



GREYNOISE

# ATTACKERS WITHOUT BORDERS:

THE VIEW OF GLOBAL MALICIOUS TRAFFIC FOR THE KINGDOM OF SAUDI ARABIA



## C O N T E N T S

- [p.03] Executive Summary
- [p.04] Malicious Inbound Traffic
- [p.08] Malicious Outbound Traffic
- [p.10] In Summary
- [p.11] Addendum

# Executive Summary

**In today's interconnected world, understanding the landscape of malicious internet cyber activity is crucial for organizations and nation states to protect their digital assets and maintain a strong security posture.**

To that end, researchers from GreyNoise Labs analysed the volume and type of malicious traffic observed by GreyNoise Intelligence's planetary scale sensor network — with a hyperfocus on the Kingdom of Saudi Arabia — to help organizations and agencies make more informed decisions about their cybersecurity strategies.

The GreyNoise operated sensor fleet primarily sees opportunistic, mass exploitation. This view provides an up-to-the-minute view of the regular drumbeat of botnet activity, but also sheds light on when new patterns or activity surfaces, especially when there are new, emergent threats.

The term “malicious” is reserved for activity that is associated with an attempt to execute an exploit against a target system.

The data for this report looked at malicious traffic coming from or directed at the Kingdom of Saudi Arabia for a period of 30 days in October 2023.

During that time GreyNoise observed 52,602 malicious exploitation attempts against the Kingdom of Saudi Arabia IP address space and 2,204 attacks from the Kingdom of Saudi Arabia being directed at other country-assigned networks.

The sections in this brief will look at the source and destination traffic in more detail and conclude with recommendations for how this information can be use to make organizations, agencies, and citizens safer.

//

# Malicious Inbound Traffic

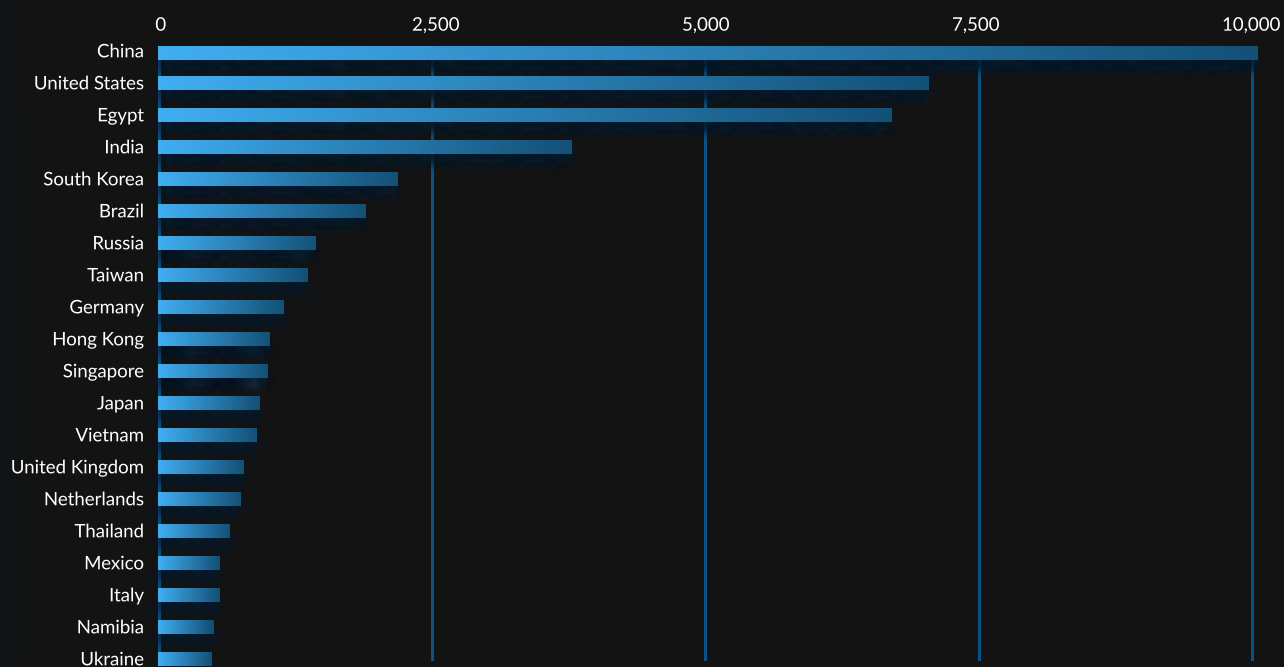
The “Research Notes And References” section provides information on the nuances of source-country attribution.

Generally speaking, organizations and agencies can expect to see their malicious source traffic to come from either (a) countries with higher allocated and in-use IP address space, or (b) countries with internet-facing device profiles that lend themselves to be more prone to exploitation.

To see how that mix plays out, Brazil and Vietnam are in sixth and thirteenth place, below, during the sample period but tenth and twenty-third when it comes to available IP address space. This is due to an inordinately high number of compromised internet of things (IoT) devices, such as IP-accessible cameras, and both white-box and popular-but-regularly-vulnerable networking equipment, such as MicroTik.

## TOP 20 SOURCE COUNTRIES

MALICIOUS EXPLOITATION ATTEMPTS

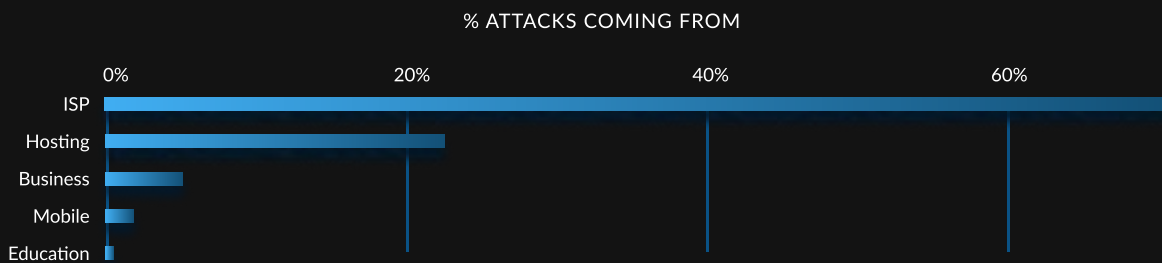


This inbound country view will be dynamic if you use the GreyNoise Visualizer or API to perform future assessments. Meaning, members of the list will trade places depending on what adversary controlled infrastructure is in use within any given time period.

You can use geographic source information as one means of risk-assessing connections you see in logs or network flows to help inform blocking or incident response decisions.

The source networks these IP addresses are hosted in can be classified in many ways. For this report, we will focus our attention on the assigned category – ISP, Hosting, Mobile, Business, or Education – for these malicious connection attempts:

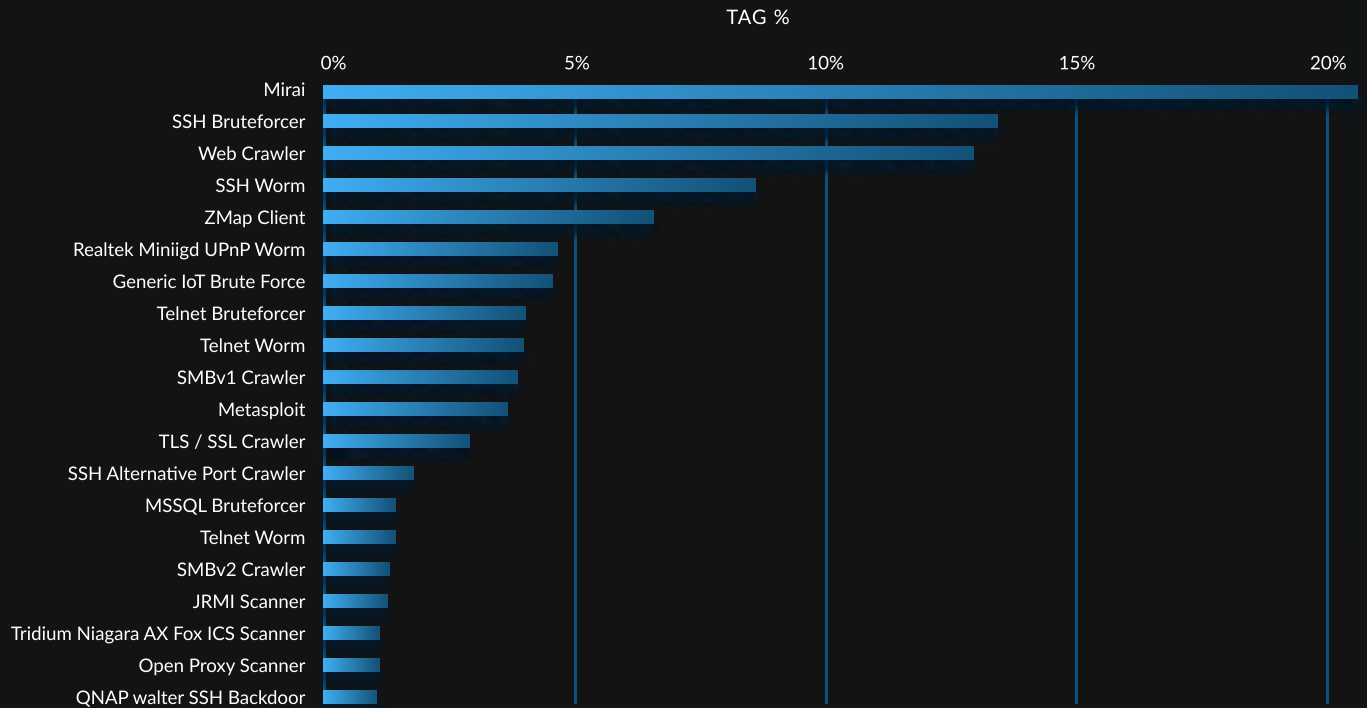
## MALICIOUS INBOUND TRAFFIC NETWORK CLASSIFICATION



Of initial note is that “Mobile” is fourth on the list. Researchers in GreyNoise Labs have observed a steady up tick in mobile networks – whether it be from tethered systems or compromised Android devices – becoming the source of attack traffic. This increases the burden on defenders, since it is difficult to convince application owners to block any connections from what is around 40-50% of all incoming benign traffic to most websites and web applications. The timely nature of GreyNoise block lists may make such conversations less problematic.

Routers, exposed storage and IoT devices, and compromised laptops/desktops are a large part of why residential and small business ISPs regularly top the list. To understand why, all we need to do is look at the top “tags” (“detections” in intrusion detection and prevention nomenclature) GreyNoise sees in this the Kingdom of Saudi Arabia inbound traffic:


# MALICIOUS INBOUND TRAFFIC TAGS




The Mirai botnet is almost always in the number one spot when it comes to malicious, opportunistic activity engaged by our adversaries, but it often trades places with “SSH Bruteforcer”, which is in the number two spot for this date range in the Kingdom of Saudi Arabia IP space. Both of these traffic sources are part of the “heartbeat” of the internet. Not a single minute passes without members of the Mirai botnet searching for new and existing hosts to assimilate into its collective. Similarly, attackers regularly hurl thousands of credentials at every remote login point they can reach. This activity, combined with other “Worm”s, help ensure a healthy inventory that can be used in targeted attacks against your agency or organization.

The “Bruteforcer”s can also be used to build up botnet inventories, but they have a secondary nefarious purpose of working to gain Initial Access, which can be sold to bidders on attacker forums. All it takes is for an organization or individual to leave a default or misconfigured system on the internet for less than an hour to have it become part of this adversarial inventory. It is rare for targeted attack infrastructure to be used for this, quiet noisy, activity. Therefore, it is strongly advised to consider blocking these attempts at the network level and checking for outbound requests to IP addresses exhibiting this behaviour.

Before we look at what systems and devices in the Kingdom of Saudi Arabia are targeting, we should note that of the 52,602 inbound malicious exploitation attempts, 304 (0.58%) were directed only at the Kingdom of Saudi Arabia during the observation period. This may indicate that organizations, such as the Kingdom of Saudi Arabia's National Cybersecurity Authority (NCA) is helping to make country networks sufficiently resilient against attacks to force attackers to direct country-centric efforts elsewhere.



*“The Mirai botnet is almost always in the number one spot when it comes to malicious, opportunistic activity engaged by our adversaries, but it often trades places with “SSH Bruteforcer”, which is in the number two spot for this date range in the Kingdom of Saudi Arabia IP space. Both of these traffic sources are part of the “heartbeat” of the internet. Not a single minute passes without members of the Mirai botnet searching for new and existing hosts to assimilate into its collective. Similarly, attackers regularly hurl thousands of credentials at every remote login point they can reach. This activity, combined with other “Worm”s, help ensure a healthy inventory that can be used in targeted attacks against your agency or organization.”*



//

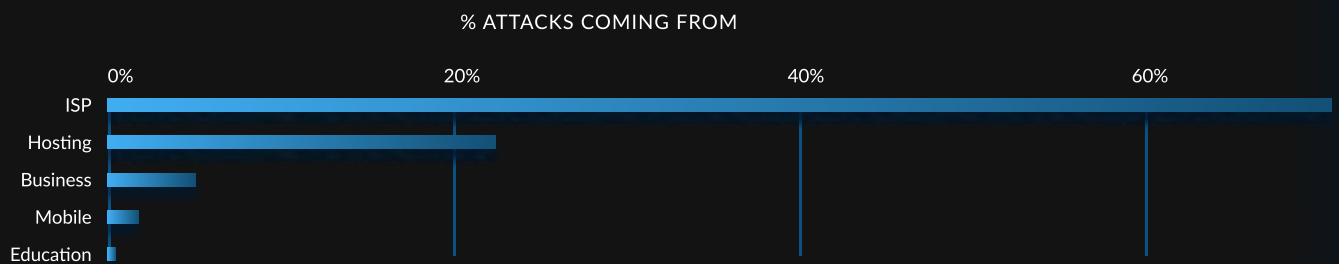
# Malicious Outbound Traffic

During the study period, GreyNoise researchers observed a mere 2,204 malicious exploitation attempts coming from the Kingdom of Saudi Arabia-attributed network sources.

The outbound tag distribution is nearly identical to the inbound, so we'll avoid repetition and focus on two points of interest.

First, "Business" networks are third on the list, and "Mobile" are fourth:

## MALICIOUS OUTBOUND TRAFFIC NETWORK CLASSIFICATION



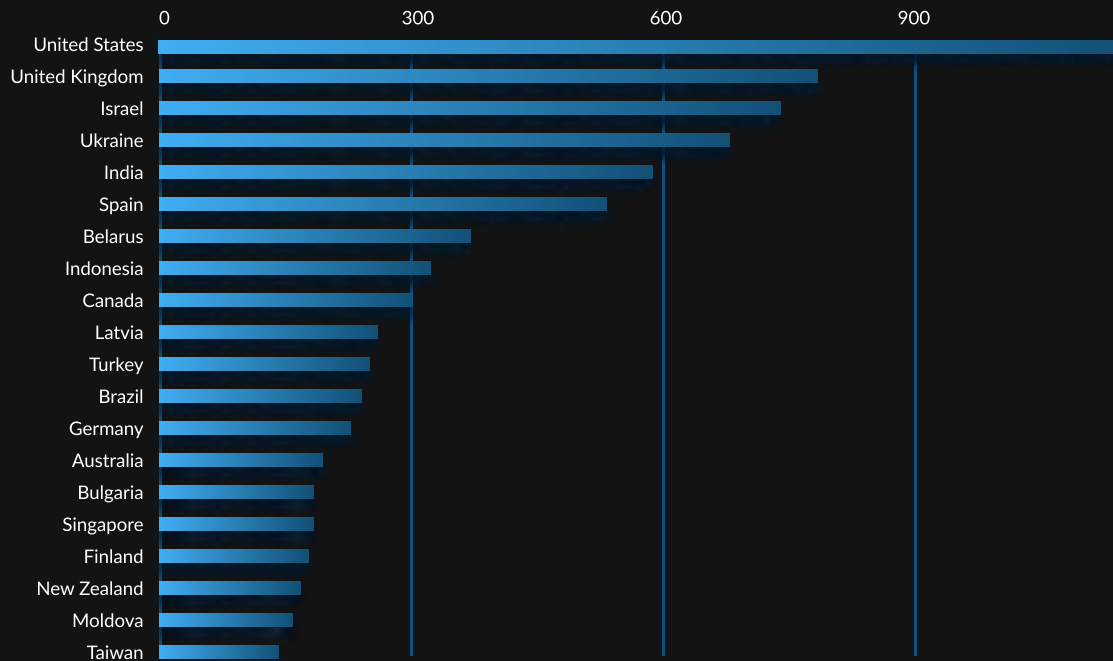
This is somewhat disconcerting given the discussion in the "Inbound" section. Both the NCA and organizations that help provide cybersecurity services to mobile providers and small-to-medium-sized Business in the Kingdom of Saudi Arabia may want to consider implementing more rigorous malicious activity checks to reduce the likelihood of these networks being increasingly used in adversarial campaigns.

The next, and final, point is that nodes under adversarial control in the Kingdom of Saudi Arabia seem to be aiming at non-sovereign IP address space, though the malicious traffic is also spread around:



# TOP 20 DESTINATION COUNTRIES

## MALICIOUS EXPLOITATION ATTEMPTS



The Kingdom of Saudi Arabia has a robust cybersecurity framework in place. The country has passed information and communication technology laws that criminalize cyberattacks and other malicious online activities. The most comprehensive of these is the [Anti-Cyber Crime Law of 2007](#). The country also has a National Cybersecurity Strategy, developed to balance security, trust, and growth, and to create a safe and reliable Saudi cyberspace. If the government observes IP addresses within the Kingdom of Saudi Arabia attacking other IP addresses in the country, the penalties can include imprisonment for up to one year and/or fines up to SAR 500,000, depending on the specific crime. This strategy and framework seems to have done its job.

Organizations can use GreyNoise to see if they're "part of the problem", and agencies in the Kingdom of Saudi Arabia should work closely with ISPs, hosting providers, mobile carriers, and businesses to ensure the Kingdom of Saudi Arabia's IP space reputation continues to trend positive.

//

# In Summary

**Every GreyNoise user can use the same data provided in this report to gain hourly insights into malicious activity coming from or to organization and agency networks in the Kingdom of Saudi Arabia.**

Those same queries can be tailored to provide timely alerts for emergent threats being targeted at, or coming from the Kingdom of Saudi Arabia networks. By working together, we can help reduce the number of active botnet nodes on the internet, and make the internet that much safer for the humans we're aiming to protect.

//

# Addendum: Research Notes, References, And Definitions

## GREYNOISE TAGS

A GreyNoise “Tag” is a signature-based detection method used to capture patterns and create subsets in our planetary-scale internet sensor data. Tags cover five primary categories: Activity, Tool, Actor, Worm, and Search Engine. These tags are not limited to CVE-based activity but also include behaviours, attribution, and unique traffic characteristics.

Activity tags cover crawlers, vulnerability checks & exploitation, authentication attempts, and other behaviours observed from interactions with GreyNoise sensors. Tool tags can include open-source scanning tools and programming language libraries, such as NMap, Nuclei, Metasploit, Paramiko, and Go HTTP. Actor tags describe the actor behind the activity, including commercial/enterprise entities, researchers, and universities. Please note that all current Actor tags denote Benign actors. This may change in the future, but GreyNoise does not presently engage in malicious actor attribution.

GreyNoise tags provide insight into IP addresses that are scanning the internet or attempting to opportunistically exploit hosts across the internet. Tag data associated with a specific IP address offers an overview of the activity that GreyNoise has observed from that IP, as well as insight into the intention of the activity originating from it.

## GREYNOISE QUERIES USED

The following GreyNoise Queries (GNQL) were used in this analysis:

- destination\_country\_code:SA spoofable:false classification:malicious
- destination\_country\_code:SA spoofable:false single\_destination:true classification:malicious
- source\_country\_code:SA spoofable:false classification:malicious

These can be viewed on the [GreyNoise Visualizer](#), and the data behind them accessed via the [GreyNoise API/CLI](#).

## COUNTRY ATTRIBUTION

[IANA](#) (the Internet Assigned Numbers Authority) is charged with allocating internet address space to regional registries; and, [RIPE](#) is responsible for the Kingdom of Saudi Arabia address space allocations. Traffic coming from IP address space allocated to a given country does not mean that country has malicious intent. It generally means systems and devices in that country were either vulnerable to some exploit that coopted them into the service of adversaries. However, there are numerous “bulletproof hosting” companies – think of them as a “malicious Amazon AWS” or “evil Google Cloud Platform” – that regularly emerge in any given IP address space as well.

## IP ADDRESS METADATA

GreyNoise uses [IPInfo.io](#) for IP geolocation, autonomous system (ASN), and hosting classification metadata information. [Spur](#) is used for identifying VPN, Tor and other network classifications. [Kasada](#) is used for bot identification.

//



GREYNOISE  
INTELLIGENCE

[greynoise.io](https://greynoise.io)

Copyright © 2023 GreyNoise, Inc.