CERT.LV

Informācijas tehnoloģiju
drošības incidentu
novēršanas institūcija

CYBERCRIME FRIENDLY SALES POLICY...

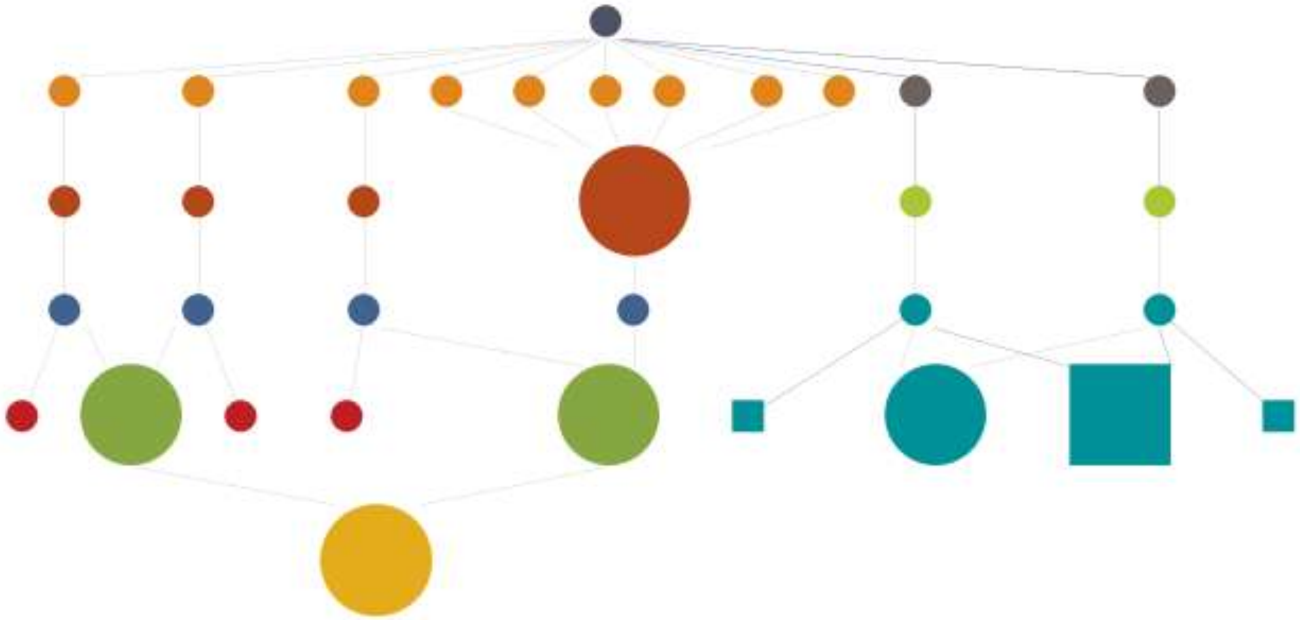
Varis Teivans 05.10.2017.
Kiberšahs 2017, Riga, Latvia

Why Cybercrime friendly?

- Free SSL – "Let's Encrypt" is reducing costs for attackers to stay covert in their operations
- Low Cost domain names, fast registration & activation, anonymity, crypto currency
- Low cost hosting services, anonymity, crypto currency
  - IP source address spoofing

Data is needed to find the answers

- Indicators Of Compromise
  - IP
  - DNS
  - URI
- HOSTING
  - ORG-name
  - Accepts cryptocurrency?
- Historical data sets
  - PDNS & P-Whois
  - PSSL



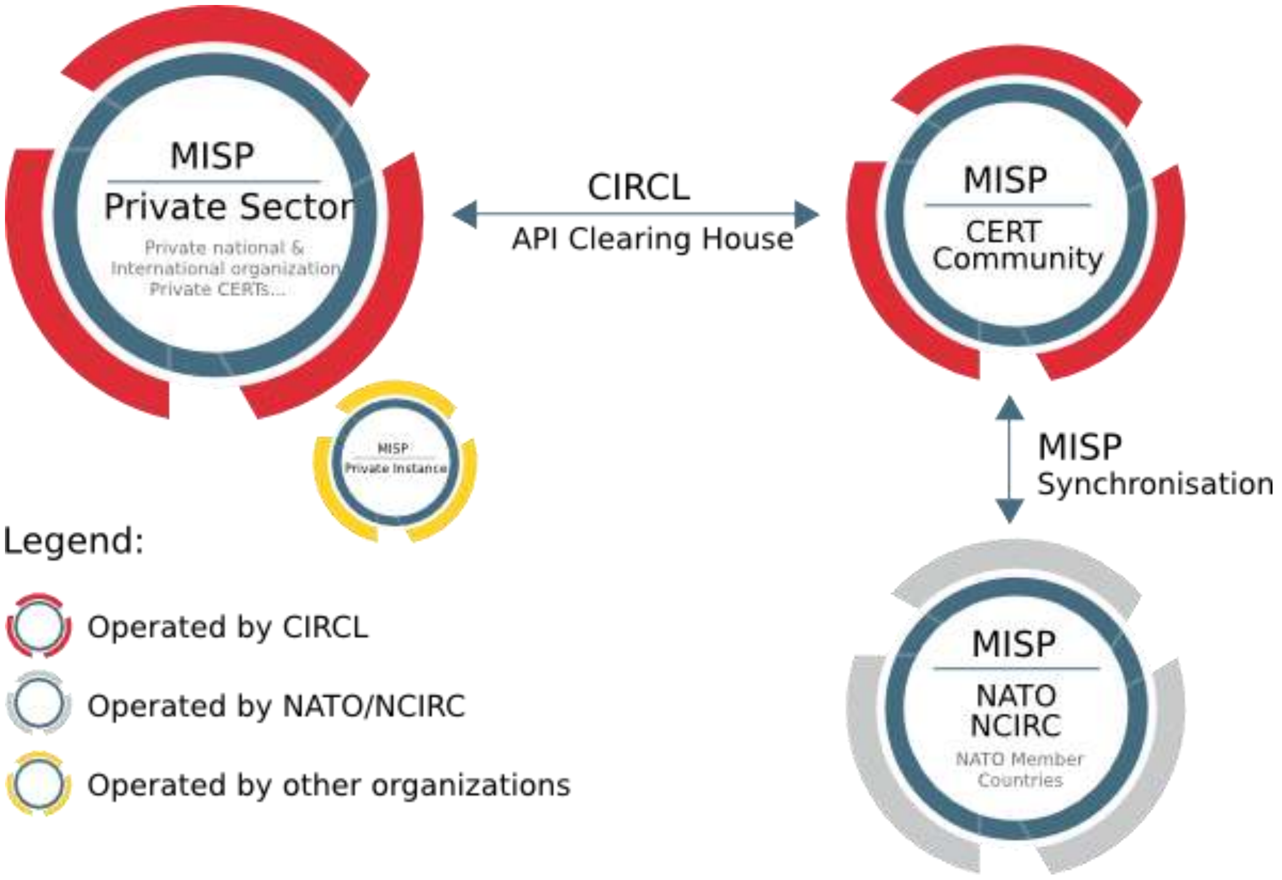
Data sources - IOC

- 2.3 million records

CERT.LV

Information Technologies
Security Incident
Response Institution

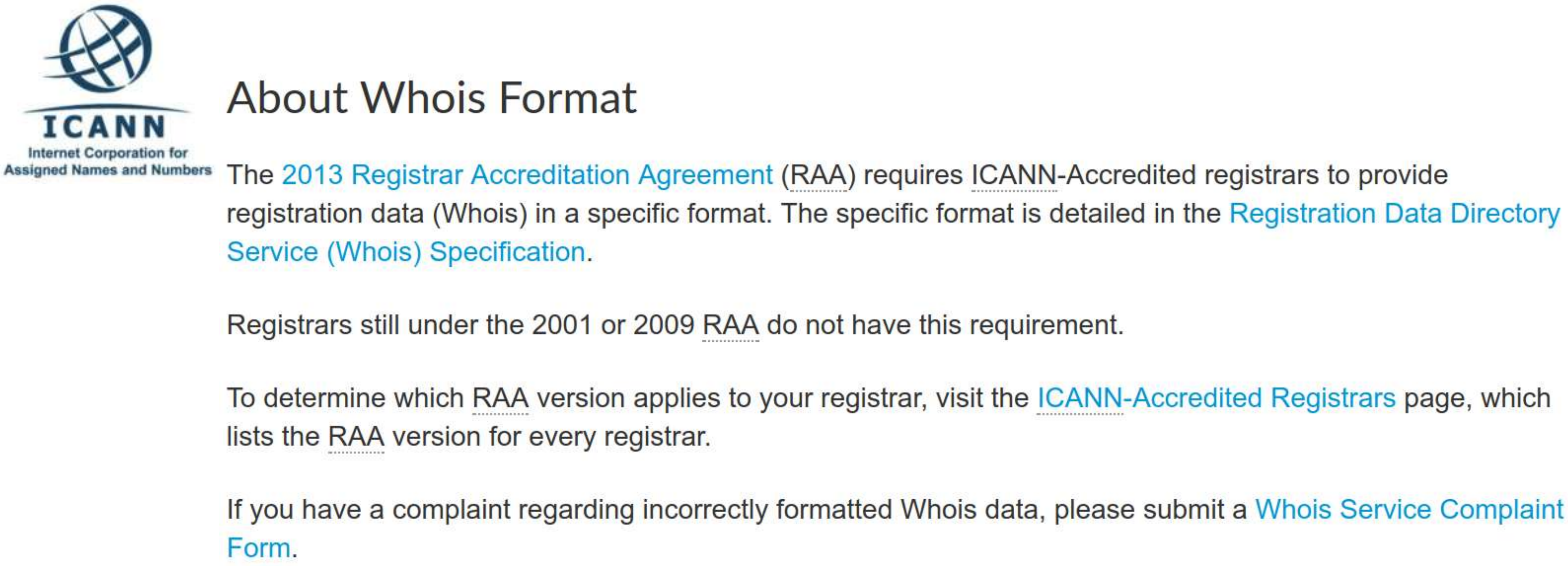
EUROPOL



DNS & some difficulties along the way

- **DNS price range 0 – 5 $ / yr – mapping them on IOCs**
- **Safeguards to mitigate DNS abuse?**
  - **Yes, DNS crowd is working on that… ICANN working group**
  https://www.icann.org/news/announcement-2-2016-03-15-en
- ***Common TOS – helping CERTs to make a difference***
- ***Common whois requirements – thick and machine friendly data***

DNS



About Whois Format

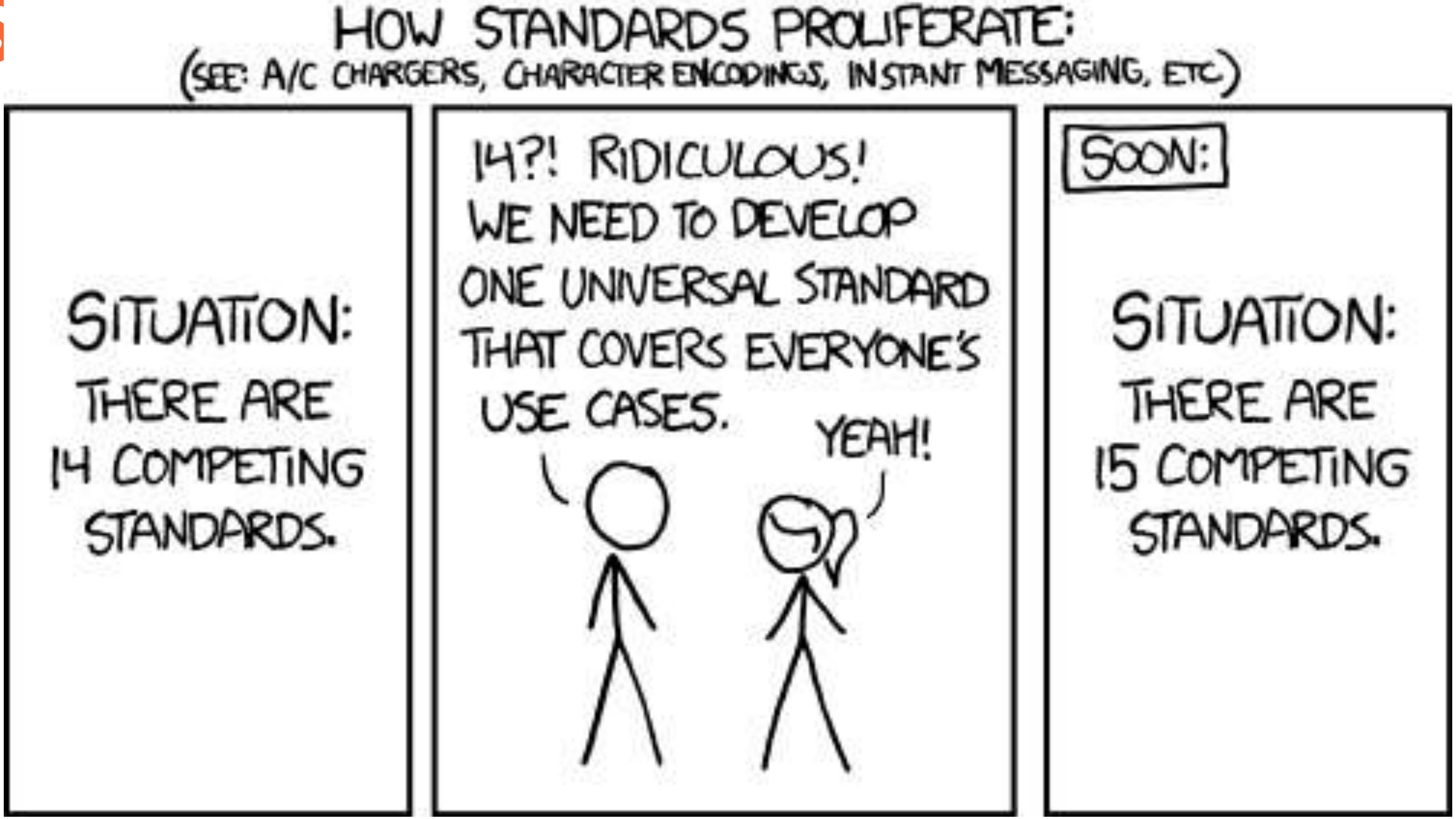
The 2013 Registrar Accreditation Agreement (RAA) requires ICANN-Accredited registrars to provide registration data (Whois) in a specific format. The specific format is detailed in the Registration Data Directory Service (Whois) Specification.

Registrars still under the 2001 or 2009 RAA do not have this requirement.

To determine which RAA version applies to your registrar, visit the ICANN-Accredited Registrars page, which lists the RAA version for every registrar.

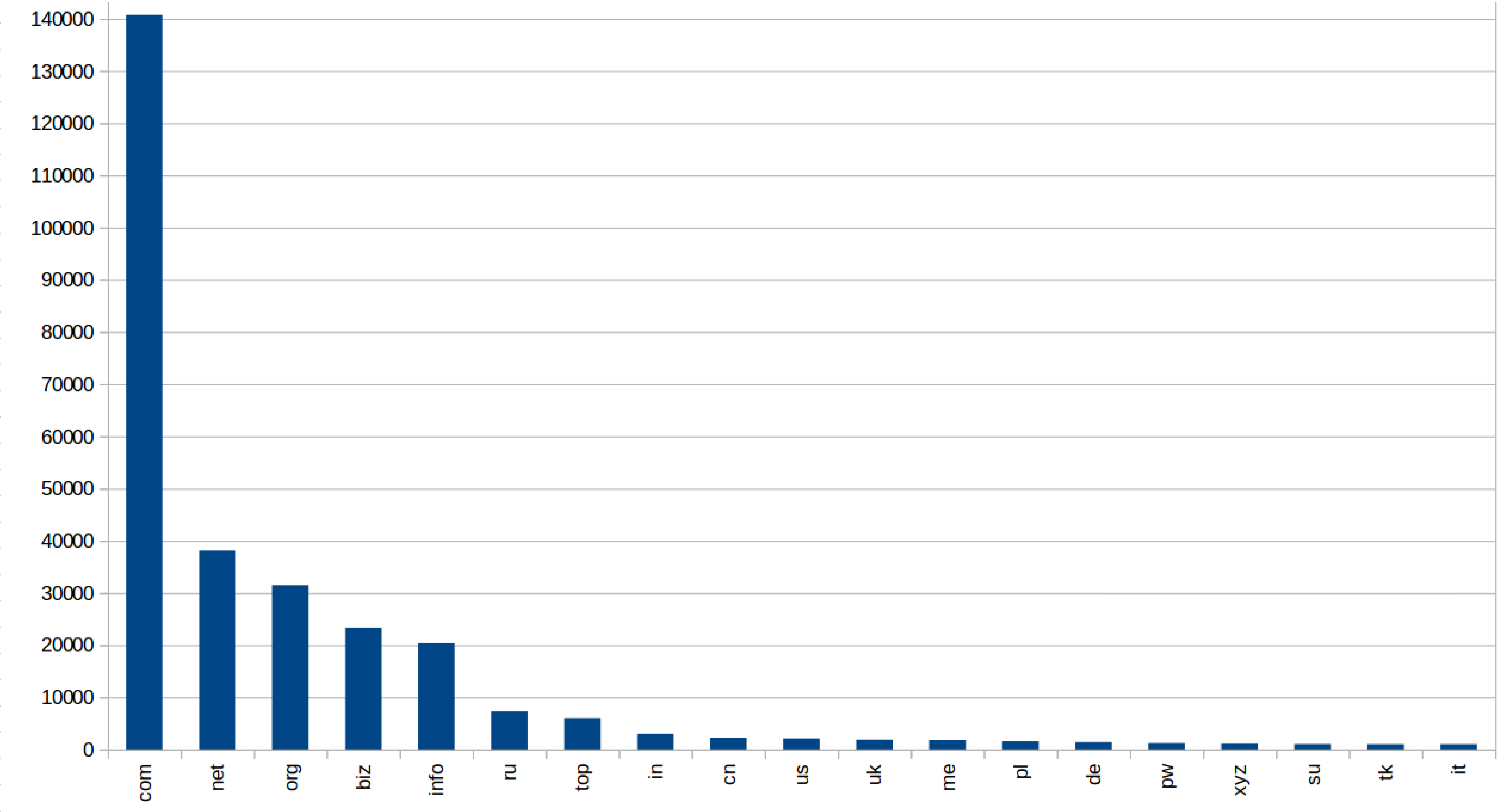
If you have a complaint regarding incorrectly formatted Whois data, please submit a Whois Service Complaint Form.

DNS


HOW STANDARDS PROLIFERATE:
(SEE: A/C CHARGERS, CHARACTER ENCODINGS, INSTANT MESSAGING, ETC.)
SITUATION: THERE ARE 14 COMPETING STANDARDS.
14?! RIDICULOUS! WE NEED TO DEVELOP ONE UNIVERSAL STANDARD THAT COVERS EVERYONE'S USE CASES.
YEAH!
SOON:
SITUATION: THERE ARE 15 COMPETING STANDARDS.

DNS

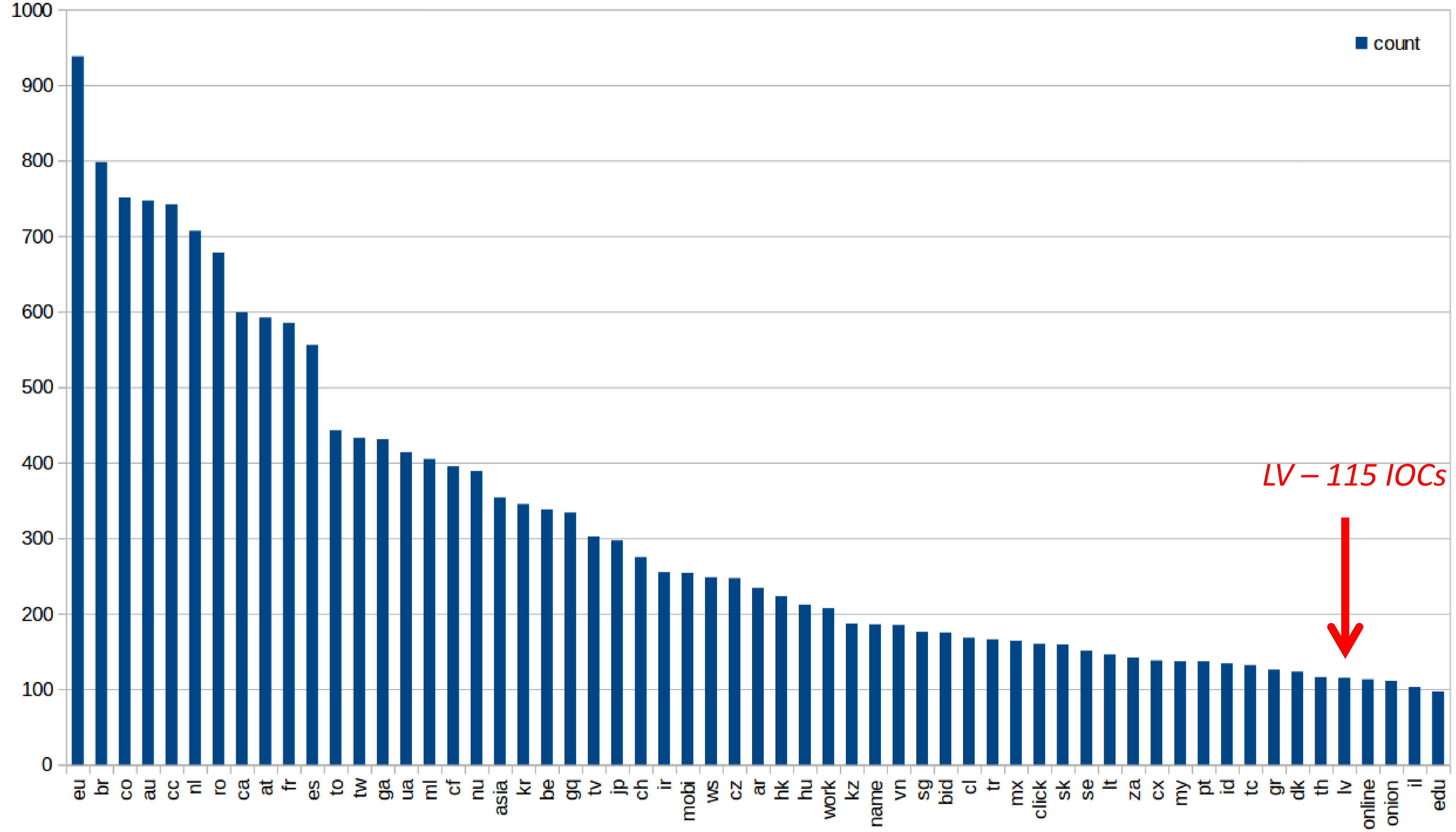
- Com
- *Net*
- *Org*
- *Biz*
- *Info*
- *Ru*



CERT.LV

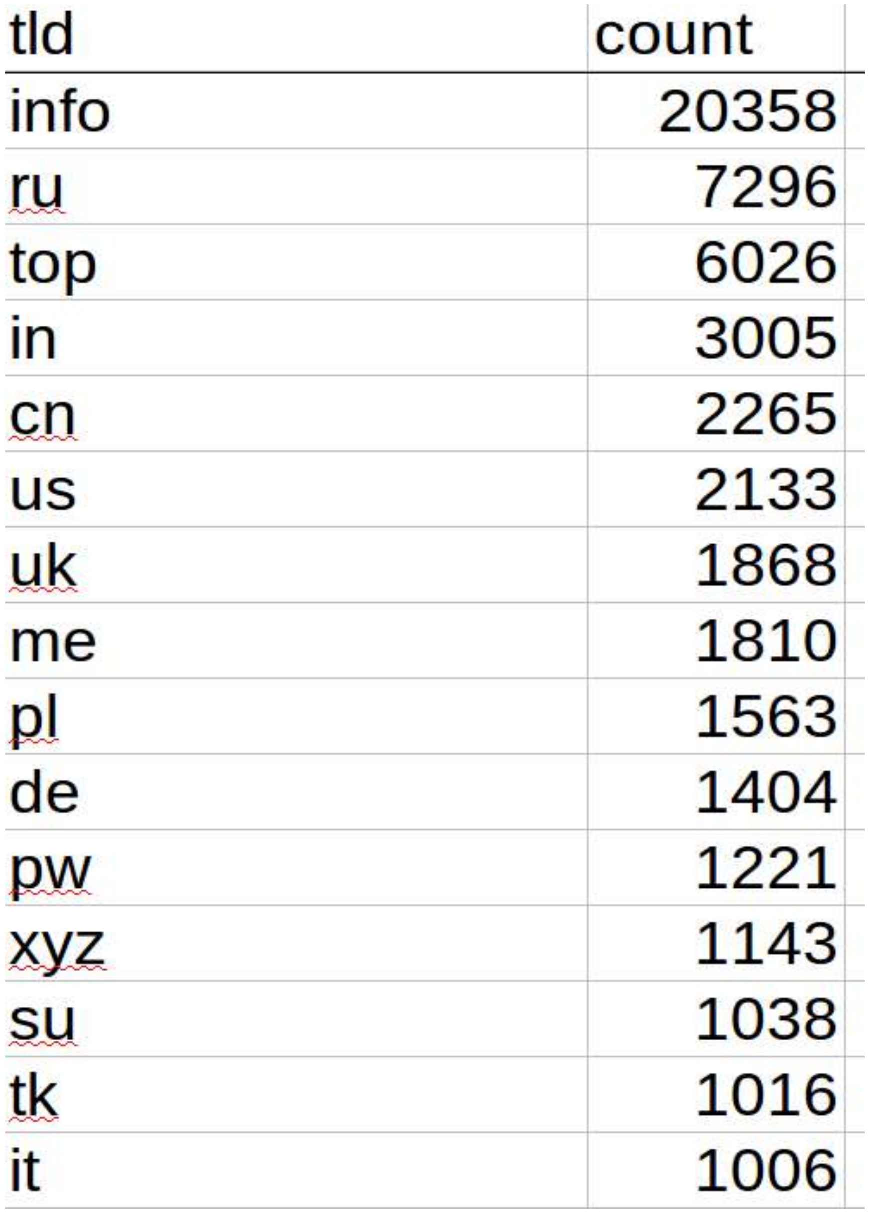
DNS

- **Eu**
- ***Br***
- ***Co***
- ***Au***
- ***Cc***



LV – 115 IOCs

DNS

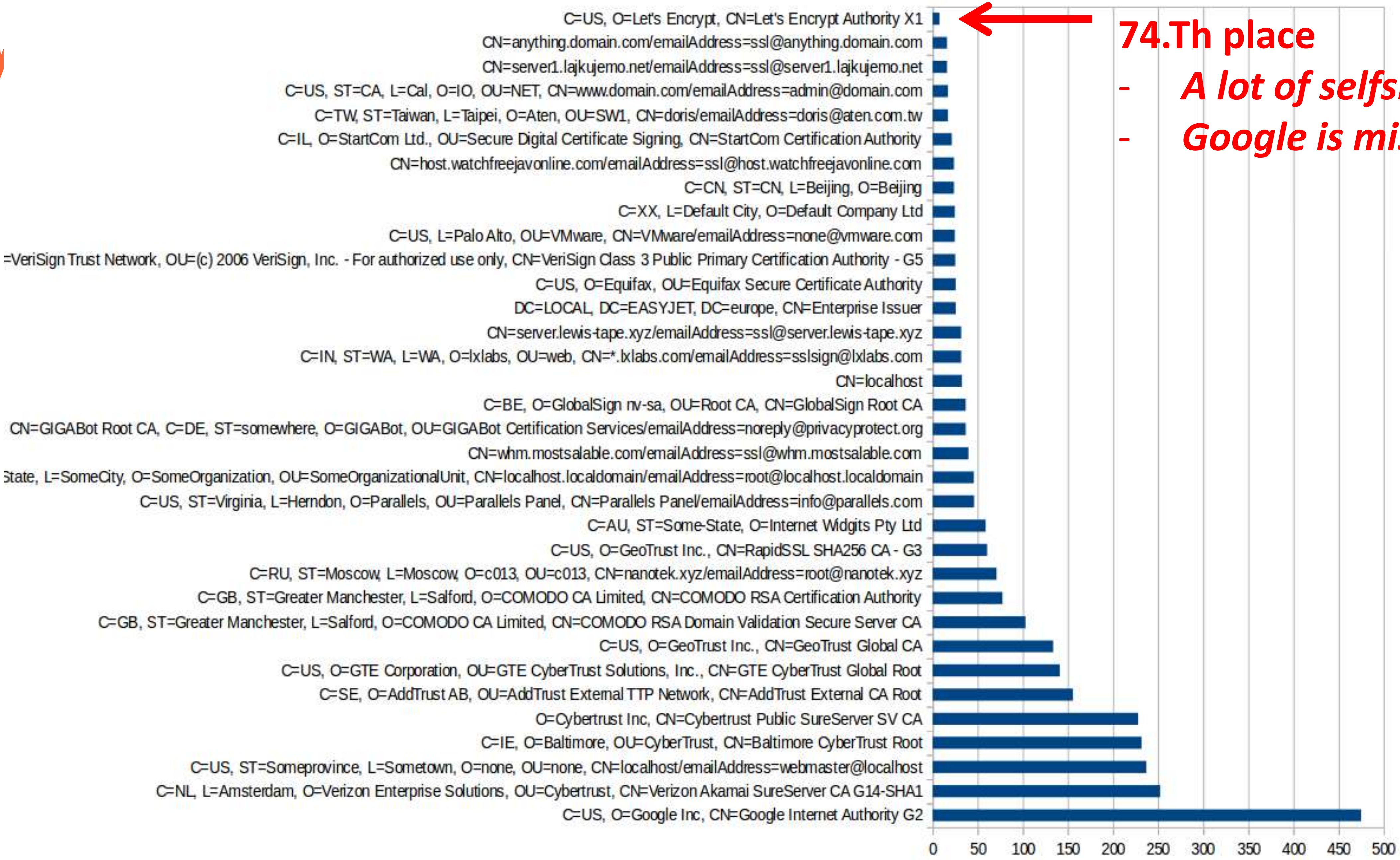


tld	count
info	20358
ru	7296
top	6026
in	3005
cn	2265
us	2133
uk	1868
me	1810
pl	1563
de	1404
pw	1221
xyz	1143
su	1038
tk	1016
it	1006

15 - 25 EUR → su

SSL

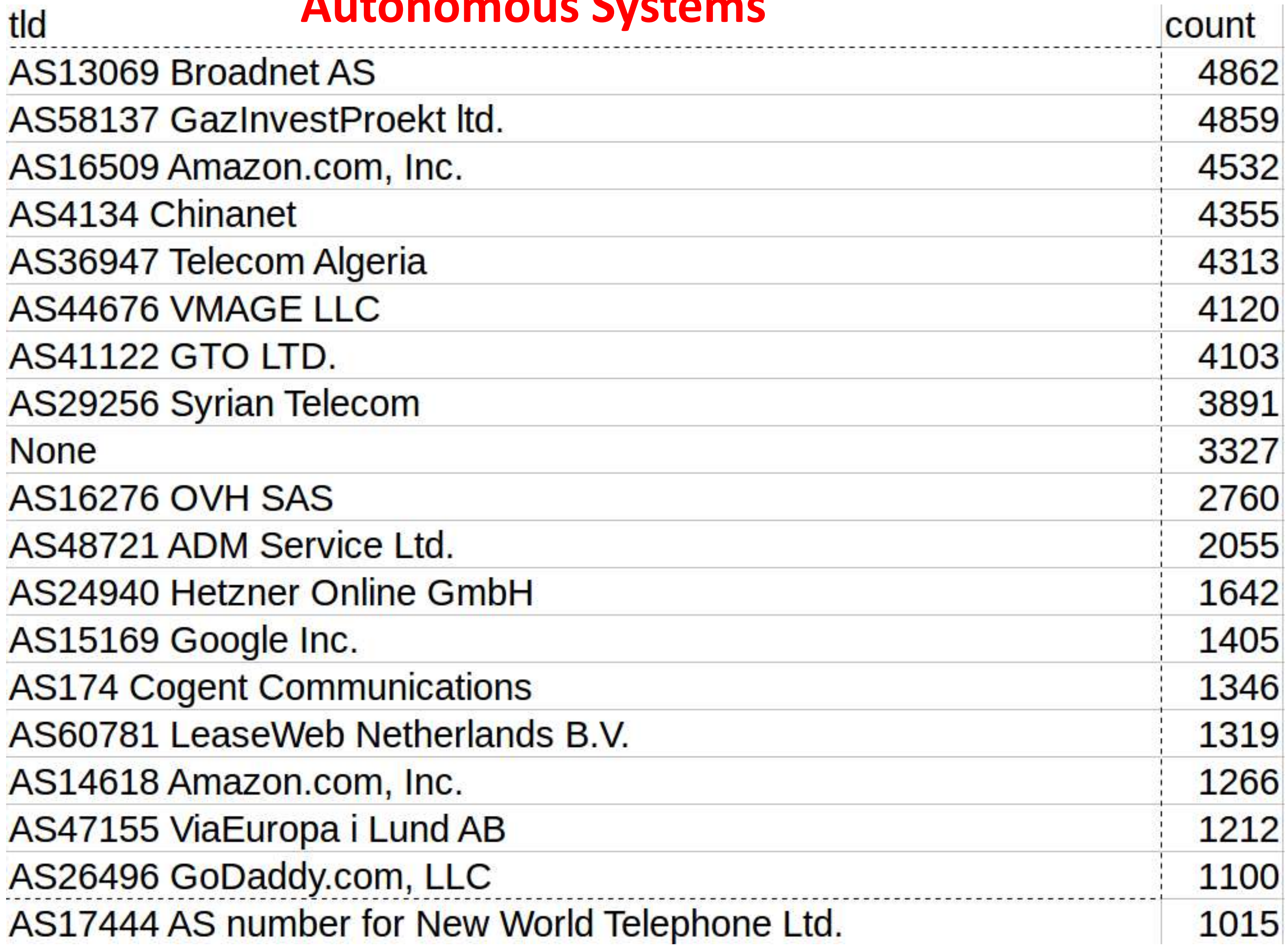
- Observations
- *Trustworthiness*
- *Good VS Bad*
- *PSSL – Passive SSL Database – CIRCL.LU*
  - *Idea from GCHQ project “Flying Pig”*



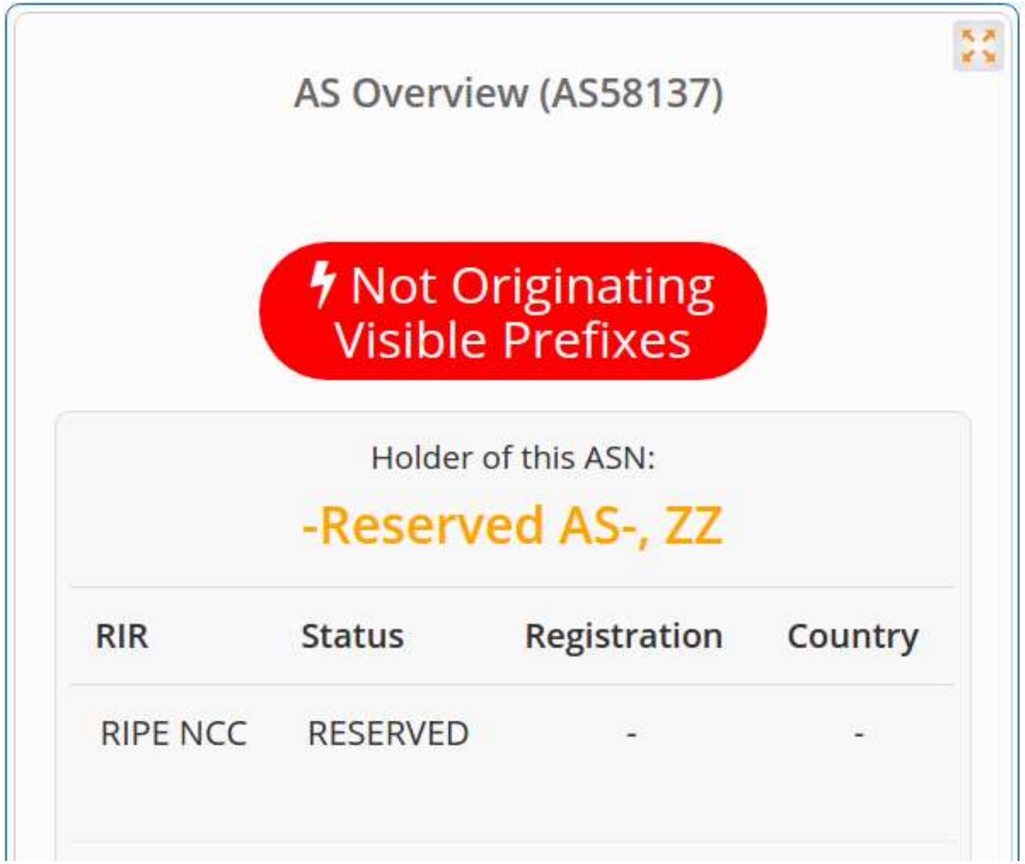
74.Th place

- *A lot of selfsigned*
- *Google is misleading*

Autonomous Systems



tld	count
AS13069 Broadnet AS	4862
AS58137 GazInvestProekt ltd.	4859
AS16509 Amazon.com, Inc.	4532
AS4134 Chinanet	4355
AS36947 Telecom Algeria	4313
AS44676 VMAGE LLC	4120
AS41122 GTO LTD.	4103
AS29256 Syrian Telecom	3891
None	3327
AS16276 OVH SAS	2760
AS48721 ADM Service Ltd.	2055
AS24940 Hetzner Online GmbH	1642
AS15169 Google Inc.	1405
AS174 Cogent Communications	1346
AS60781 LeaseWeb Netherlands B.V.	1319
AS14618 Amazon.com, Inc.	1266
AS47155 ViaEuropa i Lund AB	1212
AS26496 GoDaddy.com, LLC	1100
AS17444 AS number for New World Telephone Ltd.	1015



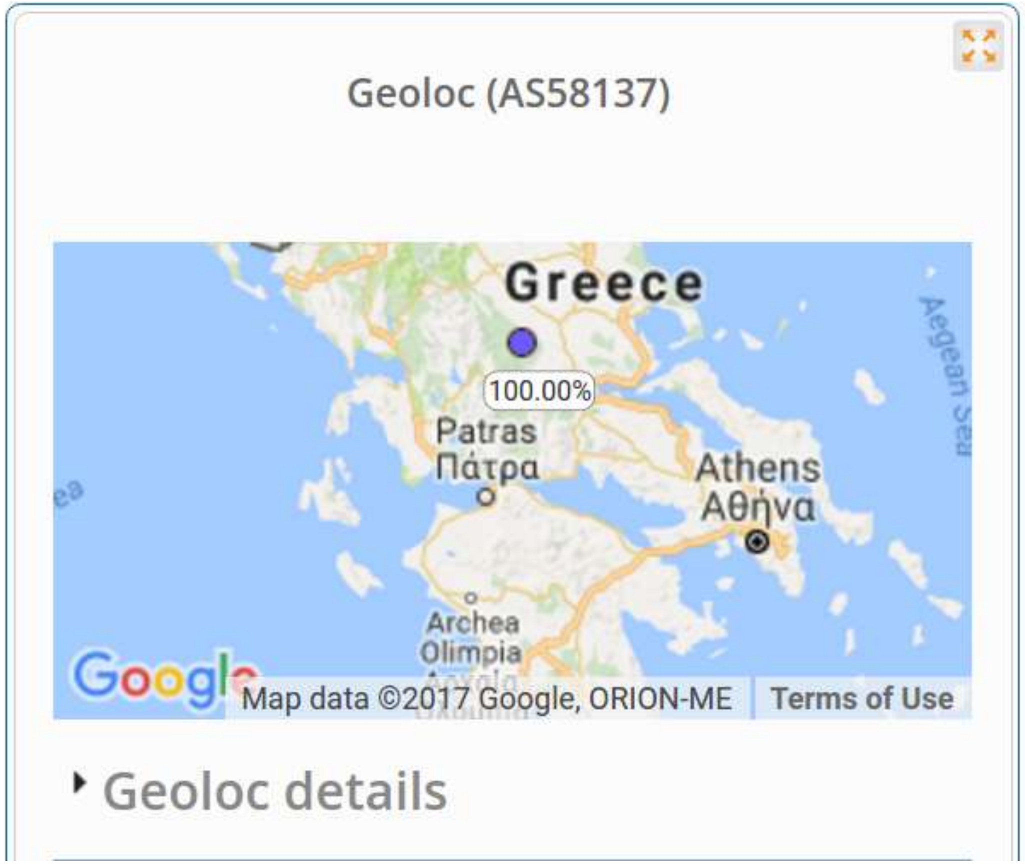
AS Overview (AS58137)

ϟ Not Originating Visible Prefixes

Holder of this ASN:

-Reserved AS-, ZZ

RIR	Status	Registration	Country
RIPE NCC	RESERVED	-	-



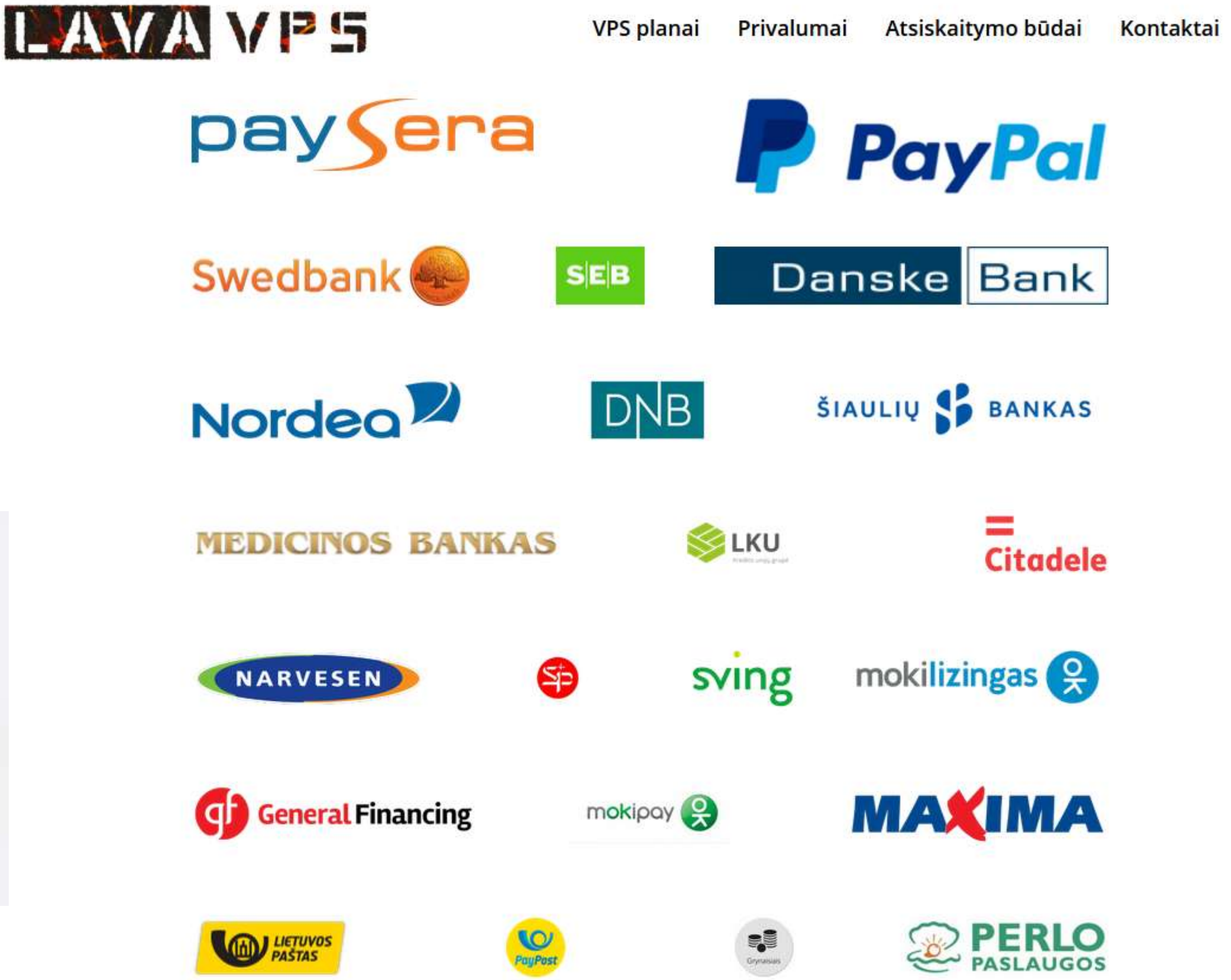
Geoloc (AS58137)

‣ Geloc details

Possibly prefix hijacking of network that is not in use

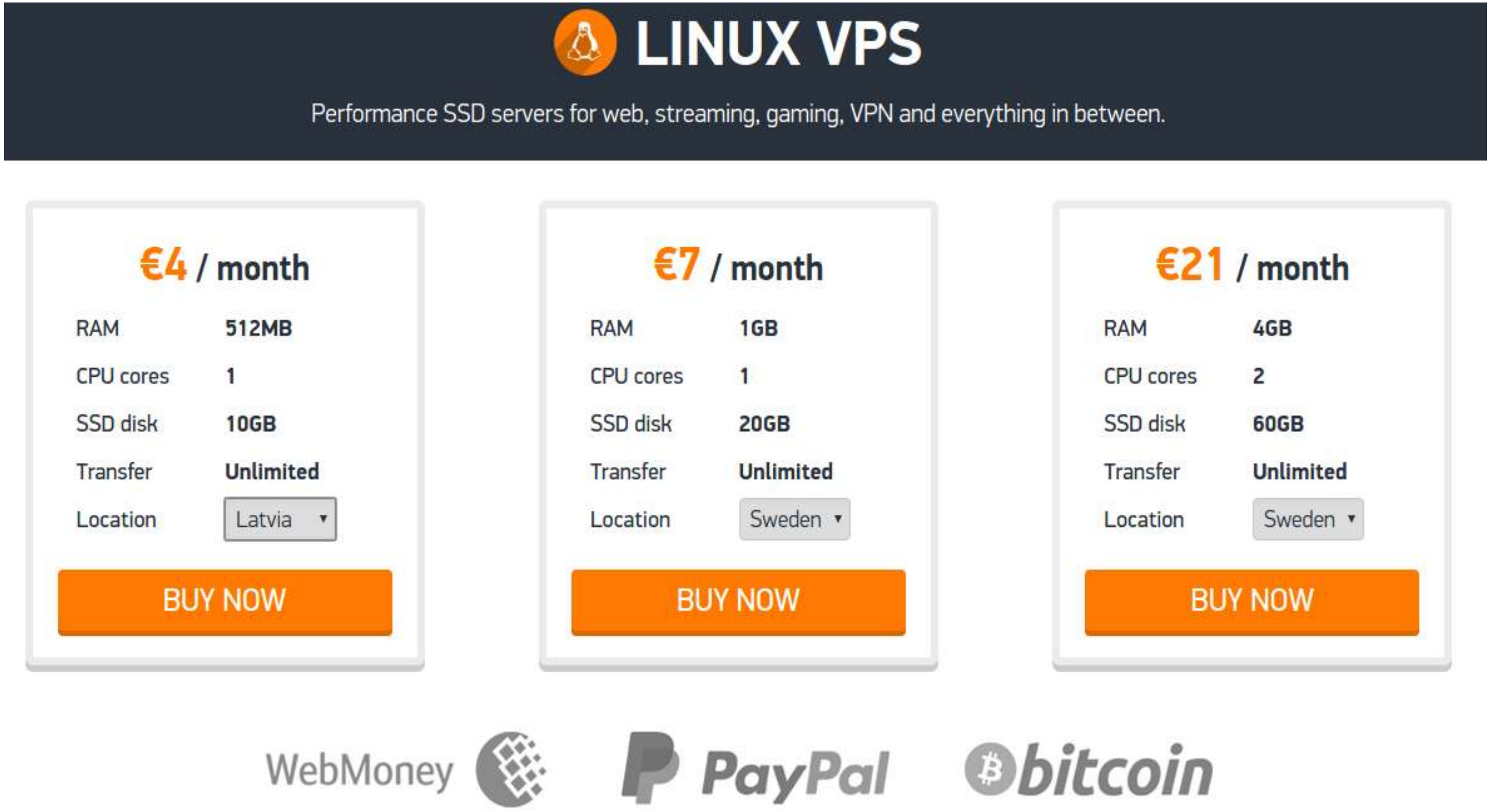
Hosting & Payme

- **Does anyone even regulate which payment systems should be accepted?**



Hosting

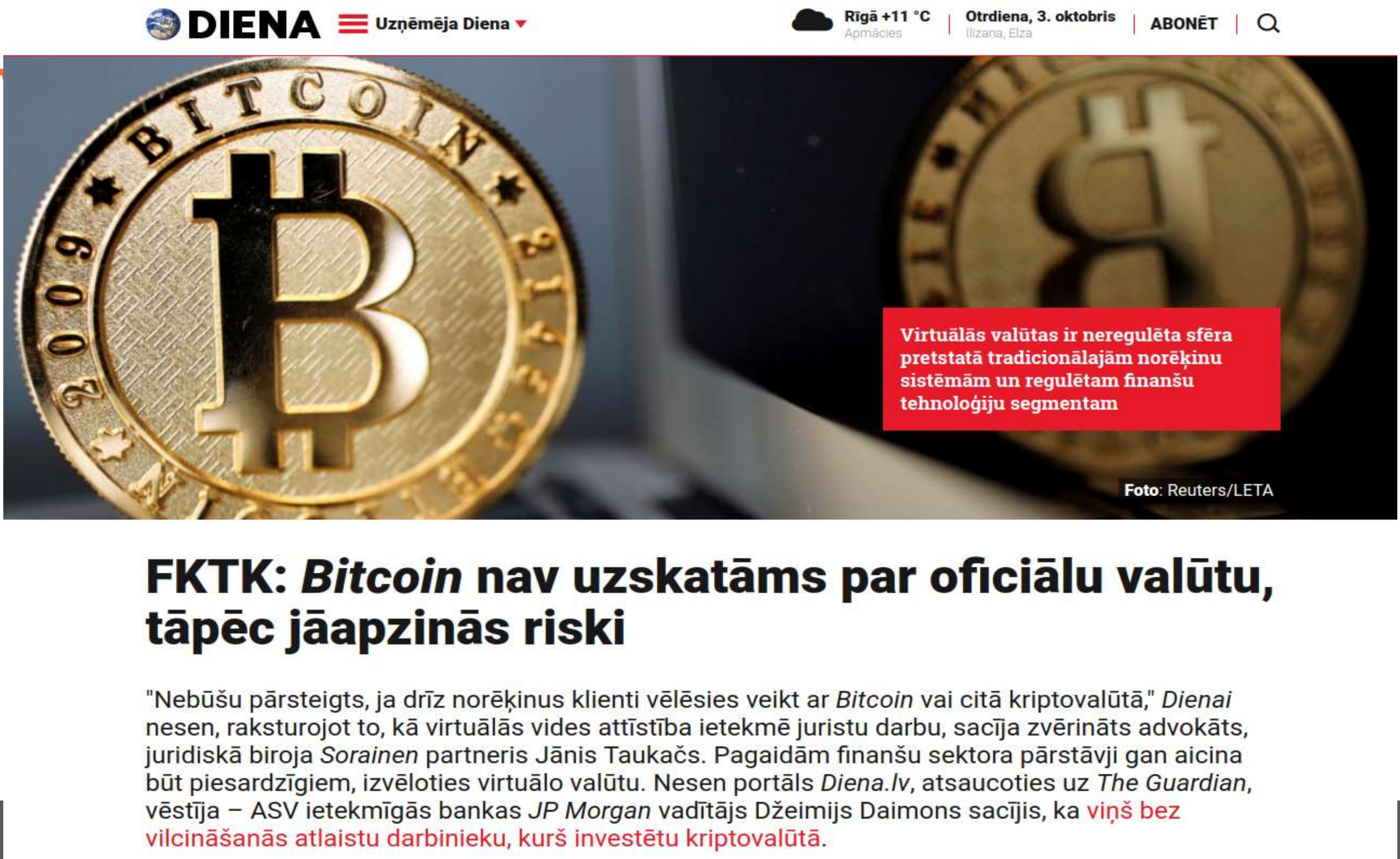
- Best practices are nice as long as there is somebody who cares…



LINUX VPS

Performance SSD servers for web, streaming, gaming, VPN and everything in between.

	€4 / month	€7 / month	€21 / month
RAM	512MB	1GB	4GB
CPU cores	1	1	2
SSD disk	10GB	20GB	60GB
Transfer	Unlimited	Unlimited	Unlimited
Location	Latvia ▾	Sweden ▾	Sweden ▾
	BUY NOW	BUY NOW	BUY NOW



Virtuālās valūtas ir neregulēta sfēra pretstatā tradicionālajām norēķinu sistēmām un regulētam finanšu tehnoloģiju segmentam

Foto: Reuters/LETA

FKTK: *Bitcoin* nav uzskatāms par oficiālu valūtu, tāpēc jāapzinās riski

"Nebūšu pārsteigts, ja drīz norēķinus klienti vēlēsies veikt ar *Bitcoin* vai citā kriptovalūtā," *Dienai* nesen, raksturojot to, kā virtuālās vides attīstība ietekmē juristu darbu, sacīja zvērināts advokāts, juridiskā biroja *Sorainen* partneris Jānis Taukačs. Pagaidām finanšu sektora pārstāvji gan aicina būt piesardzīgiem, izvēloties virtuālo valūtu. Nesen portāls *Diena.lv*, atsaucoties uz *The Guardian*, vēstīja – ASV ietekmīgās bankas *JP Morgan* vadītājs Džeimijs Daimons sacījis, ka viņš bez vilcināšanās atlaistu darbinieku, kurš investētu kriptovalūtā.

Conclusions

- Results from the available IOC data analysis do not reveal an overwhelming abuse of low cost IT services however, there are strong indications of specific Cybercrime interest (research should be extended)

Conclusions

- *Low cost domains (with exceptions) – Cyber Crime Friendly*
- *VPS hosting accepting crypto currency – Cyber Crime Friendly*
- *Free SSL – not really but soon..*
- *Malware hosting & Cyber Crime tourism*
- *Policy & regulations will come.. Casualties VS Time*

Thank you!

https://www.cert.lv
varis.teivans@cert.lv
Varis Teivans