Trends February 2023: Cyber Insights

Emilia Cebrat-Maslowski (Quad9 CTI)

Danielle Deibler (Quad9 CISO)

About This Report

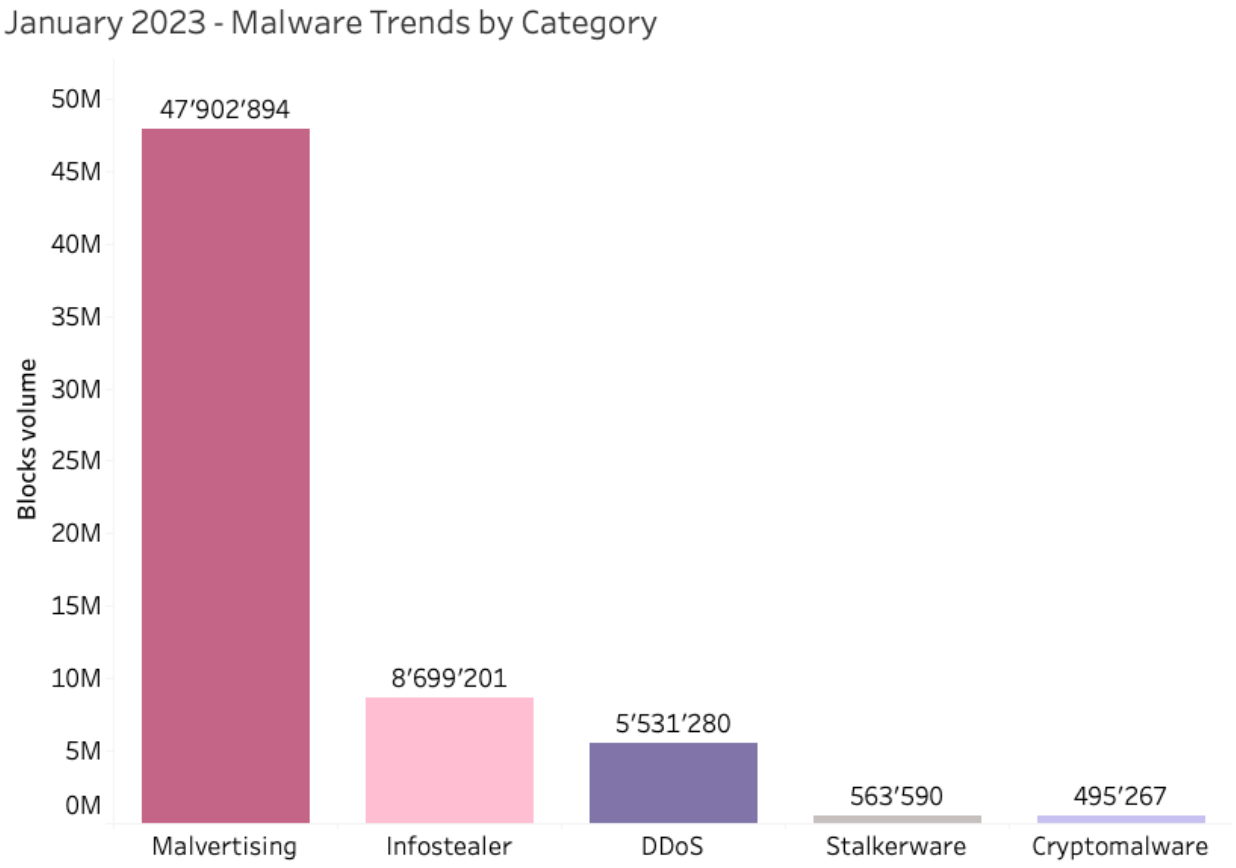
To protect our users, Quad9 blocks DNS lookups of malicious host names from an up-to-the-minute list of threats. This blocking action protects your computer, mobile device, or IoT systems against a wide range of threats such as malware, phishing, spyware, and botnets, and it can improve performance in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

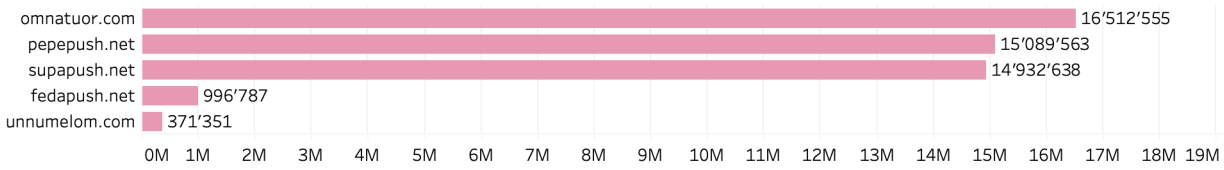
In January 2023, we observed users targeted with diverse threat categories, including but not limited to malvertising, information stealers and DDoS. This monthly report analyzes the top notable malicious domains blocked by Quad9 DNS and their associated threats.



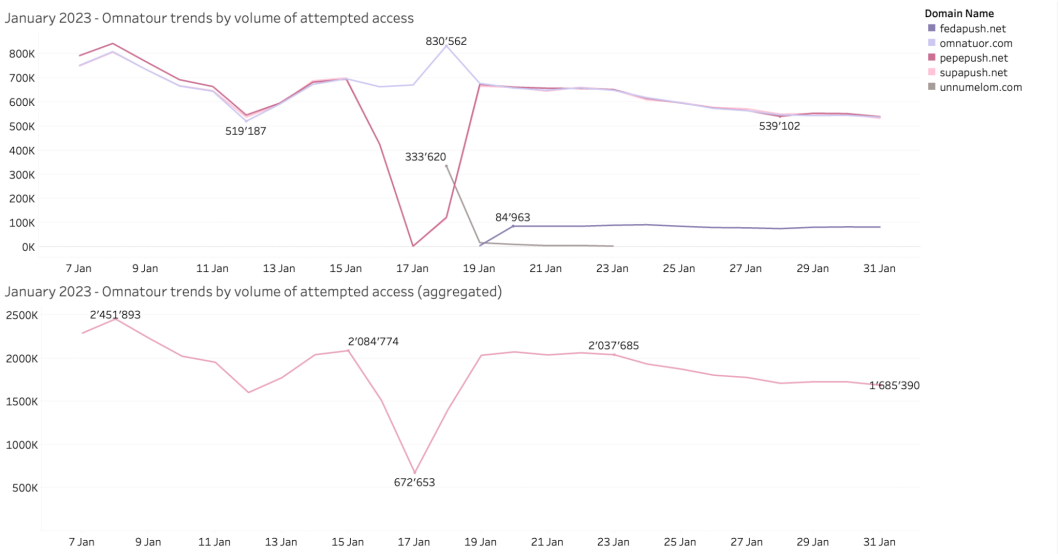
For more detailed data on the specific threat categories and volumes of attempted access, please refer to the dedicated sections of this report.

Omnatuor Malvertising Network

In the recent months, we have seen an increasing number of queries to the domains related to Omnatour malvertising network. In January 2023, we observed over 16.5 million resolved queries to omnatuor[.]com domain. 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].

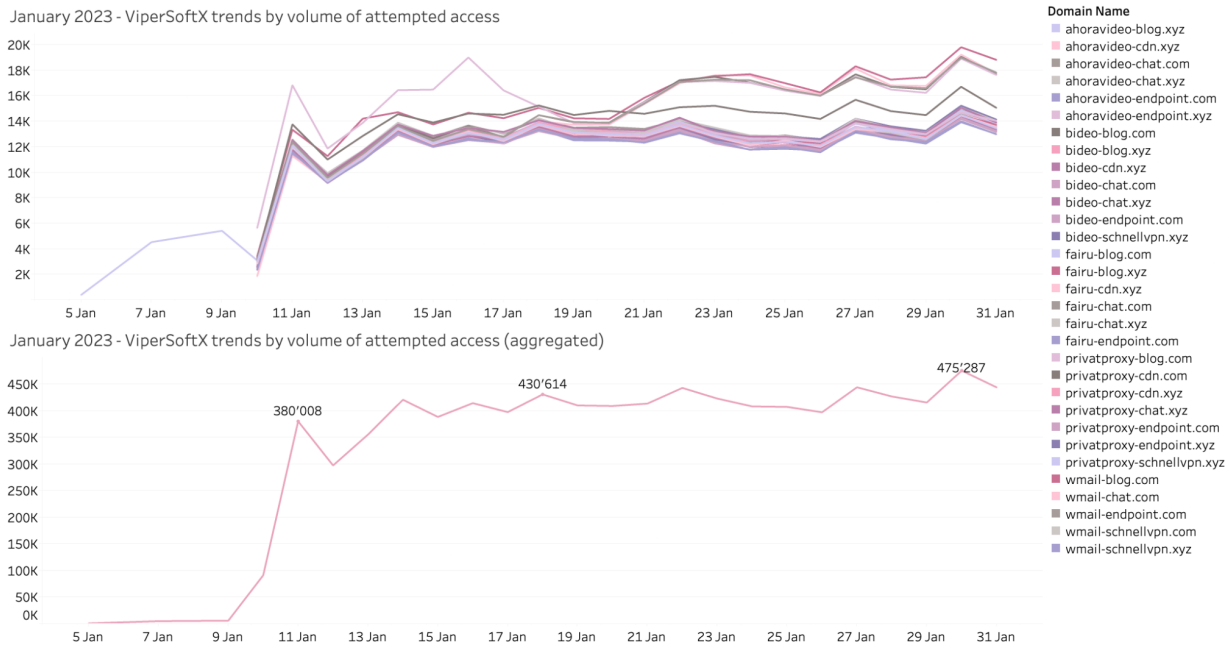


[1] https://urlscan.io/ip/139.45.197.253

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

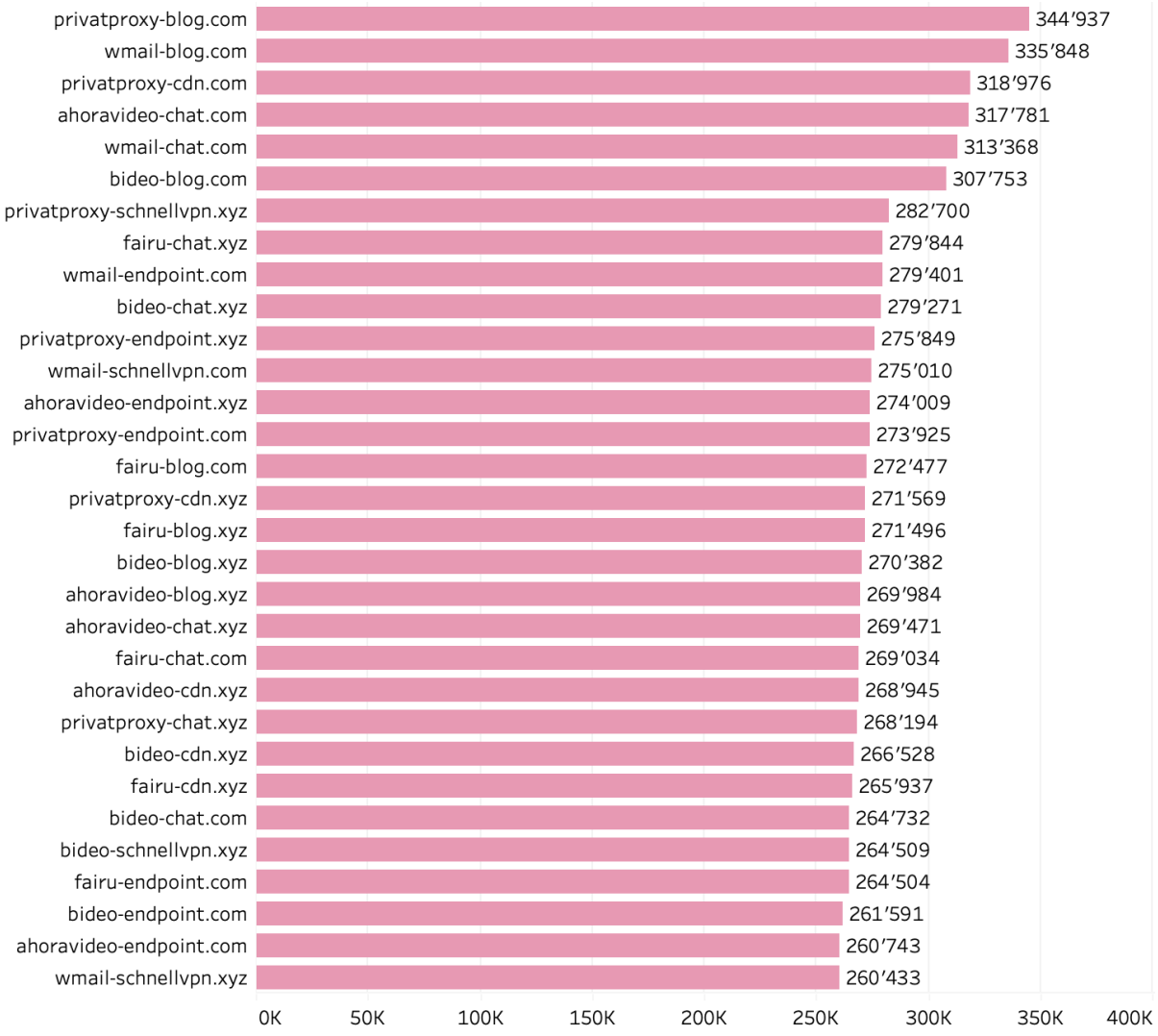
ViperSoftX - Java Script Threat

ViperSoftX is a multi-stage cryptocurrency stealer which is spread within torrents and file sharing 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 generated using DGA which were also reported by threat researchers[3]. Among top 100 domains blocked by Quad9, 31 domains were referenced by ViperSoftX's dropper.



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

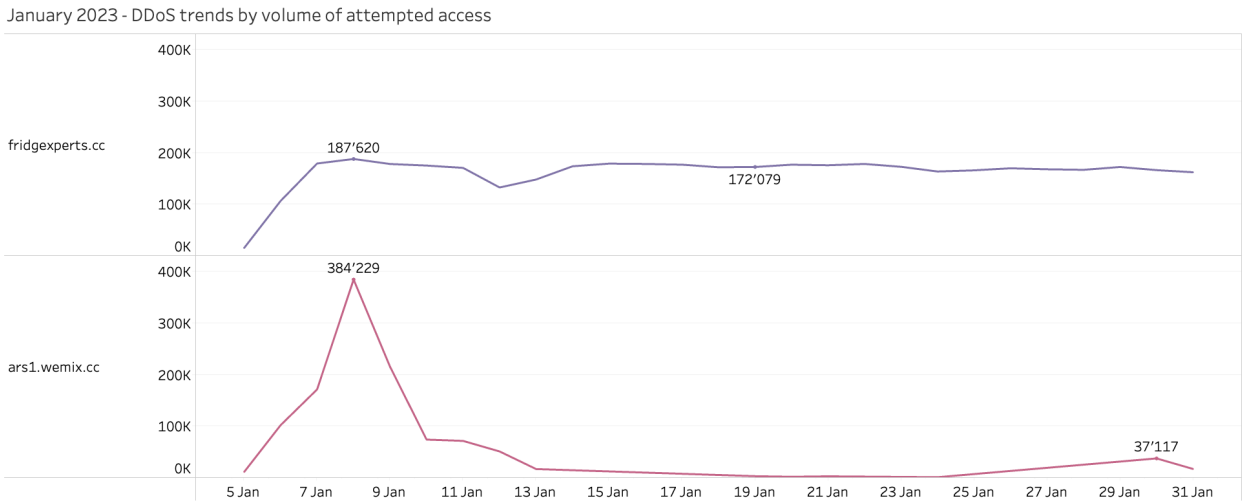
According to our observations, ViperSoftX campaigns were more active in January when compared to previous months. Volume of attempted access to the ViperSoftX-related domains:



Supply chain exploited in DDoS attacks

As depicted in the figure above, among the top 10 domains blocked by Quad9, we observed the following malware families attributed to DDoS:

1) **Fodcha** - The high volume of users attempted to access fridgexperts[.]cc, which we attribute 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 January. **Also, attackers will be still interested in supply chain vulnerabilities, which are difficult for the users to identify and remediate.**
2) **Chaos** - Among the top three accessed domains we observed ars1.wemix[.]cc. This domain is associated with Chaos malware, predecessor of Kaiji malware[6][7][8]. Chaos is a multifunctional malware written in the Go programming language that has been spotted in the wild, targeting both Windows and Linux systems and Internet of Things (IoT) devices. The last notable reported attack was observed in September 2022. The bot launched DDoS attacks against over 20 organizations' domains or IPs across different sectors. Although the volume of attempted access for DDoS-related domains was lower in January, we have seen a big spike in attempts in the beginning of the month for Chaos malware.

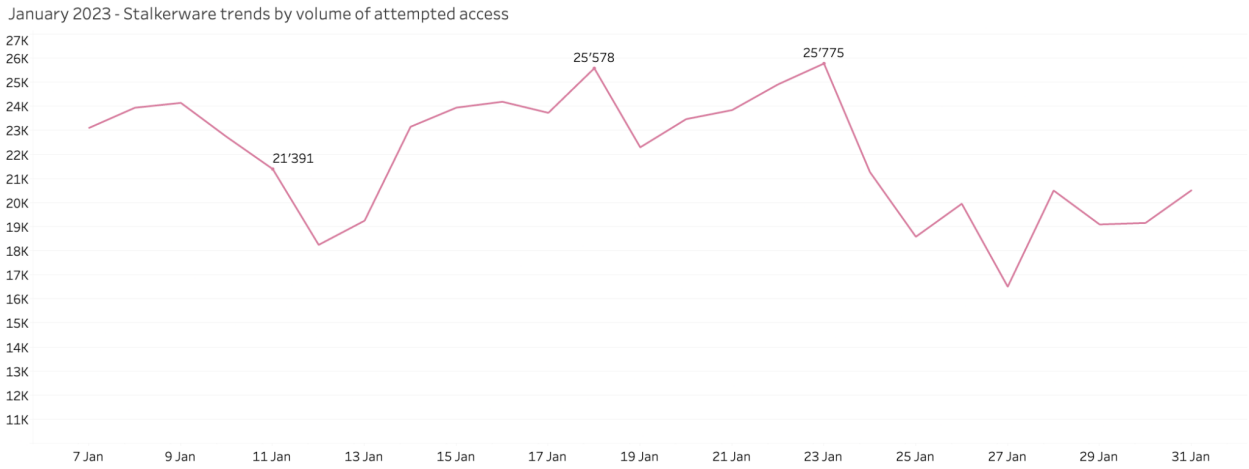


[4] https://blog.netlab.360.com/fodcha-a-new-ddos-botnet/
[5] https://unit42.paloaltonetworks.com/realtek-sdk-vulnerability/
[6] https://blog.lumen.com/chaos-is-a-go-based-swiss-army-knife-of-malware/
[7] https://therecord.media/botnet-of-devices-infected-with-chaos-malware-rapidly-growing-across-europe/
[8] https://www.infosecurity-magazine.com/news/chaos-new-golang-botnet/

Stalkerware Apps Are Proliferating

Stalkerware applications are spyware that record user's conversations, location and everything the user types, all while camouflaged as a legitimate application such as a calculator or a calendar. Based on our Open Source Research (OSINT) research, the programs communicating with ixhtb.s9gxw8[.]com[9] 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.

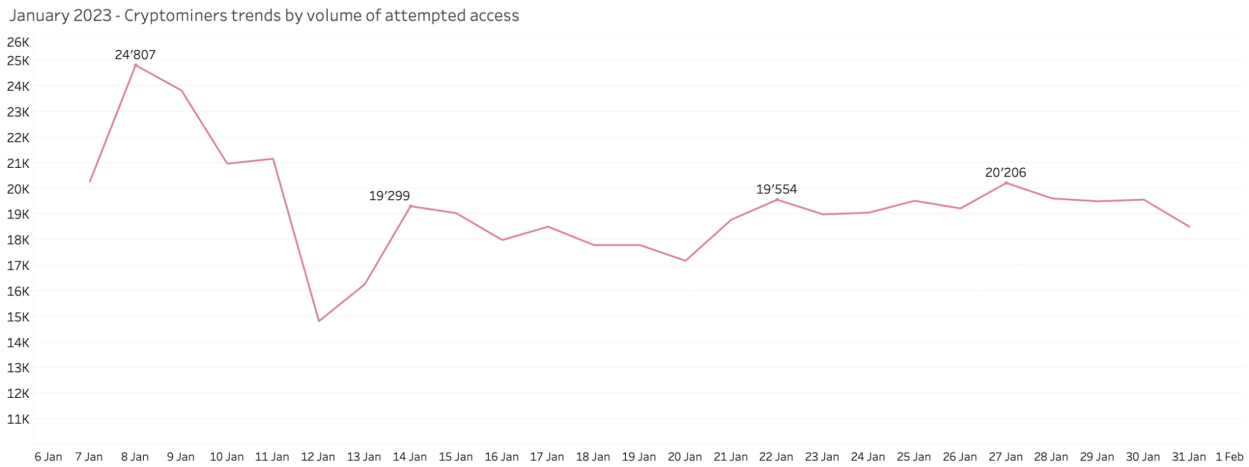
We observe constant number of attempted access throughout January suggesting that many Quad9 users have unwanted programs running on their Android devices:



[9] https://raw.githubusercontent.com/AssoEchap/stalkerware-indicators/master/generated/hosts

Malicious crypto mining is still popular

Although cryptocurrency prices are dropping, malicious mining is still popular among cybercriminals. Among the top domains blocked for Quad9 users, was ip.3322[.]net domains related to the XMRig malware[10] which was mentioned in the December 2022 Quad9 report. XMRig is an open-source CPU mining software used to mine the Monero cryptocurrency and according to the external reports was among top 3 most prevalent malware families with a global impact of 3% of worldwide organizations in December 2022[11].



Conclusions

Over the years, it has become easier and cheaper for the 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 risks and more effective in their daily online interactions - even in the face of growing number of cyber attacks.

By preventing connections to malicious sites, Quad9 eliminates exposure to risks before they are even downloaded to computers or before a victim can see the fraudulent website. The

10 https://www.virustotal.com/gui/file/f7a8d3fb89711f208f281c267ed8dd647cda207ecb514d37892b56a0ddafbe9a/details

11 https://www.checkpoint.com/press-releases/december-2022s-most-wanted-malware-glupteba-entering-top-ten-and-qbot-in-first-place/

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 cyber protection services to the emerging world via secure and private DNS. Quad9 currently operates over 200 locations across more than 90 nations, blocking hundreds of millions of malware, phishing, and spyware events each day for hundreds of millions of end users. Quad9 reduces harm in vulnerable regions, increases privacy against criminal or institutionalized interception of Internet data, and improves performance in vulnerable communities.