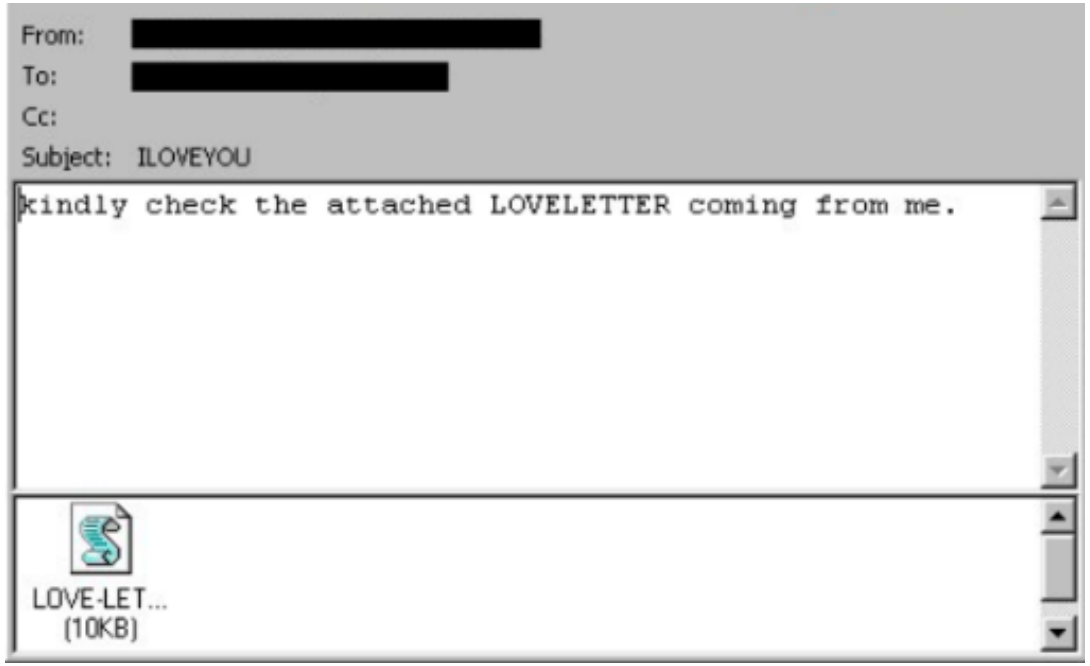
Cīņa pret ļaunprātīgu DNS izmantošanu. Kāds ir rezultāts?

Katrīna Sataki

NIC.LV

2024. gada 12. septembrī

ESET Drošības konference


From:
To:
Cc:
Subject: ILOVEYOU
kindly check the attached LOVELETTER coming from me.
LOVE-LET...
(10KB)

Daudzi nikni lietotāji
(ieskaitot mani)

IPS

Policija

Internets

x2

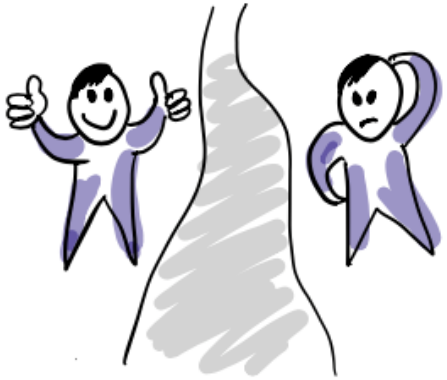
Ļaundari

?

Valsts

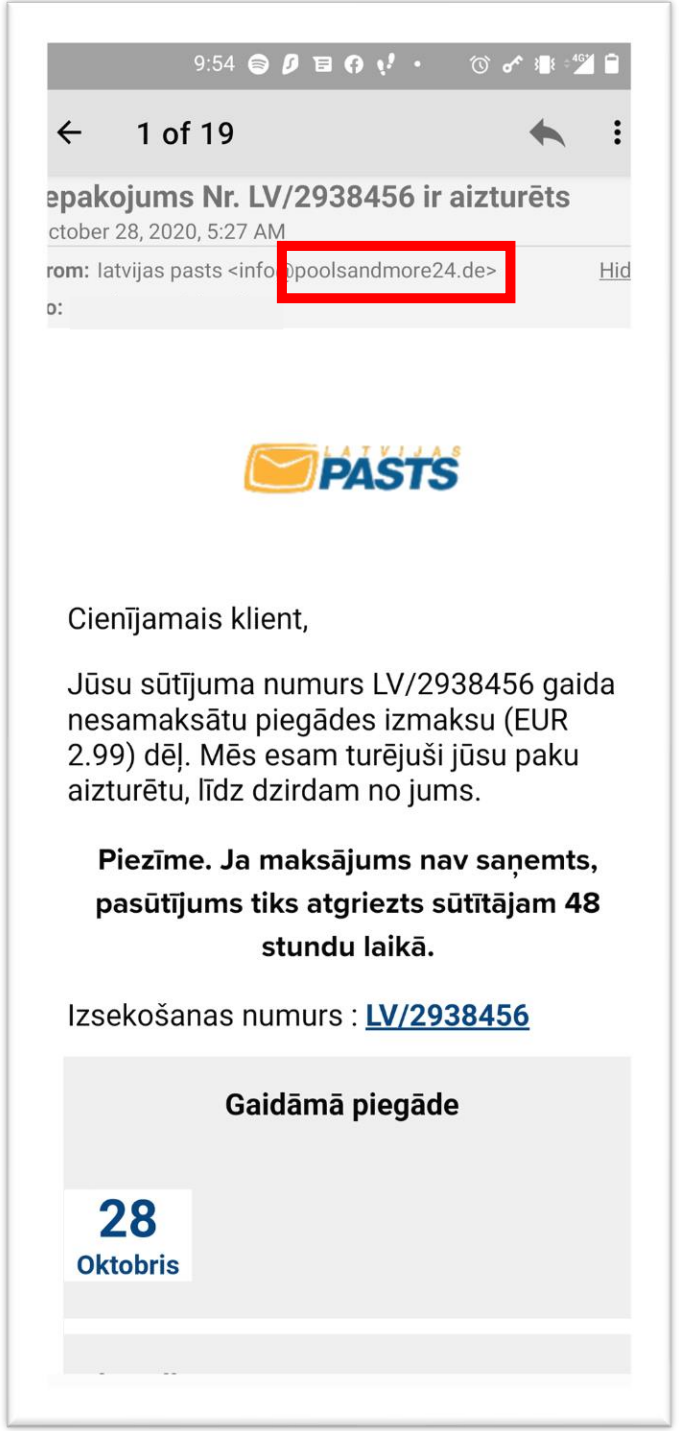
Mūžu dzīvo - mūžu mācies

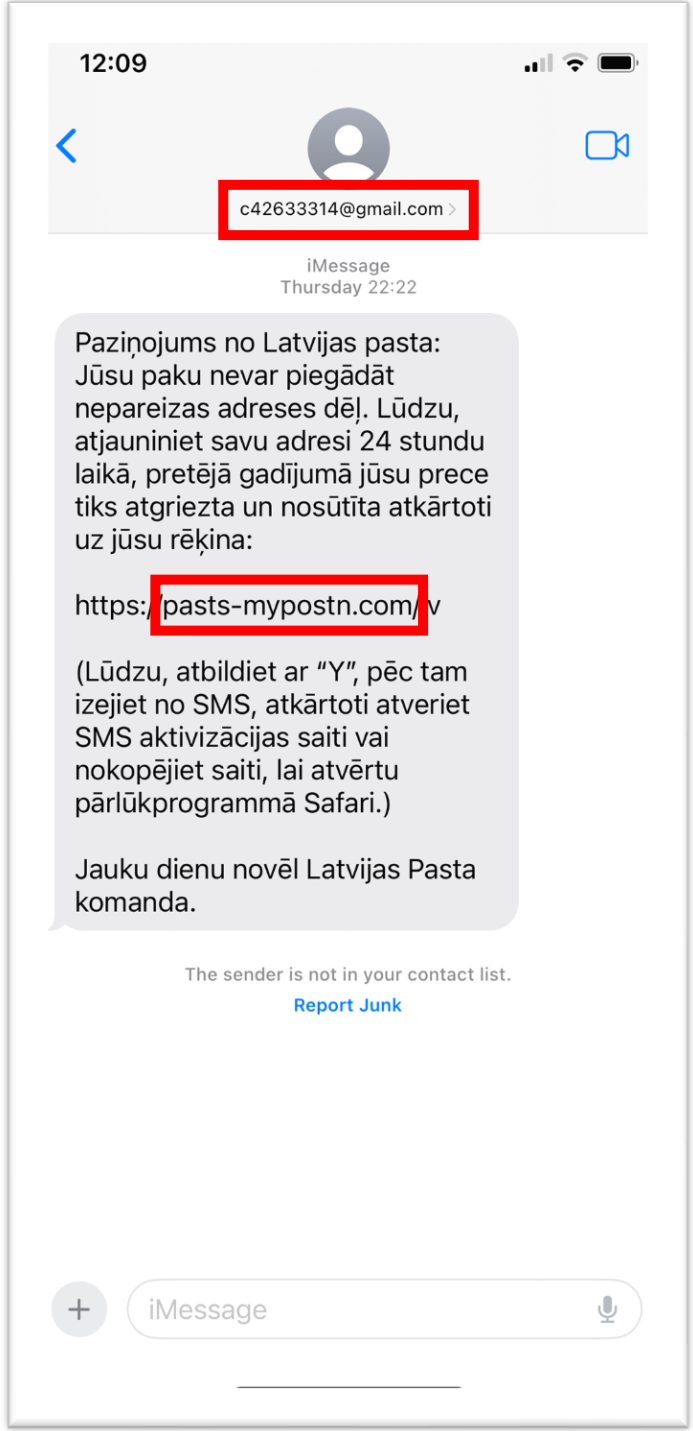
Neklikšķini, kur nevajag



Ne viss ir zelts, kas spīd

Cerība - muļķa mierinājums


9:54
1 of 19
epakojums Nr. LV/2938456 ir aizturēts
ctober 28, 2020, 5:27 AM
rom: latvijas pasts <info@poolsandmore24.de>
Hid
o:
LATVIJAS PASTS
Cienījamais klient,
Jūsu sūtījuma numurs LV/2938456 gaida nesamaksātu piegādes izmaksu (EUR 2.99) dēļ. Mēs esam turējuši jūsu paku aizturētu, līdz dzirdam no jums.
Piezīme. Ja maksājums nav saņemts, pasūtījums tiks atgriezts sūtītājam 48 stundu laikā.
Izsekošanas numurs : LV/2938456
Gaidāmā piegāde
28
Oktobris


12:09
c42633314@gmail.com
iMessage
Thursday 22:22
Paziņojums no Latvijas pasta: Jūsu paku nevar piegādāt nepareizas adreses dēļ. Lūdzu, atjauniniet savu adresi 24 stundu laikā, pretējā gadījumā jūsu prece tiks atgriezta un nosūtīta atkārtoti uz jūsu rēķina:
https://pasts-mypostn.com/v
(Lūdzu, atbildiet ar "Y", pēc tam izejiet no SMS, atkārtoti atveriet SMS aktivizācijas saiti vai nokopējiet saiti, lai atvērtu pārlūkprogrammā Safari.)
Jauku dienu novēl Latvijas Pasta komanda.
The sender is not in your contact list.
Report Junk
iMessage

Kas ir ļaunprātīga DNS izmantošana?

- ļaunatūra, **8%**
- robottīkli,
- pikšķerēšana, **46%**

? • domēnsagroze (*pharming*) un

- mēstules (*spam*), ja tās kalpo kā mehānisms citu ļaunprātīgas DNS izmantošanas veidu izplatīšanai. **44%**

Avots: iQ Global

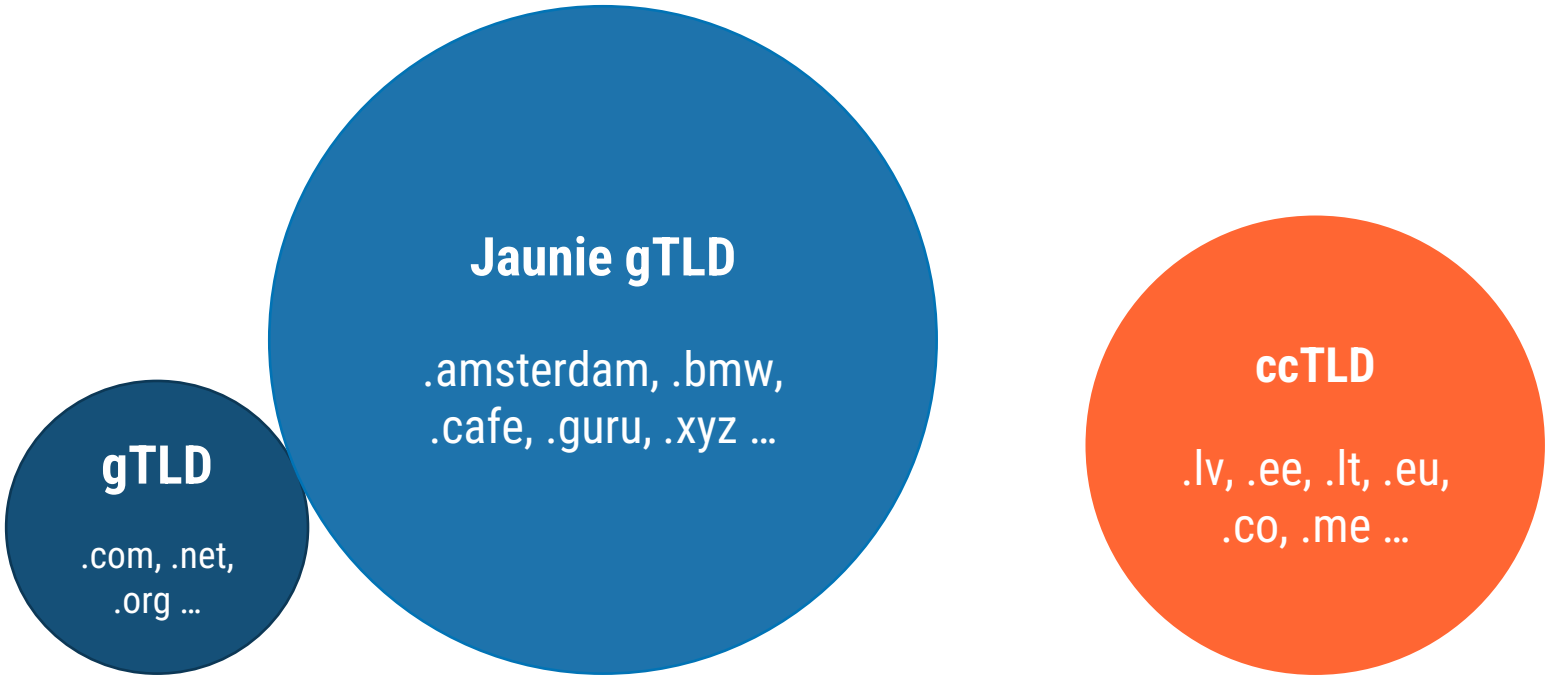
1. Ļaunprātīgi reģistrēti domēna vārdi

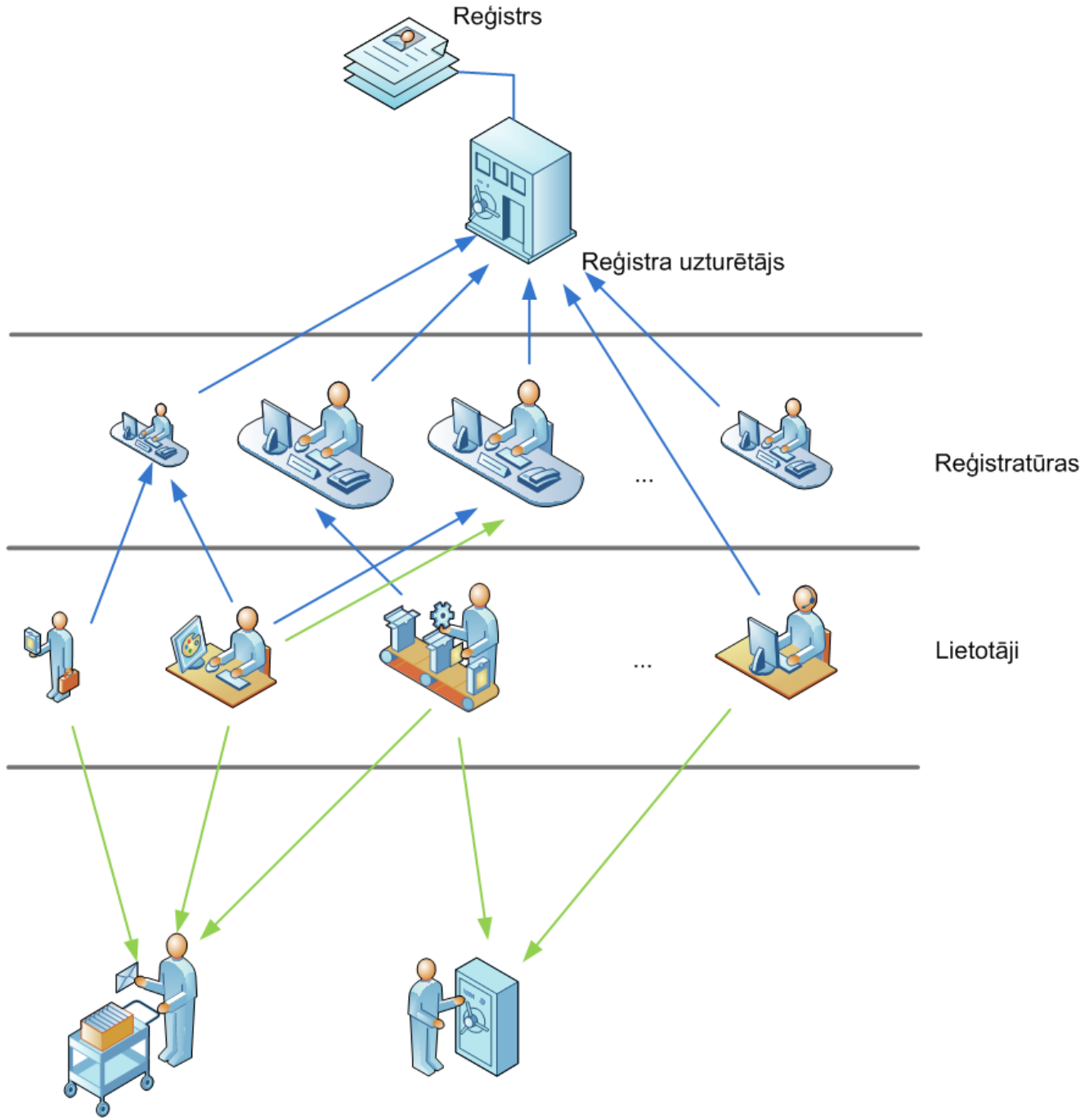
2. Kompromitēti domēna vārdi

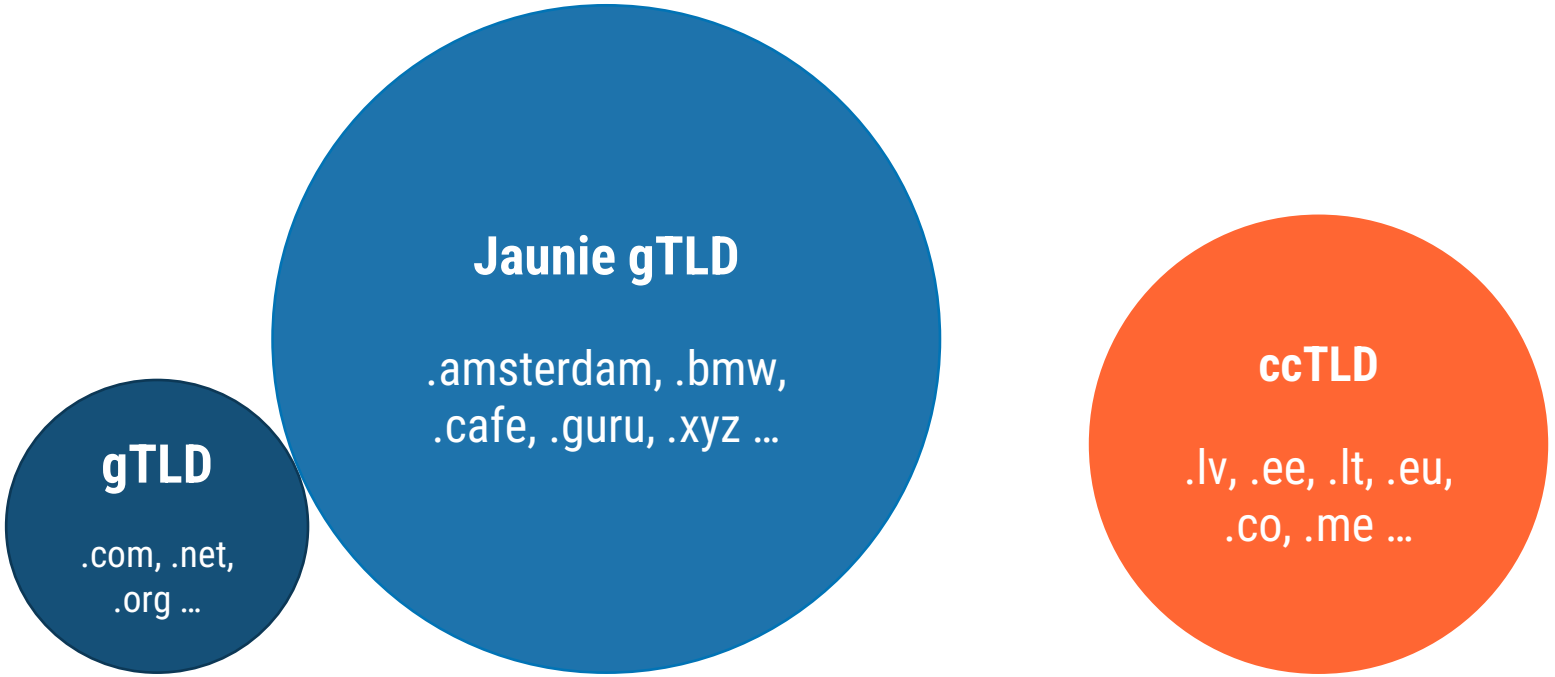
Avots: Study on Domain Name System (DNS) abuse

Augstākā līmeņa domēni (ALD)

Top-Level Domains (TLD)




Reģistrs
Reģistra uzturētājs
Reģistratūras
Lietotāji
...
...

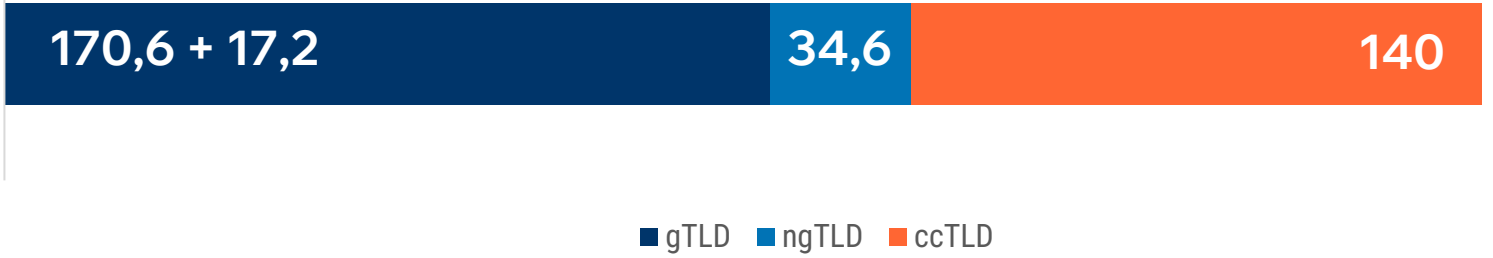


ICANN akreditētās reģistratūras

Tālākpārdevēji

Citas reģistratūras

Kopējais domēna vārdu skaits: **362,4 miljoni**



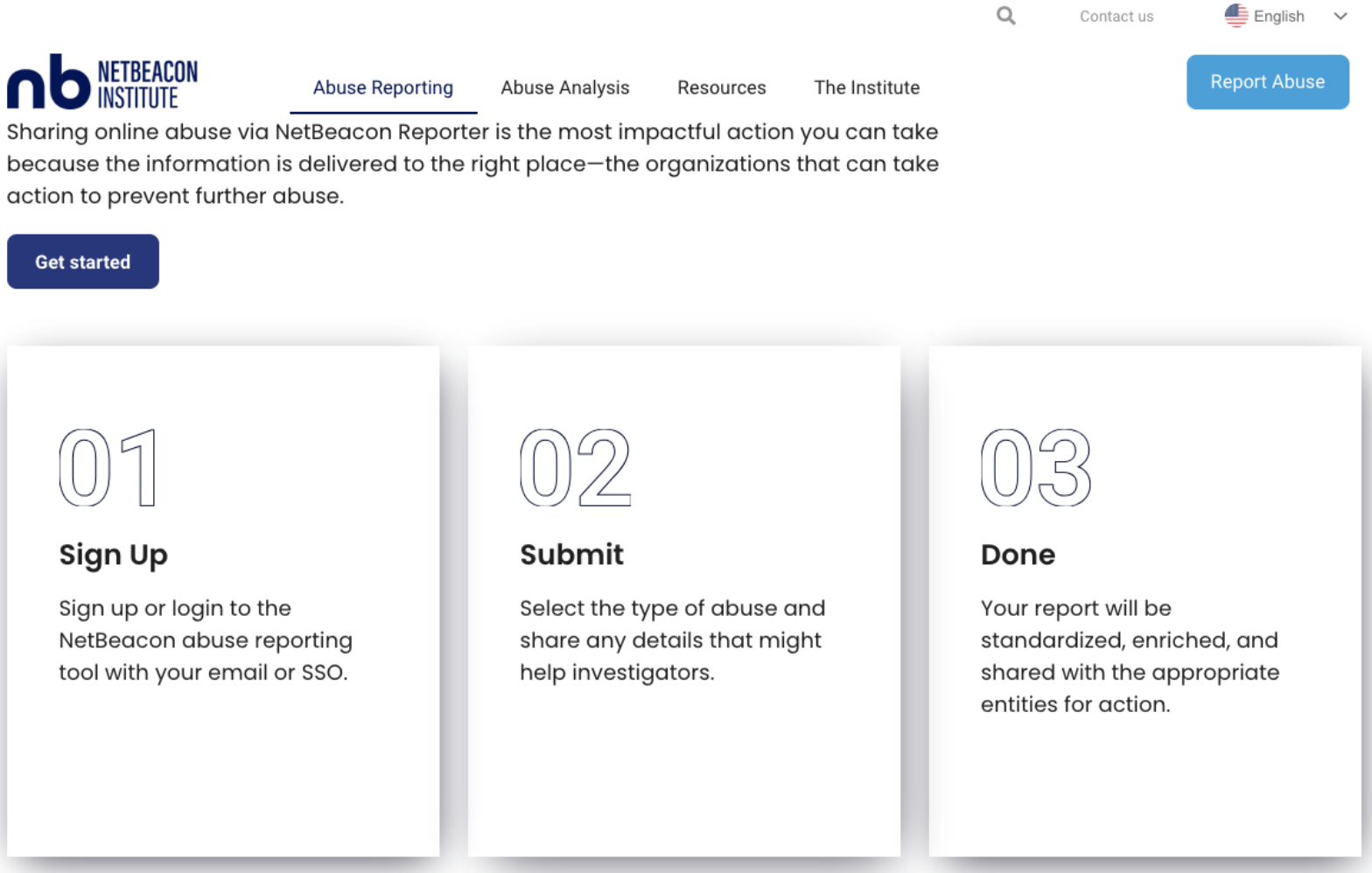
Avots: Verisign DNIB

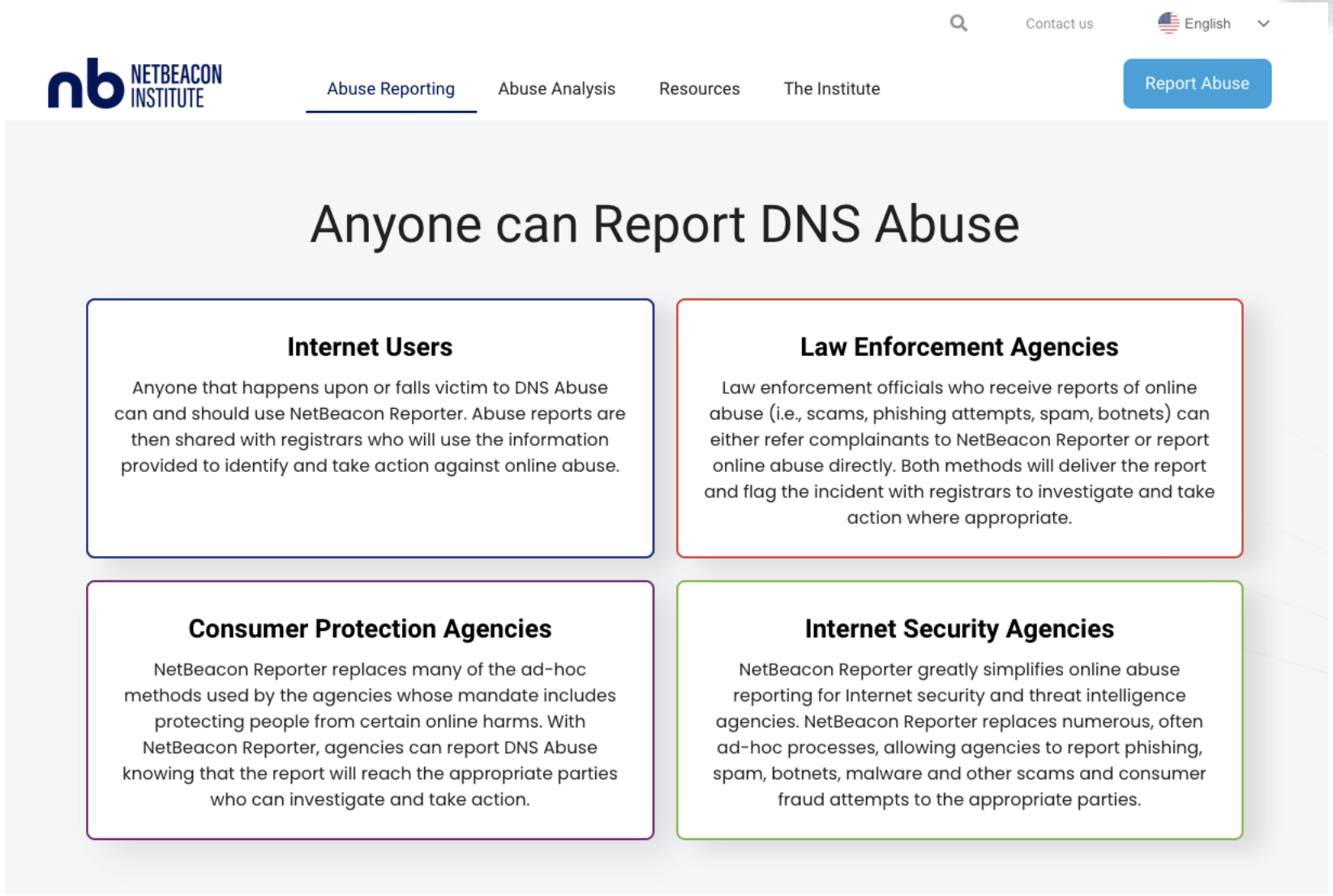
1 no **368** domēna vārdiem

Avots: iQ Global

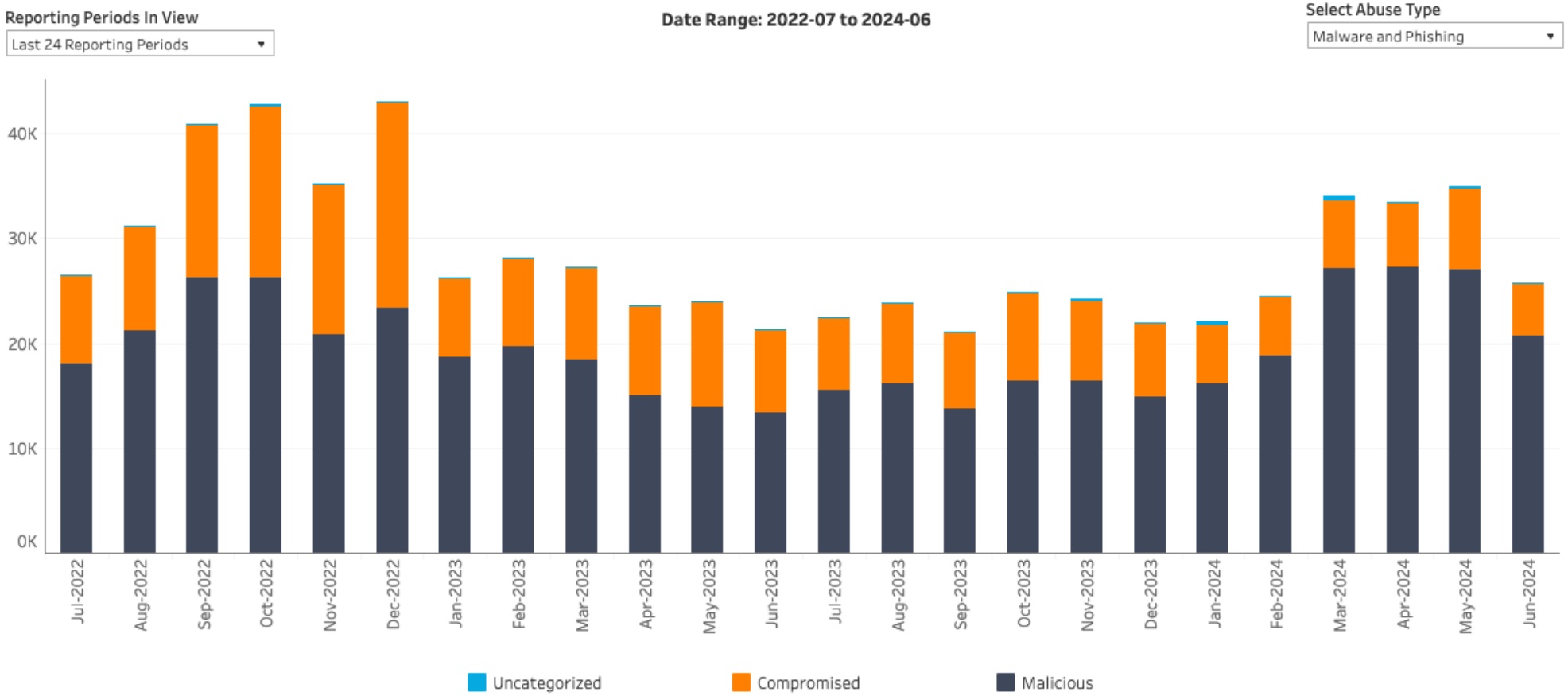
cert@cert.lv

https://netbeacon.org/reporting/

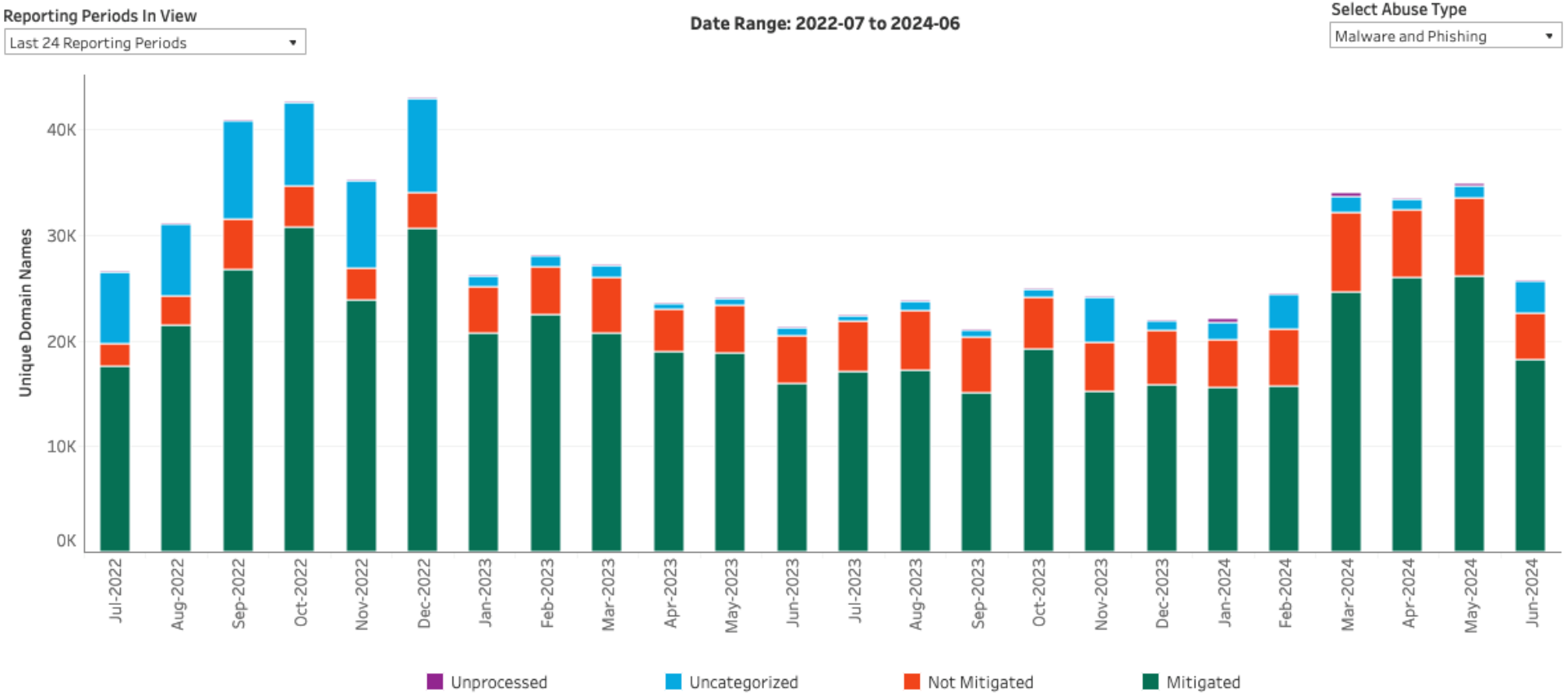



Contact us
English
NETBEACON INSTITUTE
Abuse Reporting
Abuse Analysis
Resources
The Institute
Report Abuse
Anyone can Report DNS Abuse
Internet Users
Anyone that happens upon or falls victim to DNS Abuse can and should use NetBeacon Reporter. Abuse reports are then shared with registrars who will use the information provided to identify and take action against online abuse.
Law Enforcement Agencies
Law enforcement officials who receive reports of online abuse (i.e., scams, phishing attempts, spam, botnets) can either refer complainants to NetBeacon Reporter or report online abuse directly. Both methods will deliver the report and flag the incident with registrars to investigate and take action where appropriate.
Consumer Protection Agencies
NetBeacon Reporter replaces many of the ad-hoc methods used by the agencies whose mandate includes protecting people from certain online harms. With NetBeacon Reporter, agencies can report DNS Abuse knowing that the report will reach the appropriate parties who can investigate and take action.
Internet Security Agencies
NetBeacon Reporter greatly simplifies online abuse reporting for Internet security and threat intelligence agencies. NetBeacon Reporter replaces numerous, often ad-hoc processes, allowing agencies to report phishing, spam, botnets, malware and other scams and consumer fraud attempts to the appropriate parties.

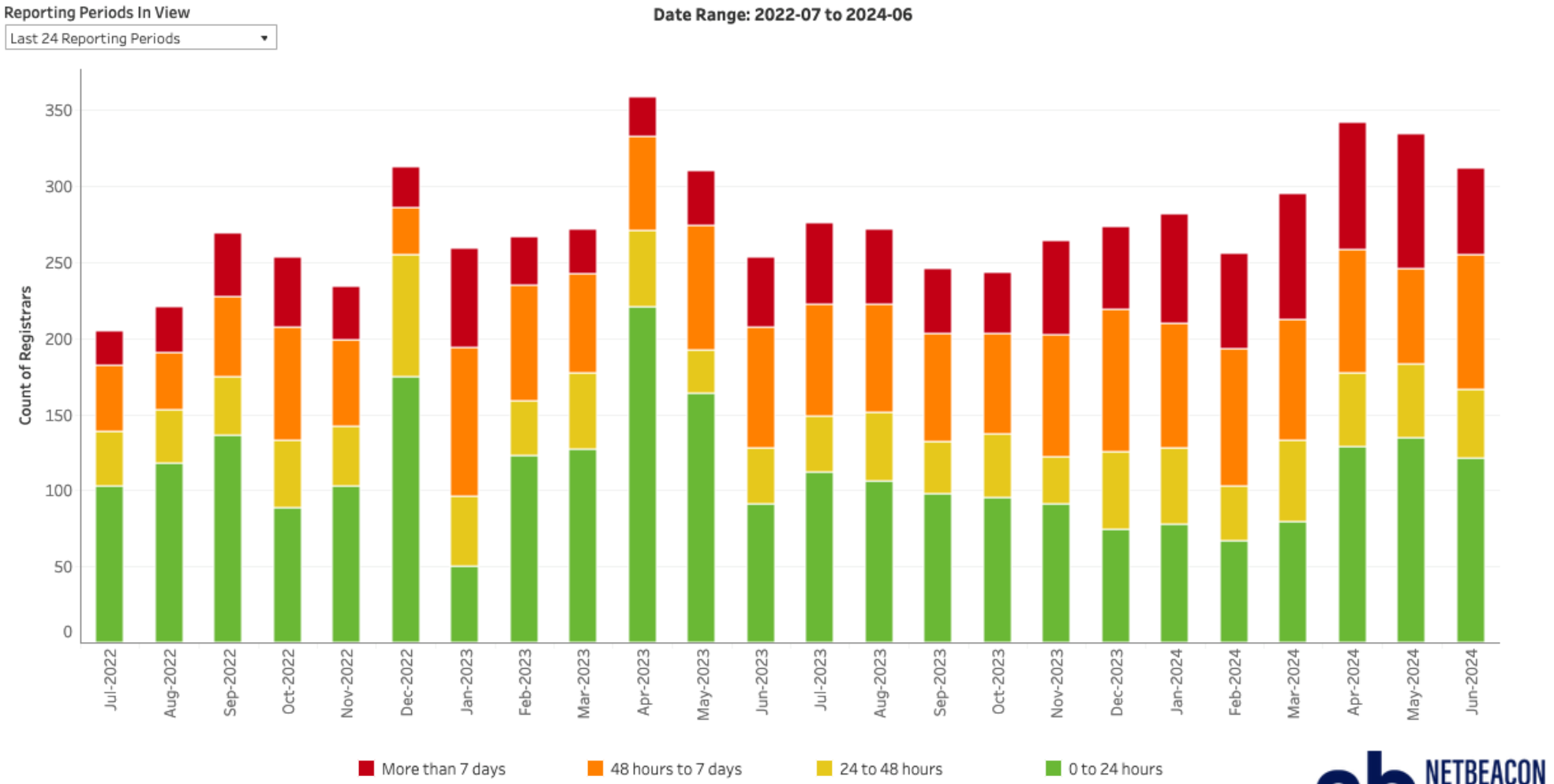
Malicious vs. Compromised



Abuse Mitigation



Registrar Median Mitigation Time



Ko darīt? Ar ko sākt?

Interneta lietotāji

Pakalpojumu sniedzēji

TSIe

Internets

Ļaundari

Eiropas Komisija

Pētījums: *Study on Domain Name System (DNS) abuse*

Divi «vadošie» – **41%**

- jaunie ALD: visvairāk «cieš» no ļaunprātīgas izmantošanas

- **25%** pikšķerēšanas un **41%** ļaunatūras vārdus reģistrējuši leģitīmi lietotāji

- Piecām reģistratūrām **48%** ļaunprātīgo reģistrāciju

Pētījums: *Study on Domain Name System (DNS) abuse*

- Mitināšanas pakalpojumu sniedzējiem ar augstu spama «koncentrāciju» – **3000** ļaunprātīgi vārdi uz **10 000** reģistrēto vārdu

- **2,5 miljoni** atvērtie DNS atrisinātāji (*resolver*)

- **ES valstu** domēni visdrošākie

Septiņi biežāk izmantotie – **76%**

TLD League Table
From January 1st 2022 - Today

Search league table

All Global regions | Asia Global regions | Europe Global regions | Africa Global regions | Oceania Global regions | Americas Global regions

	LW	TLD	Country	Abuse rate (%)	No. Domains
1	1	.DK	DENMARK	0.0366	1,359,434
2	2	.NO	NORWAY	0.0398	826,551
3	3	.GI	GIBRALTAR	0.0402	2,486
4	4	.BE	BELGIUM	0.0787	1,655,929
5	5	.CH	SWITZERLAND	0.0816	2,503,284
6	6	.MC	MONACO	0.0834	3,598
7	7	.IE	IRELAND	0.0929	311,054
8	8	.NL	NETHERLANDS	0.1031	6,027,494
9	9	.FI	FINLAND	0.1041	528,563
10	10	.MT	MALTA	0.1070	19,631

DNS RESEARCH FEDERATION

NIC

TLD League Table
From January 1st 2022 - Today

Search league table

	LW	TLD	Country	Abuse rate (%)	No. Domains
33	33	**.LV**	LATVIA	0.3953	128,523
41	41	**.FO**	FAROE ISLANDS	0.5993	6,674
42	42	**.MK**	NORTH MACEDONIA	0.7284	34,872
43	43	**.LI**	LIECHTENSTEIN	0.7476	69,821
44	44	**.AX**	ÃLAND ISLANDS	0.7741	4,134
45	45	**.RO**	ROMANIA	0.7879	563,524
46	46	**.MD**	MOLDOVA	0.8187	29,071
47	47	**.EE**	ESTONIA	0.9387	159,255
48	48	**.RU**	RUSSIAN FEDERATION	2.2262	4,894,382
49	49	**.ME**	MONTENEGRO	2.4884	1,179,093
50	50	**.IM**	ISLE OF MAN	2.7181	39,071

There is insufficient data for the following top-level domains in this region .SJ (Svalbard and Jan Mayen Islands), .VA (Holy See)

Interneta lietotāji

Pakalpojumu sniedzēji

TSIe

Internets

Ļaundari

Eiropas Komisija

Vai jau jāsāk satraukties?

TID2 (NIS2) 28.pants cita starpā prasa:

ALD nosaukumu reģistri un vienības, kas sniedz domēnu nosaukumu reģistrācijas pakalpojumus, ar pienācīgu rūpību vāc un uztur **precīzus un pilnīgus** domēnu nosaukumu reģistrācijas datus.

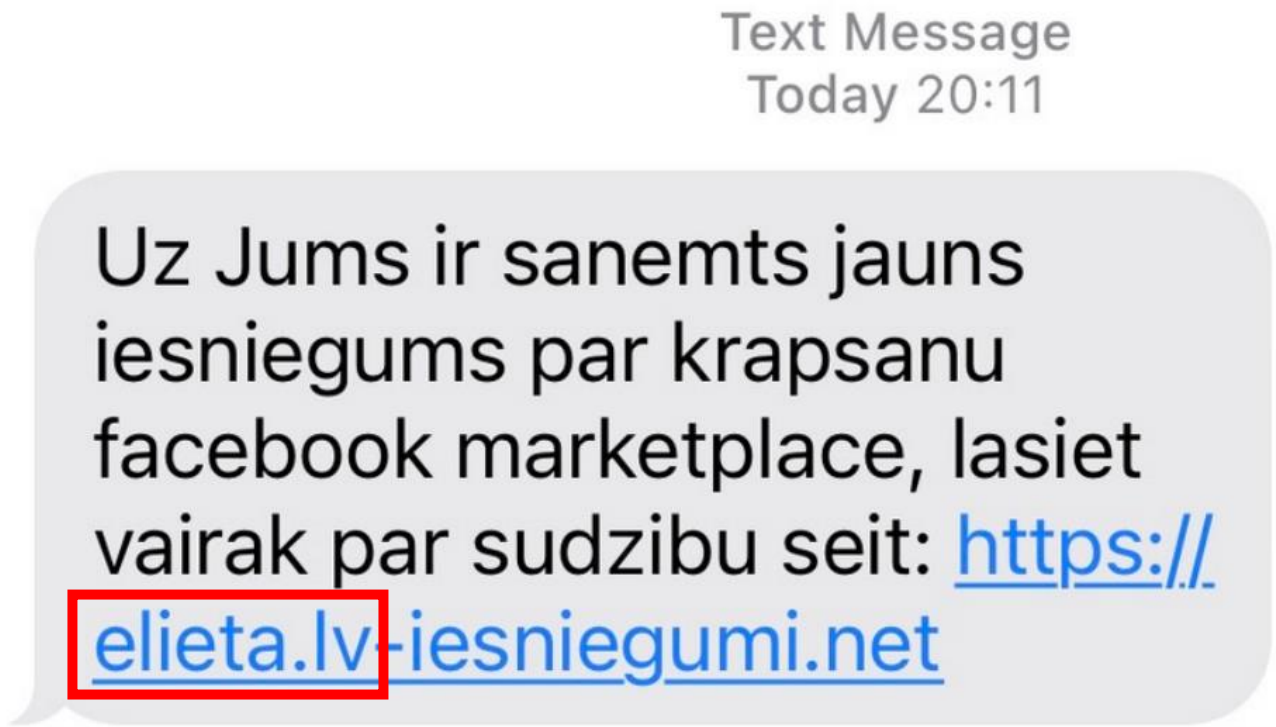
Domēnu nosaukumu reģistrācijas datubāzē jāietver vajadzīgā informācija, kas ļautu identificēt domēnu nosaukumu turētājus un kontaktpunktus, kuri pārvalda domēnu nosaukumus, un sazināties ar tiem. Šāda informācija ietver:

a) domēna nosaukumu;
b) reģistrācijas datumu;
c) reģistrētāja vārdu un uzvārdu, e-pasta adresi un tālruņa numuru;
d) tā kontaktpunkta e-pasta adresi un tālruņa numuru, kurš pārvalda domēna nosaukumu, ja tie atšķiras no reģistrētāja e-pasta adreses un tālruņa numura.

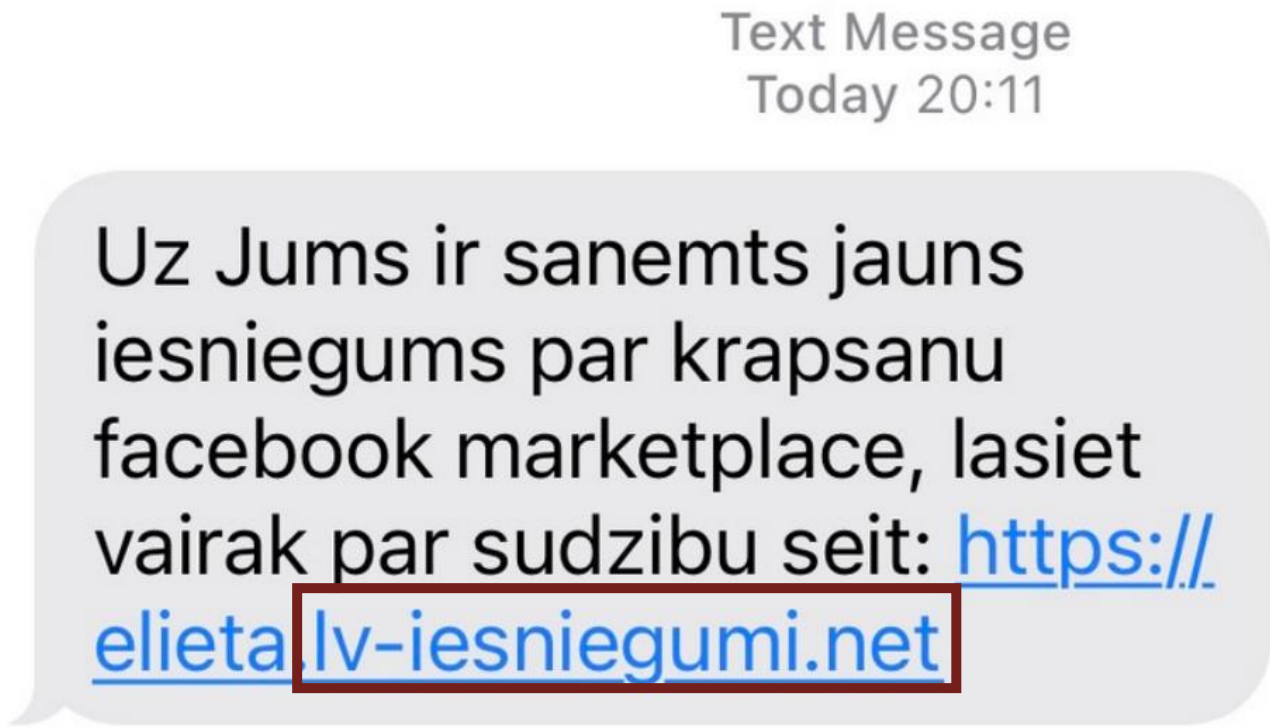
ALD nosaukumu reģistriem un vienībām, kas sniedz domēnu nosaukumu reģistrācijas pakalpojumus, jāievieš rīcībpolitikas un procedūras, tostarp **verifikācijas procedūras**, lai nodrošinātu, ka minētajā datubāzē ir iekļauta precīza un pilnīga informācija.

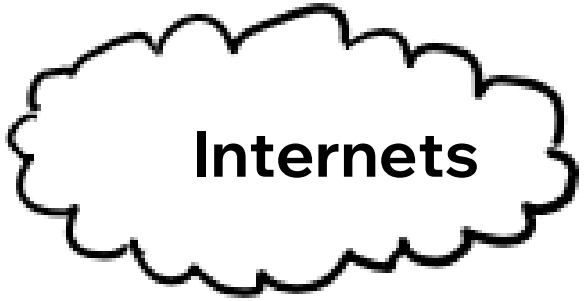
Vai tagad visu atrisināsim?

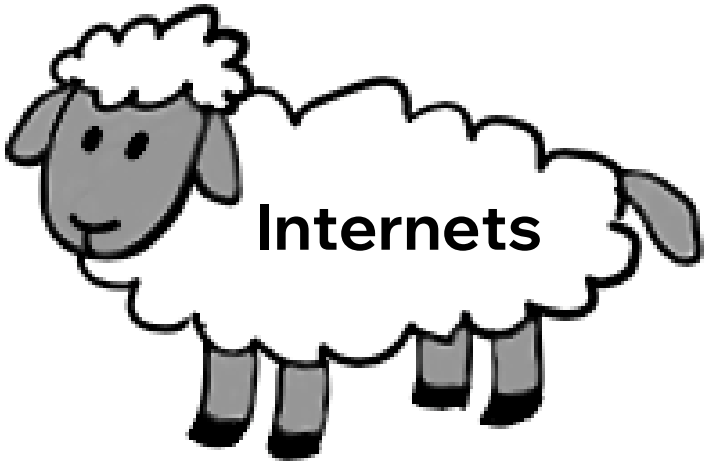

Text Message
Today 20:11
Uz Jums ir sanemts jauns iesniegums par krapsanu facebook marketplace, lasiet vairak par sudzibu seit: https://elieta.lv-iesniegumi.net



Izskatās gaužām ticami...


Text Message
Today 20:11
Uz Jums ir sanemts jauns iesniegums par krapsanu facebook marketplace, lasiet vairak par sudzibu seit: https://elieta.lv-iesniegumi.net


Internets


Internets

Jāmācās un jāmāca!

Photo by Gilly on Unsplash

Paldies par uzmanību!

DNS@NIC.LV

HTTPS://WWW.NIC.LV