RAPID7

RUS
RANK 14
OF 187

NATIONAL EXPOSURE INDEX

RUSSIA | 2018

In 2016, Rapid7 Labs launched the National Exposure Index in order to get a measurable, quantitative answer to a fairly fundamental question: What is the nature of internet exposure—services that either do not offer modern cryptographic protection, or are otherwise unsuitable to offer on the increasingly hostile internet—and where, physically, are these exposed services located?

Now in our third year, we continue this ongoing investigation into the risk of passive eavesdropping and active attack on the internet, and offer insight into the continuing changes involving these exposed services. We've also added a third dimension for exposure, "amplification potential," where inappropriately exposed UDP services can be used in amplified, distributed denial of service (DDoS-A) attacks.

Overall Key Findings

- The United States ranks as the most exposed in the 2018 National Exposure Index, scoring the highest in nearly every exposure metric we measure. Following the U.S. is China, Canada, South Korea, and the United Kingdom, which together control over 61 million servers listening on at least one of the surveyed ports.

- There are 13 million exposed endpoints associated with direct database access, half of which are associated with MySQL. Along with millions of exposed PostgreSQL, Oracle DB, Microsoft SQL Server, Redis, DB2, and MongoDB endpoints, this exposure presents significant risk of crucial data loss in a coordinated attack.

- While the number of exposed Microsoft SMB Servers dropped considerably after the WannaCry attack of 2017, there remain about a half a million targets today, primarily in the U.S., Taiwan, Japan, Russia, and Germany.

- Amplification-based distributed denial of service (DDoS-A) remains a powerful technique for harming enterprises and providing cover for more sophisticated attacks. While the number of exposed UDP-based memcached servers is less than 4,000, there are about 40,000 unpatched, out-of-date memcached servers, which are at risk of being drafted into the next record-breaking DDoS attack.

These key findings tell us that the most risk to the internet originates in countries that have significant investment in, and reliance on, a safe and stable internet. This indicates to us that national internet service providers in these countries can use these findings to understand the risks of internet exposure, and that they, along with policymakers and other technical leaders, are in an excellent position to make significant progress in securing the global internet.

Key Statistics for Russia

Country (ISO3C)	Russia (RUS)
Rank	14
IPv4 Allocated Address Space	45,286,528
Responsive IPv4 Servers (Percentage)[1]	3,502,430 (7.73%)
Encrypted Web Ratio[2]	31.37%
Encrypted Shell Ratio[3]	72.18%
Exposed SMB Total (Percentage)[4]	107,641 (3.07%)
Exposed Database Total (Percentage)[5]	150,215 (4.29%)
Inappropriate UDP Total (Percentage)[6]	376,043 (10.74%)

Key Findings for Russia

In the 2018 survey for the National Exposure Index, Russia ranks as the **14th** most exposed country among the 187 countries Rapid7's study. This placement is owed largely to both Russia's unusually large inappropriate UDP service profile as well as its lower than average encrypted web site population.

Economic peers to Russia tend to enjoy an encrypted web service ratio of over 35%; anything less than this indicates that the region is lagging behind its neighbors in converting its web-based internet presence to the much safer HTTPS protocol. This is especially troublesome since we know that Russian people have a preference for Russia-hosted websites presented in the Cyrillic character set over their internationally-hosted equivalents written in Latin character sets.

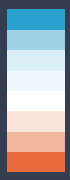
Of special concern, though, is Russia's unusually large population of Simple Service Discovery Protocol (SSDP) servers, a protocol that is both inappropriate to expose to the internet (given its association with internal, LAN-based network management) and is useful as an amplification vector in amplified distributed denial of service (DDoS-A) attacks. In many regions around the world, SSDP is simply unavailable outside of a regional ISP, but this is not the case in Russia. Russian technical leadership is urged to take care of this specific exposure quickly, since it is already being used in active DDoS-A attacks, as reported by Cloudflare and other DDoS mitigation services.

For Rapid7's complete National Exposure Index, which includes many additional findings related to both national and global exposure metrics, please visit www.rapid7.com/national-exposure.

Russia has an allocation of over 45 million IPv4 addresses, and about 3.5 million servers were responsive to scanning by Rapid7 researchers.

Exposure Index Key

Least Exposed



Most Exposed

[1] The sum of all IPv4 nodes which respond affirmatively to a TCP SYN or a UDP request, over that country's allocated IPv4 space.

[2] The fraction of common HTTPS ports (443 and 8443) over all HTTP and HTTPS ports (443, 8443, 80, 81, 8000, 8080, and 8888)

[3] The fraction of responsive SSH probes on port 22 over the sum of all the SSH and telnet (port 23) responders in that country

[4] The fraction of responsive SMB probes over the total IPv4 utilization figure for that country

[5] The fraction of responsive probes on ports 1433, 1521, 3306, 5432, 6379, 27017, and 50000 over the total IPv4 utilization figure

[6] The fraction of responsive probes on UDP ports 19, 137, 389, 1900, 5353, 5060, and 11211 over the total IPv4 utilization figure