# Cyber Insights: from Malawi

Quad9's Post-Deployment Observations of Malawi's Cybersecurity Landscape

## Executive Summary

Quad9 is a global DNS service that offers enhanced cybersecurity measures, privacy protection, and improved Internet performance. Quad9's arrival in Malawi marks a pivotal advancement in fortifying the country's digital infrastructure, bringing with it enhanced cybersecurity safeguards, robust privacy protection, and a boost in Internet performance.

Digital literacy is still evolving in Malawi. The communities here are prime targets for the Internet's sophisticated measures to seed malware.  Quad9's ability to block access to malicious websites is thus of paramount importance to this nascent Internet economy. Providing vital protections from phishing, malware, and ransomware for both individual users and organizations, especially in sectors like government, education, and healthcare, which often handle sensitive data is part of Quad9's primary objective.

The implementation of Quad9 in Malawi is a low-cost, high-impact solution to enhance digital security, performance, and privacy. It aligns with the nation's goals to advance its digital infrastructure while protecting and empowering its citizens in the digital domain.

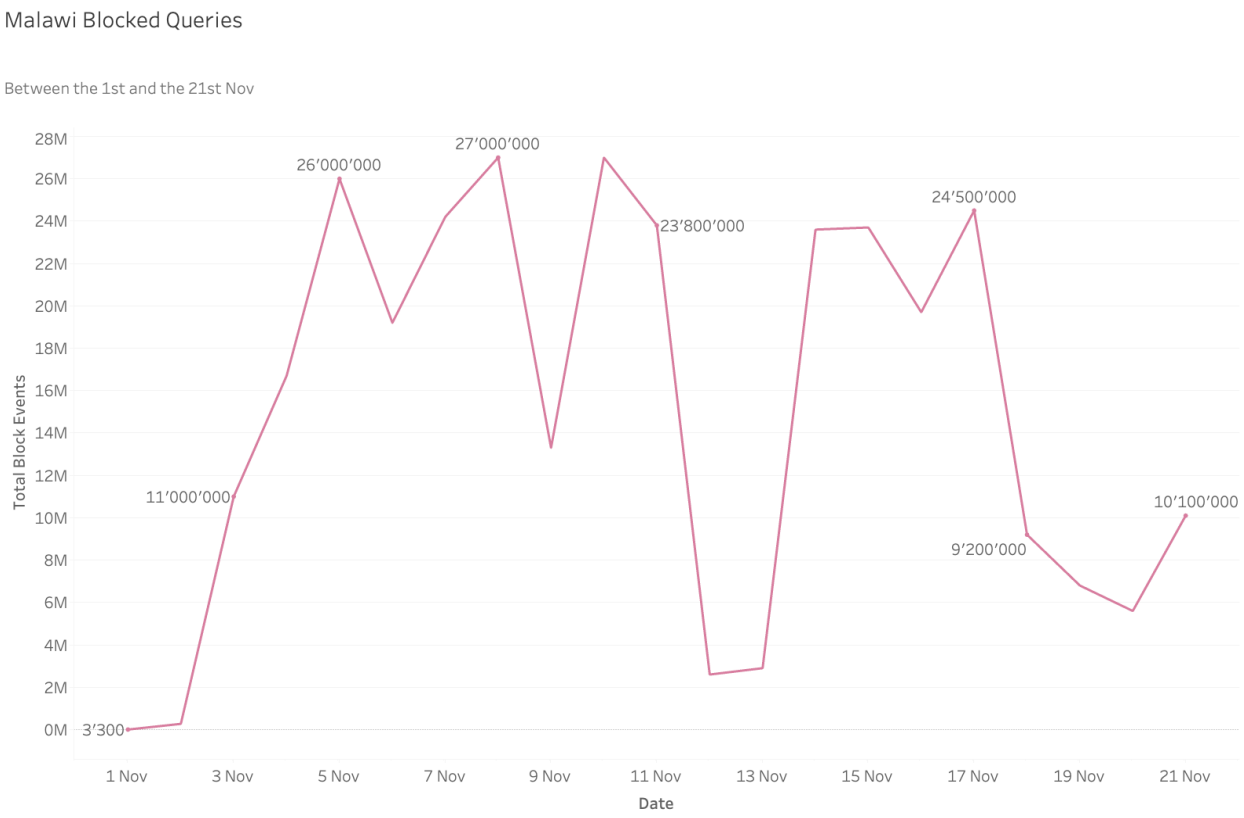
DNS
Privacy
Security
Performance

# Introduction

Quad9's extensive global network of servers ensures a faster, more reliable Internet experience. DNS responses are provided from infrastructure hosted at the country's established Internet Exchange Point, meaning that this is the most neutral, and fastest possible route for Malawian network operators.  In a country where Internet data pricing is still comparatively high and Internet speeds can be inconsistent, reducing the spread of malvertising, as detailed in the report provides immediate economic benefits to end-users.  Overall, this means improved access to digital resources, more seamless online transactions, and a boost in overall user experience.

To safeguard our users, Quad9 blocks DNS lookups of malicious host names using continually updated threat information. This proactive measure protects computers, mobile devices, or IoT systems from a broad spectrum of cyber threats, such as malware, phishing, spyware, and botnets Quad9's DNS-based blocking cannot prevent all possible risks – only those that are attributable to attacks that have a DNS component, which is estimated to be 30% of all cyber attacks[1]. This report provides an overview of the security threats that Quad9 DNS has blocked in Malawi since its deployment in November 2023.

[1] https://www.globalcyberalliance.org/wp-content/uploads/GCA-DNS-Security-Report.pdf



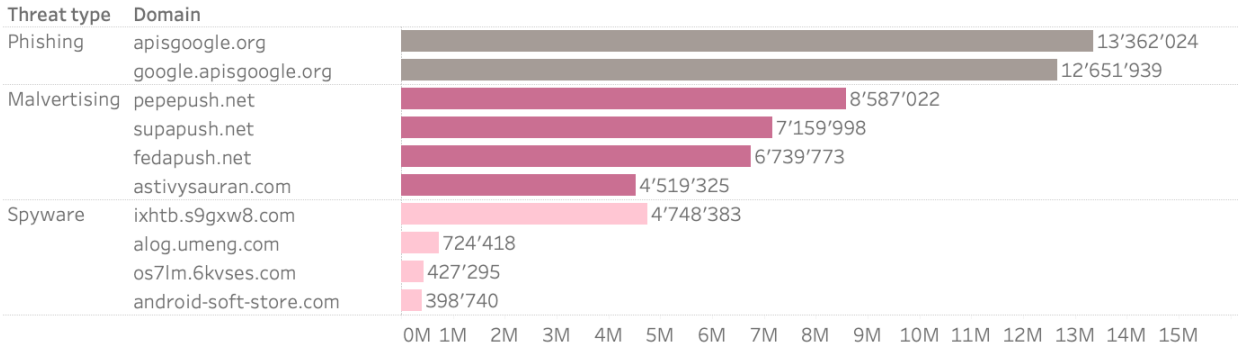

*Total daily volume of Quad9 blocked queries in Malawi since the 1st November 2023*

# Most prevalent threats

Since the deployment of Quad9 services in Malawi in November 2023, many Malawian users have been shielded from a variety of cyber threats, including phishing, stalkerware, spyware, and malvertising. In this section, we will discuss the key threats that target Malawian Internet users.

Top 10 Blocked Domains in Malawi

Between the 1st Nov and the 21st Nov 2023



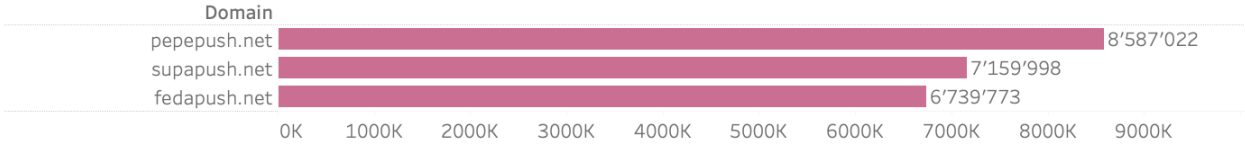

## The High Volume of Blocked Queries to the Domain Spoofing Google.org

The domain that had the highest number of blocked queries was one impersonating google.org. According to our Threat Intelligence partners, the domain apisgoogle[.]org is used for phishing attacks. Phishing is a type of cyberattack where scammers attempt to trick people into revealing sensitive information, such as passwords, credit card data, and social security numbers. Phishing attacks can be carried out via email, text messages, social media, or even phone calls. Phishing emails are often disguised as messages from legitimate companies, such as banks, credit card companies, or government agencies. They often contain links to fake websites that look like the real websites of these companies. If the victim clicks on one of these links and enters their personal information, the scammer will be able to steal it.

## Campaigns Redirecting Users to Malicious Advertisements

We have observed a significant number of queries to the domains related to the Omnatour malvertising network. This campaign compromises vulnerable WordPress sites through embedded malicious JavaScript or PHP code. The injected malicious code

then redirects users to view and click malvertisements via pop-ups and push notifications[2].



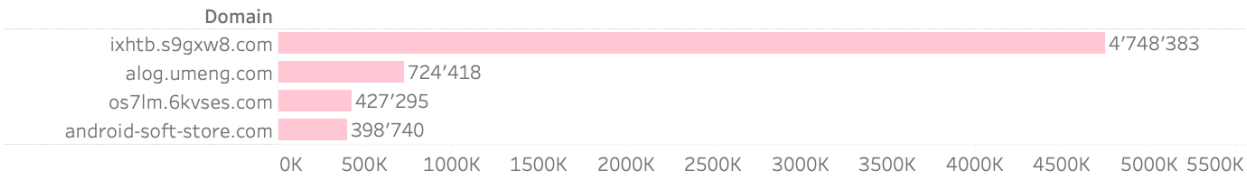

*Blocked queries to the Omnatour malvertising network*

Another malvertising domain to which we observed a high volume of queries is astivysauran[.]com. This website redirects users' browser to a variety of undesirable content, including ads for unwanted browser extensions, surveys, adult sites, online web games, fake software updates, and unwanted programs. Users might encounter this website through redirections from other websites push notifications, or involuntarily, by malware that opens the site without their consent.

## The Silent Menace of Stalkerware

Stalkerware and spyware applications are used to record users' conversations, location and everything the user types, all while camouflaged as a legitimate application such as a calculator or a calendar.

[2] https://blogs.infoblox.com/cyber-threat-intelligence/cyber-threat-advisory/vast-malvertising-network-hijacks-browser-settings-to-spread-riskware/




*Blocked queries to the domains attributed to spyware and stalkerware*

Based on our Open Source Research (OSINT) research, the programs communicating with ixhtb.s9gxw8[.]com are often downloaded from untrusted sources in the form of Android applications, especially fake games such as Flappy Bird or Apex Legends. We were able to find multiple fake game samples confirming such malicious connections to this domain. After the user downloads the fake software, the application drops unwanted programs (PUPs) that perform activities without the user's knowledge. These activities commonly include establishing remote access connections, capturing keyboard input, collecting system information, downloading/uploading files, dropping other malware into the infected system, performing denial-of-service (DoS) attacks, and running/terminating processes.

Android-soft-store[.]com was attributed by Kaspersky researchers to the Command and Control server of the WhatsApp spy mod spread through Telegram[3]. The trojan is disguised as a mod that offers extra features, such as the ability to see deleted messages. Once installed, the trojan steals personal information from the victim's device and sends it to a criminal's server. The criminal can then use this information to blackmail or impersonate the victim. It is important to be aware of the dangers of installing mods from unknown sources, and to only install apps from trusted developers. The trojan was previously noted as mostly targeting Arabic-speaking users.

[3] https://securelist.com/spyware-whatsapp-mod/110984/

# Caveats

To maintain our own strict privacy policy, and to align with Swiss regulated privacy standards, Quad9 does not store end-user IP address information. (See https://www.quad9.net/service/privacy for details on our policy.) Therefore, it is not possible to associate individual block events with end users – it is known only that the event was blocked, and the user was prevented from reaching the malicious destination.

Normally, Quad9 has no insight into the actual number of end users, but in this case our team worked in concert with a large domestic carrier, who directed their user community to us, as the same time that we activated our location in Blantyre. This is a rare circumstance that allowed us to have more accurate figures for this research. Normally, Quad9 has little control over, or understanding of the user community in a location after activation. Additionally technical issues such as forwarding DNS caches disguise end user queries.

# Conclusions

Over the years, it has become easier and cheaper for cyber criminals to attack Internet users. Quad9's mission is to improve the security and stability of the Internet and reduce users' vulnerability to risk and become more effective in their daily online interactions - even in the face of growing cyber attacks.

By preventing connections to malicious sites, Quad9 eliminates exposure to risks before they are downloaded to computers or a victim can see the fraudulent website. The inability to reach a malicious host means that defenses such as virus protection or user-based detection such as certificate examination are never called into action.

The substantial amount of mitigation events observed in Malawi suggests a heightened rate of cyber threats, including malware, phishing attacks, and stalkerware insertions. Notably, the ratio of blocked queries to legitimate DNS queries is often more than 4%, a figure that's considerably higher than in other regions where Quad9 has gathered data. In some cases, this block rate level exceeds that of other locations by up to two orders of magnitude, underscoring the significantly elevated cyber threat landscape in Malawi.

Quad9 is a non-profit organization, whose main goal is to protect end users against harm while providing them private and trustworthy access to DNS resources, all at no cost to the end user. The ability to provide reports, either automated or researched, is an option that is a supportable output of our larger mission to improve cybersecurity and Internet stability.

This partnership between Quad9 and the Malawi Internet Exchange Point (MIX) in Blantyre has emerged as a cornerstone in the landscape of cybersecurity in Malawi. The cooperation between these two entities underscores the significance of collaborative efforts in enhancing Internet security and infrastructure. MIX's commitment to providing a robust platform for Internet exchange has been pivotal in supporting Quad9's objective of delivering secure DNS services. This synergy not only fortifies cybersecurity within Malawi but also extends its impact globally. Such partnerships are essential in navigating the evolving challenges of cybersecurity and in safeguarding the digital ecosystem into the future.

Report Generated December 2023

Emilia Cebrat-Masłowski, Director of Threat Intelligence, emilia@quad9.net