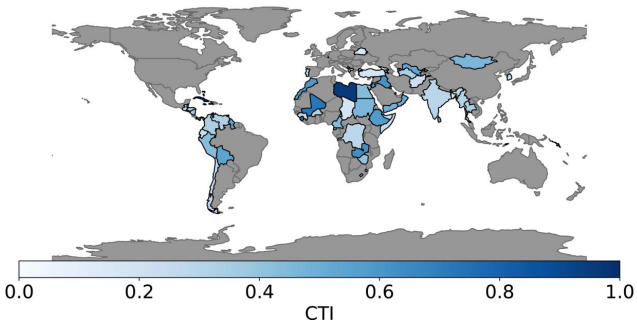
Paper reveals a quarter of the world's internet users rely on infrastructure that is susceptible to attacks

26 May 2022



Fraction of each country's IP addresses that are exposed to observation or selective tampering by companies that connect Internet service providers to the global Internet. Countries are shaded in progressive shades of blue, with wost exposed countries in the darkest blue. Countries in gray excluded from the study. Credit: University of California San Diego

About a quarter of the world's internet users live in countries that are more susceptible than previously thought to targeted attacks on their internet infrastructure. Many of the at-risk countries are located in the Global South.

That's the conclusion of a sweeping, large-scale study conducted by computer scientists at the University of California San Diego. The researchers surveyed 75 countries.

"We wanted to study the topology of the internet to find weak links that, if compromised, would expose an entire nation's traffic," said Alexander Gamero-Garrido, the paper's first author, who earned his Ph.D. in computer science at UC San Diego.

Researchers presented their findings at the Passive and Active Measurement Conference 2022 online this spring.

The structure of the internet can differ dramatically in different parts of the world. In many developed countries, like the United States, a large number of internet providers compete to provide services for a large number of users. These networks are directly connected to one another and exchange content, a process known as direct peering. All the providers can also plug directly into the world's internet infrastructure.

"But a large portion of the internet doesn't function with peering agreements for network connectivity," Gamero-Garrido pointed out.

In other nations, many of them still developing countries, most users rely on a handful of providers for internet access, and one of these providers serves an overwhelming majority of users. Not only that, but those providers rely on a limited number of companies called transit autonomous systems to get access to the global internet and traffic from other countries. Researchers found that often these transit autonomous system providers are state owned.

This, of course, makes countries with this type of internet infrastructure particularly vulnerable to attacks because all that is needed is to cripple a small number of transit autonomous systems. These countries, of course, are also vulnerable if a main internet provider experiences outages.

In the worst case scenario, one transit autonomous system serves all users. Cuba and Sierra Leone are close to this state of affairs. By contrast, Bangladesh went from only two to over 30 system providers, after the government opened that sector of the economy to private enterprise.

This underlines the importance of government regulation when it comes to the number of internet

providers and transit autonomous systems available in a country. For example, researchers were surprised to find that many operators of submarine internet cables are state-owned rather than privately operated.

Researchers also found traces of colonialism in the topology of the internet in the Global South. For example, French company Orange has a strong presence in some African countries.

Researchers relied on Border Gateway Protocol data, which tracks exchanges of routing and reachability information among autonomous systems on the internet. They are aware that the data can be incomplete, introducing potential inaccuracies, though these are mitigated by the study's methodology and validation with real, in-country internet operators.

Next steps include looking at how critical facilities, such as hospitals, are connected to the internet and how vulnerable they are.

More information:
www.caida.org/catalog/papers/2 … exposure_traffic.pdf

Provided by University of California - San Diego