RAPID7

CHN
RANK 2
OF 187

NATIONAL EXPOSURE INDEX

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 While the number of exposed UDP-based memcached servers is less than 4,000, there are about 40,000 unpatched, out-of-date memcached servers, which are at risk of being drafted into the next record-breaking DDoS attack.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

Country (ISO3C)	China (CHN)
Rank	2
IPv4 Allocated Address Space	340,344,064
Responsive IPv4 Servers (Percentage)[1]	13,689,772 (4.02%)
Encrypted Web Ratio[2]	26.27%
Encrypted Shell Ratio[3]	58.11%
Exposed SMB Total (Percentage)[4]	30,425 (0.22%)
Exposed Database Total (Percentage)[5]	1,837,630 (13.42%)
Inappropriate UDP Total (Percentage)[6]	649,536 (4.74%)

Key Findings for China

China is **2nd** among the most exposed countries among the 187 nations surveyed in 2018, coming in after the United States, a troubling statistic given that it has less than 1/3rd of the total responsive servers as found in the US. One major contributor to this ranking is China's notable lack of encrypted services, which enables passive, pervasive monitoring and active attacks on insecure, cleartext protocols. China's web server population severely lags behind the rest of the world in this regard—an encrypted web ratio of 26% is well below the 35% we'd like to see in HTTPS adoption. This is especially troublesome since we know that Chinese people tend to favor China-hosted websites over equivalent internationally-hosted services. Similarly, China's 58% encrypted shell ratio is much lower than the average of 75% or so by its economic peers, causing the region to be more exposed to another Mirai-like botnet that can take advantage of some fraction of China's **1.3 million responsive telnet service ports**.

Finally, China's database exposure is rather alarming, both in absolute terms and as a percentage of its IPv4 space utilization, with its **1.8 million responsive database service ports**. It is never a good idea to directly expose database servers to the internet; rarely are the passwords chosen for such servers sufficiently complex, and database servers do not come with built-in rate-limiting measures to prevent online bruteforcing of those passwords.

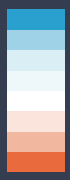
For Rapid7's complete National Exposure Index, which includes many additional findings related to both national and global exposure metrics, please visit www.rapid7.com/national-exposure.

CHN
RANK 2
OF 187

China has an allocation of over 340 million IPv4 addresses, and about 14 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