

Online Business Models Infringing Intellectual Property Rights - Phase 2 Suspected trade mark infringing e- shops utilising previously used domain names

EUIPO Webinar

24 October 2017

Erling Vestergaard

European Observatory on Infringements of Intellectual Property Rights, EUIPO

Content

The Online Business Models Infringing IPR Series

Phase 2 Background and Methodology

Main Research Findings

Conclusions

The Online Business Models Infringing IPR Series

The Online Business Models Infringing IPR Series

The Online Business Models Infringing IPR Series

The Series So Far

The Provider

- Deloitte Advisory S.L. supported by
- An Attorney-at-Law specialising in internet cases, a panellist in WIPO UDRP
- An IT Forensic expert, previously working for a cybercrime police unit
- Published 12 July 2016

Research on Online Business Models
Infringing Intellectual Property Rights

Phase 1
Establishing an overview of online business
models infringing intellectual property rights



Matrix	Online Digital Platform	A	B	C	D	E	F
		Internet Site Controlled by Infringer	Third Party Marketplace	Social Media or Blog	Gaming or Virtual World	E-mail, Chatroom or Newsgroup	Mobile Devices
IPR Infringing Activity							
1 Domain Name or Digital Identifier Misuse of IPR		A1	B1	C1	D1	E1	F1
2 Physical or Virtual Product Marketing		A2	B2	C2	D2	E2	F2
3 Digital Content Sharing		A3	B3	C3	D3	E3	F3
4 Account Access or Codes to Digital Content Sharing		A4	B4	C4	D4	E4	F4
5 Phishing, Malware Dissemination or Fraud		A5	B5	C5	D5	E5	F5
6 Contributing to Infringement		A6	B6	C6	D6	E6	F6



Online Intellectual Property Rights Infringing Business Model: Short Description of the Business Model

Reference: Identification of legal decision (if any)

Date of Decision: Date of Analysis

Based on the "Business Model Canvas" by Strategyzer.com

Business Model Summary:

Short summary description of the business model with focus on specific features or traits.

Indication of whether the business model is to be considered deceptive or non-deceptive.

In the Matrix, the specific digital platform and infringing activity is indicated with a grey background.

Matrix	Online Digital Platform	A	B	C	D	E	F
		Internet Site Controlled by Infringer	Third Party Marketplace	Social Media or Blog	Gaming or Virtual World	E-mail, Chatroom or Newsgroup	Mobile Devices
1	Domain Name or Digital Identifier Misuse of IPR	A1	B1	C1	D1	E1	F1
2	Physical or Virtual Product Marketing	A2	B2	C2	D2	E2	F2
3	Digital Content Sharing	A3	B3	C3	D3	E3	F3
4	Account Access or Codes to Digital Content Sharing	A4	B4	C4	D4	E4	F4
5	Phishing, Malware Dissemination or Fraud	A5	B5	C5	D5	E5	F5
6	Contributing to Infringement	A6	B6	C6	D6	E6	F6

The Online Business Models Infringing IPR Series

The Series So Far

Open Internet Marketing Misusing IPR in Domain Name or Digital Identifier

Open Internet Marketing Without Misusing IPR in Domain Name or Digital Identifier

Darknet Hidden Services

Phishing, Malware Dissemination and Fraud

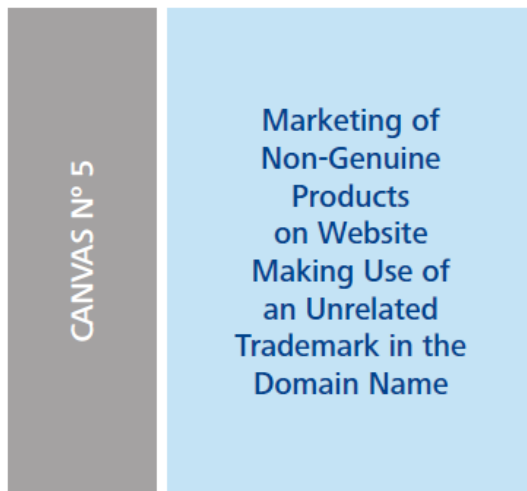
Digital Content Sharing on Open Internet

Phase 2 Background and Methodology

Phase 2 Background and Methodology

Phase 2 Background and Methodology

Case Study no. 5 in Phase 1 Report



	A	B	C	D	E	F
1	A1	B1	C1	D1	E1	F1
2	A2	B2	C2	D2	E2	F2
3	A3	B3	C3	D3	E3	F3
4	A4	B4	C4	D4	E4	F4
5	A5	B5	C5	D5	E5	F5
6	A6	B6	C6	D6	E6	F6

Danish Dispute Board for Domain Names,
Case 2015-0093, Decision of 15 September 2015

Phase 2 Background and Methodology

Case Study no. 5 in Phase 1 Report

The figures extracted from the Danish study mentioned show that for the period between October 2014 and October 2015, there were 566 .dk domains that were re-registered by suspected infringers of trade marks immediately after the domain names had been given up by their previous registrants and became available for re-registration.

The research, which had been conducted by the Danish cybercrime specialist Henrik Bjørner, is available here: <http://cybercrime.eu/analysis/analysing-registration-of-previously-used-danish-domain-names/>.

Phase 2 Background and Methodology

Objective of Phase 2

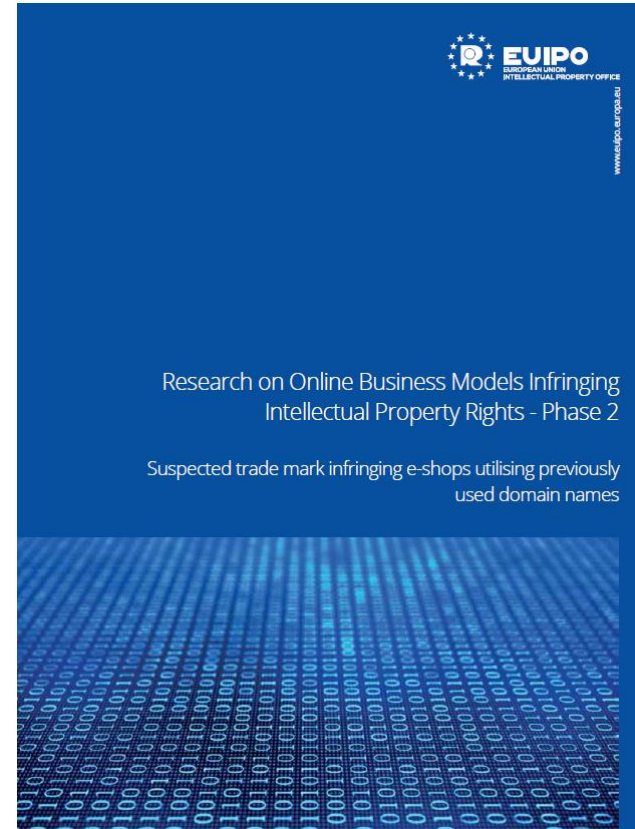
- The Danish study indicated that the same activity most likely was also happening in other countries
- Research 4 EU MS's with large e-commerce sectors
- Look for commonalities and affiliation
- For case studies apply the Phase 1 methodology: Matrix and Canvas

Phase 2 Background and Methodology

Phase 2 Report

The Provider

- Deloitte Advisory S.L. supported by
- A Danish Cybercrime expert
- An IT Forensic expert, previously working for a cybercrime police unit
- Published 24 October 2017





.uk
10.6 million domains



UK



Sweden



.se
1.4 million domains



Germany



.de
16 million domains



Spain

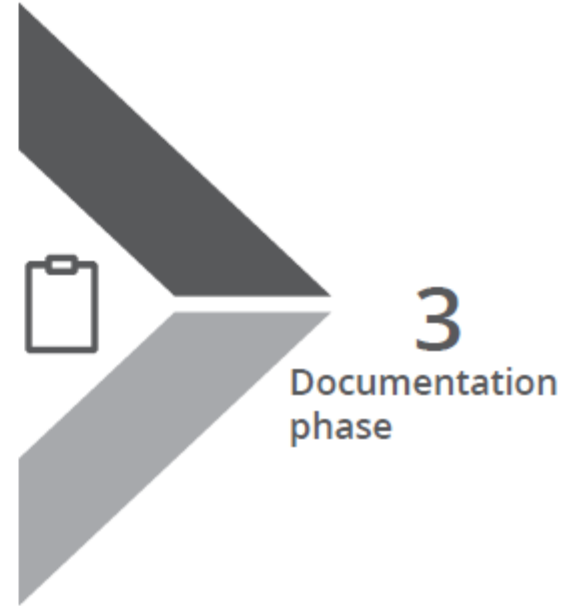
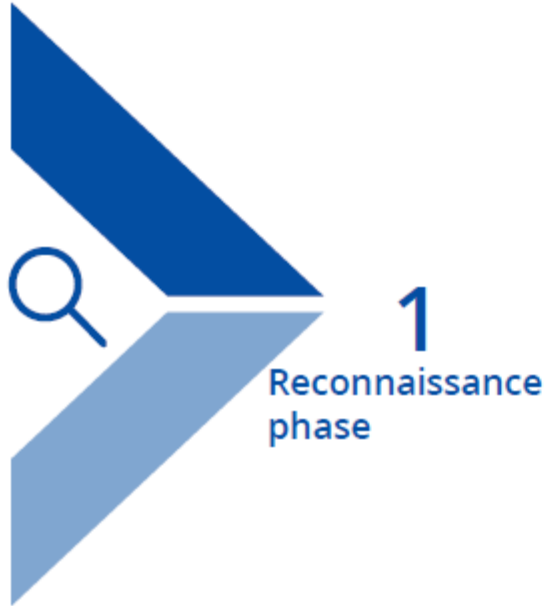


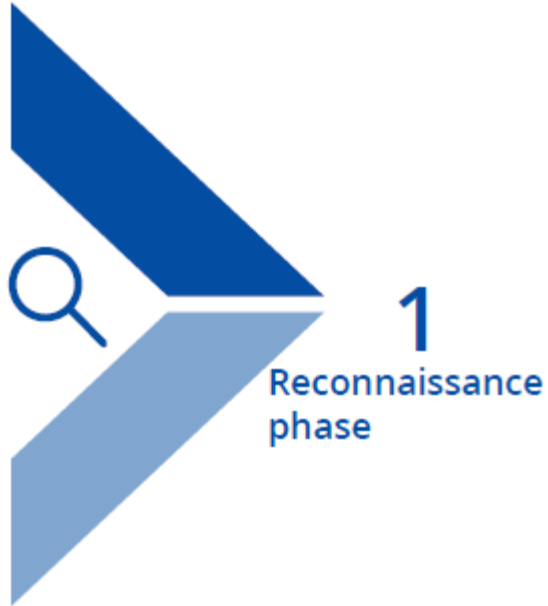
.es
1.8 million domains

Phase 2 Background and Methodology

Phase 2 Methodology

- Detection of e-shops susceptible of trade mark infringement
- Analysis of
 - utilisation of previously used domain names
 - affiliation
 - resilience against enforcement measures

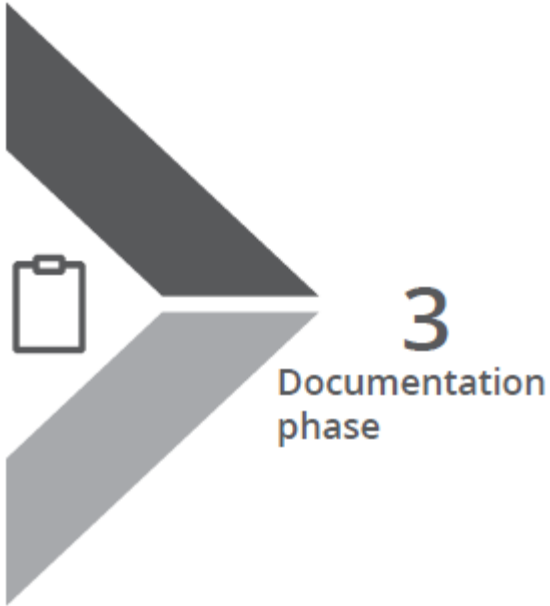




- Gather information about registered domain names in each ccTLD
- Determine which domain names were actively connected to a website
- Determine if the website was an e-shop
- If yes: Gather metadata, HTML elements, source code and other technical information



- Website information passed through a set of technical modules
- Detection of e-shop infrastructure and specific source code characteristic of e-shops suspected of marketing of trade mark infringing goods:
Unusual price tags, massive discount, lack of proper company information and recurring website structure
- A proprietary algorithm calculated a score determining if the website could be suspected



- Collection and generation of documentation for each e-shop
- Collection of information about possible previous use of domain name
- Development of 40 in-depth case studies
- Securing anonymisation of findings in the research report
- Finalising research report

Phase 2 Background and Methodology

Phase 2 Methodology

10 categories of previous use of domain names was defined

1. Public, international and interest organisations
2. Financial sector
3. News, media and information websites
4. Other businesses
5. Political debate and propaganda
6. Voluntary work
7. Cultural and religious websites
8. Private associations
9. Famous people and fan clubs
10. Adult and dating websites.

Main Research Findings

Main Research Findings

ccTLD	Sweden .se	Germany .de	United Kingdom .uk	Spain .es	Total
Period of analysis	8-10 December 2016	23 November – 6 December 2016	26 January– 10 February 2017	10–11 January 2017	
Total number of detected active domain names under the ccTLD resolving to an active website	1 259 990	11 057 426	8 158 245	1 047 780	21 523 441

ccTLD	Sweden .se	Germany .de	United Kingdom .uk	Spain .es	Total
Total number of detected e-shops using a domain name under the ccTLD	33 212	208 939	224 154	49 147	515 452
Total number of detected e-shops suspected of infringing the trade marks of others using a domain name under the ccTLD	3 161 (9.5 % of total number of e shops)	6 066 (2.9 % of total number of e-shops)	14 182 (6.3 % of total number of e-shops)	4 461 (9.1 % of total number of e-shops)	27 870 (5.41 % of total number of e-shops)

Minimum number



ccTLD	Sweden .se	Germany .de	United Kingdom .uk	Spain .es	Total
Total number of detected e-shops suspected of infringing the trade marks of others using a domain name under the ccTLD where the domain name had been previously used by another registrant	2 444 (77.3 % of suspected e-shops)	4 864 (80.2 % of suspected e-shops)	10 081 (71.1 % of suspected e-shops)	3 612 (81.0 % of suspected e-shops)	21 001 (75.35 % of suspected e-shops)

Minimum number



Main Research Findings

Case Studies

Domain001

In the *Domain001*-se case study the prior use of the domain name was to direct internet traffic to a Swedish language website with information from the European Parliament to the Swedish public.

Domain007

In the *Domain007*-de case study the prior use of the domain name was to direct internet traffic to a German language website with information about a ballet school.

Domain010

In the *Domain010*-co.uk case study the prior use of the domain name was to direct internet traffic to an English language website with information about a local escort service.

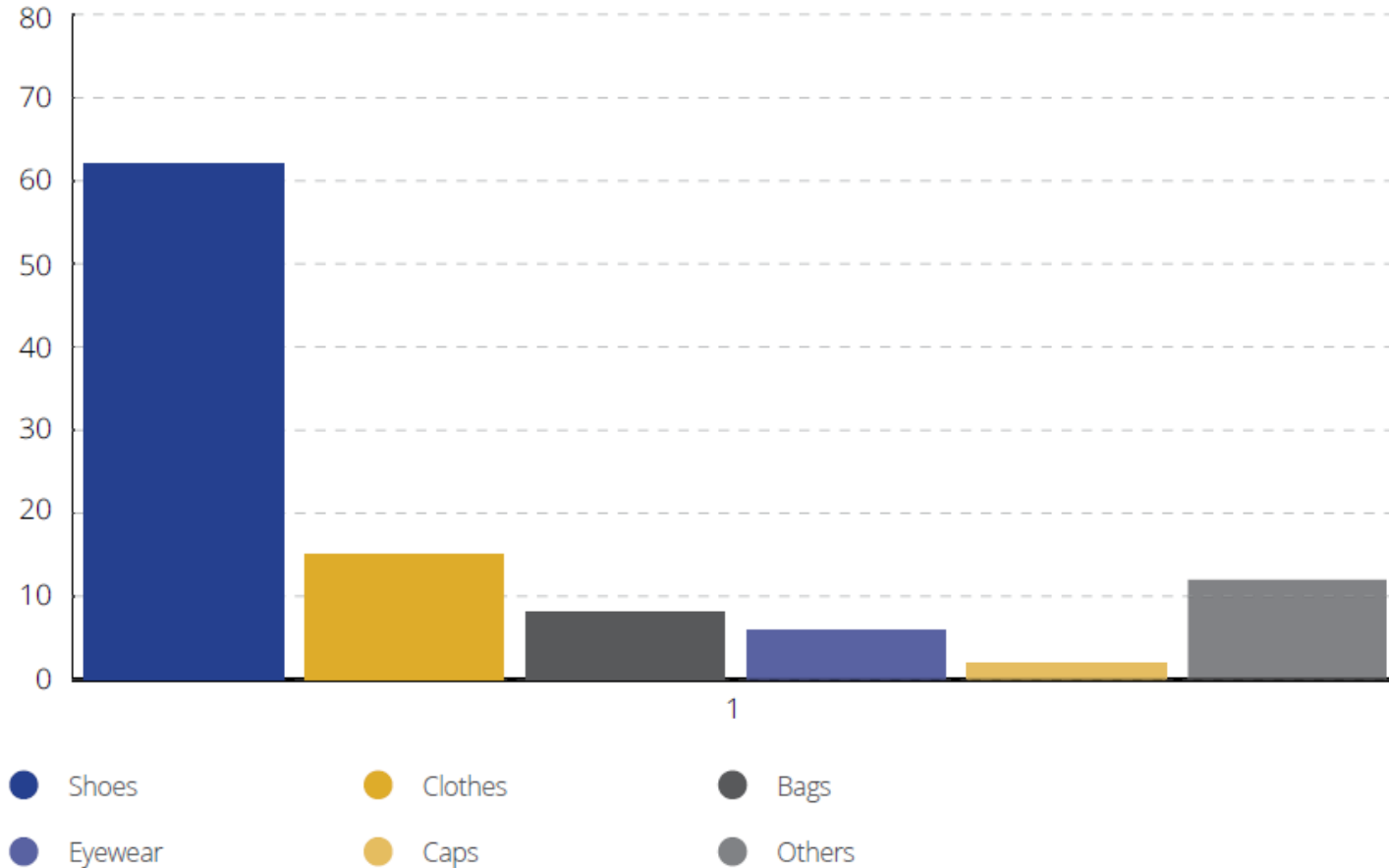
Domain003

In the *Domain003*-es case study the prior use of the domain name was to direct internet traffic to a Spanish language website with information about cancer and related treatments

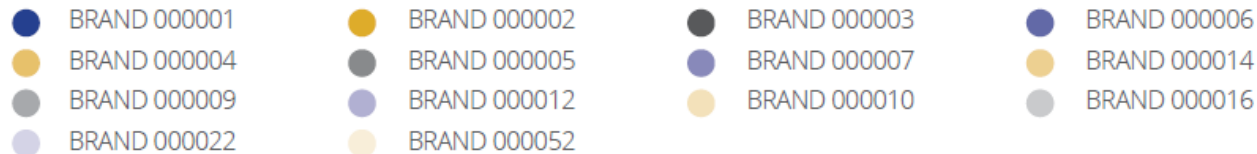
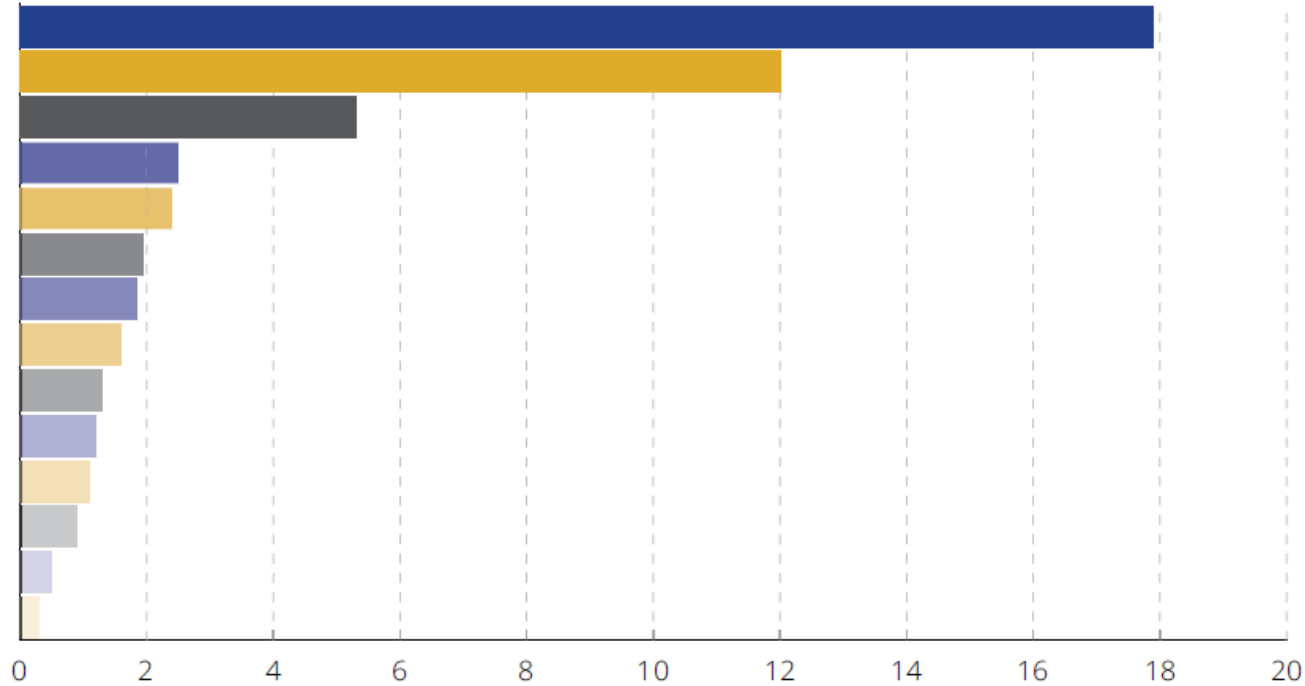
Main Research Findings

Commonalities

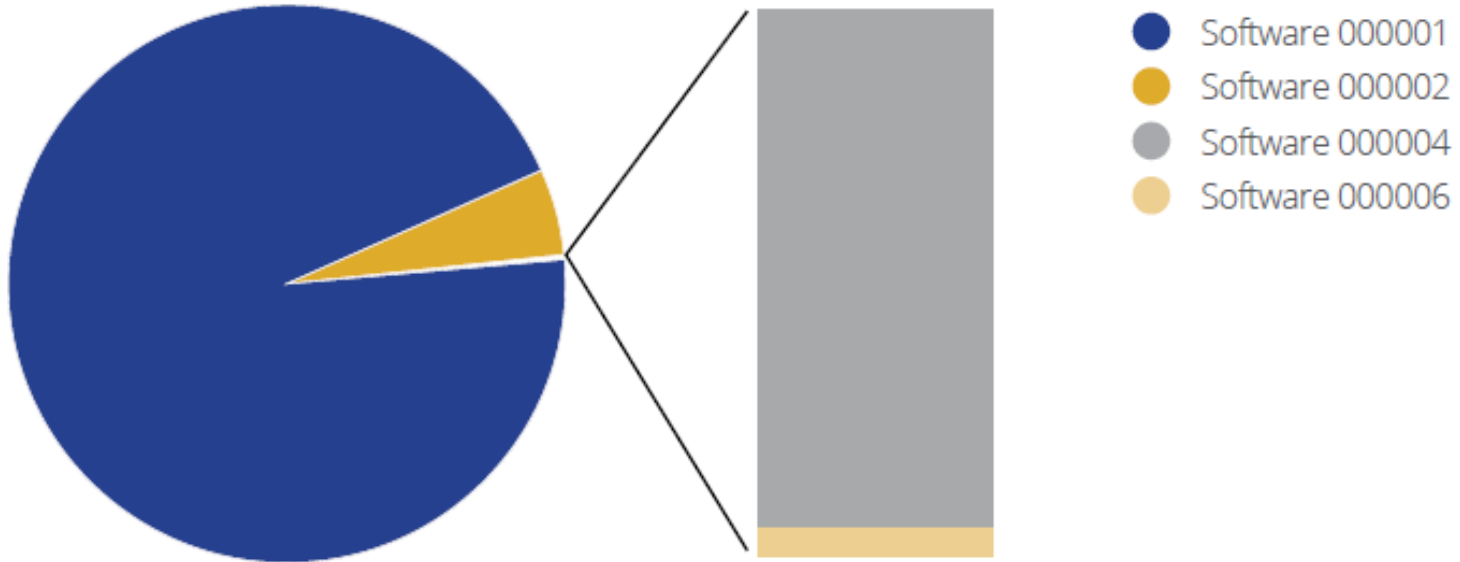
Main Product Category



Mainly Affected Brand



E-commerce Software Used



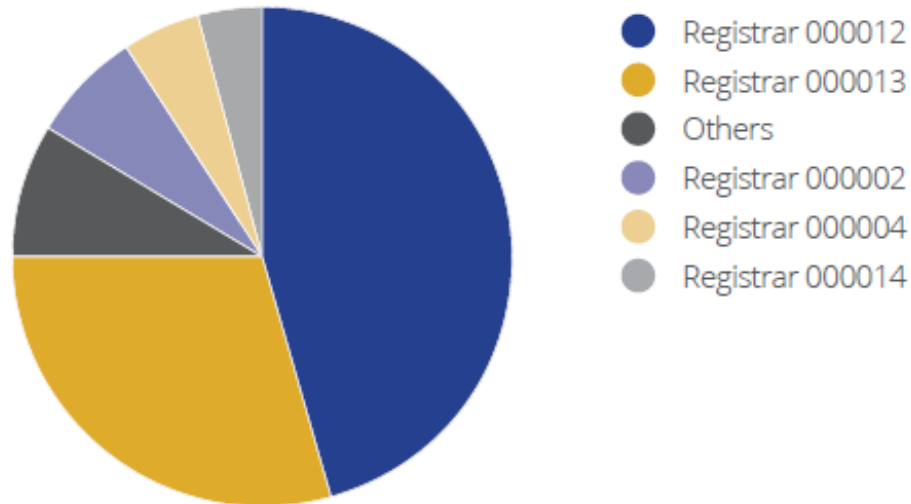


4. Domain name registrars⁹⁰

Of the domain names directing internet traffic to the suspected e-shops in Sweden and the United Kingdom, 7 555 were registered through Registrar 000012 (40.78 %). In total, 4 696 suspected e-shops (25.35 %) were registered through Registrar 000013.

Registrar

Only Sweden and UK

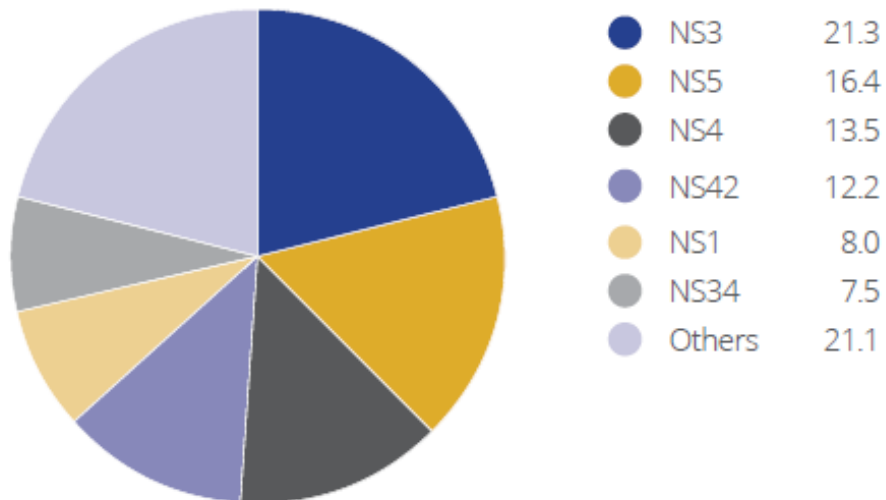




5. Name servers

Of the domain names directing internet traffic to the suspected e-shops, 21.3 % use NS 000003⁹¹ as a name server.

Name Servers



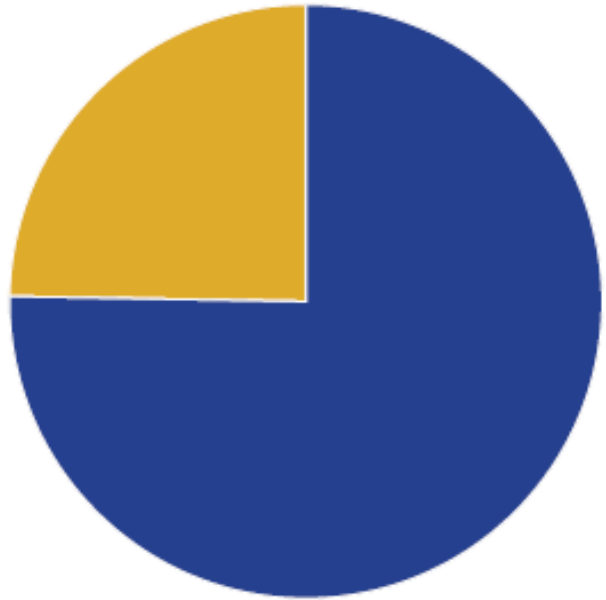


6. Country of hosting provider

The analysis has detected that the hosting provider of 25.9 % of the suspected e-shops is located in Turkey, and that the hosting provider for 19.3 % of the suspected e shops is in the Netherlands, while the hosting provider of 18.3 % of the suspected e shops is in the United States.





Previous Use



Minimum percentage



	Existed before	75.35%
	N/A	24.65%

8. Patterns detected in the case studies

The above patterns are clearly reflected in the case studies, for example⁹³:

- In the Domain009-se case study, the prior use of the domain name was to direct internet traffic to a Swedish language website for a famous Swedish poet and writer. The website is suspected of selling non-genuine branded shoes; the main brand affected is Brand 000002 and it had a total of 2 427 products for sale. The website is hosted in the Netherlands and it was re-registered in 2016. The name server used is NS 000034 and the software used is Software 000001.
- In the Domain008-de case study, the prior use of the domain name was to direct internet traffic to a German language website for an international motorcycle club in Regensburg, Germany. The website is suspected of selling non-genuine branded shoes and clothes; the main brand affected in Brand 000003 and it had a total of 4 051 products for sale. The website is hosted in Turkey and it was re-registered in 2016. The name server used is NS 000004 and the software used is Software 000001.

8. Patterns detected in the case studies

The above patterns are clearly reflected in the case studies, for example⁹³:

- In the Domain003-co-uk case study, the prior use of the domain name was to direct internet traffic to an English language website with information for the town of Buckingham, where local business owners could advertise and local news and activities could be listed for residents and visitors. The website is suspected of selling non-genuine branded shoes; the main brand affected in Brand 000002 and it had a total of 4 952 products for sale. The website is hosted in the United States and it was re-registered in 2016. The name server used is NS 000004 and the software used is Software 000001.
- In the Domain002-es case study, the prior use of the domain name was to direct internet traffic to a Spanish language website with information about a financial website, specifically offering loans to private individuals. The website is suspected of selling non-genuine branded shoes; the main brand affected is Brand 000002 and it had a total of 5 522 products for sale. The website is hosted in Turkey and it was re-registered in 2016. The name server used is NS 000003 and the software used is Software 000001.

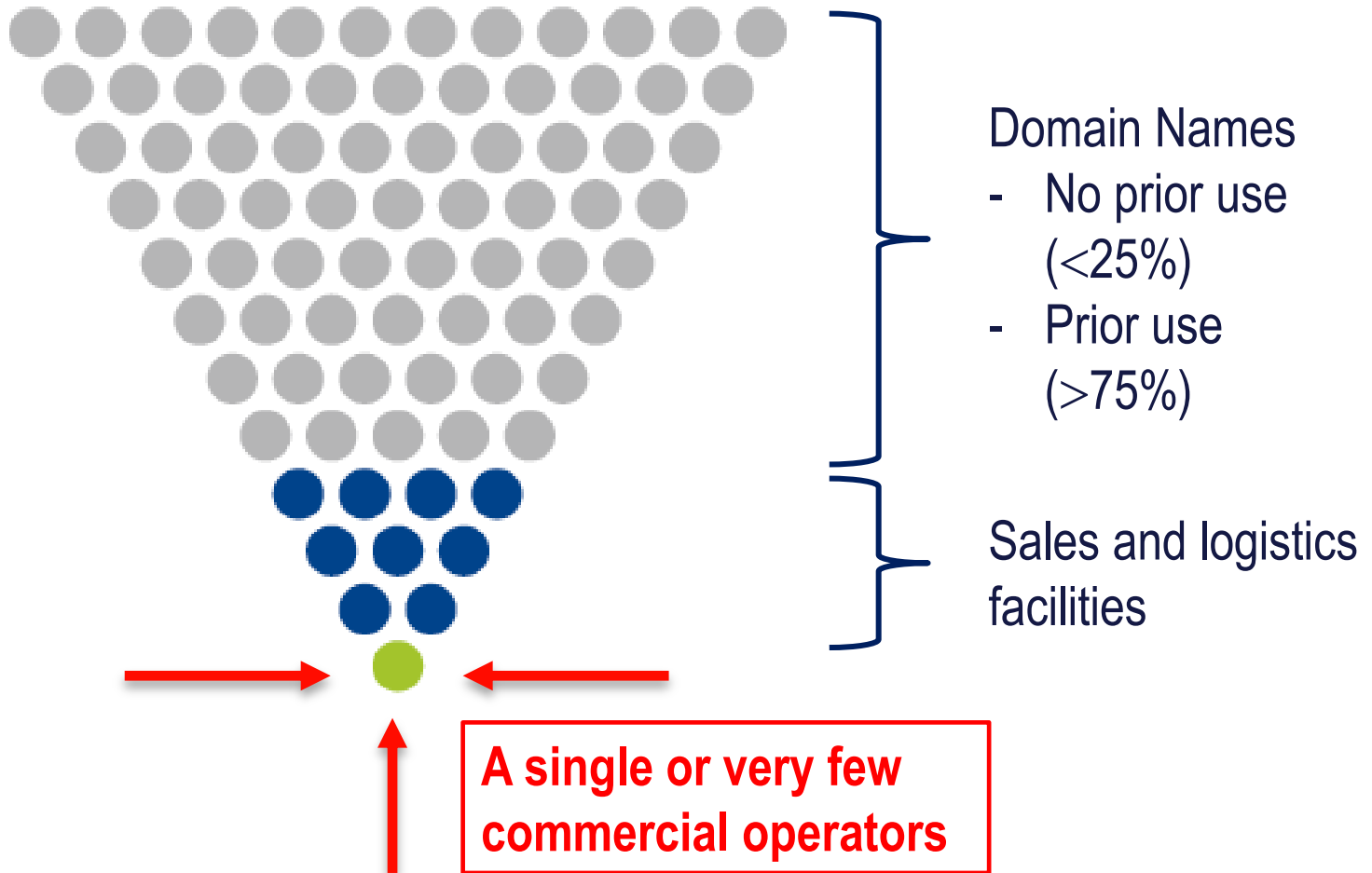
Conclusions

Conclusions

Conclusions

Conclusions

- The business model detected in Denmark is also used to market goods to consumers in Sweden, Germany, UK and Spain
- It is probably used in even more EU MS's, but that has not been researched
- The e-shops initially appear unrelated
- However various commonalities have been detected
- The commonalities indicate a single or very few commercial operators behind the activity





EUIPO
EUROPEAN UNION
INTELLECTUAL PROPERTY OFFICE

www.euipo.europa.eu



#oamitweets



youtube/oamitubes

Thank you

erling.vestergaard@ext.euipo.europa.eu