impact of domain name drop-catching on business security

possible.lv

Research carried out by:

- Kirils Solovjovs
- Mārtiņš Rozenbergs
- Toms Liepājnieks

- When was the last time your non-IT friend typed something
  - like this 172.217.18.78?
  - or this 2a00:1450:4016:809::200e?
- Yep, 100%-ε of non-malicious connections start with a DNS request

- Most domains aren't free
- Negligence:
  - forgot to renew domain
  - credit card expired
- Abandonment:
  - project is over
  - company merger
  - court order

- What attack vectors can be observed in real life?
- mid-2018
- .lv ccTLD
  - including IDN
- no phishing
- no active attacks

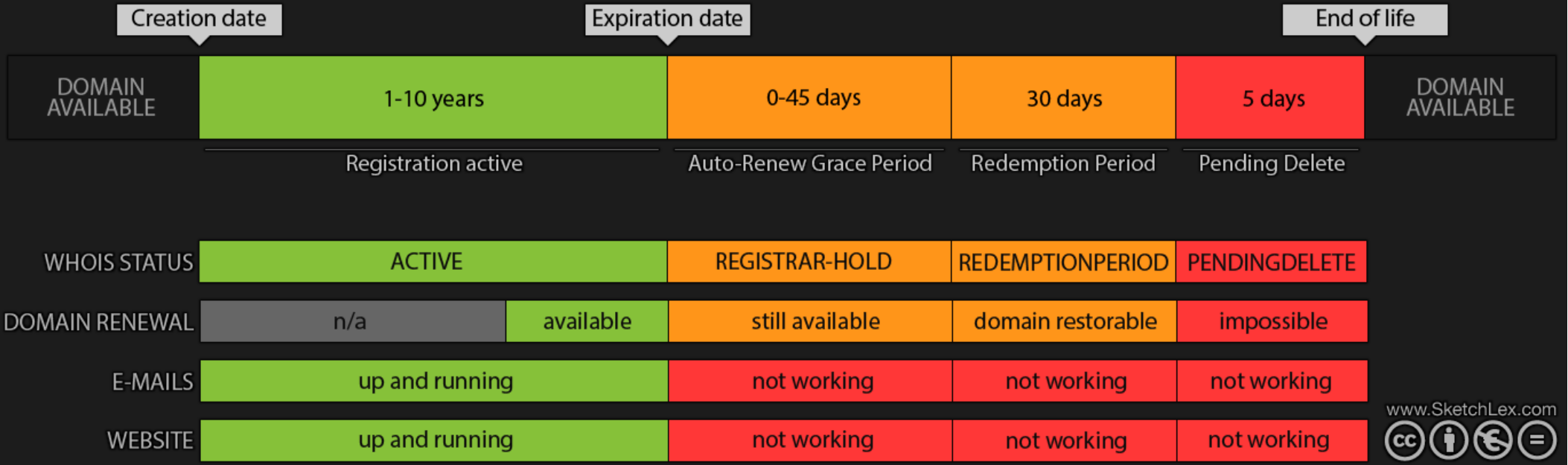
- quantitative and qualitative methods
- ftp, ssh, telnet, smtp, dns, http, pop3, imap, https, ~~rdp, vnc~~

- C. Healey. Domain tasting is taking over the internet as a result of ICANN's "Add Grace Period", 2007
- S. Hao, M. Thomas, V. Paxson, N. Feamster, C. Kreibich, C. Grier, S. Hollenbeck. Understanding the domain registration behavior of spammers, 2013
- G. Szathmari. Hacking law firms with abandoned domain names, 2018

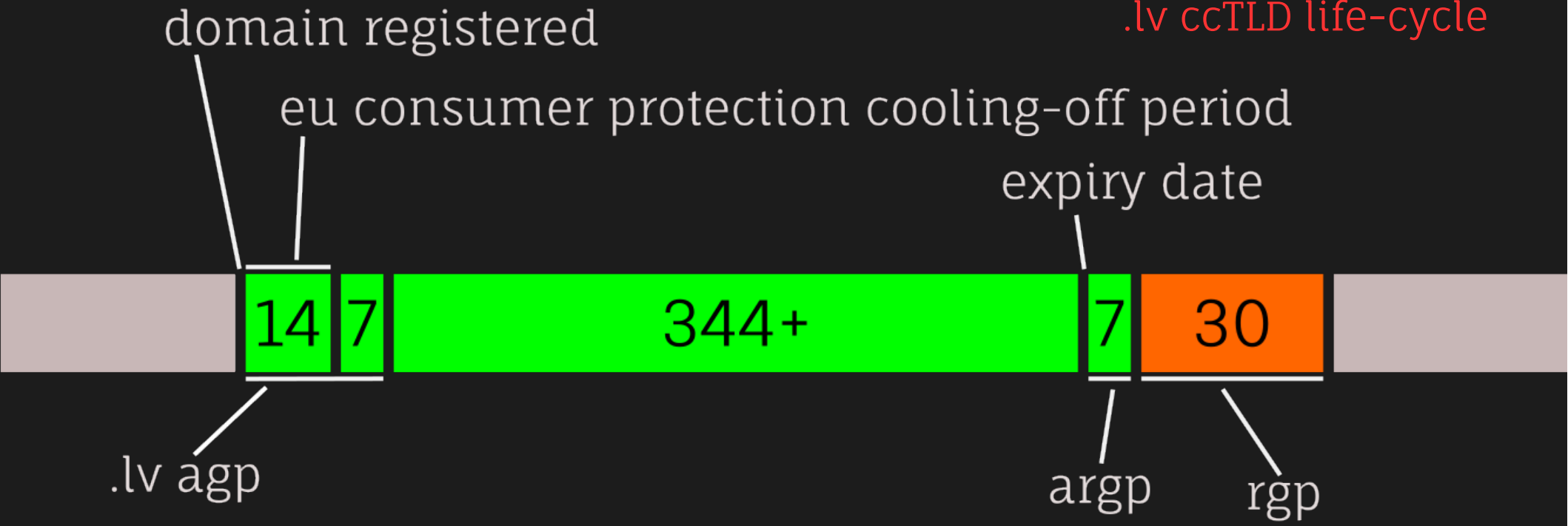
- Drop-catching

  re-registering a freshly expired domain name
- Domain back-orders
  - many registrar offer a service to catch the domain
  - some registries (.ru, .pl, ...) cooperate on that service
- Domain tasting
  - registering a domain name for the add-grace period

LIFE CYCLE OF A TYPICAL gTLD DOMAIN NAME



.lv ccTLD life-cycle



whois & zone working

whois working, zone empty

whois & zone empty, domain available

enough theory;
let's dig in!

- 180 domains on 1 IP
- Lots of scanners and other bad guys
- Bots vs humans

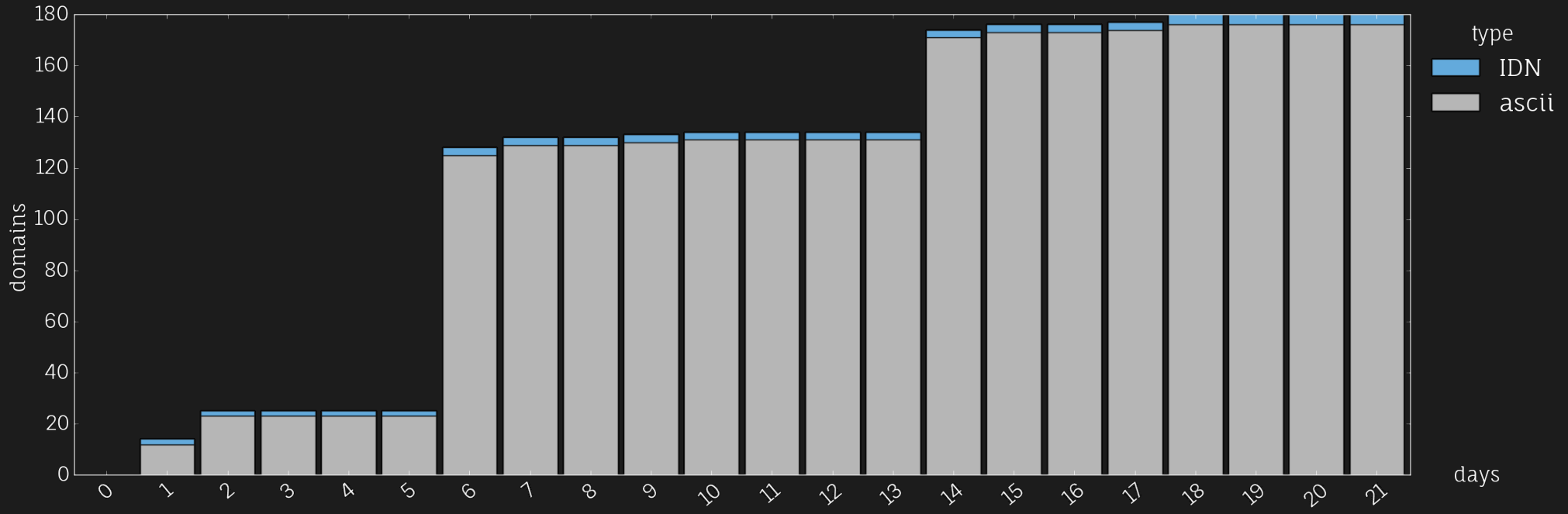
- custom DNS server based on twisted
- a bunch of honeypots:
  - mailoney, netwatch, imap-honey, malbait, RDPY, vnclowpot
- netfilter
- apache
  - custom PHP honeypot
- acme.sh
  + custom dns api
- custom .sh & .py

- Register recently expired domains that:
  - have search engine presence
  - relate to an existing company/person
  - are typos of popular domains
- Request SSL certificate for those domains ASAP

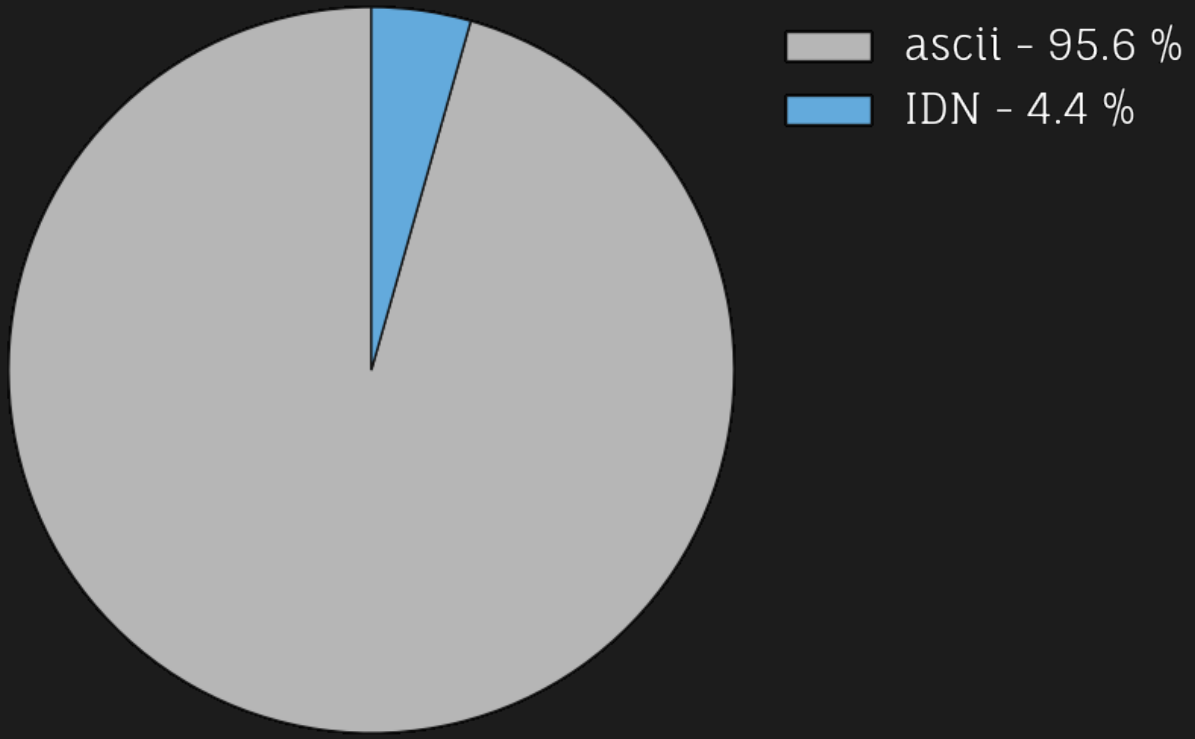
- Link DNS request logs with other request logs
  - heuristics: timing + AS
- Detect bots (web)
- Detect network scanners and bruteforcers
- Look at the remaining data in detail
  - qualitative analysis on e-mails and web requests
  - quantitative analysis on other protocols

yeah, yeah, yeah,
but have you got any data?

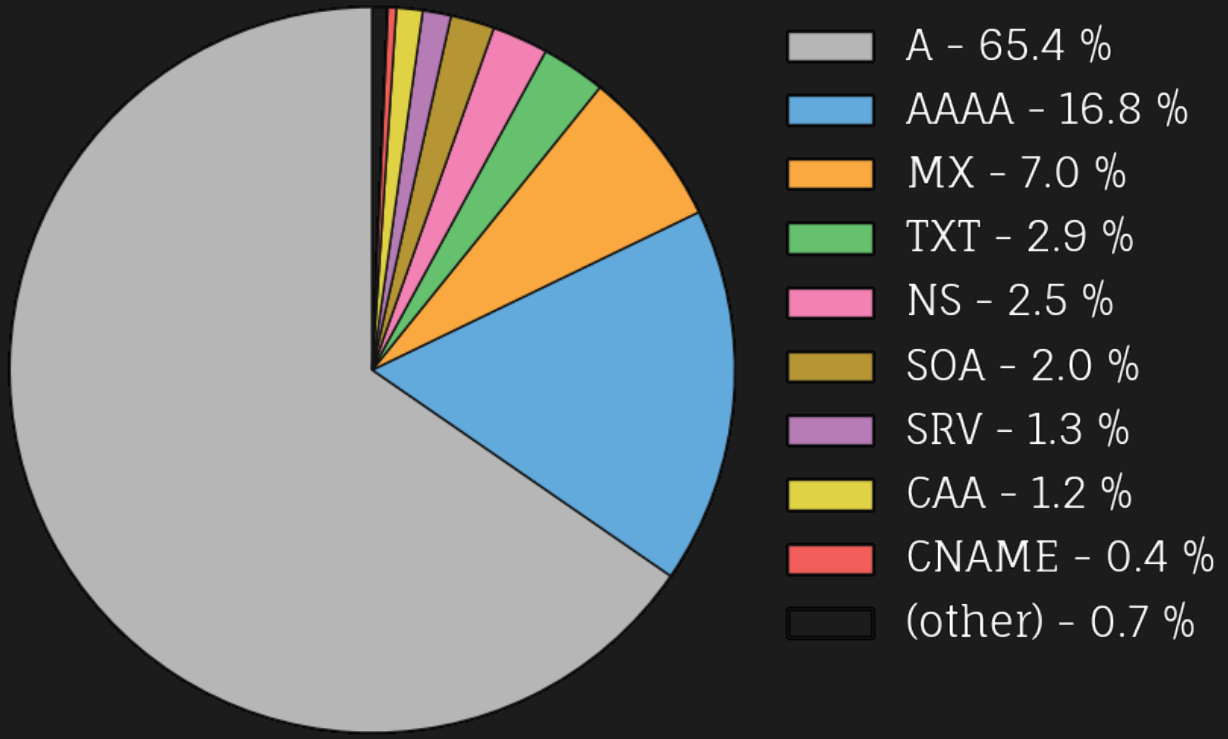
domains registered



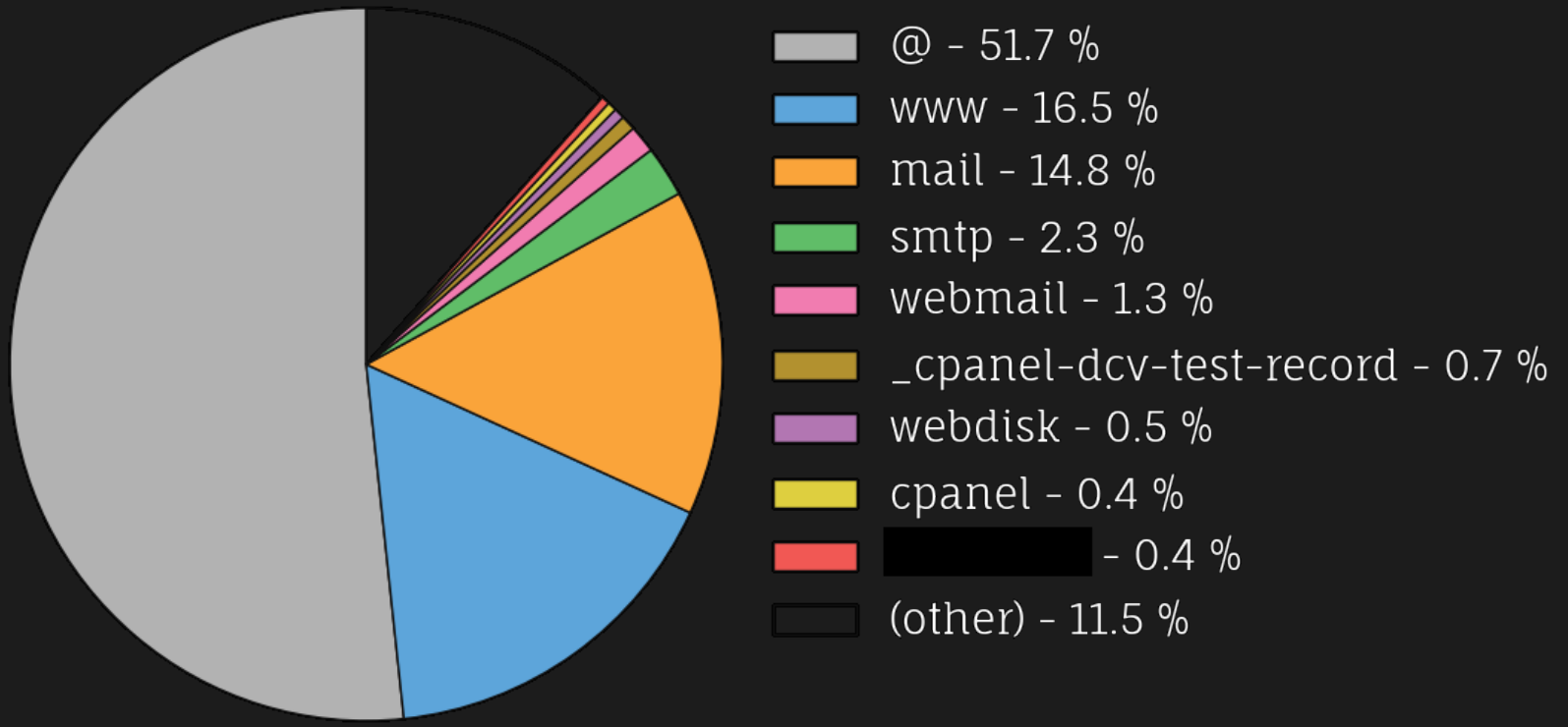
dns/requests (weighted)



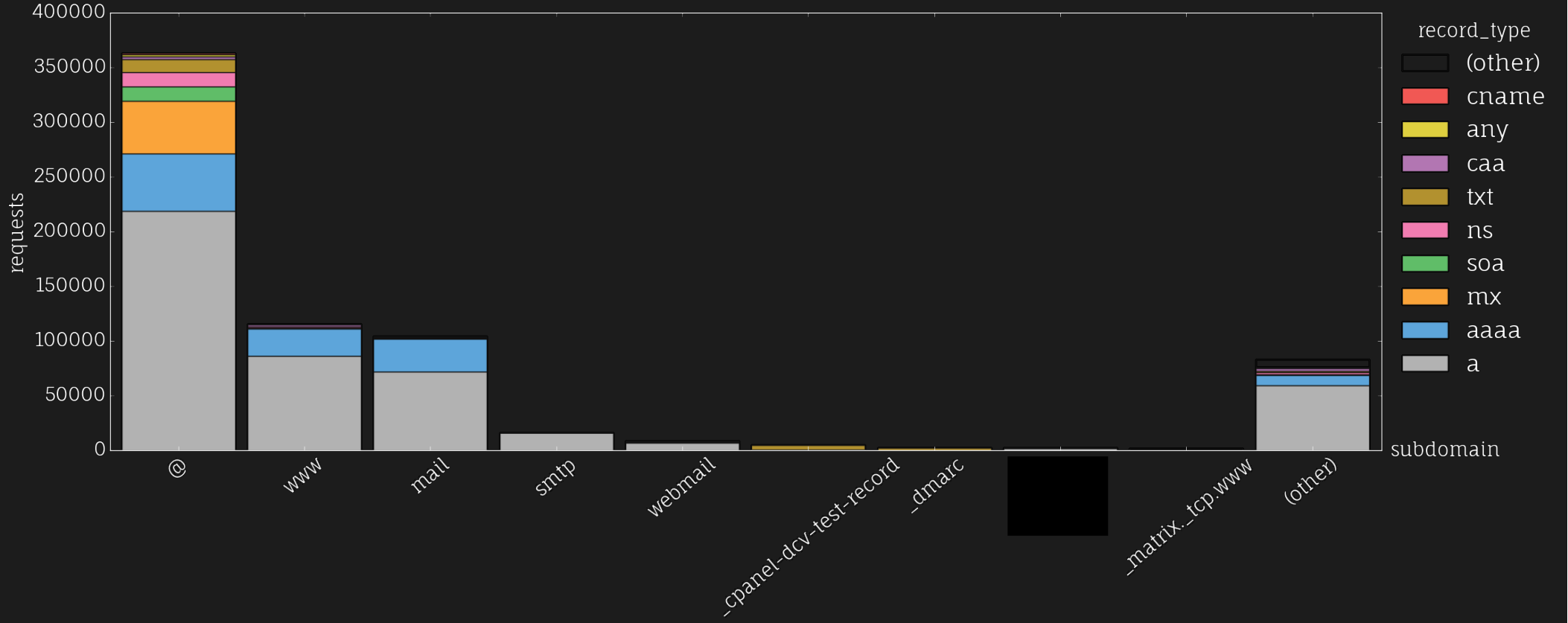
dns/record_types



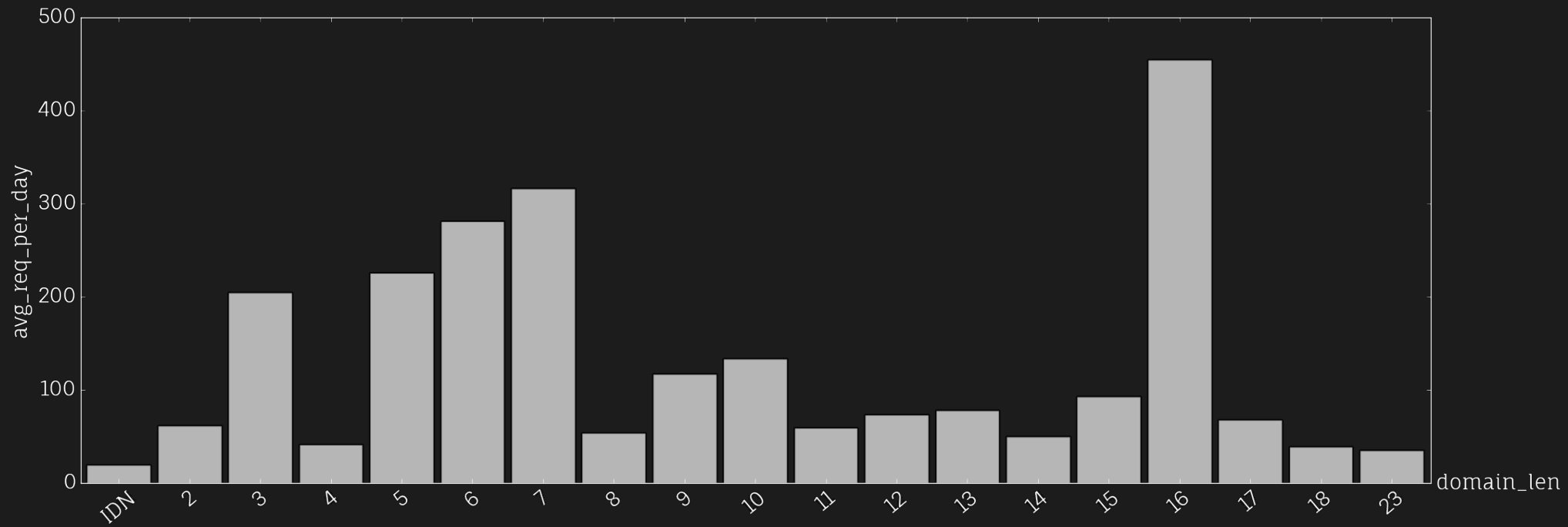
dns/subdomains



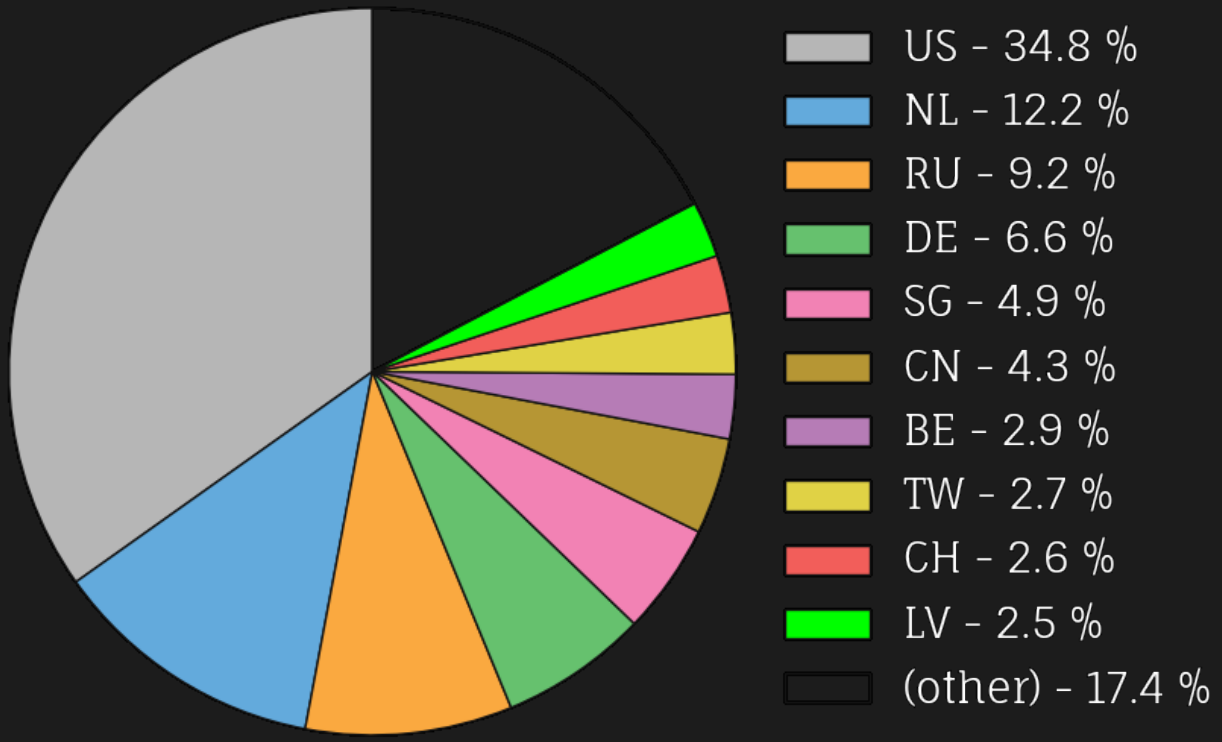
dns/subdomains/record_types



dns/avg_req_by_length (weighted)



dns/countries



Username:

1) [redacted]
2) changeme
3) webmaster
4) admin
5) root
6) test
7) clearvision
8) ubuntu
9) nagios
10) ftpuser

Password:

1) 1q2w3e4r
2) test
3) admin
4) 123456
5) 1q2w3e
6) 12345
7) test123
8) qwerty
9) q1w2e3
10) 1234

Username:

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

Password:

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

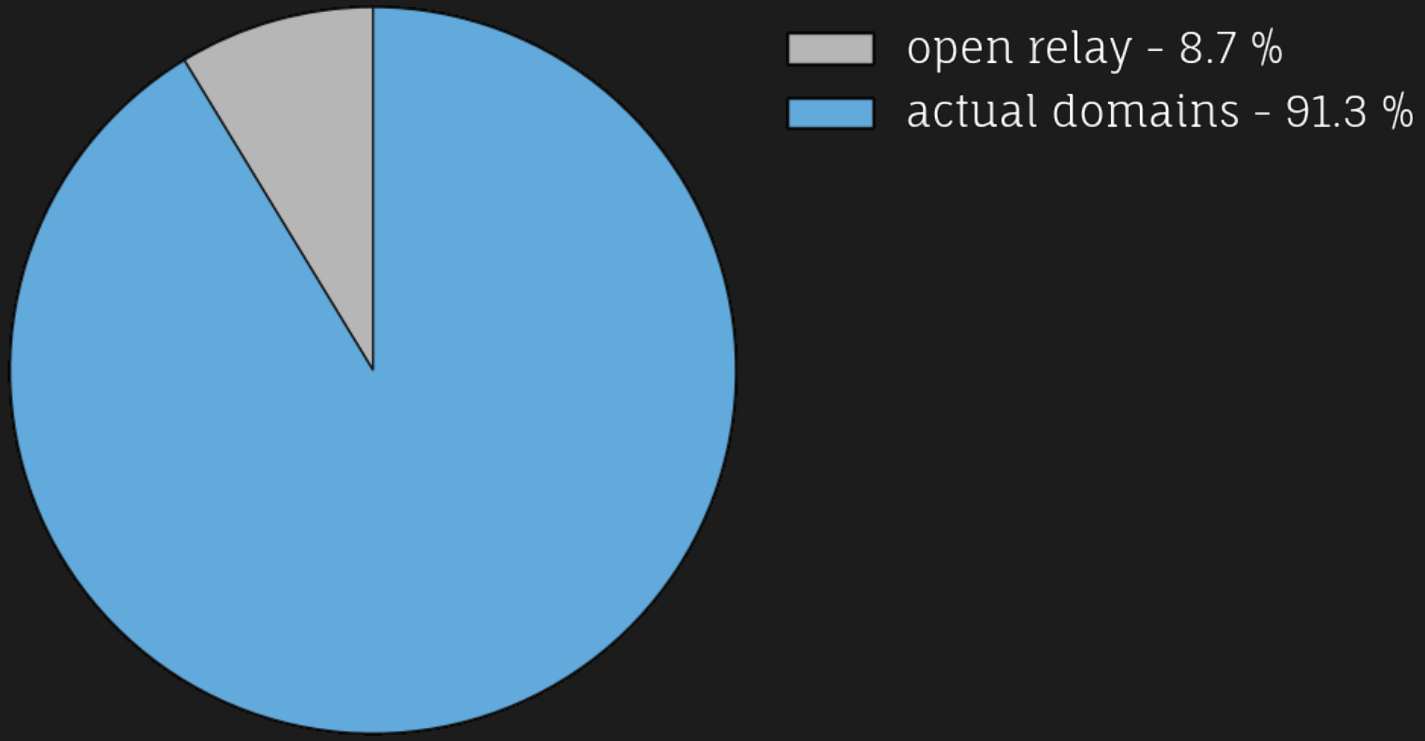
Username:

1) root
2) admin
3) guest
4) supervisor
5) default
6) support
7) user
8) ubnt
9) Administrator
10) 888888

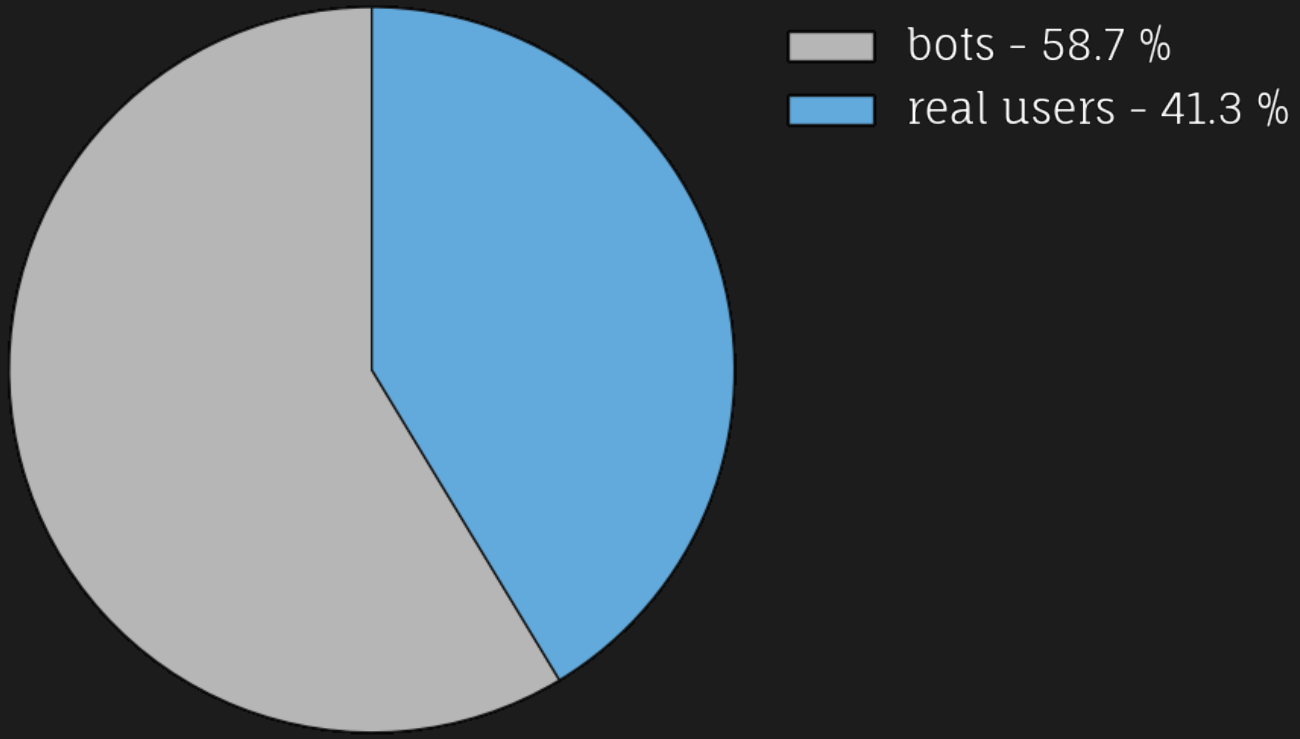
Password:

1) 1234
2) admin
3) 12345
4) password
5) 123456
6) 7ujMko0admin
7) 5up
8) 888888
9) aquario
10) 54321

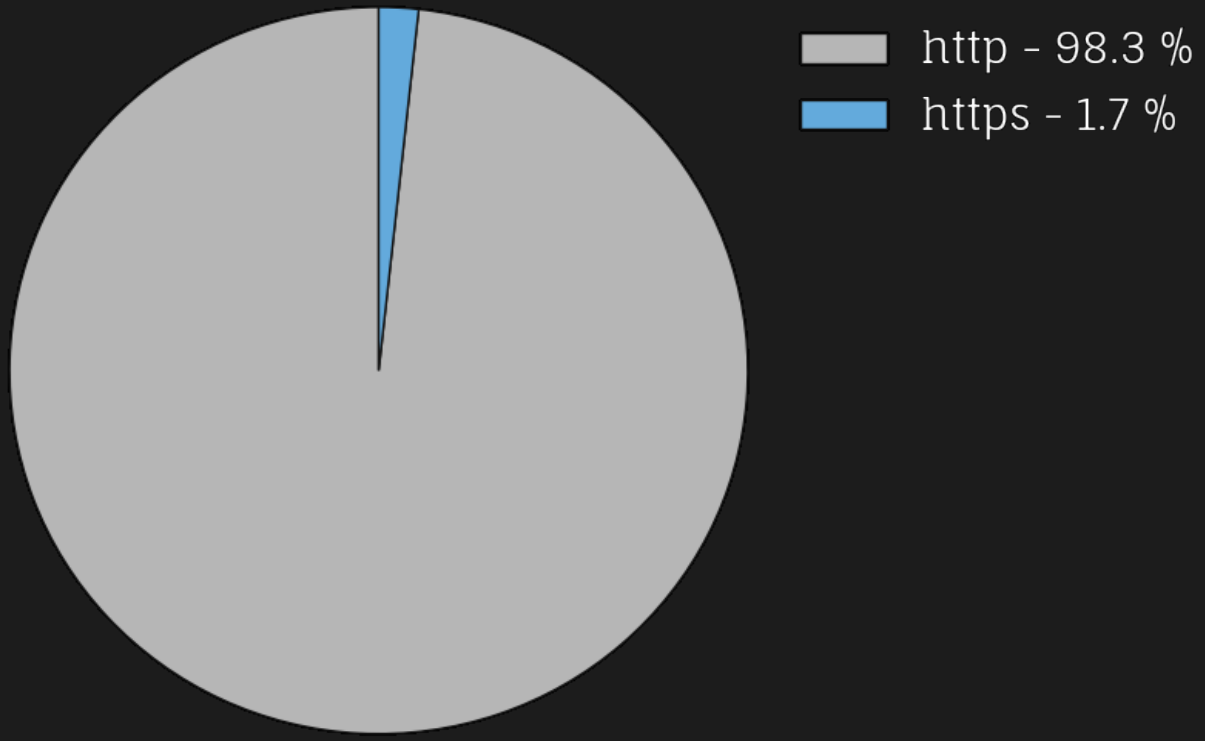
mail/open_relay_attempts



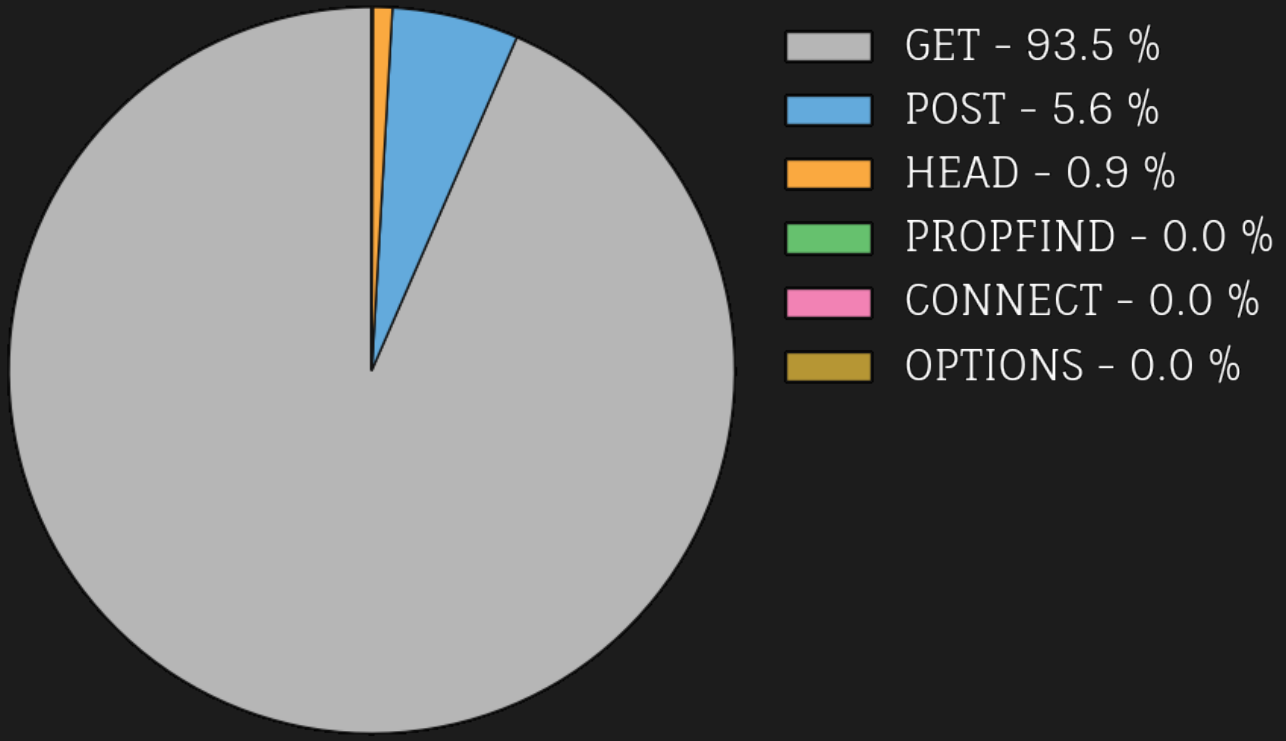
web/requests



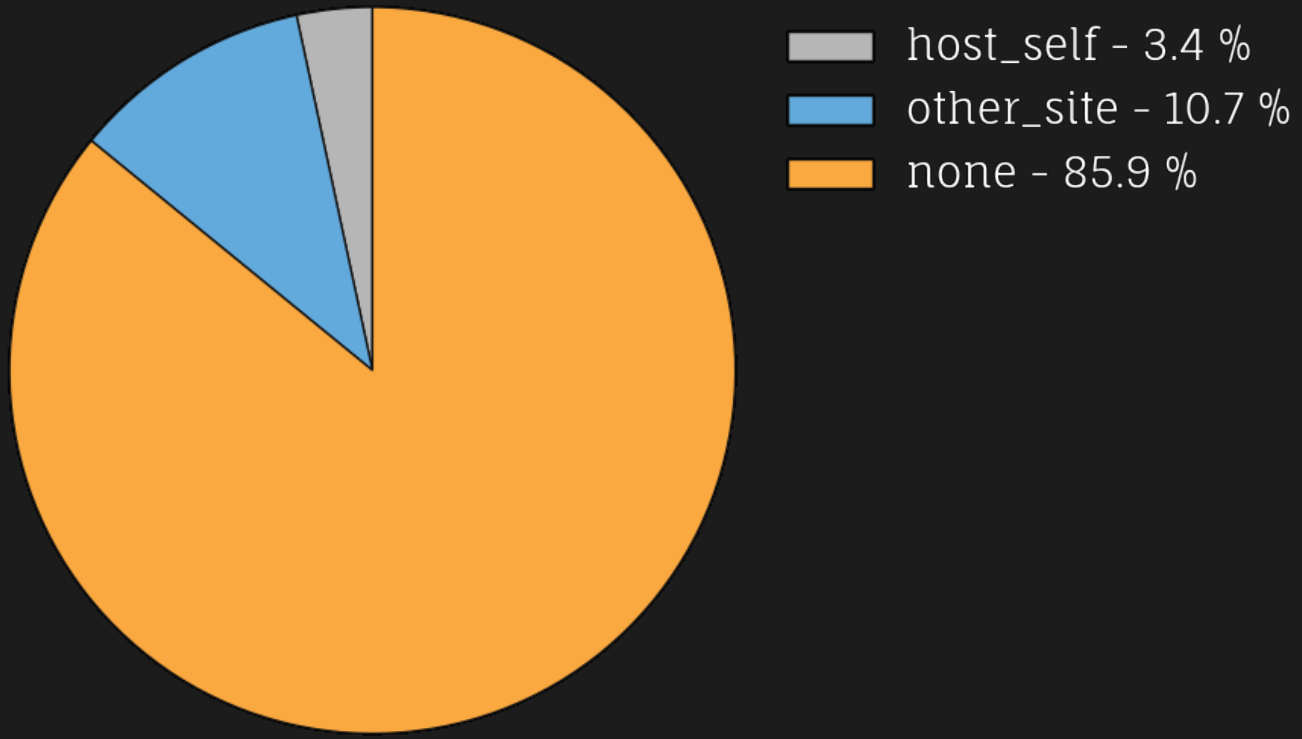
enough of looking at bad guys;
from now on — only legit data

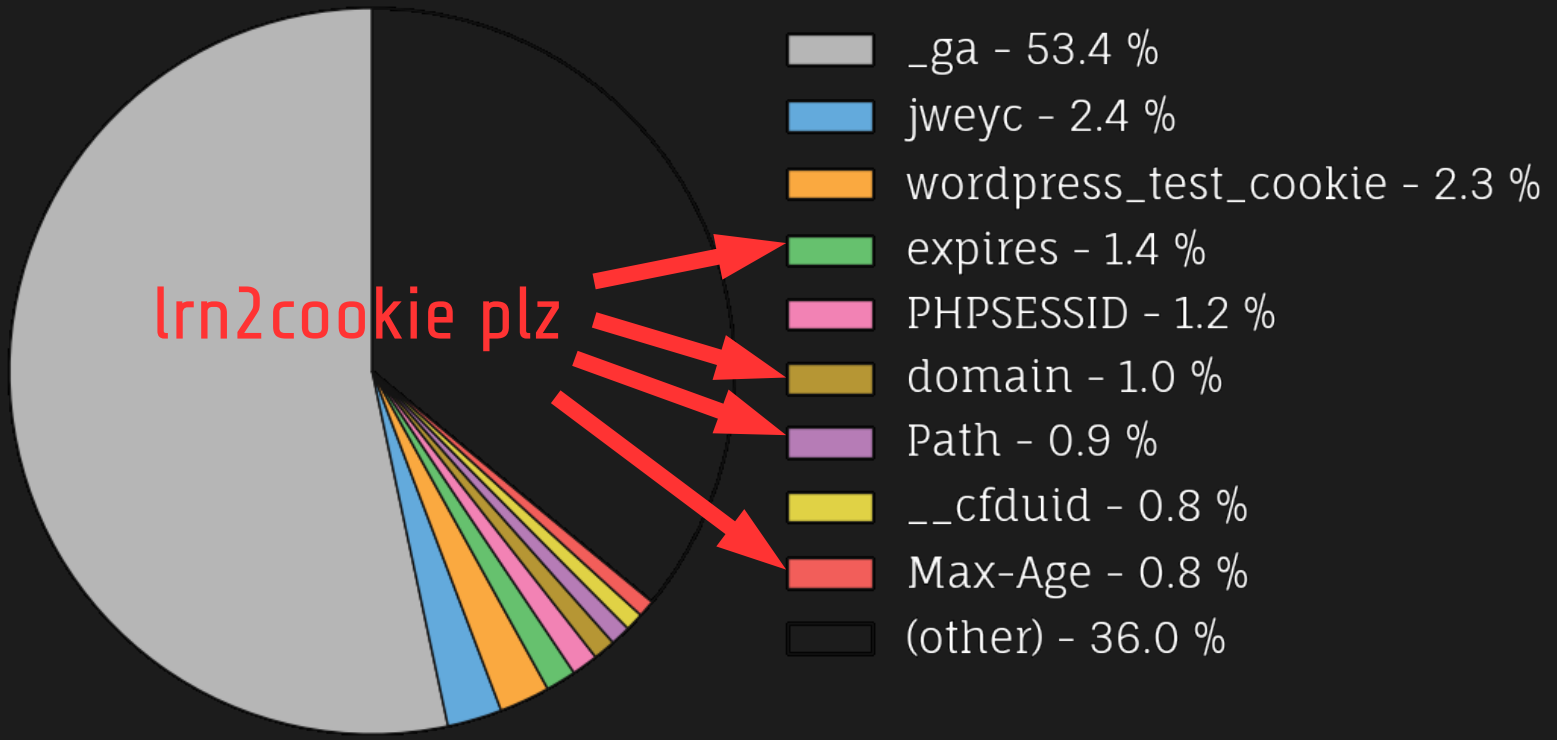

http - 98.3 %
https - 1.7 %

web/methods

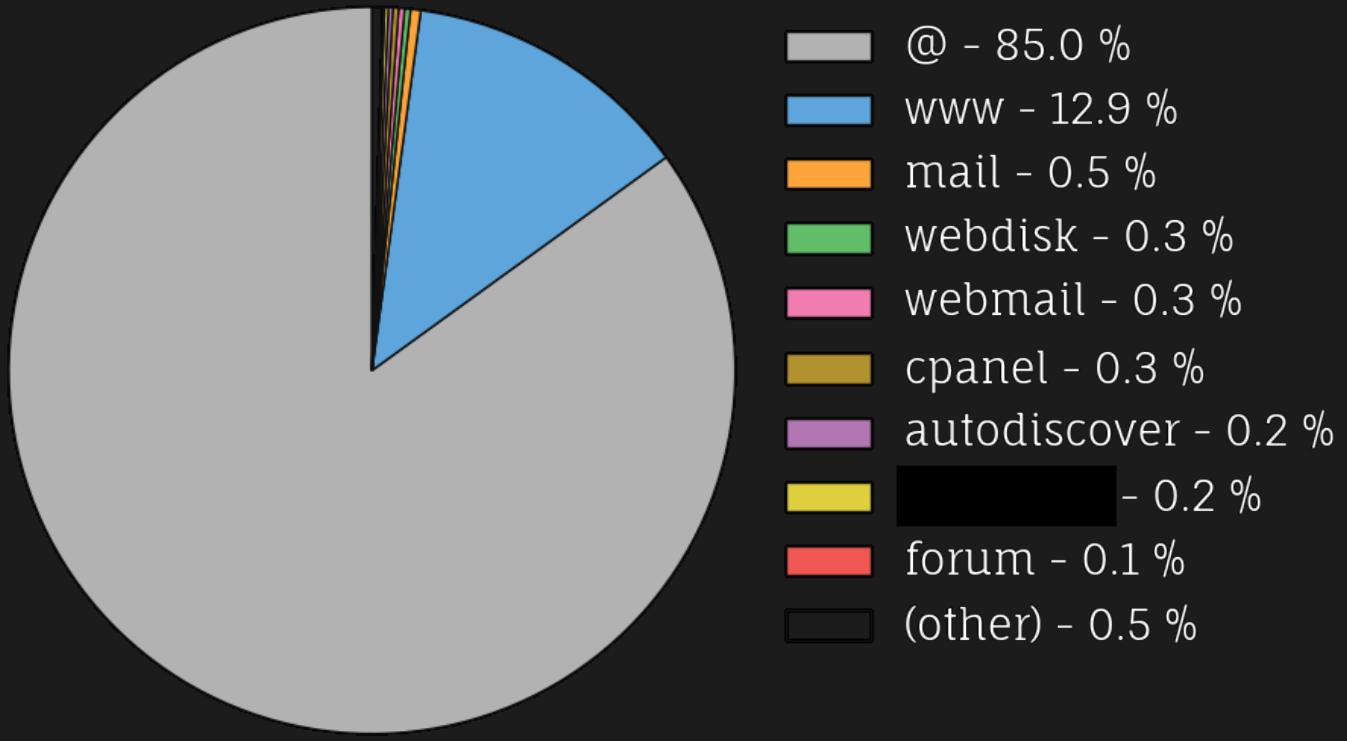


web/referrers

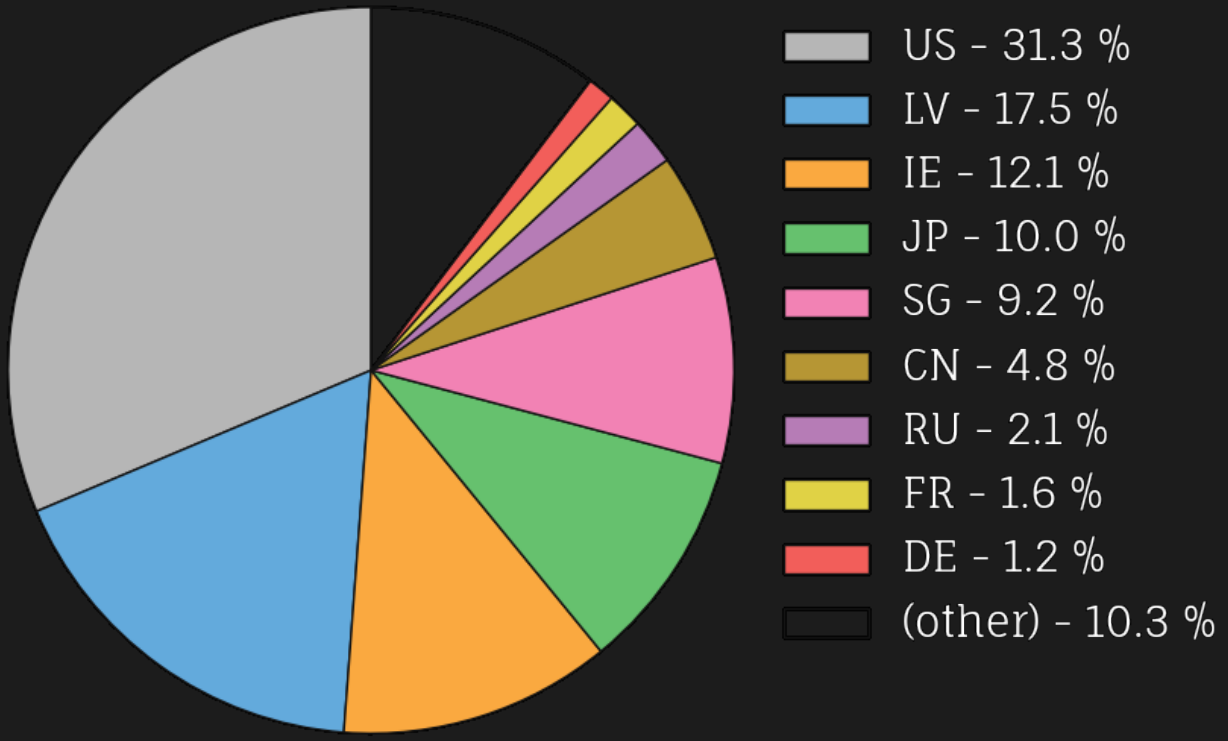



lrn2cookie plz
_ga - 53.4 %
jweyc - 2.4 %
wordpress_test_cookie - 2.3 %
expires - 1.4 %
PHPSESSID - 1.2 %
domain - 1.0 %
Path - 0.9 %
__cfduid - 0.8 %
Max-Age - 0.8 %
(other) - 36.0 %

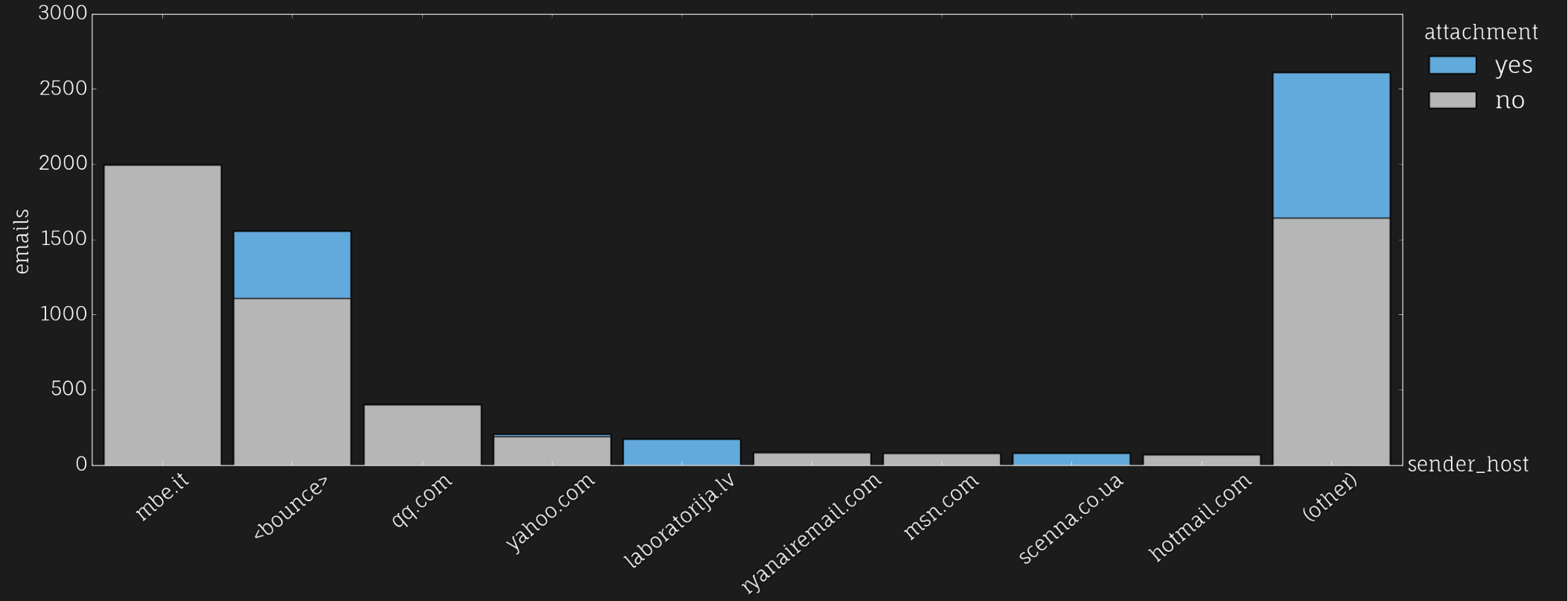
web/subdomains



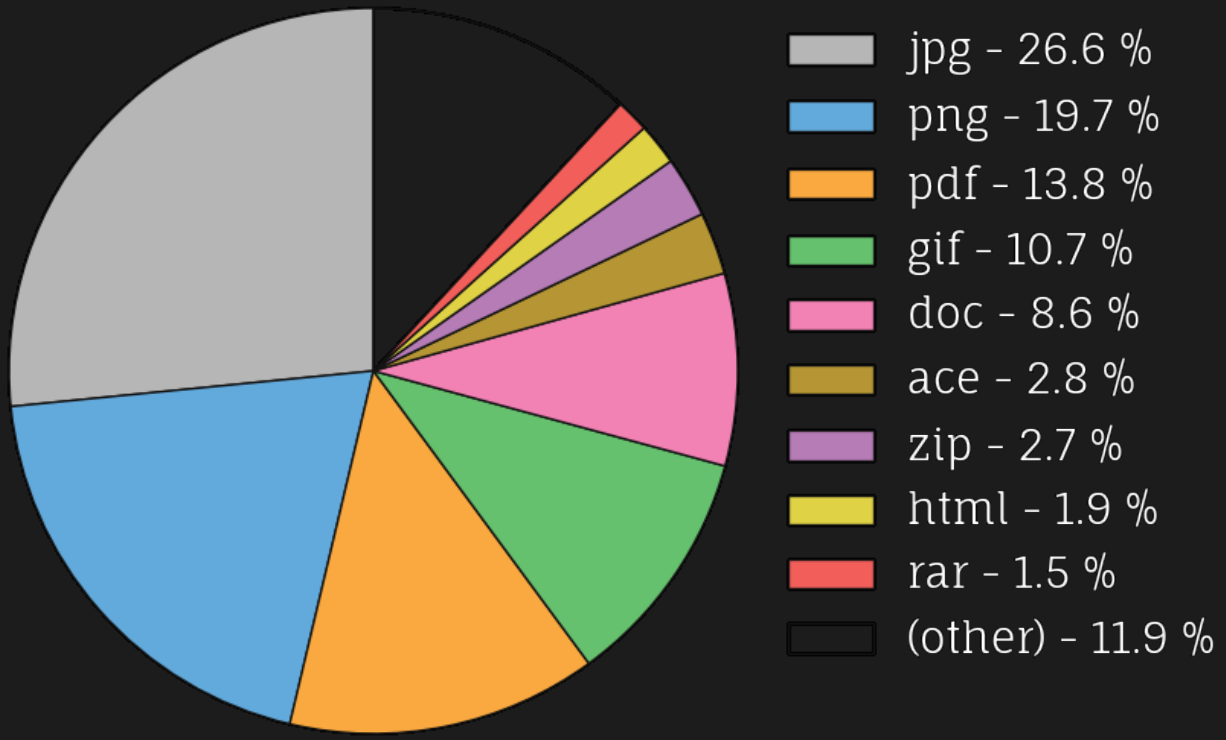
web/countries



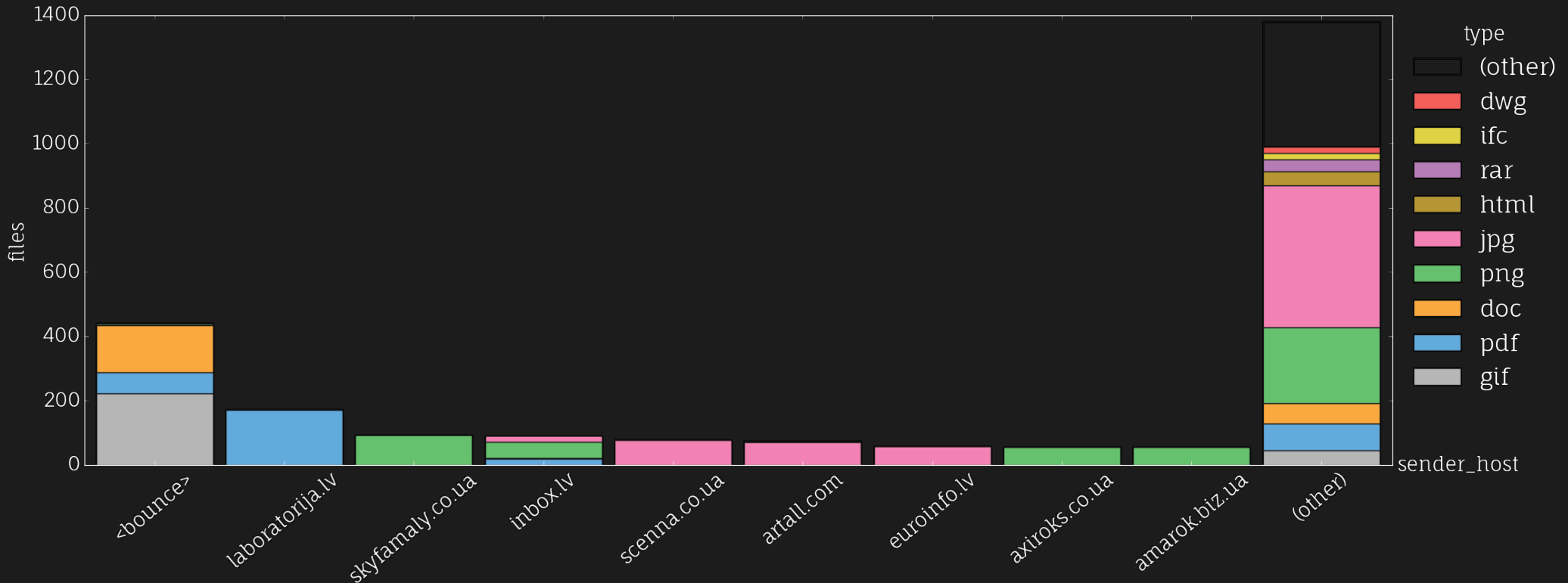
mail/sender_domains/attachments



mail/attachment_types

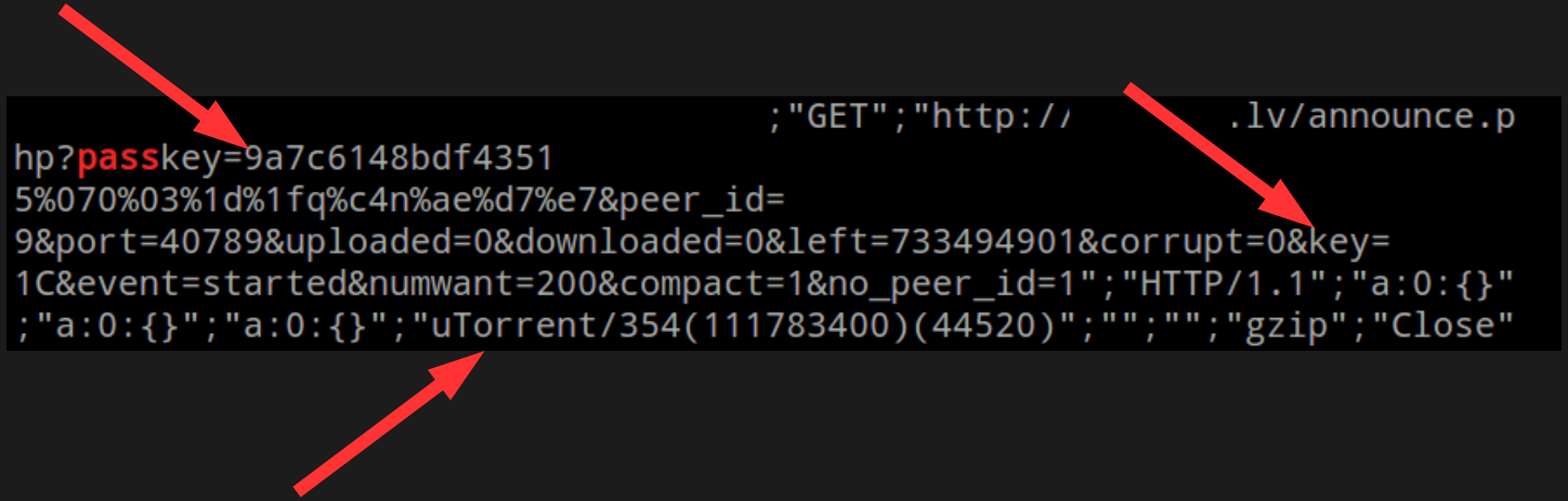


mail/sender_domains/attachment_types

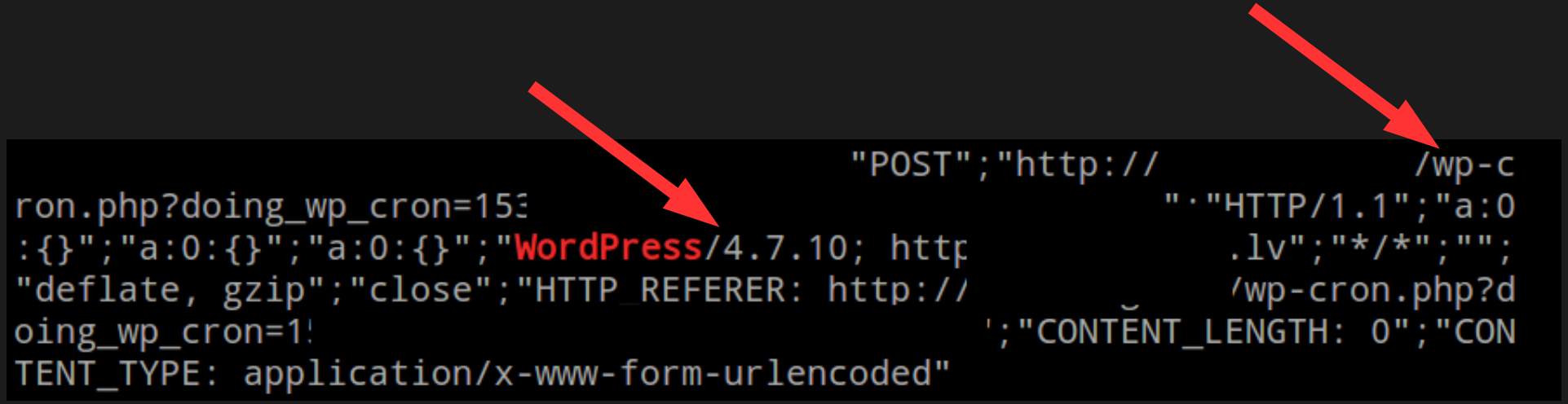


I think it's about enough of this;
let's look at some qualitative data

a torrent tracker

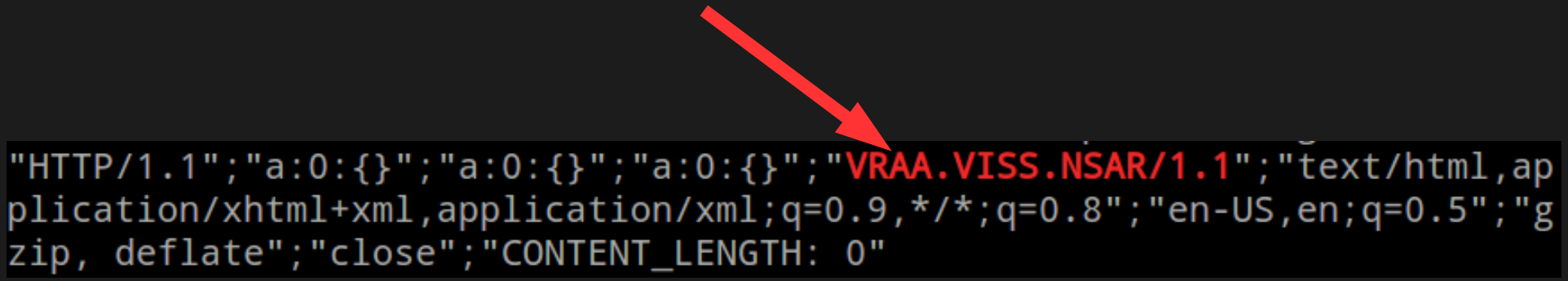


cron requests from abandoned wordpress instances

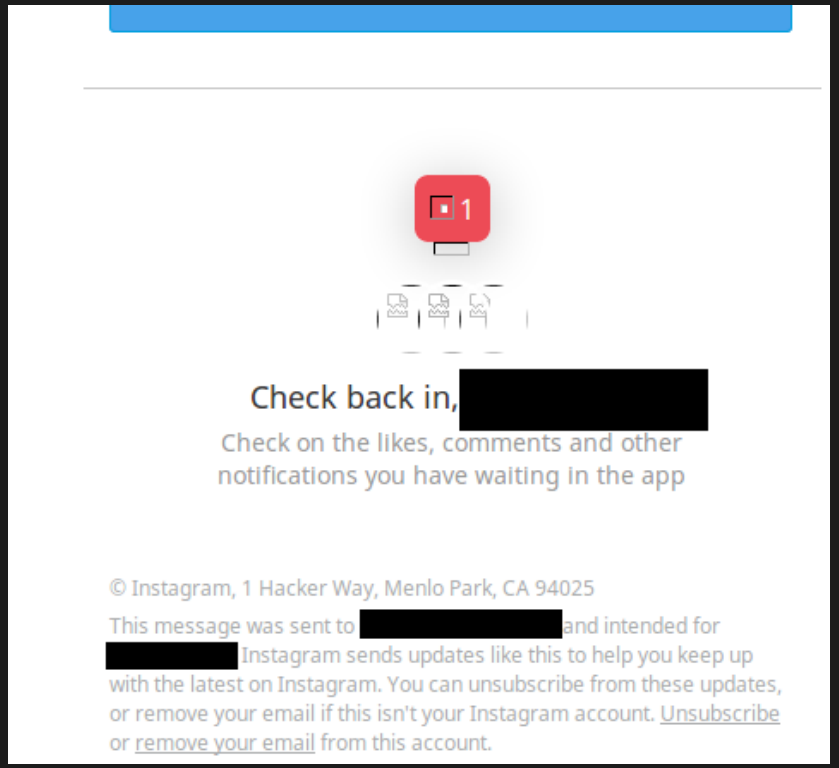


embedded HTML elements from .gov.lv

inter-connector of e-government systems



notifications from a social network

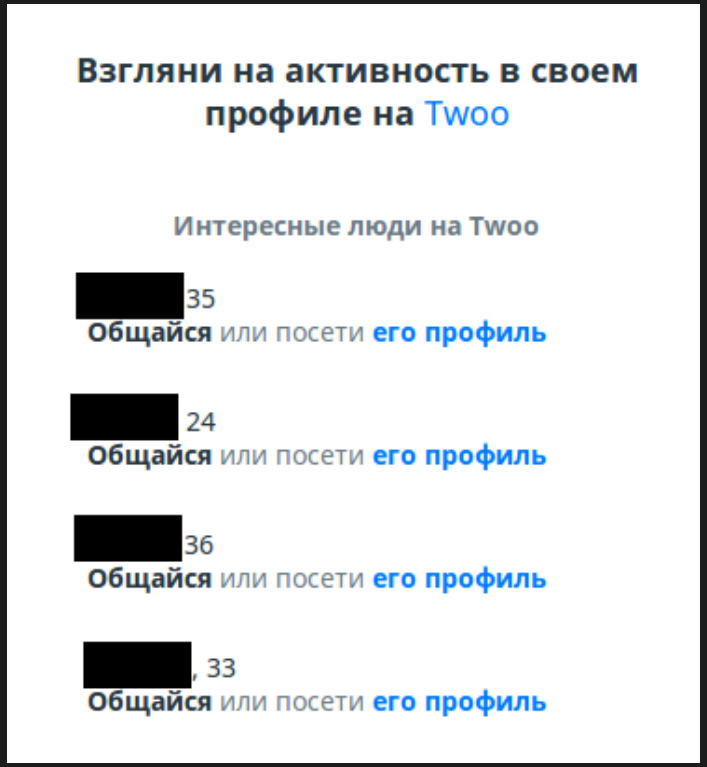



```
no-reply@mail.instagram.com_153
no-reply@mail.instagram.com_153
no-reply@mail.instagram.com_153
no-reply@mail.instagram.com_153
no-reply@mail.instagram.com_153
no-reply@mail.instagram.com_153
```

notification from a latvian social network

Tu saņēmi šo e-pastu, jo esi izveidojis draugiem.lv lapu. Ja turpmāk nevēlies saņemt šādus e-pasta sūtījumus, vari no tiem atteikties katras draugiem.lv lapas uzstādījumos. "Manas lapas rīki -> Profila informācija -> Paziņojumi uz e-pastu".
Ja vēlies uzreiz atteikties no šī e-pasta saņemšanas par visām lapām, kurām ir piesaistīts Tavs e-pasts, tad dodies uz šo saiti.

notification from a belgian social network



group reservation for a hotel

CITY WEST
HOTEL RESTAURANT EVENTS

[redacted]

E-Mail: [redacted]

[redacted]

Confirmation

Dear Mrs. [redacted]

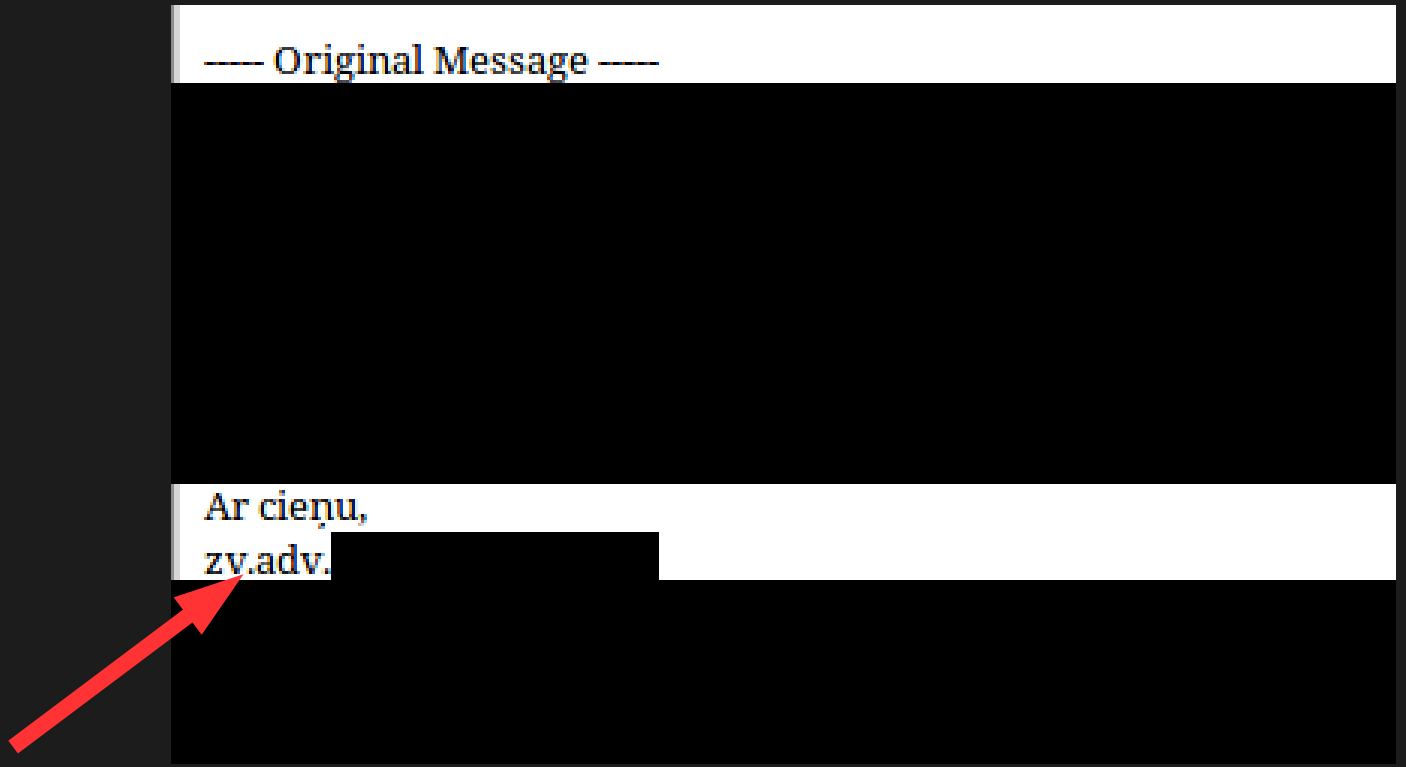
Thank you for your interest in the **CITY** WEST **HOTEL RESTAURANT EVENTS**. For the stay in our hotel we confirm the following:

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.	

e-mail from a lawyer



message from state revenue service

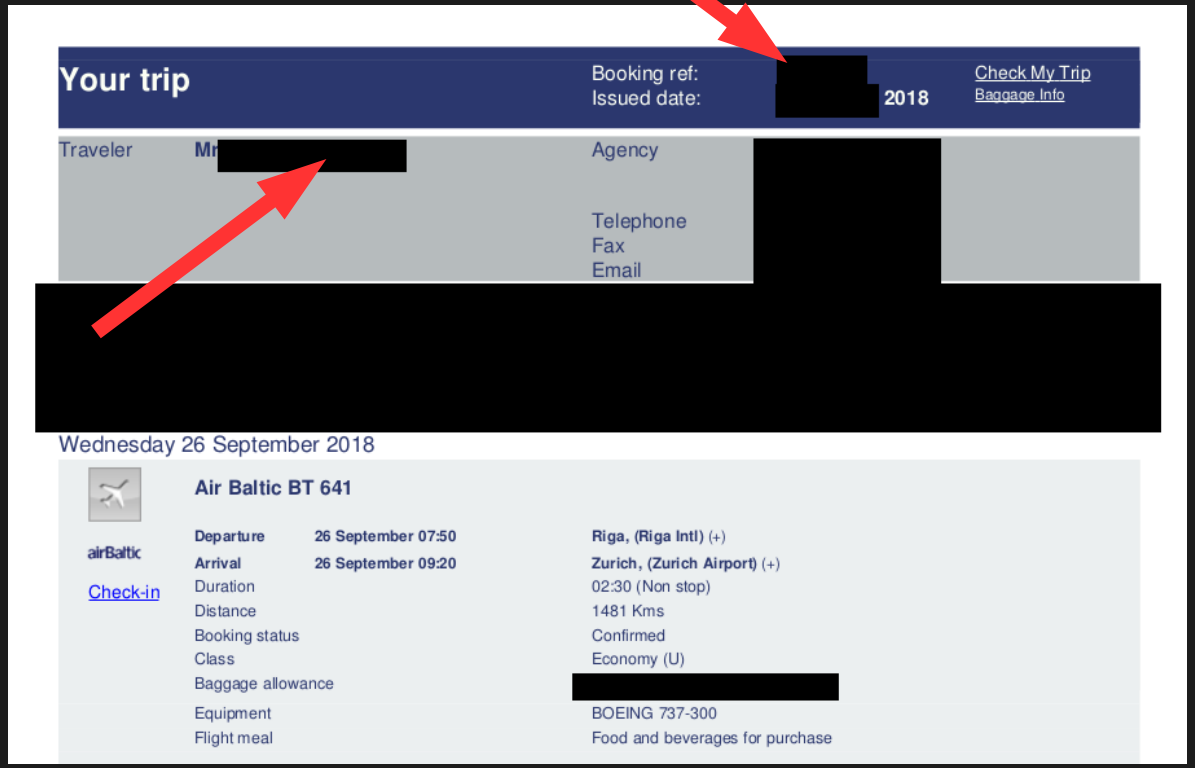
Informācija no Valsts ieņēmumu dienesta

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.

flight reservation



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

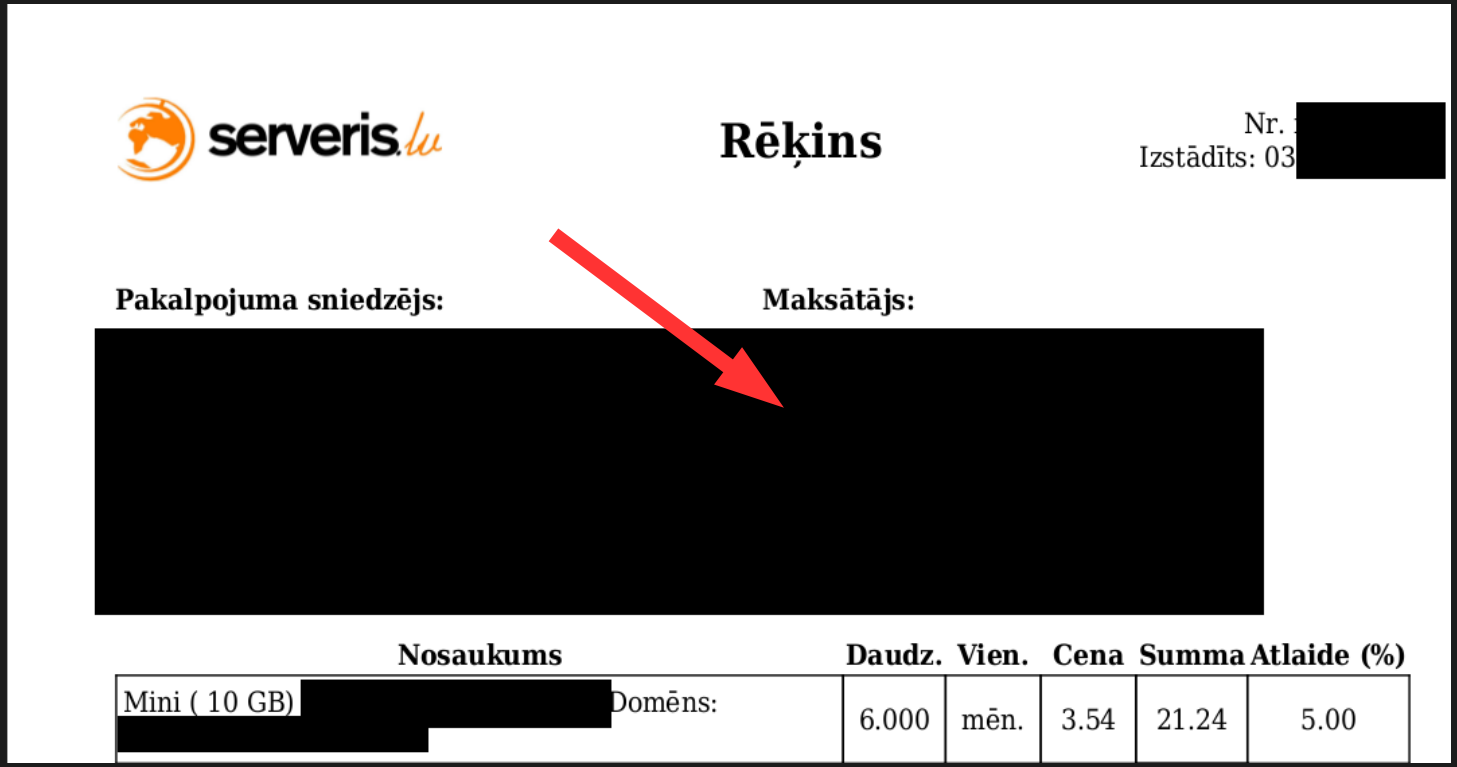
Air Baltic BT 641

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

bill with a lot of private data



serveris.lv

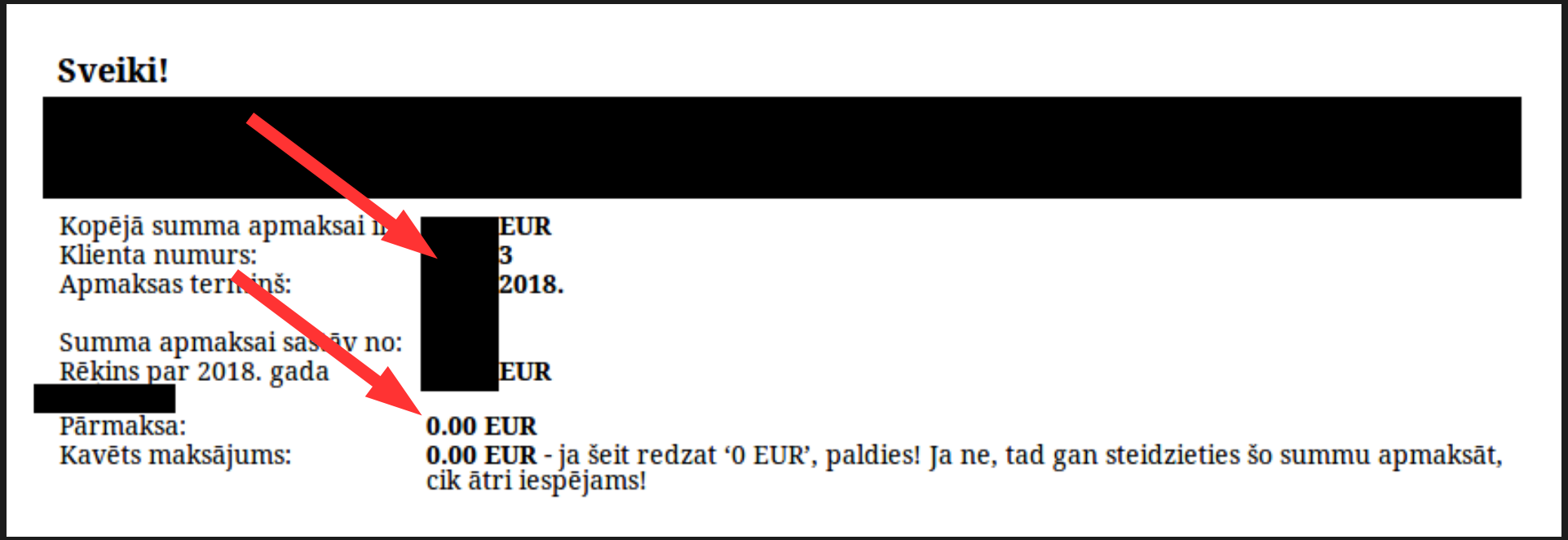
Rēķins

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



Sveiki!

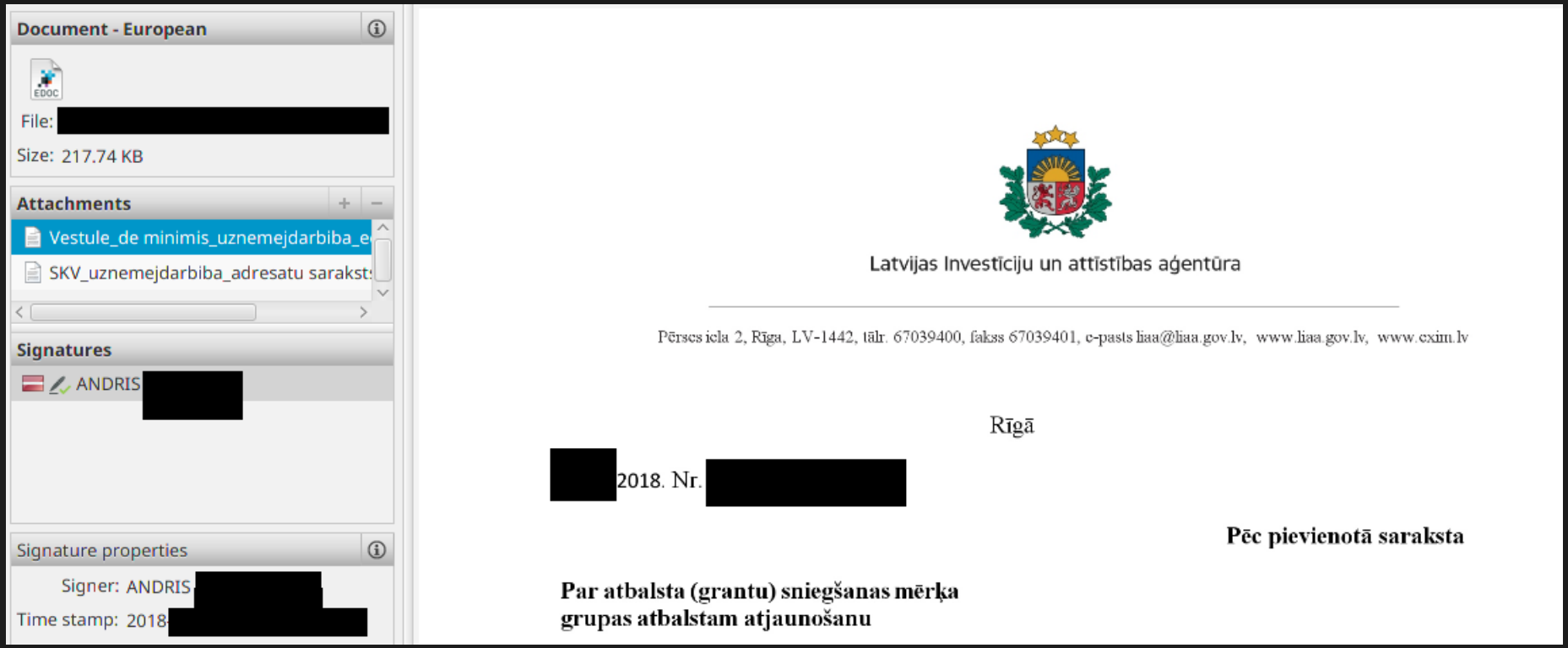
[redacted]

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

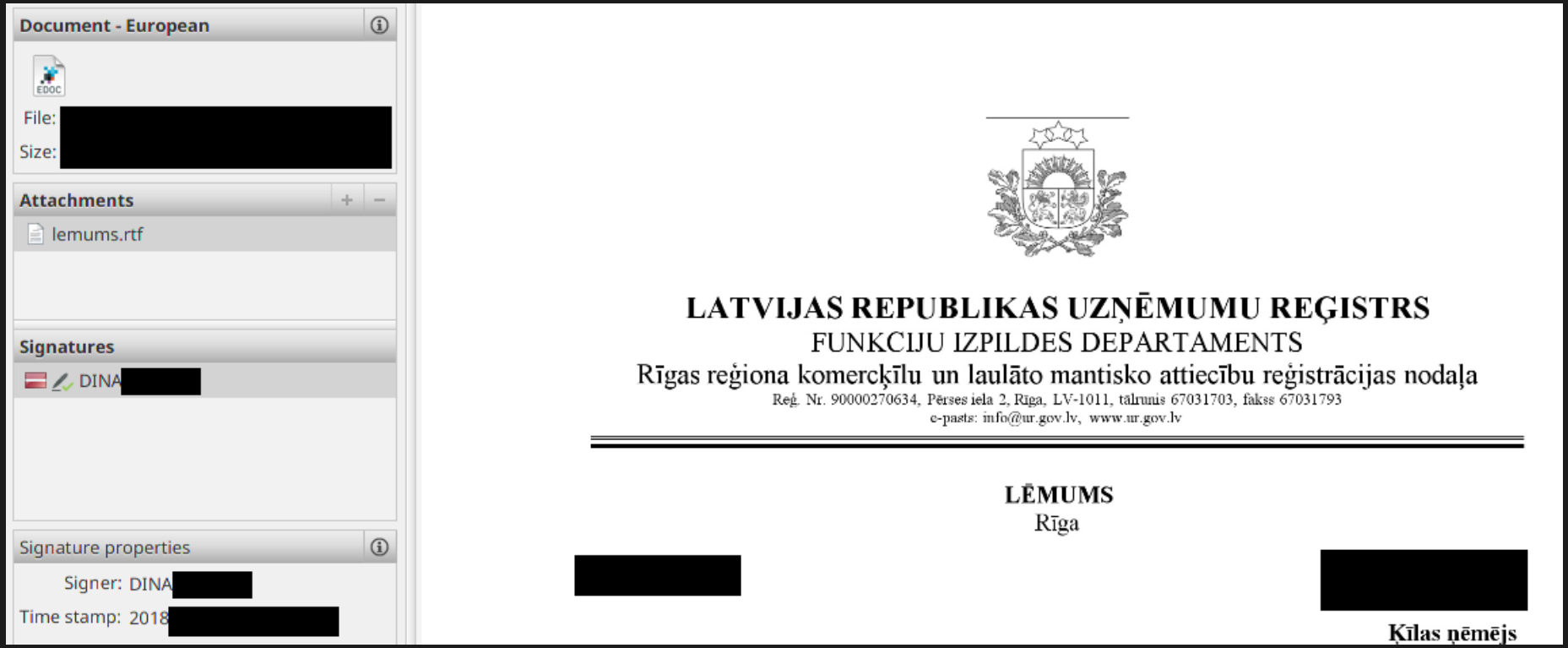
Summa apmaksai sastāv no:
Rēkins par 2018. gada [redacted] **EUR**

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!

electronically signed letter from the government

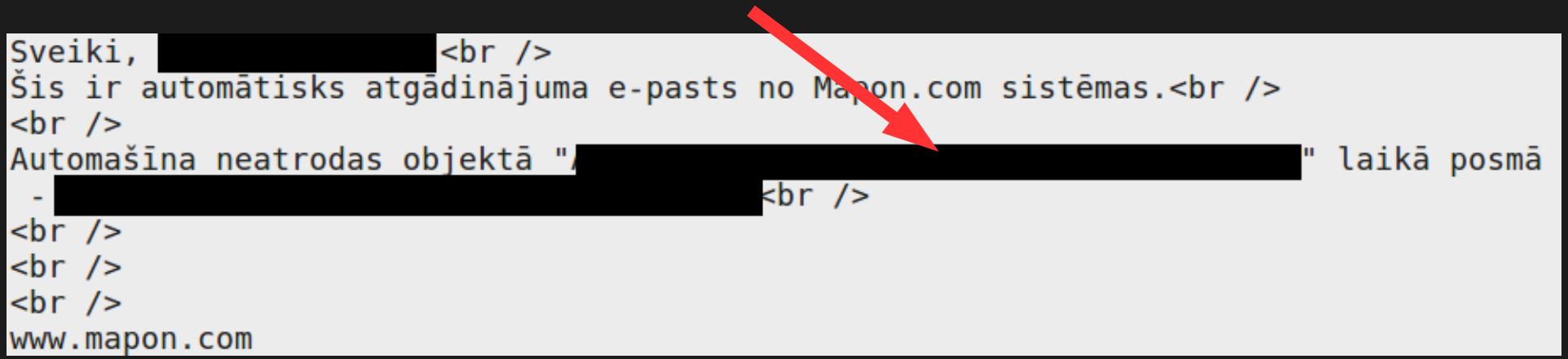


officially binding electronically signed government decision



#BalCCon2k18 http://kirils.org @KirilsSolovjovs

GPS tracking alert on a car



```
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
```

full bank statement

BlueOrange

Kontu pārskats

[redacted]

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

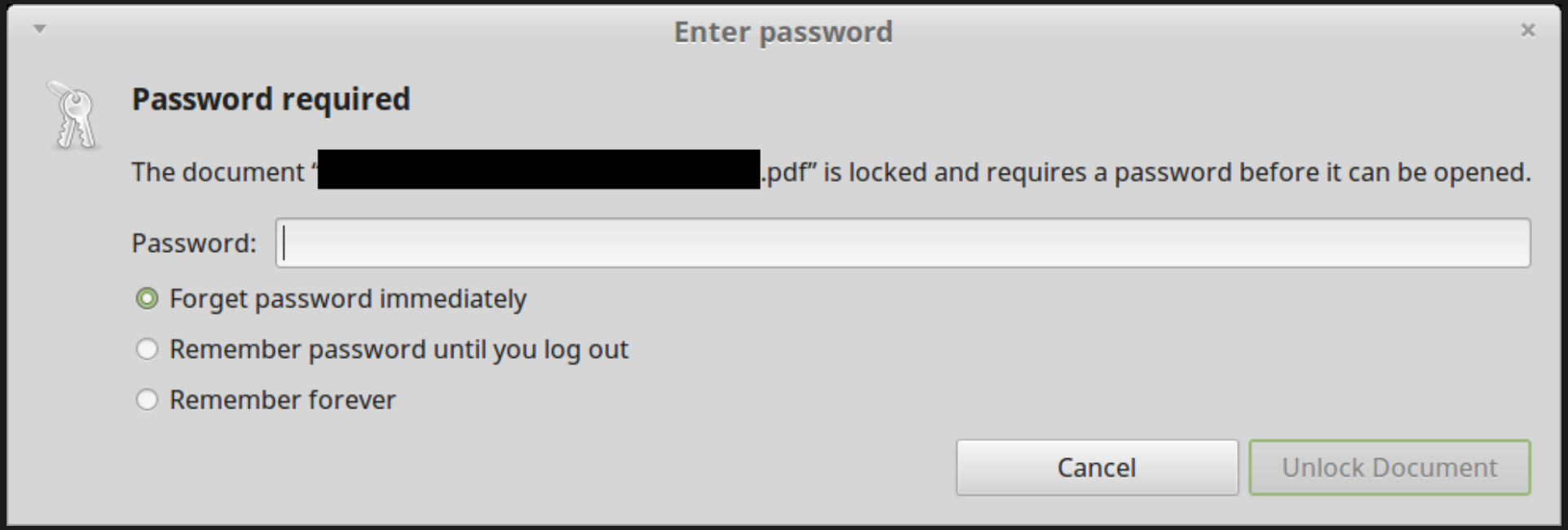
Periods:
01.01.2018 - [redacted]
Sagatavots: [redacted]

Pārskaitījumu virzieni:
Visi
Summa:
Visi

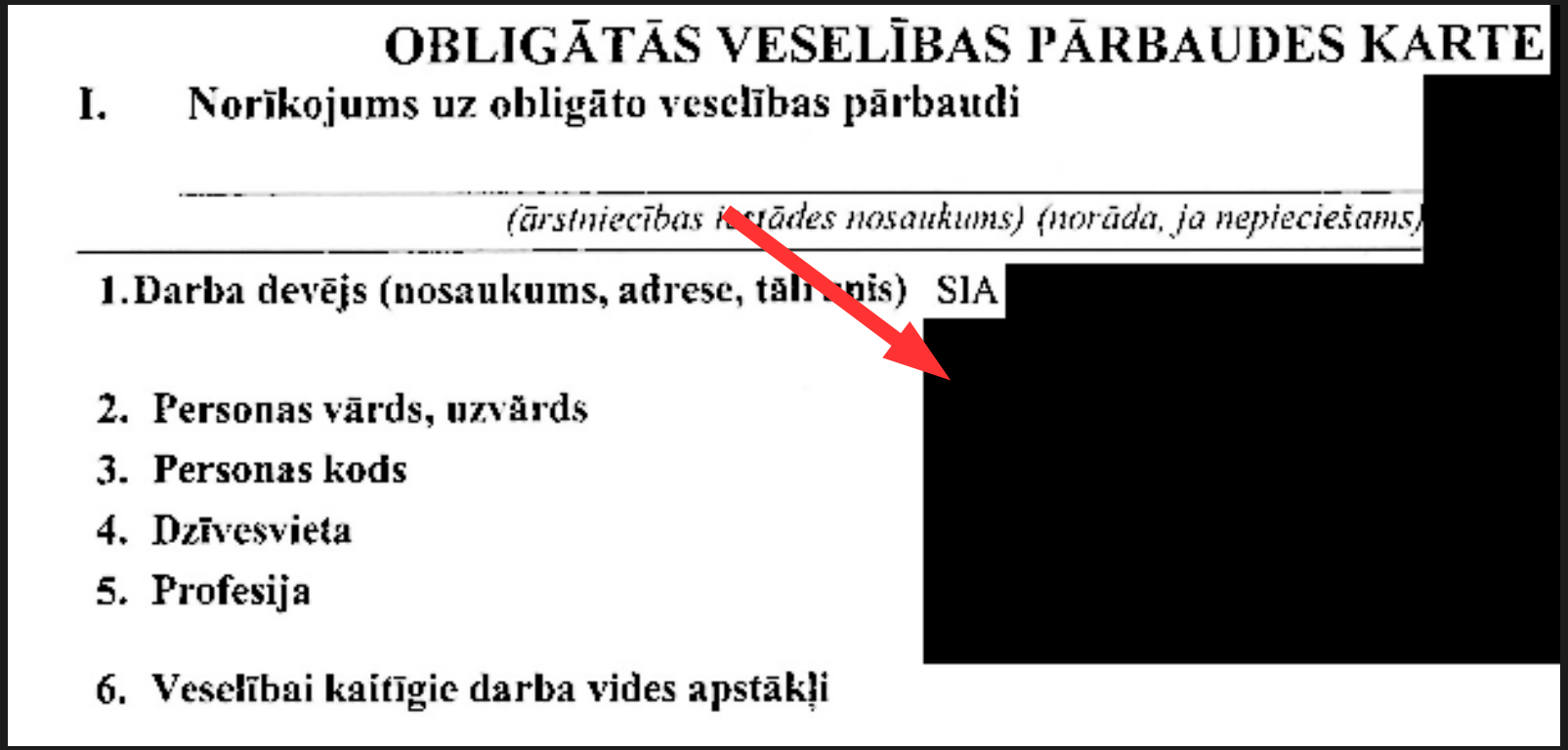
Sākuma atlikums **EUR:** [redacted]

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

sensitive health documents (encrypted)



occupational health check-up sheet



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

damn, that was intense!
let’s wrap up & chill out

- Previous owner endangers:
  - their clients and business partners
  - employees who've used e-mails for personal accounts
    - via password reset
  - banking, insurance and sensitive health information

- Attackers may gain control over:
  - commercial secrets
  - old installations of your website
  - government systems
  - information about passwords of the users
    - via breach notification sites
  - SSL certificates for the future website

- Use 2FA
- Pay for your damn domains
- If not, then:
  - notify everybody — partners, employees, and third parties using your API
  - remove old e-mail addresses from online accounts
- Check for suspicious behavior of mail servers; blacklist them

- Gather a larger, more representative data set
- Practically verify the following attack scenarios:
  - Use AGP to request SSL certificates valid for as long as possible
    - mitm connection to the domain after it's been re-registered
    - write an advisory, if needed
  - Locate and access the old server by looking at cron-like requests
  - Register breach notification alerts for a domain and wait

impact of domain name drop-catching on business security

visit for more goodies

#BalCCon2k18

http://kirils.org

@KirilsSolovjovs