Интернет сүлжээний орчин дахь кибер аюул занал, өнөөгийн нөхцөл байдал

Др. М.Отгонпүрэв

MNCERT/CC

About MNCERT/CC

- Established in 2014 as security community meetup
- Transformed as non-governmental, non-profit organization in 2015
- Since 2015:
  - Member of APCERT, FIRST
  - Contractual relationship: NCFTA, Team Cymru, Microsoft Security, Shadowserver
  - Local members: 12 organizations
- Incident coordination and information sharing
- Public awareness and community building
  - MNSEC
  - HaruulZangi

Монгол Улсын Интернет сүлжээ хар жагсаалтанд орсон байдал

Б.Дашзэвэг, Г.Билгүүн

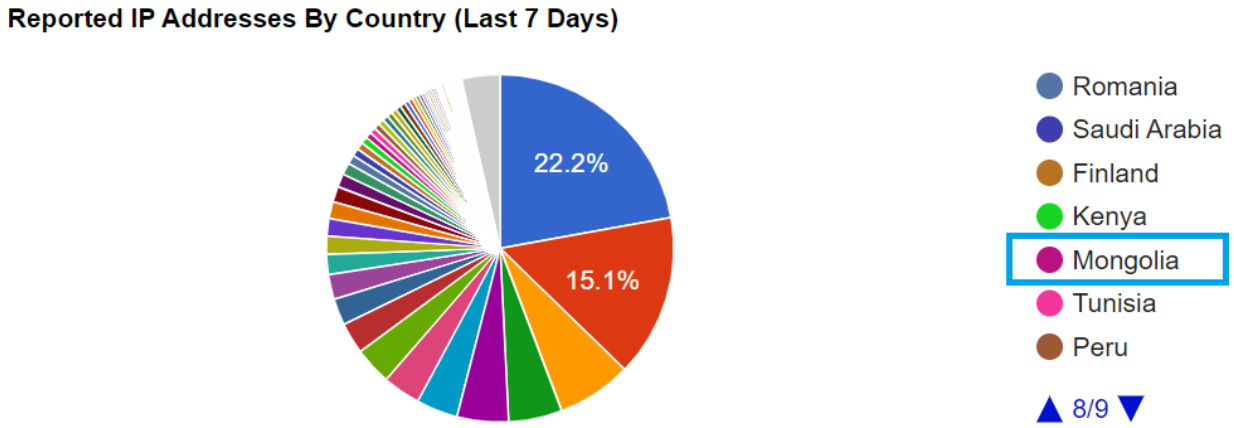
Юнитель групп

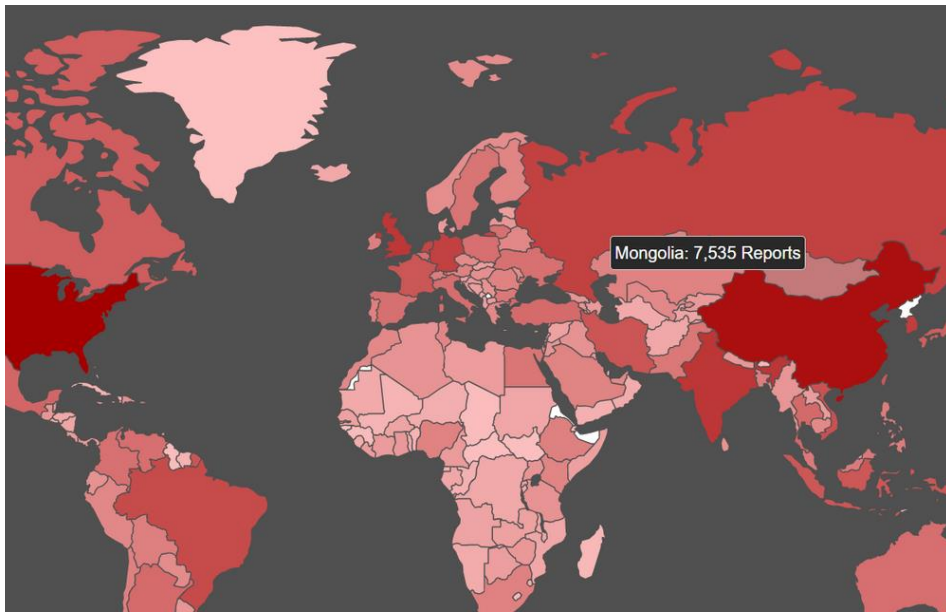
What is blacklist?

A blacklist is a process of creating a registration list by detecting abnormal behavior of users connected to the Internet on many sensors located around the world.

- Download or distribute copyright-violating content. For example illegal content, such as pirated software, copyrighted material, or child exploitation material
- Abnormal behavior - Sending spam mail or information, sending malicious traffic from a user's device infected with a virus., or attempting to attack other networks, etc.

As of week of 26th June to 30th June



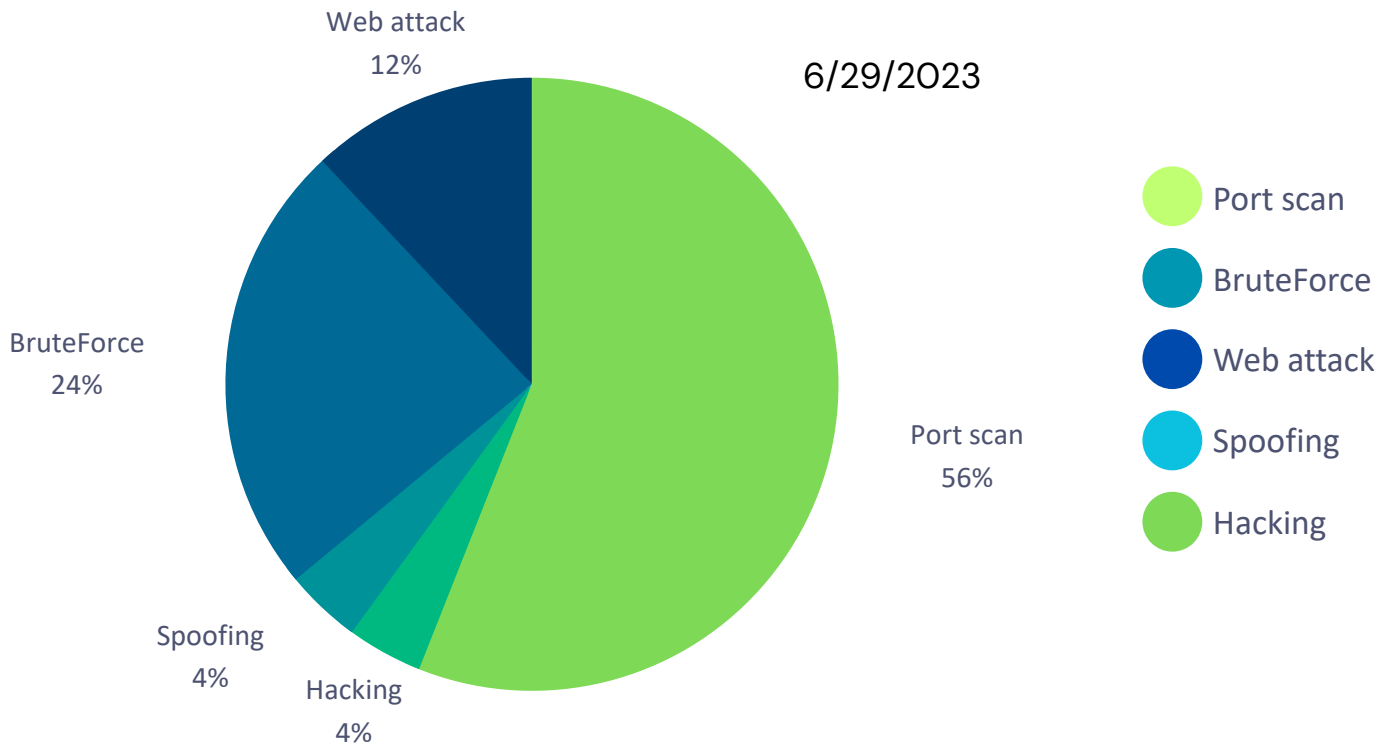


- Based on abuseipdb:
  - 7,535 IP registered in Blacklist
  - 54th place
- 4.2% of total active IP

- No1: USA – 1,014,465 IP blacklisted
  - 0.06% of total IP
- No2: China – 687,366
  - 0.19% of total IP
- No3: Singapore – 315,696
  - 1.5% of total IP

https://www.abuseipdb.com/statistics

Abuse reasons



Risks of IP blacklist

- Risk of all other users will be subject to content restrictions due to one abnormal event (NAT)
- Blocked email communication
- Reputational damage to the country
- Difficulty accessing certain services
- Reduced website traffic
- To become an Independent “Internet” or isolated island

Blacklist situation in Mongolia

- Total IP address assigned (APNIC): 215,808
- Active IP address (in use): 177,920
- Surveyed IP’s of major ISPs: 156,976
- Blacklisted IP: 60,267
- 33% of total active IP addresses are in Blacklist
- Highest blacklisted IP for given IP pool

Монгол Улсын Интернет сүлжээний орчин дахь эрсдэлтэй нөхцөл байдал

В.Нямсүрэн
З.Цолмон
Т.Билэгдэмбэрэл
MNCERT/CC

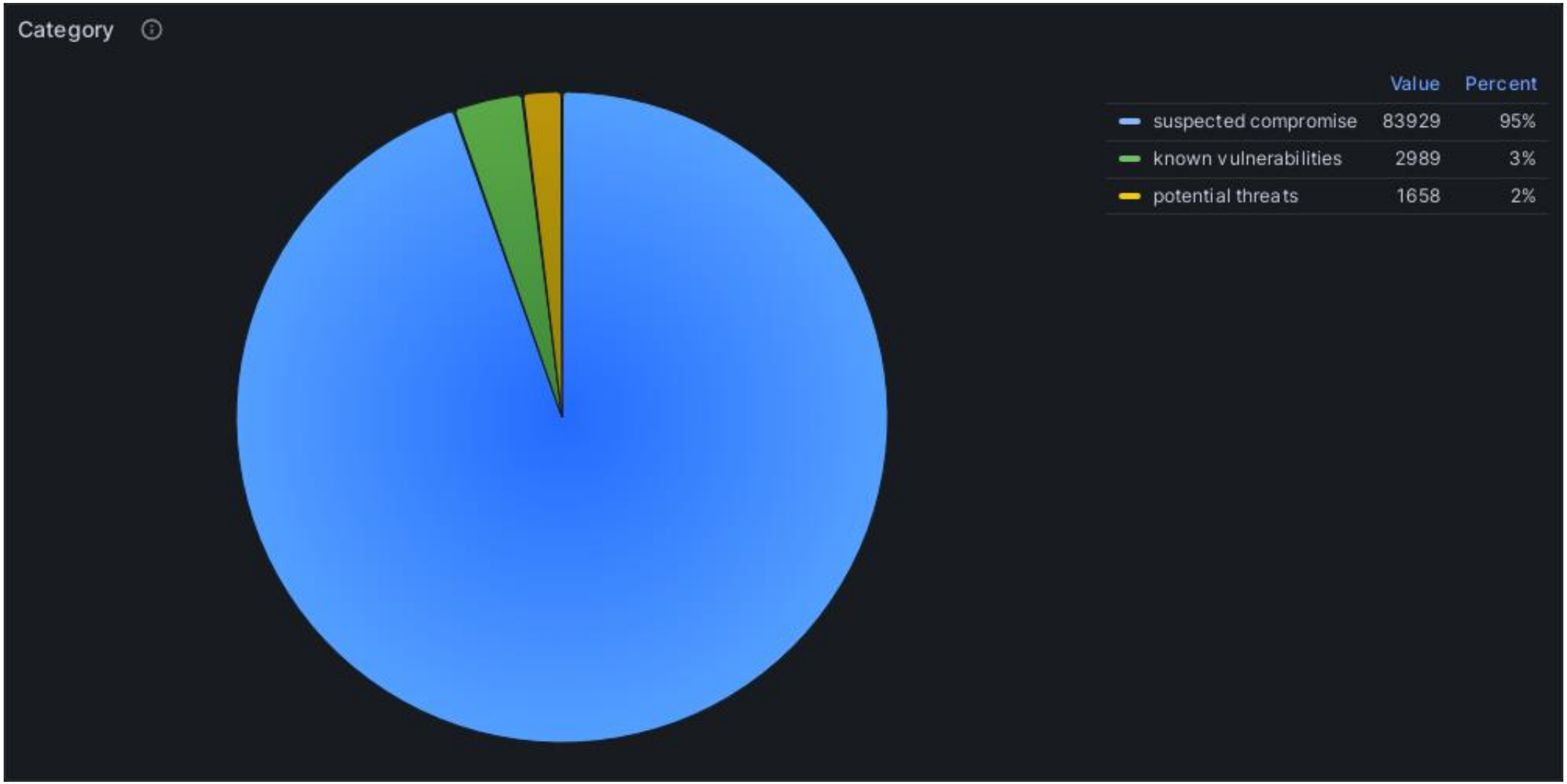
As of 13th to 20th October

- 38 ISP
- 8,642 IP address
- 88,576 events

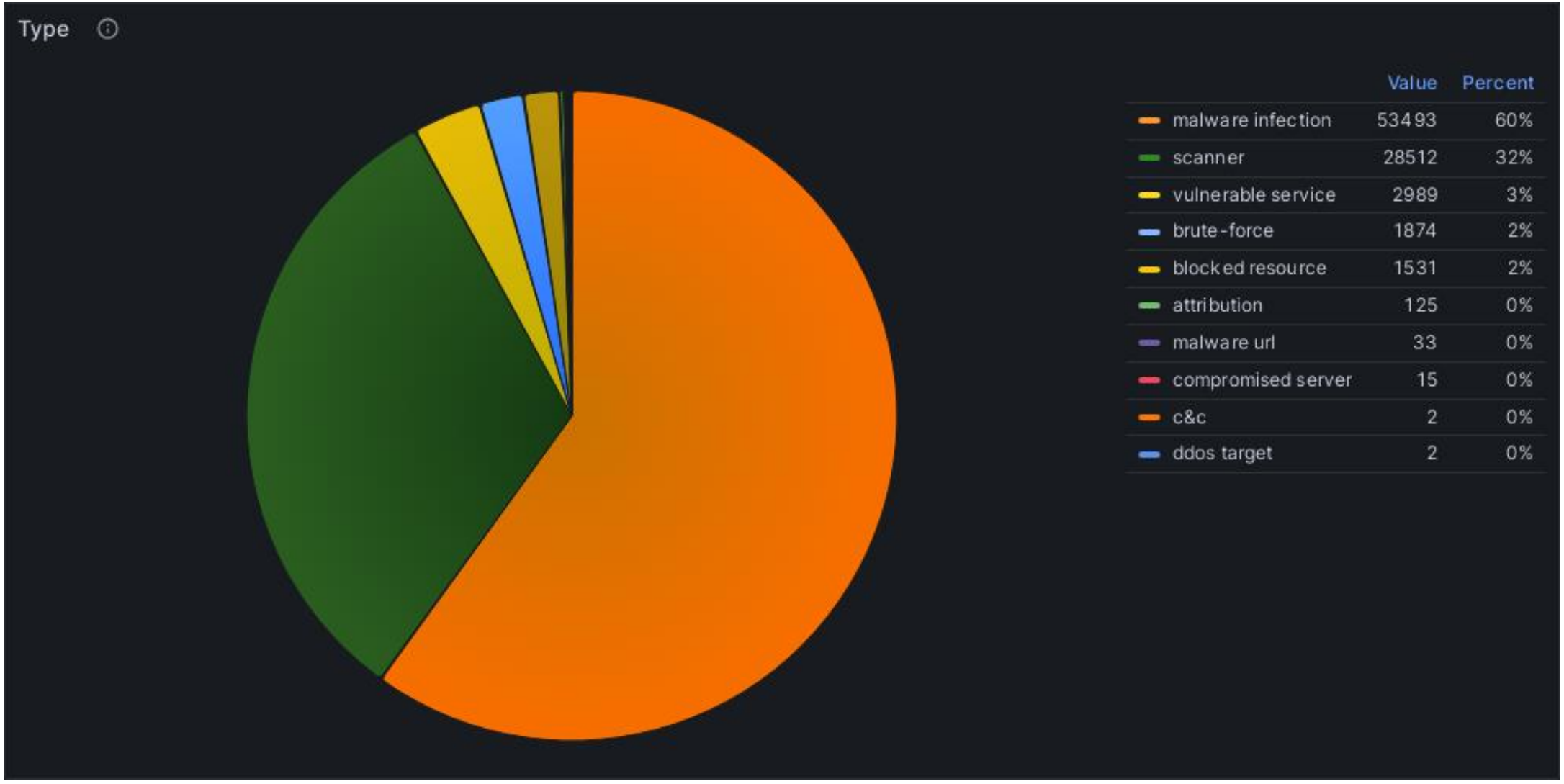
Event types

- ***Suspected Compromise*** - Халдлагад өртсөн байж болзошгүйг илэрхийлнэ. Өөрөөр хэлбэл, вирусээр халдварласан, Команд Удирдлагын Сервер (C&C)-д хандах оролдлого хийсэн зэрэг тухайн хост халдлагад өртсөн байж болзошгүйг илэрхийлнэ.
- ***Known Vulnerabilities*** - Тухайн хост дээр ажиллаж буй аливаа программ, сервист нийтэд ил болсон эмзэг байдал буйг илэрхийлнэ.
- ***Potential Threats*** - Тухайн эвентээс шалтгаалан энэхүү хост ажиллаж буй байгууллагын кибер орчинд аюул заналхийлэл учирч болзошгүйг илэрхийлнэ.

Events during the week



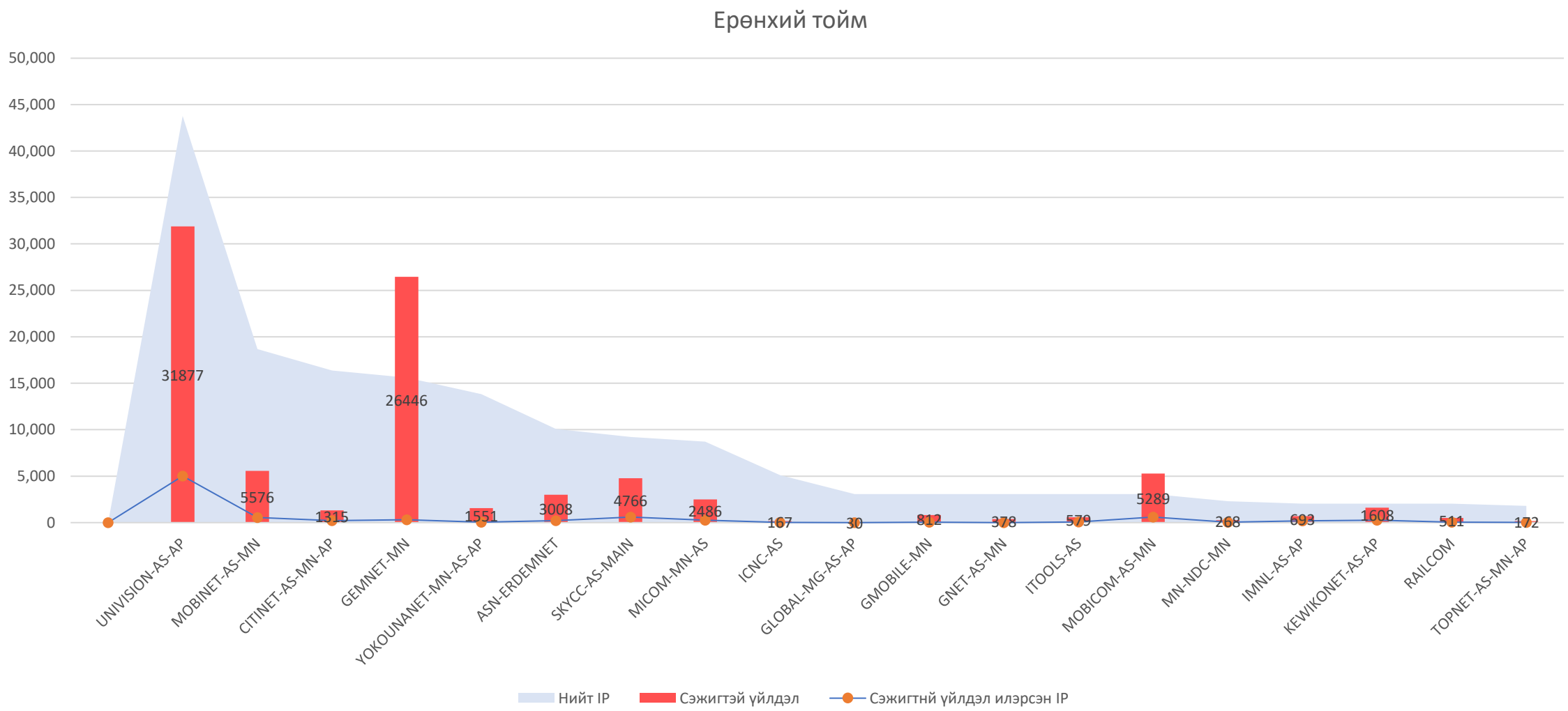
Compromise types



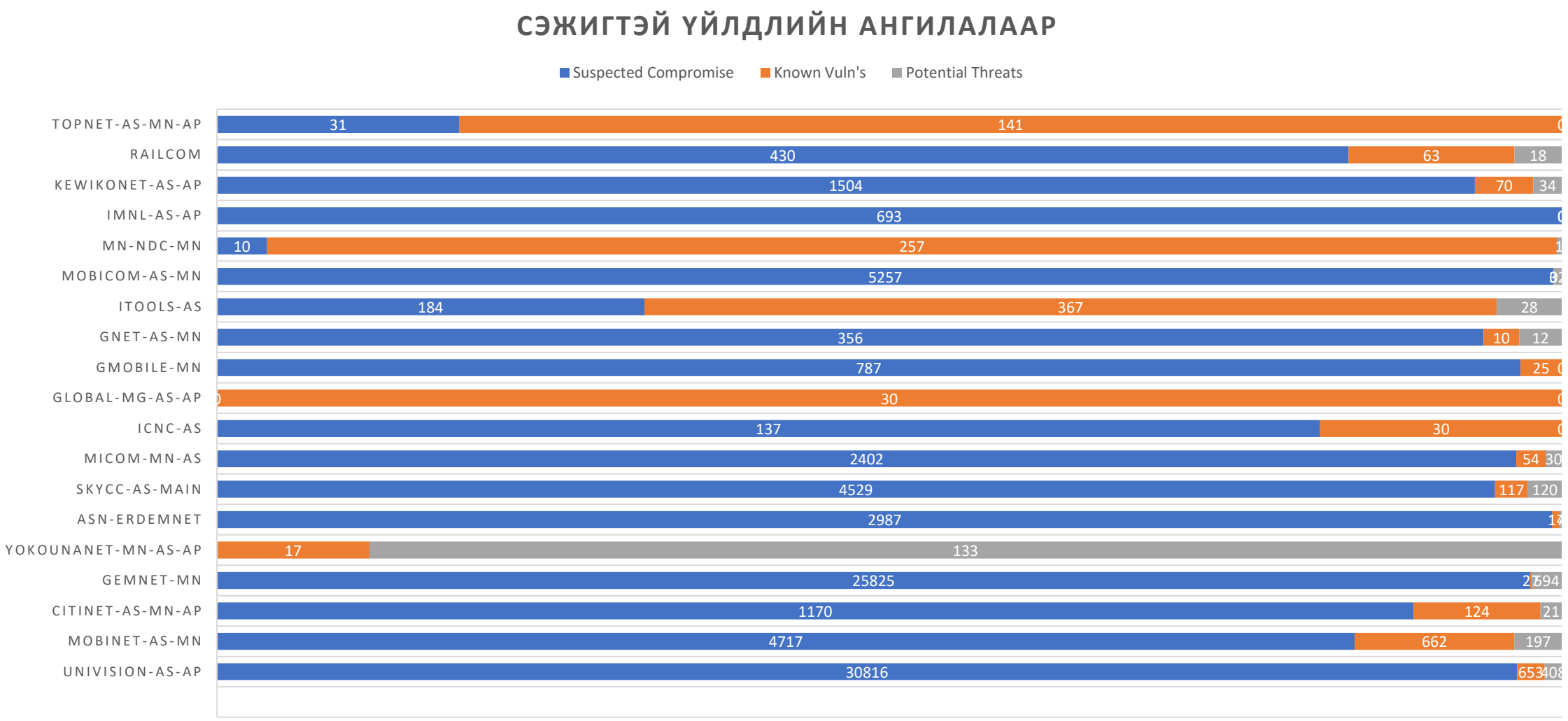
Top vulnerabilities

- SSL Poodle
  - Disclosed in 2014
  - SSL 3.0 and TLS 1.2
  - 1,886 hosts in Mongolia
- VMware ESXi Remote Code Execution Vulnerability
  - Disclosed in 2019
  - 490 hosts in Mongolia
- SSL Freak
  - Disclosed in 2015
  - 235 hosts in Mongolia

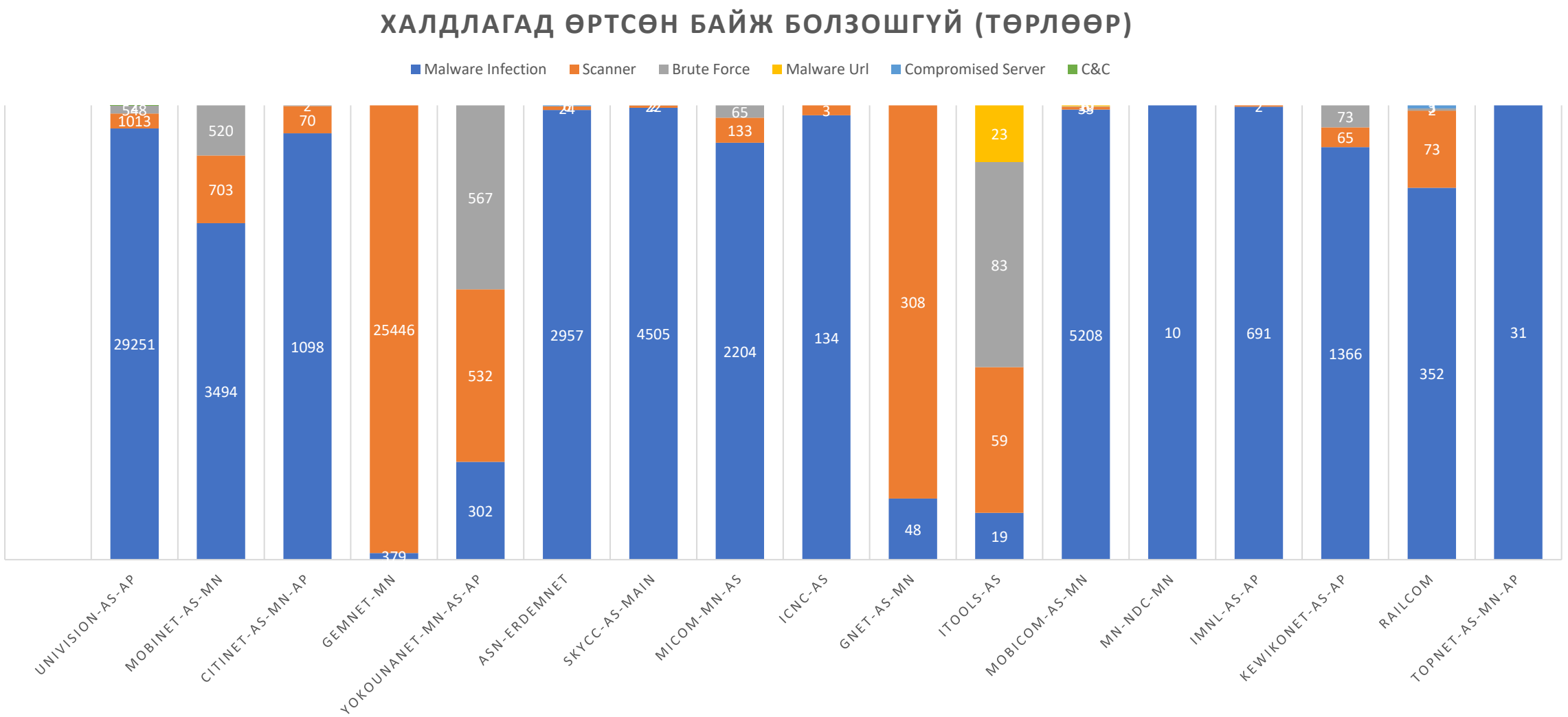
Top ISPs with most events



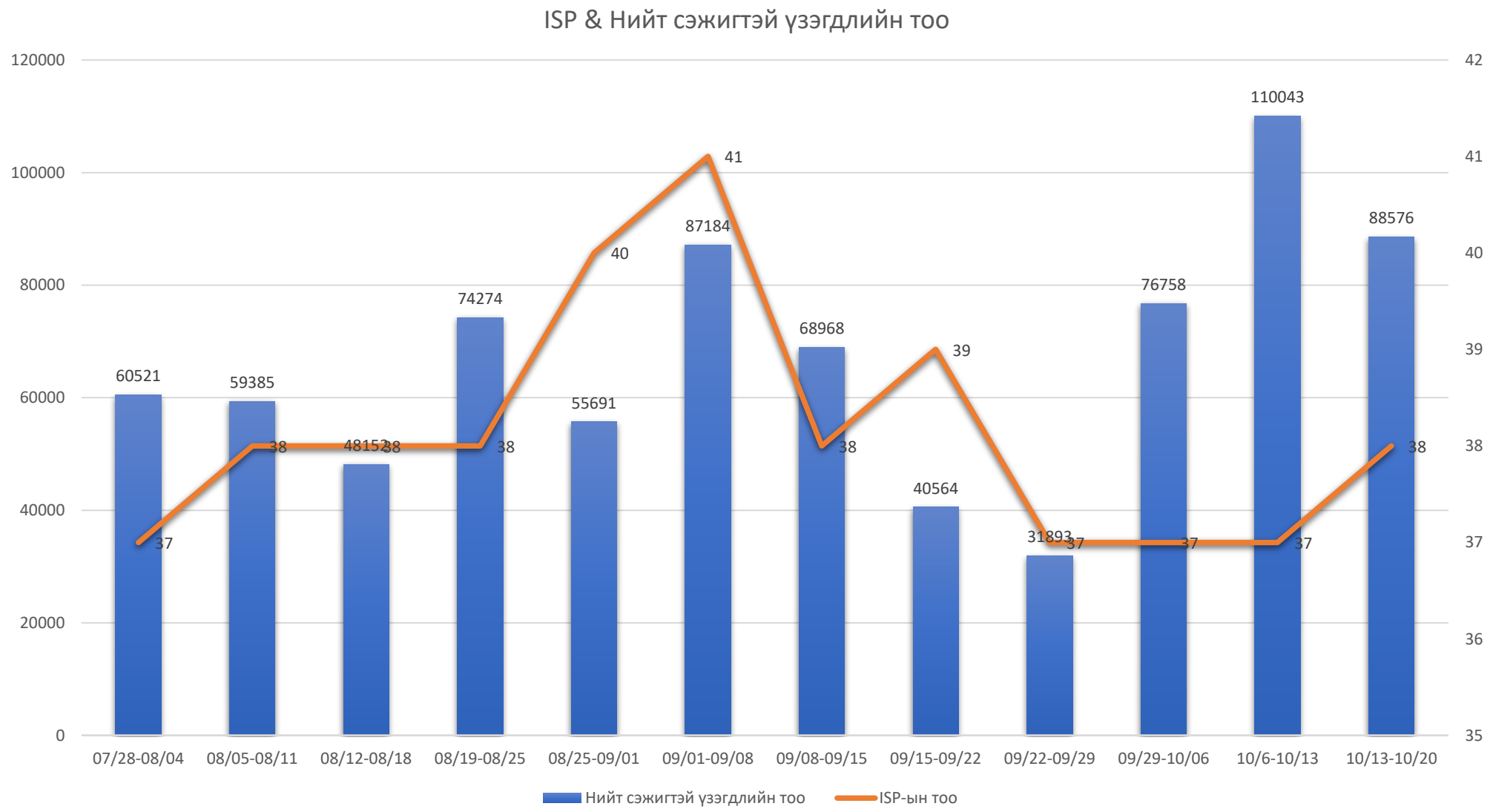
Event types per ISP



Compromise types



Event reports



Хортой кодонд нэрвэгдсэн байдал

В.Нямсүрэн
З.Цолмон
Т.Билэгдэмбэрэл
MNCERT/CC

Malwares found in Mongolian cyberspace

- Duration: 1st to 20th October
- Total number of malwares: 20

PlugX

- Number of known infections in Mongolia: 126
- Known to be used by APT group called Mustang Panda
- Remote access trojan for espionage
- Malicious actions: screen capture, keylogger, information stealing
- Infection vector: through zip, rar, sfx files in phishing

Sality

- Number of known infections in Mongolia: 51
- Criminal actor
- Malicious actions: resource consumption, member of botnet
- Infection vector: USB drive, network share

Иргэдийн цахим хэрэглээ, нууц үг сонголтын эрсдэл

М.Отгонпүрэв

Д.Дэлгэрбат

Б.Номуун

Previous study

- Done by MMCG under the contract of CRC
- Random sample on 1,030 people in 2021
- *“ИРГЭДИЙН ИНТЕРНЭТИЙН ХЭРЭГЛЭЭНИЙ ТАЛААРХ СУУРЬ СУДАЛГААНЫ ТАЙЛАН”*[1]

[1]https://crc.gov.mn/storage/busad/03_Survey%20report_MMCG_final-2021.pdf

Key highlights

- *38% нь цахим хаяг дах нууц үгээ 6 сар тутам солихыг хичээдэг боловч 9% нь тогтмол сольдог байна.*
- *5 хүн тутмын 1 нь сошиал медиа, имэйл хаягаа ямар нэгэн байдлаар өөрөө болон бусдыг хакердуулж байсан тохиолдол өөрт нь болон ойр дотны нэгэнд нь тулгарч байсан байна.*
- *Иргэдийн 27.0% нь өөрийн төхөөрөмждөө ямар нэг байдлаар вирусийн хамгаалалт, firewall, хатуу диск зэргийг хэрэглэж байгаа бол 42.6% нь хамгаалалтгүй, 30.5% нь хамгаалалт байгаа эсэхийг мэдэхгүй байна.*

88%

Цахим орчинд нууц үг үүсгэхдээ аль болох өөрт эргэн санахад хялбар зөвхөн тоо эсвэл тэмдэгт ашиглах нь амар.

82%

Сошиал хаяг болон санхүүгийн төлбөр тооцоо хийдэг апп-уудын (банкны апп зэрэг) нууц үг өөр өөр байдаг.

With the advent of the cloud computing

- Password cracking became accessible[1]
  - AWS p3.16xlarge
  - 632GH/s (632.000.000.000 NTLM hashes)
  - 25$ per hour

[1]https://thesecurityfactory.be/password-cracking-speed/

Average duration of password crack

Password Length	Numerical 0-9	Upper & Lower case a-Z	Numerical Upper & Lower case 0-9 a-Z	Numerical Upper & Lower case Special characters 0-9 a-Z %$
1	instantly	instantly	instantly	instantly
2	instantly	instantly	instantly	instantly
3	instantly	instantly	instantly	instantly
4	instantly	instantly	instantly	instantly
5	instantly	instantly	instantly	instantly
6	instantly	instantly	instantly	20 sec
7	instantly	2 sec	6 sec	49 min
8	instantly	1 min	6 min	5 days
9	instantly	1 hr	6 hr	2 years
10	instantly	3 days	15 days	330 years
11	instantly	138 days	3 years	50k years
12	2 sec	20 years	162 years	8m years
13	16 sec	1k years	10k years	1bn years
14	3 min	53k years	622k years	176bn years
15	26 min	3m years	39m years	27tn years
16	4 hr	143m years	2bn years	4qdn years

Redline password stealer

- Malware as a Service (MaaS)
- First observed in 2020
- Steals: browser credentials, crypto wallets
- Attack vector: malicious attachments, twitter, instagramm DMs
- Exfiltration: HTTP Post to C2
- Monthly, weekly, lifetime subscriptions (100$, 150$, 800$)

Dump file

- Bought on underground forum
- Filtered by .mn domain
- Provided by a partner of MNCERT/CC
- 1 record = URL, username, password

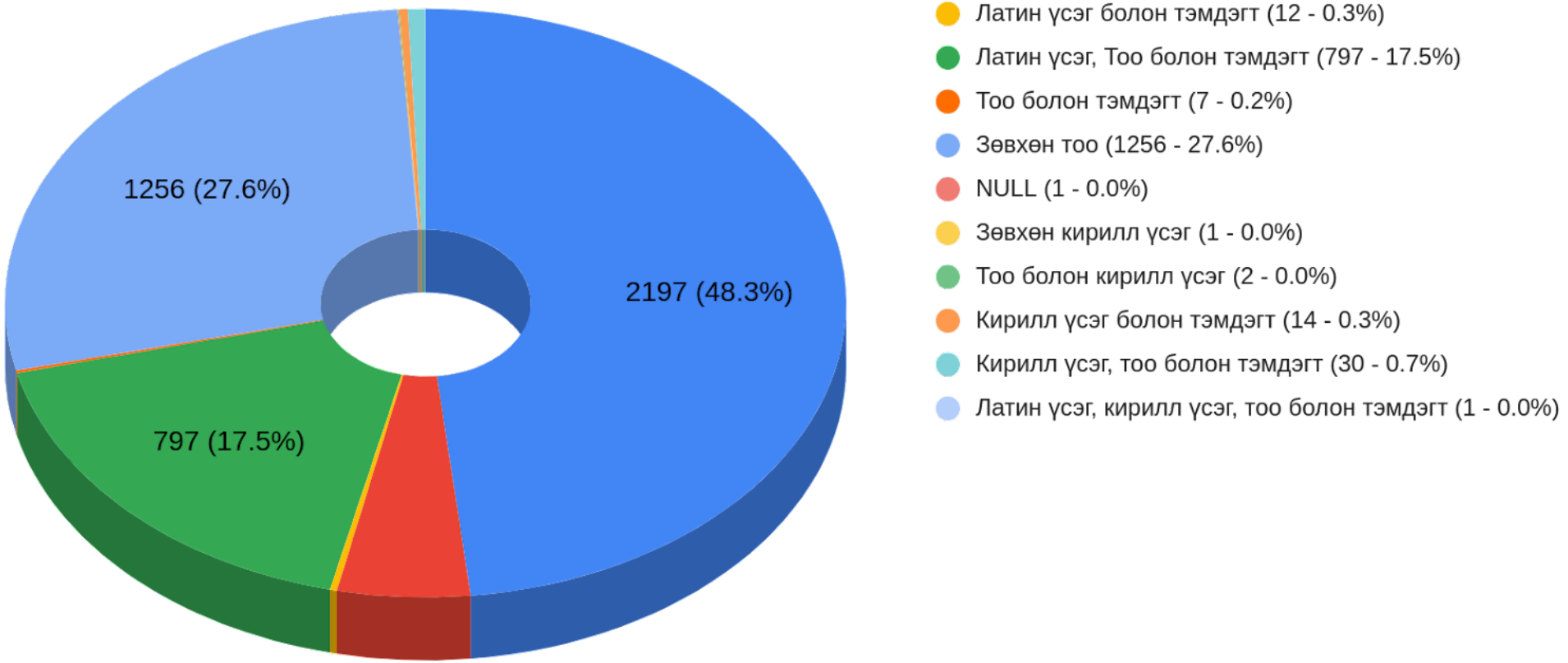
Data to be analyzed

	Redline 2022	Redline 2023
Total records	10050	19448
Duplicate entry	5500	10930
Duplicate in previous repo	0	78
Total unique	4550	8440
Unique username	3374	6260
Unique password	3217	5669
Unique domain	579	1057

Data Analysis Results

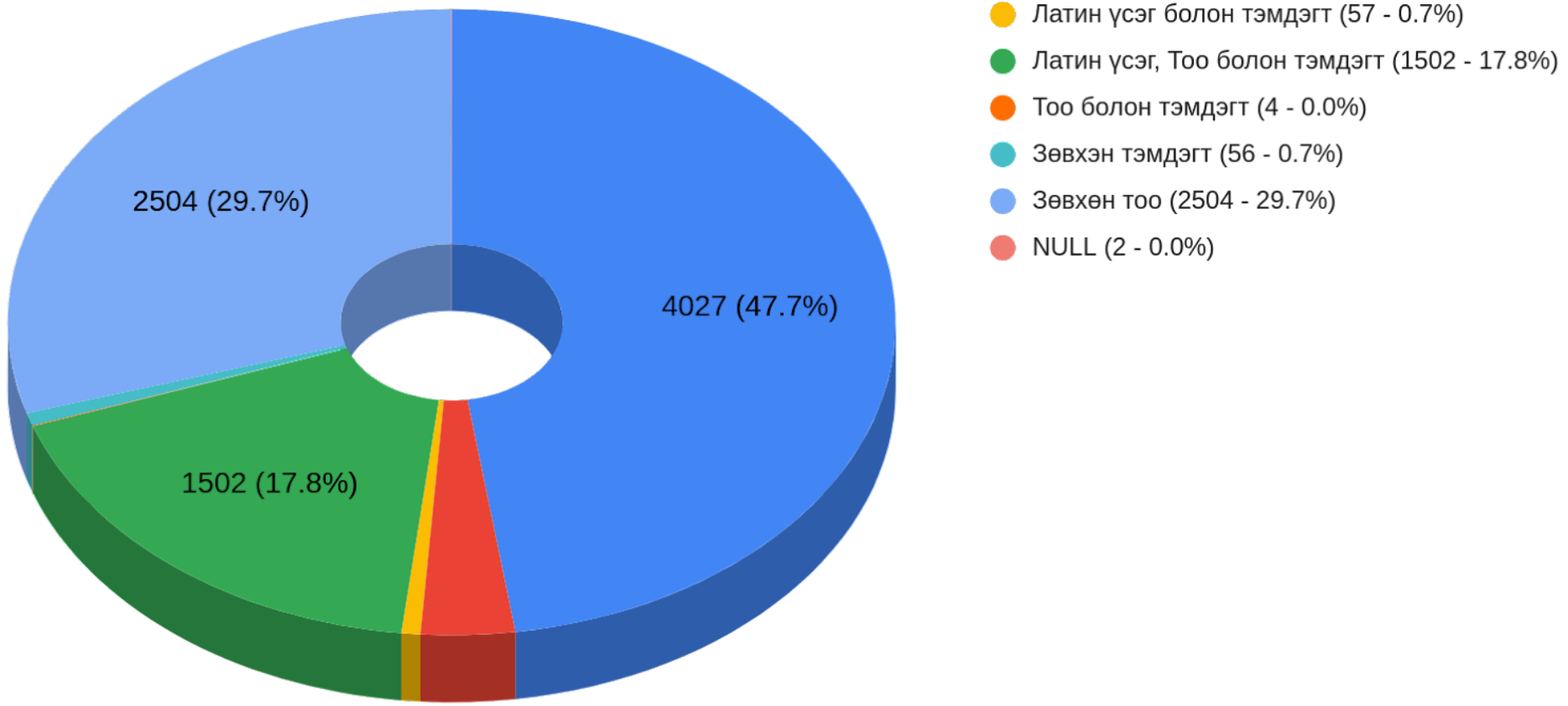
Redline 2022

- Composition on unique 4550 passwords

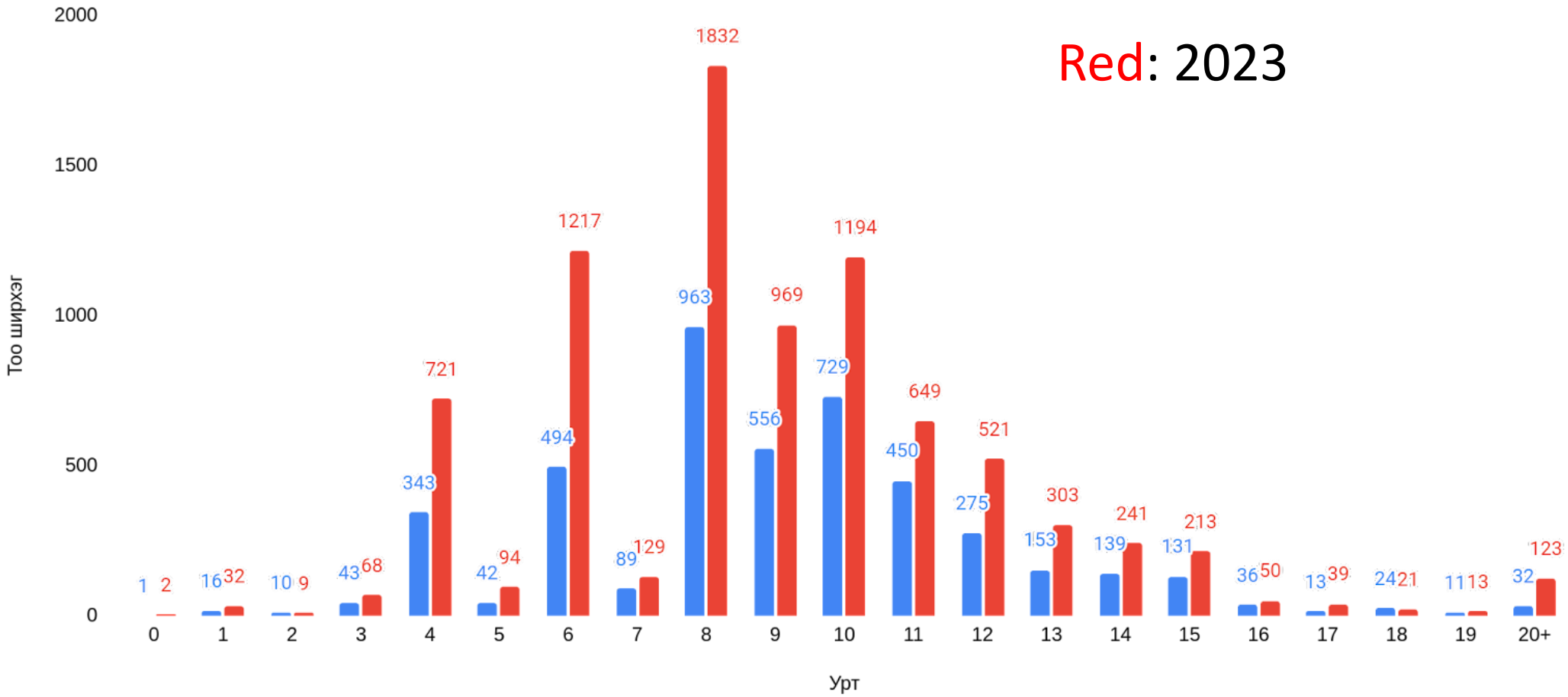


Redline 2023

- Composition on unique 8440 passwords

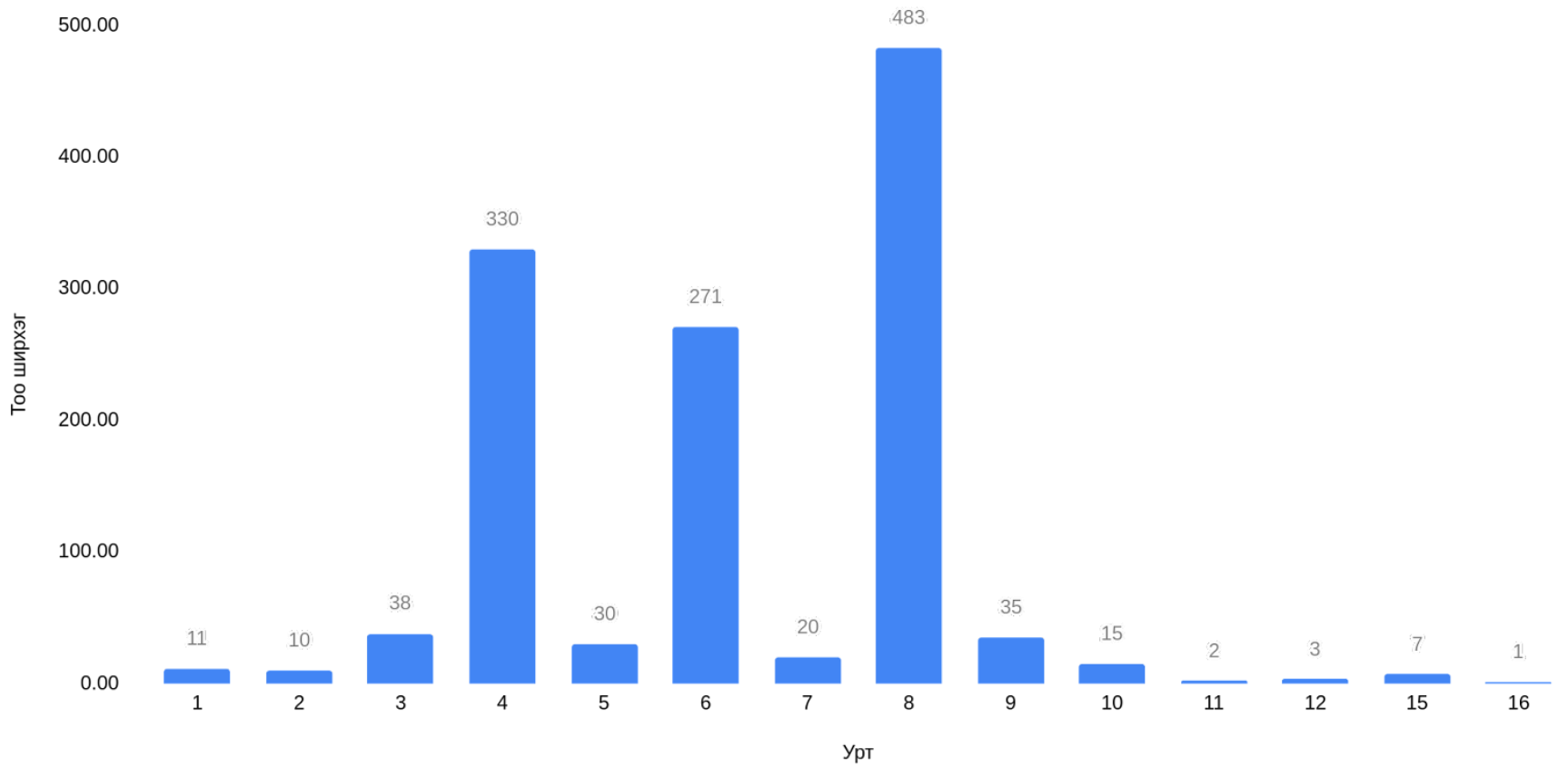


Password length



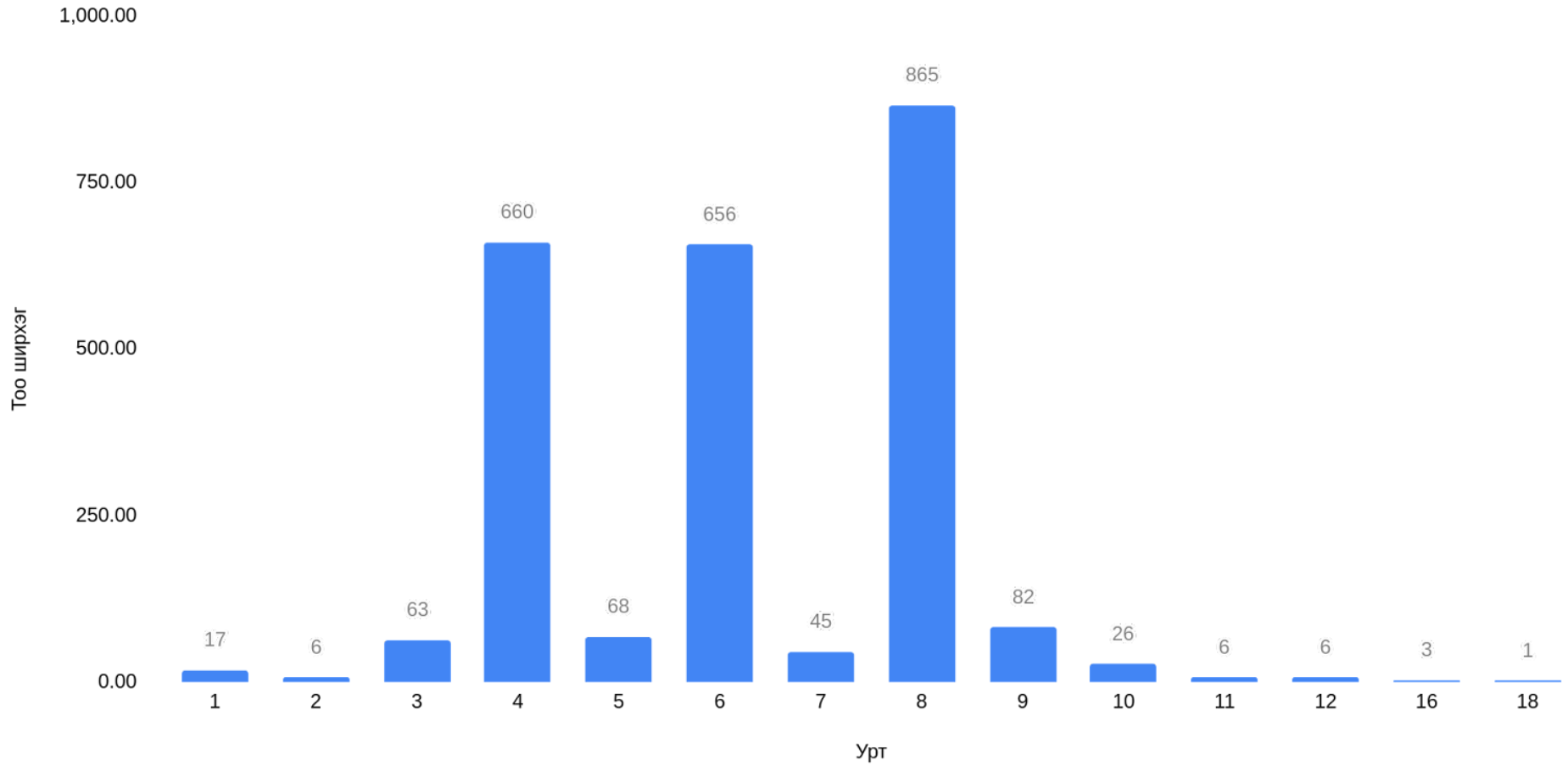
Length of numeric only passwords: 2022

Total: 1,256



Length of numeric only passwords: 2023

Total: 2,504



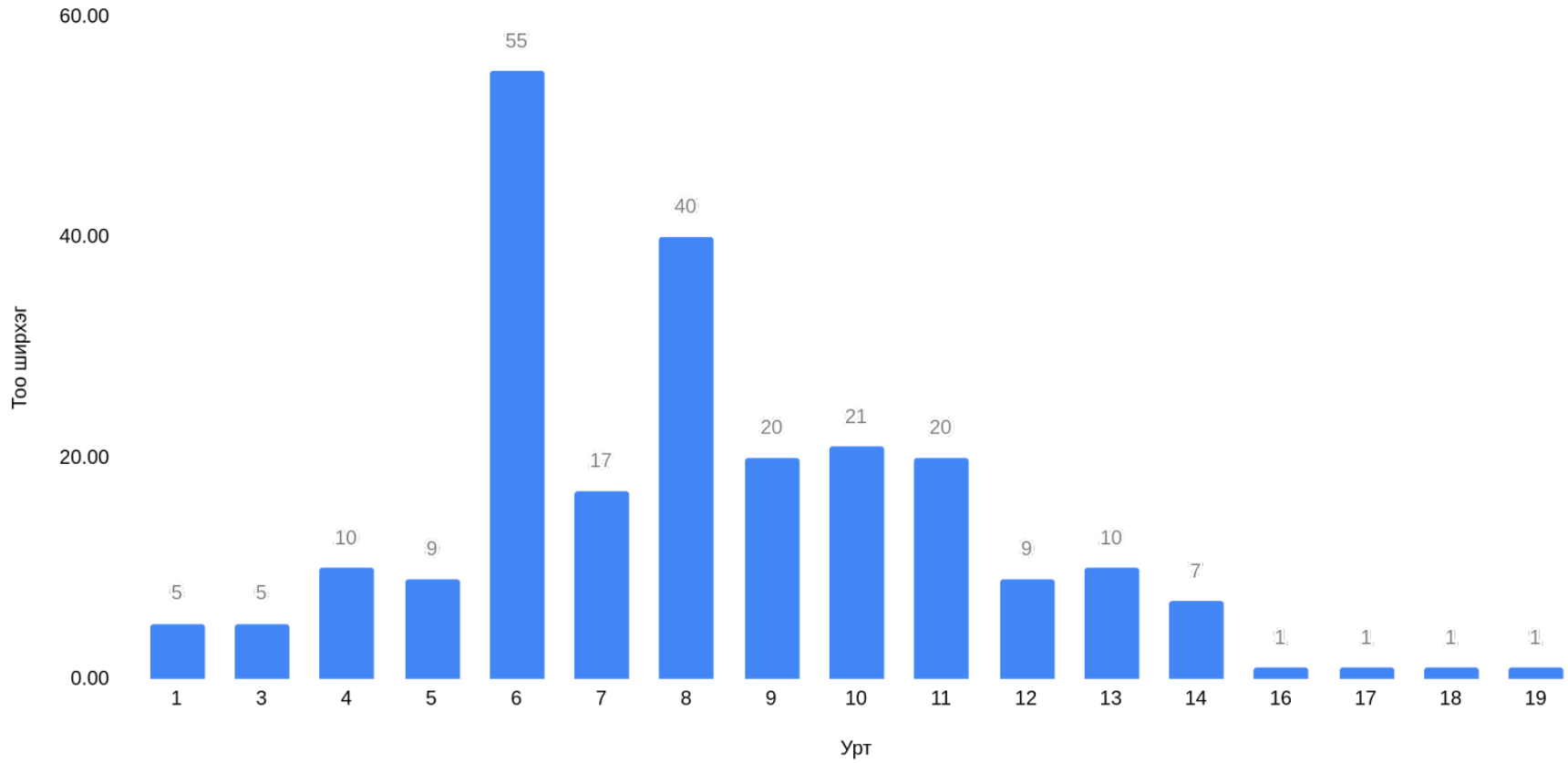
Crackability:

2022: 99.92%
2023: 99.84%

Password Length	Numerical 0-9
1	instantly
2	instantly
3	instantly
4	instantly
5	instantly
6	instantly
7	instantly
8	instantly
9	instantly
10	instantly
11	instantly
12	2 sec
13	16 sec
14	3 min
15	26 min
16	4 hr

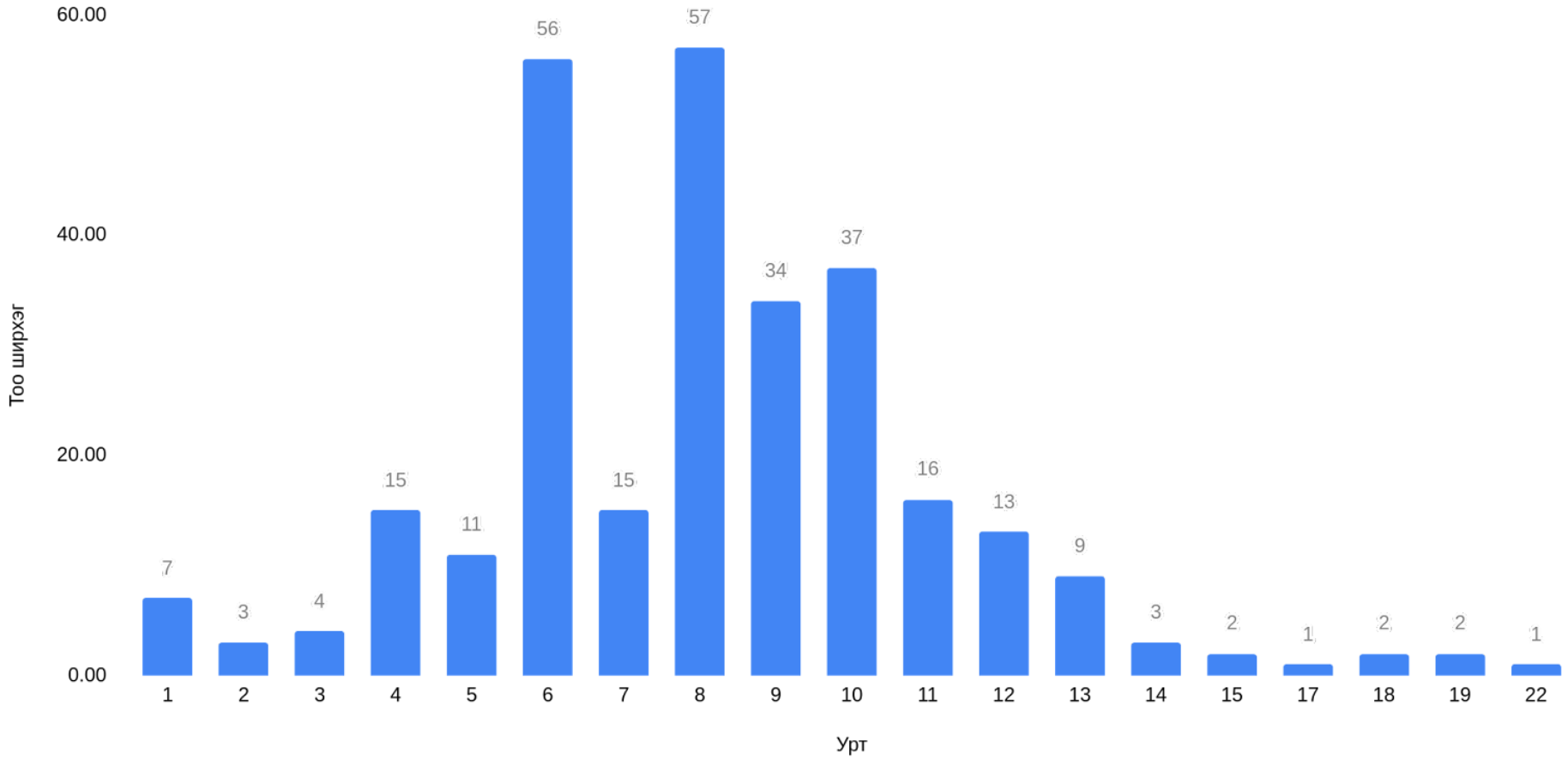
Upper & Lowercase a-Z: 2022

Total: 232



Upper & Lowercase a-Z: 2023

Total: 288



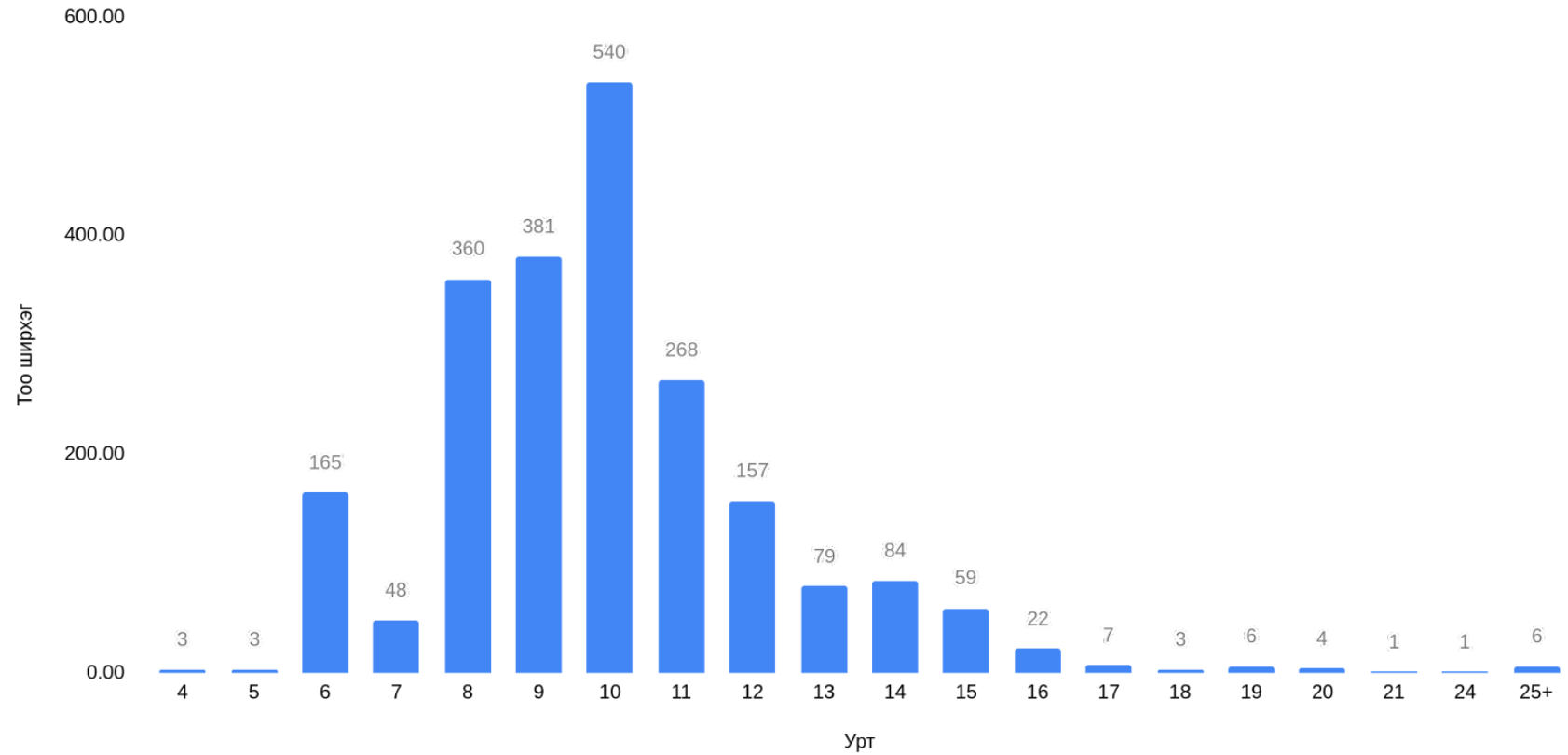
Crackability:

2022: 69.4%
2023: 70.14%

Password Length	Upper & Lower case a-Z
1	instantly
2	instantly
3	instantly
4	instantly
5	instantly
6	instantly
7	2 sec
8	1 min
9	1 hr
10	3 days
11	138 days
12	20 years
13	1k years
14	53k years
15	3m years
16	143m years

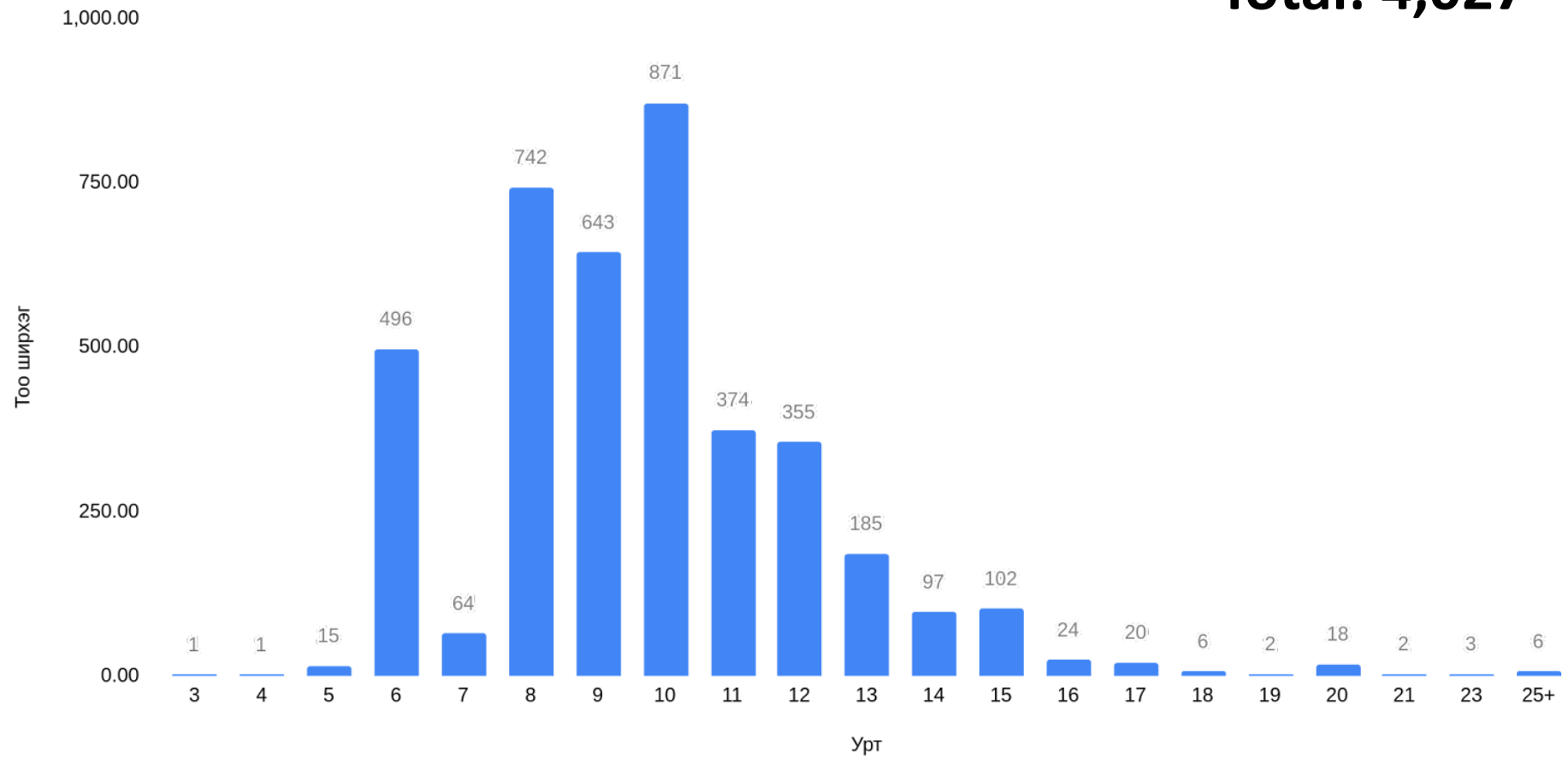
Numerical and upper & lowercase: 2022

Total: 2,197



Numerical and upper & lowercase: 2023

Total: 4,027



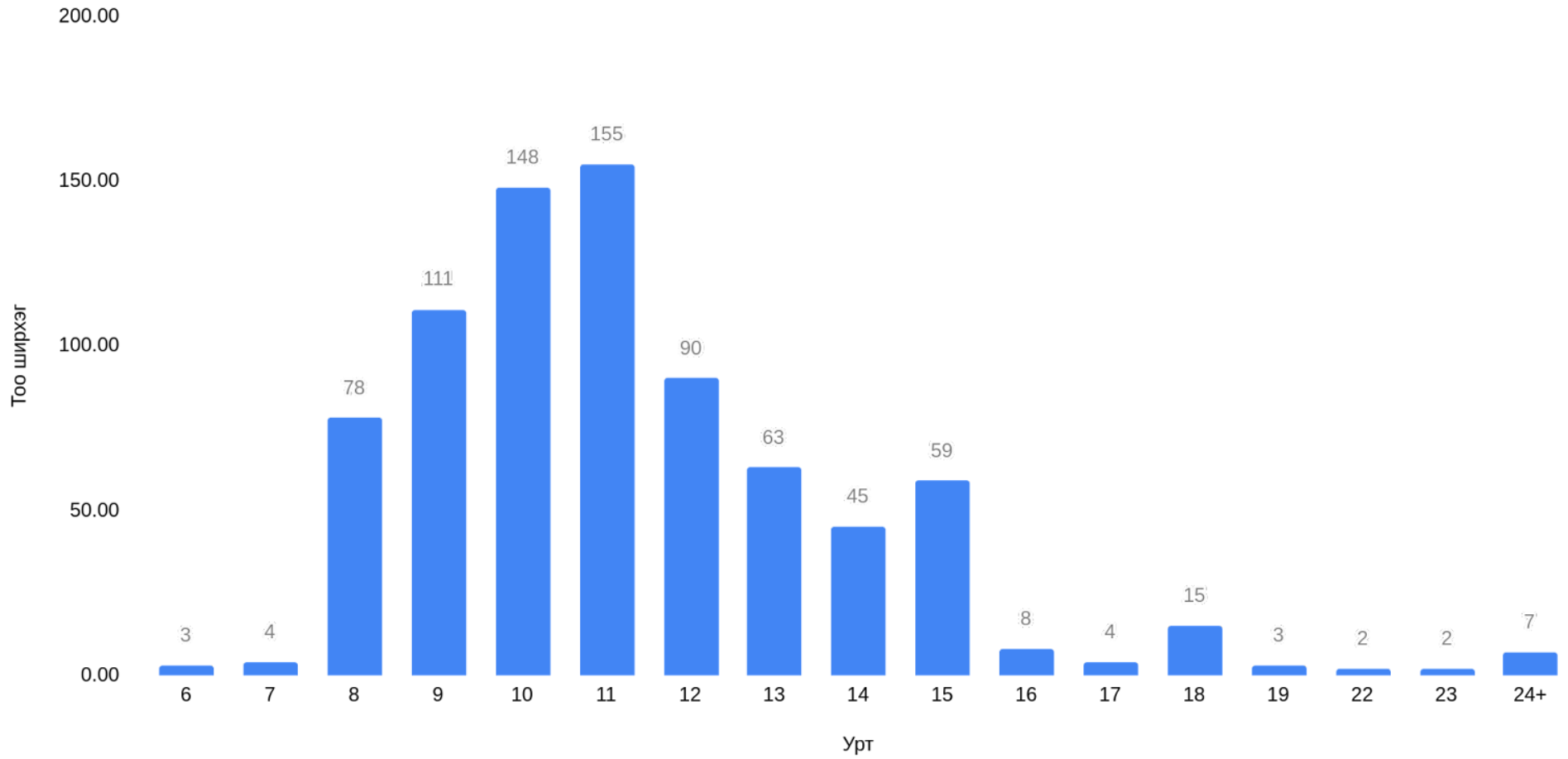
Crackability:

2022: 26.35%
2023: 32.75%

Password Length	Numerical Upper & Lower case 0-9 a-Z
1	instantly
2	instantly
3	instantly
4	instantly
5	instantly
6	instantly
7	6 sec
8	6 min
9	6 hr
10	15 days
11	3 years
12	162 years
13	10k years
14	622k years
15	39m years
16	2bn years

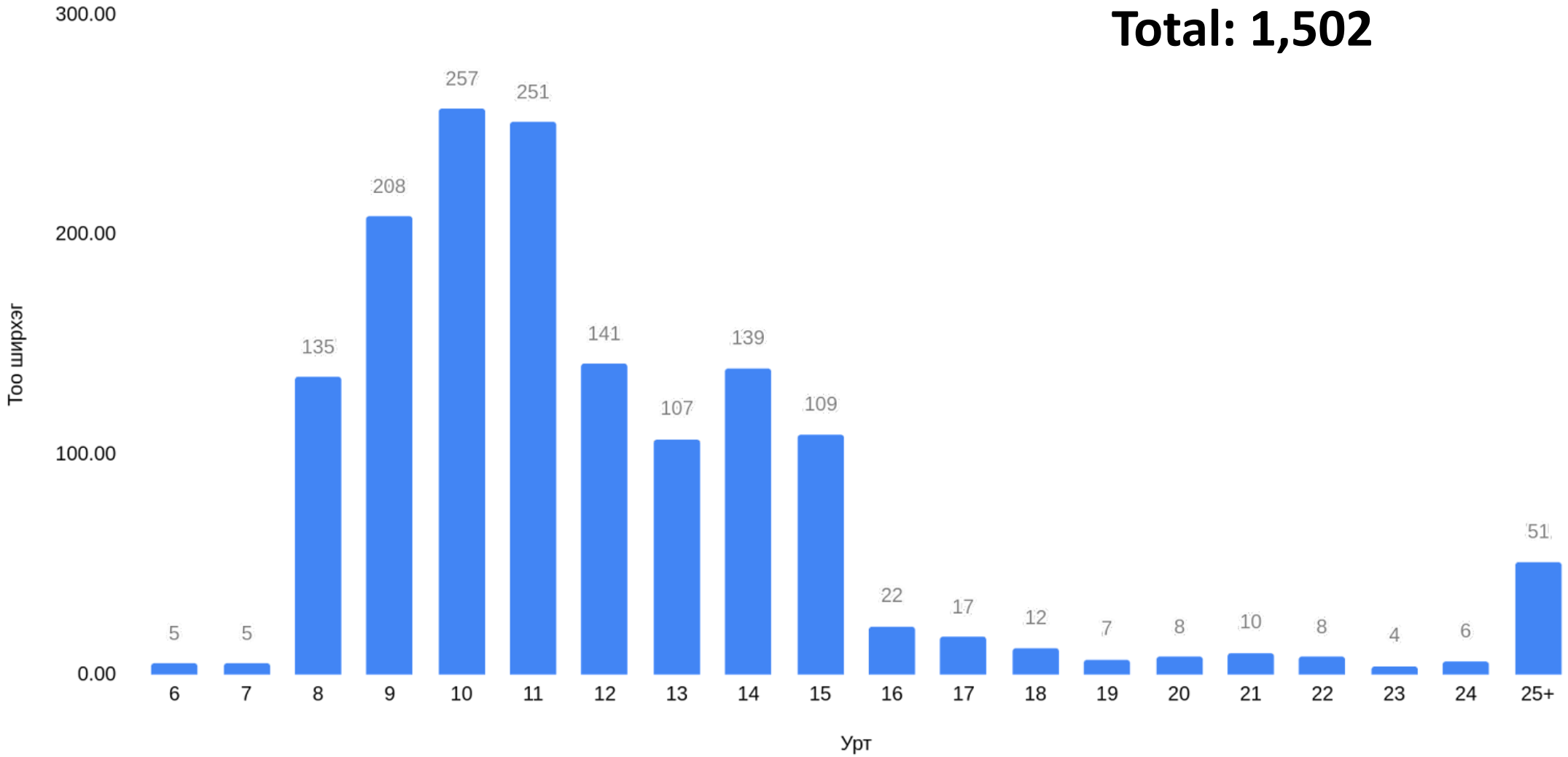
All characters: 2022

Total: 797



All characters: 2023

Total: 1,502



Crackability:

2022: 0.87%
2023: 0.66%

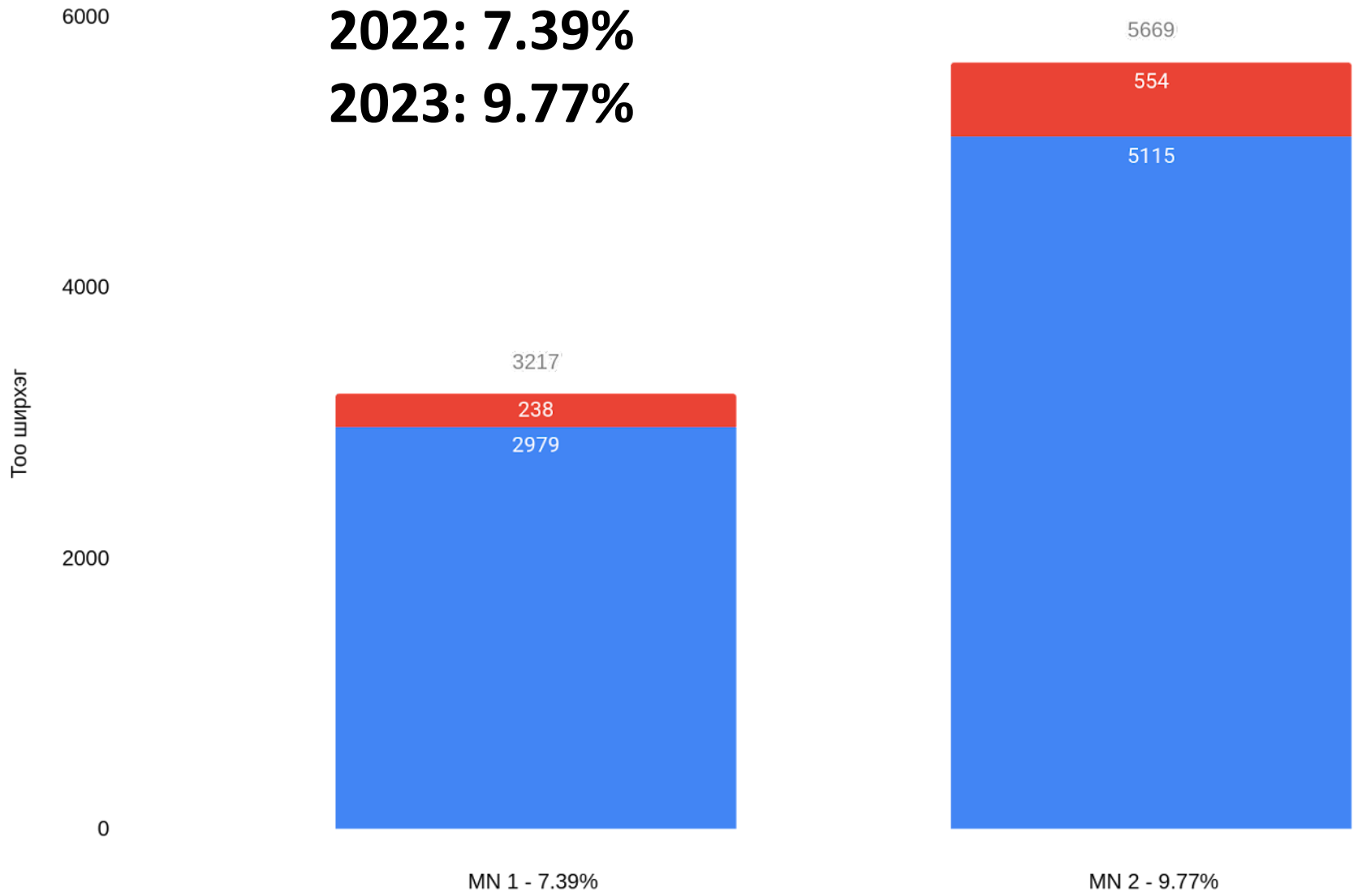
Password Length	Numerical Upper & Lower case Special characters 0-9 a-Z %$
1	instantly
2	instantly
3	instantly
4	instantly
5	instantly
6	20 sec
7	49 min
8	5 days
9	2 years
10	330 years
11	50k years
12	8m years
13	1bn years
14	176bn years
15	27tn years
16	4qdn years

Dictionary Attacks

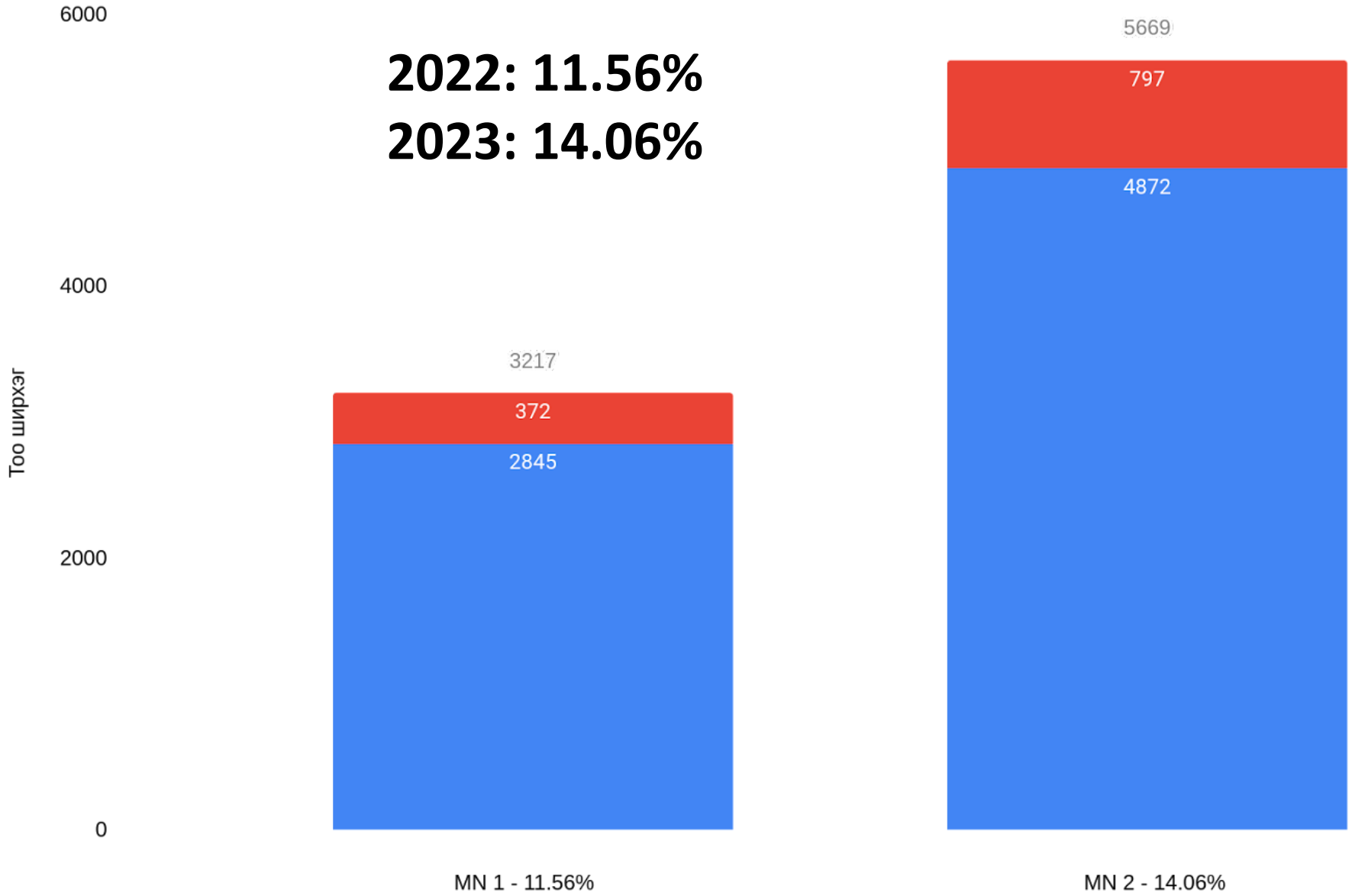
- Most common 10,000 English words
- Most common 100,000 English words

- Less than 1 second on AWS p3.16xlarge

Susceptibility to Dictionary Attacks: 10K words



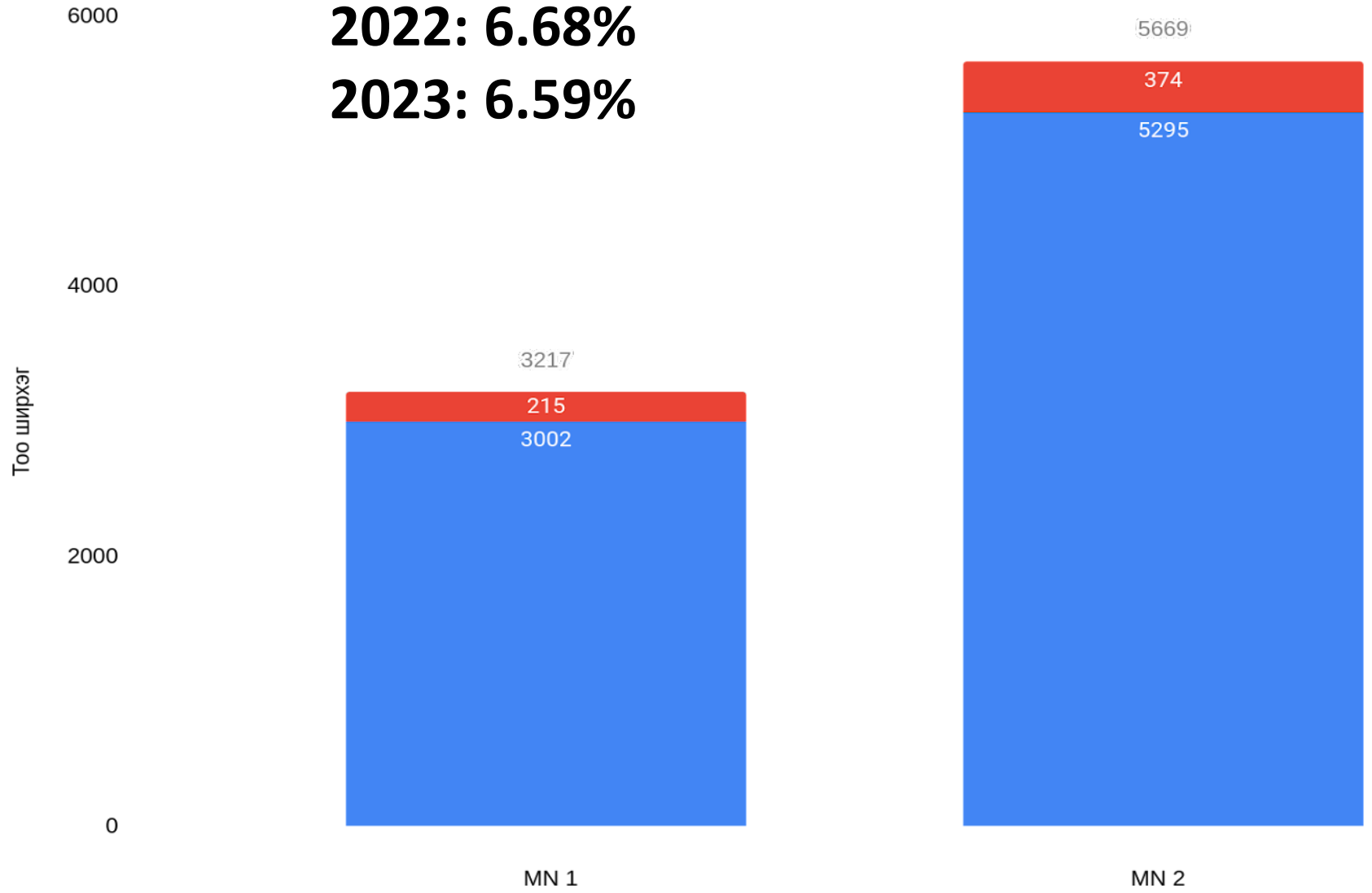
Susceptibility to Dictionary Attacks: 100K words



Password reuse

2022: 6.68%

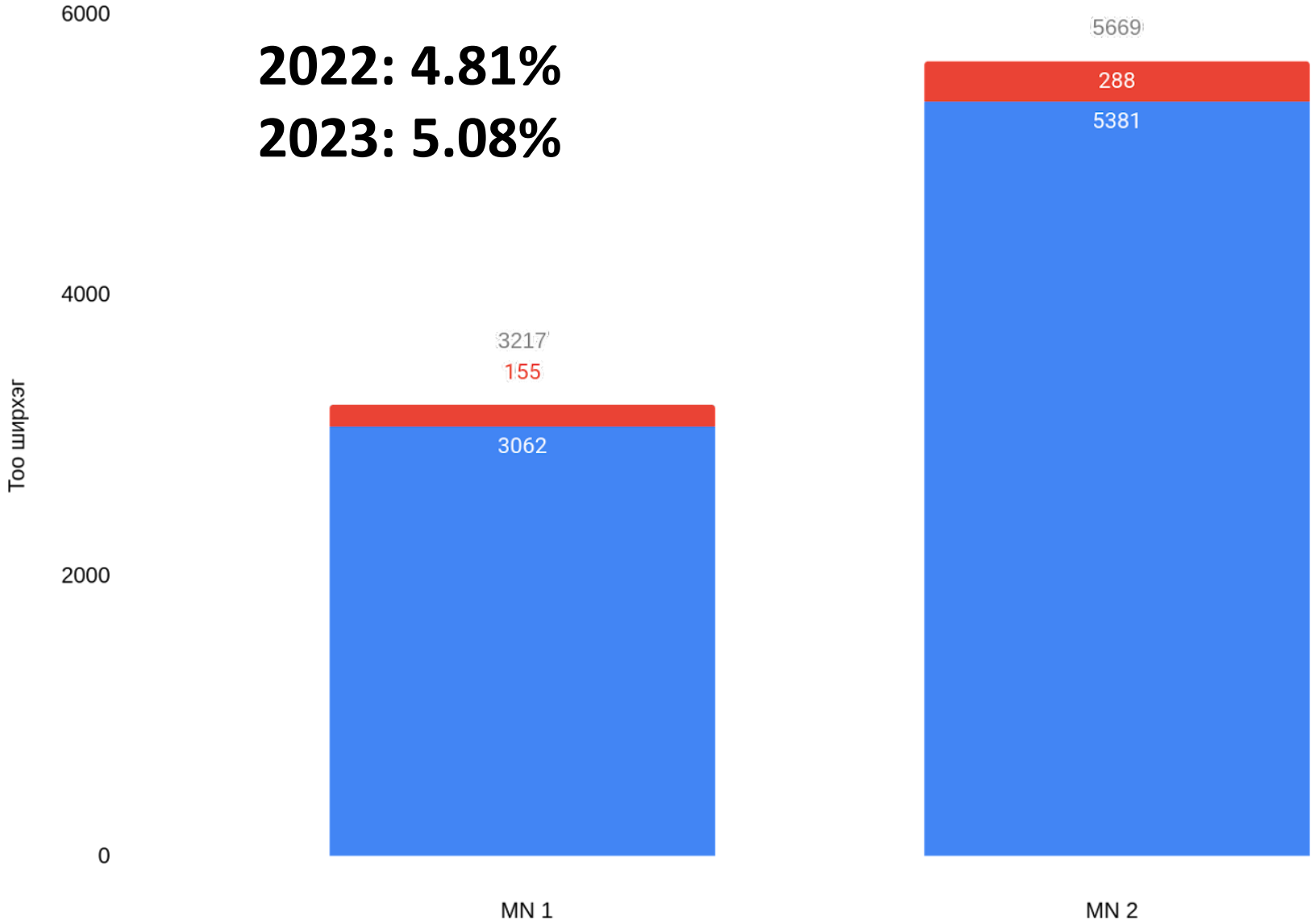
2023: 6.59%



Username contained in password

2022: 4.81%

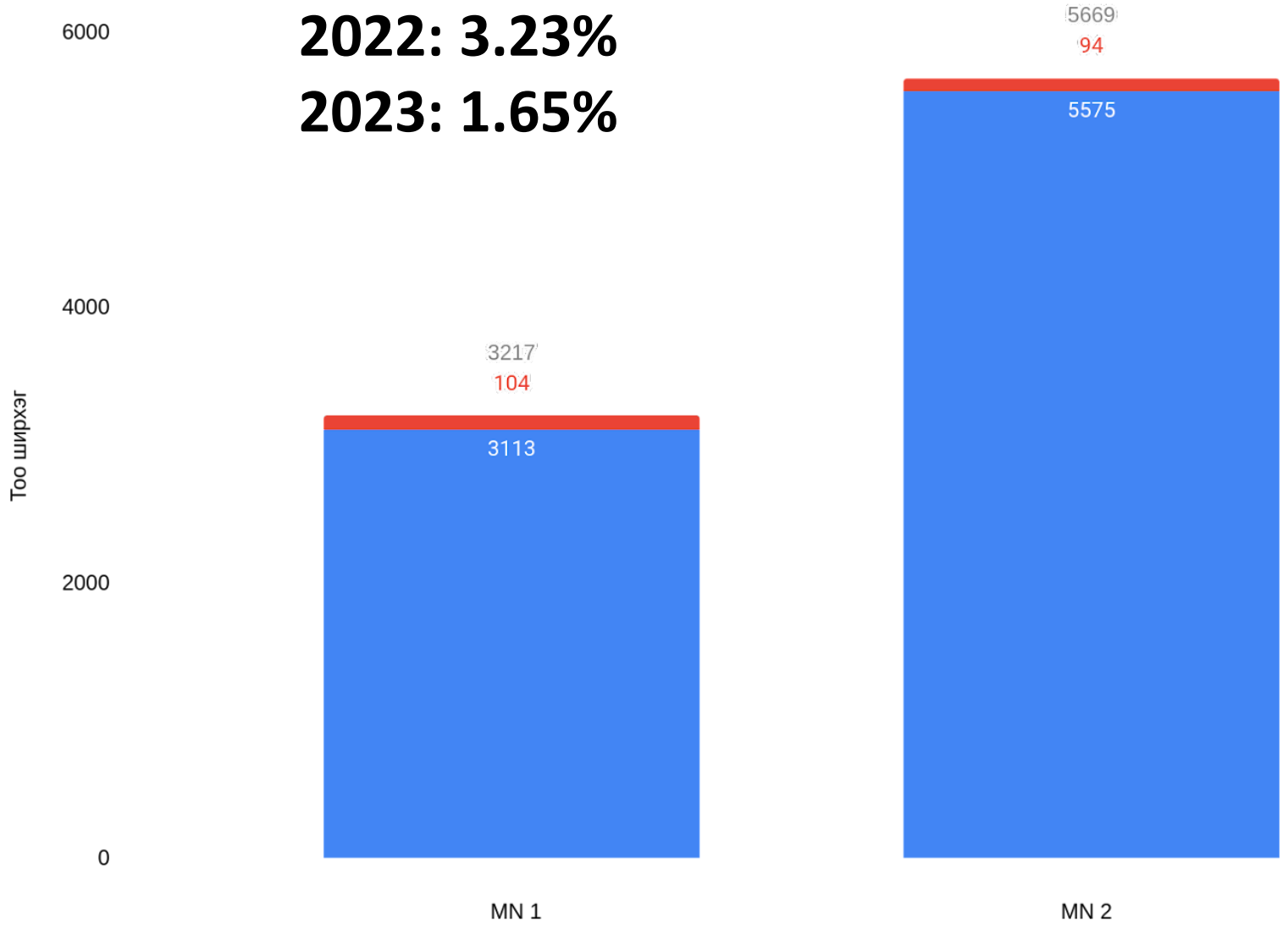
2023: 5.08%



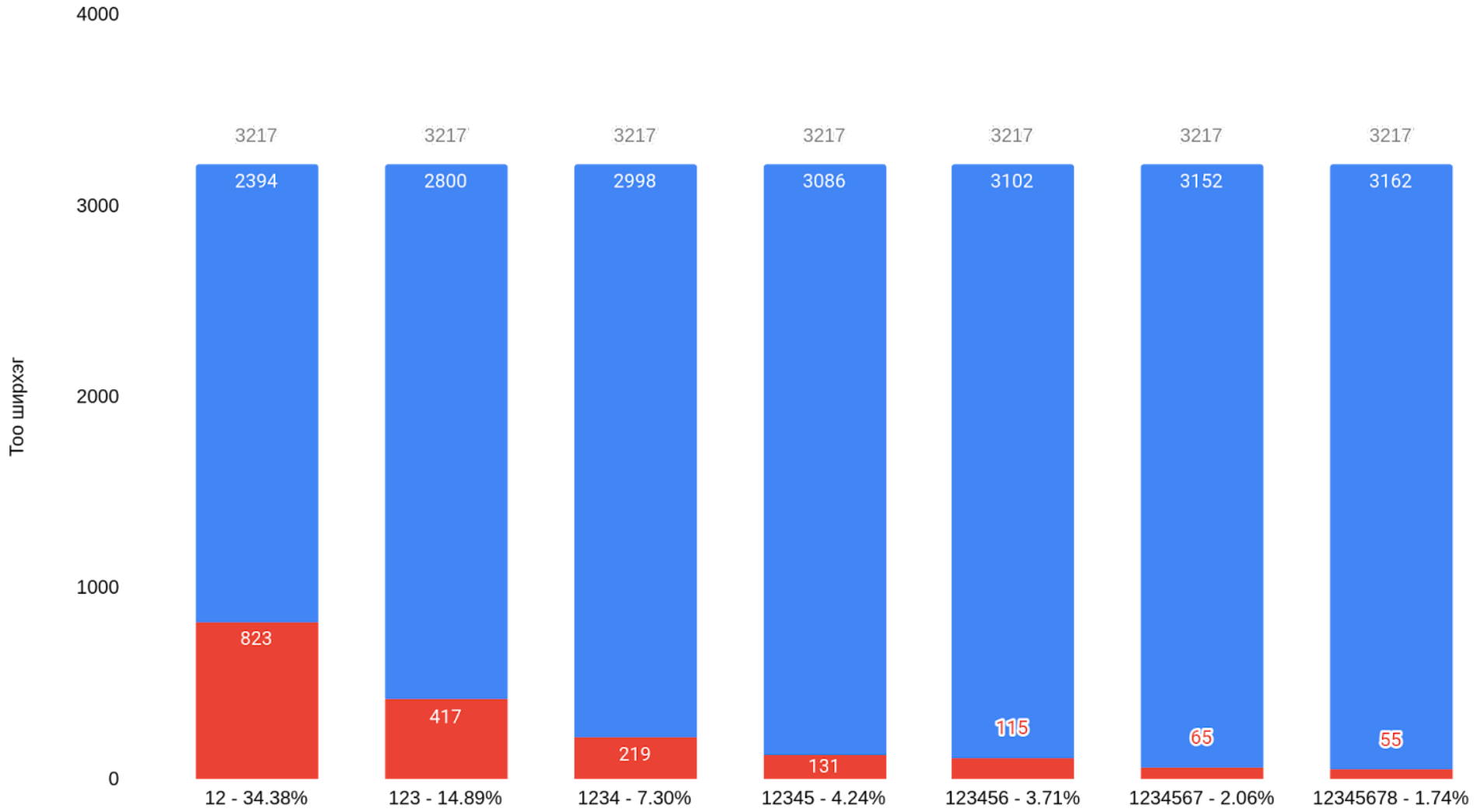
Domain name contained in password

2022: 3.23%

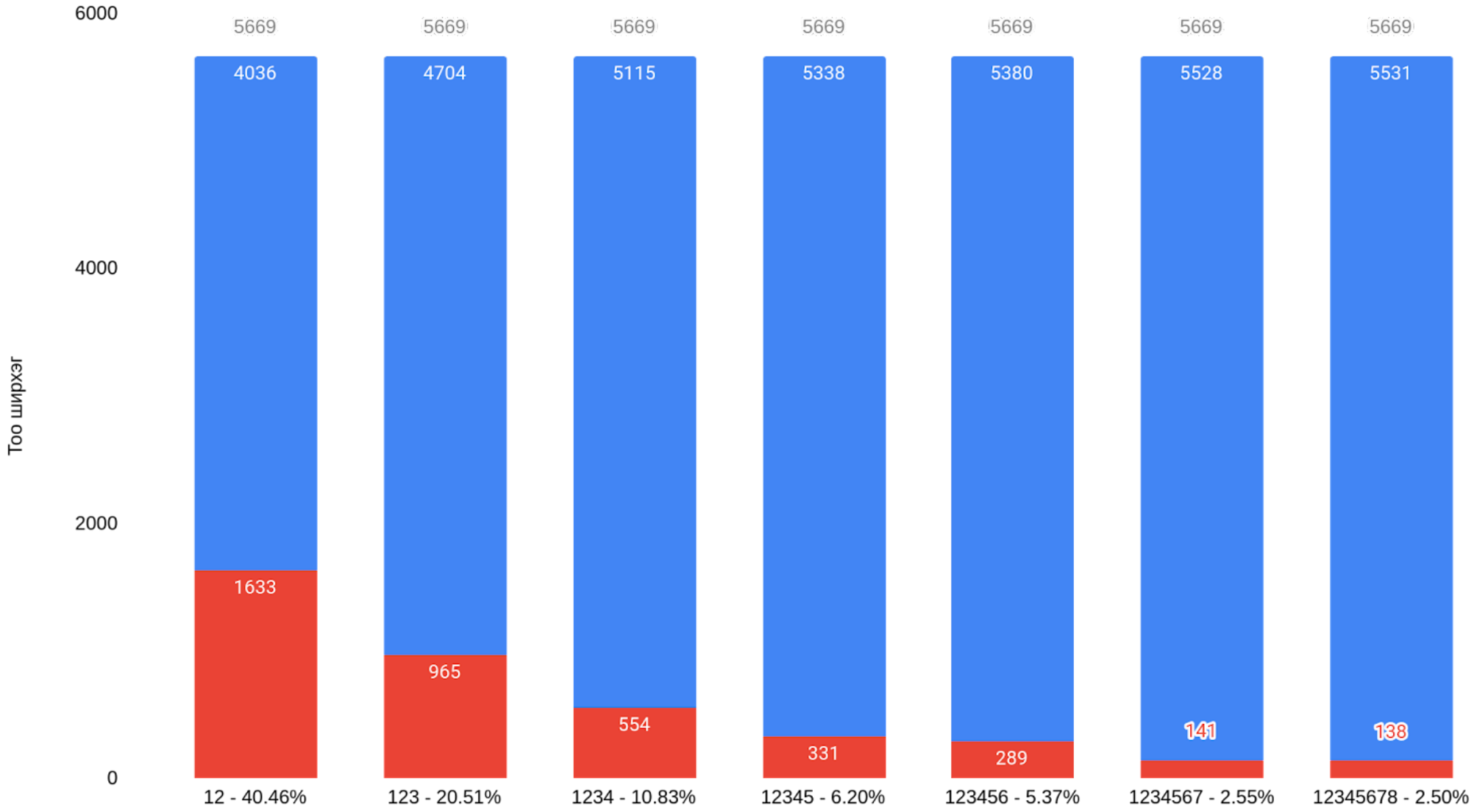
2023: 1.65%



Sequential numbers: 2022



Sequential numbers: 2023



Conclusion

Internet

- 1 in 3 IP’s are in blacklist
- Weekly ~40,000 security events in ~177,000 active Ips
- 95% of security events are compromise
- Hosts still have vulnerabilities disclosed in 2014
- 75% of infected malware in Mongolia is trojan

Passwords

- 47% of passwords are less than 8 characters
- 71% of Mongolian users are susceptible to password cracking (increase from 62% from 2022)
- 14% of Mongolian users are susceptible to dictionary attacks
- 82% of online service providers are not enforcing strong password policy

“If you think technology can solve your security problems, then you don’t understand the problems and you don’t understand the technology.”

- Bruce Schneier