77.top')		
tiktokguide.fun	tiktok	Full Word Match	('www.pay.tiktokguide.fun', 'pay.tiktokguide.fun')		
faebookcebook.com	facebook	Similarity Jaccard	('ww16.faebookcebook.com', '*.faebookcebook.com', 'ww11.faebookcebook.com', 'fawwcebook.com', '*.fawwcebook.com', 'ww2.fawwcebook.com', 'ww25.fawwcebook.com')		
googgie.com	google	Similarity Jaro-Winkler	('googgie.com', '*.googgie.com', 'ww1.googgie.com')		

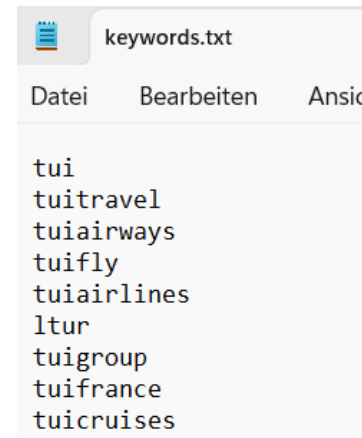
Domainmonitoring based on daily, newly registered Domains (Version 3.02)

Before the first run - How it Works:

1. Put your brand names or mailing domain names into the TXT file "keywords.txt" for monitoring operations (without the TLD).

These keywords will be used for searching / matching in domain names

Some "TUI" Names are listed per default.



2. Put common typical word collisions into the TXT file "blacklist_keywords.txt" line per line you want to exclude from the results to reduce false positives.

- e.g. blacklist "lotto" if you monitor keyword "otto", e.g. blacklist "intuitive" if you want to monitor "tui", ...

3. Put commonly used words into this TXT file "topic_keywords.txt" that are describing your brands, industry, brand names or products on websites. **These keywords will be used for searching / matching in page source codes.** Default language is english for performing automated translation operations from HTML Title and Description Tag via Google Translator API.

- e.g. Keyword "fashion" for a fashion company, e.g. "sneaker" for shoe company, e.g. "Zero Sugar" for Coca Cola Inc., ..., e.g. "holiday" for TUI

Domainmonitoring based on daily, newly registered Domains (Version 3.02)

Sample Output:

	A	B	C	D	E
1	Domains	Keyword Found	Date	Topic found in Source Code	Detected by
2	a6tui.com	tui	13.02.2023	[]	Full Word Match
3	nuantui5.top	tui	13.02.2023	['journey']	Full Word Match
4	nuitrinaire.shop	tui	13.02.2023	[]	Full Word Match
5	tiu.life	tui	13.02.2023	[]	Jaccard
6	tuigfurnituren.com	tui	13.02.2023	[]	Full Word Match
7	tuivirtualgroup.co.uk	tui	13.02.2023	[]	Full Word Match
8	aiitravel.com	tuitravel	13.02.2023	[]	Damerau
9	resultati.online	tuitravel	13.02.2023	[]	Jaccard
10	robinsonsbayvalley.com	robinson	13.02.2023	['holiday']	Full Word Match
11	robinsonuche.com	robinson	13.02.2023	[]	Full Word Match
12	turfinc.org	tuifrance	13.02.2023	[]	Jaro-Winkler
13	curtainfire.com	tuifrance	13.02.2023	[]	Jaccard
14	theaitakeover.com	tuitakeoff	13.02.2023	[]	LCS
15	museminx.com	musement	13.02.2023	[]	Damerau
16	dulichtui.com	tui	14.02.2023	['travel']	Full Word Match
17	tui999333.online	tui	14.02.2023	[]	Full Word Match

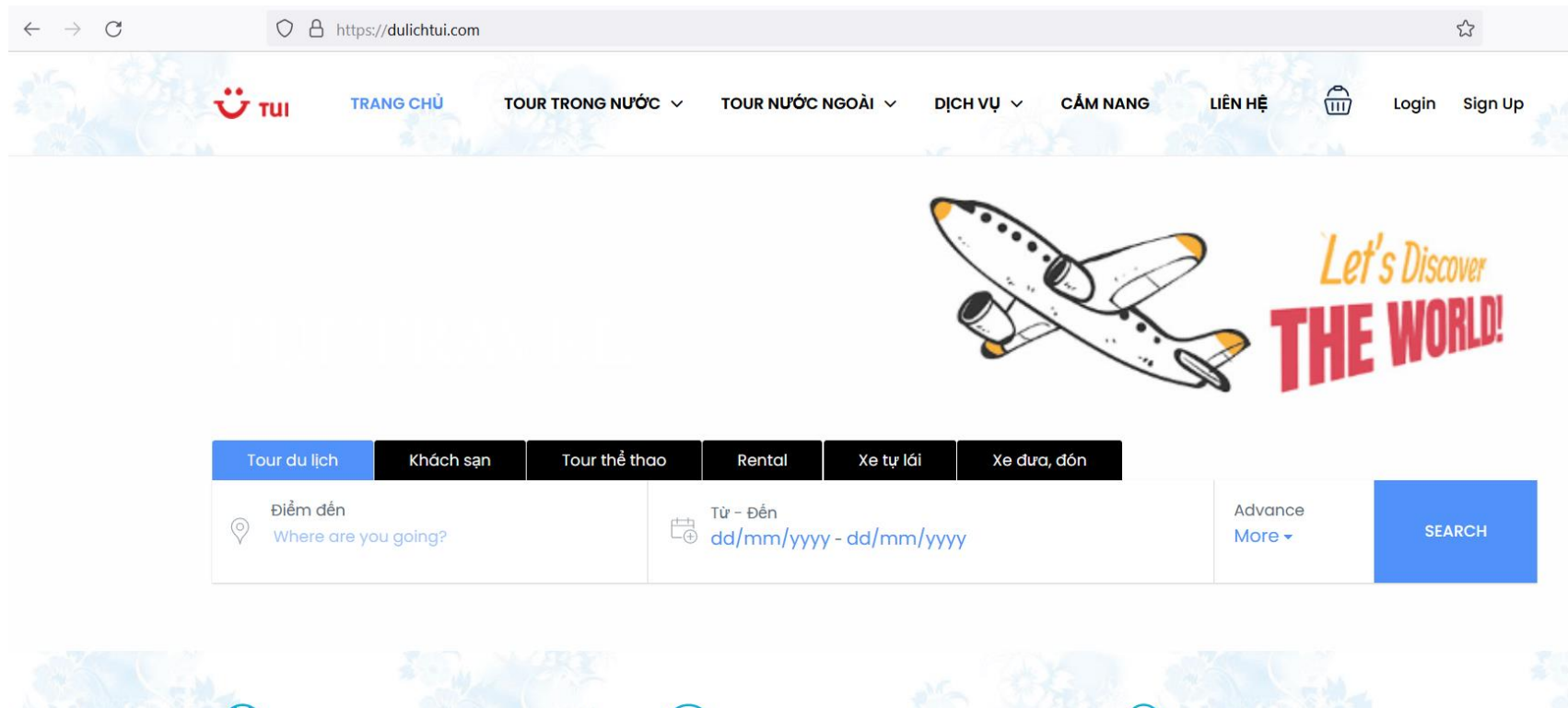
➔ Algorithm has automatically found the word “travel” in the page source code of detected newly, registered domain dulichtui.com

➔ “Travel” is listed as a keyword in the self defined TXT file “topic_keywords.txt”, you want to find in webpages

Touch Points to Fraud Management



Singular Event:


- One fraudulent website in another country without any local business impact?




The screenshot displays the TUI website interface. At the top, the navigation bar includes the TUI logo, a 'TRANG CHỦ' link, and several menu items: 'TOUR TRONG NƯỚC', 'TOUR NƯỚC NGOÀI', 'DỊCH VỤ', 'CẨM NANG', 'LIÊN HỆ', a shopping cart icon, 'Login', and 'Sign Up'. Below the navigation bar is a large banner featuring a stylized airplane and the text 'Let's Discover THE WORLD!'. The main content area contains a search bar with a horizontal menu of categories: 'Tour du lịch', 'Khách sạn', 'Tour thể thao', 'Rental', 'Xe tự lái', and 'Xe đưa, đón'. The search bar itself has three input fields: 'Điểm đến' (Where are you going?), 'Từ - Đến' (dd/mm/yyyy - dd/mm/yyyy), and 'Advance More'. A blue 'SEARCH' button is positioned to the right of the search bar.


← → ↻ <https://dulichtui.com> ☆

 [TRANG CHỦ](#) [TOUR TRONG NƯỚC](#) [TOUR NƯỚC NGOÀI](#) [DỊCH VỤ](#) [CẨM NANG](#) [LIÊN HỆ](#)  [Login](#) [Sign Up](#)

 *Let's Discover*
THE WORLD!

[Tour du lịch](#) [Khách sạn](#) [Tour thể thao](#) [Rental](#) [Xe tự lái](#) [Xe đưa, đón](#)

 **Điểm đến**
Where are you going?

 **Từ - Đến**
dd/mm/yyyy - dd/mm/yyyy

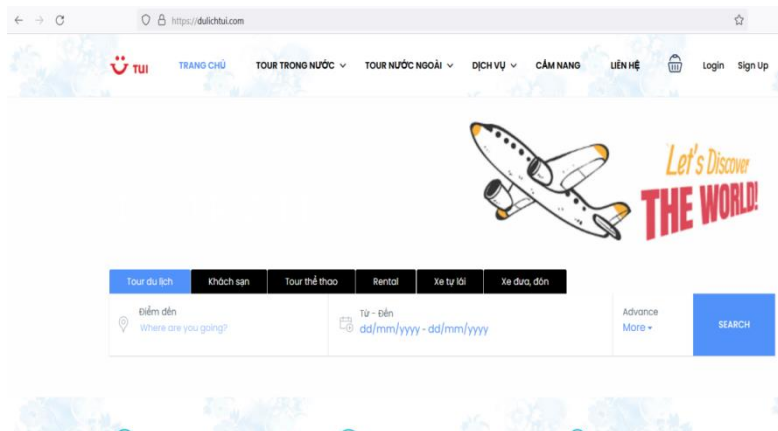
Advance
More ▾

SEARCH

Touch Points to Fraud Management

Singular Event → Holistic Approach

- Website is an object of different unique identifiers (true positive labeled information) which are identifying state / behaviour or pattern of criminal actors
 - example identifiers: html title, mail address, mail sending ip, dns records, cookies, image (meta data), backlinks, etc.
- Ability to differentiate between organized business models and “pranks” are important for companies for budget decisions
 - Which cases are more important to take actions (e.g. enforcements / police department collaborations, etc)



Collaboration Points



Fraud Investigation as a mix of semi automated techniques / technologies for information gathering depending on the particular case:

- building web spiders (e.g. finding all domains with same registration date and same A-Records, ...)
- building probability models (mix of different data points with different weights - e.g. another website with same mail address)
- Using different data feeds (e.g. blacklists, passive dns data, social media feeds (SOCMINT), ...)
-
- And also google (dorking) ...

Touch Points to Fraud Management

and also google (dorking) ...


Google

intext:"Tourism Union Indochina" X  

<https://tuitravel.com> > giới thiệu · Diese Seite übersetzen


Giới thiệu - TUI Travel - Nhà tổ chức tour online hàng đầu

TUI Travel (Tourism Union Indochina). TUI Travel được gây dựng từ năm 1993. Từ một cơ sở ở Thành phố Hồ Chí Minh (Sài Gòn), ý tưởng của chúng tôi rất đơn ...


 vietnamcambodiatours.com
<https://vietnamcambodiatours.com> > ... · Diese Seite übersetzen

Blog • TUI Travel - Vietnam Cambodia Tours

Copyright © TUI Travel (Tourism Union Indochina) . All rights reserved. Make An Inquiry.
Name *. First. Last. Email *. Special Requirements/Comments/ ...


 YouTube
<https://m.youtube.com/watch> · Diese Seite übersetzen

TUI offers tailor-made vacations in Vietnam, Cambodia, Laos ...

 6:32

TUI **TOURISM UNION INDOCHINA**. Subscribe. 0. Share. Save. Report.
Comments. thumbnail-image. Add a comment... 35:08 · Go to channel ...

YouTube · TUI TOURISM UNION INDOCHINA · vor 3 Wochen

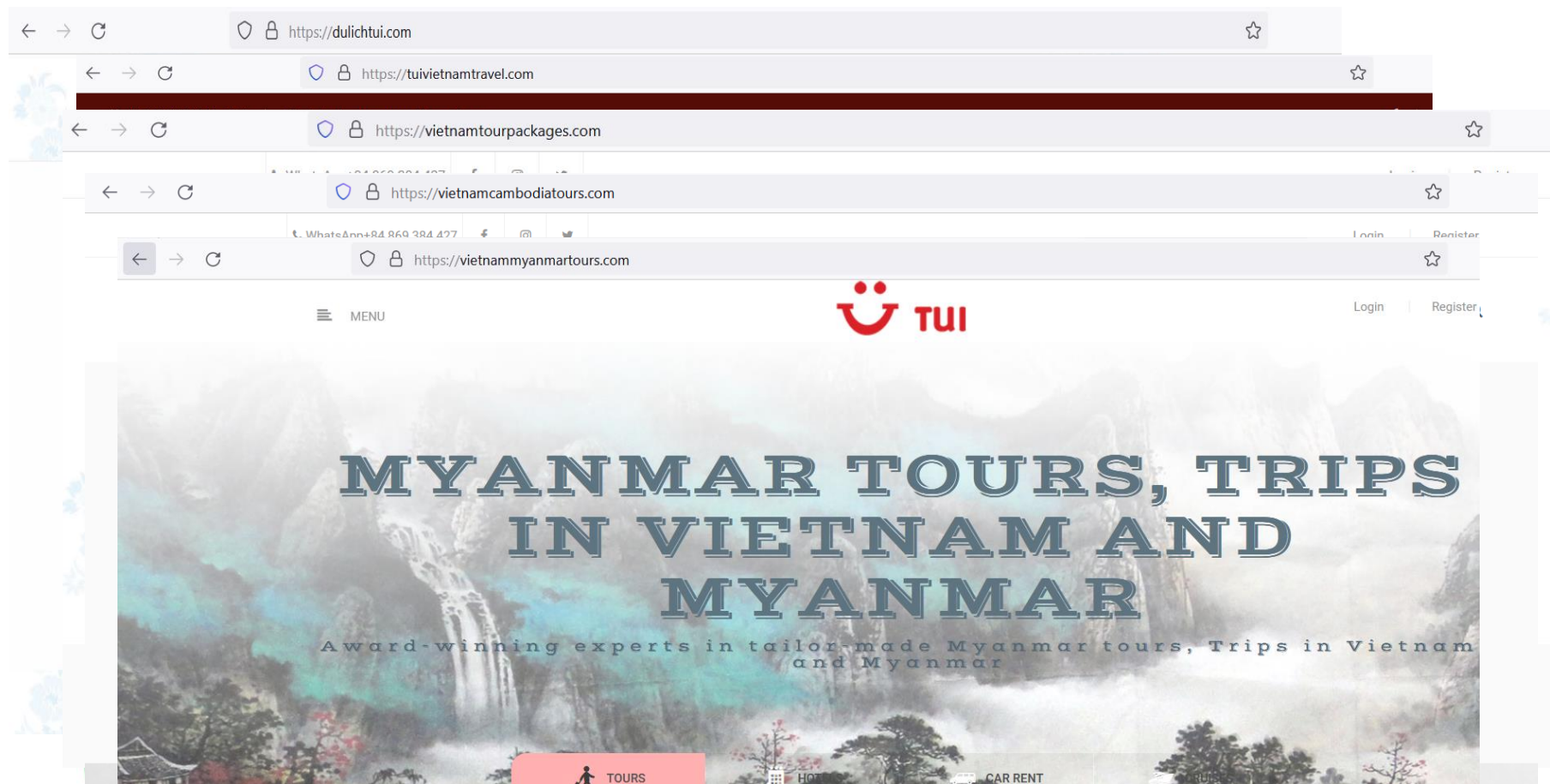
 vietnammyanmartours.com
<https://vietnammyanmartours.com> > ... · Diese Seite übersetzen

Hotels List • TUI Travel - Vietnam Myanmar Tours

Partner 03. Partner 05. Partner 06. Partner 07. Partner 08. Partner 01. Partner 02. Partner 04.
Copyright © TUI Travel (Tourism Union Indochina) . All rights ...

Touch Points to Fraud Management

Exploring technical correlations



Outlook

→ Enhance Detection Scope by AI based Logo Detection Mechanism



End

Questions?

Scripts:

<https://github.com/PAST2212>

Contacts:

E-Mail: patrick.steinhoff@hotmail.com

linkedin: <https://www.linkedin.com/in/patrick-steinhoff-168892222/>