possible.lv

nu un kas, ja nepagarinu domēna vārdu?

Pētījuma autori:

- Kirils Solovjovs
- Mārtiņš Rozenbergs
- Toms Liepājnieks

- Kad Tu pēdējo reizi rakstīji kaut ko
  - šādu 172.217.18.78?
  - vai šādu 2a00:1450:4016:809::200e?
- Gandrīz visi labdabīgie savienojumi sākas ar DNS pieprasījumu

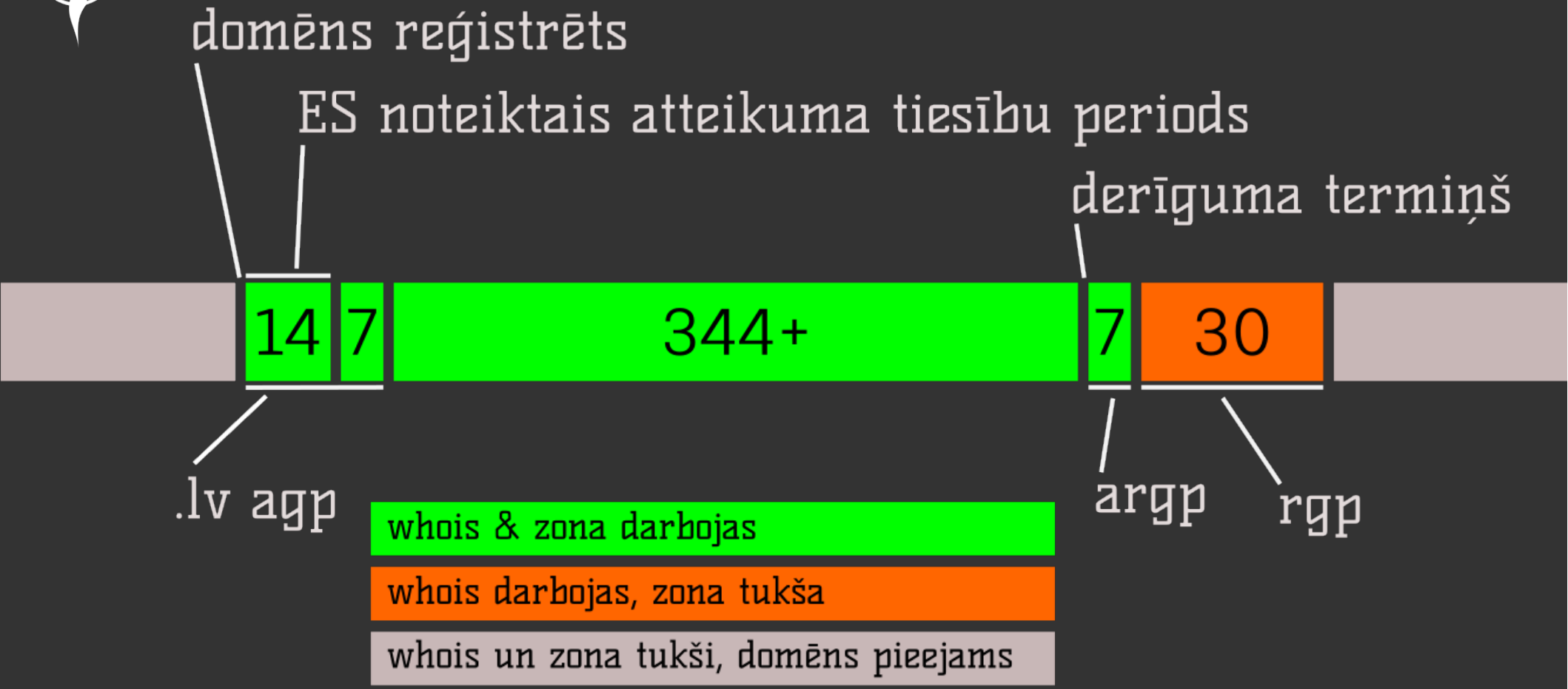
- Vairums domēnu ir maksas pakalpojums
- Neuzmanība:
  - aizmirsts pagarināt
  - beidzies bankas kartes derīgums
- Pamešana:
  - projekts beidzies
  - uzņēmumu apvienošana
  - tiesas rīkojums

- Kādus uzbrukuma vektorus varam novērot dabā?
- 2018. gada vidus
- .lv ccTLD
  - arī “latviskie” vārdi
- ~~pikšķerēšana~~
- ~~aktīvie uzbrukumi~~

- kvantitatīvais un kvalitatīvais pētījums
- *ftp, ssh, telnet, smtp, dns, http, pop3, imap, https, ~~rdp, vnc~~*

possible.lv

.lv ccTLD domēna dzīves cikls



possible.lv

gana teorijas;
ķeramies klāt!

- 180 domēni uz 1 IP adreses
- Daudz skenēšanas mēģinājumu un citu ļauno
- Robots vai cilvēks?

- Reģistrējam nesen beigušos domēnus, kas
  - ir atrodami tīmekļa meklētājos vai
  - saistās ar kādu personu, vai
  - ir līdzīgi citiem populāriem domēniem
- Nekavējoties pieprasām SSL sertifikātu

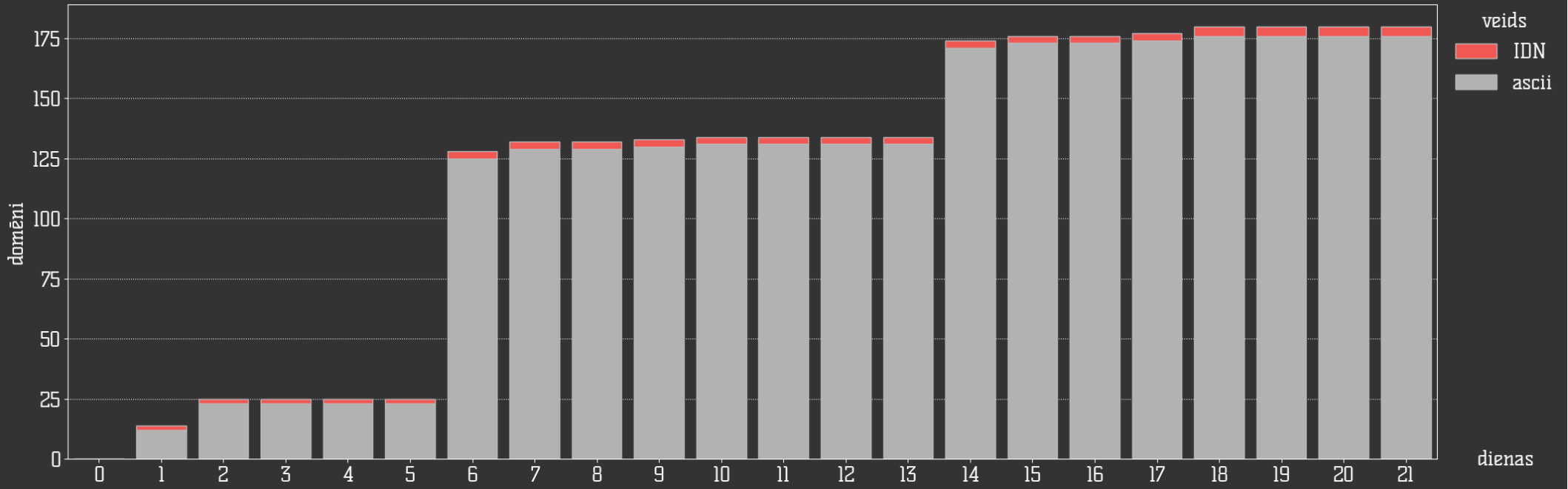
- Korelējam DNS pieprasījumus ar citiem pieprasījumiem
  - heiristika: laiks + AS
- Atlasām robotus (HTTP)
- Atlasām skenēšanu un paroļu minēšanas uzbrukumus
- Detalizēti apskatām atlikušos datus
  - e-pastu un tīmekļa pieprasījumu kvalitatīvā analīze
  - pārējo protokolu kvantitatīvā analīze

possible.lv

viss skaidrs,
bet vai parādīsi arī kādus datus?

possible.lv

reģistrēto domēnu skaits

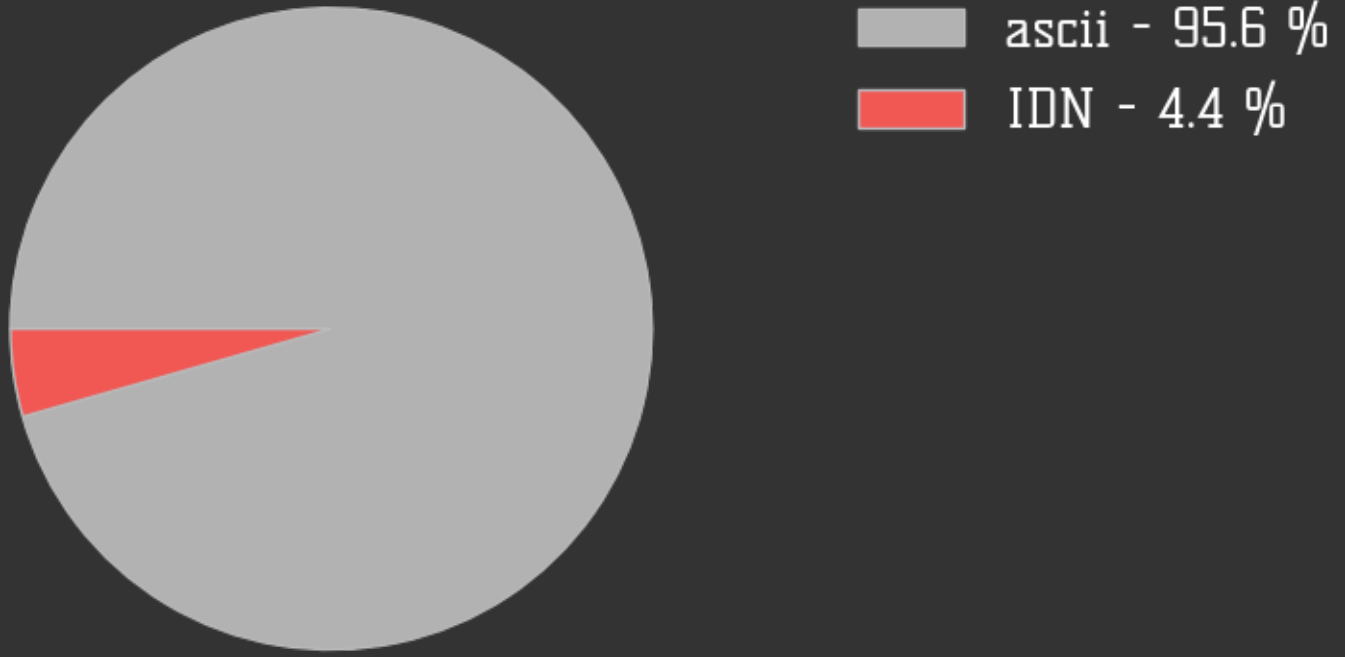


06.12.2018.

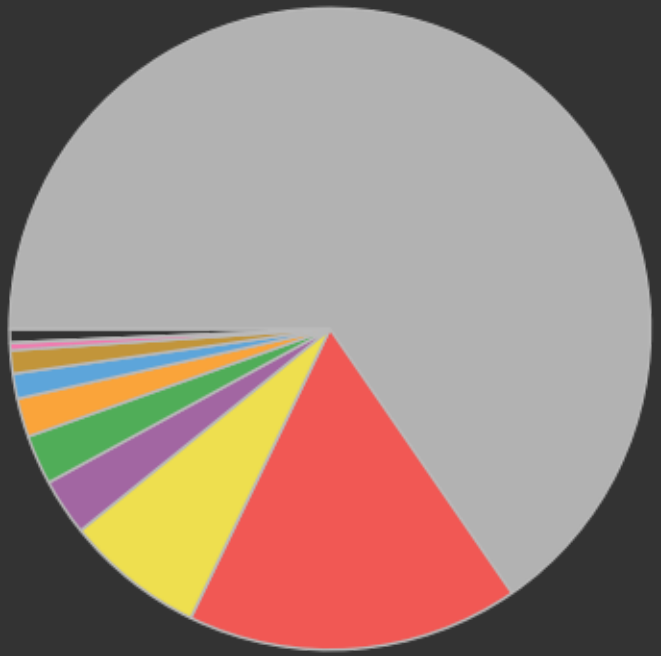
“Esi drošs”

@KirilsSolovjovs

dns/pieprasījumi (svērti)

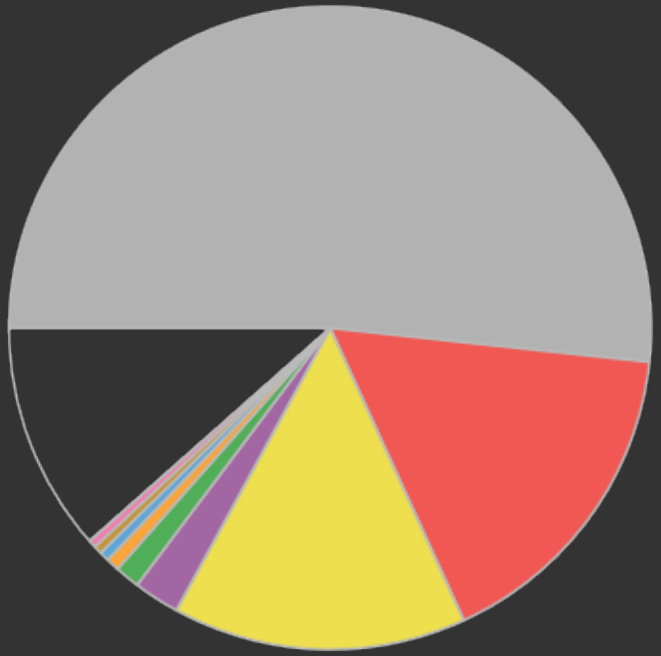


dns/ierakstu_veidi



- A - 65.4 %
- AAAA - 16.8 %
- MX - 7.0 %
- TXT - 2.9 %
- NS - 2.5 %
- SOA - 2.0 %
- SRV - 1.3 %
- CAA - 1.2 %
- CNAME - 0.4 %
- (citi) - 0.5 %

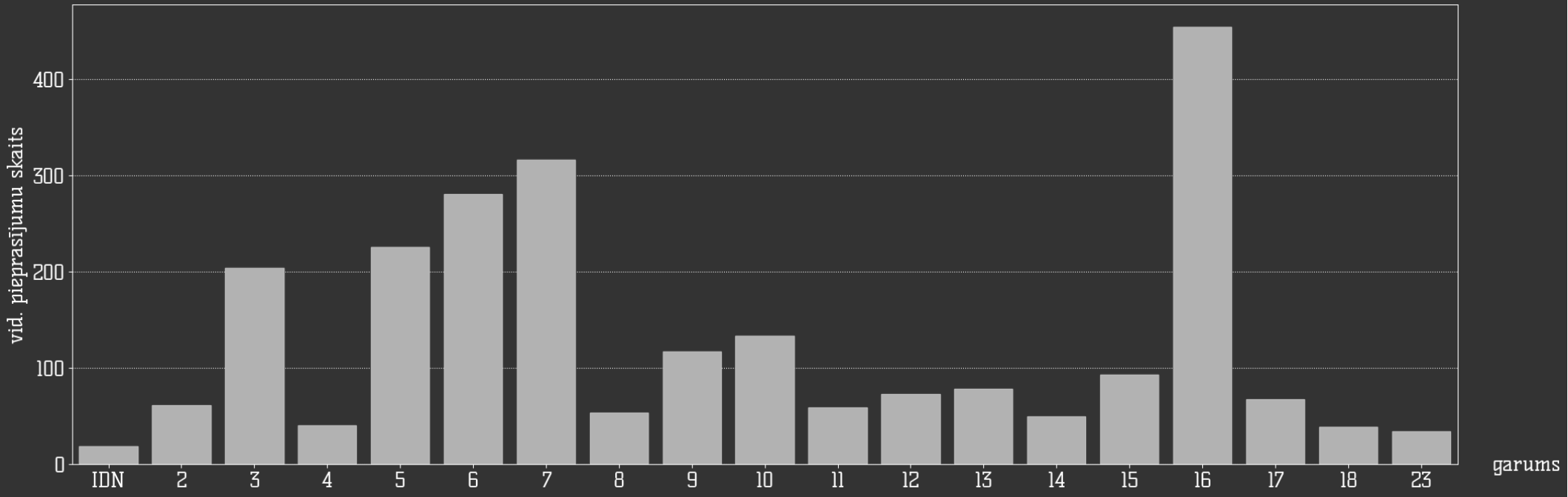
dns/apakšdomēni



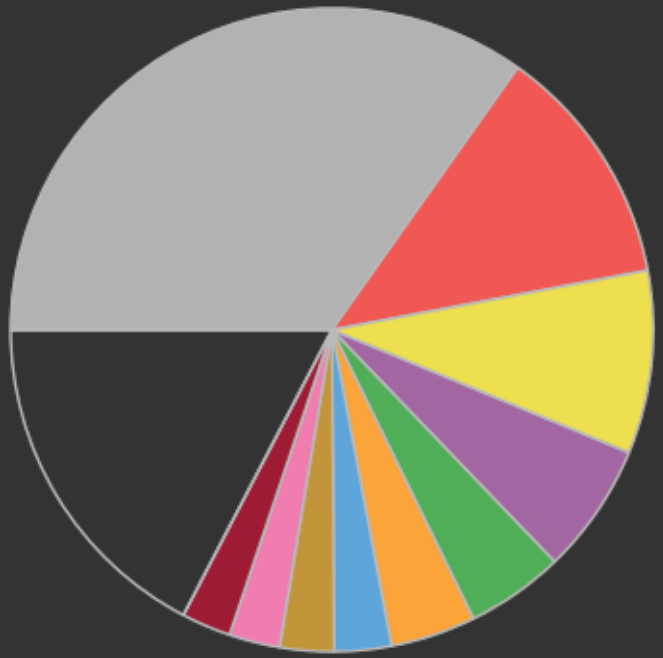
- @ - 51.7 %
- www - 16.5 %
- mail - 14.8 %
- smtp - 2.3 %
- webmail - 1.3 %
- webdisk - 0.5 %
- cpanel - 0.4 %
- [redacted] - 0.4 %
- (citi) - 11.4 %

possible.lv

dns/vidējais_pieprasījumi_skaits_pēc_garuma (svērti)



dns/valstis



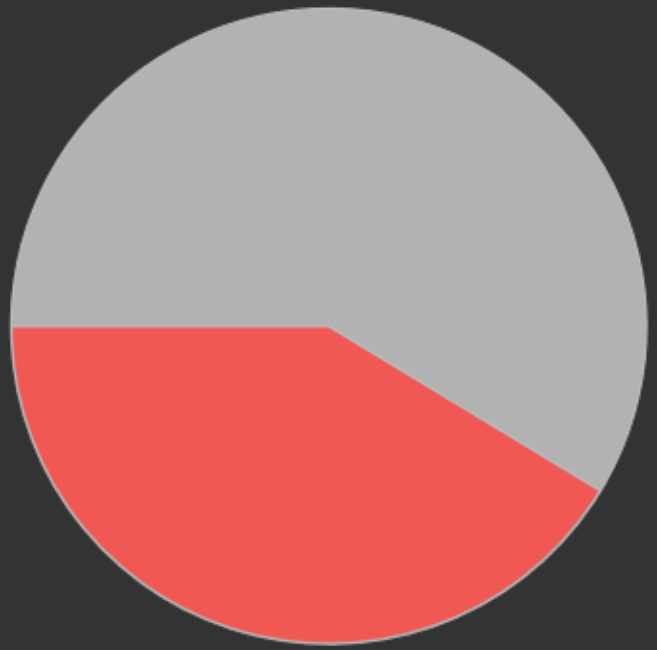
- US - 34.8 %
- NL - 12.2 %
- RU - 9.2 %
- DE - 6.6 %
- SG - 4.9 %
- CN - 4.3 %
- BE - 2.9 %
- TW - 2.7 %
- CH - 2.6 %
- LV - 2.5 %
- (citas) - 17.3 %

Lietotājs:

1) root
2) admin
3) test
4) user
5) support
6) ubnt
7) oracle
8) ubuntu
9) postgres
10) adm

Parole:

1) 123456
2) password
3) 12345
4) 1234
5) 123
6) admin
7) test
8) wubao
9) 1
10) root

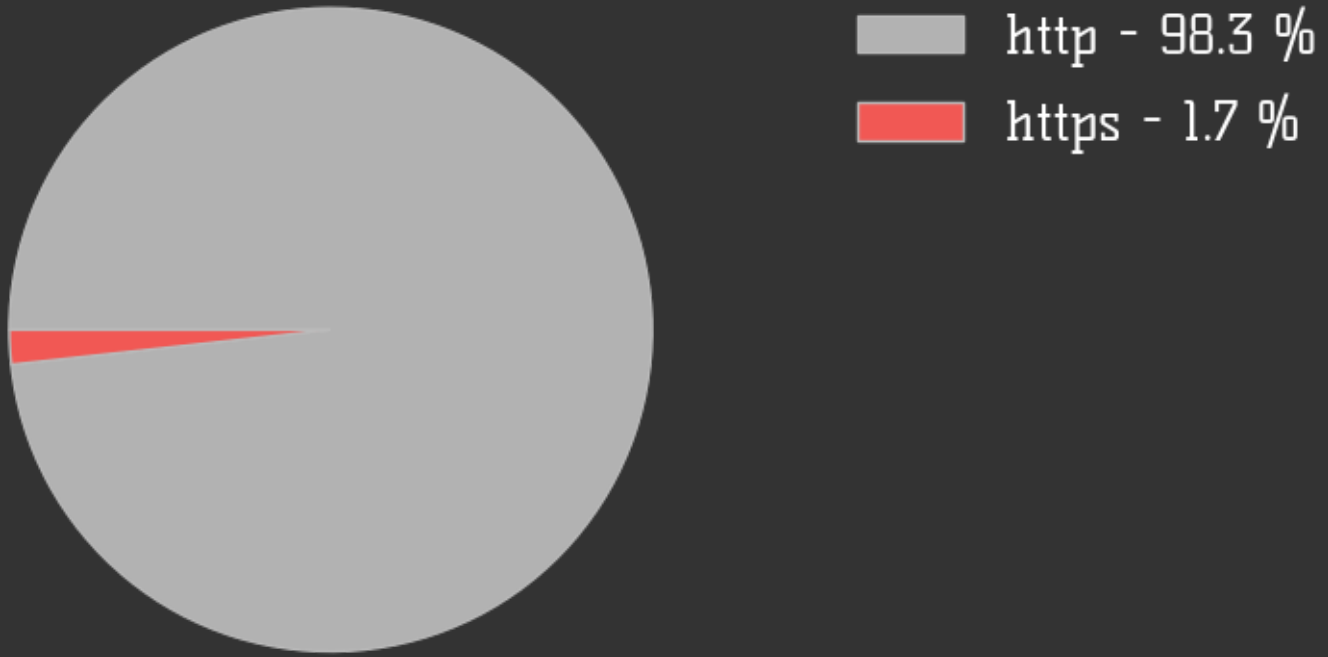


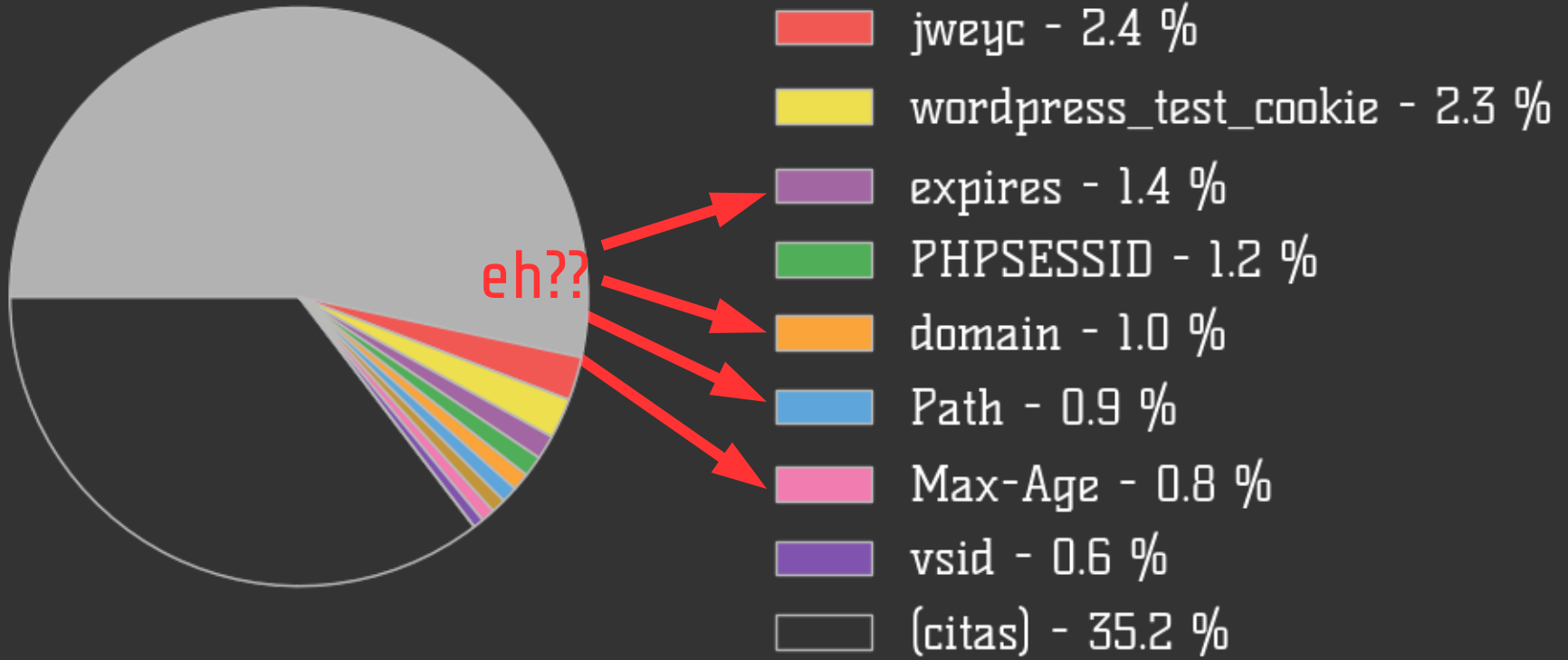
roboti - 58.7 %

leģitīmi lietotāji - 41.3 %

possible.lv

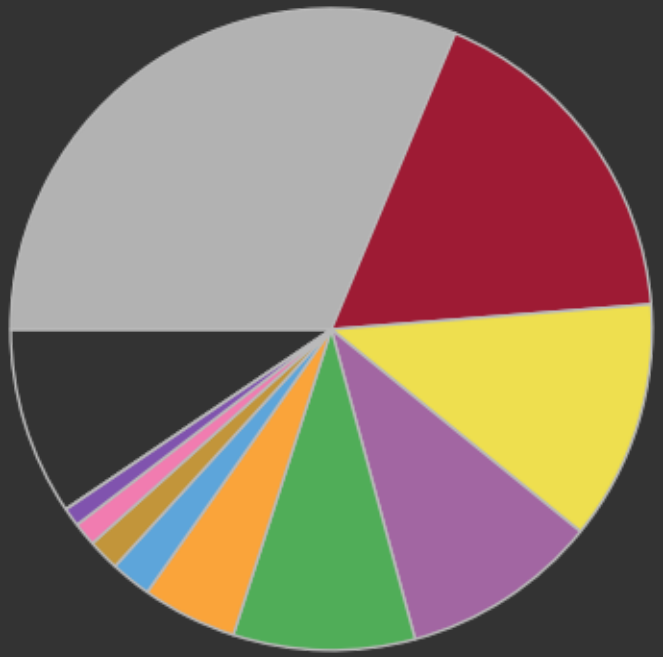
pietiks skatīties uz hakeriem!
turpmāk – tikai reālu lietotāju dati


http - 98.3 %
https - 1.7 %


eh??
jweyc - 2.4 %
wordpress_test_cookie - 2.3 %
expires - 1.4 %
PHPSESSID - 1.2 %
domain - 1.0 %
Path - 0.9 %
Max-Age - 0.8 %
vsid - 0.6 %
(citas) - 35.2 %

possible.lv

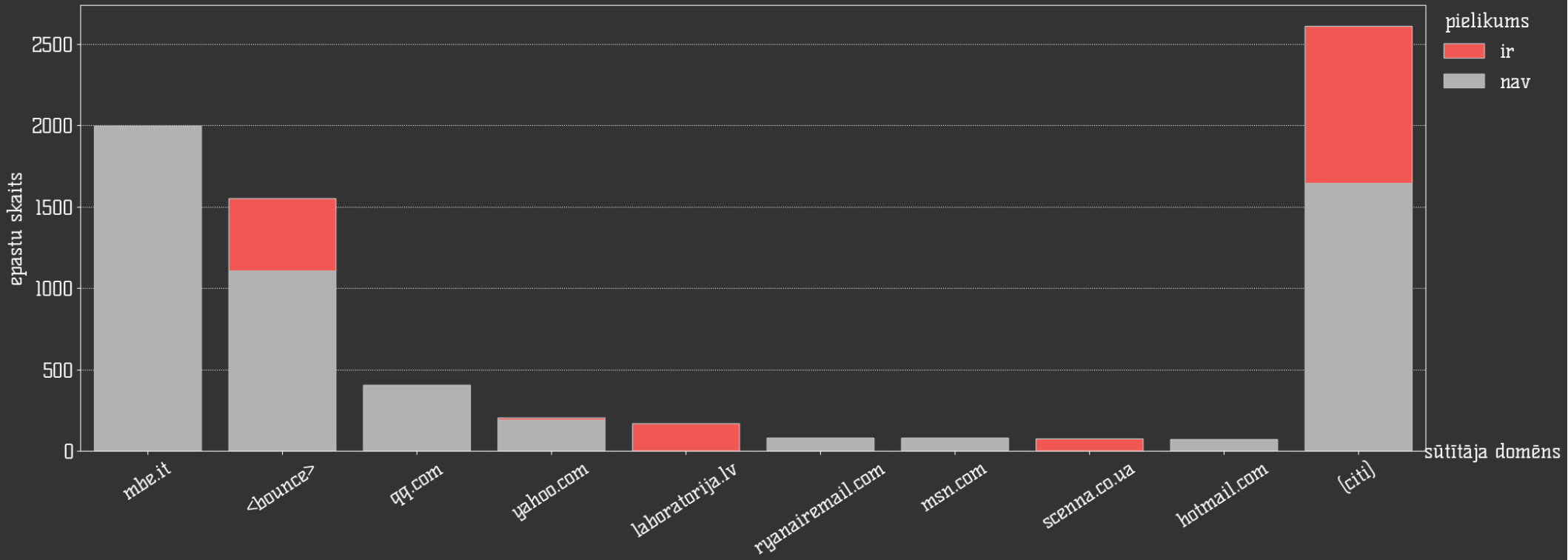
tīmeklis/valstis



- US - 31.3 %
- LV - 17.4 %
- IE - 12.1 %
- JP - 9.9 %
- SG - 9.1 %
- CN - 4.8 %
- RU - 2.1 %
- FR - 1.6 %
- DE - 1.2 %
- UA - 0.9 %
- (citas) - 9.6 %

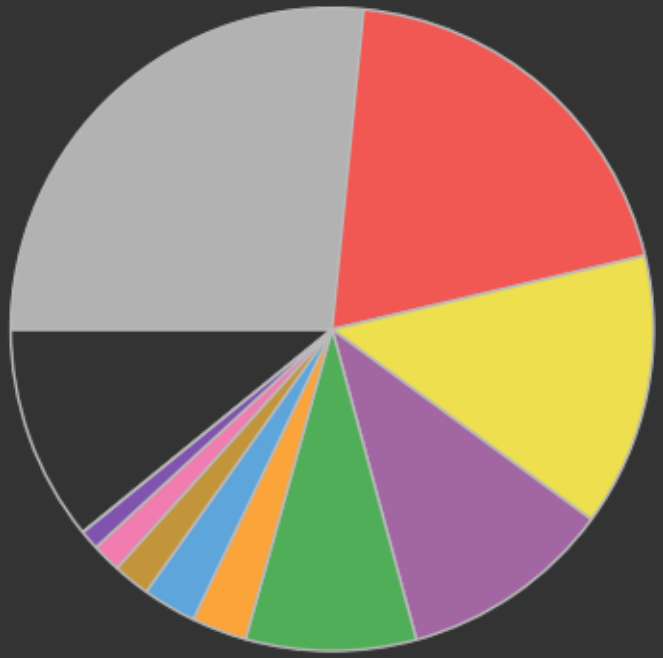
possible.lv

pasts/sūtītāja_domēni/pielikumi



possible.lv

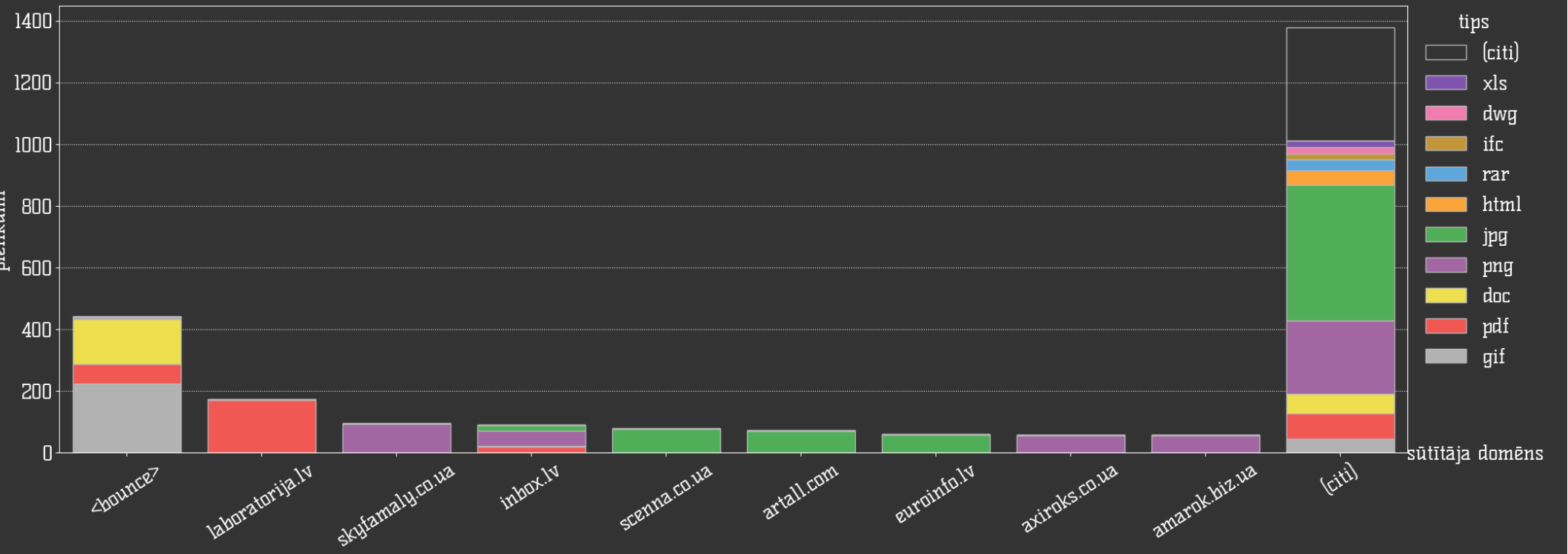
pasts/pielikumu_tips



- jpg - 26.6 %
- png - 19.7 %
- pdf - 13.8 %
- gif - 10.7 %
- doc - 8.6 %
- ace - 2.8 %
- zip - 2.7 %
- html - 1.9 %
- rar - 1.5 %
- gz - 1.0 %
- (citi) - 10.7 %

possible.lv

pasts/sūtītāja_domēni/pielikumu_tips

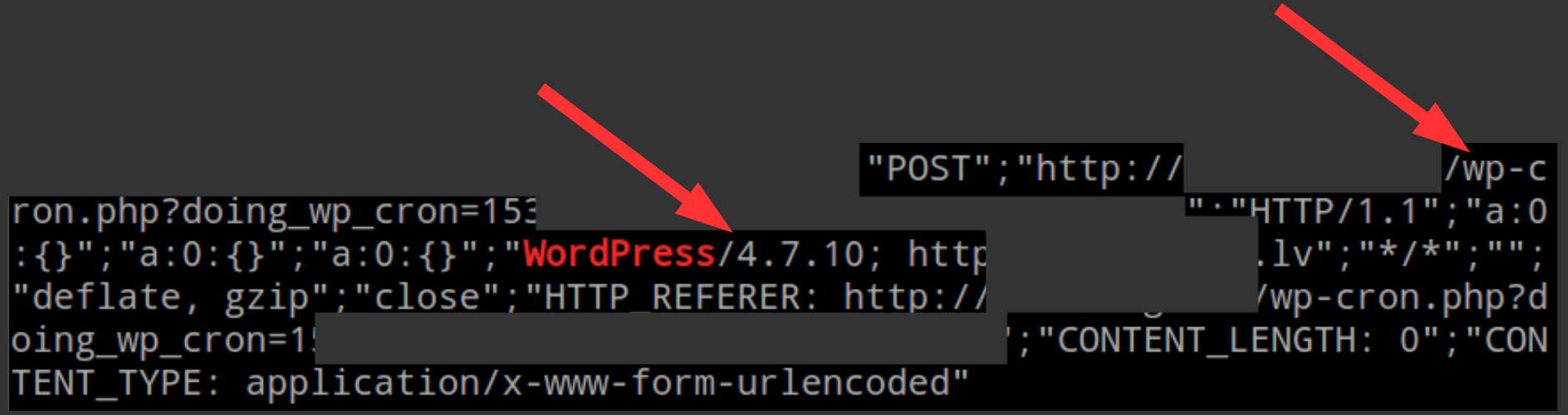


possible.lv

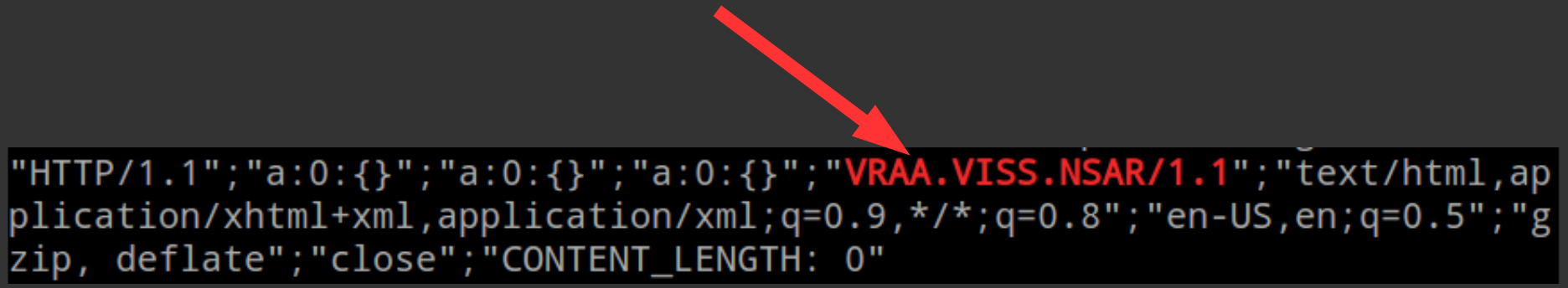
būs jau gana;
apskatīsim konkrētus piemērus

```
                                        ;"GET";"http://          .lv/announce.p
hp?passkey=9a7c6148bdf4351
5%070%03%1d%1fq%c4n%ae%d7%e7&peer_id=
9&port=40789&uploaded=0&downloaded=0&left=733494901&corrupt=0&key=
1C&event=started&numwant=200&compact=1&no_peer_id=1";"HTTP/1.1";"a:0:{}"
;"a:0:{}";"a:0:{}";"uTorrent/354(111783400)(44520)";"";"";"gzip";"Close"
```

ieplānotie pieprasījumi no pamesta wordpress

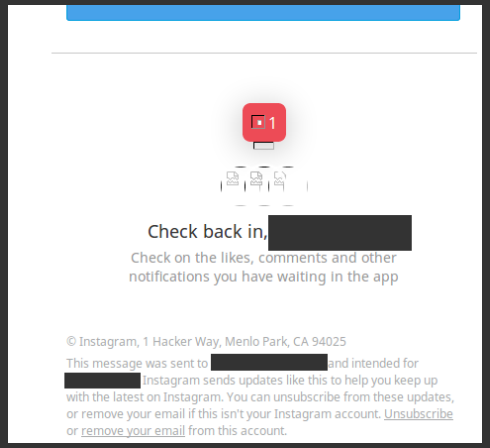


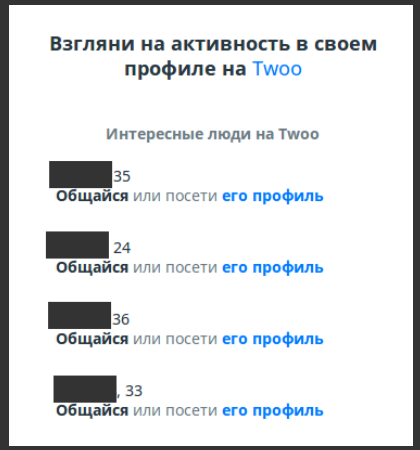
iegultie HTML elementi .gov.lv lapā

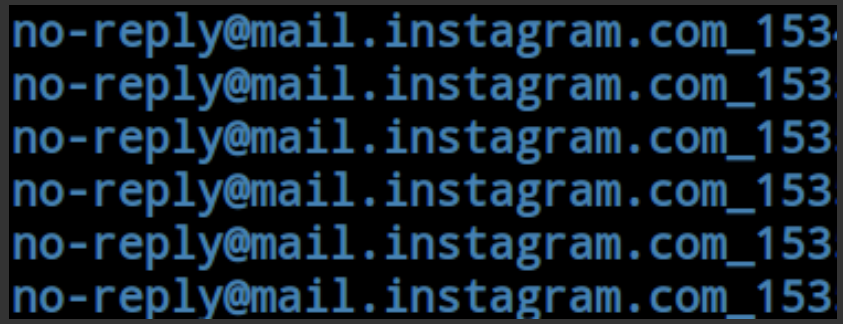

"HTTP/1.1";"a:0:{}";"a:0:{}";"a:0:{}";"VRAA.VISS.NSAR/1.1";"text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8";"en-US,en;q=0.5";"gzip, deflate";"close";"CONTENT_LENGTH: 0"

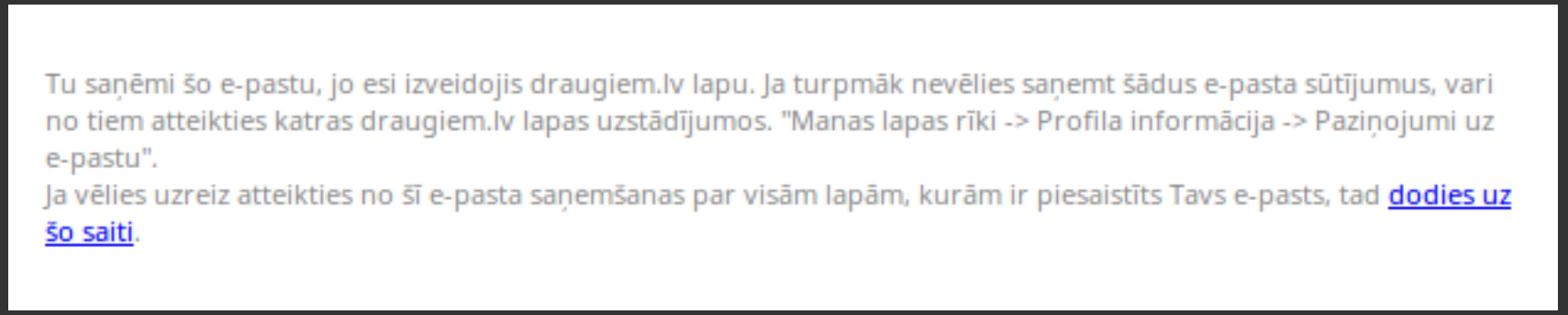
possible.lv

paziņojumi no sociālajiem tīkliem

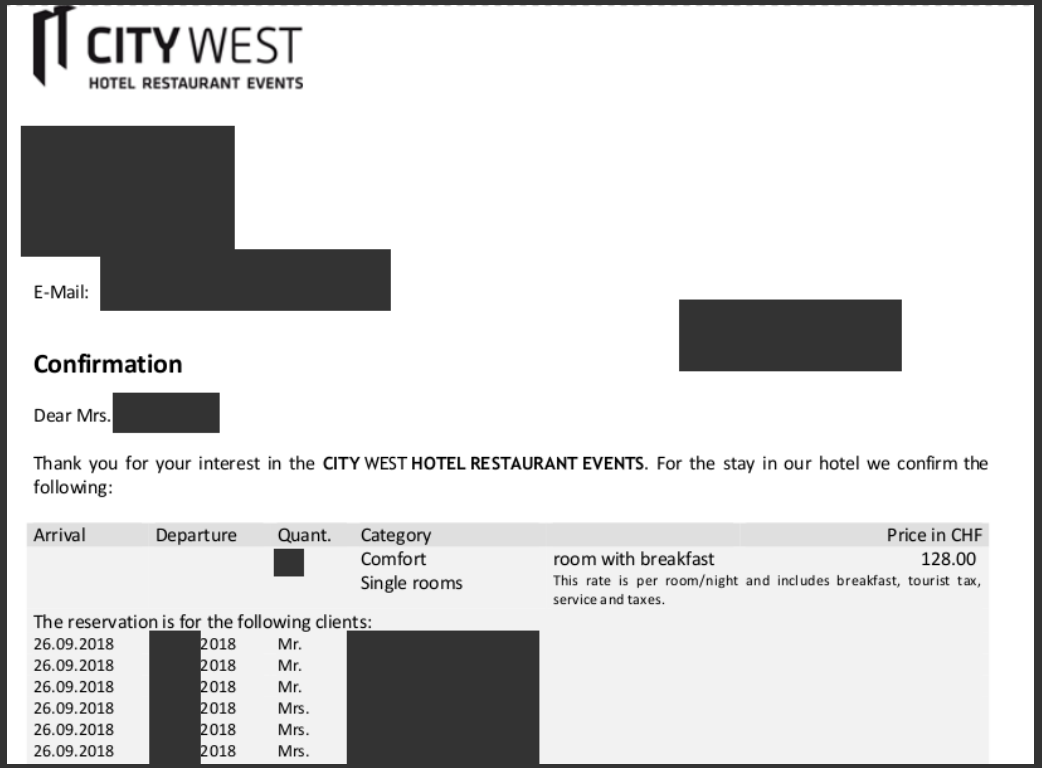








viesnīcas grupas rezervācija



CITY WEST
HOTEL RESTAURANT EVENTS

[redacted]

E-Mail: [redacted]

[redacted]

Confirmation

Dear Mrs. [redacted]

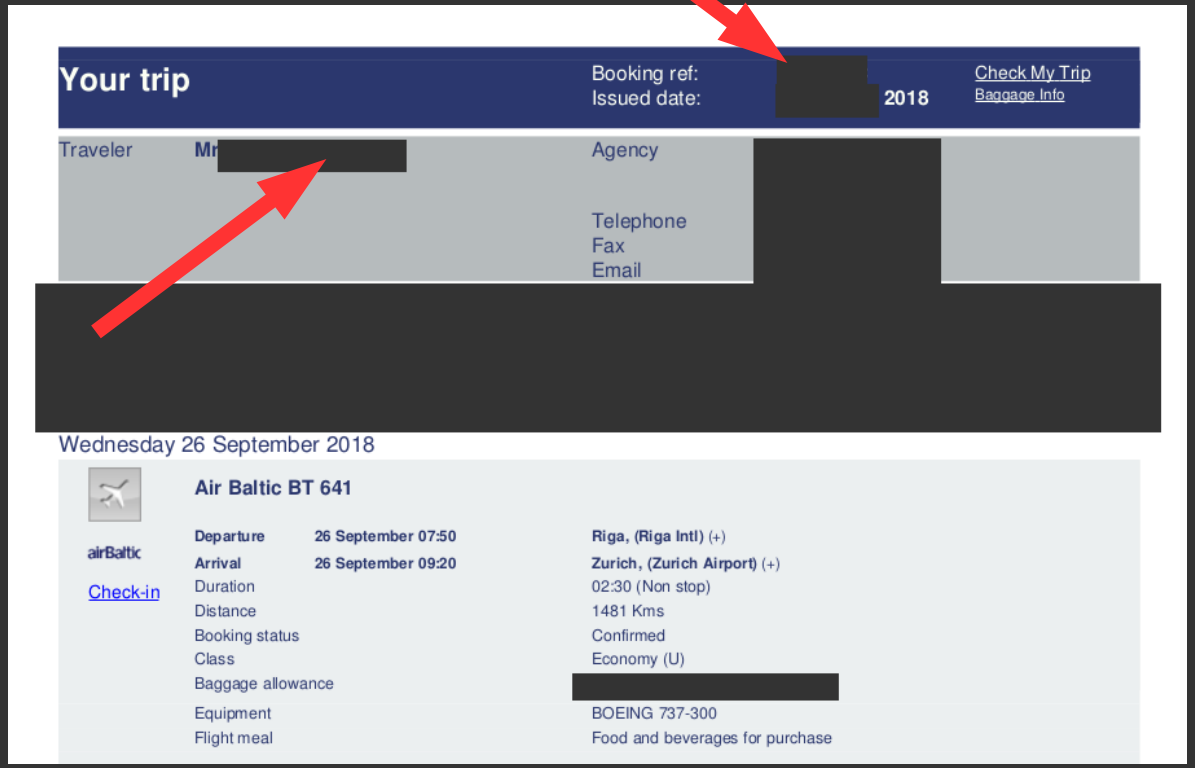
Thank you for your interest in the **CITY** WEST **HOTEL RESTAURANT EVENTS**. For the stay in our hotel we confirm the following:

Arrival	Departure	Quant.	Category		Price in CHF
		[redacted]	Comfort Single rooms	room with breakfast This rate is per room/night and includes breakfast, tourist tax, service and taxes.	128.00

The reservation is for the following clients:

26.09.2018	[redacted] 2018	Mr.	[redacted]
26.09.2018	2018	Mr.	
26.09.2018	2018	Mr.	
26.09.2018	2018	Mrs.	
26.09.2018	2018	Mrs.	
26.09.2018	2018	Mrs.	

lidojuma rezervācija



Your trip

Booking ref: [redacted]
Issued date: [redacted] 2018

Check My Trip
Baggage Info

Traveler Mr [redacted]

Agency [redacted]

Telephone
Fax
Email

[redacted]

Wednesday 26 September 2018

Air Baltic BT 641

airBaltic

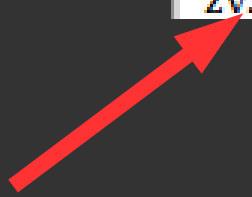
Check-in

Departure	26 September 07:50	Riga, (Riga Intl) (+)
Arrival	26 September 09:20	Zurich, (Zurich Airport) (+)
Duration		02:30 (Non stop)
Distance		1481 Kms
Booking status		Confirmed
Class		Economy (U)
Baggage allowance		[redacted]
Equipment		BOEING 737-300
Flight meal		Food and beverages for purchase

e-pasts no zvērināta advokāta

> ----- Original Message -----

> Ar cieņu,
> zv.adv. [redacted]



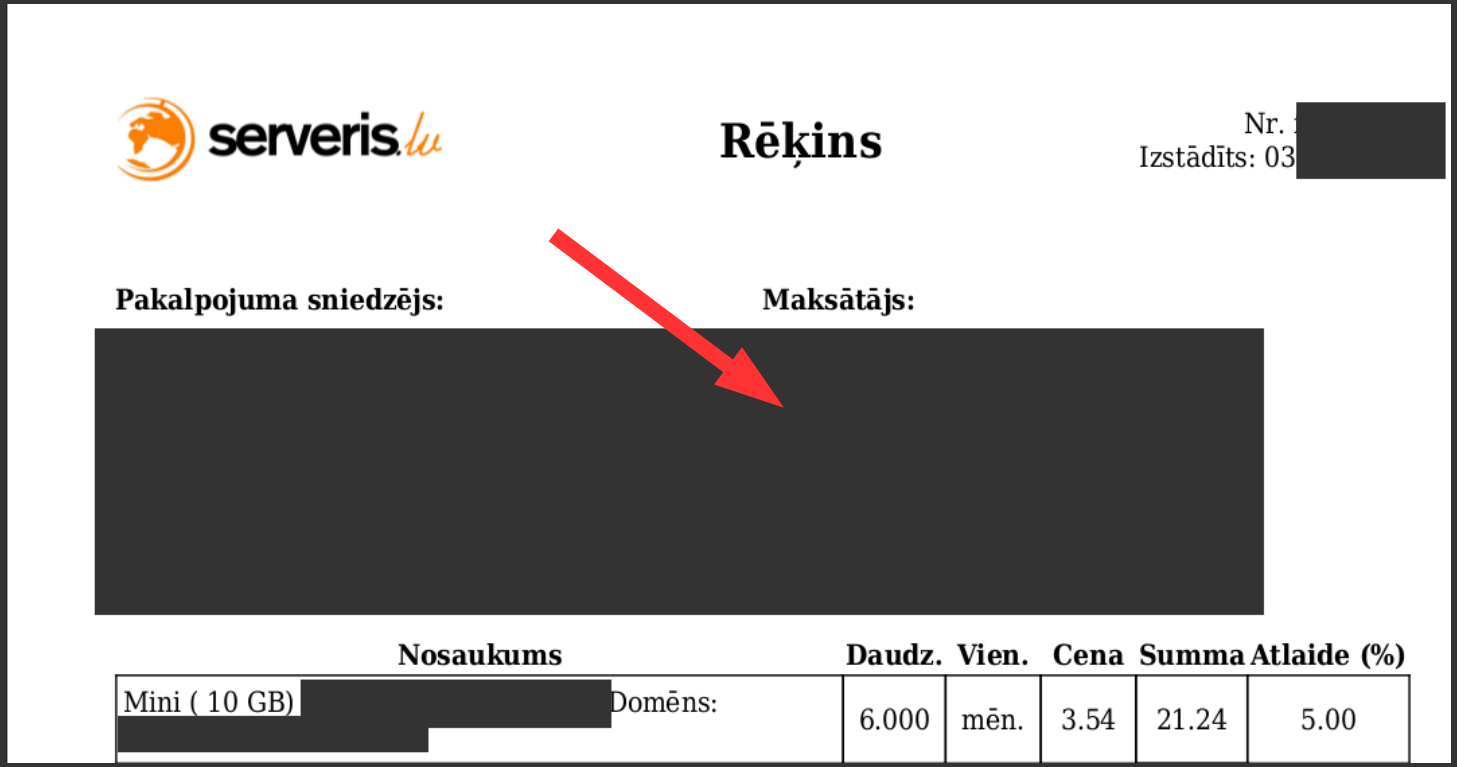
Informācija no Valsts ieņēmumu dienesta

Dokuments pieņemts

Nodokļu maksātāja Nr. [redacted] iesniegtais dokuments "**Darba devēja ziņojums (VSAOI un IIN)**" Nr. [redacted] par taksācijas periodu no [redacted] **2018** līdz [redacted] **2018** pieņemts un iekļauts VID datubāzē.
Dokumentā ir 1 obligāti sociāli apdrošināmi darba ņēmēji, kam uzrādīta riska nodeva, bet nostrādāto stundu skaits ir 0.

Šis e-pasts ir izveidots automātiski, lūdzam uz to neatbildēt.
Pieslēgties VID Elektroniskās deklarēšanas sistēmai: eds.vid.gov.lv.

rēķins ar lielu daudzumu privāto datu



serveris.lv

Rēķins

Nr. [redacted]
Izstādīts: 03[redacted]

Pakalpojuma sniedzējs:

[redacted]

Maksātājs:

[redacted]

Nosaukums	Daudz.	Vien.	Cena	Summa	Atlaide (%)
Mini (10 GB) [redacted] Domēns: [redacted]	6.000	mēn.	3.54	21.24	5.00

telekomunikāciju pakalpojumu rēķins

Sveiki!

[redacted]

Kopējā summa apmaksai i[redacted] [redacted] **EUR**
Klienta numurs: **3**
Apmaksas termiņš: **2018.**

Summa apmaksai sastāv no:
Rēķins par 2018. gada [redacted] **EUR**

Pārmaksa: **0.00 EUR**
Kavēts maksājums: **0.00 EUR** - ja šeit redzat '0 EUR', paldies! Ja ne, tad gan steidzieties šo summu apmaksāt, cik ātri iespējams!

paziņojums par kavētu maksājumu

[redacted]

[redacted]

ATGĀDINĀJUMS PAR APMAKSU

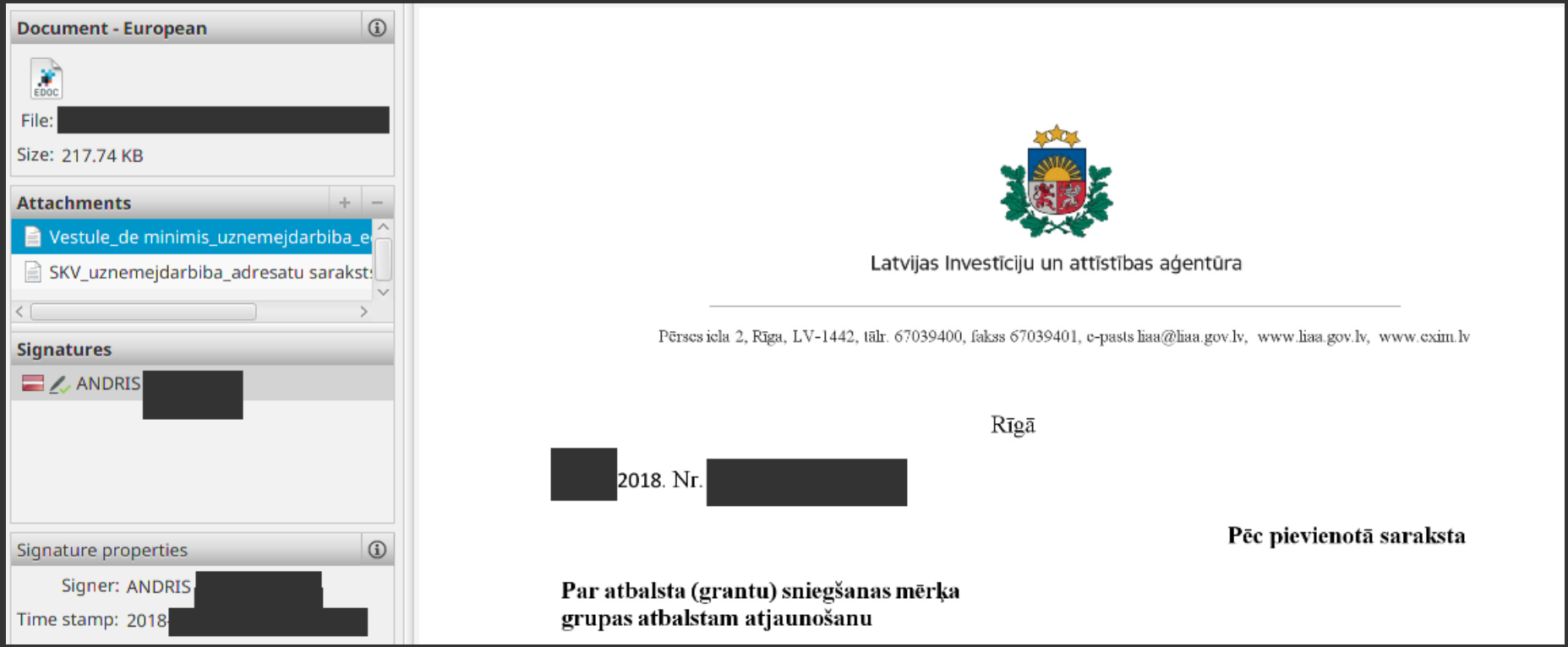
uz datumu 27.[redacted]2018

Pēc mūsu rīcībā esošās informācijas, neesam saņēmuši apmaksu par zemāk minētajiem rēķiniem noteiktajā termiņā.
Mēs būtu pateicīgi, ja jūs samaksātu tūlīt pēc šī atgādinājuma saņemšanas.

Dokumenta numurs	Dokumenta datums	Apmaksas datums	Summa	Valūta	Kavēto dienu skaits	Laikā neapmaksātā summa
[redacted]		2018	6,62		82	6,62
		2018	5,13		29	5,13
	Kopā:		**9,14**			11,75

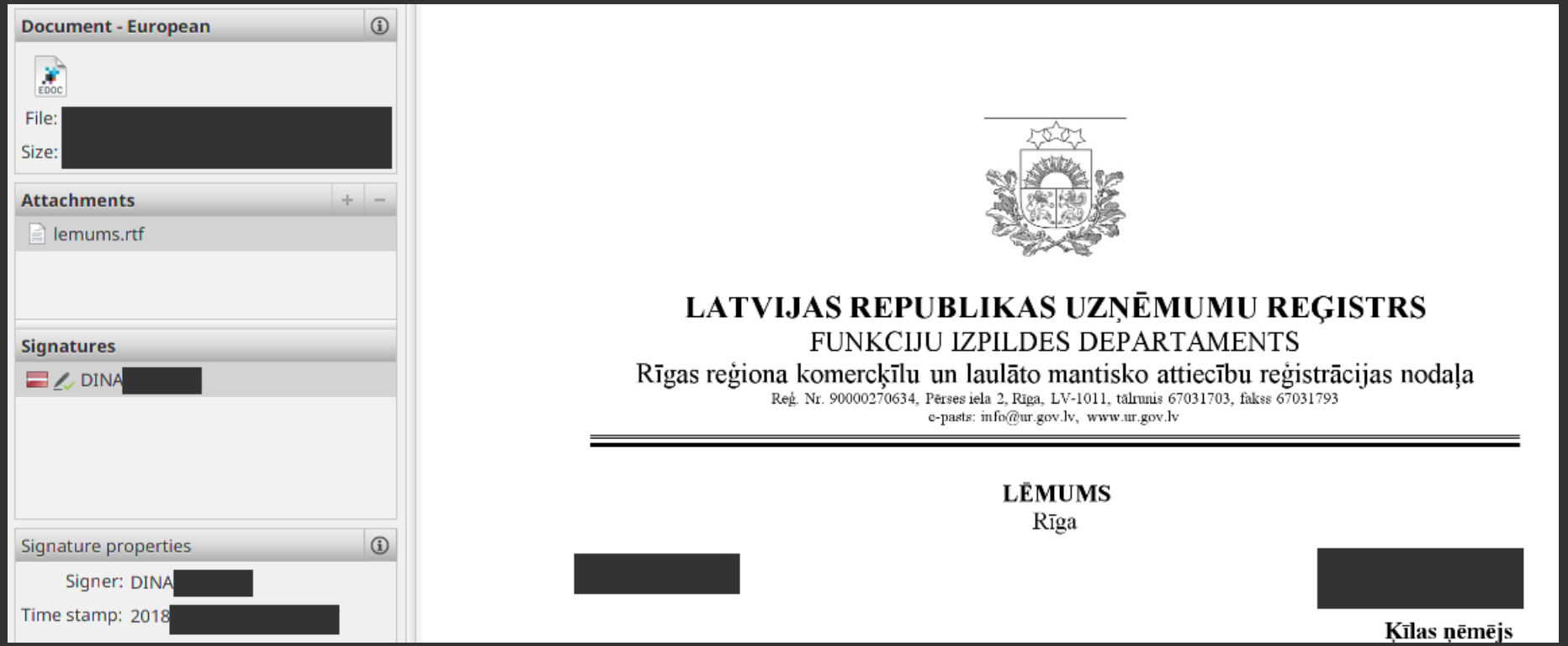
possible.lv

e-parakstīts dokuments no valsts iestādes

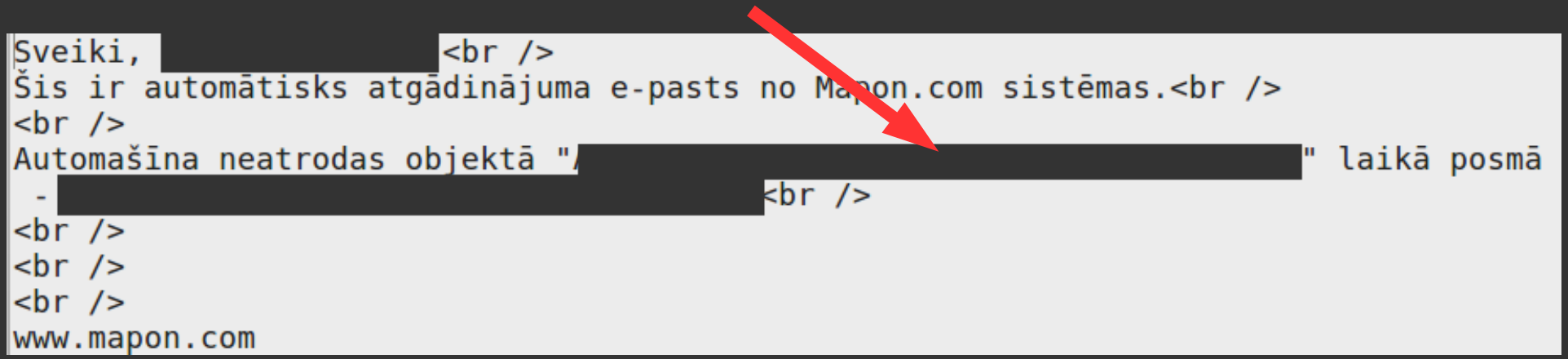


possible.lv

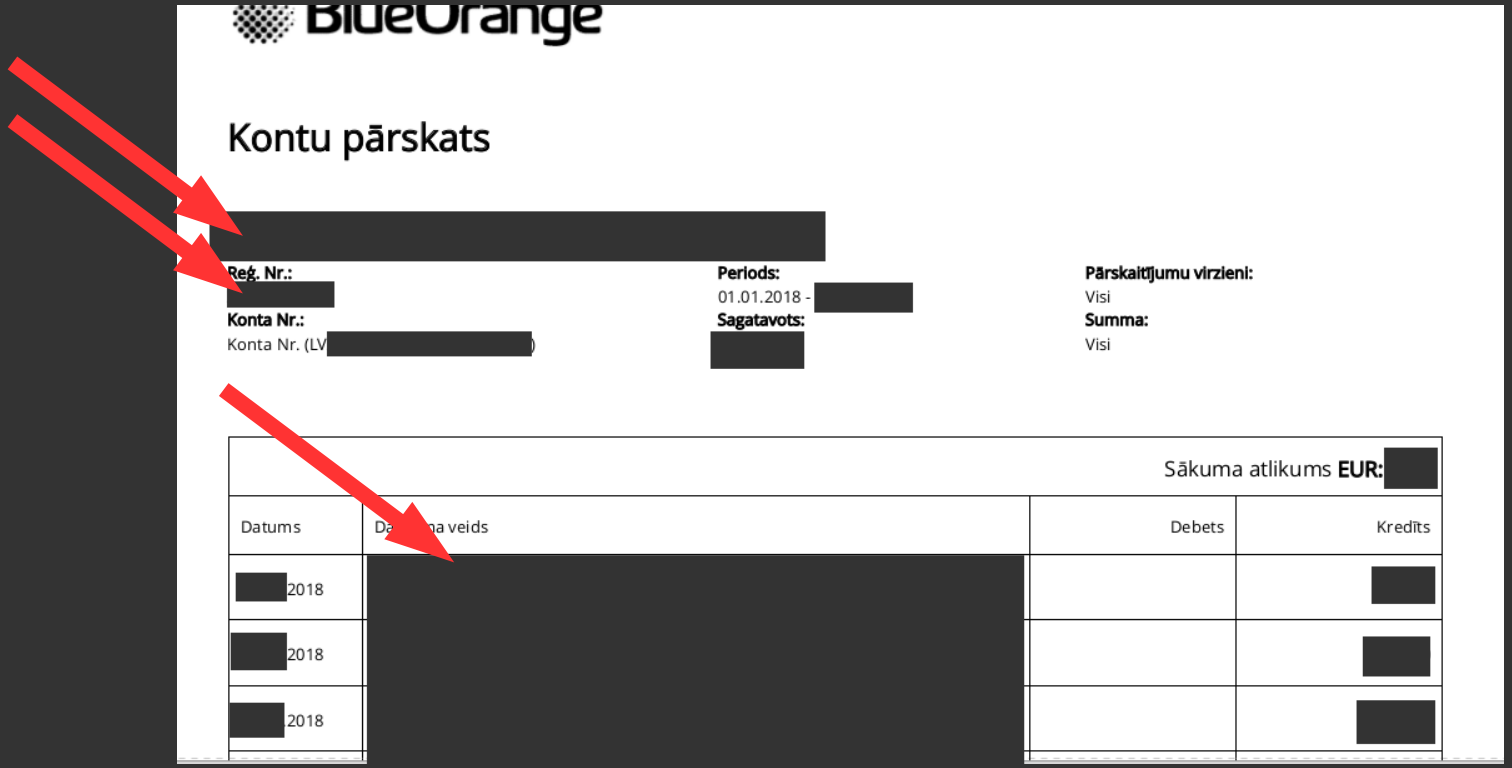
e-parakstīts valsts iestādes lēmums



paziņojums no gps sekošanas sistēmas



```
Sveiki, [redacted]<br />
Šis ir automātisks atgādinājuma e-pasts no Mapon.com sistēmas.<br />
<br />
Automašīna neatrodas objektā "[redacted]" laikā posmā
 - [redacted]<br />
<br />
<br />
<br />
www.mapon.com
```



BlueOrange

Kontu pārskats

[redacted]

Reģ. Nr.: [redacted]

Konta Nr.:
Konta Nr. (LV[redacted])

Periods:
01.01.2018 - [redacted]

Sagatavots: [redacted]

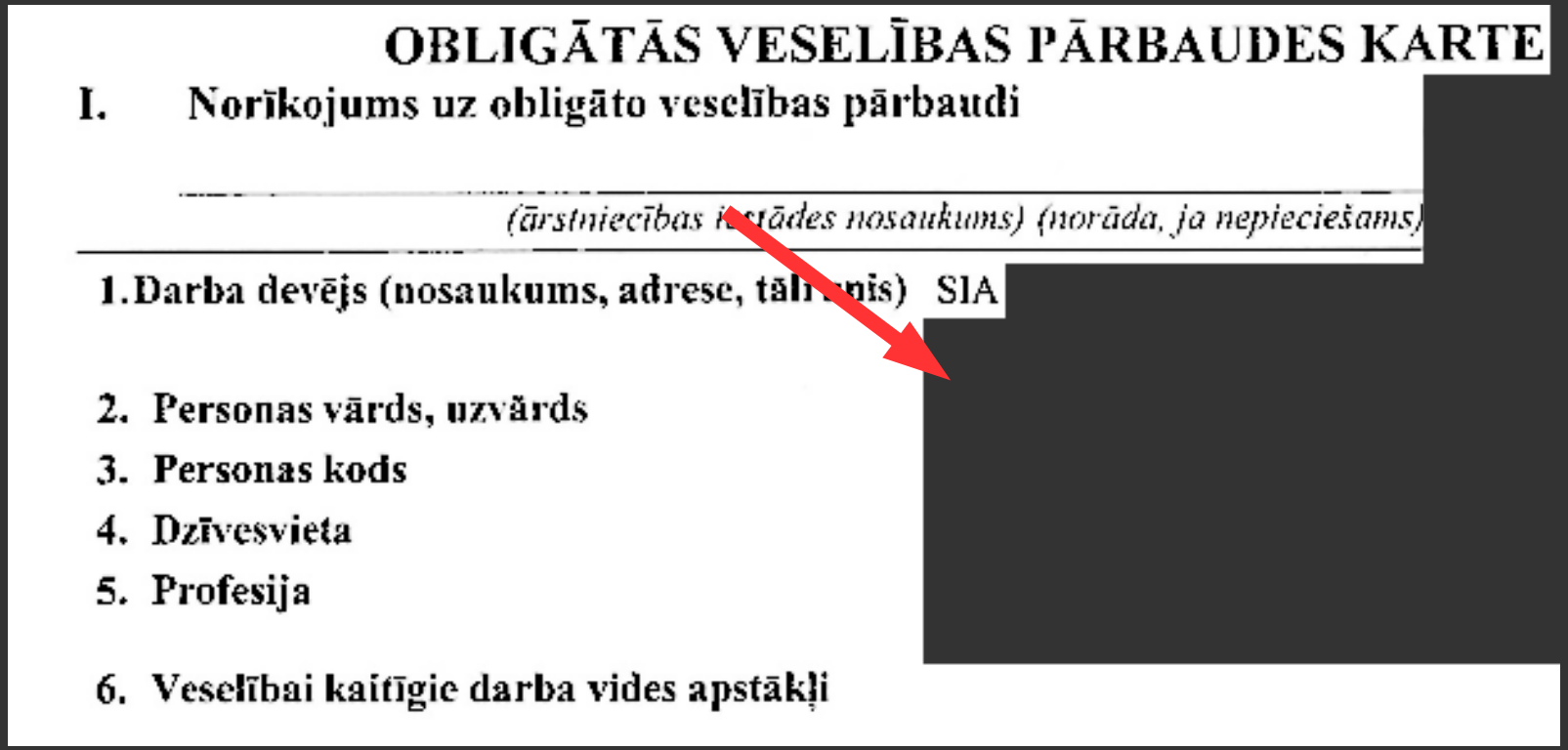
Pārskaitījumu virzieni:
Visi

Summa:
Visi

Sākuma atlikums **EUR:** [redacted]

Datums	Da[redacted]na veids	Debets	Kredīts
[redacted]2018			[redacted]
[redacted]2018			[redacted]
[redacted]2018			[redacted]

digitalizēta obligātās veselības pārbaudes karte



OBLIGĀTĀS VESELĪBAS PĀRBAUDES KARTE

I. Norīkojums uz obligāto veselības pārbaudi

(ārstniecības iestādes nosaukums) (norāda, ja nepieciešams)

1. Darba devējs (nosaukums, adrese, tālrunis) SIA

2. Personas vārds, uzvārds

3. Personas kods

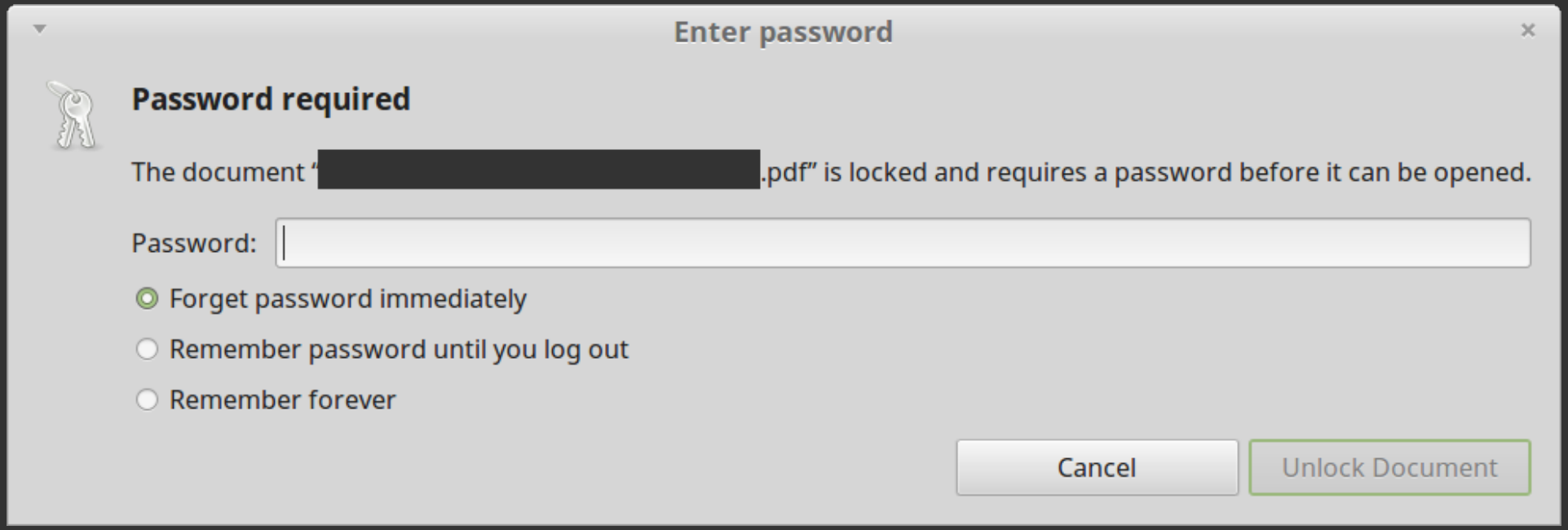
4. Dzīvesvieta

5. Profesija

6. Veselībai kaitīgie darba vides apstākļi

possible.lv

liels daudzums sensitīvu veselības datu (šifrēti)



liels daudzums sensitīvu veselības datu (šifrēti)

```
$ time pdfcrack

PDF version 1.4
Security Handler: Standard
V:
R:
P:
Length: 40
Encrypted Metadata: True
```

```
found user-password: '

real    0m1.201s
user    0m1.200s
sys     0m0.000s
```

possible.lv

trakums!
laiks kopsavilkumam

- Domēna īpašnieks apdraud
  - savus klientus un biznesa partnerus
  - darbiniekus, kas izmantojuši e-pasta adreses personisko kontu izveidei
    - paroles atjaunošana
  - finanšu, apdrošināšanas un sensitīvus veselības datus

- Uzbrucējs var iegūt kontroli pār
  - komercnoslēpumu
  - mājaslapas vecajām versijām
  - valsts sistēmām
  - informāciju par lietotāju parolēm
    - uzlaušanas monitoringa lapas
  - SSL sertifikātus topošajai tīmekļa vietnei

- Lietot divu faktoru autentifikāciju
- Apmaksāt domēna vārdus
  - skat., piem., hanzanet.lv
- Pretējā gadījumā:
  - apziņot visus – partnerus, darbiniekus un trešās puses, kas izmanto jūsu API
  - atsaistīt vecās e-pasta adreses no tiešsaistes kontiem
- Analizēt netipisku e-pasta serveru uzvedību; bloķēt tos

possible.lv

nu un kas, ja nepagarinu domēna vārdu?

Šo un citus pētījumus un prezentācijas meklē

http://kirils.org/

un

http://possible.lv/jaunumi/

06.12.2018.

"Esi drošs"

@KirilsSolovjovs