Is Monkeypox Following COVID-19's (Digital) Footsteps?

Table of Contents

Executive Report

The public attention COVID-19 got was truly reflected in the Domain Name System (DNS). And Monkeypox seems to be following the trail the pandemic blazed, though to a smaller extent, as threat actors seem to be using it as the latest phishing lure. How has this new virus been affecting domain registration?

We took a closer look at the DNS space and found:

- Two IP addresses a domain identified as an indicator of compromise (IoC) resolved to
- 600+ domains that shared the IoCs' IP addresses, one of which was found to be malicious
- 700+ domains containing the text string "monkeypox" registered between 1 January and 31 July 2022, a couple of which were dubbed "malware hosts"
- 70+ subdomains containing the text string "monkeypox" registered from 1 January to 31 July 2022

Monkeypox in the News

Monkeypox made headlines in the U.S. when the Centers for Disease Control and Prevention (CDC) first received infection reports in May this year. To date, the CDC has 7,510 reported cases.

Given the rising volume of infections worldwide (30,189 cases at present), the World Health Organization (WHO) has declared monkeypox a public health emergency on 23 July 2022.

Monkeypox may not just affect more people's health, it could also go viral online and present digital risks.

Is Monkeypox presenting digital risks?

Monkeypox is seemingly following COVID-19's digital footsteps in that it's impacting the DNS, albeit at a smaller scale. The virus has been used as a phishing lure in at least one campaign with a single domain (rawshan[.]com) identified as an indicator of compromise (IoC).

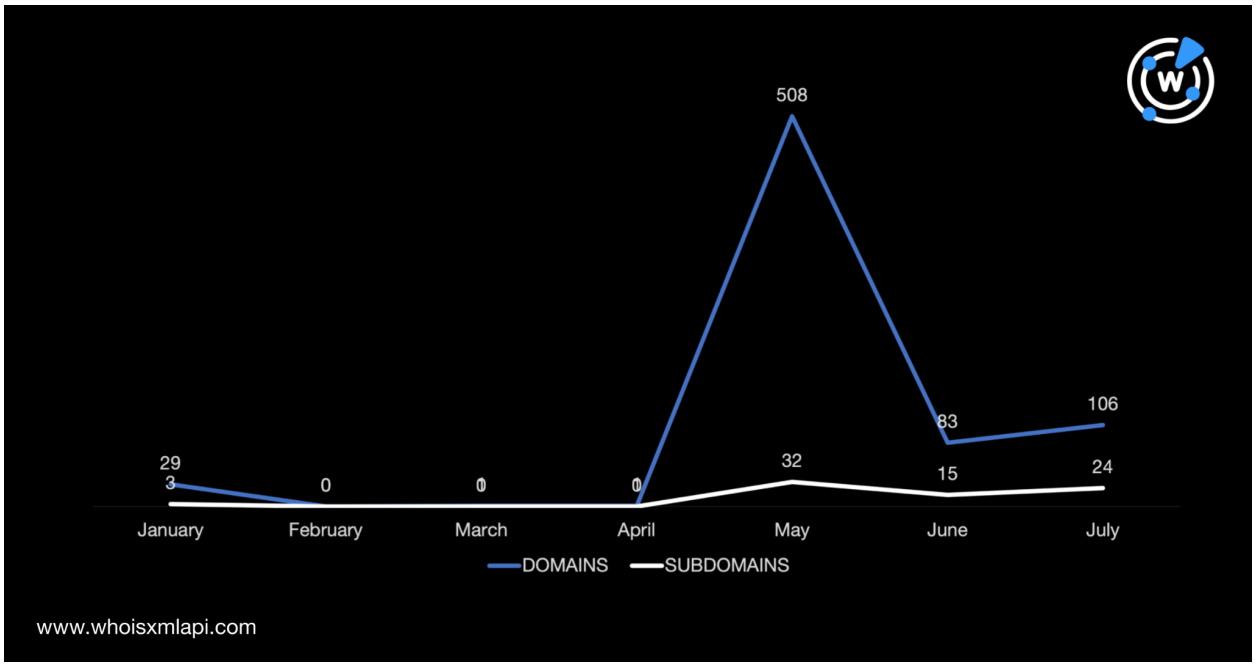
A WHOIS lookup revealed that it's a pretty old domain, created way back in November 2003—possibly hinting at a tactic to evade automatic blocking for being a newly registered domain (NRD).

A DNS lookup showed it resolved to two unique IP addresses—172[.]67[.]134[.]10 and 104[.]21[.]5[.]242. While they aren't malicious, they are shared hosts. At least 600 domains shared them, in fact. One of the web properties—almandoz-tobago[.]com—was deemed "malicious" by a bulk Threat Intelligence Platform (TIP) malware check.

To see if monkeypox is gaining traction in terms of domain registration, we used "monkeypox" as a Domains & Subdomains Discovery search term. That unveiled 728 domains and 75 subdomains, six of which were deemed "malicious." These are:

- 4monkeypox[.]com
- monkeypoxmap[.]xyz
- themonkeypoxvaccine[.]org
- monkeypoxvaccination[.]org
- bookyourmonkeypoxtest[.]com
- monkeypoxcovid-19lies[.]com

A closer scrutiny of the web properties allowed us to map the domain and subdomain registration trends.



The domain and subdomain registration volumes peaked in May 2022, the same time the first case was reported to the CDC. We've often said trends followed current events, and this case proves just that.

An even closer look showed that given the increasing number of monkeypox infections in the U.S., it's quite normal for people to troop online to get information on the virus itself, testing, and cures. That was reflected as well since most of the "monkeypox"-containing domains and subdomains also had the strings led by "test," "virus," and "info."

A lot of the web properties we found are currently up for sale, which phishers might find enticing to host fake Monkeypox-related sites.

—

While only a few of the additional artifacts we found are considered malicious so far, a few of them could be compromised to serve as malware hosts. Organizations looking to ward off potential phishing campaigns should at the very least monitor potentially related artifacts and block access to the malicious ones.

If you wish to perform a similar investigation or get access to the full data behind this research, please don't hesitate to contact us.

Appendix: Sample Artifacts and IoCs

Sample Domains That Shared the IoC's IP Host

- 2ipl[.]com
- 2ipl[.]com
- 2tzalamim[.]co[.]il
- 2tzalamim[.]co[.]il
- 52mv[.]vip
- 52mv[.]vip
- 5best[.]top
- 5best[.]top

- 65qj[.]com
- 65qj[.]com
- 69358872-7bca-11ec-b0f8-b46e08c9a3d7[.]lavendercollection[.]com
- 69358872-7bca-11ec-b0f8-b46e08c9a3d7[.]lavendercollection[.]com
- 735511f[.]com
- 735511f[.]com
- 77o4[.]com
- 77o4[.]com
- 846h[.]link
- 846h[.]link
- 8ywwo8sw[.]com
- 8ywwo8sw[.]com
- a-great-in-real-estate-investment-usa[.]fyi
- a-great-in-real-estate-investment-usa[.]fyi
- a-great-intl-hr-courses[.]zone
- a-great-intl-hr-courses[.]zone
- a-great-us-online-mba[.]zone
- a-great-us-online-mba[.]zone
- a-snag-leukemia[.]zone
- a-snag-leukemia[.]zone
- abgwqllc[.]tk
- abgwqllc[.]tk
- absolutelyspotless[.]us
- absolutelyspotless[.]us
- abungenta[.]cf
- abungenta[.]cf
- acalapelicsmith[.]cf
- acalapelicsmith[.]cf
- accfooddelivery[.]com
- accfooddelivery[.]com
- acpanateco[.]tk
- acpanateco[.]tk
- acrihartswived[.]tk
- acrihartswived[.]tk
- active[.]st
- active[.]st
- actuallyrightthreat[.]biz
- actuallyrightthreat[.]biz
- adastickege[.]gq
- adastickege[.]gq
- add-an-intl-work-from-ok[.]haus
- add-an-intl-work-from-ok[.]haus
- admin[.]lavendercollection[.]com
- admin[.]lavendercollection[.]com
- admincrm[.]gusviradigital[.]co[.]id
- admincrm[.]gusviradigital[.]co[.]id
- adophelinrao[.]tk
- adophelinrao[.]tk
- adtarancachar[.]tk
- adtarancachar[.]tk
- adtradlini[.]tk
- adtradlini[.]tk
- agentnowagercasino[.]club
- agentnowagercasino[.]club
- aktradamursoubna[.]tk
- aktradamursoubna[.]tk
- alcoholrehaboregon[.]com
- alcoholrehaboregon[.]com
- alfalifts[.]com[.]sa
- alfalifts[.]com[.]sa
- alineccycal[.]tk
- alineccycal[.]tk
- all-accesswaxlo[.]com
- all-accesswaxlo[.]com
- almandoz-tobago[.]com
- almandoz-tobago[.]com
- alnabramecomcoo[.]tk
- alnabramecomcoo[.]tk
- alovestore[.]top
- alovestore[.]top
- alsmisgicontheo[.]ml
- alsmisgicontheo[.]ml

- alyasaglik[.]xyz
- alyasaglik[.]xyz
- amazingpayday[.]ca
- amazingpayday[.]ca
- amenegypt[.]net
- amenegypt[.]net
- ameranweb[.]tk
- ameranweb[.]tk
- amoebidldj[.]ru
- amoebidldj[.]ru
- amruosmk[.]monster
- amruosmk[.]monster
- amusesphere[.]com
- amusesphere[.]com
- anasmodila[.]gq
- anasmodila[.]gq
- andrew-schneider[.]com
- andrew-schneider[.]com
- anmanateszue[.]tk
- anmanateszue[.]tk

Sample Domains Containing “monkeypox” Registered between 1 January and 31 July 2022

- monkeypox[.]it
- monkeypox[.]fr
- monkeypox[.]dk
- monkeypox[.]in
- monkeypox[.]ie
- monkeypox[.]ee
- monkeypox[.]ch
- monkeypox[.]se
- monkeypox[.]pl
- monkeypox[.]me
- monkeypox[.]gr
- monkeypox[.]at
- monkeypox[.]ru
- monkeypox[.]cc
- monkeypox[.]ph
- monkeypox[.]ma
- monkeypox[.]su
- monkeypox[.]uk
- monkeypox[.]nl
- monkeypox[.]de
- monkeypox[.]mx
- monkeypox[.]sk
- monkeypox[.]jp
- monkeypox[.]hu
- monkeypox[.]is
- monkeypox[.]es
- monkeypox[.]pt
- monkeypox[.]lt
- monkeypox[.]lol
- monkeypox[.]rip
- monkeypox[.]fun
- monkeypox[.]men
- monkeypox[.]sbs
- monkeypox[.]art
- monkeypox[.]wtf
- monkeypox[.]one
- monkeypox[.]top
- monkeypox[.]cfd
- monkeypox[.]gay
- monkeypox[.]uno
- monkeypox[.]icu
- monkeypox[.]ltd
- monkeypox[.]vip
- monkeypox[.]app
- monkeypox[.]pro
- monkeypox[.]bar
- monkeypox[.]nyc
- monkeypox[.]fyi

- monkeypox[.]buzz
- monkeypox[.]love
- monkeypox[.]asia
- monkeypox[.]fans
- 4monkeypox[.]com
- monkeypox1[.]com
- monkeypoxy[.]net
- monkeypoxa[.]net
- monkeypoxa[.]org
- monkeypoxs[.]com
- monkeypox[.]link
- monkeypox[.]tips
- monkeypox[.]host
- monkeypox[.]live
- monkeypox[.]zone
- monkeypox[.]mobi
- monkeypox[.]blog
- monkeypox[.]site
- monkeypox[.]ruhr
- monkeypox[.]rest
- monkeypox[.]care
- monkeypoxx[.]com
- monkeypox[.]bond
- monkeypox[.]life
- monkeypox[.]skin
- monkeypox[.]pics
- monkeypox[.]wiki
- monkeypox[.]cash
- monkeypoxa[.]com
- monkeypox[.]news
- monkeypox[.]guru
- monkeypox[.]cyou
- monkeypoxz[.]com
- monkeypoxy[.]com
- monkeypox[.]club
- monkeypox[.]tech
- monkeypox[.]shop
- monkeypox[.]space
- monkeypox[.]watch
- monkeypox[.]quest
- monkeypoxrx[.]com
- themonkeypox[.]co
- monkeypoxed[.]com
- monkeypox[.]press
- monkeypoxca[.]com
- monkeypoxdr[.]org
- monkeypox[.]guide
- monkeypox[.]money
- monkeypox[.]email
- monkeypoxct[.]com
- monkeypoxtx[.]com
- monkeypoxmd[.]com

Sample Subdomains Containing “monkeypox” Registered between 1 January and 31 July 2022

- monkeypox[.]paperbackswap[.]com
- monkeypox[.]vercel[.]app
- monkeypox[.]igagenetics[.]es
- monkeypox[.]global[.]health
- monkeypox[.]biolabsantibody[.]com
- monkeypox[.]healthmap[.]org
- monkeypox[.]livemailsupport[.]com
- monkeypox[.]elispiegel[.]codes
- monkeypox[.]catsandcode[.]net
- monkeypox[.]ayudaparaviajeros[.]com
- monkeypox[.]quintoandar[.]com[.]br
- monkeypox[.]info[.]at
- monkeypox[.]stanford[.]edu

- monkeypox[.]cyberia[.]gay
- monkeypox[.]ecoutesante[.]org
- monkeypox[.]uk[.]com
- monkeypox[.]netresolver[.]net
- monkeypox[.]pycoa[.]fr
- monkeypox[.]seidat[.]net
- monkeypox[.]ru[.]com