



SPAMHAUS

Botnet Threat Report

The big picture

- 2018 saw an 8% increase in detected botnet C&C compared to 2017
- 10,000 C&C mark reached for the first time in 2018
- Increased focus on stealing credentials directly from end users rather than resorting to phishing (phishing is still trending up too!)

Global overview

| Rank | Botnet controllers | Country |
|------|--------------------|---------|
| 1 | 2272 | US |
| 2 | 1939 | RU |
| 3 | 1080 | NL |
| 4 | 457 | DE |
| 5 | 350 | FR |
| 6 | 305 | GB |
| 7 | 265 | UA |
| 8 | 233 | CA |
| 9 | 21 | CH |
| 10 | 177 | LT |
| 11 | 175 | BG |
| 12 | 173 | TR |
| 13 | 157 | CN |
| 14 | 150 | CL |
| 15 | 149 | RO |
| 16 | 122 | SG |
| 17 | 101 | IT |
| 18 | 99 | MY |
| 19 | 95 | ZA |
| 20 | 93 | PL |



Malware families associated with C&Cs

| Rank | C&Cs | Malware | Note |
|------|-------|--------------------|-------------------------------------|
| 1 | 2,347 | Lokibot | Credential Stealer |
| 2 | 1,300 | JBifrost | Java based Remote Access Tool (RAT) |
| 3 | 955 | Pony | Dropper/Credential Stealer |
| 4 | 915 | AZORult | Credential Stealer |
| 5 | 686 | Heodo/Emotet | Dropper/Backdoor |
| 6 | 413 | Gozi ISFB | e-banking Trojan |
| 7 | 322 | NanoCore | Remote Access Tool (RAT) |
| 8 | 269 | Smoke Loader | Dropper/Backdoor |
| 9 | 241 | TrickBot | e-banking Trojan |
| 10 | 203 | RemcosRAT | Remote Access Tool (RAT) |
| 11 | 157 | RedAlert | Android Trojan |
| 12 | 122 | NetWire | Remote Access Tool (RAT) |
| 13 | 117 | AgentTesla | KeyLogger/Remote Access Tool (RAT) |
| 14 | 107 | Chthonic | e-banking Trojan |
| 15 | 106 | PandaZeuS | e-banking Trojan |
| 16 | 98 | ImminentRat | Remote Access Tool (RAT) |
| 17 | 96 | Neurevt | e-banking Trojan |
| 18 | 82 | ISRStealer | Credential Stealer |
| 19 | 70 | ArkeiStealer | Credential Stealer |
| 20 | 51 | NjRAT | Remote Access Tool (RAT) |
| - | 89 | CoinMiners malware | Various crypto currency miners |
| - | 46 | IoT malware | Various IoT malware |
| - | 456 | Generic | * |
| - | 1,015 | Others | Other malware families |

* C&Cs where the associated malware could not be identified

Malware families: a closer look



Credential stealers

Lead the pack in proliferation



Remote Access Tools

Significant increase over 2018



Banking Trojans & Ransomware

Decreased by nearly 100%



Cryptominers

Newcomers to the report



Mining Pools

Abuse has been observed

Botnet C&C domains

Top abused TLDs

| Rank | Domains | TLD | Note |
|------|---------|----------|--|
| 1 | 13,422 | pw | ccTLD of Palau |
| 2 | 11,815 | com | gTLD |
| 3 | 10,909 | review | gTLD |
| 4 | 9,399 | top | gTLD |
| 5 | 7,464 | stream | gTLD |
| 6 | 6,894 | download | gTLD |
| 7 | 5,983 | tk | originally ccTLD, now effectively gTLD |
| 8 | 5,704 | xyz | gTLD |
| 9 | 5,427 | ml | originally ccTLD, now effectively gTLD |
| 10 | 3,735 | bid | gTLD |
| 11 | 2,461 | ga | originally ccTLD, now effectively gTLD |
| 12 | 2,183 | gq | originally ccTLD, now effectively gTLD |
| 13 | 2,137 | cf | originally ccTLD, now effectively gTLD |
| 14 | 1,684 | info | gTLD |
| 15 | 1,504 | sx | ccTLD of Sint Maarten |
| 16 | 1,350 | trade | gTLD |
| 17 | 1,182 | ru | ccTLD of Russia |
| 18 | 1,081 | science | gTLD |
| 19 | 1,026 | win | gTLD |
| 20 | 650 | club | gTLD |

Botnet C&C Domains






















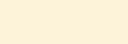
Free gTLDs all moving into the top 20 (surprise!) of fraudulent or abused domains



Decentralized Top-Level Domains (dTLD) are not yet in the top 20

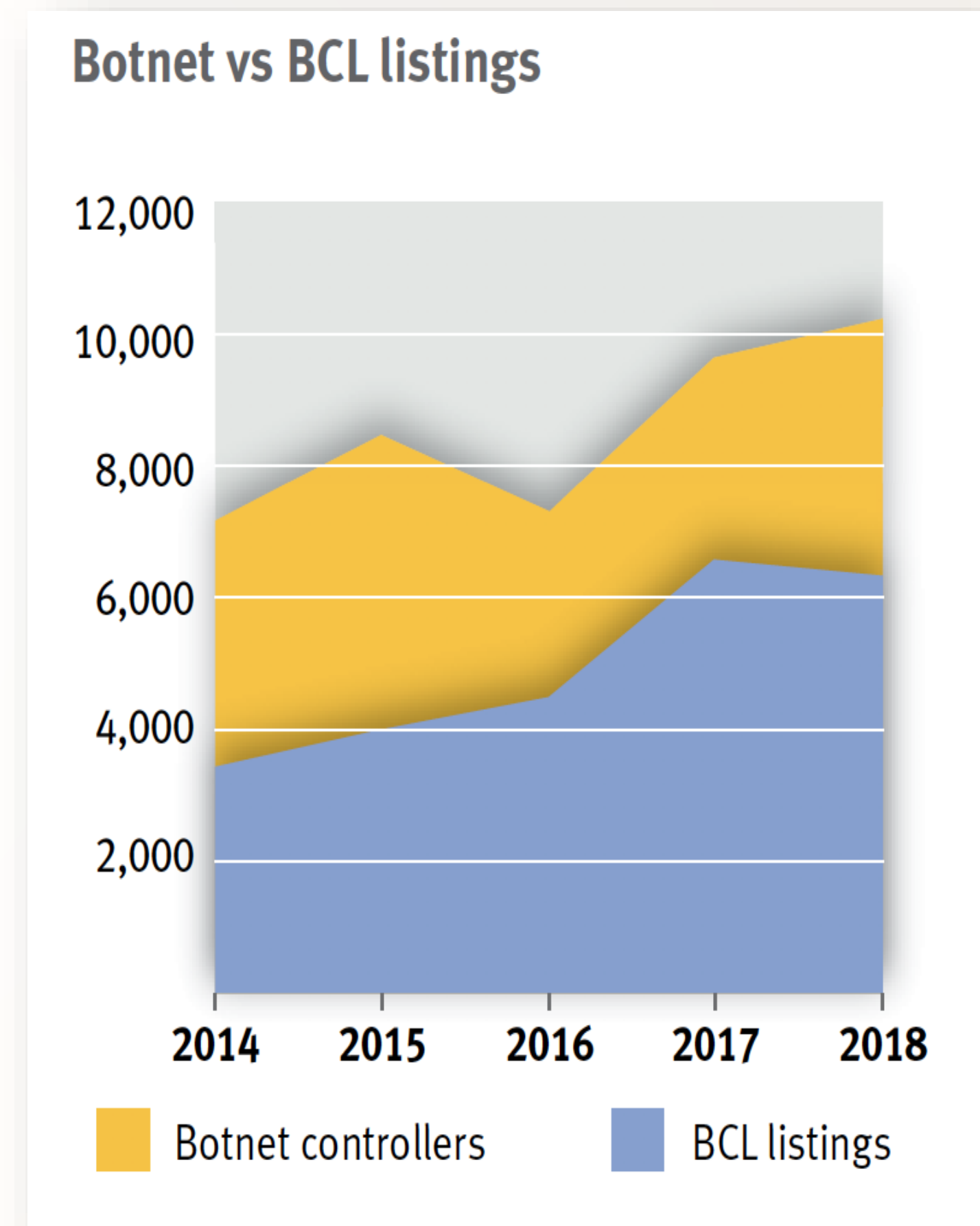
- No takedown/suspension process as there is no governing body
- Difficulty in restricting access due to not being accessible over common DNS

Fraudulent domain registrations

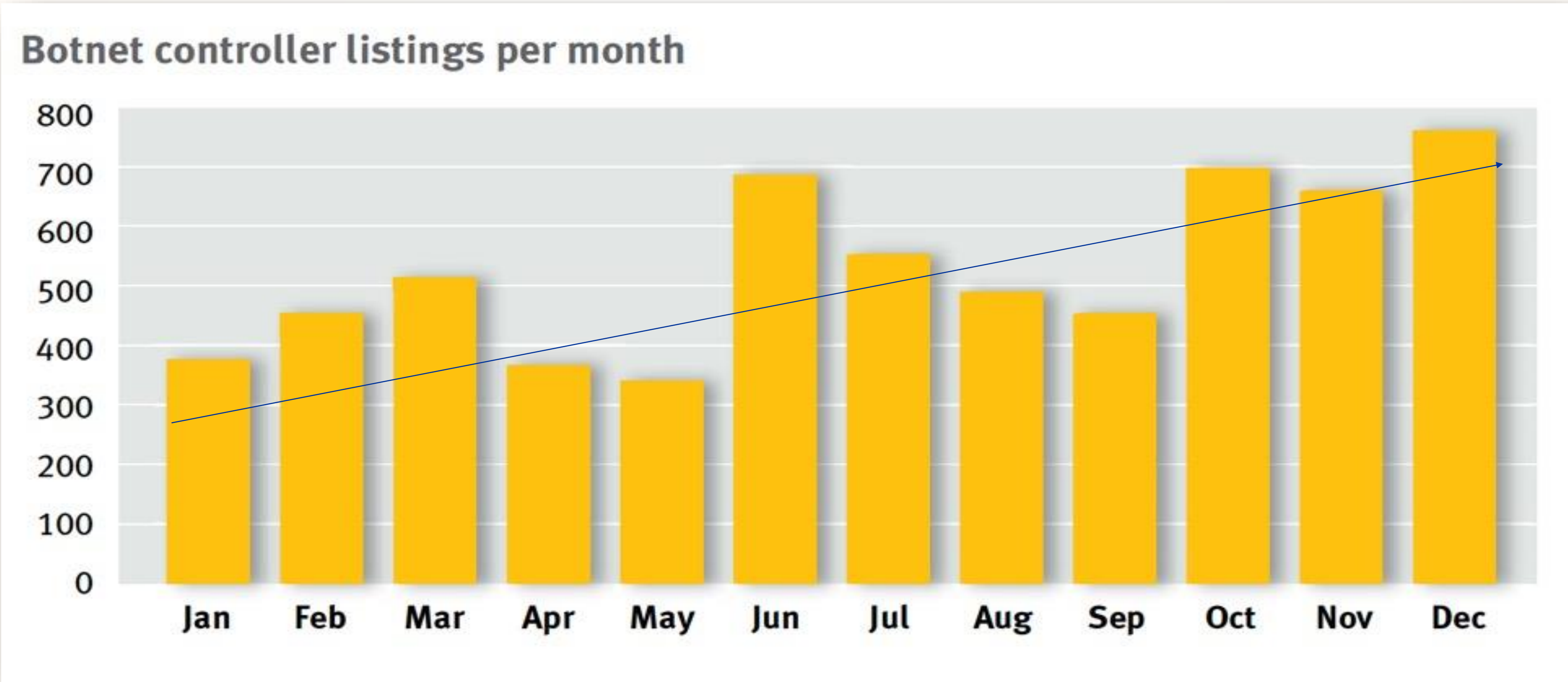
| Rank | Domains | Country |
|------|---------|--|
| 1 | 38,072 | United States  |
| 2 | 13,261 | India  |
| 3 | 3,322 | China  |
| 4 | 1,448 | Russia  |
| 5 | 908 | China  |
| 6 | 764 | United States  |
| 7 | 438 | United States  |
| 8 | 378 | United States  |
| 9 | 366 | China  |
| 10 | 339 | United States  |
| 11 | 311 | Spain  |
| 12 | 309 | Great Britain  |
| 13 | 291 | China  |
| 14 | 274 | United States  |
| 15 | 239 | Czech Republic  |
| 16 | 190 | Russia  |
| 17 | 175 | United States  |
| 18 | 167 | United States  |
| 19 | 159 | Russia  |
| 20 | 158 | Gibraltar  |

Fraudulent sign-ups fueling botnet proliferation

- 61 % of observed C&C activity were identified as fraud (68 percent in 2017)
- Operators prefer their “own” infrastructure to carry out their operations



Growth over botnet controllers in 2018



Total botnet C&C by ISP/hoster

Total botnet C&C hosting numbers by ISP

| Rank | C&Cs 2017 | C&Cs 2018 | % change | Country |
|------|-----------|-----------|-----------|----------------------|
| 1 | 100 | 704 | +604 ▲ | United States |
| 2 | 14 | 603 | +4,207 ▲ | Switzerland |
| 3 | 256 | 431 | +68 ▲ | Russia |
| 4 | 402 | 358 | -11 ▼ | France |
| 5 | 95 | 274 | +188 ▲ | Russia |
| 6 | 197 | 185 | -6 ▼ | China |
| 7 | 101 | 147 | +46 ▲ | France |
| 8 | 127 | 143 | +13 ▲ | Russia |
| 9 | 94 | 135 | +44 ▲ | Unites States |
| =10 | 200 | 116 | -42 ▼ | United Arab Emirates |
| =10 | 37 | 116 | +214 ▲ | Russia |
| 11 | 105 | 115 | +10 ▲ | Netherlands |
| =12 | 112 | 111 | -1 ▼ | Russia |
| =12 | 144 | 111 | -23 ▼ | Russia |
| 13 | 179 | 110 | -39 ▼ | United States |
| 14 | 1 | 107 | +10,600 ▲ | Ukraine |
| 15 | 39 | 97 | +149 ▲ | Russia |
| 16 | 0 | 91 | — | Russia |
| 17 | 81 | 90 | +11 ▲ | Belize |
| 18 | 231 | 86 | -63 ▼ | US |
| 19 | 0 | 77 | — | Turkey |
| 20 | 47 | 75 | +60 ▲ | United Kingdom |

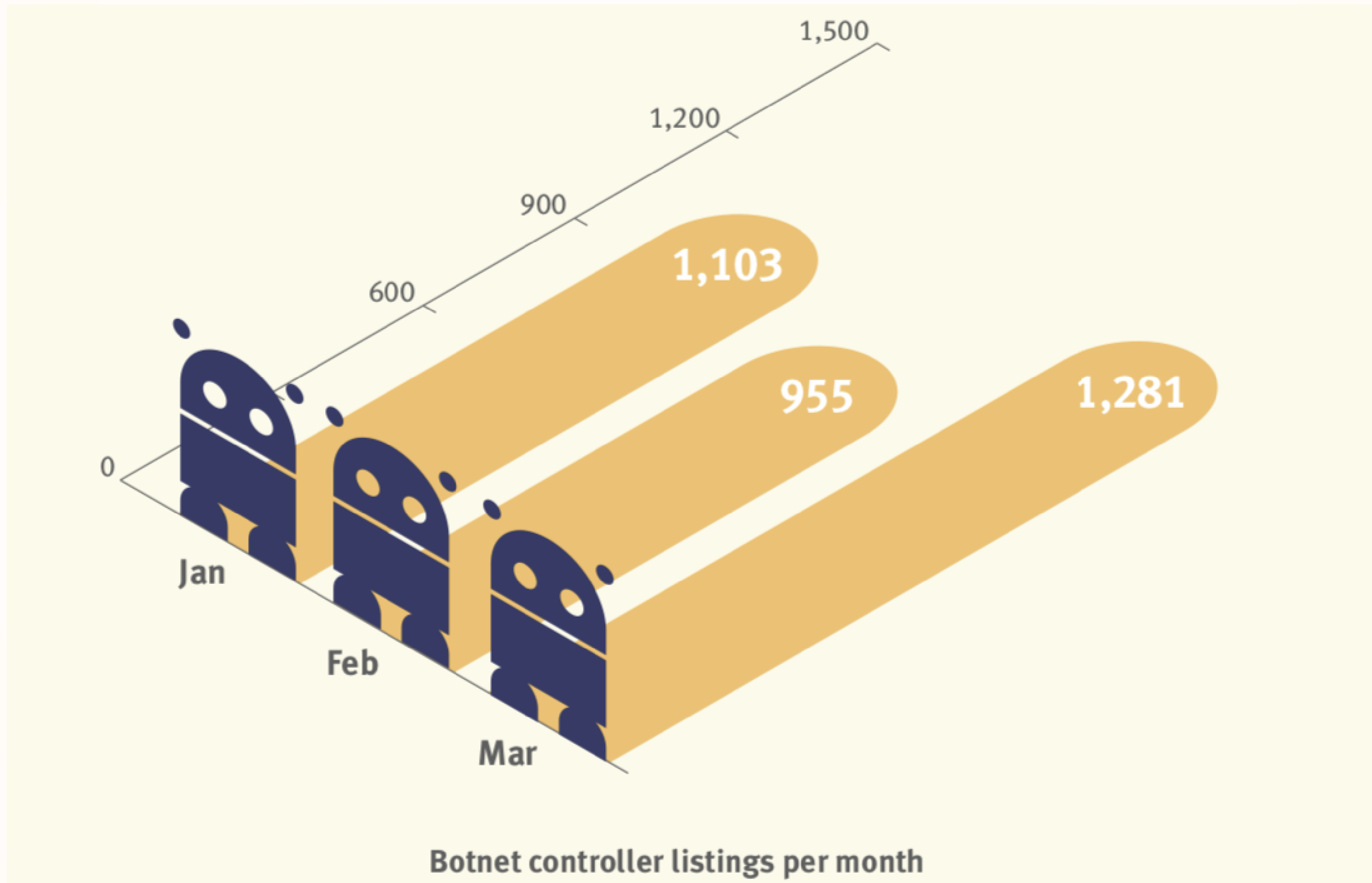
Botnet C&C hosting numbers, by ISP, as a result of fraudulent sign-ups

| Rank | C&Cs 2017 | C&Cs 2018 | % change | Country |
|------|-----------|-----------|----------|----------------------|
| 1 | 100 | 704 | +604 ▲ | United States |
| 2 | 14 | 603 | +4,207 ▲ | Switzerland |
| 3 | 273 | 431 | +58 ▲ | Russia |
| 4 | 70 | 238 | +240 ▲ | Russia |
| 5 | 186 | 163 | -12 ▼ | China |
| 6 | 87 | 138 | +59 ▲ | France |
| 7 | 36 | 113 | +214 ▲ | Russia |
| 8 | 1 | 92 | +9,100 ▲ | Ukraine |
| 9 | 88 | 86 | -2 ▼ | Netherlands |
| 10 | 37 | 81 | +119 ▲ | Russia |
| 11 | 80 | 80 | 0 | Belize |
| 12 | 160 | 78 | -51 ▼ | United Arab Emirates |
| =13 | 0 | 77 | — ▲ | Turkey |
| =13 | 96 | 77 | -20 ▼ | Russia |
| 14 | 128 | 75 | -41 ▼ | United States |
| 15 | 207 | 87 | -58 ▼ | United States |
| 16 | 0 | 69 | — ▲ | Russia |
| 17 | 66 | 67 | +1 ▲ | Russia |
| 18 | 4 | 66 | +1,550 ▲ | Russia |
| 19 | 85 | 62 | -27 ▼ | United States |
| 20 | 19 | 58 | +205 ▲ | United Kingdom |
| =21 | 27 | 57 | +111 ▲ | United Kingdom |
| =21 | 175 | 57 | -67 ▼ | China |

Quarter 1 2019 update

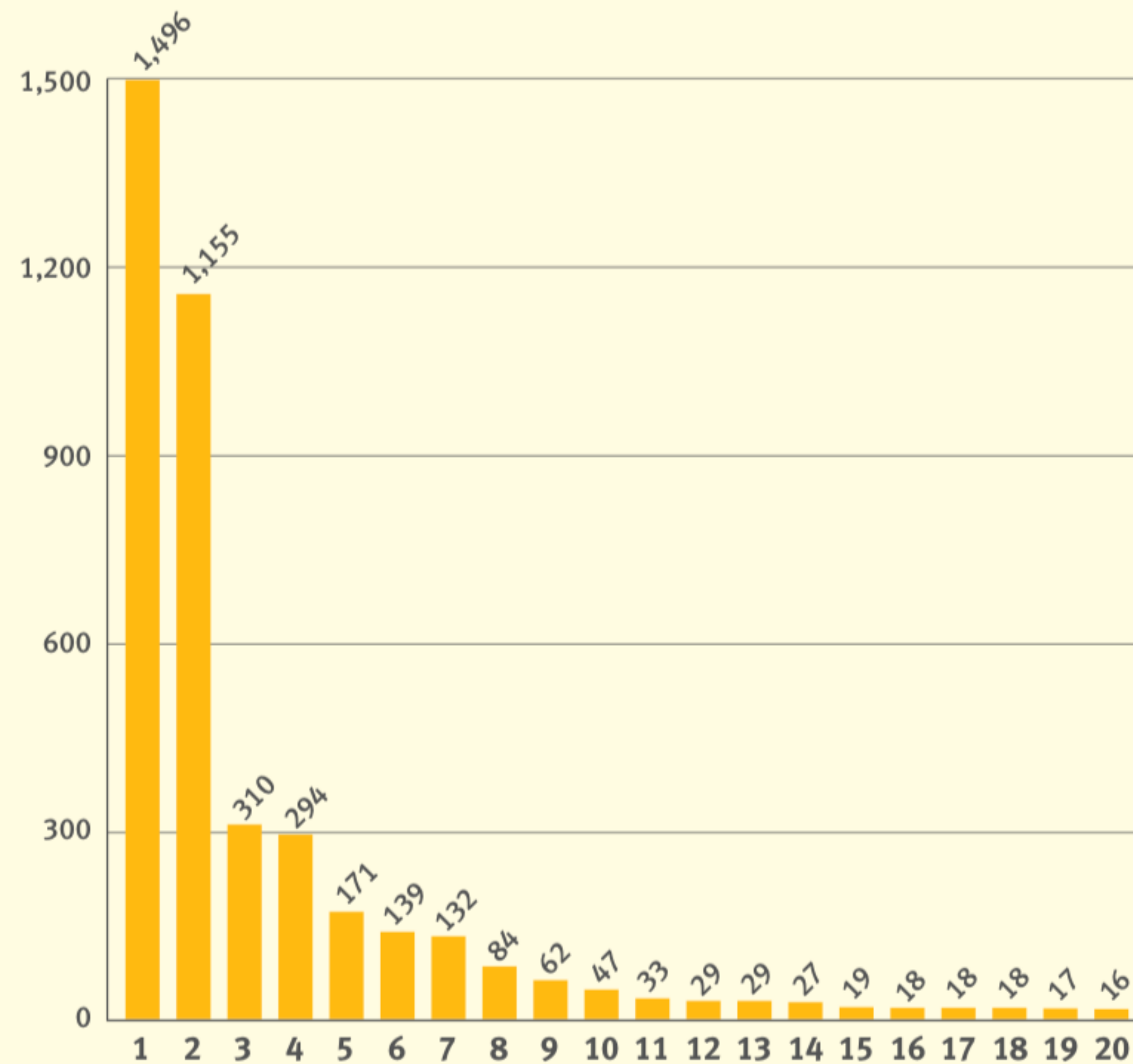
- Key Observations
 - A larger increase in botnet traffic
 - Increased “commodization” of Botnets with Crimeware kits.
 - Shift in TLD abuse
 - The top offender of hosted Botnet C&C retains the top spot

Botnet C&Cs 2019 Q1



Malware Families 2019 Q1

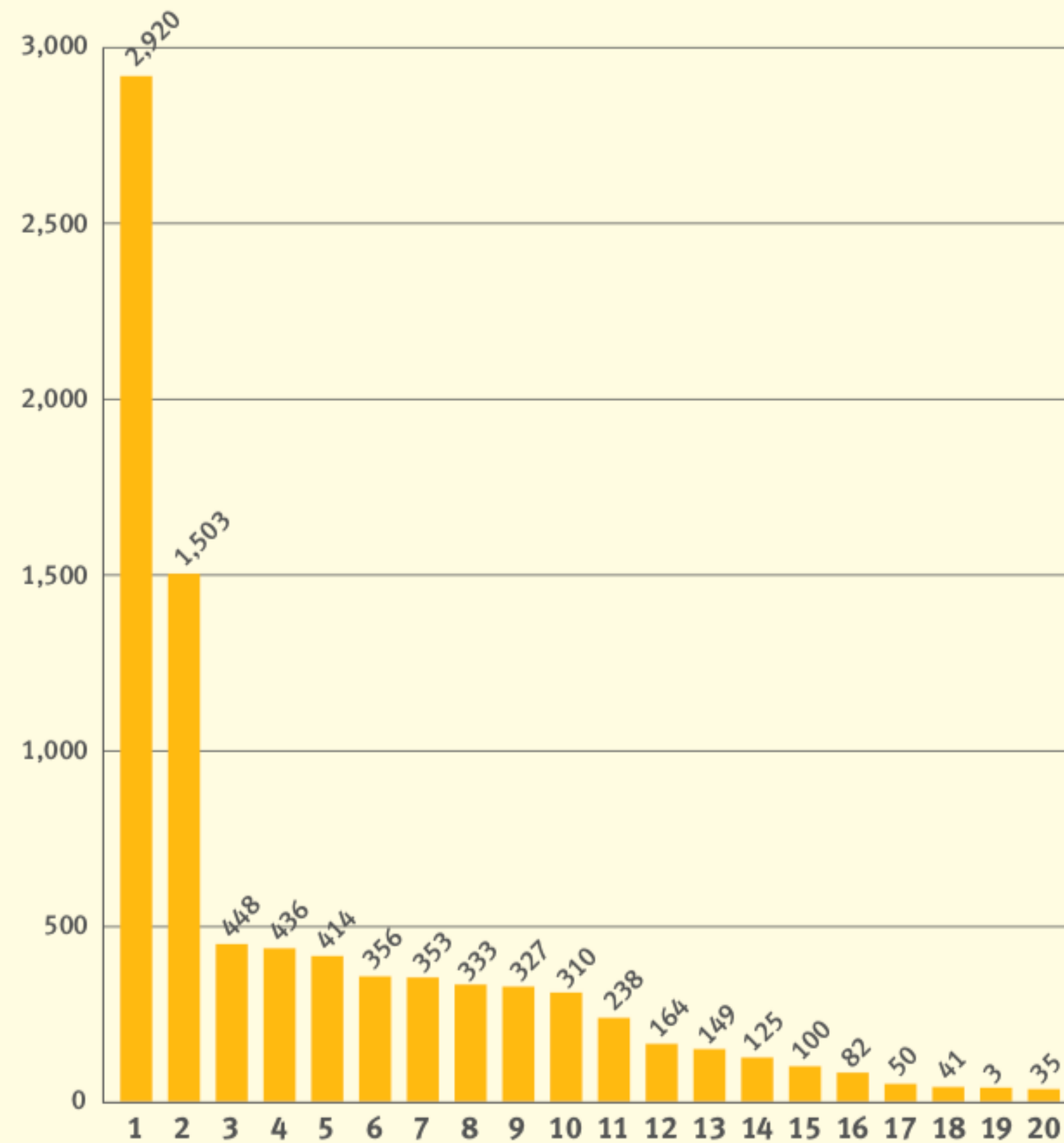
Malware families associated with botnet C&C listings Q1 2019



| Rank | Malware | Note |
|------|-----------------|----------------------------|
| 1 | Lokibot | Credential Stealer |
| 2 | AZORult | Credential Stealer |
| 3 | Pony | Dropper/Credential Stealer |
| 4 | NanoCore | Remote Access Tool (RAT) |
| 5 | RemcosRAT | Remote Access Tool (RAT) |
| 6 | JBifrost | Remote Access Tool (RAT) |
| 7 | Gozi | e-banking Trojan |
| 8 | ArkeiStealer | Credential Stealer |
| 9 | NetWire | Remote Access Tool (RAT) |
| 10 | Neurevt | e-banking Trojan |
| 11 | njrat | Remote Access Tool (RAT) |
| 12 | PredatorStealer | Credential Stealer |
| 13 | ImminentRAT | Remote Access Tool (RAT) |
| 14 | KPOTStealer | Credential Stealer |
| 15 | TinyNuke | Credential Stealer |
| 16 | RevCodeRAT | Remote Access Tool (RAT) |
| 17 | Gootkit | e-banking Trojan |
| 18 | IcedID | e-banking Trojan |
| 19 | OrcusRAT | Remote Access Tool (RAT) |
| 20 | Redosdru | Remote Access Tool (RAT) |

Abused TLDs 2019 Q1

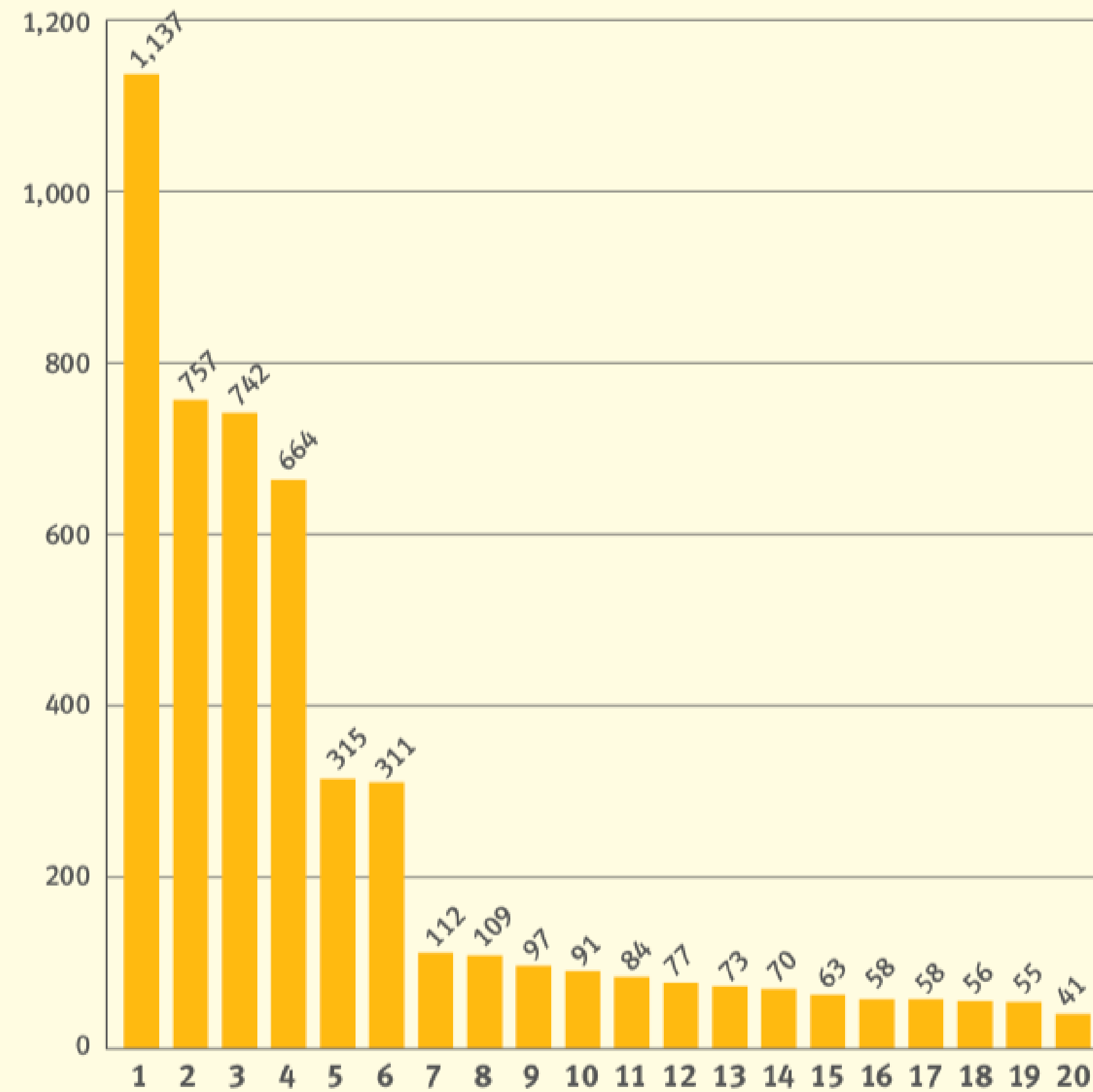
Top abused TLDs – number of domains



| Rank | TLD | Note |
|------|---------|--|
| 1 | com | gTLD |
| 2 | uk | ccTLD of United Kingdom |
| 3 | tk | originally ccTLD, now effectively gTLD |
| 4 | net | gTLD |
| 5 | ga | originally ccTLD, now effectively gTLD |
| 6 | cf | originally ccTLD, now effectively gTLD |
| 7 | pw | ccTLD of Palau |
| 8 | info | gTLD |
| 9 | ru | ccTLD |
| 10 | cm | ccTLD of Cameroon |
| 11 | ml | originally ccTLD, now effectively gTLD |
| 12 | gq | originally ccTLD, now effectively gTLD |
| 13 | xyz | gTLD |
| 14 | org | gTLD |
| 15 | ug | ccTLD of Uganda |
| 16 | icu | gTLD |
| 17 | top | gTLD |
| 18 | website | gTLD |
| 19 | host | gTLD |
| 20 | su | ccTLD of Soviet Union |

Abused Registrars

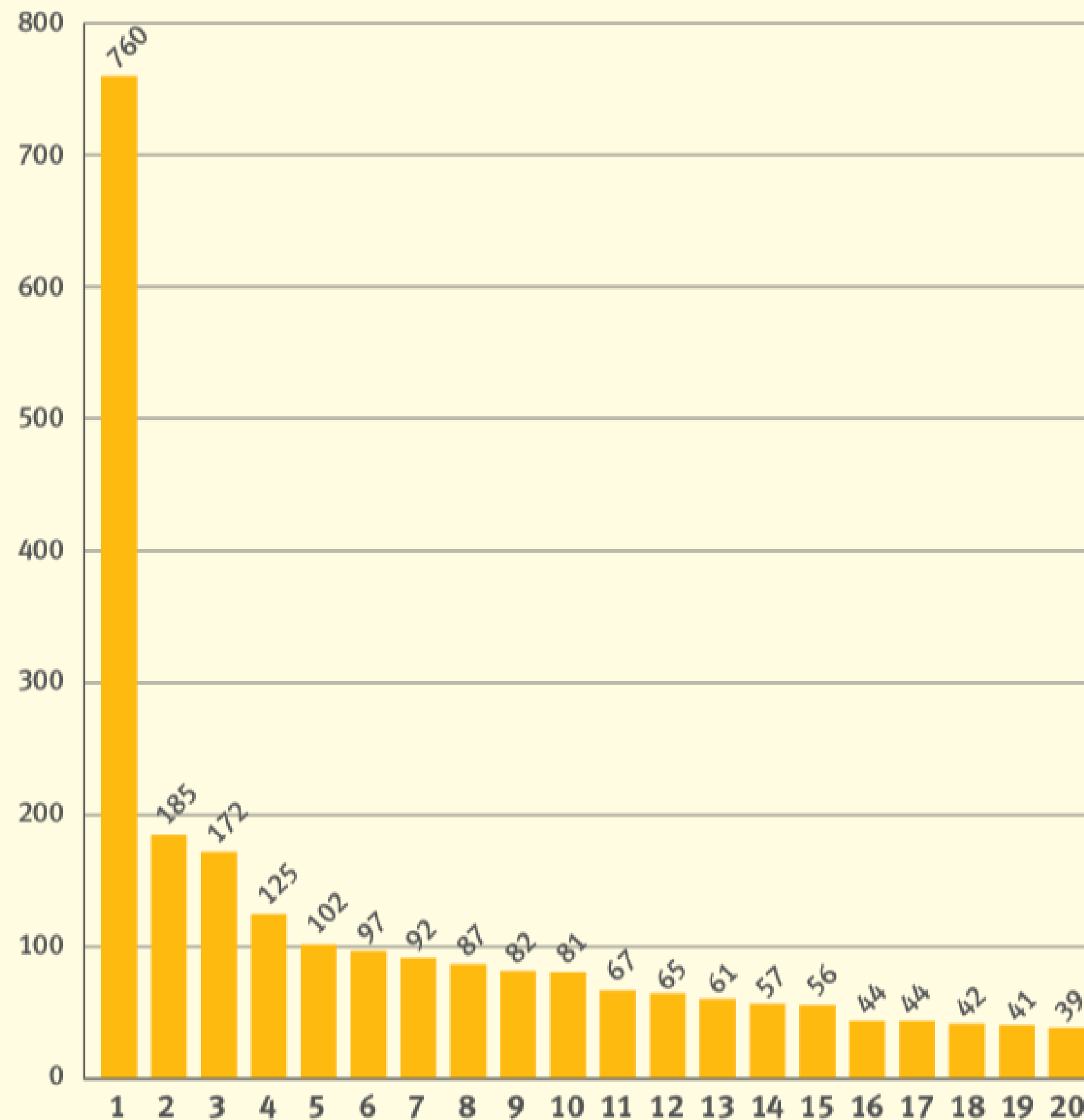
Most abused domain registrars – number of domains




| Rank | Registrar | Country |
|------|---------------------------------|---|
| 1 | Register.com | United States  |
| 2 | Namecheap | United States  |
| 3 | Network Solutions (aka web.com) | United States  |
| 4 | PDR | India  |
| 5 | RegRu | Russia  |
| 6 | NameSilo | United States  |
| 7 | GMO | Japan  |
| 8 | Arsys | Spain  |
| 9 | CentralNic | United Kingdom  |
| 10 | ENom | United States  |
| 11 | RU-Center | Russia  |
| 12 | Hostinger | Lithuania  |
| 13 | WebNic.cc | Singapore  |
| 14 | Eranet International | China  |
| 15 | Xin Net | China  |
| 16 | NameBright/DropCatch | United States  |
| 17 | Tucows | United States  |
| 18 | R01 | Russia  |
| 19 | Alibaba (aka HiChina/net.cn) | China  |
| 20 | OnlineNIC | United States  |

Hosted Botnet C&C

Total botnet C&C hosting numbers by ISP



| Rank | Network | Country |
|------|-----------------|---|
| 1 | cloudflare.com | United States  |
| 2 | stajazk.ru | Russia  |
| 3 | timeweb.ru | Russia  |
| 4 | reg.ru | Russia  |
| 5 | ovh.net | France  |
| 6 | mchost.ru | Russia  |
| 7 | melbicom.ru | Russia  |
| 8 | simplecloud.ru | Russia  |
| 9 | iliad.fr | France  |
| 10 | mtw.ru | Russia  |
| 11 | greenvps.net | Russia  |
| 12 | m247.ro | Romania  |
| 13 | alibaba-inc.com | China  |
| 14 | fos-vpn.org | Seychelles  |
| 15 | rivavpn.com | United States  |
| 16 | well-web.net | Russia  |
| 17 | skyvps.ru | Russia  |
| 18 | gerber-edv.net | Bulgaria  |
| 19 | select.ru | Russia  |
| 20 | dataclub.biz | Belize  |

Impact of GDPR and WHOIS

- Loss of indicators between good and bad
- Historical data
- Skewing the threat intelligence industry's data
- Inability to contact a domain owner in the event that a compromise has occurred

Mitigation recommendations

Preventing compromises

- Out of date software
- Secure account management and access
- Monitor drastic changes
- 2FA and SSH Keys

Vetting process

- Follow best practices
- Resellers
- Provide them with tools/training
- Hold them accountable

Mitigation recommendations

- Block access to cryptocurrency mining pools (opt-in for those that require access)
- Block traffic to anonymization services (opt-in for those that require access)
- Use BGP to block threats that would be utilizing dTLDs

Thanks for having us!