A Security Posture Analysis of Starlink Customers Through Internet Scanning

Omar Elamri
omar@cs.ucla.edu
UCLA

Isaac-Neil Zanoria
zanoria@ucla.edu
UCLA

Jacob Zhi
zhi@cs.ucla.edu
UCLA

A Security Posture Analysis of Starlink Customers Through Internet Scanning

Omar Elamri
omar@cs.ucla.edu
UCLA

Isaac-Neil Zanoria
zanoria@ucla.edu
UCLA

Jacob Zhi
zhi@cs.ucla.edu
UCLA

Abstract

Starlink (ASN 14593) is one of the latest new ways to connect to the internet. They have a unique market advantage: Low Earth Orbit (LEO) and SpaceX deployment, which has led to recent mass adoption. However, Starlink is opening up the internet to a completely new type of host, potentially with different technological needs and attributes. To analyze their security posture, we utilize data from Censys to discover differences between Starlink hosts and regular hosts. We analyze security differences from three perspectives: operating system security, protocol-level security, and operational security. We find that across many geographies, Starlink hosts exposed to the internet have a different security profile than the internet at large. For example, across all three perspectives, we see a disproportionate pattern in insecure Starlink hosts in South American countries, where a single operating system type makes up 70% of hosts–a significantly different landscape than the internet at large. From our findings based on the three perspectives, we offer recommendations for both LEO network operators and machine administrators.

1 Introduction

According to Pew Research, 3 out of 10 rural Americans do not have a broadband internet connection at home [20]. Of the rural Americans who do have broadband, preliminary results show that their security practices are less than fortunate and pose a legitimate risk to their digital wellbeing [15].

In short, rural areas are a huge, untapped market for internet service providers; however, this new market comes with its own security concerns.

Starlink is a Low Earth Orbit (LEO) satellite operator that provides internet access to customers. Customers buy a Starlink dish which communicates with one of their satellites. These satellites relay this communication to one of Starlink's Points-of-Presence (PoP) where Starlink is connected to the terrestrial internet.

LEO technology is situated to be more convenient for rural users; compared to Geosynchronous satellites (GEO), LEO satellites are much closer, significantly reducing latency [18].

Starlink is able to connect rural communities to the internet with relative ease; however, with this relative easy comes a completely new type of internet host. How different are these new hosts? Where are these new hosts? How is their security posture? We use Censys data to describe these differences from three lenses. The first lens is from an Operating System security standpoint. What operating systems do Starlink hosts run? Are they less secure? The second lens is from a protocol perspective—do they use outdated versions/deprecated options? The third and final lens is from an operational security standpoint. What ports are open—how does this distribution differ from a geographic standpoint? From these differences, how can we roll out Starlink in a safer manner that improves overall internet security?

We find that Starlink hosts may tend to run completely different operating systems, use insecure protocols, and have different distributions of open ports. Each may vary geographically (for example, insecure hosts have a concentration in South America, Southeast Asia, and Eastern Europe). We advise that machine administrators should take extra care in ensuring that their hosts are up-to-date and LEO network operators should perform some sort of ingress filtering.

2 Related Works

Internet-based scanning is hardly new; work exists that scan the internet for Heartbleed vulnerabilities [7], responsive FTP hosts [17], the Mirai botnet [2], and various IoT devices [13]. Scanning may also yield different results based on where the origin is [21].

Other works exist that use Censys data to characterize internet hosts, namely in the LEO landscape (in which this study found some publicly-exposed Industrial Control Systems) [19], and another that provides a generalized methodology for LEO specifically [11]. Certain works focus on Starlink specifically, such as SeeStar, which characterizes different devices on a Starlink network (e.g. Points-of-Presence) [22].

While other works have analyzed Starlink and other LEO networks, this work contributes a novel characterization of specific security tendencies of Starlink-connected hosts, and compares these tendencies to a broader internet baseline–both against the global population and stratified on a host's geographic region. We focus on hosts of all types connected to the Starlink network (as long as the machine has exposed ports) and not just internal Starlink infrastructure or industrial control systems. We view host security from a unique lens, analyzing operating system security, protocol security, operational security, and the interaction between each.

3 Methodology

To analyze and explain the security of Starlink Customers, we leverage quantitative data obtained through internet scanning over the IPv4 address and port space. We utilize data obtained through Censys scanning [6] starting on April 7th, 2025. These scans provide general information about responsive hosts (such as their IP address, autonomous system, and location) as well as any system and service-related information obtained through protocol banners or other hints obtained during interaction with opened ports. For example, interacting with an exposed HTTPS service will often give information about the operating system family and version, HTTP server software, and TLS version.

However, one limitation of this approach is that only hosts that have at least one responsive port running a service are included in the data set. For the Starlink internet service provider, this generally correspond to select Starlink Business plan customers [4]. This limitation is discussed in more detail in Section 5.

We separate the data obtained from Censys into hosts belonging to the Starlink Autonomous System (AS), AS 14593, and hosts that belong to any other AS. We then load the Censys data into Google BigQuery [9], a cloud-based data warehouse. There are approximately 33,000 rows (representing 33k hosts) in our Starlink dataset dataset and approximately 1.78 million rows in our non-Starlink host dataset. To prevent combinatorial explosion when performing complex joins with other datasets, we had trimmed our original dataset of non-Starlink hosts consisting of approximately 230 million rows to 1.78 million rows by randomly sampling 10,000 hosts per country, slightly larger than the maximum amount of hosts in a country in the Starlink host dataset.

To analyze operating system and operational security, we must determine active vulnerabilities on the system. For ethical and scope constraints, we do so in a manner that does not involve interacting with any host systems. First, we obtain information about recent CVE's–those between 2020 and 2025–through the National Institute of Standards and Technology's National Vulnerability Databse program [16]. 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 [5] to obtain a join table of CVE-host pairs.

To draw conclusions about security posture across geographies and between Starlink and non-Starlink hosts, we analyze quantitative trends and perform statistical testing. Internet scanning data is joined to other datasets (such as geographic datasets representing populations) and analyzed using BigQuery SQL. Data is visualized using the Python matplotlib library as well as ArcGIS (for geographic data). To compare the population of Starlink and non-Starlink hosts and check for significance of certain variables, we employ tests of statistical significance such as the one-tailed Z test.

4 Results

We present our results from three different lenses, firstly from an operating system standpoint. We analyze the distribution of operating systems that Starlink hosts run, how are these OSes are distributed geographically, and whether certain hosts are susceptible to certain OS-related CVEs. Overall, we observe significant geographic variation in types of operating systems connected to Starlink, especially when compared to the internet-connected IPv4 space at large. We also find that in certain geographies, vulnerable operating systems are over-represented at a statistically significant level.

Secondly, we analyze our population of Starlink hosts from a protocol standpoint. Over exposed ports, we analyze which protocols do Starlink hosts run, what proportion of those hosted protocols are insecure, and whether there are over-represented protocols in Starlink hosts. Generally, through a blended metric combining TLS, SSH, and SMB security, we observe several countries with a significant increase in insecure hosted protocols over the baseline of all hosts, especially in regions such as South America, Europe, and Asia.

Finally, we analyze Starlink hosts from an operational persepctive. We focus on the which ports are open on each Starlink host, and how how different these ports are from non-Starlink hosts? Generally, we see numerous hosts running protcols on non-standard (i.e., non-IANA assigned) ports, with strong geographic variation in certain regions when compared to the baseline.

4.1 Operating System Security

Our first perspective to analyze security posture is the security of the host operating systems themselves. By analyzing operating system security, we gain a better understanding of the vulnerabilities agnostic to any protocol or service. Security issues with an operating system may be remarkably dangerous, as many OS-based security issues can be exploited over the internet, such as buffer overflows or improper input validation [3].

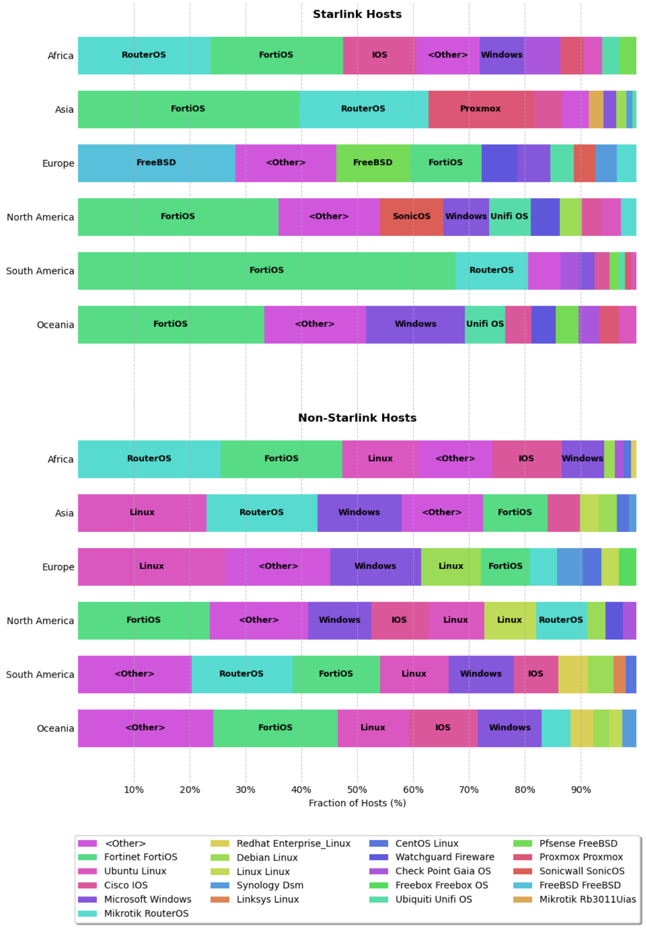

Figure 1: **Starlink Host OSes are Distributed Unevenly**–Proportion of Starlink hosts and non-Starlink hosts visible to Censys grouped by the operating systems they are running.

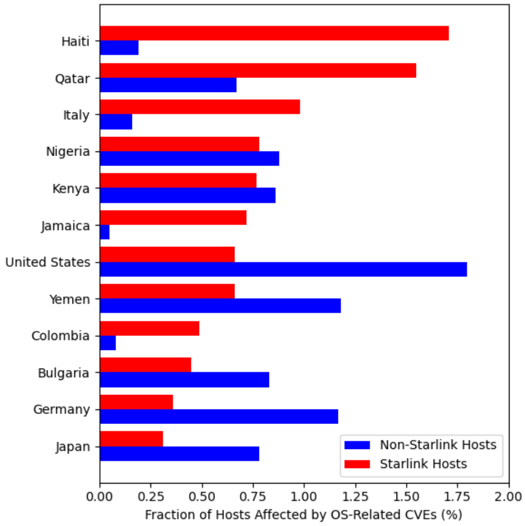

Figure 2: **Disparity in Distribution of Insecure Operating Systems**–12 most common countries with Starlink-connected hosts affected by an operating system CVE versus non-Starlink hosts. Data is normalized by the total number of hosts.

We observe significant **geographic variation** in the vendor and type of operating system connected to the Starlink internet service. As Figure 1 shows, while a significant fraction of operating systems seen on Starlink are router operating systems, the type and frequency of these operating systems shift dramatically between continents. South America sees 70% of exposed hosts running Fortinet FortiOS, while Europe sees less than 20% of the same operating system. We see a small proportion of standard server operating systems as well, such as FreeBSD, Windows Server, and Linux, which themselves exhibit significant differences in popularity. While Windows Server has a 17.7% share in Oceania, it accounts for only 2.34% of hosts in Asia. Just as different operating systems exhibit different security profiles, different regions of the world see different patterns in the popularity of different operating systems. Thus, vulnerabilities may affect various regions disproportionately, and remediation and prevention of attacks requires different attention and focus throughout different geographies. These geographic variations are especially apparent when compared to the (relatively even) distribution of non-Starlink hosts. For example, for non-Starlink hosts, FortiOS takes up a modest 15.72% market share in South America. Across all continents, no operating system takes up more than 30% market share for non-Starlink hosts, while varied market dominance is more evident in Starlink hosts.

When looking at operating system vulnerabilities themselves, we also see significant disparity in the **rate of vulnerability** between Starlink and non-Starlink hosts. Figure 2 shows that Point-of-Presence (PoP) countries with the high-

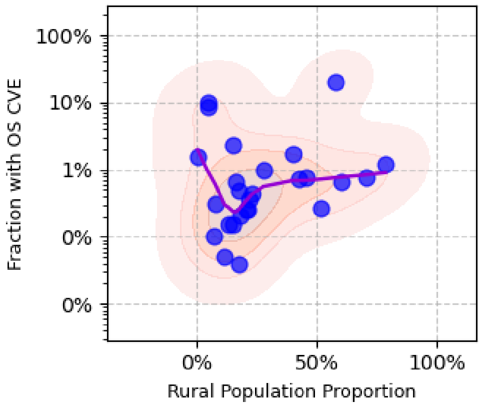

Figure 3: **Rural Populations use More Insecure OSes**– Per-country correlation of rural population percentage (as measured by the World Bank) and proportion of Starlink-connected hosts with an operating system affected by a CVE. LOESS trend line is shown in purple and data density in orange.

est rate of an operating system CVE for Starlink hosts are not necessarily countries with a high rate of OS CVE for non-Starlink hosts. Notably, Haiti sees a nine-fold increase in per-capita CVE vulnerabilities for hosts that are connected to Starlink versus those not, while Colombia sees a six-fold increase. This further indicates that Starlink hosts do not use the same operating systems as non-Starlink hosts or do not generally follow a similar practice of updating their operating systems that non-Starlink hosts do.

Utilizing statistical modeling, we observe that a number of countries' population of exposed-port, internet-connected hosts with operating system CVEs are likely drawn from different populations for Starlink-connected hosts versus non-Starlink-connected hosts. A binomial test shows with threshold $p \leq 0.05$ yields Colombia, Italy, and Haiti (notably, on three different continents) as countries where OS vulnerability is drawn from a different population for Starlink-connected hosts. Relaxing the threshold to 0.25 yields an additional four countries, Jamaica, Oman, New Zealand, and Qatar.

Finally, as a possible factor linking disparity in Starlink users' security posture, we analyze potential trends in the usage and applications of internet-connected hosts with **general population metrics**. As Starlink allows new areas and thus new demographics and industries to obtain a high-quality internet connection; we measure whether countries with more rural populations (and thus more Starlink usage in non-urban areas) tend to connect more insecure hosts to Starlink. Using data from the World Bank [1], we correlate the fraction of Starlink hosts with an OS CVE on a per-country basis with the proportion of the country's population living in a rural area. We observe that no countries with more than 20% rural population have fewer than 1 vulnerable machine out of 1000. South Sudan, a country with 79% of its population living in a rural area, sees CVEs in 1.18% of its Starlink-connected hosts.

4.2 Protocol Security

We also observe at Starlink hosts from a protocol perspective. We investigate the types of protocols that Starlink hosts run and assess their security. Given the diversity and number of existing protocols, this analysis focuses on three specific protocols–TLS, SSH, and SMB–to highlight a subset of protocol-level insecurities.

We find that Starlink hosts (especially in South America, Eastern Europe, and Southeast Asia) are particularly more compatible with insecure protocols. According to a Z-test for independence, Starlink hosts from 25 countries operate on insecure protocols at a significantly higher ratio than non-Starlink hosts from those respective countries.

4.2.1 TLS

One protocol we consider is Transport Layer Security (TLS), specifically, the version of TLS a host's service is running. TLS 1.0 and 1.1 are widely considered insecure due to their use of older cryptographic standards that are easily broken [14]. Analyzing TLS configurations provides a valudable method for detecting insecurity, as many common services (including HTTPS) operate on top of TLS, making it a target for attackers.

4.2.2 SSH

Another examined protocol is Secure Shell (SSH). SSH is another prevalent protocol for secure remote access, typically used to access a command-line interface on the host machine or for file transfer. Similarly to TLS, SSH uses different cipher modes to encrypt the connection. Some SSH servers may support insecure ciphers-—namely Cipher Block Chaining (CBC). This cipher is vulnerable due to padding oracle attacks [8], compromising its security. There are two versions of SSH: SSH-1 is generally completely insecure whereas SSH-2 is the most commonly used version.

4.2.3 SMB

The Server Message Block (SMB) protocol is used for sharing various resources over a network, including files and printers. However, earlier versions of the protocol, such as SMBv1 are recognized as insecure. Notably, SMBv1 does not support encryption at all. The use of SMBv1 is therefore included in our criteria for classifying a host as insecure, addressing specific scenarios not covered by TLS or SSH vulnerabilities alone.

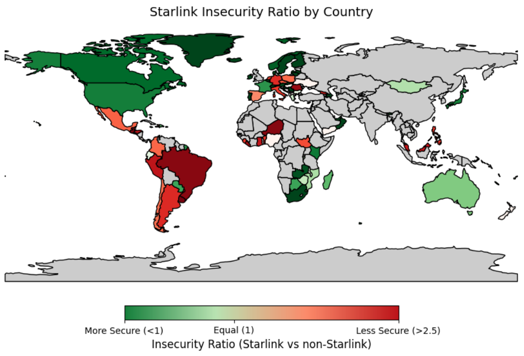
Starlink Insecurity Ratio by Country
More Secure (<1)
Equal (1)
Less Secure (>2.5)
Insecurity Ratio (Starlink vs non-Starlink)

Figure 4: **Disparity in distributions of insecure Starlink clients**–Calculated by the Starlink insecure rate over the total insecure rate. Countries with Starlink clients overrepresenting insecure clients (ratio > 1) are colored in red, while the opposite is in green.

Interestingly, according to Starlink Support, SMB should be blocked on all Starlink hosts—yet, some hosts do show up as SMB compatible [4].

4.2.4 Determining Insecurity

In our methodology, a host is classified as insecure if it exhibits any of the aforementioned vulnerabilities (e.g., outdated TLS, insecure SSH ciphers, or use of SMBv1). Other methods, such as a weighted insecurity score, are potential avenues of future research.

4.2.5 Global Distribution

Figure 4 shows the global distribution of hosts identified as insecure based on these protocol criteria. By dividing the proportion of insecure Starlink hosts by the rate of insecure hosts in the general population, a ratio is derived, which is depicted geographically to show the relative insecurity of Starlink hosts. Countries rendered in green indicate a ratio below 1, signifying lower insecurity rates among Starlink hosts compared to the general population, whereas a ratio above 1 (in red) indicates the opposite. We can see that Starlink overrepresents insecurity in certain regions, notably in namely Central/South America, Eastern Europe, and South East Asia.

Figure 5 shows the same comparative data in tabular form. Notably, Singapore exhibits the highest Starlink protocol insecurity ratio of 1342%.

4.2.6 Calculating Significance

A useful interpretation of the data necessitates an analysis of statistical significance. Using a Z-test for independence (and Fisher's test for $N < 30$), we calculate the probability that the Starlink hosts running insecure protocols come from a different distribution from hosts running insecure protocols over

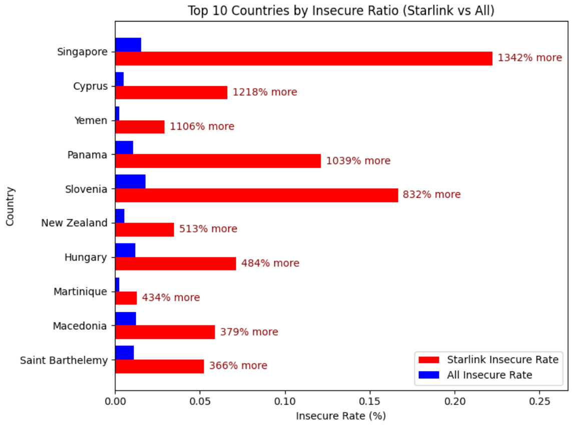

Figure 5: **Insecure Starlink clients per country (top 10**–Each country's insecure rate among just Starlink clients and among all clients. Ordered by average insecure rate.

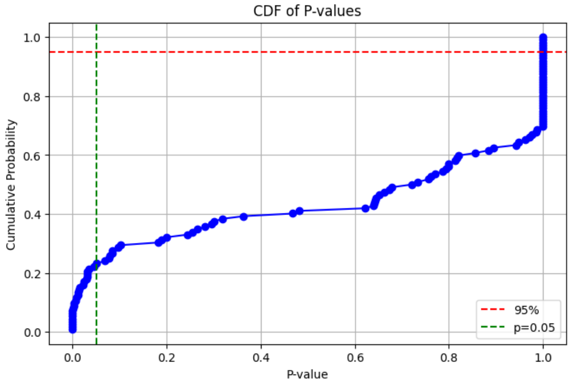

Figure 6: **CDF of Protocol Security Measure One-Tailed Z-test (and Fisher's test) resulting P-values**–25 countries analyzed have a p-value less than 0.05 (the common threshold for significance).

the internet at large. Figure 6 shows a CDF of each country's p-value. A small number of countries demonstrated statistically significant differences: specifically, 25 countries yielded p-values below the conventional significance threshold of 0.05.

4.3 Operational Security

Our third security perspective comes from analyzing the operational security of hosts, here defined as the security of services running on the host device. We analyze the number of open ports per host, which gives a rough approximation of the potential attack surface of each host. We also analyze the distribution of hosts running common services on non-standard (i.e. non-IANA specified) ports. Previous works on fully scanning the IPv4 address space have revealed these services are more likely to be insecure [10]. Overall, we observe that, like in the other perspectives, the operational security posture of Starlink hosts varies, both between different geographic regions and within the same geographic region between Starlink and non-Starlink hosts. Regarding open ports, we find that Starlink hosts in Asia are much more likely to have several accessible ports, with a different distribution shape than both the Starlink hosts in other continents and the non-Starlink hosts in Asia. With respect to non-IANA services, we observe that overall smaller proportions of Starlink users in North America and Oceania host unexpected services compared to the non-Starlink populations, while this proportion increases for hosts in South America.

4.3.1 Open Ports

We look at the number of open ports on each host as a proxy measure for its attack surface. In Fig 7, we compare the cumulative density functions of the number of open ports between the Starlink and Non-Starlink datasets, stratifying on the host continent.

In CDF plots for the Starlink dataset, we observe a much fatter-tailed distribution of open ports in Asia versus in the other 5 continents present in the dataset (Africa, Europe, North America, Oceania, and South America). The Starlink/Asia CDF accumulates 90% of the probability mass at 27 open ports per host, compared to 5 for the other 5 continents. There is a large proportion (44.4%) of the Asian sample with 10-30 ports open compared to <1.5% in every other continent in the set. This points to a second mode in in the Asian open ports distribution, whereas the other continental distributions seem to be roughly unimodal.

Comparing with the baseline data, the fatter-tailed distribution of open ports for Asian hosts persists, albeit with much less deviation from the other continents and without the bimodal distribution observed in the Starlink dataset. Additionally, the relative orderings of the continents (with respect to CDF accumulation speed) are not consistent between the Starlink and Non-Starlink datasets, with the exception of the Asia CDF which accumulates slowest in both datasets.

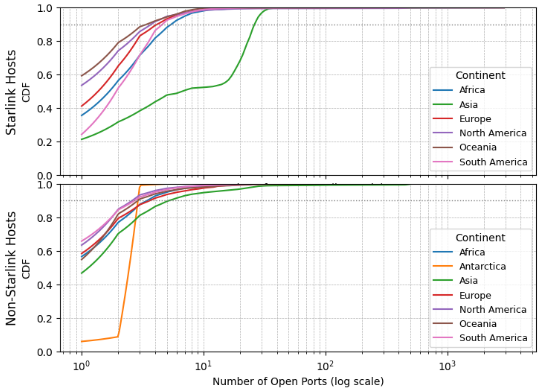

Figure 7: **CDF of open ports per baseline host**–Cumulative density function of open ports on the Starlink and non-Starlink datasets, sorted by continent.

4.3.2 Services on Non-Standard Ports

We also investigate the services running on Starlink hosts, specifically the quantities and types of services running on non-standard ports. We pick a set of 15 common services listed in Table 4.3.2, and count the instances of those services on ports besides the IANA-specified port, both on the Starlink and Non-Starlink samples.

Figure 9 shows the per-country difference in the proportion of hosts with at least one common service on a non-IANA port, between the Starlink dataset and the internet-wide baseline dataset.

Figure 8 shows that the distribution of non-standard services running on Starlink hosts differs between countries. We see a trend that the vast majority of non-standard services are HTTP, with SSH being a far second. In the certain countries (France, Philippines, Brazil), we see that SSH makes up a larger than expected proportion of non-standard services, potentially even outnumbering HTTP (Canada). In Peru, we see a different trend, RDP and HTTP make up the majority of unexpected services, with RDP being the majority. We do not see RDP make up a large proportion of non-IANA services in any other country in the dataset.

5 Discussion

Generally, we see patterns consistent with Starlink hosts–at least those not in front of CGNAT–having a different security profile than the internet at large. We argue that the use cases and location of Starlink customers–generally in more rural areas–strongly skews the protocols, operating systems, and operational security of hosts on the ISP. Generally, this manifests as a more insecure posture on the typical Starlink host,

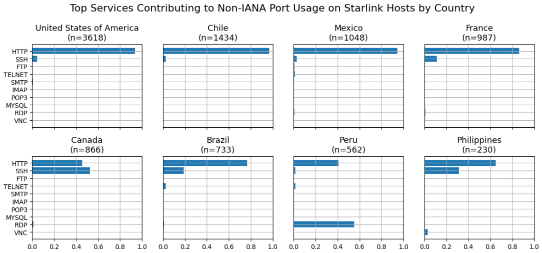

Figure 8: **Types of non-standard services per country (Starlink)**–Proportion of total non-IANA services contributed by each of the common services analyzed, per country

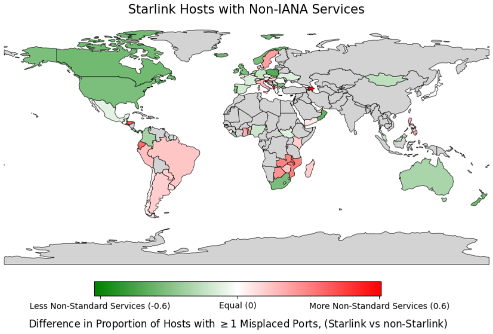
Starlink Hosts with Non-IANA Services
Less Non-Standard Services (-0.6)
Equal (0)
More Non-Standard Services (0.6)
Difference in Proportion of Hosts with ≥ 1 Misplaced Ports, (Starlink vs non-Starlink)

Figure 9: **Non-Standard Service Prevalence**–The difference in proportion of hosts with at least one common service on a non-IANA port between Starlink and non-Starlink. Green-shaded countries have a lower proportion of Starlink hosts with a misplaced service than the non-Starlink sample, with red representing the opposite. Grey countries were not represented in the Starlink dataset, so could not be compared.

Service	IANA Standard Port
HTTP	80
HTTPS	443
SSH	22
FTP	21
Telnet	23
SMTP	25
IMAP	143
POP3	110
DNS	53
MySQL	3306
RDP	3389
MongoDB	27017
Redis	6379
PostgreSQL	5432
VNC	5900

Table 1: **Common services and their standard IANA-assigned ports**–15 popular services used to identify unexpected service deployments on non-standard ports.

leaving it more vulnerable to attack. For operating system security, our LOESS trend line for countries with a rural population proportion above 25% exhibits a positive correlation, indicating that more rural countries have a higher fraction of insecure operating systems. Yemen, a country with 60% of its population living in rural area, sees an 11x increase in proportion of hosts running insecure protocols compared to the baseline of non-Starlink hosts. Across rural areas, security practices (and perhaps an unfamiliarity with Starlink) may contribute to a weaker security posture in Starlink hosts: areas which have traditionally not had access to the internet may have directly connected previously disconnected machines (running on a local network) to Starlink.

Simultaneously, there is a strong geographic bias in the level of security of Starlink hosts, with distinct geographic distributions of operating systems and protocols. Patterns in this bias do not align with usual levels seen in traditional ISPs, perhaps due to Starlink's use in locations not served by traditional ISPs. Across operating system security, protocol security, and operational security, we observe certain localities (countries) with a statistically significant negative difference in security level. One area where this trend is distinctly strong is South America, where FortiOS accounts for nearly 70% of of hosts with at least one port open, whereas no operating system dominates our baseline of non-Starlink hosts. Similarly, our blended protocol security metric shows that many countries in South America, such as Brazil, have Starlink hosts that are more insecure than their non-Starlink counterparts, while the prevalence of services non-standard ports across most countries in South America is higher with Starlink. On the other hand, Oceania demonstrates not only a more even distribution of operating systems with no single dominant one, but also fewer running insecure protocols and fewer services running on non-standard ports compared to the baseline. While any single perspective can indicate a real disparity in host security, a consistency in disparity in a single geographic region across the three perspectives shows that individual security practices and approaches are not necessarily isolated. Users, operators, and administrators in a geography may take different approaches in different geographies to maintain host security across all three fronts.

5.1 A Note on IP Geolocation

Starlink satellites do not just use "bent pipe" routing schemes; instead, sometimes satellites will link directly to each other using Inter-Satellite links (ISL). The final satellite may communicate with a PoP that isn't near the Starlink host, which skews the ability to geolocate based on IP [11]. Thus, the per-country statistics that we analyze may be skewed by Starlink's internal PoP preference configurations. Additionally, hosts in countries without Points of Presence may be grouped into a neighboring country. However, we do not expect this phenomena to strongly affect our aggregate statistics, as neighboring geographies often share similar characteristics.

5.2 Takeaways for Machine Administrators

Across our three security perspectives, machine administrators can take action to improve their attack surface. First, for machines exposed to the internet, regardless of which operating system is used, installing security updates frequently may avoid CVE vulnerabilities affecting older operating system versions. Additionally, our blended metric for protocol security highlights the prevalence of old TLS versions, outdated SSH ciphers, and SMB shares. Services running these protocols should be firewalled to internal network access only; for services absolutely necessary to be exposed, the protocol version should be used and any access mechanisms should be restricted to the strongest ciphers. Lastly, across operational security, as protocols running on non-standard ports may indicate a less secure ICS/IoT deployment [10], many of which are unnecessarily exposed to the internet, adding a firewall to prevent exposure of these ports to the public internet may dramatically decrease the attack surface.

5.3 Takeaways for LEO Network Operators

Generally, the threats to security studied in this paper are threats to machines exposed to the internet. The Starlink network already minimizes such threats by offering port exposure to business customers only; most customers are behind CG-NAT. For the remaining business customers with exposed ports, performing or strengthening upstream protection for customers may improve the security of the Network at large. For example, performing strong ingress filtering to block inbound connections to hosts running SMB may largely remove the threat of hosts leaking files through the insecure protocol. Similarly, network operators may opt to focus on a strong abuse monitoring program, where the service provider scans the network or passively monitors traffic and alert customers towards certain threats (e.g., banners indicating an insecure TLS version). Such a program would alleviate many security concerns from all three security perspectives discussed in this work, as any information indicating a poor security posture on a Starlink host was found through internet scanning.

5.4 Future Work

Some additional work can be undertaken to not only broaden the dataset we utilize but enable us to draw broader conclusions across all Starlink hosts. First–and perhaps most saliently–we hope to be able to include hosts not reachable by scanner-issued connections from the public internet, namely, those behind CGNAT. This effort may require an entirely different approach to scanning, such as through voluntary scanning from inside each customer's network, similar to work undertaken by Kumar et al [12].

Additionally, more information about visible hosts can perhaps be obtained by actively scanning those hosts based on preliminary information gathered from Censys. For example, being able to traverse un-protected SMB shares may allow us to glean information about how certain Starlink hosts are being used.

It may also be informative to characterize differences in security posture between the users of different satellite internet providers. Different providers cater to varying types of users (rural/residential, maritime, in-flight, etc.) with different priorities (latency, coverage) dependent on satellite orbit altitude; it could be interesting to compare the security practices of each group with one another, as well as a purely terrestrial baseline.

Finally, we hope to achieve better correlation of CVE vulnerabilities to each host. The Starlink Censys dataset contains a large number of columns, many of which describe software which can be linked to particular CVEs. Using more of these columns across of variety of software types (such as daemons and webservers and operating system components), combined with enhanced descriptions of the effect and scope of each CVE, can more broadly find CVEs affecting each host.

6 Conclusion

In this work, we performed a comparative analysis of the security characteristics of hosts connected to the Starlink AS versus a global sample of non-Starlink users. We compared from three perspectives: operating system security, protocol security, and operational security, and show some divergence from non-Starlink trends in all perspectives. A notable result is the distinct pattern of Starlink hosts in South America in which FortiOS makes up a 70% majority of host OSes, and where posture is broadly worse than the non-Starlink sample when considering misplaced services and protocol insecurity. We discuss results, and present takeaways and suggestions for both Starlink customers and network operators. Generally, we advise that machine administrators ensure that insecure OS/protocols are deprecated and that LEO Network Operators are cognizant of these potential issues and perform strong ingress filtering. While the Internet is globally expansive with many different hosts, clear patterns may emerge from characterizing said hosts.

7 Authorship & Contribution

Jacob Zhi contributed towards the investigation of operating system security across Starlink and non-Starlink hosts (analyzing the data, running statistical tests, and creating figures) as well as initial setup of the dataset and joins. Additionally, he wrote the methodology, operating system security results, and a majority of the discussion section in the paper.

Isaac Zanoria contributed towards the comparison of operational security between Starlink and non-Starlink users: the queries on the BigQuery datasets, the data analysis, and figure generation. He wrote the corresponding section in the paper, and contributed to the conclusion, the takeaways/future works, and introduction.

Omar Elamri wrote the introduction and related works section. He also contributed to the protocol security section by analyzing the data in the BigQuery datasets, running statistical tests, creating figures, and drawing conclusions from this data.

References

[1] World Bank Open Data. https://data.worldbank.org.

[2] Manos Antonakakis, Tim April, Michael Bailey, Matt Bernhard, Elie Bursztein, Jaime Cochran, Zakir Durumeric, et al. Understanding the mirai botnet. In *26th USENIX Security Symposium (USENIX Security 17)*, pages 1093–1110. USENIX Association, 2017.

[3] Manish Bhurtel and Danda B Rawat. Unveiling the landscape of operating system vulnerabilities. *Future Internet*, 15(7):248, 2023.

[4] Space Exploration Technologies Corp. What ip address does starlink provide? https://www.starlink.com/support/article/1192f3ef-2a17-31d9-261a-a59d215629f4.

[5] The MITRE Corporation. Cpe specifications — archive. https://cpe.mitre.org/specification/.

[6] Zakir Durumeric, David Adrian, Ariana Mirian, Michael Bailey, and J Alex Halderman. A search engine backed by internet-wide scanning. In *Proceedings of the 22nd ACM SIGSAC conference on computer and communications security*, pages 542–553, 2015.

[7] Zakir Durumeric, Frank Li, James Kasten, Johanna Amann, Jethro Beekman, Mathias Payer, Nicolas Weaver, et al. The matter of heartbleed. In *Proceedings of the 2014 Conference on Internet Measurement Conference*, pages 475–488. ACM, 2014.

[8] Christopher John Gerber. *Cybersecurity Risk Effects of Starlink on Rural Populations in the United States*. PhD thesis, Capitol Technology University, 2023.

[9] Google Inc. Bigquery overview. https://cloud.google.com/bigquery/docs/introduction.

[10] Liz Izhikevich, Renata Teixeira, and Zakir Durumeric. LZR: Identifying unexpected internet services. In *30th USENIX Security Symposium (USENIX Security 21)*, pages 3111–3128. USENIX Association, August 2021.

[11] Liz Izhikevich, Manda Tran, Katherine Izhikevich, Gautam Akiwate, and Zakir Durumeric. Democratizing leo satellite network measurement. *Proceedings of the ACM on Measurement and Analysis of Computing Systems*, 8(1):1–26, 2024.

[12] Deepak Kumar, Kelly Shen, Benton Case, Deepali Garg, Galina Alperovich, Dmitry Kuznetsov, Rajarshi Gupta, and Zakir Durumeric. All things considered: An analysis of IoT devices on home networks. In *28th USENIX Security Symposium (USENIX Security 19)*, pages 1169–1185, Santa Clara, CA, August 2019. USENIX Association.

[13] Antonio Mangino, Morteza Safaei Pour, and Elias Bou-Harb. Internet-scale insecurity of consumer internet of things: An empirical measurements perspective. *ACM Transactions on Management Information Systems (TMIS)*, 11(4):1–24, 2020.

[14] National Security Agency. Eliminating obsolete transport layer security (tls) protocol configurations. Technical Report U/OO/197443-20, National Security Agency, January 2021. Accessed: 2025-05-16.

[15] Jussi Nikander, Onni Manninen, and Mikko Laajalahti. Requirements for cybersecurity in agricultural communication networks. *Computers and Electronics in Agriculture*, 179:105776, 2020.

[16] National Institute of Standards and Technology. Nvd data feeds. https://nvd.nist.gov/vuln/data-feeds.

[17] Drew Springall, Zakir Durumeric, and J. Alex Halderman. Ftp: The forgotten cloud. In *2016 46th Annual IEEE/IFIP International Conference on Dependable Systems and Networks (DSN)*, pages 503–513. IEEE, 2016.

[18] Starlink. Technology. `https://www.starlink.com/technology`. Accessed: 2025-05-16.

[19] Nasser Tieby, Joseph Khoury, and Elias Bou-Harb. Characterizing and analyzing leo satellite cyber landscape: A starlink case study. In *ICC 2024 - IEEE International Conference on Communications*, pages 1352–1357. IEEE, 2024.

[20] Emily A. Vogels. Some digital divides persist between rural, urban and suburban america. *Pew Research Center*, August 2021.

[21] Gerry Wan, Liz Izhikevich, David Adrian, Katsunari Yoshioka, Ralph Holz, Christian Rossow, and Zakir Durumeric. On the origin of scanning: The impact of location on internet-wide scans. In *Proceedings of the ACM Internet Measurement Conference*, pages 662–679. ACM, 2020.

[22] Linkang Zhang, Yunyang Qin, Yujia Zhu, Yifei Cheng, Zhen Jie, and Qingyun Liu. Seestar: An efficient starlink asset detection framework. In *International Conference on Science of Cyber Security*, pages 139–156, Cham, 2023. Springer Nature Switzerland.