

NATIONAL EXPOSURE INDEX

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 While the number of exposed UDP-based memcached servers is less than 4,000, there are about 40,000 unpatched, out-of-date memcached servers, which are at risk of being drafted into the next record-breaking DDoS attack.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

Country (ISO3C)	Japan (JPN)
Rank	8
IPv4 Allocated Address Space	203,815,936
Responsive IPv4 Servers (Percentage) ¹	5,903,301 (2.90%)
Encrypted Web Ratio ²	37.44%
Encrypted Shell Ratio ³	74.60%
Exposed SMB Total (Percentage) ⁴	90,017 (1.66%)
Exposed Database Total (Percentage) ⁵	306,655 (5.19%)
Inappropriate UDP Total (Percentage) ⁶	1,971,036 (33.39%)

Key Findings for Japan

In this year's National Exposure Index survey, Japan ranks as the **8th** most exposed country in Rapid7's scans. While Japan has a fairly good encrypted web ratio of 37% (anything over 35% is a healthy ratio today), it also has an extremely unhealthy exposure of nearly **two million** inappropriately exposed UDP services, the most egregious of which is its population of 1.87 million SIP endpoints listening on port 5060/UDP. Among the top 10 most exposed countries, only Germany has more, at 6 million SIP servers.

SIP presents a unique exposure for Japan—it is a notoriously difficult protocol to adequately secure against both active and passive eavesdropping for contact lists, traffic analysis, and often some forms of toll fraud and voice communications eavesdropping. Encrypted SIP (SIP-TLS on port 5061/TCP) is really the only way to defend against this, but legacy, cleartext SIP is still immensely popular in Japan. In addition, Japan appears to have a database exposure problem; about 5% of all the servers in Japan are responsive on ports commonly associated with database servers, a little over half of which are MySQL's port, 3306/TCP. These servers should never be exposed to the internet; database access passwords are rarely sufficiently complex, and database servers do not ship with built-in rate-limiting to prevent online credential bruteforcing.

On the bright side, Japan's SSH game is pretty strong—at a 74% encrypted shell ratio, it's doing better than most when it comes to stamping out legacy telnet servers for remote administration.

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.

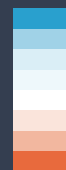


Japan has an allocation of over 203 million IPv4 addresses, and about 5.9 million servers were responsive to scanning by Rapid7 researchers.



Exposure Index Key

Least Exposed



Most Exposed

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

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

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

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

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

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