Trends January 2023:
Cyber Insights

Emilia Cebrat-Maslowski (Quad9 CTI)

Danielle Deibler (Quad9 CISO)

About This Report

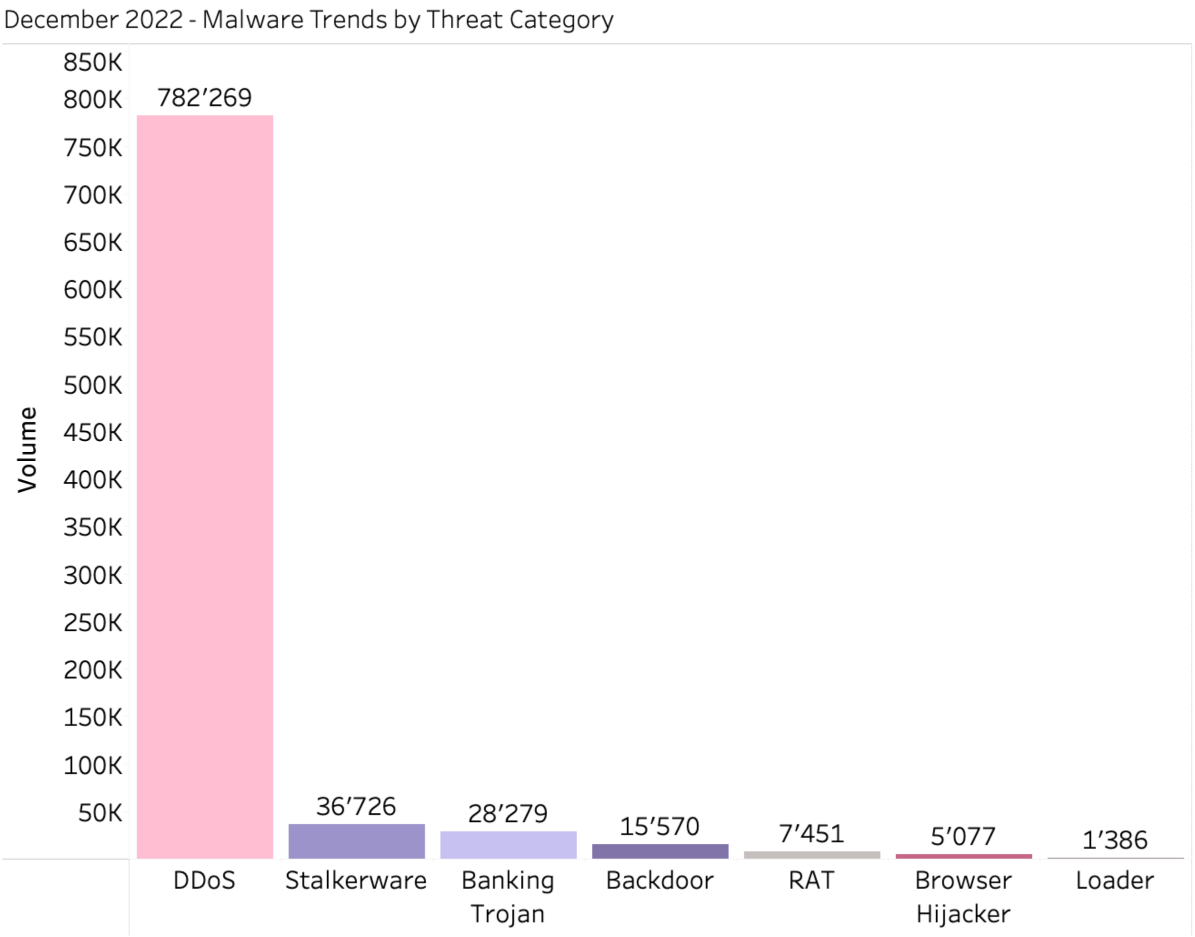
To protect our users, Quad9 blocks DNS lookups of malicious host names from an up-to-the-minute list of threats. This blocking action protects your computer, mobile device, or IoT systems against a wide range of threats such as malware, phishing, spyware, and botnets, and it can improve performance in 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 December 2022. Due to the volume of DNS requests, Quad9 does not collect all the DNS requests. Thus, analyzed samples were recorded two times a day for 60 seconds. Improvement of this process is a work in progress.

Overview

In December 2022, we observed users targeted with diverse threat categories, including but not limited to Stalkerware, DDoS, Backdoors, Loaders and Banking Trojans. This monthly report analyzes the top 10 notable malicious domains blocked by Quad9 DNS and their associated threats.



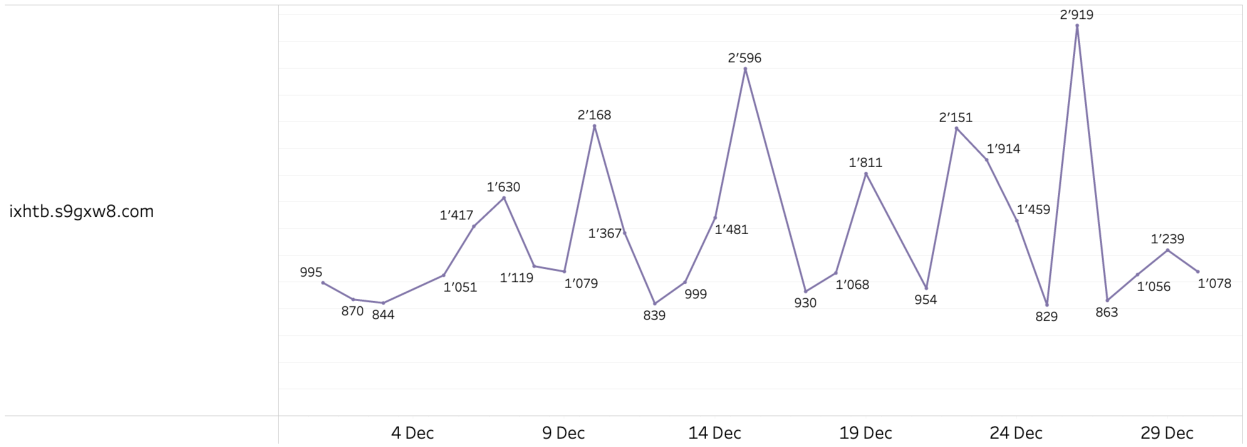
For more detailed data on the specific threat categories and volumes of attempted access, please refer to the dedicated sections of this report.

Stalkerware Apps Are Proliferating

This is a new threat category which Quad9 did not report in the past report. 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.

The domain with a high access rate we attributed to stalkerware is ixhtb.s9gxw8[.]com[1] and the total number of access attempts was 36,726.

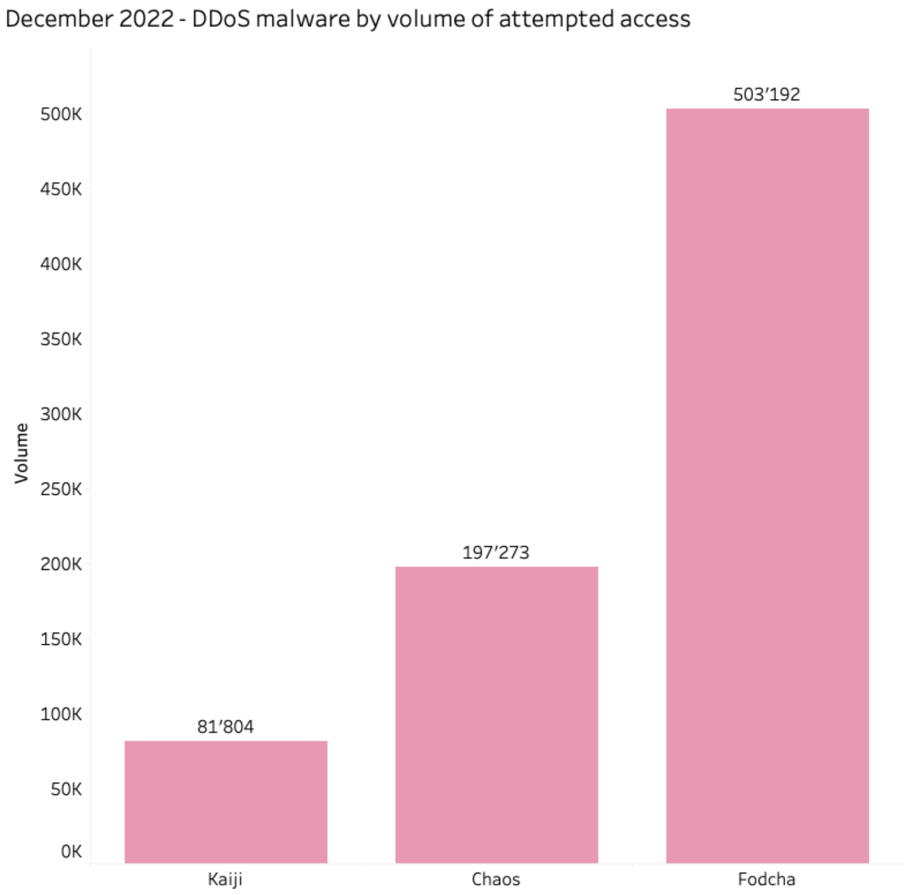
December 2022 - Stalkerware trends by volume of attempted access



DDoS Attacks Remain The Biggest Threat

In December, again we have seen a high number of attempts to the domains attributed to Distributed Denial of Service (DDoS) malware.

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



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

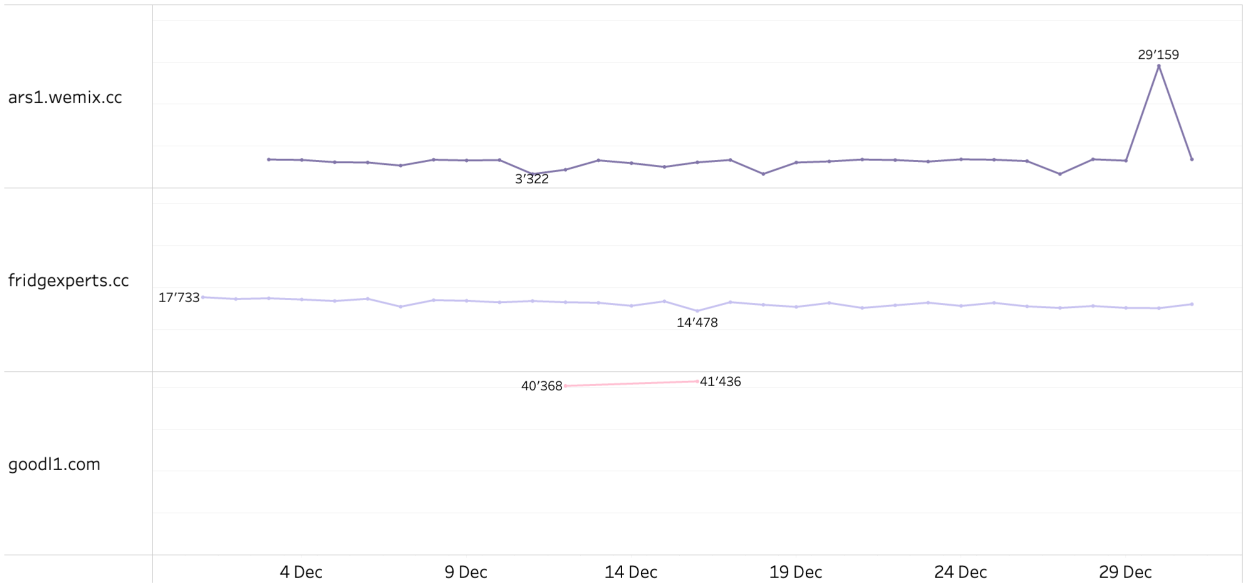
1) **Fodcha** - The highest number of users attempted to access fridgexperts[.]cc, which we attributed to Fodcha Command and Control (C2) server. Fodcha is a relatively new DDoS botnet discovered by the Netlab360 team attributed to Chinese Threat Actors[2]. The malware spreads through the NDay vulnerabilities and Telnet/SSH weak passwords.
2) **Chaos** - Among the top three accessed domains we observed ars1.wemix[.]cc. This domain is associated with Chaos malware, predecessor of Kaiji malware[345]. Chaos is a multifunctional malware written in the Go programming language that has been spotted

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

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.

3) **Kaiji** - The Kaiji-associated malicious domain, goodl1[.]com, was among the top-visited domains. This malware is attributed to Chinese Threat Actors, a distributed denial-of-service (DDoS) botnet targeting enterprises and large organizations. The Golang-based Kaiji malware emerged in early 2020 and targeted Linux systems and internet of things (IoT) devices via SSH brute force attacks[6]. By mid-2020, the Threat Actors also targeted Docker servers[7].

December 2022 - DDoS trends by volume of attempted access



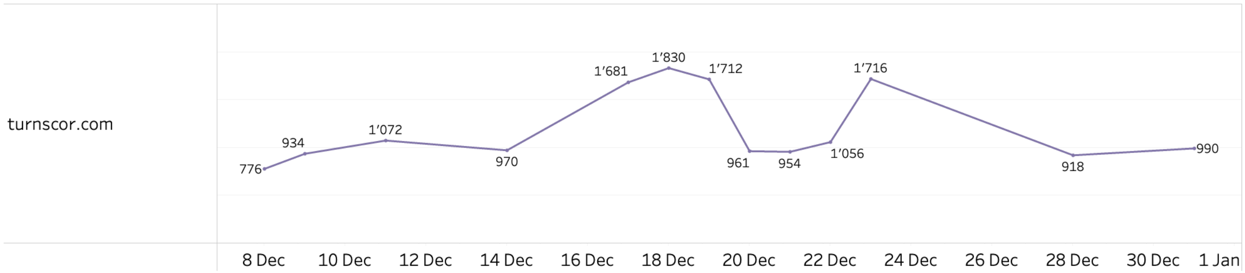
North Korean Backdoor

The new domain we observed with a high attempt access rate was attributed by Mandiant to North Korean backdoor, BLINDINGCAN[8]. The early versions of backdoor supported multiple backdoor commands including file transfer, file management, and command execution. In the most recent version, the malware uses a plugin-based approach that supports several

[6] https://malpedia.caad.fkie.fraunhofer.de/details/elf.kaiji
[7] https://www.securityweek.com/kaiji-botnet-successor-chaos-targeting-linux-windows-systems
[8] https://blogs.jpcert.or.jp/en/2020/09/BLINDINGCAN.html

communication modes[9]. The malware was used by infamous Lazarus/APT38 group[10] and recently is used by UNC4034 Threat Actors in their phishing campaigns abusing WhatsApp. During this campaign, the group lured their victims to download a malicious ISO package regarding a fake job offering that led to the deployment of the backdoor through a trojanized instance of the PuTTY utility. According to our observations, the campaign using the UNC4034 C2 servers was active throughout December and the volume of attempts in measured time periods was 15 570.

December 2022 - BLINDINGCAN Backdoor trends by volume of attempted access

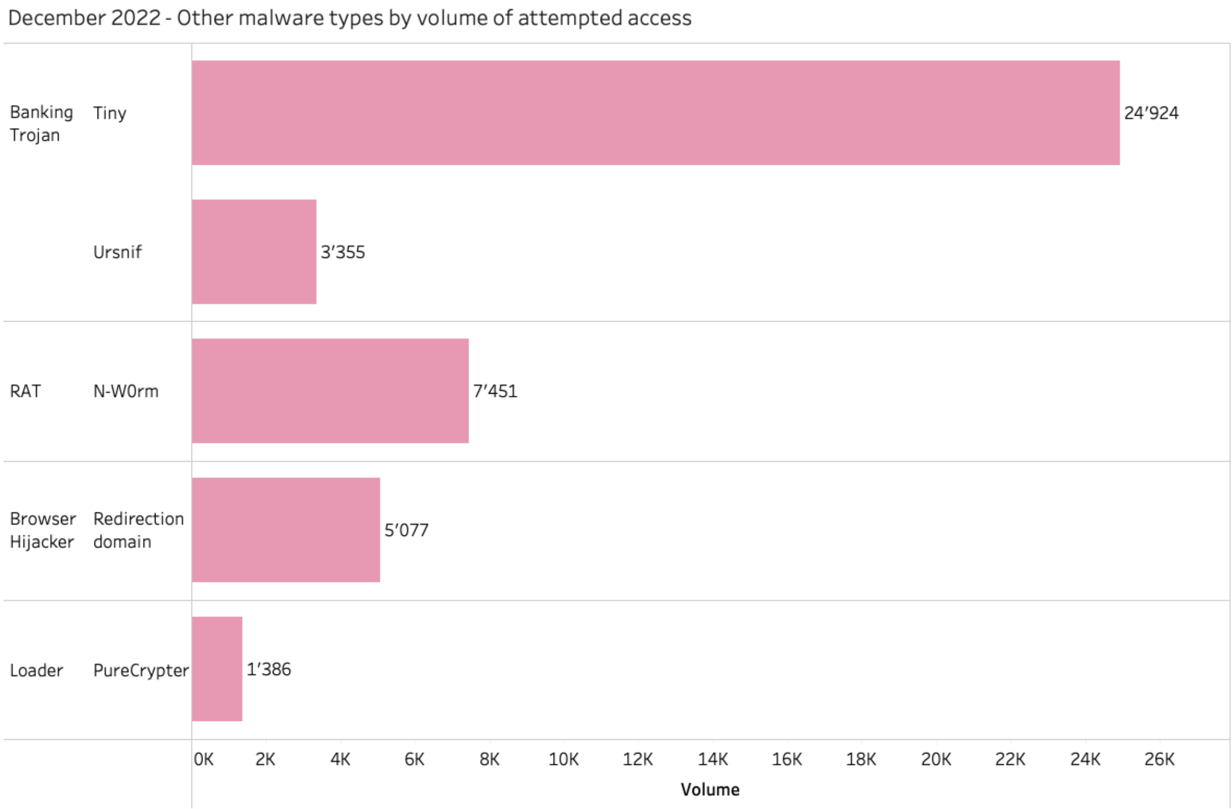


[9] https://www.mandiant.com/resources/blog/dprk-whatsapp-phishing

[10] https://malpedia.caad.fkie.fraunhofer.de/actor/lazarus_group

Banking Trojans, Loaders And Other Threats

Quad9 analyzed five domains with a high access attempt rate. We attributed these domains to Banking Trojans, Remote Access Trojan, Loader and Browser Hijacker.

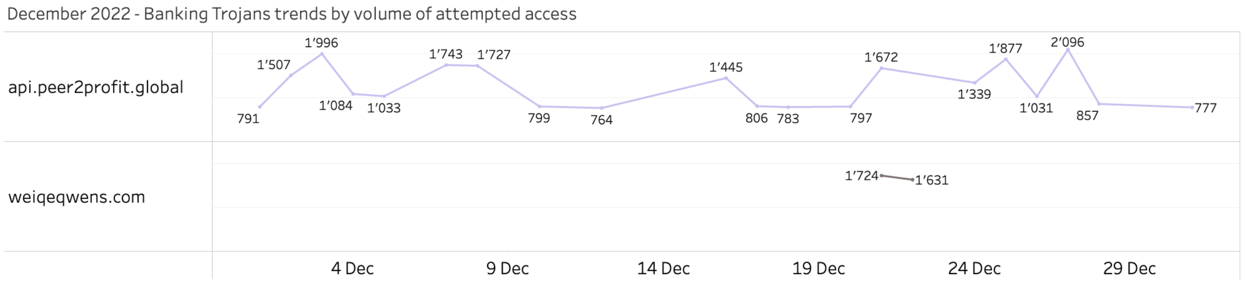


In December 2022, we observed high volumes for two Banking Trojan C2 servers:

1) api.peer2profit[.]global was also reported in November and was attributed with low confidence attribution to Tiny Banking Trojan[11]. Tiny Banker Trojan is a trojan that infects end-user devices and attempts to compromise their financial accounts and steal funds. The campaigns using the Tiny C2 servers were active throughout November and December 2022.

[11] https://malshare.com/sample.php?action=detail&hash=610f0f8caa2928e53a802e4df8670ceb

2) weiqeqwens[.]com was attributed to Ursnif/Gozi. Ursnif malware is effectively delivered through malicious spam campaigns. According to the external reports, the C2 domain reported above was used in the recent campaign impersonating Fortinet[12][13].



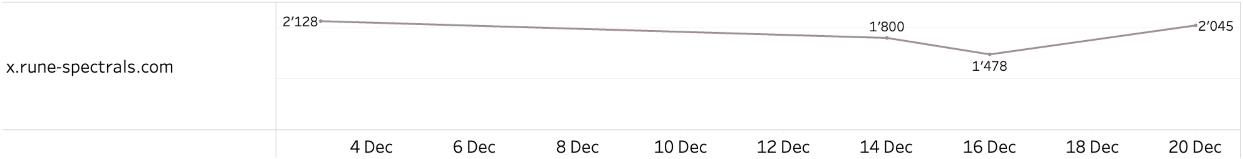
Another analyzed domain links to a Remote Access Trojan (RAT). A RAT is a malware an attacker uses to gain full administrative privileges and remote control of a target computer. In the case of x.rune-spectrals[.]com we attribute the domain with low confidence to N-W0rm[14]. The N-W0rm RAT is distributed via a VBS file and collects the sensitive user's information[15].

Redirection domain and browser hijackers are a common threat we observe among domains blocked by the Quad9 DNS. In December, we observed a high rate of attempted access to 123w0w[.]com[16]. This redirection website diverts the users to a number of unwanted websites. It can divert the browser to dating sites, gambling sites, VPN websites and lastly, malicious drive-by download domains.

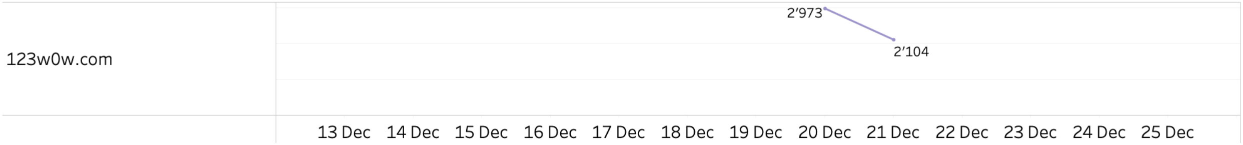
The final domain links to a PureCrypter Loader, a fully-featured malware loader[17]. The malware is used by cyber criminals to deliver remote access trojans (RATs) and information stealers such as AgentTesla and Remcos[18]. As reported in our previous report, the 8220 Gang also leverages PureCrypter for their attacks[19].

[12] https://twitter.com/1ZRR4H/status/1575364101148114944
[13] https://bazaar.abuse.ch/sample/e807c46ba7cd53bf6900d1a8f32baba9a118410483faa68d51b233de738483e3/
[14] https://urlhaus.abuse.ch/browse/tag/N-W0rm/
[15] https://www.secuinfra.com/en/techtalk/n-w0rm-analysis-part-1/
[16] https://www.cyclonis.com/remove-123w0wcom/
[17] https://www.zscaler.com/blogs/security-research/technical-analysis-purecrypter
[18] https://urlhaus.abuse.ch/host/cleaning.homesecuritypc.com/
[19] https://www.sentinelone.com/blog/8220-gang-cloud-botnet-targets-misconfigured-cloud-workloads/

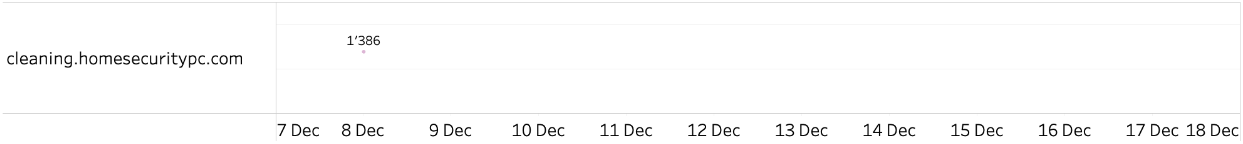
December 2022 - N-W0rm RAT trends by volume of attempted access



December 2022 - Browser Hijacker trends by volume of attempted access



December 2022 - PureCrypter Loader trends by volume of attempted access



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 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 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)

IOC	Details
ixhtb.s9gxw8.com	Stalkerware
fridgexperts.cc	Fodcha C2
goodl1.com	Kaiji C2
ars1.wemix.cc	Chaos C2
turnscor.com	BLINDINGCAN Backdoor
api.peer2profit.global	Tiny Banking Trojan C2
weiqeqwens.com	Ursnif/Gozi Banking Trojan C2
x.rune-spectrals.com	N-W0rm C2
123w0w.com	Browser Hijacker/Redirection domain
cleaning.homesecuritypc.com	PureCrypter C2