Trends December 2022: Cyber Insights

Emilia Cebrat-Maslowski (Quad9 CTI)

Danielle Deibler (Quad9 CISO)

About this report

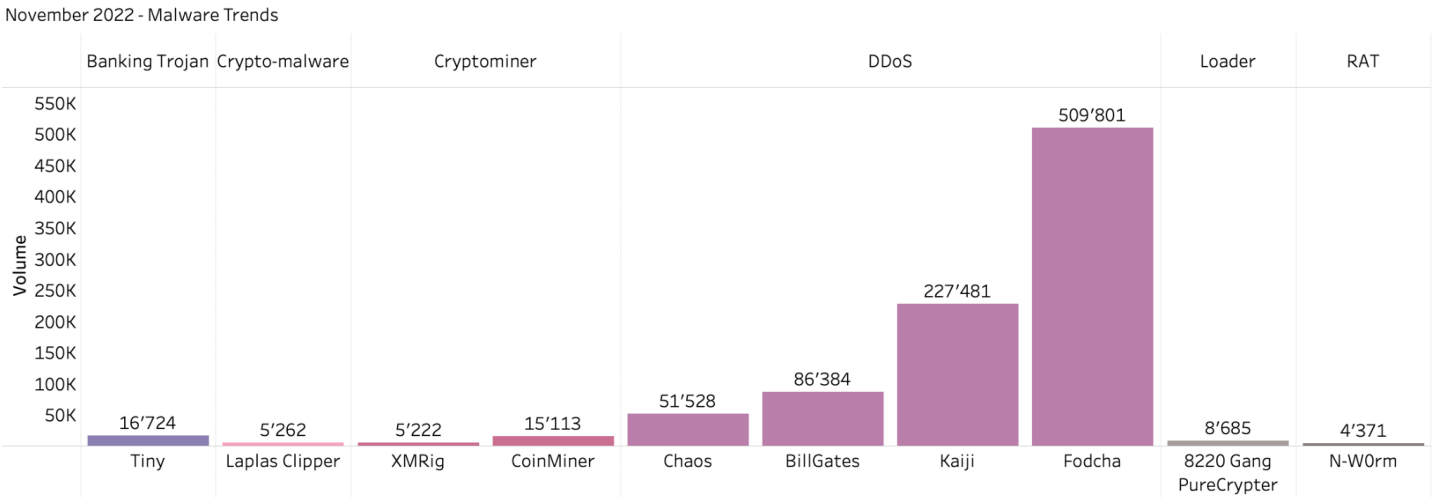
To protect our users, Quad9 blocks DNS lookups of malicious host names from an up-to-the-minute list of threats. This blocking action protects your computer, mobile device, or IoT systems against a wide range of threats such as malware, phishing, spyware, and botnets, and it can improve performance in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

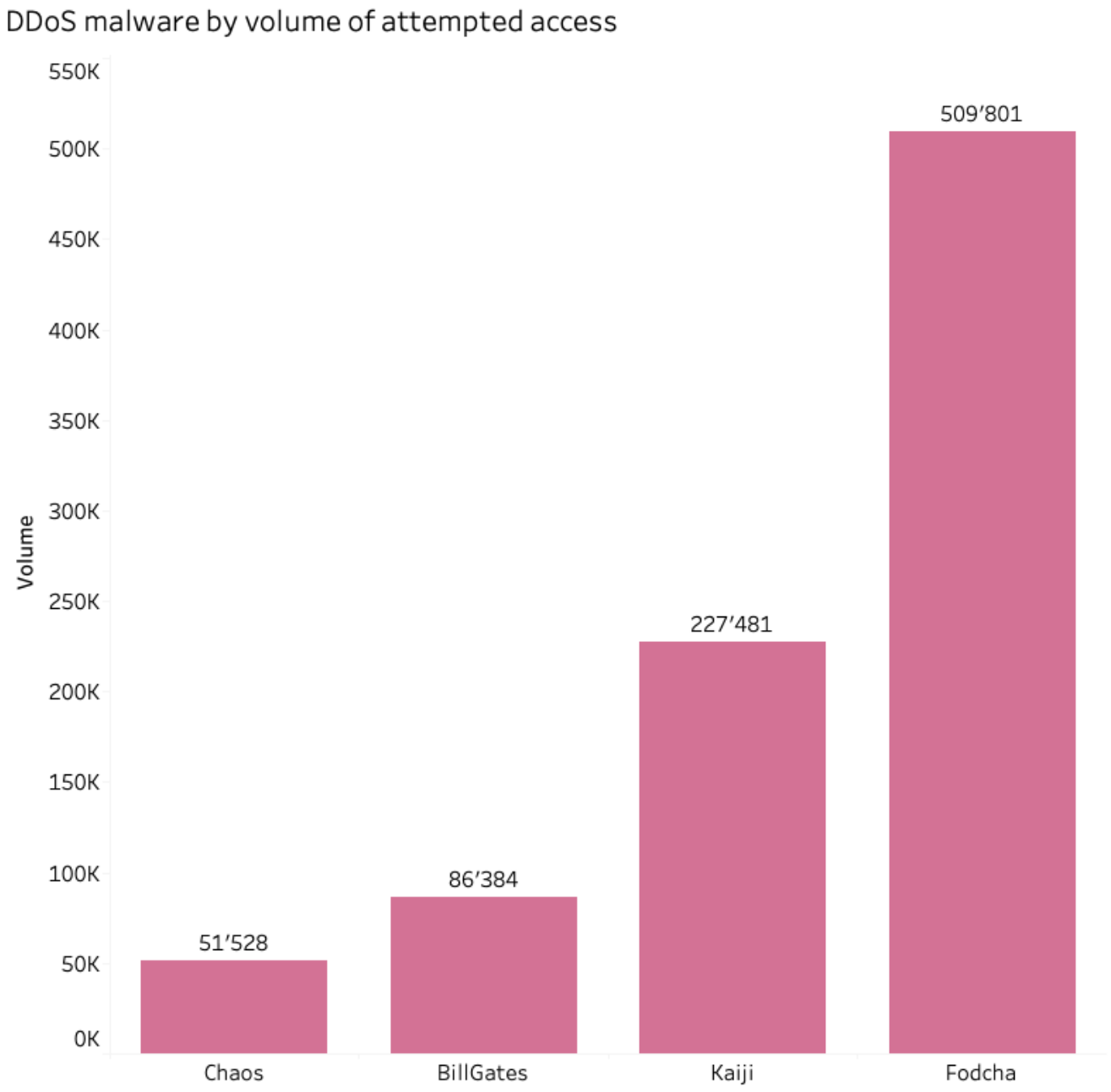
Overview

In November 2022, we observed users targeted with diverse threat categories, including but not limited to DDoS, Banking Trojans, Remote Access Trojans (RATs), and crypto-related malware. This monthly report analyzes the top 10 malicious domains blocked by Quad9 DNS and their associated threats.



DDoS attacks are still on the rise

Among the top 10 domains blocked by Quad9, we attributed four to Distributed Denial of Service (DDoS) malware.



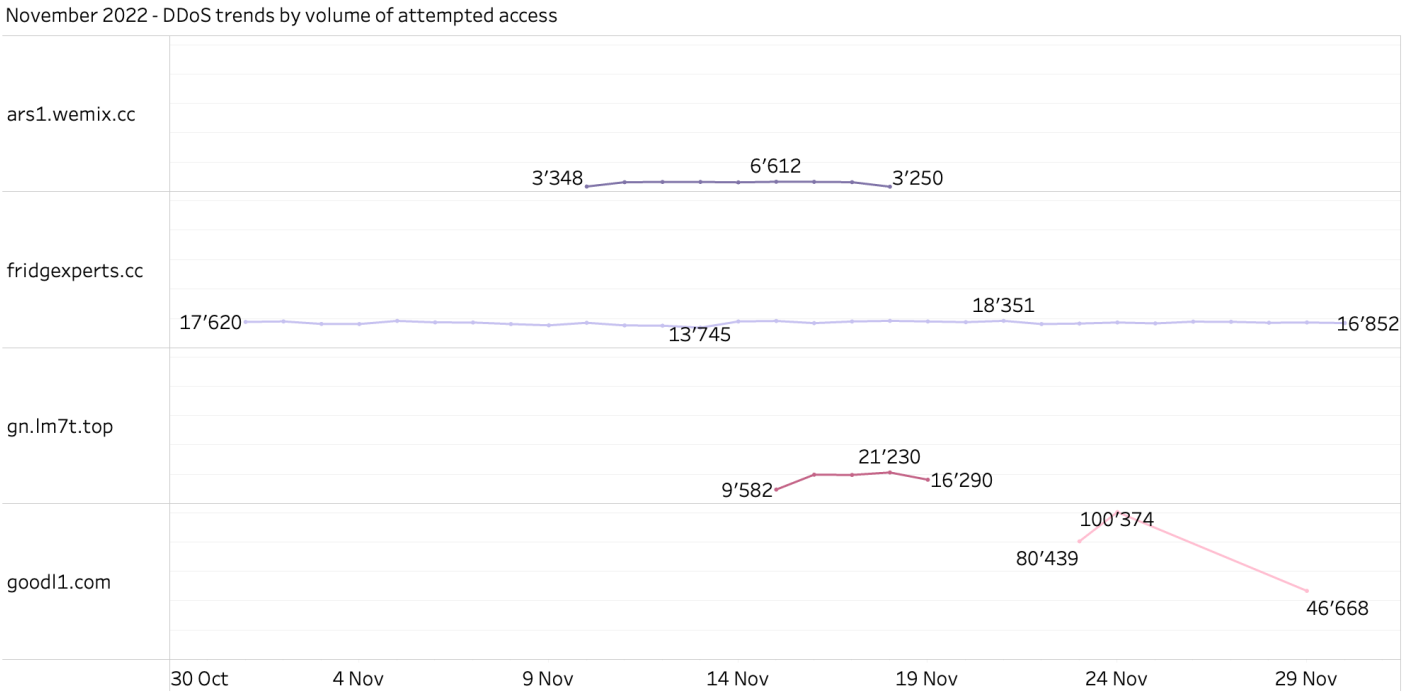
The highest number of users attempted to access fridgexperts[.]cc, which we attributed to Fodcha Command and Control (C2) server. Fodcha is a relatively new DDoS botnet discovered

by the Netlab360 team attributed to Chinese Threat Actors[1]. The malware spreads through the NDay vulnerabilities and Telnet/SSH weak passwords.

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[2]. By mid-2020, the Threat Actors also targeted Docker servers[3].

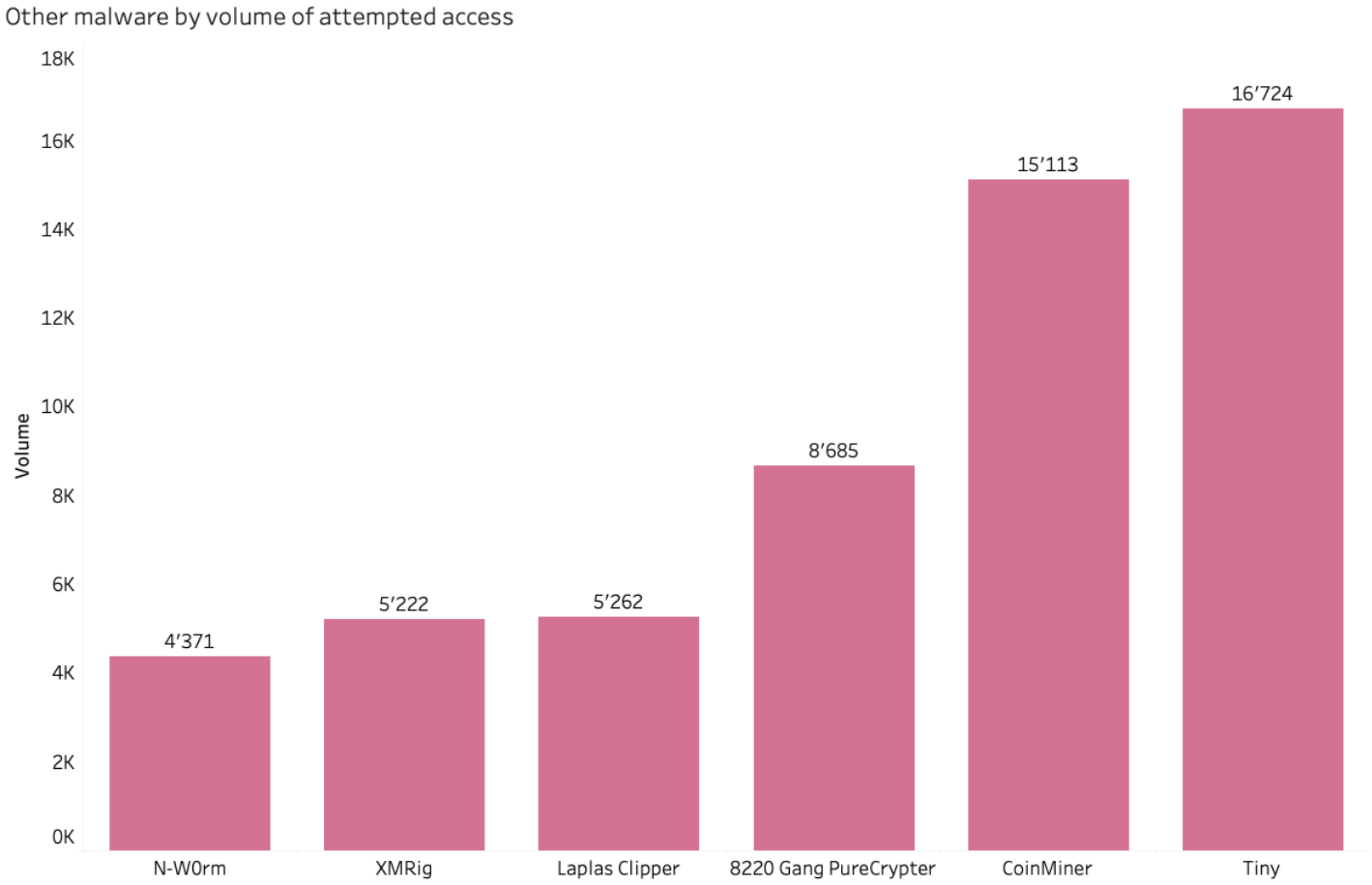
Among top accessed domains we observed two additional domains attributed to DDoS malware: gn.lm7t[.]top and ars1.wemix[.]cc. First of them, the Quad9 team attributed to BillGates malware, which is associated with Chinese Threat Actors and its main functionality is to perform DDoS attacks, with support for DNS amplification[4]. In March 2022, BillGates malware was observed exploiting the infamous Log4shell vulnerability[5]. The last domain, ars1.wemix[.]cc 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.

[1] https://blog.netlab.360.com/fodcha-a-new-ddos-botnet/
[2] https://malpedia.caad.fkie.fraunhofer.de/details/elf.kaiji
[3] https://www.securityweek.com/kaiji-botnet-successor-chaos-targeting-linux-windows-systems
[4] https://malpedia.caad.fkie.fraunhofer.de/details/win.billgates#:~:text=BillGates%20is%20a%20modularized%20malware,as%20well%20as%20for%20Windows
[5] https://www.bleepingcomputer.com/news/security/log4shell-exploits-now-used-mostly-for-ddos-botnets-cryptominers/
[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/



Trojans, loaders and crypto-related malware as the main threats to the users

Quad9 analyzed six domains with a high access attempt rate. We attributed these domains to Banking Trojans, Remote Access Trojans (RATs), crypto-malware and cryptominers.



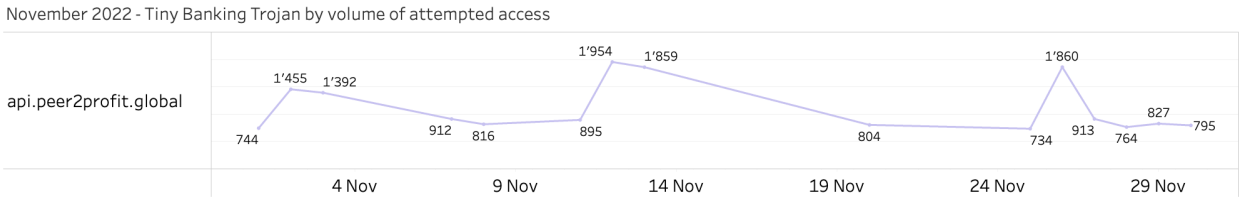
The highest number of attempted access was associated with api.peer2profit[.]global. A low confidence attribution exists to Tiny Banking Trojan[9]. Tiny Banker Trojan is a trojan that infects end-user devices and attempts to compromise their financial accounts and steal funds.

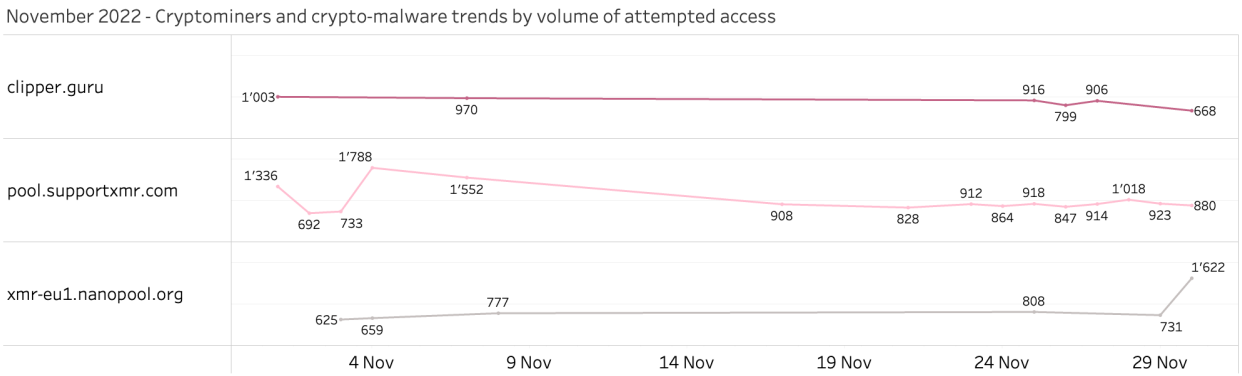
We also observed high volumes for two crypto mining domains: pool.supportxmr[.]com and xmr-eu1.nanopool[.]org.

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

1. CoinMiner has been recently observed abusing Apache Tomcat Web Server vulnerabilities[10] and Atlassian Confluence servers vulnerabilities[11]
2. Monero crypto miner, XMRig[12][13]

We have also observed that many users tried to access the domain attributed to the 8220 Gang and PureCrypter infrastructure. This crimeware group is infamous for infecting cloud hosts through known vulnerabilities and remote access brute forcing infection vectors. In October 2022, the group continued to change compromised hosts into its botnet and distribute cryptocurrency mining malware[14][15]. PureCrypter is a fully-featured loader sold since at least March 2021 and has distributed a variety of remote access trojans and information stealers.



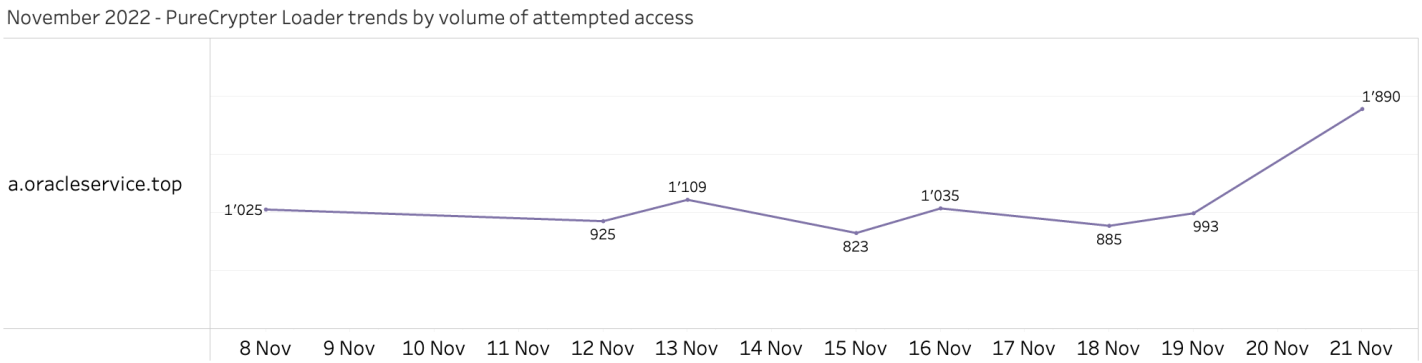


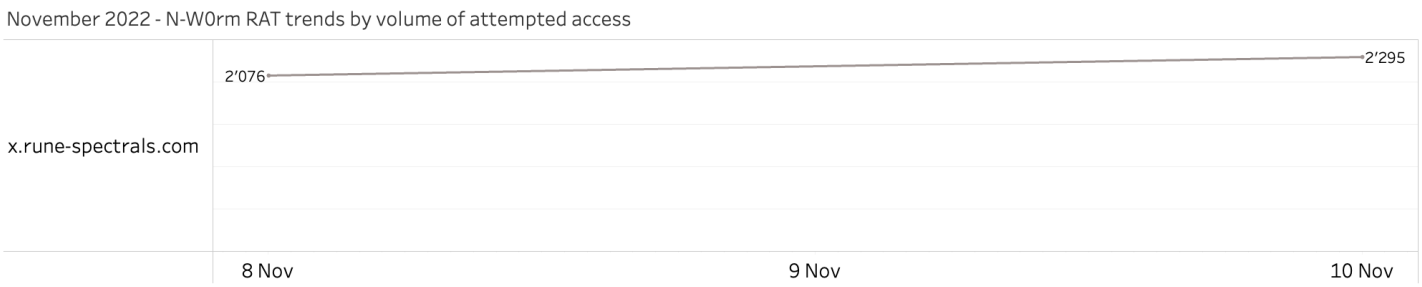
The Quad9 team also observed a higher number of attacks targeting cryptocurrency users. We have seen an increased number of users accessing clipper[.]guru domain attributed to the Laplas Clipper malware. This malware hijacks a cryptocurrency transaction by swapping a

[10] https://asec.ahnlab.com/en/40673/
[11] https://asec.ahnlab.com/en/36820/
[12] https://thedfirreport.com/2020/04/20/sqlserver-or-the-miner-in-the-basement/
[13] https://securityintelligence.com/xmrig-father-zeus-of-cryptocurrency-mining-malware/
[14] https://www.sentinelone.com/blog/8220-gang-cloud-botnet-targets-misconfigured-cloud-workloads/
[15] https://urlhaus.abuse.ch/host/a.oracleservice.top/

victim's wallet address with the wallet address owned by Threat Actors. After the user makes a payment from their cryptocurrency account, the transaction is redirected to the Threat Actor's account instead of the original recipient[16].

The final 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[17]. The N-W0rm RAT is distributed via a VBS file and collects the sensitive user's information[18].





[16] https://blog.cyble.com/2022/11/02/new-laplas-clipper-distributed-by-smokeloader/
[17] https://urlhaus.abuse.ch/browse/tag/N-W0rm/
[18] https://www.secuinfra.com/en/techtalk/n-w0rm-analysis-part-1/

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 in 150 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
fridgexperts.cc	Fodcha C2
goodl1.com	Kaiji C2
e6432f09b652cd3f577cde0671ef18ad9cd6fe5d0b45460a740254dd097f4d51	Kaiji sample[19]
gn.lm7t.top	BillGates C2
ars1.wemix.cc	Chaos C2
api.peer2profit.global	Tiny Banking Trojan C2
pool.supportxmr.com	CoinMiner Mining Pool Address
mr-eu1.nanopool.org	XMRig Mining Pool Address
a.oracleservice.top	8220 Gang C2
clipper.guru	Laplas Clipper C2
x.rune-spectrals.com	N-W0rm C2

[19] https://urlhaus.abuse.ch/url/2345522/