Trends March 2023: Cyber Insights

Emilia Cebrat-Maslowski (Quad9 CTI)

Danielle Deibler (Quad9 CISO)

About This Report

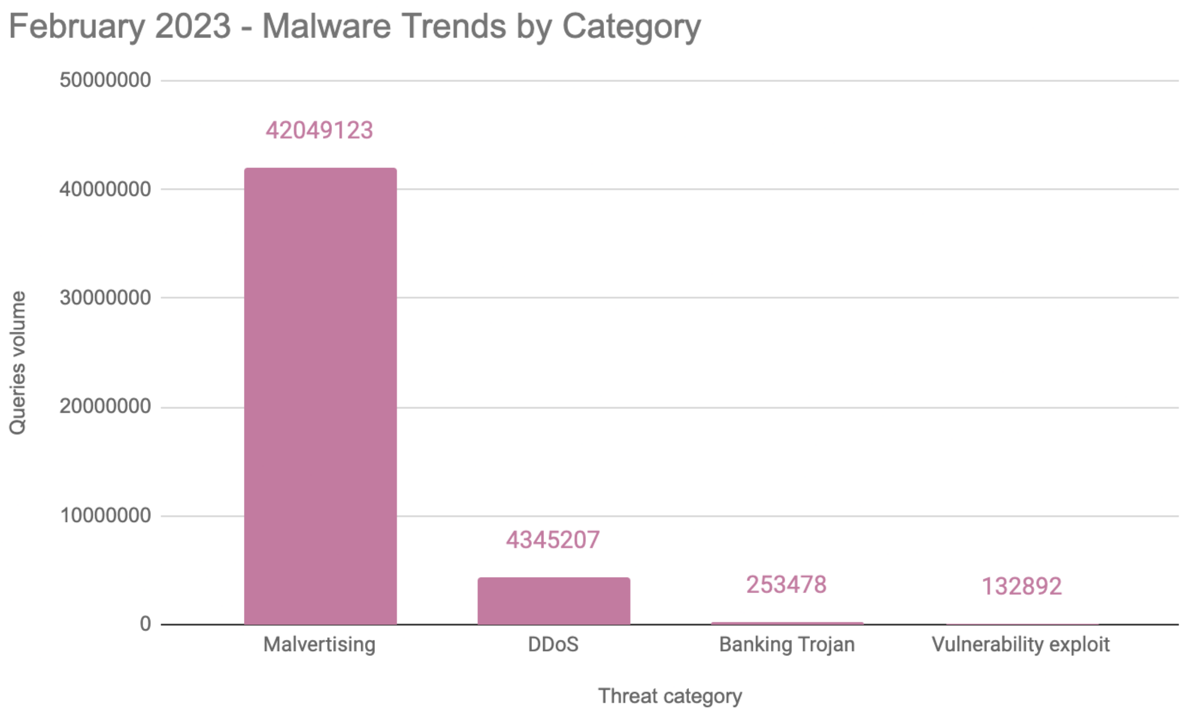
To protect our users, Quad9 blocks DNS lookups of malicious host names from an up-to-the-minute list of threats. This blocking action protects your computer, mobile device, or IoT systems against various threats such as malware, phishing, spyware, and botnets. It can improve performance and guarantee privacy. This monthly report provides insights on the threats blocked by Quad9 DNS. The information 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 February 2023. Due to the volume of DNS requests, Quad9 does not collect all the DNS requests. This month we changed the methodology by recording the analyzed samples daily, every hour for 60 seconds. Improvement of this process is a work in progress.

Overview

In February 2023, we observed users targeted with diverse threat categories, including but not limited to malvertising, Banking Trojans, vulnerability exploits, and DDoS. 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.

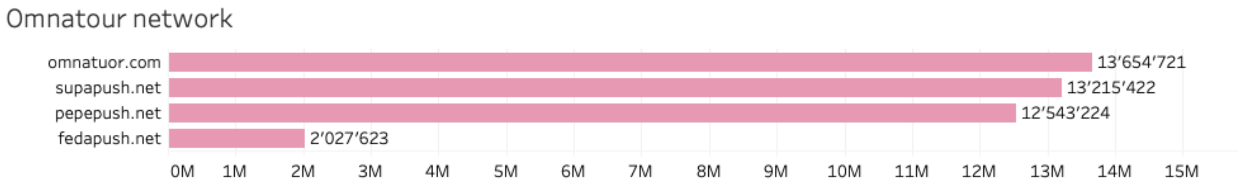
Two Active Malvertising Networks

In February, we observed a high volume of users' queries to two malvertising networks:

- Omnatour Malvertising Network
- 62.122.171.6 Malvertising Network

Omnatour Malvertising Network

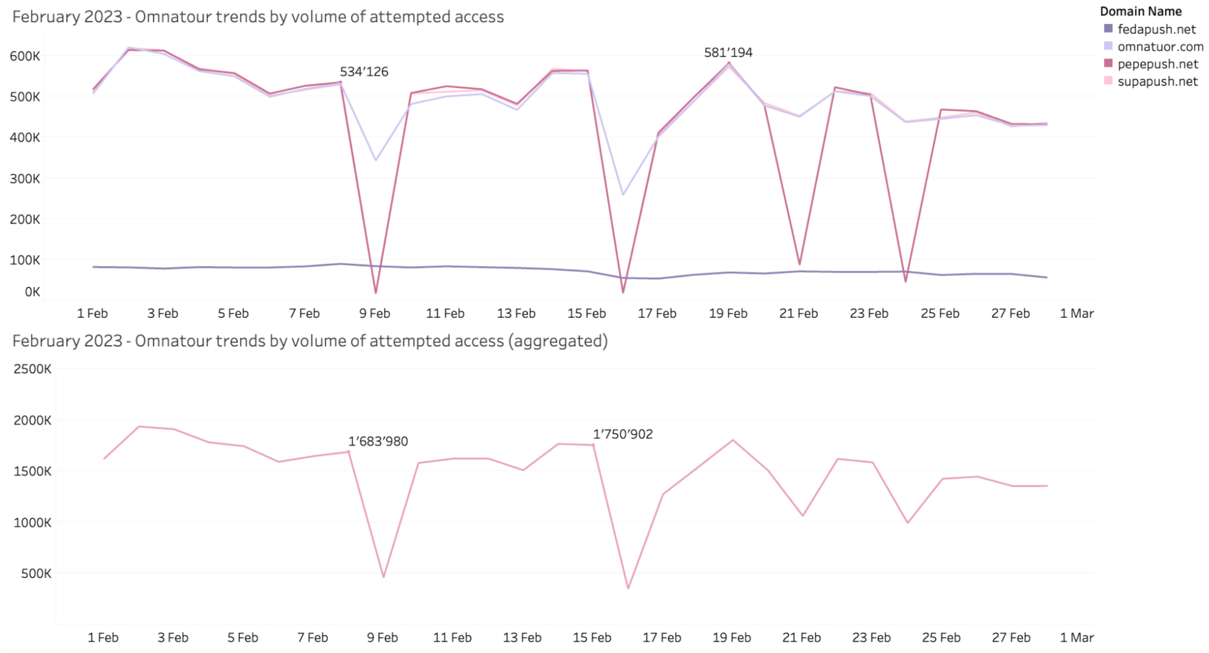
In recent months, we have seen increasing queries to the domains related to the Omnatour malvertising network. The IP range 139.45.192.0/19 belongs to AS9002 - RETN-AS, GB[1] and hosts all of the top blocked domains belonging to the Omnatour. In February, we recorded 41.4 million blocked queries to this malvertising network, and this month we only identified four domains belonging to Omnatour Malvertising Network.



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

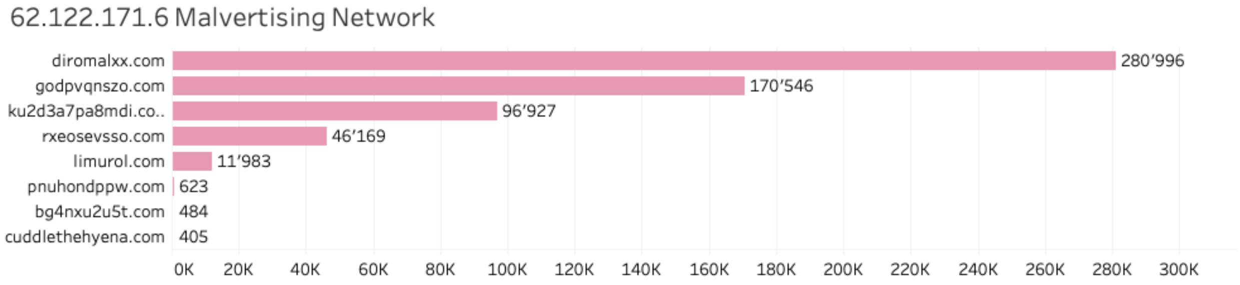
[2] https://blogs.infoblox.com/cyber-threat-intelligence/cyber-threat-advisory/vast-malvertising-network-hijacks-browser-settings-to-spread-riskware/



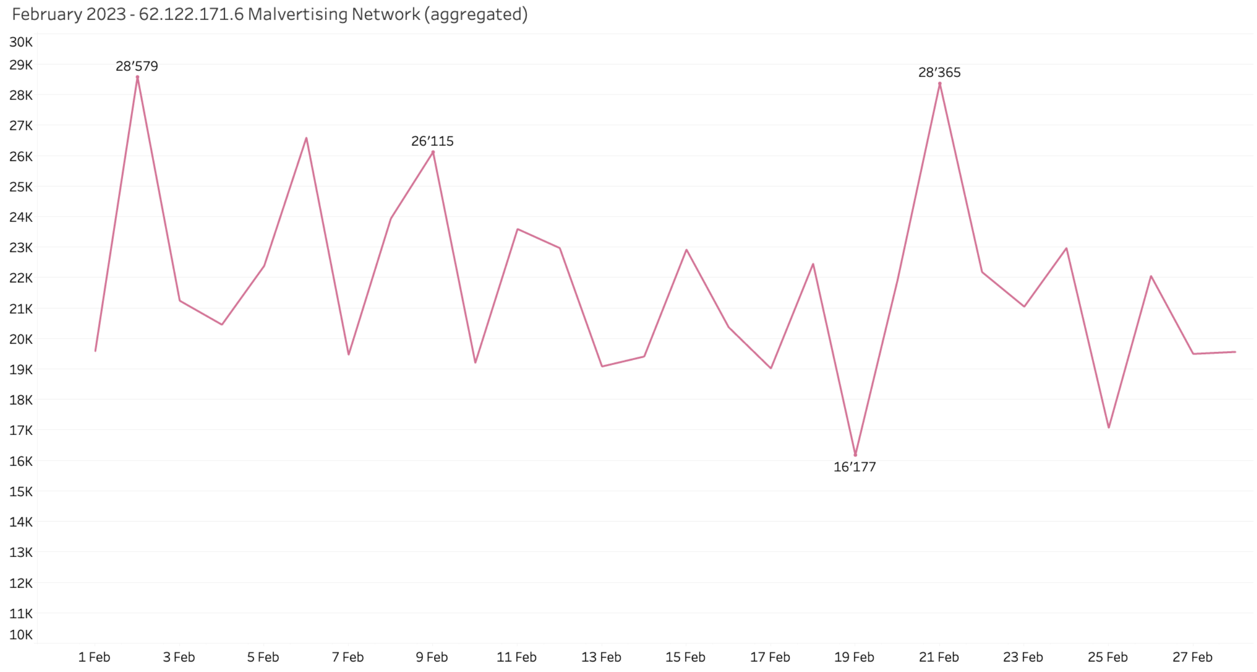
62.122.171.6 Malvertising Network

The malvertising threat is on the rise. 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. We identified eight domains for this malvertising network among the top blocked domains.

[3] https://urlscan.io/search/#page.ip:%2262.122.171.6%22



In February, we logged more than 600.000 queries to the domains related to this malvertising network:

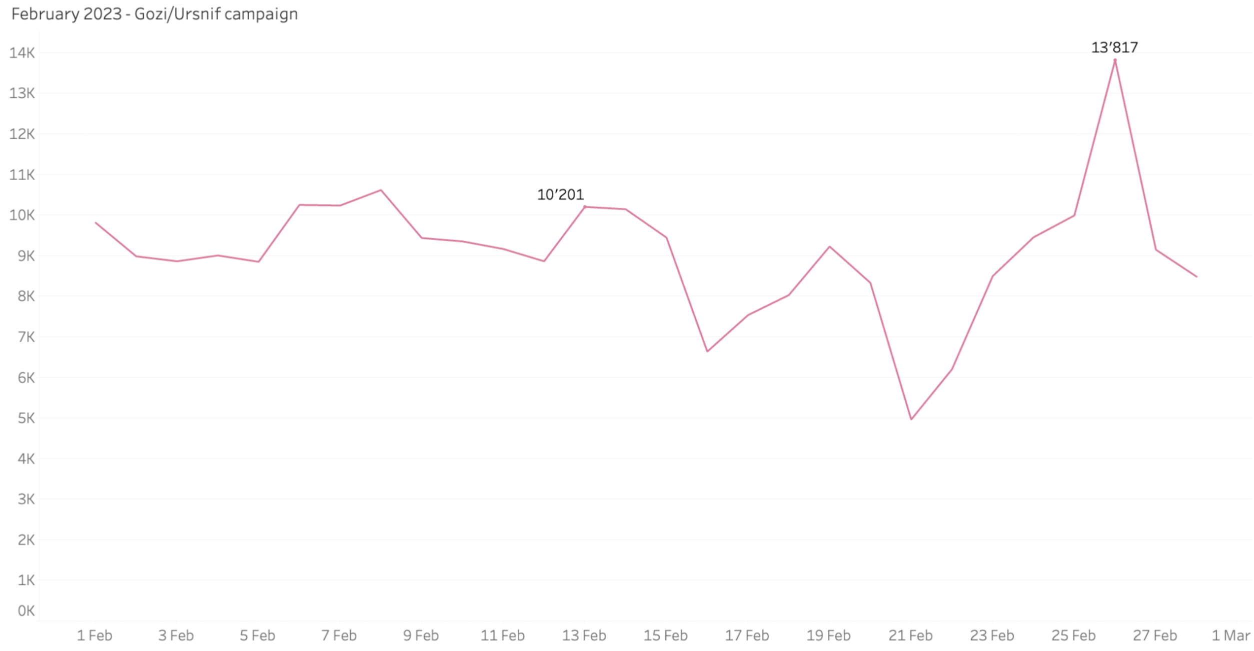


Fodcha Botnet Activity

In contrast to previous months, we observed a lower volume of queries to the domains attributed to DDoS in February. 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[4]. In 2022 the malware abused CVE-2021-35394 (remote code execution vulnerability in Realtek Jungle SDK)[5]. 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 February. **Also, attackers will still be interested in supply chain vulnerabilities, which are difficult for the users to identify and remediate.**

Gozi, aka Ursnif campaign

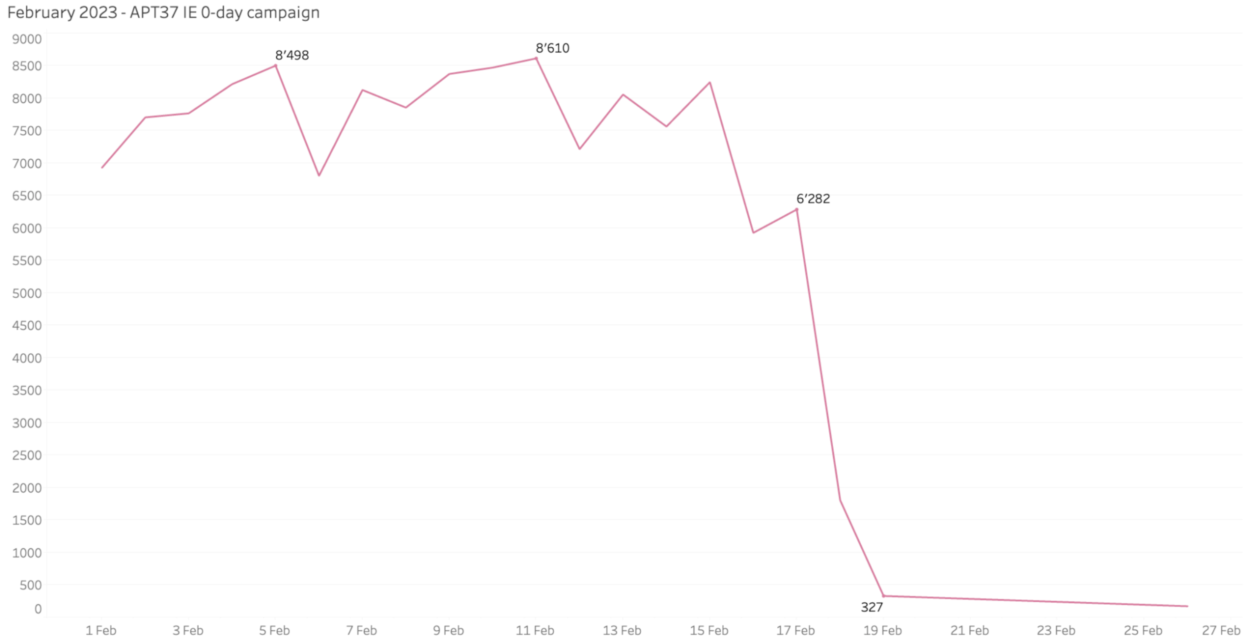
We first observed queries to the domain attributed to the Gozi's campaign in December. At that time, we saw a high activity level for only a few days.In February, we saw many attempts to weiqeqwens[.]com, domain attributed to Gozi's campaigns throughout the whole month.Ursnif is a banking trojan spread through malspam with a Microsoft Office document attached or a ZIP file. Ursnif collects victim information from cookies, login pages, and web forms.



[4] https://blog.netlab.360.com/fodcha-a-new-ddos-botnet/
[5] https://unit42.paloaltonetworks.com/realtek-sdk-vulnerability/

APT37 Leveraging IE 0-Day to Target Users

The last notable active campaign we observed at Quad9 in February is the APT37 campaign distributing Word Documents disguised as standard MS Office URLs. APT37 is a North Korean state-sponsored cyber espionage group targeting victims primarily in South Korea. In the most recent campaign, not for the first time, Threat Actors have used Internet Explorer 0-day exploits to target users. The abused 0-day vulnerability is in the JScript engine of Internet Explorer[6]. Also, the notable point is that the URL used in the fake Word document (ms-offices[.]com) cleverly disguises itself to resemble the standard URL closely. Researchers could not determine the final payload of the campaign at the time of this report..



Conclusions

Over the years, malicious actors have gained cheaper and easier access to attack Internet users. Quad9's mission is to improve the security and stability of the Internet, allowing everyone to be

[6] https://blog.google/threat-analysis-group/internet-explorer-0-day-exploited-by-north-korean-actor-apt37/

less vulnerable to risks and more effective in their daily online interactions - even in the face of a growing number of cyber attacks

By preventing connections to malicious sites, Quad9 eliminates exposure to risks before victims see fraudulent websites or download malware. 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 180 locations across more than 90 nations, blocking hundreds of millions of malware, phishing, and spyware events each day 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

Domain	Threat Category	Details
diromalxx.com	Malvertising	62.122.171.6
godpvqnszo.com	Malvertising	62.122.171.6
ku2d3a7pa8mdi.com	Malvertising	62.122.171.6
limurol.com	Malvertising	62.122.171.6
rxeosevsso.com	Malvertising	62.122.171.6
pnuhondppw.com	Malvertising	62.122.171.6
bg4nxu2u5t.com	Malvertising	62.122.171.6
cuddlethehyena.com	Malvertising	62.122.171.6

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

DDoS

fridgexperts.cc	DDoS	Fodcha

Banking Trojans

weiqeqwens.com	Banking Trojan	Ursnif/Gozi

Vulnerability exploits

ms-offices.com	Vulnerability exploit	APT37