Trends April 2023:
Cyber Insights

Emilia Cebrat-Maslowski (Quad9 CTI)

Danielle Deibler (Quad9 CISO)

About This Report

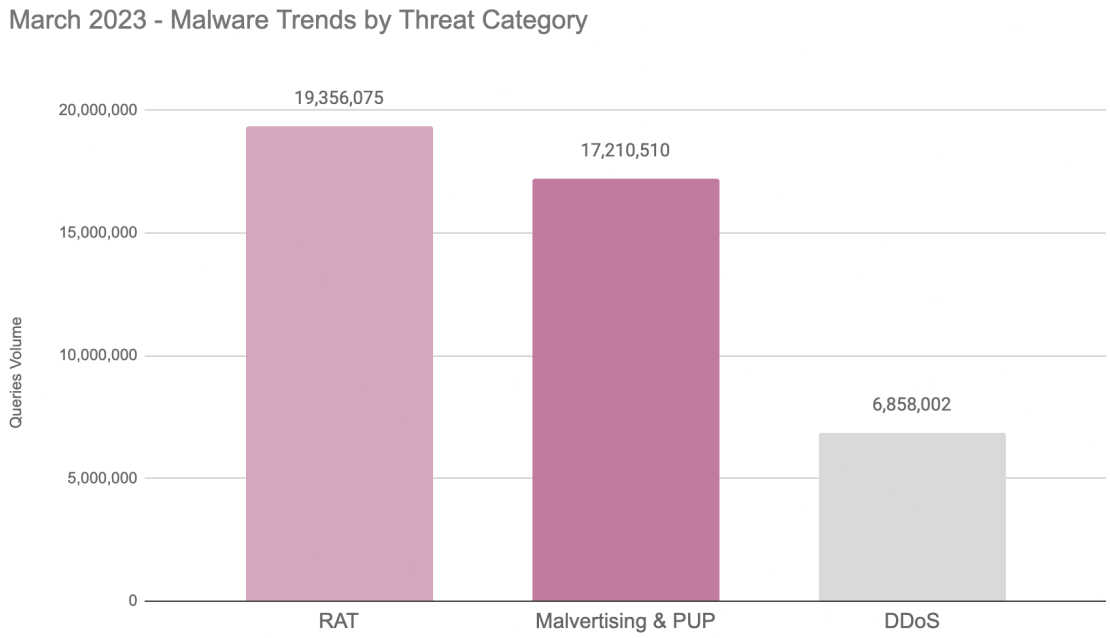
To protect our users, Quad9 blocks DNS lookups of malicious host names from an up-to-the-minute list of threats. This blocking action protects your computer, mobile device, or IoT systems against a wide range of threats, such as malware, phishing, spyware, and botnets, and it can improve performance and guarantee 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.

Methodology

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

Overview

In March 2023, we observed users targeted with diverse threat categories, including but not limited to malvertising, Potentially Unwanted Programs (PUPs), DDoS, and Remote Access Trojans (RAT). This monthly report analyzes the top notable malicious domains blocked by Quad9 DNS and their associated threats.

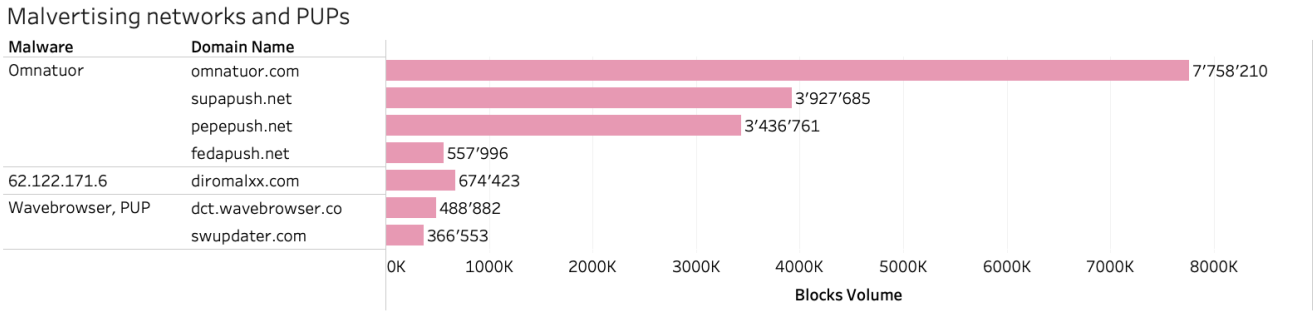


For more detailed data on the specific threat categories and volumes of attempted access, please refer to the dedicated sections of this report.

Malvertising and PUPs

In March, we observed a high volume of users' queries to the following malvertising networks and domains attributed to Potentially Unwanted Programs (PUPs):

- Omnatour Malvertising Network
- 62.122.171.6 Malvertising Network
- Wave Browser



Omnatour Malvertising Network

In the recent months, we have seen an increasing number of queries to the domains related to Omnatour malvertising network. All of the top blocked domains belonging to the Omnatour network are hosted on the IP range 139.45.192.0/19, which belongs to AS9002 - RETN-AS, GB[1]. The Omnatour campaign compromises vulnerable WordPress sites through embedded malicious JavaScript or PHP code. The code then redirects users to view and click malvertisements via pop-ups and push notifications[2].

[1] https://urlscan.io/ip/139.45.197.253

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

62.122.171.6 Malvertising Network

The rising malvertising threat. Among the top blocked domains, we identified the second malvertising network, hosted on the IP address 62.122.171.6[3] belonging to AS50245 - SERVEREL-AS in the U.S. during our research. In February, we identified eight domains of this malvertising network among the top blocked domains. This month, only one domain from this network was highly active - diromalxx[.]com

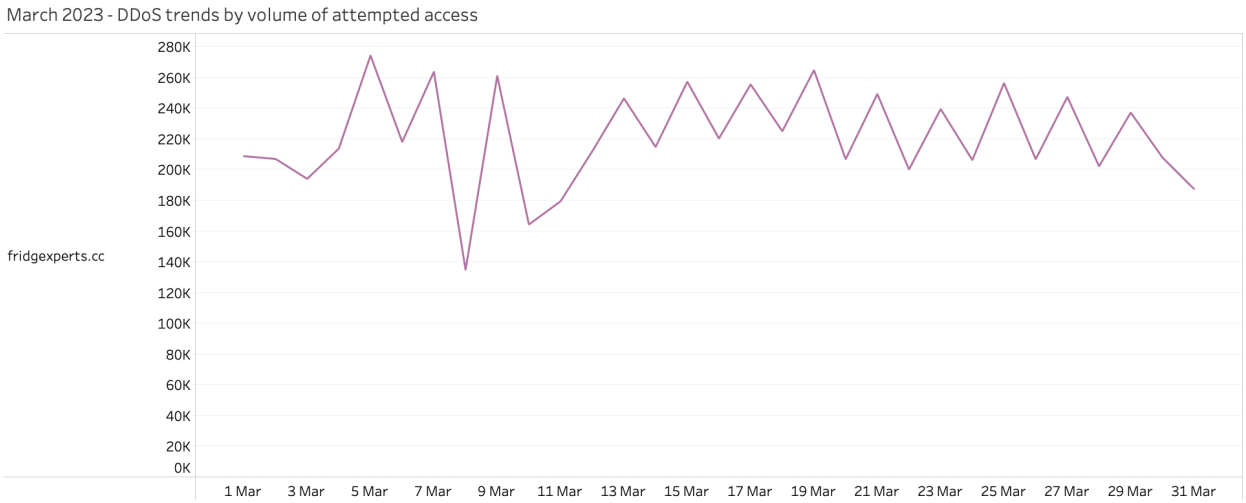
Wave Browser

The Wave browser is a PUP that installs what looks just like Google Chrome. However, it's entirely different software designed to display unwanted ads. While the Wave browser is not a virus or malware, it can make users' computers vulnerable to malicious software. The browser can also track users' data and make it accessible to cybercriminals[4]. Additionally, the browser can make unauthorized changes on users' computers.

Fodcha Botnet Activity

Again, as in February, in March, we observed a lower volume of queries to the domains attributed to DDoS. The domain which recorded the highest volume of DDoS traffic was attributed to Fodcha Command and Control (C2) server. Fodcha is a relatively new DDoS botnet discovered by the Netlab360 team attributed to Chinese Threat Actors[5]. In 2022 the malware abused CVE-2021-35394 (remote code execution vulnerability in Realtek Jungle SDK)[6]. In 2023, we suspect that we will continue to observe cybercriminals exploiting this vulnerability for distributed denial-of-service (DDoS) operations which is confirmed by our data - the volume of access attempts was constant throughout the month of March. **Also, attackers will still be interested in supply chain vulnerabilities, which are difficult for the users to identify and remediate.**

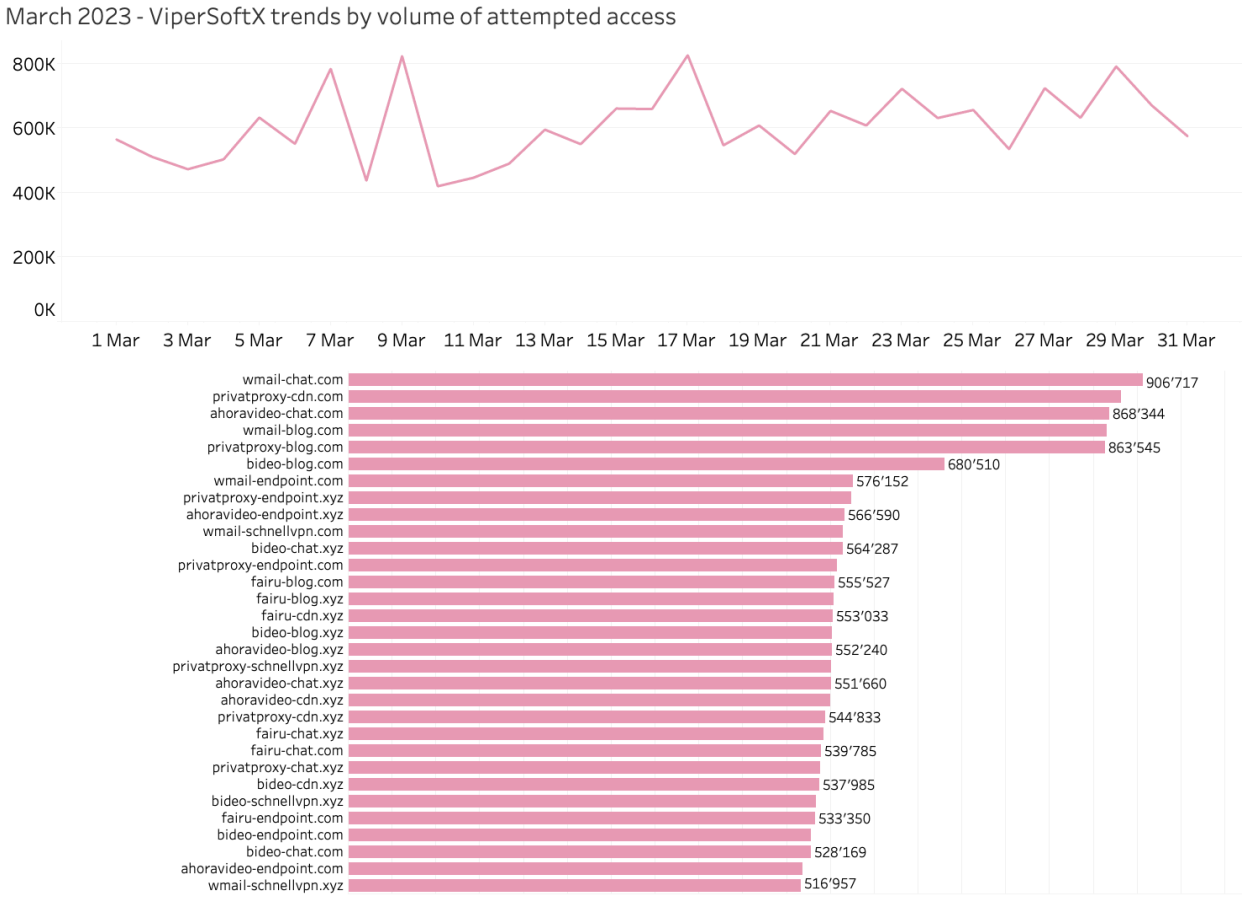
[3] https://urlscan.io/search/#page.ip:%2262.122.171.6%22
[4] https://www.technewstoday.com/wave-browser/
[5] https://blog.netlab.360.com/fodcha-a-new-ddos-botnet/
[6] https://unit42.paloaltonetworks.com/realtek-sdk-vulnerability/



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 were also reported by threat researchers[7].

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



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.

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 currently 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)

Malvertising & PUPs

Domain	Threat Category	Details
diromalxx.com	Malvertising	62.122.171.6

omnatuor.com	Malvertising	Omnatuor
pepepush.net	Malvertising	Omnatuor
supapush.net	Malvertising	Omnatuor
fedapush.net	Malvertising	Omnatuor

dct.wavebrowser.co	PUP	Wave Browser
swupdater.com	PUP	Wave Browser

DDoS

fridgexperts.cc	DDoS	Fodcha

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