Trends May 2023:
Cyber Insights

Emilia Cebrat-Maslowski (Quad9 CTI)

Danielle Deibler (Quad9 CISO)

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 monthly 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 10 malicious domains visited by our users and blocked by Quad9 DNS. Additionally, the report presents top regional threats targeting Quad9 users

Methodology

Data were gathered during the month of April 2023. Due to the volume, Quad9 does not collect all the DNS requests. The analyzed samples were recorded daily, every hour, for 60 seconds. Improvement to this process is a work in progress.

Overview

In April 2023, we observed users targeted with diverse threat categories, including but not limited to Banking Trojans, Advanced Persistent Threat (APT) campaigns, DDoS, and Remote Access Trojan (RAT). This monthly report analyzes the top notable malicious domains blocked by Quad9 DNS and their associated threats.

For more detailed data on the specific threat categories and volumes of attempted access, please refer to the dedicated sections of this report.

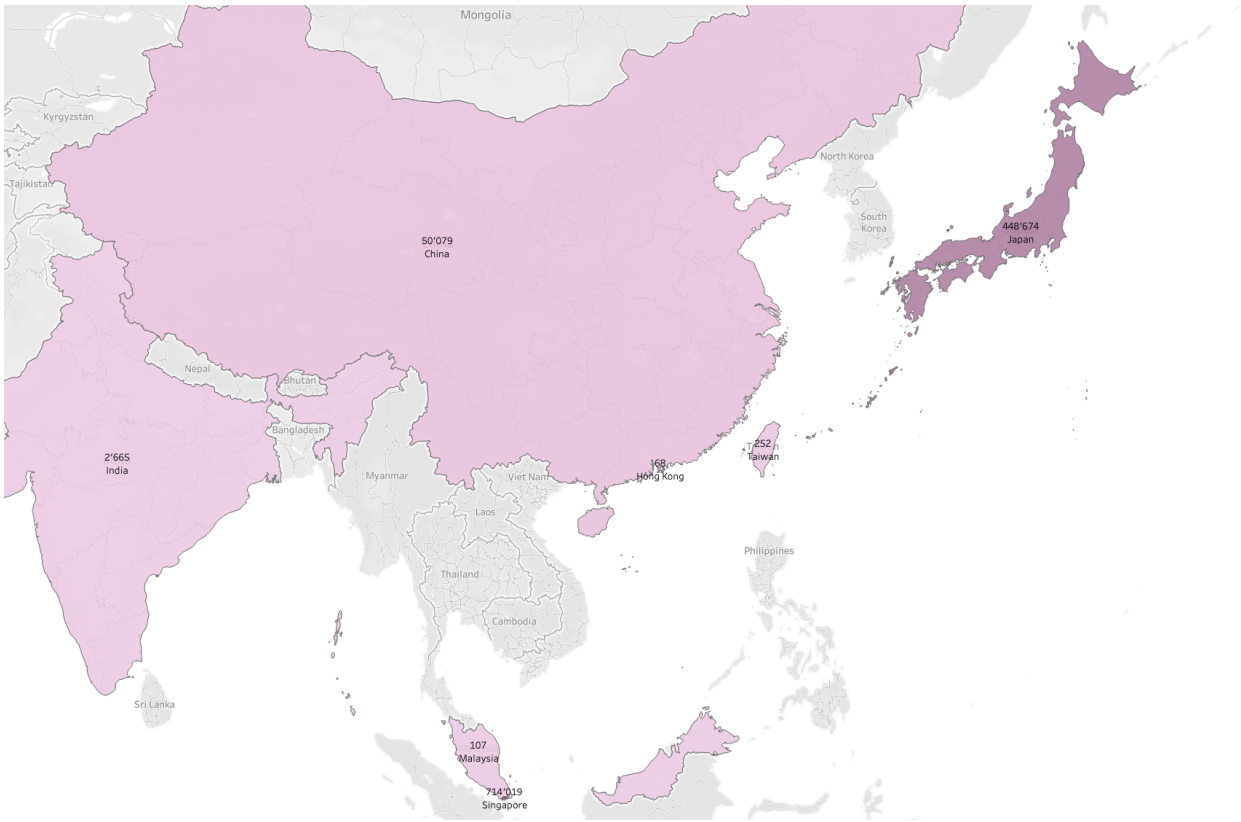
Victimology - Top Regional Threats

This month, we present our overall top threats with regional activity information for the first time. In April 2023, we observed users in three regions mainly targeted with DDoS, crypto-miners, and Banking Trojans.

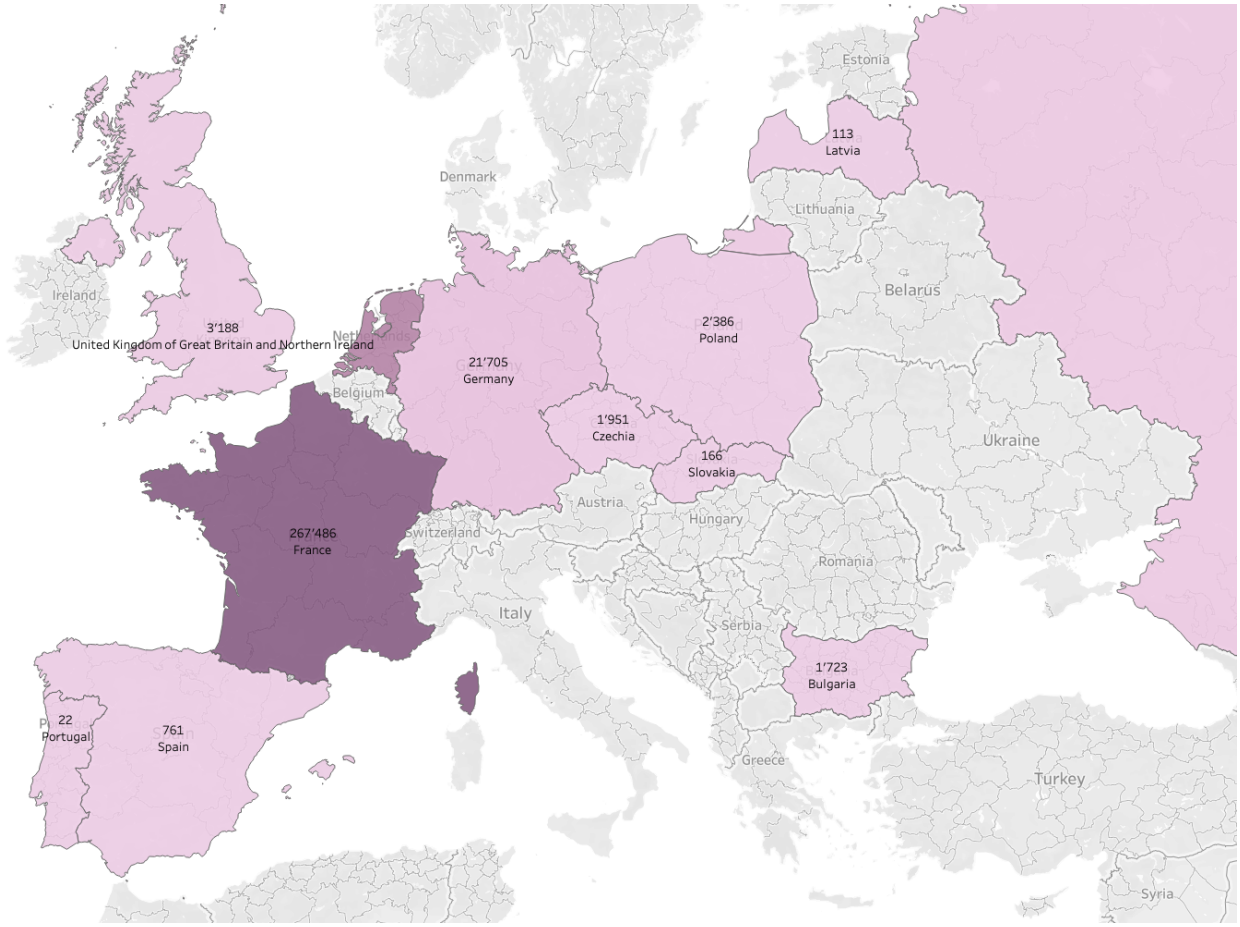
APAC & EMEA

The highest volume of queries initiated by users located in the APAC and EMEA regions was to the domain attributed to the Fodcha DDoS botnet. As we suspected, cybercriminals continue exploiting vulnerabilities for distributed denial-of-service (DDoS) operations which is confirmed by our data - the volume of access attempts was constant throughout the month of April. Also, attackers are still interested in supply chain vulnerabilities, which are difficult for users to identify and remediate.

In APAC, the most significant volume of DDoS domain queries was from users in Singapore and Japan.



In EMEA, the most impacted users come from France and the Netherlands.



AMERICAS

For users in the Americas region, the most significant threats in April were attributed to the crypto mining domains and Banking Trojans.

Crypto-currency miners use many resources to optimize the earning of virtual currency. For this reason, threat actors try to use other people's machines to do the mining for them. Coin miners can come from various sources from being installed by the users themselves to being dropped by a Trojan. According to the Quad9 telemetry data, the most impacted users are located in the US.

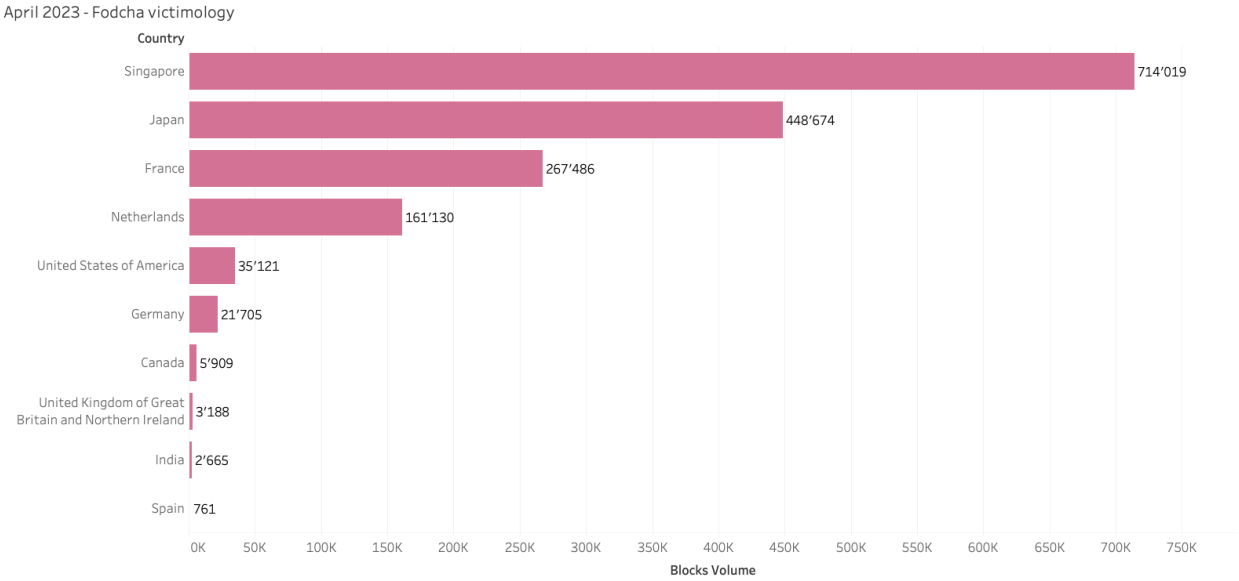
Ursnif/Gozi Banking Trojan was also among the threats targeting users in the Americas. Ursnif is a banking trojan spread through malspam with a Microsoft Office document attachment or

ZIP file. Ursnif collects victim information from cookies, login pages, and web forms. The most significant volume of queries to the Banking Trojan domain was from US users.

Geography for the coin miners and Banking Trojan threats:

DDoS Comeback

In April, the top threat targeting Quad9 users globally were attributed to DDoS. The domain which recorded the highest volume of DDoS traffic was attributed to Fodcha Command and Control (C2) server. As mentioned earlier, the most targeted regions were APAC and EMEA. The detailed geographies are presented below.



PixPirate - Brazilian Banking Trojan

Another top threat targeting Quad9 users globally was PixPirate Android malware. PixPirate is a new mobile malware targeting LATAM countries, specifically Brazil, which can be confirmed by Quad9 telemetry data on the map below. The primary goal of this malware is to steal sensitive information and defraud users that regularly use Pix platform[1]. PixPirate hides its malicious intent with familiar names and icons, posing as a legitimate application to the victims.

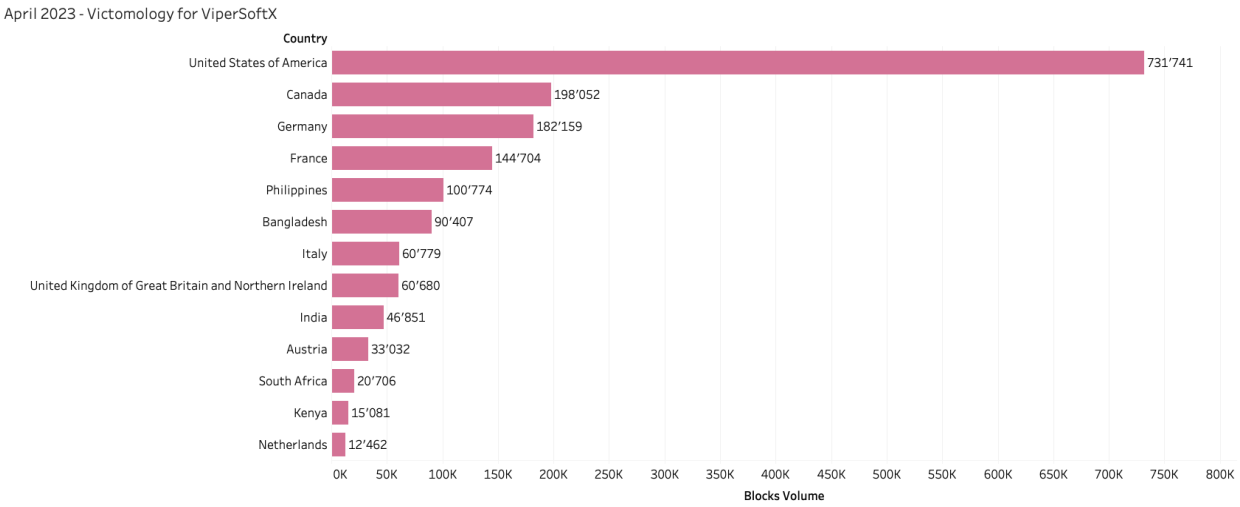
[1] https://www.cleafy.com/cleafy-labs/pixpirate-a-new-brazilian-banking-trojan

ViperSoftX - Java Script Threat

ViperSoftX is a multi-stage cryptocurrency stealer spread within torrents and file-sharing sites. The malware was initially observed in the early 2020s, but it has grown extensively, and our observations show it has been actively exploited recently. ViperSoftX is Windows malware and deploys a Google Chrome extension named 'VenomSoftX'. Quad9 observed multiple domains generated using DGA, which threat researchers also reported[2].

ViperSoftX most impacted users in the US, Canada, and Germany.

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



Dragon Breath APT - DLL Side-Loading

One of the top threats in April 2023 was attributed to the Dragon Breath APT campaign. The group has evolved its attacks, using a double-clean-app technique and DLL side-loading to target the gambling and gaming industry. The attackers have enticed victims with trojanized versions of popular applications. Additionally, the group has added new layers of complexity to its attacks with the double DLL sideloading tactic to evade detection[3]. Quad9 users who were the most targeted by this campaign were in Indonesia, Iran, Japan, and the US.

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 to allow everyone to be less vulnerable to risk and more effective in their daily online interactions - even in the face of growing cyber-attacks.

3 https://www.hivepro.com/wp-content/uploads/2023/05/Dragon-Breath-APT-Evolves-with-Double-DLL-Sideloading_TA2023216.pdf

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. Quad9 is a collaboration with Packet Clearing House (PCH), Global Cyber Alliance, and IBM.

Indicators of Compromise (IOCs)

DDoS

fridgexperts.cc	DDoS	Fodcha

Banking Trojans

weiqeqwens[.]com	Banking Trojan	Gozi/Ursnif
orange.applebalanyou.com	Banking Trojan	PixPirate

RAT (ViperSoftX)

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	VipeSoftX

Others

potatouu.com	DLL Side-Loading	VipeSoftX
2.potatouu.com	DLL Side-Loading	Dragon Breath APT