Compromised vs maliciously registered domain names

Maciej Korczyński

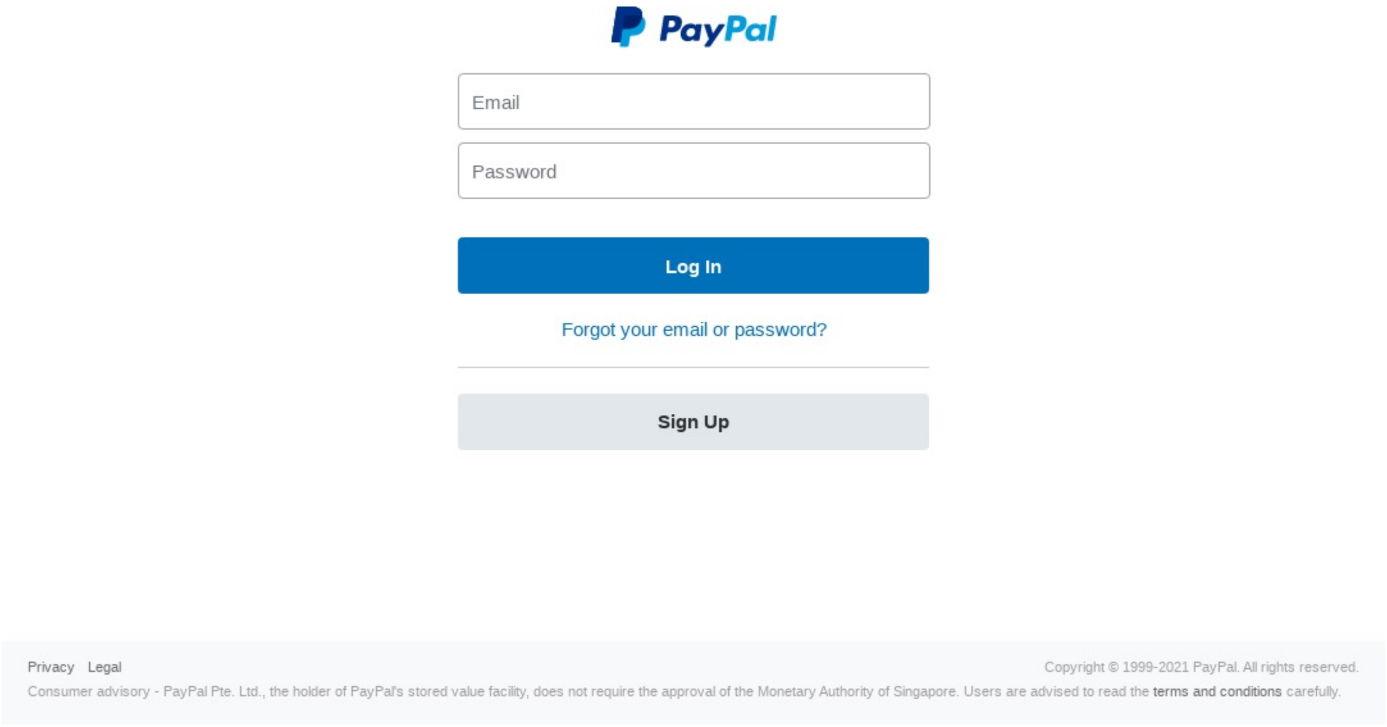
Grenoble Alps University

maciej.korczynski@univ-grenoble-alpes.fr

9 March 2022

Examples of common DNS abuse cases

https://user-paypal.oz4.top/LkQwxCf2/rfFDbZaPR9Ti/loiujYnPGh/ANWfgiB2vk8b/1



PayPal

Email

Password

Log In

Forgot your email or password?

Sign Up

Privacy Legal

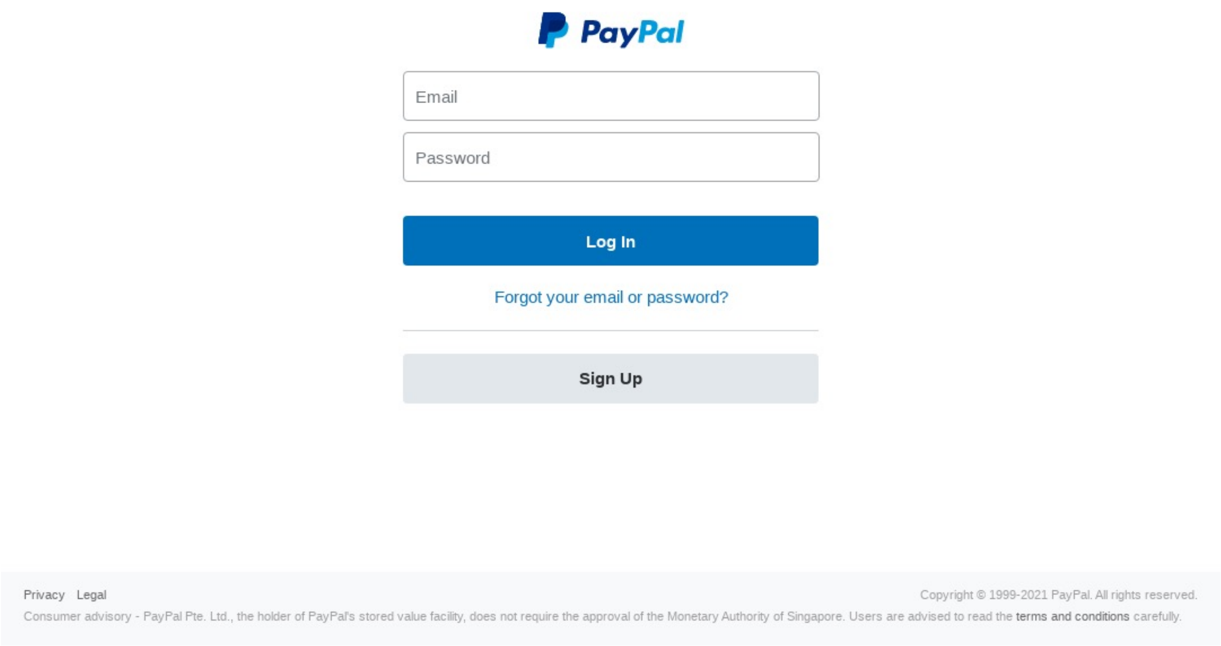
Copyright © 1999-2021 PayPal. All rights reserved.

Consumer advisory - PayPal Pte. Ltd., the holder of PayPal's stored value facility, does not require the approval of the Monetary Authority of Singapore. Users are advised to read the terms and conditions carefully.

Is the domain name maliciously registered?

Examples of common DNS abuse cases

https://user-paypal.oz4.top/LkQwxCf2/rfFDbZaPR9Ti/loiujYnPGh/ANWfgiB2vk8b/1

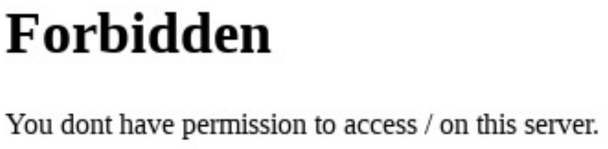


Privacy Legal

Copyright © 1999-2021 PayPal. All rights reserved.

Consumer advisory - PayPal Pte. Ltd., the holder of PayPal's stored value facility, does not require the approval of the Monetary Authority of Singapore. Users are advised to read the terms and conditions carefully.

http://oz4.top



Forbidden

You dont have permission to access / on this server.

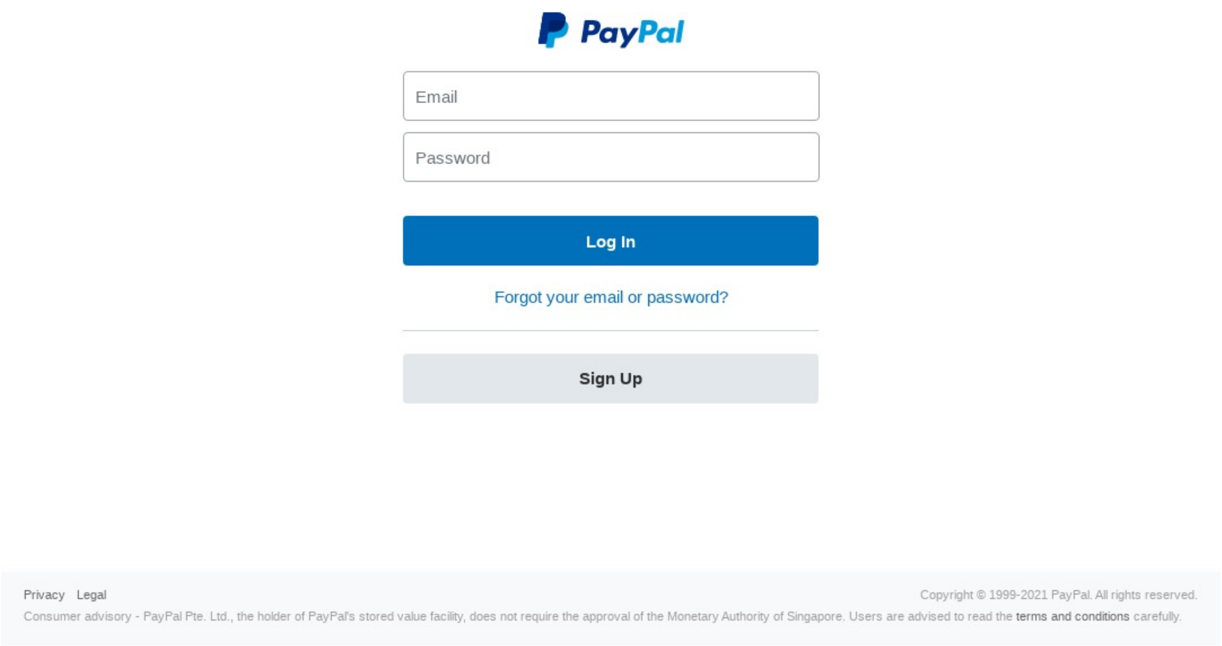
```
Submission Date: 2021-01-15 18:00:05

WHOIS:
Updated Date: 2021-01-13T15:32:36Z
Creation Date: 2021-01-13T15:26:54Z
```

Is the domain name maliciously registered?

Examples of common DNS abuse cases

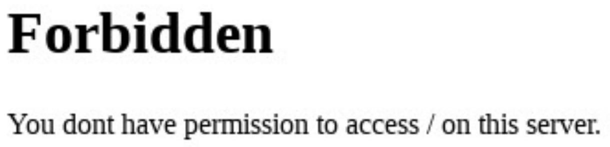
https://user-paypal.oz4.top/LkQwxCf2/rfFDbZaPR9Ti/loiujYnPGh/ANWfgiB2vk8b/1



Copyright © 1999-2021 PayPal. All rights reserved.

Consumer advisory - PayPal Pte. Ltd., the holder of PayPal's stored value facility, does not require the approval of the Monetary Authority of Singapore. Users are advised to read the terms and conditions carefully.

http://oz4.top



Forbidden

You dont have permission to access / on this server.

```
Submission Date: 2021-01-15 18:00:05

WHOIS:
Updated Date: 2021-01-13T15:32:36Z
Creation Date: 2021-01-13T15:26:54Z
```

Is the domain name maliciously registered?

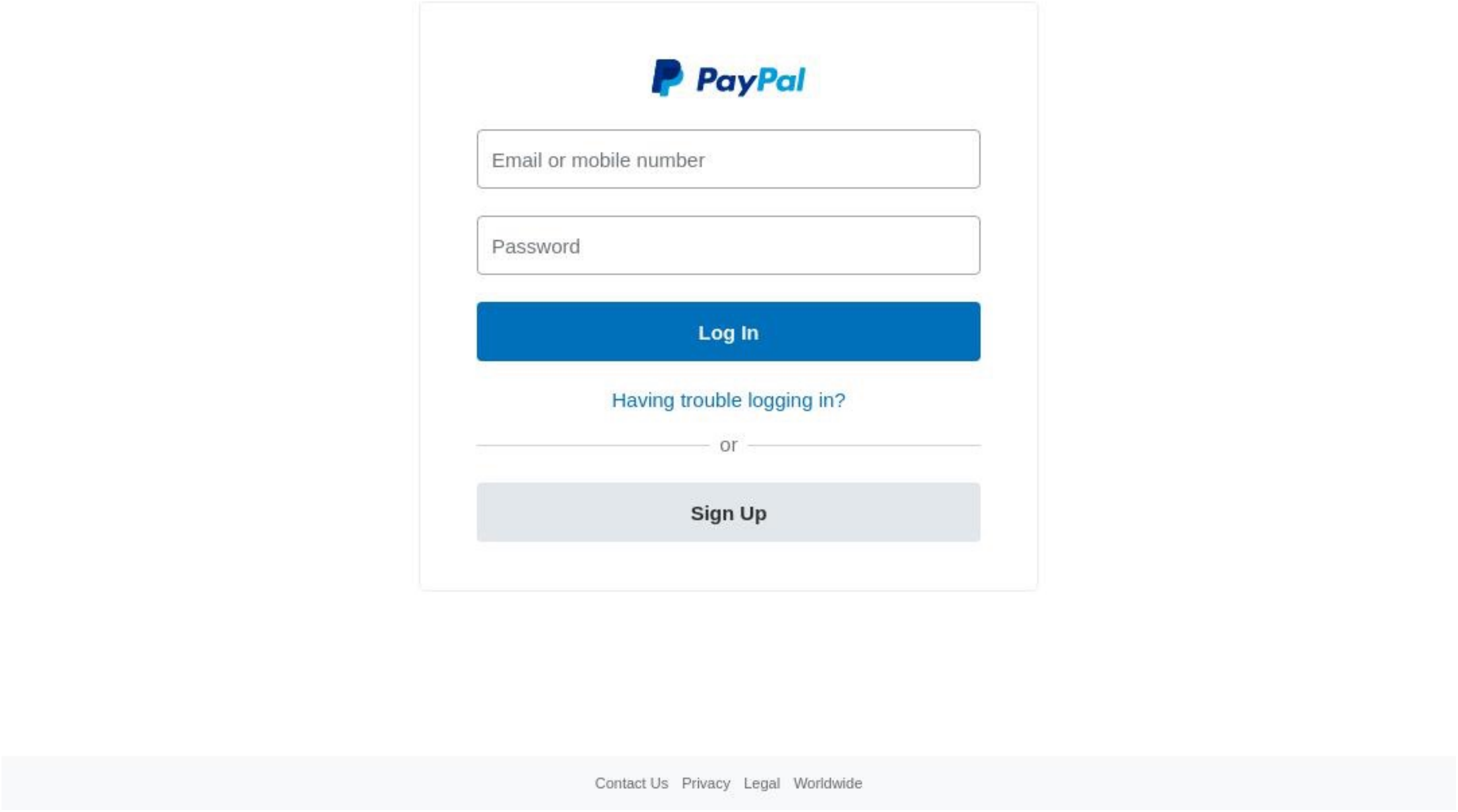
Maliciously registered domain name abused to serve illegal/abusive content: phishing of credentials and trademark infringement

What intermediary should mitigate abuse?
(from the technical perspective)

DNS service operator (registrar, registry)… and hosting provider!

Examples of common DNS abuse cases

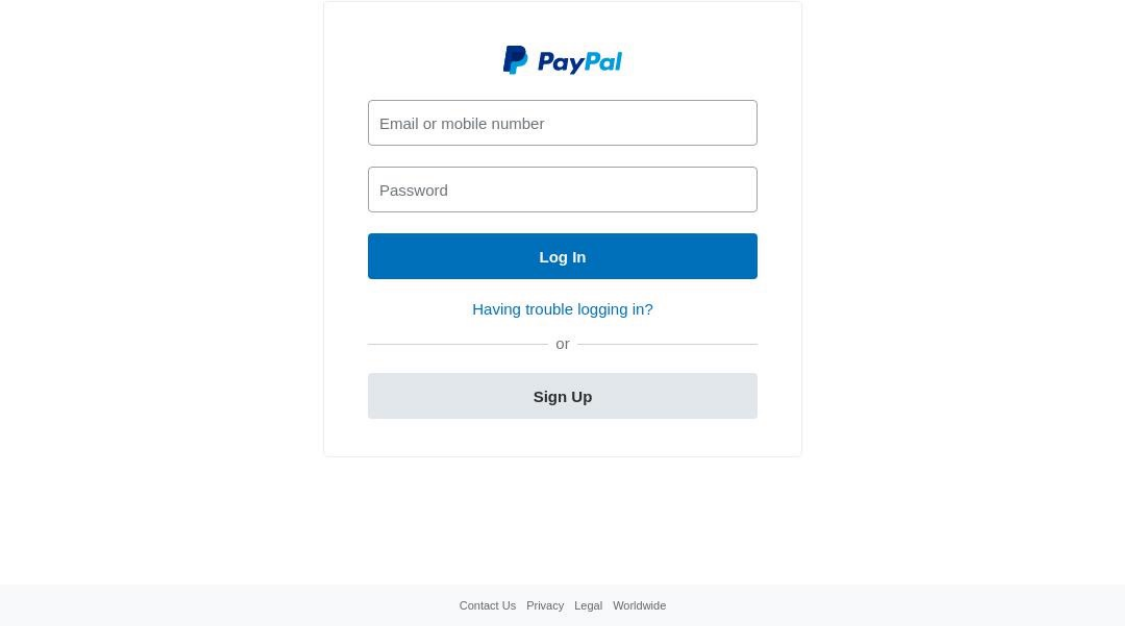
https://nutribiocorp.com/wp-includes/paypal/paypal/login/update.account-PayPal/account-has-been-limited/logins.html



Is the domain name maliciously registered?

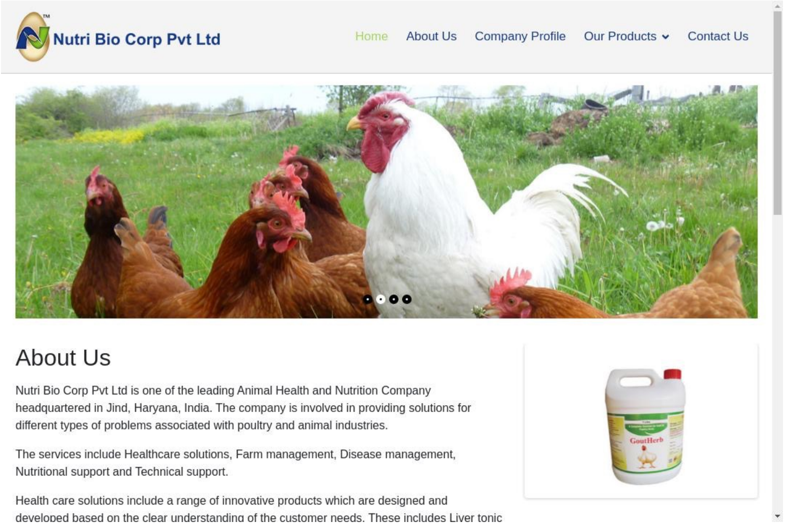
Examples of common DNS abuse cases

https://nutribiocorp.com/wp-includes/paypal/paypal/login/update.account-PayPal/account-has-been-limited/logins.html



PayPal
Email or mobile number
Password
Log In
Having trouble logging in?
or
Sign Up
Contact Us Privacy Legal Worldwide

https://nutribiocorp.com



About Us

Nutri Bio Corp Pvt Ltd is one of the leading Animal Health and Nutrition Company headquartered in Jind, Haryana, India. The company is involved in providing solutions for different types of problems associated with poultry and animal industries.

The services include Healthcare solutions, Farm management, Disease management, Nutritional support and Technical support.

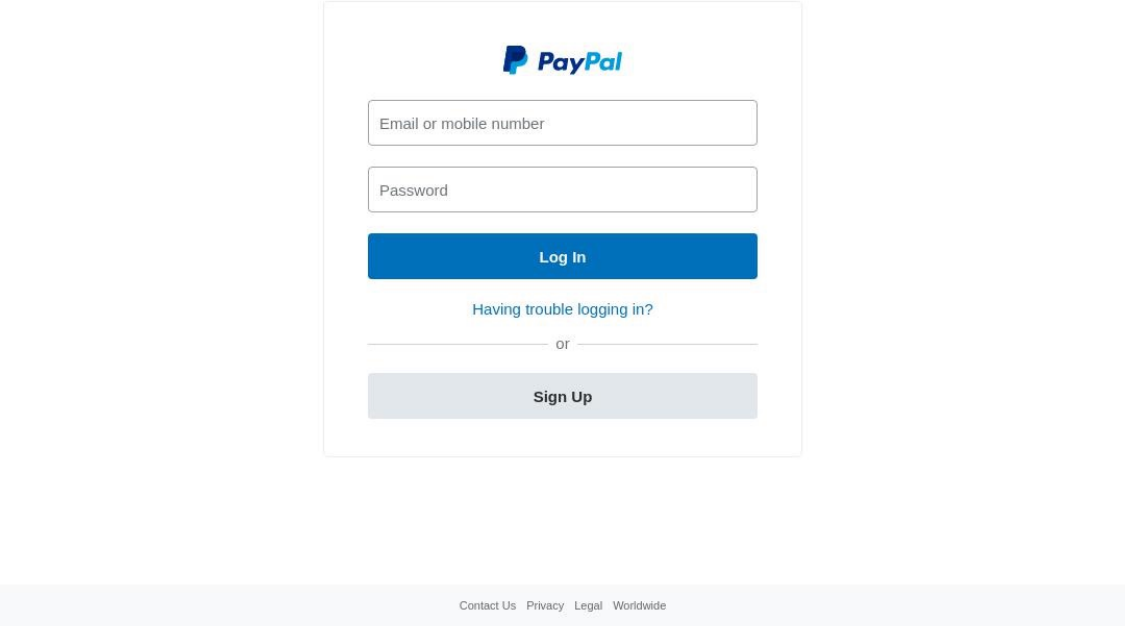
Health care solutions include a range of innovative products which are designed and developed based on the clear understanding of the customer needs. These includes Liver tonic

```
Creation Date: 2014-03-04T00:00:00Z
Registrar Registration Expiration Date:
2022-03-04T00:00:00Z
```

Is the domain name maliciously registered?

Examples of common DNS abuse cases

https://nutribiocorp.com/wp-includes/paypal/paypal/login/update.account-PayPal/account-has-been-limited/logins.html



PayPal

Email or mobile number

Password

Log In

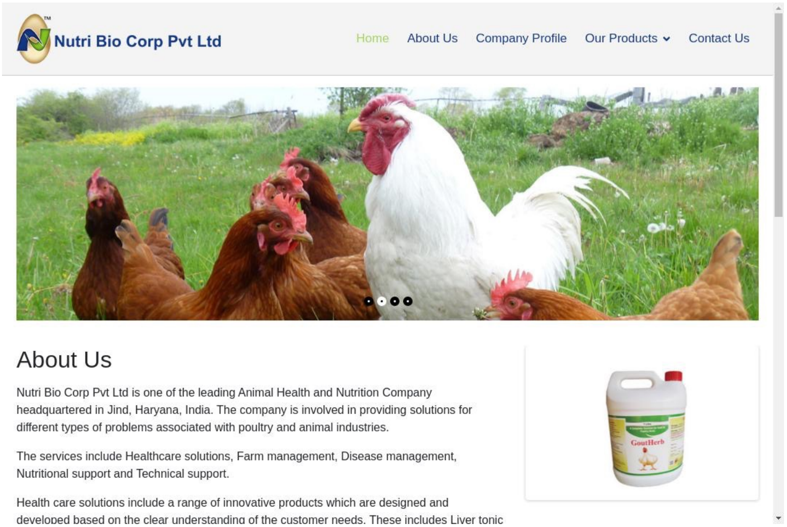
Having trouble logging in?

or

Sign Up

Contact Us Privacy Legal Worldwide

https://nutribiocorp.com



Nutri Bio Corp Pvt Ltd

Home About Us Company Profile Our Products Contact Us

About Us

Nutri Bio Corp Pvt Ltd is one of the leading Animal Health and Nutrition Company headquartered in Jind, Haryana, India. The company is involved in providing solutions for different types of problems associated with poultry and animal industries.

The services include Healthcare solutions, Farm management, Disease management, Nutritional support and Technical support.

Health care solutions include a range of innovative products which are designed and developed based on the clear understanding of the customer needs. These includes Liver tonic

```
Creation Date: 2014-03-04T00:00:00Z
Registrar Registration Expiration Date:
2022-03-04T00:00:00Z
```

Is the domain name maliciously registered?

Legitimate domain name but compromised website abused to serve illegal/abusive content: phishing of credentials and trademark infringement

What intermediary should mitigate abuse?
(from the technical perspective)

~~DNS service operator (registrar, registry)~~ hosting provider and the owner/administrator!

How legitimate domains are abused?

- Mainly at the website level (vulnerable software, e.g., content management systems), sometimes at the DNS level (e.g., domain shadowing)

Existing approaches

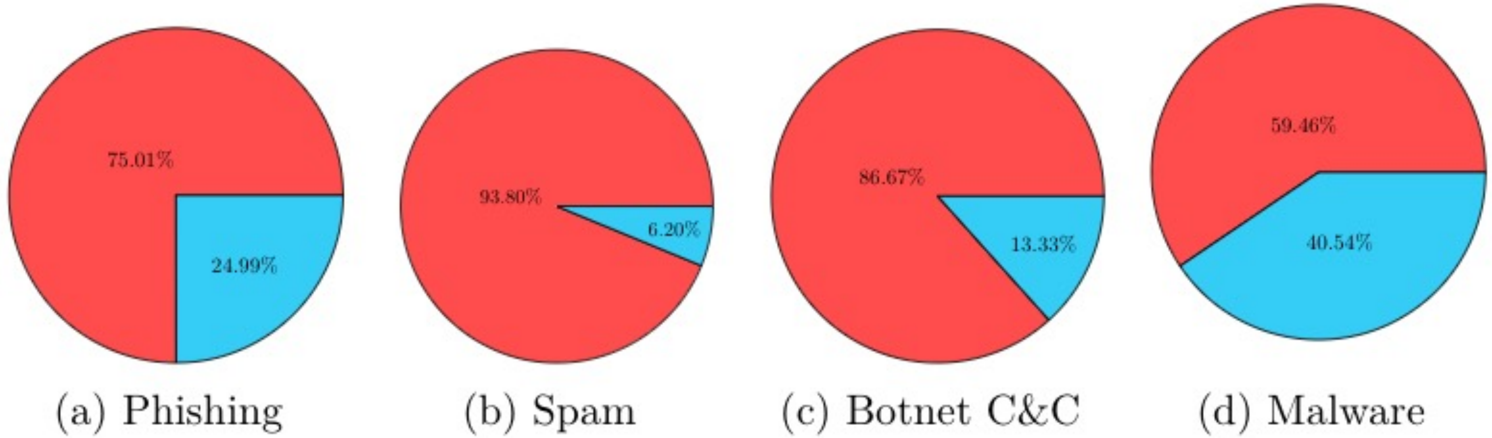
Existing approaches to distinguish compromised (legitimate) from maliciously registered domain names

- **Based on heuristics (used in industry reports)**
  - Domain name age (time between registration and blacklisting)
  - Registration in bulk
  - Patterns in registered domain names (e.g., brand names or misspelled version of the targeted service such as “paypal”)

- **Machine-learning approaches**
  - COMAR (Classification of COmpromised versus Maliciously Registered domains)*
  - Based on 38 characteristics (features)
  - Fully automated approach
  - 97% accuracy

* Developed at Grenoble Alps University, co-funded by AFNIC and SIDN

Relationship between the type of abuse and compromised vs. malicious?

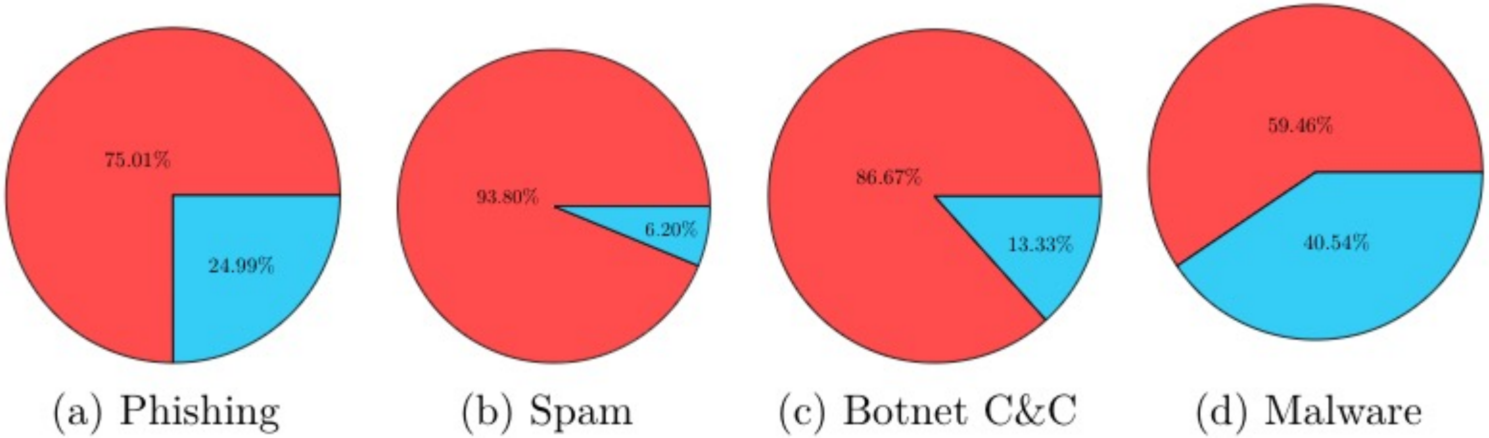


(a) Phishing (b) Spam (c) Botnet C&C (d) Malware

Figure 6: Distribution of compromised (blue) and maliciously registered (red) domain names per abuse type.

* Results from the 2nd quarter of 2021 based on the Technical Report of the EC DNS abuse study

Relationship between the type of abuse and compromised vs. malicious?

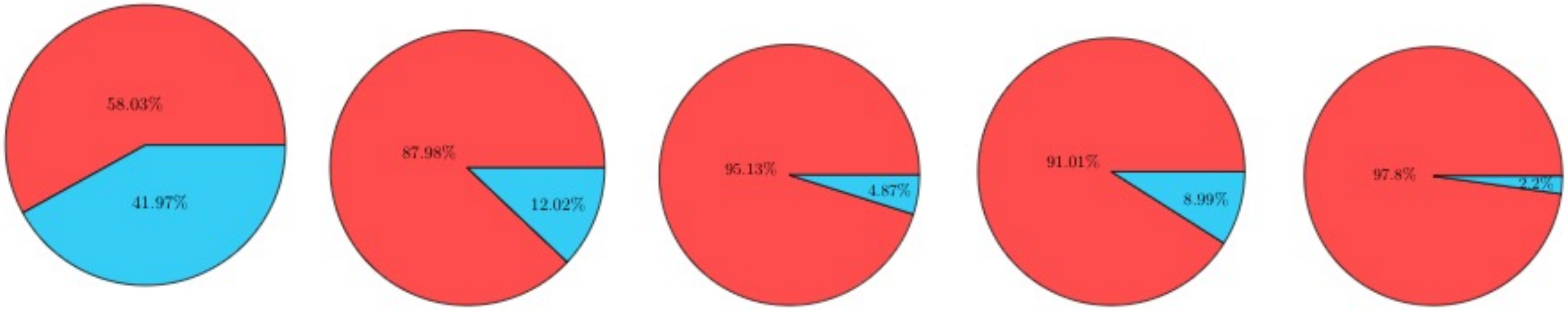


(a) Phishing (b) Spam (c) Botnet C&C (d) Malware

Figure 6: Distribution of compromised (blue) and maliciously registered (red) domain names per abuse type.

- The vast majority of spam and botnet command-and-control domain names are maliciously registered.
- About 25% of phishing domain names and 41% of malware distribution domain names are presumably registered by legitimate users, but compromised at the hosting level.

Variation across different TLD types

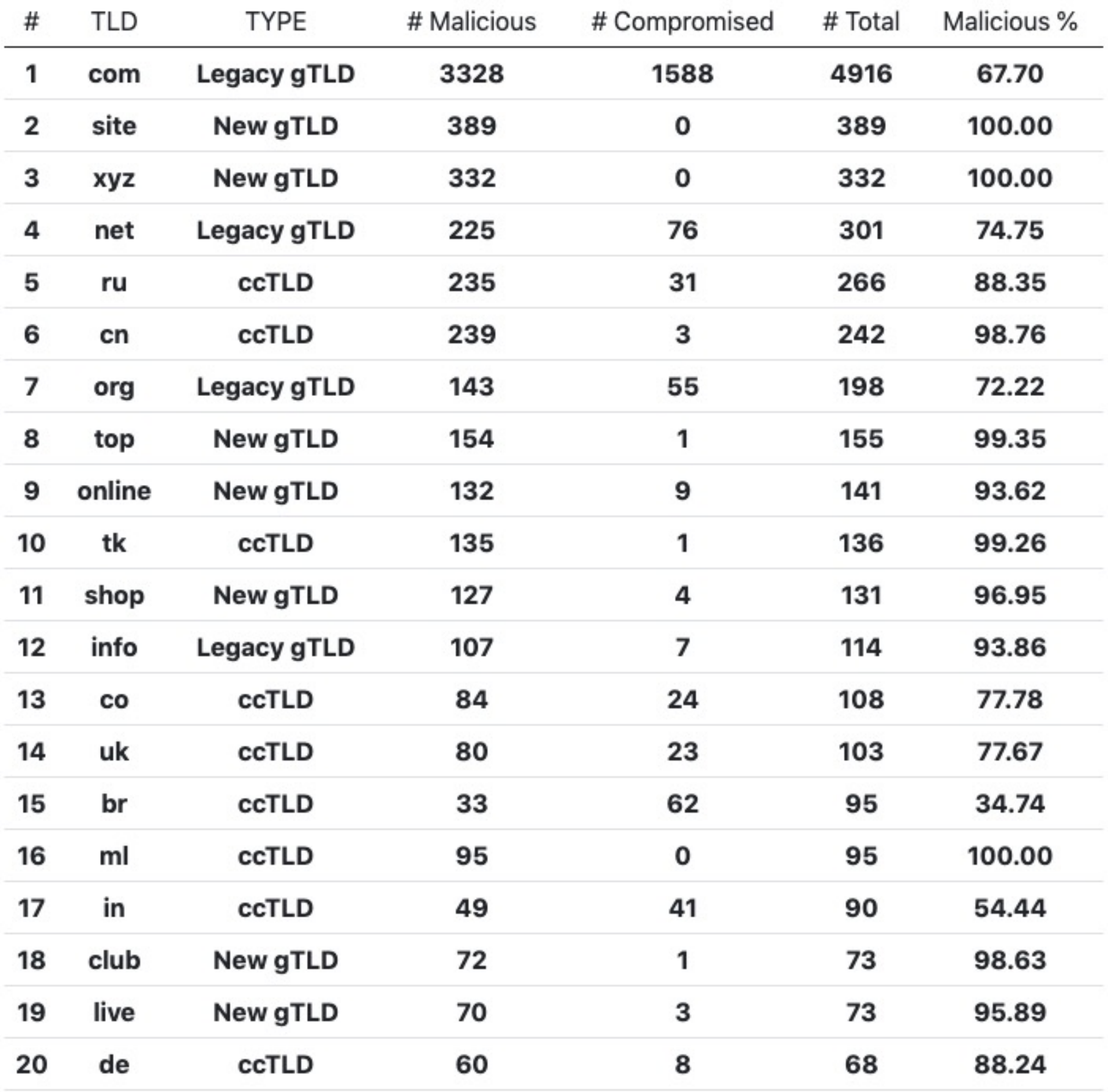


(a) EU ccTLDs (b) European ccTLDs (c) other ccTLDs (d) legacy gTLDs (e) new gTLDs

Figure 7: Distribution of compromised (blue) and maliciously registered (red) domain names per TLD type.

* Results from the 2nd quarter of 2021 based on the Technical Report of the EC DNS abuse study

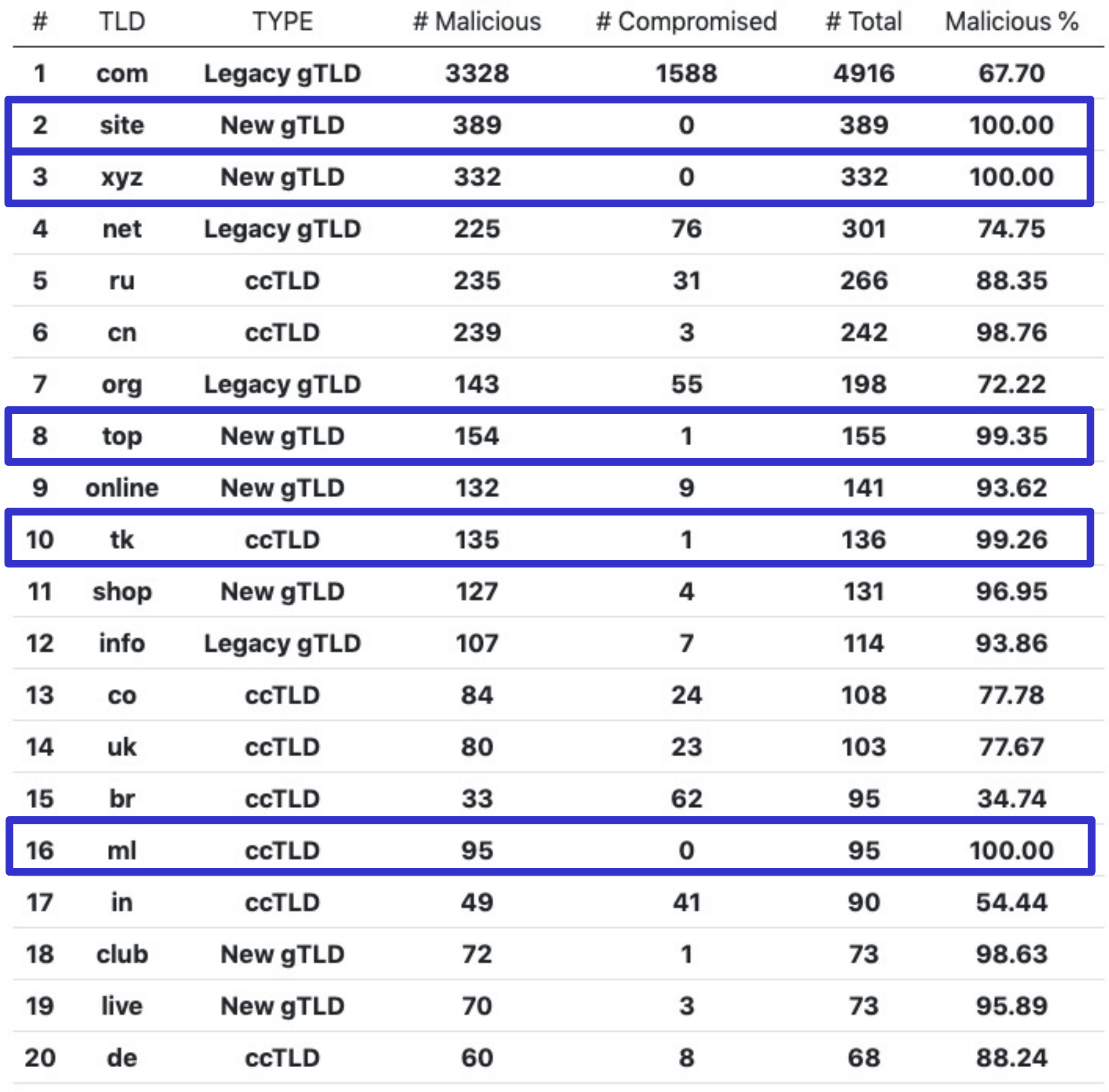
Variation across different TLDs



#	TLD	TYPE	# Malicious	# Compromised	# Total	Malicious %
1	com	Legacy gTLD	3328	1588	4916	67.70
2	site	New gTLD	389	0	389	100.00
3	xyz	New gTLD	332	0	332	100.00
4	net	Legacy gTLD	225	76	301	74.75
5	ru	ccTLD	235	31	266	88.35
6	cn	ccTLD	239	3	242	98.76
7	org	Legacy gTLD	143	55	198	72.22
8	top	New gTLD	154	1	155	99.35
9	online	New gTLD	132	9	141	93.62
10	tk	ccTLD	135	1	136	99.26
11	shop	New gTLD	127	4	131	96.95
12	info	Legacy gTLD	107	7	114	93.86
13	co	ccTLD	84	24	108	77.78
14	uk	ccTLD	80	23	103	77.67
15	br	ccTLD	33	62	95	34.74
16	ml	ccTLD	95	0	95	100.00
17	in	ccTLD	49	41	90	54.44
18	club	New gTLD	72	1	73	98.63
19	live	New gTLD	70	3	73	95.89
20	de	ccTLD	60	8	68	88.24

* Results from May 2021 based on the results from the COMAR project

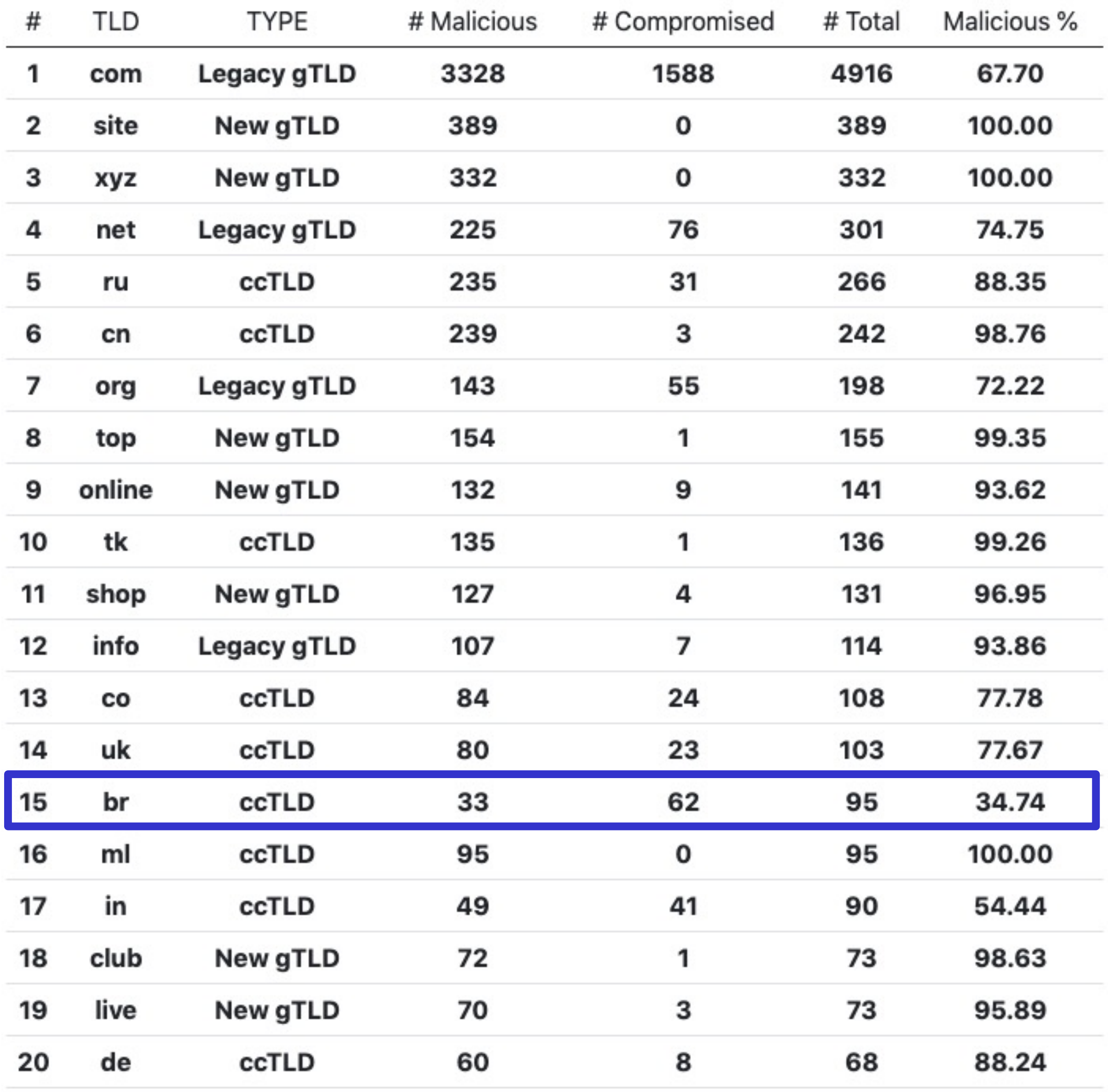
Variation across different TLDs



#	TLD	TYPE	# Malicious	# Compromised	# Total	Malicious %
1	com	Legacy gTLD	3328	1588	4916	67.70
2	site	New gTLD	389	0	389	100.00
3	xyz	New gTLD	332	0	332	100.00
4	net	Legacy gTLD	225	76	301	74.75
5	ru	ccTLD	235	31	266	88.35
6	cn	ccTLD	239	3	242	98.76
7	org	Legacy gTLD	143	55	198	72.22
8	top	New gTLD	154	1	155	99.35
9	online	New gTLD	132	9	141	93.62
10	tk	ccTLD	135	1	136	99.26
11	shop	New gTLD	127	4	131	96.95
12	info	Legacy gTLD	107	7	114	93.86
13	co	ccTLD	84	24	108	77.78
14	uk	ccTLD	80	23	103	77.67
15	br	ccTLD	33	62	95	34.74
16	ml	ccTLD	95	0	95	100.00
17	in	ccTLD	49	41	90	54.44
18	club	New gTLD	72	1	73	98.63
19	live	New gTLD	70	3	73	95.89
20	de	ccTLD	60	8	68	88.24

* Results from May 2021 based on the results from the COMAR project

Variation across different TLDs



#	TLD	TYPE	# Malicious	# Compromised	# Total	Malicious %
1	com	Legacy gTLD	3328	1588	4916	67.70
2	site	New gTLD	389	0	389	100.00
3	xyz	New gTLD	332	0	332	100.00
4	net	Legacy gTLD	225	76	301	74.75
5	ru	ccTLD	235	31	266	88.35
6	cn	ccTLD	239	3	242	98.76
7	org	Legacy gTLD	143	55	198	72.22
8	top	New gTLD	154	1	155	99.35
9	online	New gTLD	132	9	141	93.62
10	tk	ccTLD	135	1	136	99.26
11	shop	New gTLD	127	4	131	96.95
12	info	Legacy gTLD	107	7	114	93.86
13	co	ccTLD	84	24	108	77.78
14	uk	ccTLD	80	23	103	77.67
15	br	ccTLD	33	62	95	34.74
16	ml	ccTLD	95	0	95	100.00
17	in	ccTLD	49	41	90	54.44
18	club	New gTLD	72	1	73	98.63
19	live	New gTLD	70	3	73	95.89
20	de	ccTLD	60	8	68	88.24

* Results from May 2021 based on the results from the COMAR project

Thank you!

maciej.korczynski@univ-grenoble-alpes.fr

Acknowledgements

The presented results are based on the COMAR project co-funded by AFNIC and SIDN (registry operators of .fr and .nl domain names), and the study on DNS abuse commissioned by the European Commission.

Number and percentage of actionable report broken down per TLD (source: eco Complaints Office)

TLD	Amount TLD	Percentage
.com	1909	35%
.club	572	11%
.ml	450	8%
.ru	295	5%
.cf	268	5%
.ga	214	4%
.net	179	3%
.al	174	3%
.org	121	2%
.top	107	2%
.click	99	2%
.gq	86	2%
.xyz	82	2%
.pro	66	1%
.download	47	1%
.ph	47	1%
.pw	47	1%
.buzz	43	1%
.de	43	1%
.to	40	1%
.cc	34	1%
.info	34	1%
.eu	31	1%
.fun	30	1%
.uno	30	1%
.tk	28	1%

The Complaints Office of **eco – Association of the Internet Industry** is the German hotline of INHOPE and handles complaints related to the illegal Internet content (e.g., CSAM)