Trends Q3 2023:
Cyber Insights

About This Report

To protect our users, Quad9 blocks DNS lookups of malicious host names from an up-to-the-minute list of threats. This blocking action protects your computer, mobile device, or IoT systems against a wide range of threats, such as malware, phishing, spyware, and botnets, and it can improve performance and privacy. This quarterly report provides security insights on the threats blocked by Quad9 DNS. The report combines DNS telemetry data and open-source intelligence with statistics and analysis to provide security insights on the top malicious domains visited by our users and blocked by Quad9 DNS. Additionally, the report presents key regional threats targeting Quad9 users.

Methodology

Data was gathered during the third quarter of 2023. Due to the volume of DNS requests, Quad9 did not collect all of them. Instead, we recorded samples daily, every hour, for 60 seconds. Improvements to this process are ongoing.

Overview

In the third quarter, our users were targeted by a variety of threats, including phishing, banking trojans, crypto-malware, and stalkerware.

This quarterly report analyzes the top malicious domains blocked by Quad9 DNS and the threats associated with them. For more detailed data on the specific threat categories and volumes of attempted access, please refer to the dedicated sections of this report.

Victimology - Top Regional Threats

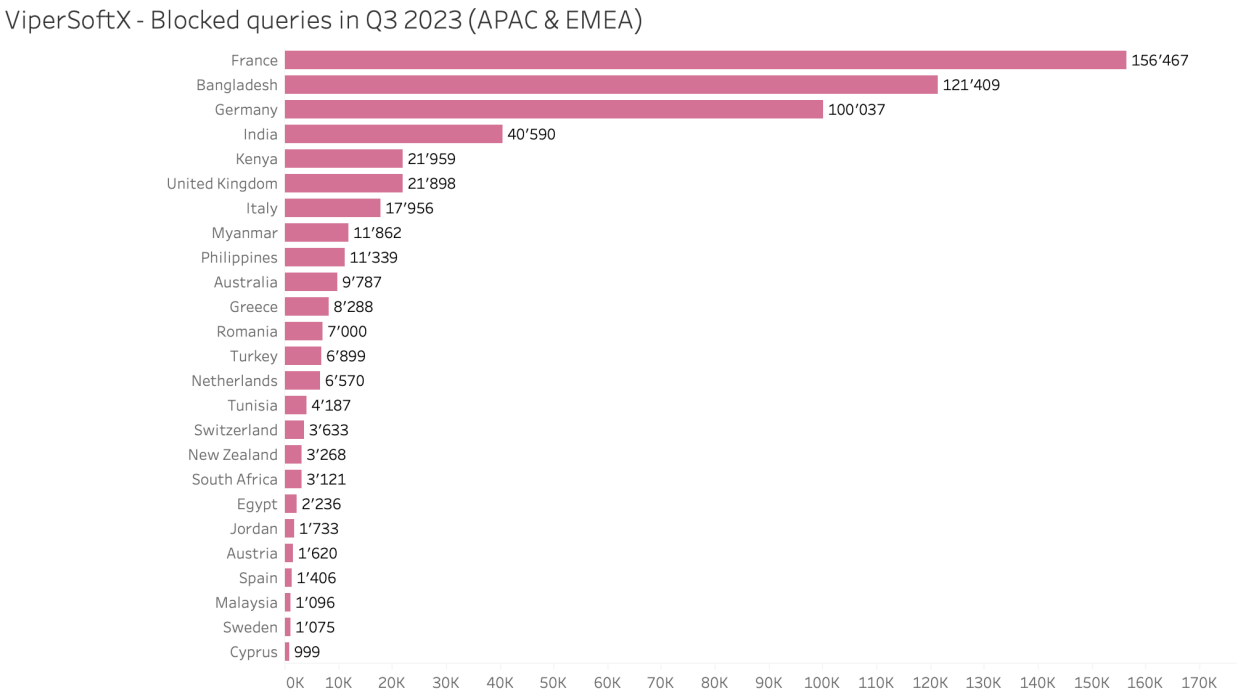
In the third quarter, we observed a shift in the threats targeting our users in the Asia-Pacific (APAC) and Europe, Middle East, and Africa (EMEA) regions. DDoS (distributed denial-of-service) attacks were no longer the top threat targeting users in these regions. However, banking trojans and phishing continued to be the top threat targeting users in the Americas region. The continued threat of banking trojans in the Americas region is likely due to the region's large financial sector and the high number of online banking users.

APAC & EMEA

Users in the APAC and EMEA regions initiated the most queries to the domain attributed to the Remote Access Trojan (RAT) - ViperSoftX. This is a malware that can steal cryptocurrency wallet addresses and password information stored in browsers and password managers. It is often distributed through the download of cracked software from suspicious domains, torrent downloads, and key generators (keygens) from third-party sites. The malware was initially observed in the early 2020s, but it has grown extensive and our observations show it is being actively exploited recently. ViperSoftX is Windows malware and deploys a Google Chrome extension named 'VenomSoftX'. Quad9 observed multiple domains attributed to this malware and generated using a domain generation algorithm (DGA which were also reported by threat researchers[1].

The most impacted Quad9 users in APAC were located in India, Myanmar, and the Philippines, followed by Australia and New Zealand. In EMEA, the most impacted users were located in France, Germany, the United Kingdom, and Kenya.

[1] https://chris.partridge.tech/2022/evolution-of-vipersoftx-dga



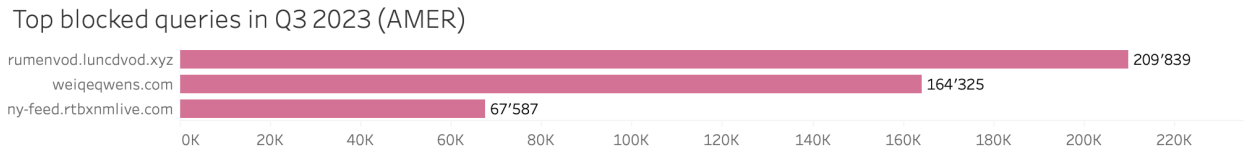
Americas

In the US, the most significant threat in the third quarter was again attributed to banking trojans and phishing attacks.

Banking trojans are malware designed to steal banking information from victims. They are often spread through malspam, which are emails that contain malicious attachments or links. One of the most common banking trojans is Ursnif/Gozi. This malware is spread through Microsoft Office document attachments or ZIP files. Once it is installed on a victim's computer, it can collect victim information from cookies, login pages, and web forms. The impacted users quering malicious domain weiqeqwens[.]com were only based in the US.

The other countries in the Americas region were impacted by phishing attacks. Phishing is a type of cyberattack where scammers attempt to trick people into revealing sensitive information, such as passwords, credit card numbers, and social security numbers. Phishing attacks can be carried out via email, text message, 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. The emails may 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. In this case the most impacted Quad9 users were located in Ecuador, Argentina and Mexico.



The Hidden Dangers of Kids Tracking Software

Stalkerware is spyware that can be used to track and monitor a person's activities without their knowledge or consent. Stalkerware applications can record conversations, track location, and even log everything a user types. These applications are often disguised as kids tracking software.

Kids tracking software is a type of software that allows parents to track their children's online activity and location. While this software can be a useful tool for parents who want to keep their children safe, there are also some potential threats associated with it.

One of the biggest dangers related to kids tracking software is security breaches. If the software is not properly secured, hackers could gain access to the data that it collects, including the child's location, browsing history, and personal information. This data could be used to stalk or harass a child. If an abuser has access to the child's tracking data, they could use it to track the child's location and movements.

The highest volume of queries to a domain attributed to kids tracking software originated from highly developed countries such as the US, Germany, United Kingdom, Netherlands and Spain.

Conclusions

Over the years, it's become easier and cheaper for hackers 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.

As a DNS provider, Quad9 has the unique opportunity to analyze the volumes and trends of malware campaigns. If you are a security researcher or threat intelligence provider and want to hear more, contact us via our website at: https://quad9.net/support/contact

About Quad9

Quad9, a nonprofit in the US and Switzerland, provides free cybersecurity services to the emerging world via secure and private DNS lookup. Quad9 operates over 200 locations across more than 90 nations, blocking hundreds of millions of malware, phishing, and spyware events daily for millions of end users. Quad9 reduces harm in vulnerable regions, increases privacy against criminal or institutionalized interception of Internet data, and improves performance in under-served areas.

Indicators of Compromise (IOCs)

Phishing

luncdvod.xyz	Phishing	
ny-feed.rtbxnmlive.com	Phishing	

Banking Trojans

weiqeqwens.com	Banking Trojan	Gozi/Ursnif

RATs

wmail-endpoint.com	RAT	ViperSoftX
wmail-blog.com	RAT	ViperSoftX
wmail-chat.com	RAT	ViperSoftX
wmail-cdn.com	RAT	ViperSoftX
wmail-schnellvpn.com	RAT	ViperSoftX
fairu-endpoint.com	RAT	ViperSoftX
fairu-blog.com	RAT	ViperSoftX
fairu-chat.com	RAT	ViperSoftX
bideo-endpoint.com	RAT	ViperSoftX
bideo-blog.com	RAT	ViperSoftX
bideo-chat.com	RAT	ViperSoftX
privatproxy-endpoint.com	RAT	ViperSoftX
privatproxy-blog.com	RAT	ViperSoftX
privatproxy-cdn.com	RAT	ViperSoftX
ahoravideo-endpoint.com	RAT	ViperSoftX
ahoravideo-cdn.com	RAT	ViperSoftX
ahoravideo-chat.com	RAT	ViperSoftX
wmail-schnellvpn.xyz	RAT	ViperSoftX
fairu-blog.xyz	RAT	ViperSoftX
fairu-chat.xyz	RAT	ViperSoftX
fairu-cdn.xyz	RAT	ViperSoftX
bideo-chat.xyz	RAT	ViperSoftX
bideo-blog.xyz	RAT	ViperSoftX
bideo-cdn.xyz	RAT	ViperSoftX
bideo-schnellvpn.xyz	RAT	ViperSoftX
privatproxy-endpoint.xyz	RAT	ViperSoftX
privatproxy-chat.xyz	RAT	ViperSoftX
privatproxy-cdn.xyz	RAT	ViperSoftX

privatproxy-schnellvpn.xyz	RAT	ViperSoftX
ahoravideo-endpoint.xyz	RAT	ViperSoftX
ahoravideo-blog.xyz	RAT	ViperSoftX
ahoravideo-chat.xyz	RAT	ViperSoftX
ahoravideo-cdn.xyz	RAT	ViperSoftX

Stalkerware

wss.findmykids.org	Stalkerware	Kids Tracking Software