Expanding Access, Exposing Risk: A Study of Starlink Hosts

Omar Elamri
UCLA
Los Angeles, USA
omar@cs.ucla.edu

Isaac-Neil Zanoria
UCLA
Los Angeles, USA
zanoria@ucla.edu

Jacob Zhi
UCLA
Los Angeles, USA
zhi@cs.ucla.edu

Ben Du
UCLA
Los Angeles, USA
c4du@ucla.edu

Liz Izhikevich
UCLA
Los Angeles, USA
lizhikev@ucla.edu

1 Introduction

Low Earth Orbit (LEO) satellite networks are reshaping global Internet access by connecting regions that have long lacked reliable terrestrial infrastructure. Among them, Starlink has seen explosive growth—reporting over 7 million users in 2025 [3], up from just 2 million in 2023 [2]—primarily targeting rural and underserved areas. This rapid expansion brings millions of new hosts online, many of which may differ in security posture from those behind traditional broadband networks

In this paper, we present a measurement-driven analysis of the security characteristics of Starlink-connected hosts and uncover several concerning trends. We find that Starlink hosts are more likely to run outdated or vulnerable operating systems and network protocols than non-Starlink hosts. These disparities are not uniform globally—regions like Latin America, Southeast Asia, and Eastern Europe show disproportionately higher risk.

Our findings raise important questions for the Internet measurement and policy communities: How can we reduce the security risks associated with newly connected populations? What role should ISPs, manufacturers, and governments play in promoting safer defaults and practices? We hope this work can serve as a basis for discussion on how to design technical and policy interventions that ensure connectivity growth also strengthens the global Internet's resilience.

2 Dataset & Methodology

We collect IPv4 and IPv6 services exposed behind Censys [1] on April 7th, 2025. These scans provide general information about responsive hosts (such as their IP address, autonomous system, and geolocation) as well as the OS and service-related information obtained through protocol banners.

We identify services hosted within AS 14593 (Starlink's autonomous system) as Starlink hosts, and all others as non-Starlink hosts. This yields approximately 33,000 Starlink hosts. To ensure a balanced comparison, we reduce our original set of 230 million non-Starlink hosts by randomly sampling up to 10,000 hosts per country, resulting in a dataset of 1.78 million non-Starlink hosts—slightly exceeding the maximum number of Starlink hosts observed in any single country.

We obtain information about recent CVE's–those between 2020 and 2025–through the NIST's National Vulnerability Databse program. The majority of the CVE descriptions in this database include a range of affected operating system and software versions. We join this dataset with both Censys datasets on a description of the host system using a wildcard match on its Common Platform Enumeration (CPE) string to obtain a join table of CVE-host pairs.

3 Results

A significant fraction of exposed Starlink hosts are routers, with the type and frequency of their operating systems varying significantly across continents. South America sees 70% of exposed hosts running Fortinet FortiOS, while Europe sees less than 20% of the same operating system. Figure 1 shows that these geographic variations are especially apparent when compared to the (relatively even) distribution of non-Starlink hosts. For example, FortiOS takes up 15.72% market share in South America for non-Starlink hosts.

Starlink hosts show significantly higher rates of operating system vulnerabilities compared to non-Starlink hosts, with notable geographic disparities. As shown in Figure 2, countries with the highest OS CVE rates for Starlink hosts do not necessarily align with those for non-Starlink hosts. Notably, Haiti experiences a nine-fold increase in per-capita OS vulnerabilities on Starlink-connected hosts, while Colombia sees a six-fold increase.

Starlink hosts are more likely to run outdated and insecure network protocols than non-Starlink hosts, with this pattern varying significantly across countries. To quantify this difference, we compute a Starlink insecurity ratio for each country—defined as the fraction of Starlink hosts using outdated protocols (including old TLS versions, weak SSH cipher suites, and legacy SMBv1) divided by the corresponding fraction among all hosts.

Starlink overrepresents insecure protocol usage in regions such as Central and South America, Eastern Europe, and Southeast Asia. Figure 3 shows the global distribution of this

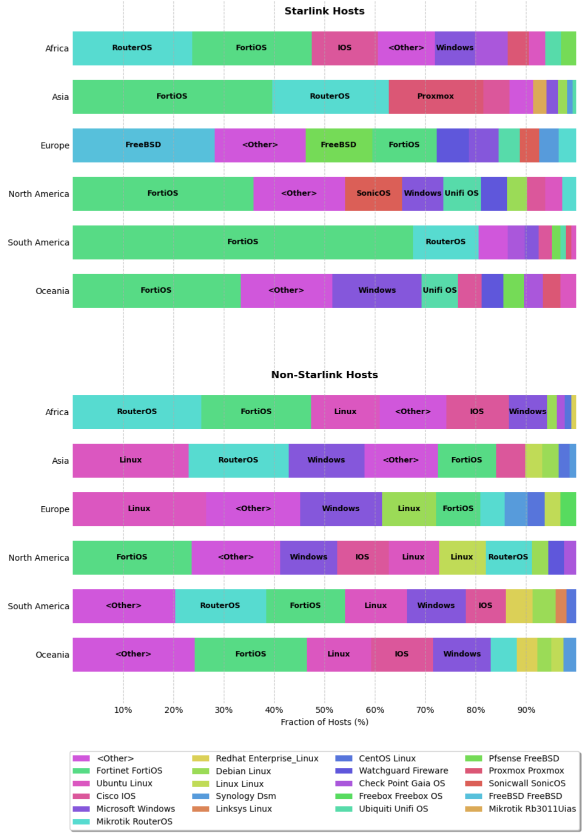

Figure 1: Starlink hosts observed in the Censys dataset are primarily routers compared to non-Starlink hosts.

ratio. Countries shaded green have a ratio below 1, indicating Starlink hosts are comparatively more secure, while those in red have a ratio above 1, reflecting higher insecurity among Starlink hosts.

4 Discussion

Our sampled results point to a critical and timely policy challenge: how to ensure that the rapid expansion of connectivity—particularly through satellite ISPs like Starlink—does not come at the expense of global Internet security. The disparities we observe in OS types, vulnerability rates, and outdated protocol use across regions suggest that the attack surface is not only growing, but also unevenly distributed. This asymmetry may correlate with regional differences in technical capacity, regulation, and user awareness—factors that policy and community efforts could potentially address.

As outdated or vulnerable devices become easy targets for botnets and exploitation, the Internet community could coordinate efforts to promote security awareness and stronger defaults in newly connected regions to ensure that expanded access does not come at the cost of resilience.

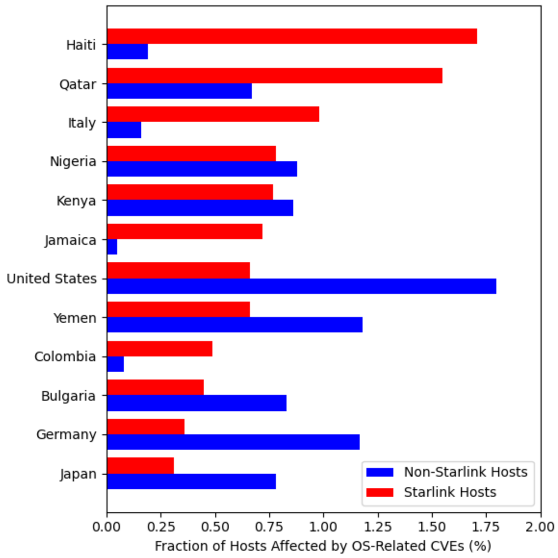

Figure 2: 12 most common countries with Starlink-connected hosts affected by an operating system CVE versus non-Starlink hosts. Data is normalized by the total number of hosts.

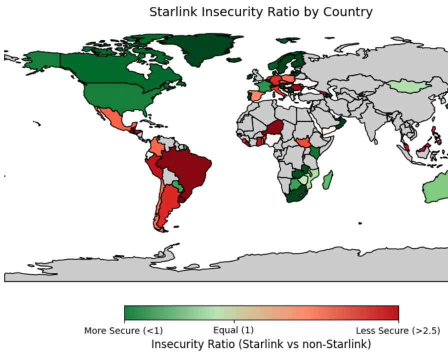
Starlink Insecurity Ratio by Country
More Secure (<1)
Equal (1)
Less Secure (>2.5)
Insecurity Ratio (Starlink vs non-Starlink)

Figure 3: Starlink hosts in South America, west Africa, and eastern Europe contribute to disportionately to overall hosts that runs outdated network protocols.

References

[1] Zakir Durumeric, Hudson Clark, Jeff Cody, Elliot Cubit, Matt Ellison, Liz Izhikevich, and Ariana Mirian. 2025. Censys: A Map of Internet Hosts and Services. In *Proceedings of the ACM SIGCOMM 2025 Conference*. 147–163.

[2] Starlink. 2023. https://x.com/Starlink/status/1705695980325323023

[3] Starlink. 2025. https://x.com/Starlink/status/1960867340951937239