Qrator Labs announces the results of a research on national Internet segment stability in the countries around the world.

Moscow, June 14, 2016 — Qrator Labs, DDoS mitigation and network availability provider, has carried out a research on how the incidents in ISPs' networks may possibly affect global availability of entire national segments of the Internet.

The research covers the segments from 236 countries – basically, all the places where you can connect to the Internet from. As the result, it has become possible to rate the countries using a special parameter value which represents the degree of availability[1] of the national segments and failure rate of specific Internet service providers.

This parameter is calculated for each given country using the following method:

On the 1st stage the data from Maxmind is processed in order to put all network prefixes announced by the ISPs on the world map judging by their national segment's location.

On the 2nd stage Qrator Labs' researchers use their proprietary system which represents the model of global networking operation, Qrator.Radar , to find out for each ISP how much influence its failures have on the specific national segment. This is done by analyzing how many prefixes belonging to this national segment will lose their global availability over the Internet.

Next, the rating table is formed taking into account only the ISPs whose downtime can rob maximum percentage of the prefixes belonging to the given national segment of their global availability. These providers are listed below in the third column.

[1] Availability means the ability of the ISP to exchange data packets with other ISPs. One necessary clause of the availability is that the prefixes of the given ISP are listed in the routing tables of other ISPs. Without the corresponding records the traffic exchange is not possible..

Fig. 1. Top 10 countries by the stability of their national Internet segments[2]

Place	Country	ISP (AS number)	Max. % of prefixes losing availability in case the ISP goes down
1	Great Britain (GB)	Virgin Media (5089)	3.4
2	United States (US)	TATA (6453)	5.0
3	Russia(RU)	Rostelecom (20485)	5.5
4	Poland (PL)	Netia SA (12741)	5.7
5	Denmark (DE)	GHOSTNET (12586)	6.0
6	Canada (CA)	Rogers Cables (812)	6.0
7	France (FR)	Orange S.A. (5511)	6.5
8	Bangladesh (BD)	BRAC BDMAIL (24342)	7.2
9	Hong Kong (HK)	Wharf T&T (9381)	7.7
10	Ireland (IE)	Telia (1299)	8.2

[2] The national segment is deemed more stable if there are fewer ISP's prefixes losing availability in case of a single ISP's downtime.

Fig. 2. Post-Soviet states rating

Place	Country	ISP (AS number)	Max. % of prefixes losing availability in case the ISP goes down
1	Russia (RU)	Rostelecom (12389)	5.5
2	Ukraine (UA)	Trialan (13188)	14.1
3	Latvia (LV)	Telia LV (5518)	19.6
4	Estonia (EE)	Linxtelecom (3327)	22.1
5	Armenia (AM)	UCOM LLC (44395)	27.7
6	Lithuania (LT)	TEO LT (8764)	31.4
7	Kazakhstan (KZ)	Kazakhtelecom (9198)	46.9
8	Georgia (GE)	Caucasus Online (20771)	47.3
9	Tajikistan (TJ)	ELCat (8449)	56.2
10	Azerbaijan (AZ)	Delta Telecom (29049)	72.02
11	Belarus (BY)	Beltelecom (6697)	86.4
12	Uzbekistan (UZ)	UZBEKTELECOM (28910)	97.32

«Global availability of the national Internet segment is deeply influenced by state of the market in the country. The more mature and diversified the market is, particularly, the more middle-sized ISPs have access to the cross-border gateway, the higher the stability values are for the entire national segment", explains Alexander Lyamin, Qrator Labs CEO.

Since the company's founding, Qrator.Radar team has been continuously carrying out research projects on global network connectivity – that makes it nearly 7 years. Their service for monitoring global ISP operation, called Qrator.Radar, is widely used by various businesses around the globe. This development creates the basis for the globally distributed Qrator traffic filtering network which is employed by the company to provide DDoS attack mitigation services.

About Qrator Labs

The company, founded in 2009, provides solutions for countering DDoS attacks in conjunction with WAF (Web Application Firewall) solutions based on technology developed by a partner company, Wallarm. To make these solutions efficient, Qrator Labs uses the data gathered by Qrator.Radar, the global network operation monitoring service. The company‘s filtering network is geographically distributed, having points of presents in the US, in Russia, EU and Asia. Together with the set of their own proprietary algorithms for detection and mitigation of the attacks, this represents the company’s competitive advantage.

The team at Qrator Labs first started working on the research in the field of DDoS mitigation in 2006. Since then the company has been perfecting their exclusive proprietary filtering algorithms, currently using the machine learning techniques among others. This allows the service to react and adapt to new types of threats in full-auto mode.

Qrator Labs’ customers list includes companies from various spheres and markets all over the world. Among their Russian customers are the leading banks and credit businesses (Tinkoff Credit Systems, UniCredit, MDM, RocketBank, OTP, National Settlement Depository), payment systems (Qiwi, Cyberplat, Eleksnet), e-commerce (Lamoda, Ulmart, Eldorado, OZON, Wildberries, Citilink), mass media (IIA Russia Today, ITAR-TASS, Echo Moscow radio, Regnum), TV channels (Zvezda, TNT, TV Rain, NTV+) and many others.

Contacts for press:
press@qrator.net

Official channels in social networks:

https://www.facebook.com/QratorLabs/

https://twitter.com/Qrator_Labs