

Unveiling Stealthy WailingCrab Aided by DNS Intelligence

Table of Contents

1. [Executive Report](#)
2. [Appendix: Sample Artifacts and IoCs](#)

Executive Report

The WailingCrab malware has gained notoriety for its stealth. IBM X-Force security researchers recently published an [in-depth analysis of the malware](#), which has been abusing Internet of Things (IoT) messaging protocol MQTT.

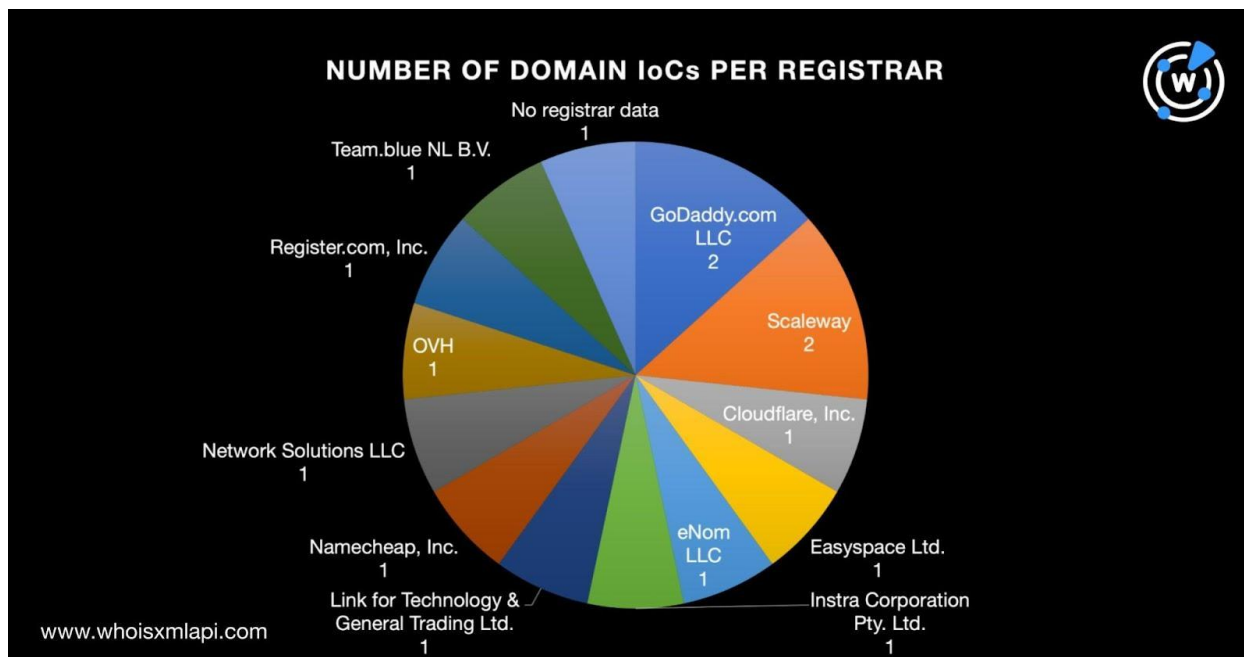
The researchers publicized 24 indicators of compromise (IoCs) as part of their report, including one domain and 14 URLs. After extracting the URLs' domains, we were left with 15 IoCs that we then subjected to an expansion analysis that led to the discovery of:

- 26 email-connected domains
- 17 IP addresses to which the IoCs resolved
- 524 IP-connected domains
- 978 string-connected domains
- 2,002 string-connected subdomains

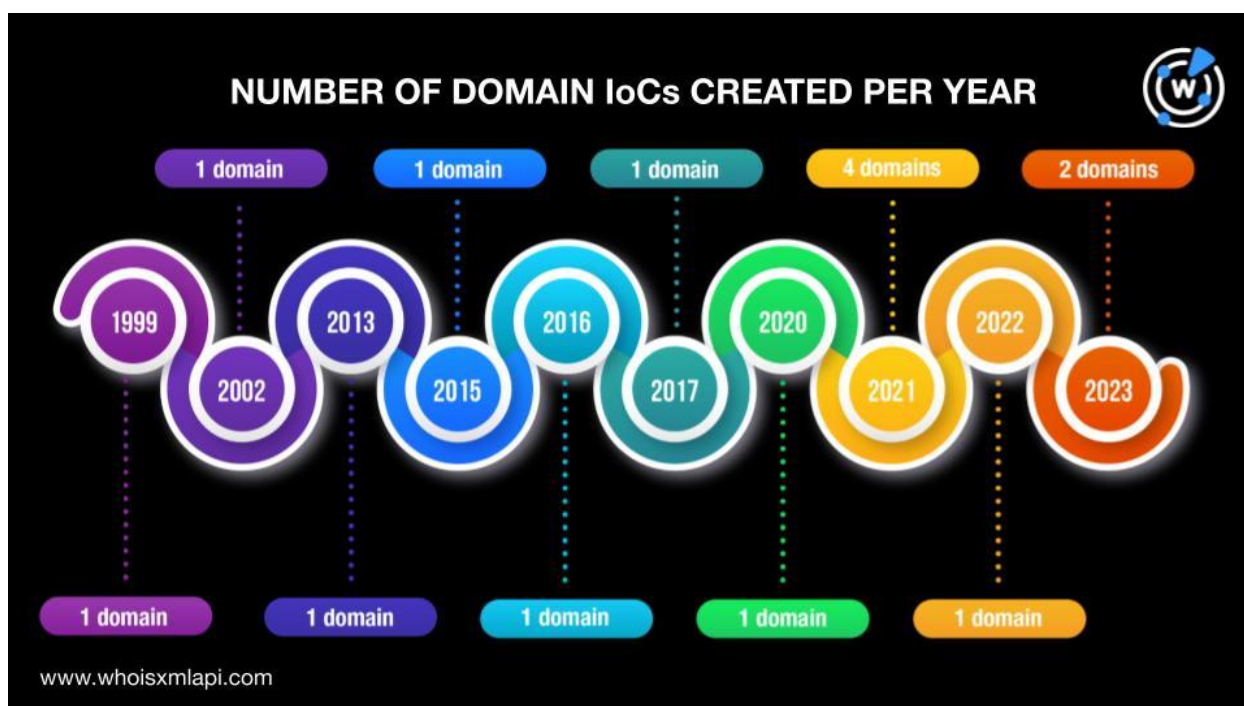
Behind the WailingCrab IoCs

We began our in-depth investigation with a [bulk WHOIS lookup](#) for the 15 domains identified as IoCs and found that:

- GoDaddy.com LLC and Scaleway tied as top 1 registrar, accounting for two domains each. Ten of the domains were distributed among the same number of registrars. One domain did not have available registrar information.



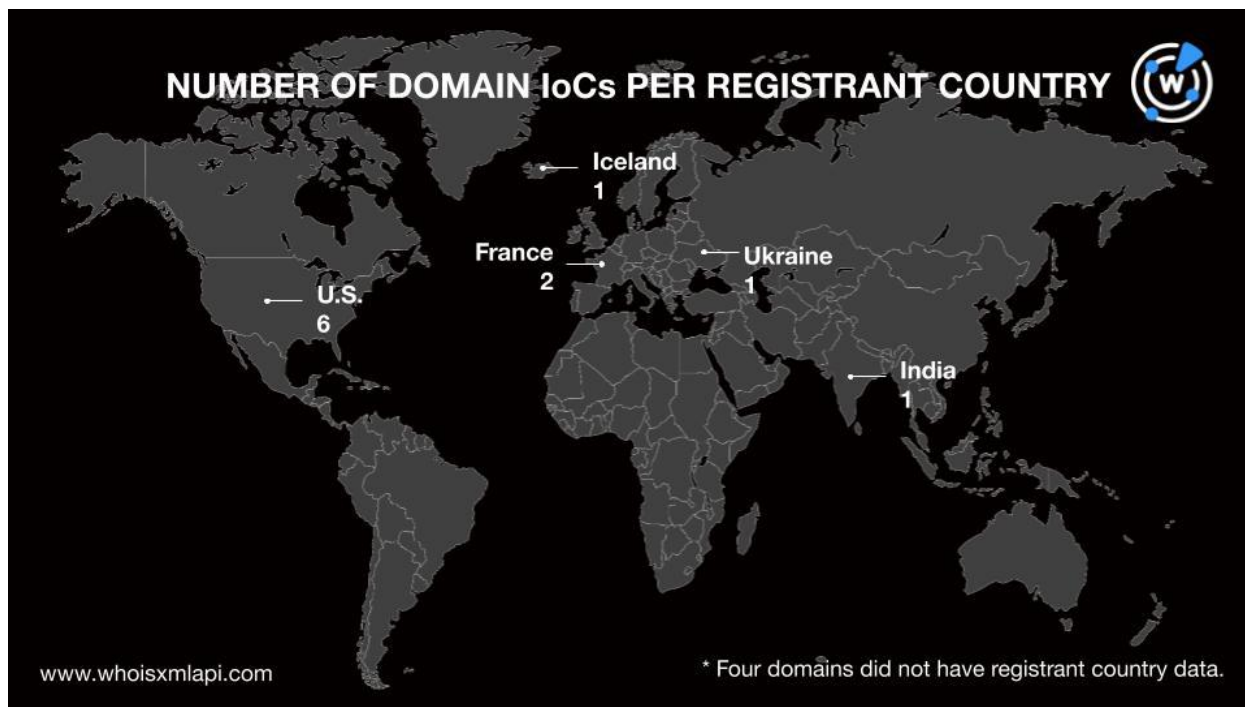
- Four domains were created in 2021; two in 2023; and one each in 1999, 2002, 2013, 2015–2017, 2020, and 2022. One domain did not have a public creation date.



- None of the domains had unredacted registrant email addresses and names. Four, however, did make their registrant organizations public.



- The U.S. was the top registrant country, accounting for six domains. France took the second spot with two domains. One domain each was created in Iceland, India, and Ukraine. Four domains did not have registrant country information.




A Look at the WailingCrab Infrastructure through the DNS Lens

To find every potentially connected artifact in the DNS, we first performed a bulk [WHOIS history search](#) for the 15 domains identified as IoCs. That allowed us to obtain 94 email addresses found anywhere in their historical WHOIS records after duplicates were removed.


A bulk [reverse WHOIS search](#) allowed us to limit the scope of this study to include only the email addresses that appeared in the current WHOIS records of 1–50 domains and were not privacy-protected. We were left with six email addresses to further analyze. They were shared by 26 other domains after duplicates and those already identified as IoCs were removed.

A bulk [screenshot lookup](#) revealed that five of the email-connected domains continued to host live content. Only two, however, led to seemingly functional websites. The three remaining domains led to error or blank pages or were parked.





Screenshot of email-connected domain 767cq[.]com

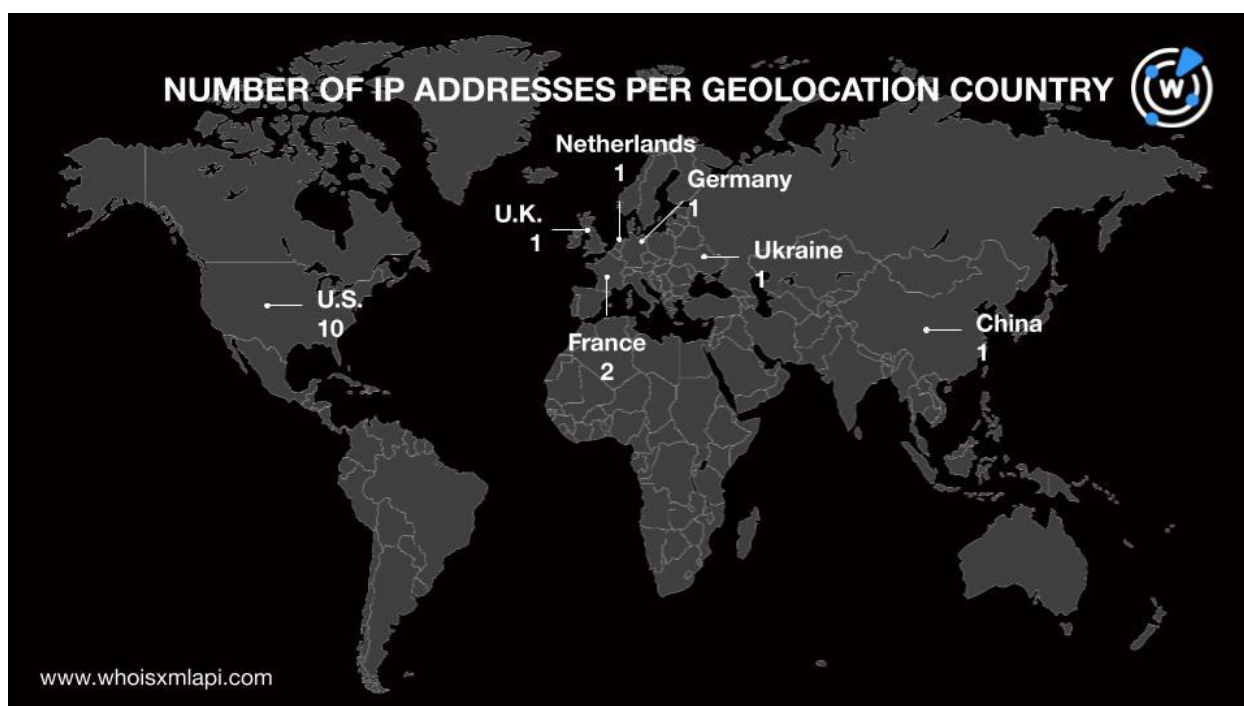


Screenshot of email-connected domain sporactif[.]fr

Next, we ran [DNS lookups](#) for the 15 domains identified as loCs and found that they resolved to 17 unique IP addresses.

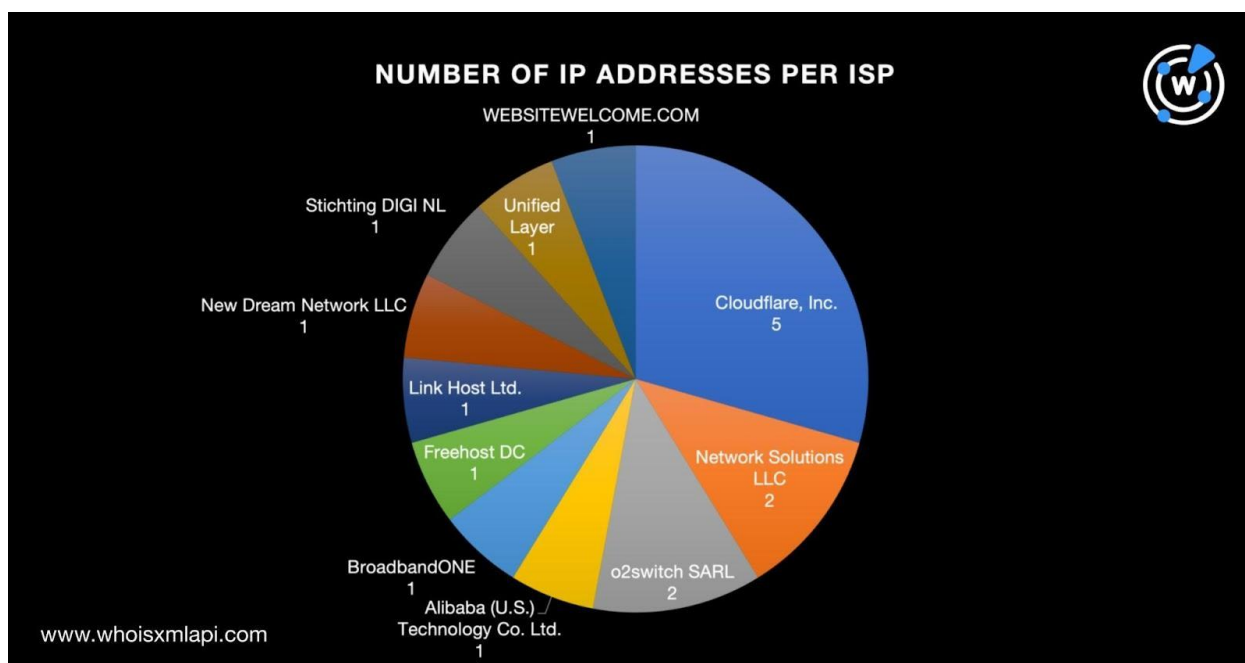
[IP geolocation lookups](#) for the 17 IP addresses showed that:

- A majority of the IP addresses, 10 to be exact, were geolocated in the U.S. France accounted for two IP addresses. One each was located in China, Germany, the Netherlands, the U.K., and Ukraine.





- Cloudflare, Inc. was the top Internet service provider (ISP), accounting for five IP addresses. Network Solutions LLC and o2switch SARL tied in second place with two IP addresses each. The remaining eight IP addresses were spread across Alibaba (U.S.) Technology Co. Ltd., BroadbandONE, Freehost DC, Link Host Ltd., New Dream Network LLC, Stichting DIGI NL, Unified Layer, and WEBSITEWELCOME.COM.



- [Threat Intelligence Lookup](#) embedded intelligence also revealed that 12 of the IP addresses were associated with 1–3 threats each. Take a look at the detailed results in the table below.

IP ADDRESS	THREAT INTELLIGENCE LOOKUP FINDING	ASSOCIATED THREAT TYPES
109[.]234[.]161[.]16	Associated with two threats	Phishing Malware
162[.]159[.]129[.]233	Associated with three threats	Malware Attack Generic
162[.]159[.]130[.]233	Associated with two threats	Malware Generic
162[.]159[.]133[.]233	Associated with two threats	Malware



		Generic
162[.]159[.]134[.]233	Associated with two threats	Malware Generic
162[.]159[.]135[.]233	Associated with two threats	Malware Generic
162[.]241[.]224[.]104	Associated with three threats	Phishing Malware Generic
185[.]104[.]29[.]64	Associated with two threats	Phishing Malware
185[.]13[.]5[.]52	Associated with one threat	Malware
188[.]64[.]139[.]53	Associated with one threat	Phishing
209[.]17[.]116[.]165	Associated with one threat	Phishing
50[.]116[.]86[.]129	Associated with two threats	Phishing Malware

[Reverse IP lookups](#) for the 17 IP addresses revealed that nine of them could be dedicated, each playing host to less than 300 domains at most. Altogether, they hosted 524 domains after duplicates, the loCs, and the email-connected domains were removed.

Three of the IP-connected domains contained popular brand names, namely:

- amazoneng[.]com[.]br
- zoom-business-simulation[.]com
- zoomsim[.]jo

WHOIS record comparisons aided by [WHOIS Lookup](#) with the official domains of Amazon (amazon[.]com) and Zoom (zoom[.]us) showed that none of the three IP-connected domains could be publicly attributed to the companies whose brands appeared in them. In particular:

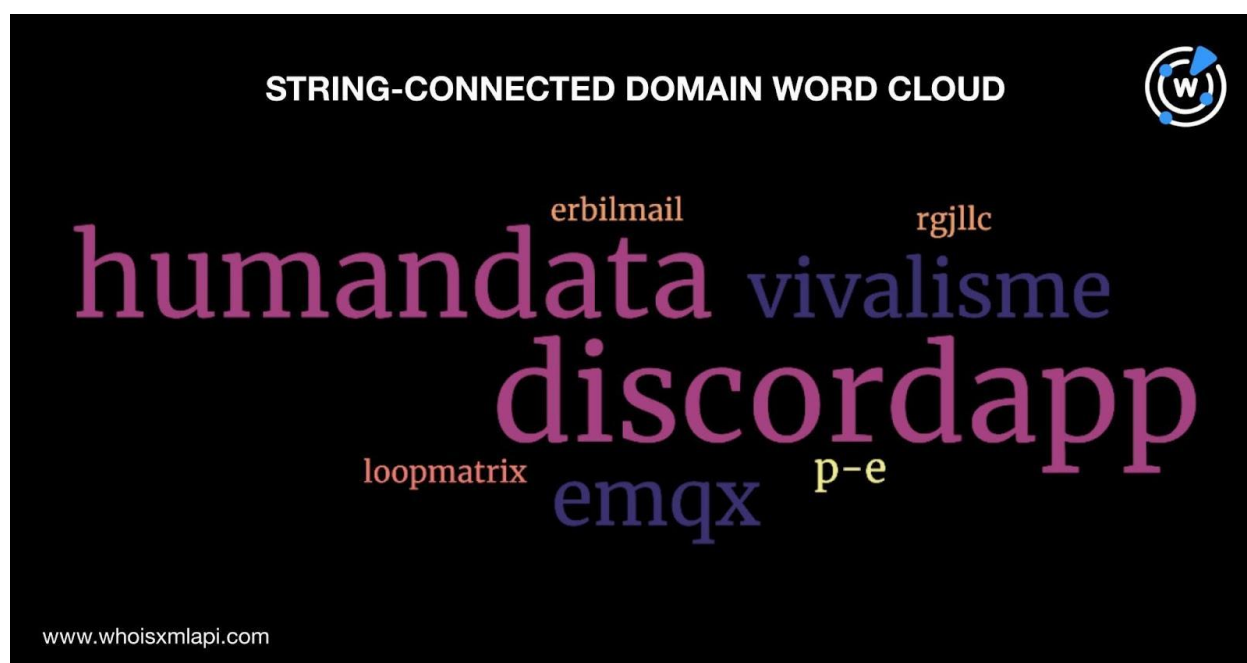
- Amazoneng[.]com[.]br did not share amazon[.]com’s registrant name, organization, and email address.
- Zoom-business-simulation[.]com and zoomsim[.]jo did not share zoom[.]us’s registrant name, organization, and email address.

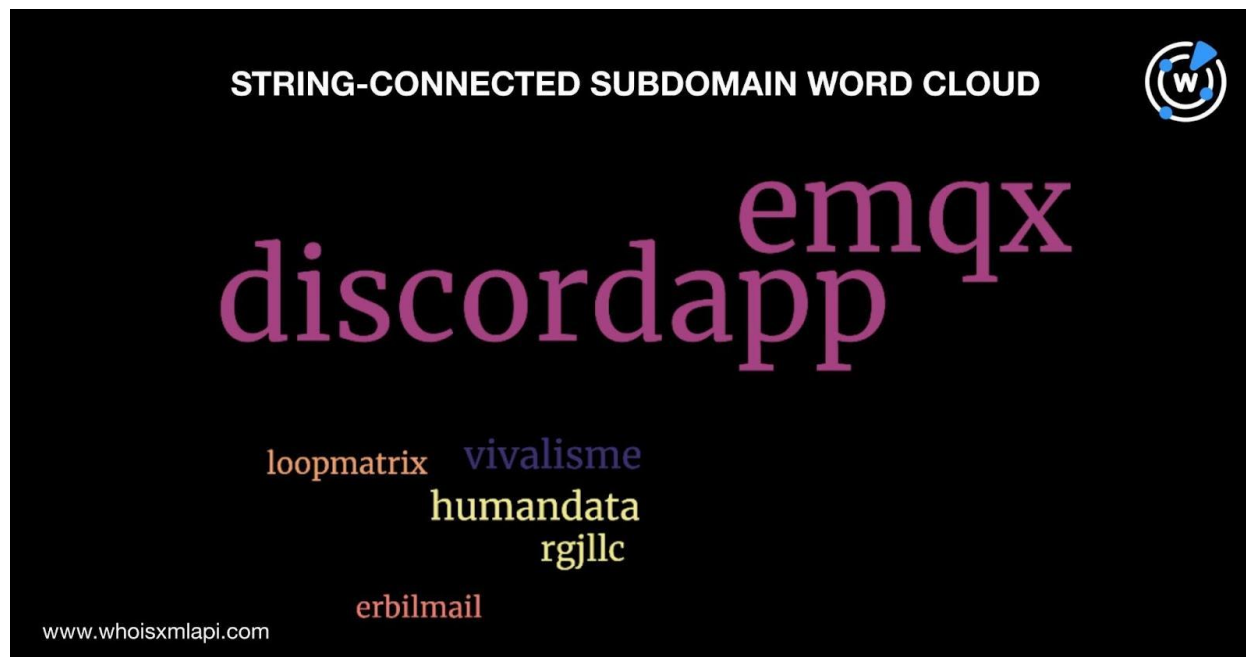


As a last step, we scoured the DNS for other domains and subdomains that contain text strings found among the loCs, specifically:

- discordapp
- emqx.
- erbilmal
- flow.
- humandata
- loopmatrix
- p-e-c.
- rgjllc
- vivalisme

[Domains & Subdomains Discovery](#) provided us with 978 domains and 2,002 subdomains after duplicates, the loCs, and email- and IP-connected domains were removed. We also excluded the domains and subdomains containing **flow.** as there were more than 10,000 results for each web property type, which could include tons of false positives. Take a look at the word clouds that represent the text strings' occurrence among the domains and subdomains.





Our expansion analysis of the WailingCrab IoCs led to the discovery of 3,547 potentially connected artifacts, including 12 IP addresses associated with 23 known threats.

If you wish to perform a similar investigation or learn more about the products used in this research, please don't hesitate to [contact us](#).

Disclaimer: We take a cautionary stance toward threat detection and aim to provide relevant information to help protect against potential dangers. Consequently, it is possible that some entities identified as “threats” or “malicious” may eventually be deemed harmless upon further investigation or changes in context. We strongly recommend conducting supplementary investigations to corroborate the information provided herein.

Appendix: Sample Artifacts and IoCs

WailingCrab IoCs

- advocates4consumerprotection[.]com
- discordapp[.]com
- emqx[.]io
- epikurgroup[.]com
- erbilmail[.]com
- flow[.]enterprises
- humandata[.]solutions
- inspiration-canopee[.]fr
- loopmatrix[.]jin



- luna-render[.]com
- p-e-c[.]nl
- rgjllc[.]pro
- studiolegalcarduccimacuzzi[.]it
- dc1-mtp[.]fr
- vivalisme[.]fr

Sample Email-Connected Domains

- 1st-360vr[.]com
- 40nb[.]com
- 4etong[.]com
- 510girl[.]com
- 51entry[.]com
- 51shangtao[.]com
- 51tgpm[.]com
- 52fanqian[.]com
- 61fushi[.]com
- 767cq[.]com
- 7lnk[.]com
- aisi301[.]com

Sample IP Addresses

- 109[.]234[.]161[.]16
- 109[.]234[.]161[.]167
- 162[.]159[.]129[.]233
- 162[.]159[.]130[.]233
- 162[.]159[.]133[.]233
- 162[.]159[.]134[.]233
- 162[.]159[.]135[.]233
- 162[.]241[.]224[.]104

Sample IP-Connected Domains

- 1wp[.]com[.]br
- 247praise[.]com
- 2wdstore[.]com[.]br
- 317board[.]com
- 40lauriedrive[.]com
- 5tons[.]com
- 5tonscreative[.]com
- 8kgestaodemarcas[.]com[.]br
- abbottsfieldreccentre[.]com
- acmautomacao[.]com[.]br
- adrianodamas[.]com[.]br
- aefretifica[.]com[.]br
- afinadoscomamusica[.]com[.]br
- agenciafiber[.]com
- agenciafiber[.]com[.]br
- aguaesanea[.]com[.]br
- ahonkinggoose[.]com
- akhilaretreat[.]com
- alcsrv01[.]com[.]br
- aliancaautocenter[.]com[.]br
- almeidaartesanato[.]com[.]br
- alphaprincess[.]com
- amazoneng[.]com[.]br
- anchietabatidos[.]com[.]br
- andreabrooks[.]net
- andreabrookslcsw[.]com
- aobe[.]com[.]br
- aplikvisual[.]com[.]br
- ardoce[.]jorg[.]br
- arqfranciscojc[.]com[.]br
- art100limites[.]com[.]br
- artemisambiental[.]com
- artemisambiental[.]com[.]br
- audioarsenal[.]com
- audioarsenal[.]net
- autoeletricadonadon[.]com[.]br
- autoescolajvc[.]com[.]br
- babykillerwhale[.]com



- baraoestruturas[.]com[.]br
- bardavilaitaim[.]com[.]br
- basefortte[.]com[.]br
- bbusiness[.]ch
- bcmncorporation[.]com
- bdlucid[.]com
- bhiwadi[.]com
- bilhetex[.]com[.]br
- birdstar[.]com[.]br
- bmfplumbingllc[.]com
- bnbsync[.]co
- bnbsync[.]net
- bnbsync[.]org
- bnbttally[.]co
- bnbttally[.]com
- bnbttally[.]io
- bnbttally[.]net
- bnbttally[.]org
- bohicaconsultingtx[.]com
- bolosetortasdafatinha[.]com[.]br
- bradyhallstuff[.]com
- brawash[.]com[.]br
- breakthroughloading[.]com
- brentheeringa[.]com
- britnipatterson[.]com
- brooksideas[.]com
- brunabochnia[.]com[.]br
- buuug[.]com
- c4tc[.]co
- caartists[.]com
- cadeiraelevatoriasurimex[.]com[.]br
- cadeirastannah[.]com[.]br
- cafeina[.]digital
- camaradepaulistas[.]mg[.]gov[.]br
- camarasobralia[.]mg[.]gov[.]br
- candeloroengenharia[.]com[.]br
- capsindustry[.]com
- carladaniele[.]com[.]br
- caroneseguranca[.]com[.]br
- carrosbatidoss[.]com[.]br
- cashdomme[.]com
- casino-elliniko[.]com
- casinomarousi[.]com
- catchmeifucanbbq[.]com
- caucaiaameular[.]com
- cbmaraba[.]com[.]br
- ccbbatidos[.]com[.]br
- cemporcentoenvelopes[.]com[.]br
- ceofloripa[.]com[.]br
- cervejariagotter[.]com[.]br
- chamine[.]cc
- charlotteswebcreations[.]com
- chriscollenberger[.]com
- citizensliberatingmichigan[.]com
- clinicaamorim[.]med[.]br
- clinicaanima[.]odo[.]br
- clinicadeolhoscottini[.]com[.]br
- clinicaespacovillage[.]com
- clinicarubiamota[.]com[.]br
- clinicaun[.]com[.]br
- clubedospsts[.]com[.]br
- cmxprojetos[.]com[.]br

Sample String-Connected Domains

- 1aemqx[.]jicu
- 3dhumandatabse[.]com
- 3dhumandataset[.]com
- 4memqx[.]tokyo
- 7emqx[.]wang
- 7s-discordapp[.]com
- a-p-e-c[.]com
- abcdemqx[.]cn
- academie-survivalisme[.]com
- academie-survivalisme[.]fr
- academiesurvivalisme[.]com
- academqx[.]ru



- academy-discordapp[.]club
- activzemqx[.]cf
- activzemqx[.]ga
- adiscordapp[.]com
- aide-survivalisme[.]fr
- aihumandata[.]com
- apprendre-survivalisme[.]fr
- aremqx[.]online
- asemqx[.]work
- assaaemqx[.]com
- autonomie-survivalisme[.]com
- autonomie-survivalisme[.]fr
- bapkemqx[.]loan
- bdiscordapp[.]com
- beta-discordapp[.]ml
- betterdiscordapp[.]com
- betterdiscordapps[.]com
- bgemqx[.]com
- bighumandata[.]com
- blademqx[.]com
- blogsurvivalisme[.]com
- boutique-survivalisme[.]com
- boutique-survivalisme[.]fr
- boutique-desurvivalisme[.]com
- boutique-dusurvivalisme[.]com
- boutique-dusurvivalisme[.]net
- boutique-dusurvivalisme[.]org
- boutique-dusurvivalisme[.]site
- brokeremqx[.]tk
- bsemqx[.]live
- btpgaemqx[.]club
- bushcraftetsurvivalisme[.]com
- bushcraftetsurvivalisme[.]eu
- bushcraftetsurvivalisme[.]fr
- c-i-p-e-c[.]com
- canarydiscordapp[.]com
- casartemqx[.]jac[.]cn
- casartemqx[.]cn
- casartemqx[.]com[.]cn
- casartemqx[.]net[.]cn
- casartemqx[.]org[.]cn
- cdd8emqx[.]top
- cddiscordapp[.]com
- cdiscordapp[.]com
- cdn-discordapp-com-attachments-532533534535-542543544545[.]ml
- cdn-discordapp[.]co
- cdn-discordapp[.]com
- cdn-discordapp[.]net
- cdn-discordapp[.]tk
- cdn-discordapp[.]xyz
- cdndiscordapp[.]com
- cdndiscordapp[.]ga
- cdndiscordapp[.]ml
- cdndiscordapp[.]xyz
- cdndotdiscordapp[.]com
- cdnxdiscordapp[.]com
- cdnydiscordapp[.]com
- chemqx[.]com
- chephumandata[.]com
- clxlb7dkzkymi7hx6br4itcekydftc80nn9m4bz5pkq5uky1w5emqx[.]ws
- codiscordapp[.]com
- comdiscordapp[.]com
- comptoir-dusurvivalisme[.]com
- comptoir-dusurvivalisme[.]fr
- corddiscordapp[.]com
- corsicasurvivalisme[.]com
- cxemqx[.]buzz
- ddiscordapp[.]com
- designhumandata[.]net
- digitalhumandata[.]com
- digitalhumandata[.]org
- discdiscordapp[.]com
- discdiscordapp[.]ws
- discordapp-academy[.]com
- discordapp-academy[.]info
- discordapp-addon[.]com
- discordapp-addons[.]com
- discordapp-addons[.]net



- discordapp-application[.]com
- discordapp-applications[.]com
- discordapp-clone[.]com
- discordapp-download[.]space
- discordapp-events[.]com
- discordapp-fix[.]com
- discordapp-forms[.]com
- discordapp-formulary[.]com
- discordapp-formulary[.]ws
- discordapp-get[.]ru

Sample String-Connected Subdomains

- discordapp[.]h6[.]fan
- billingwetransfericu-discordapps[.]firebaseapp[.]com
- discordapp[.]aisilop[.]info
- discordapp[.]copowen[.]info
- autodiscover[.]discordapp[.]com[.]de
- discordapp[.]ww9[.]myhippo-com[.]scm[.]payusaklarna[.]com
- www[.]discordapp[.]earlytrans[.]com
- www[.]discordapp[.]faceofabovebeauty[.]com[.]ng
- smtp[.]discordapplike[.]cz[.]cx
- server-discordapp[.]kathurian[.]uk
- discordapp[.]nmly[.]cc
- ww8discordapp[.]myhippo-com[.]php[.]payusaklarna[.]com
- ww4[.]discordapp-myhippo-com[.]payusaklarna[.]com
- discordapp[.]net[.]us3[.]cas[.]ms
- khakilameharddrive[.]discordapp[.]repl[.]run
- discordapp[.]auth0[.]net
- ww8[.]discordapppriv[.]payusaklarna[.]com
- discordapp[.]openai[.]army
- discordappww4[.]devstage5-com[.]payusaklarna[.]com
- ww4[.]myhippo-com[.]discordapp[.]origin-community[.]payusaklarna[.]com
- discordappdownload48259[.]jaiblogs[.]com
- 0[.]images-ext-2[.]discordapp[.]net[.]53b6[.]io-01234567[.]v4[.]pcp[.]lookout[.]com
- ww2[.]manage[.]paylution[.]shbmgidiscordappnba2k[.]comsvc[.]unifiedaccessmanagement[.]com
- discordapp[.]perfectluxsistem[.]rs
- discordapp[.]2016-milkteaday-voting[.]bnw[.]dev[.]atg[.]se
- discordapp[.]xlf68[.]cn
- cdndiscordapp[.]pages[.]dev
- cdn-discordapp[.]aliexpress[.]vip
- smooch-web-shbmgidiscordapp[.]directly[.]com
- support-testdiscordapp[.]zendesk[.]com
- discordapp[.]pages[.]dev
- ww4[.]produtomyhippo-com[.]discordapp[.]payusaklarna[.]com
- ww9[.]myhippo-comdiscordapp-secret-manager[.]payusaklarna[.]com
- discordapp[.]com[.]admin-mcas-gov[.]us
- cdn-discordapp-com[.]guardstudio[.]com
- discordapp[.]comone2fan[.]mobz[.]link
- discordapp[.]net[.]cit[.]congruentinda[.]com
- discordapp[.]fhadeyprofessionalhairstylist[.]com
- discordapp[.]bitzy[.]cn



- www[.]discordapp[.]1ck[.]me
- discordapp[.]page[.]link
- www[.]discordapp[.]samphilsdiapers[.]com
- 0[.]cdn[.]discordapp[.]com[.]be37[.]lo-01234567[.]v4[.]pcp[.]lookout[.]com
- discordappww8[.]mybackend[.]payusaklarna[.]com
- discord--discordapp[.]repl[.]co
- ww8[.]us-east-1-stagingdiscordapp[.]payusaklarna[.]com
- cdn-discordapp[.]7-7[.]fun
- ww8[.]myhippo-com-controldiscordapp[.]payusaklarna[.]com
- discordapp[.]useropen[.]cloud
- ww9[.]hippo-com-br[.]discordapp[.]payusaklarna[.]com
- discordapp[.]ww9[.]rivals-com[.]payusaklarna[.]com
- 1-dl--ptb-discordapp-net[.]translate[.]goog
- discordapp[.]blinewd[.]info
- cdn[.]discordapp[.]attachments[.]com
- images-ext-1[.]discordapp[.]net[.]psyche[.]tny[.]town
- discordapp[.]dozacinv[.]com[.]ng
- cdn[.]discordapp[.]xacx[.]net
- rabbitmq-admin[.]sandbox-comdiscordapp[.]directly[.]com
- discordapp-ww4[.]myhippo-com-central[.]payusaklarna[.]com
- discordapp-com[.]connext[.]com[.]co
- discordapplications[.]cf[.]discord[.]holiday
- discordapp[.]signalcorefx[.]com
- discordapp[.]balgend[.]info
- 0[.]media[.]discordapp[.]net[.]c1f5[.]lo-01234567[.]v4[.]pcp[.]lookout[.]com
- news-wetransfericu-discordapps[.]firebaseapp[.]com
- www[.]discordapp[.]comone2fan[.]mobj[.]link
- discordapp[.]repl[.]run
- cdn-discordapp-com[.]273679[.]xyz
- discordapp[.]metesys[.]com
- ml-service[.]discordappbox[.]directly[.]com
- cdn[.]discordapp[.]com[.]ididitfor[.]fun
- vnc-discordapp[.]artifactory[.]evonik[.]com
- ww9[.]myhippo-com[.]discordapp[.]pub1[.]payusaklarna[.]com
- media[.]discordapp[.]net[.]mtsrouter[.]net
- comdiscordapp-ww2[.]manage[.]payloadion[.]nba2k[.]comsvc[.]unifiedaccessmanagement[.]com
- discordapp[.]calderaconsultants[.]com
- www[.]discordapp[.]just[.]a2hosted[.]com
- discordapp[.]galacticinvestors[.]com
- discordapp-ww4[.]myconnectwisemyhippo-com[.]payusaklarna[.]com
- ww4[.]uploads[.]discordapp-myhippo-com[.]payusaklarna[.]com
- ww9[.]wholesaleae1[.]discordapp[.]ae1warrior[.]payusaklarna[.]com
- ww9[.]discordapp-comnojs[.]payusaklarna[.]com
- ww2[.]discordappleimdsrp[.]payloadionnba2k[.]com[.]unifiedaccessmanagement[.]com



- www[.]discordapp[.]com[.]hyperboy13[.]cf
- discordapp[.]co[.]com[.]au
- discordapp[.]berynch[.]info
- discordapp[.]com[.]admin-us[.]cas[.]ms
- discordapptest[.]gitlab[.]appsflyer[.]com
- discordapp[.]ww8[.]myhippo-com-fronpage[.]payusaklarna[.]com
- www[.]discordapp[.]roemahmarthatilaaar[.]org
- discordapp[.]clpker[.]info
- discordapps-whatsapp-clone-738d9[.]firebaseapp[.]com
- discordapp[.]sapioclub[.]com
- ww2[.]mobileimdsrp[.]shbmgidiscordapp-paylution[.]nba2k[.]com[.]unifiedaccessmanagement[.]com
- cdn[.]discordapp[.]zhitiands[.]net
- www[.]discordapp[.]earlycargo[.]com
- ww2[.]mobileimdsrp[.]shbmgidiscordapppaylution[.]nba2k-com[.]unifiedaccessmanagement[.]com
- cdn[.]discordapp[.]com[.]infiniterecall[.]com
- www[.]discordapp[.]ndukakpompcs[.]com[.]ng
- ww8-discordapp[.]ctl-myhippo-com[.]payusaklarna[.]com