GBR
RANK 5
OF 187

NATIONAL EXPOSURE INDEX

THE UNITED KINGDOM | 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 While the number of exposed UDP-based memcached servers is less than 4,000, there are about 40,000 unpatched, out-of-date memcached servers, which are at risk of being drafted into the next record-breaking DDoS attack.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 the United Kingdom

Country (ISO3C)	The United Kingdom (GBR)
Rank	5
IPv4 Allocated Address Space	125,988,760
Responsive IPv4 Servers (Percentage)[1]	3,052,186 (2.42%)
Encrypted Web Ratio[2]	41.23%
Encrypted Shell Ratio[3]	78.69%
Exposed SMB Total (Percentage)[4]	125,513 (4.11%)
Exposed Database Total (Percentage)[5]	251,362 (8.24%)
Inappropriate UDP Total (Percentage)[6]	94,653 (3.10%)

Key Findings for the United Kingdom

The United Kingdom finds itself in the 5th place among the 187 countries surveyed for internet exposure in the first quarter of 2018. This placement is due to a number of inputs in our National Exposure Index ranking algorithm, the most significant of which is the UK's relatively large exposure of SMB (port 445/TCP) and database-related ports (those ports most commonly associated with PostgreSQL, Oracle DB, Microsoft SQL Server, Redis, IBM DB2, and MongoDB). We also found over 94,000 exposed UDP services (excluding DNS and NTP). In total, **there are over 470,000 dangerously exposed services located in the UK**. This presents significant risk of mass compromise in the ongoing EternalBlue family of worms, any future Windows SMB attack or database attack, and the risk of using British infrastructure in UDP amplification DDoS attacks around the world.

On a positive note, the ratio of encrypted web servers in the UK appears to be quite healthy—countries with more than 35% of encrypted web servers to cleartext web servers tend to be regions where HTTPS is well on its way to becoming the standard web-browsing protocol. In addition, the UK has a relatively high encrypted shell ratio, with over half a million SSH servers compared to its population of 137,311 legacy telnet servers. However, of those SSH servers, there are about ten thousand outdated v1.99 servers, and over seven thousand servers identify with a duplicated SSH host key. So, while the large population is good to see, a small percentage of them could use some administrative attention.

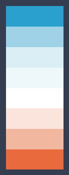
For Rapid7's complete National Exposure Index, which includes many additional findings related to both national and global exposure metrics, please visit www.rapid7.com/national-exposure.

GBR
RANK 5
OF 187

The United Kingdom has an allocation of over 125 million IPv4 addresses, and about 3 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