サプライチェーン攻撃に悪用されるチャットアプリの存在に迫る

目次

要旨

2022 年 9 月、脅威アクターが「Comm100」と「LiveHelp100」というチャットアプリを悪用してサプライチェーン攻撃を開始したとトレンドマイクロが報告しました。この問題を抑制するため、同社は以下の 9 つのセキュリティ侵害インジケーター（IoC）、具体的には C＆C サーバアドレスを公開しました。

- analyaze[.]s3amazonbucket[.]com
- services[.]livehelp100services[.]com
- service[.]livehelpl00service[.]com
- app[.]livehelpl00services[.]com
- analysis[.]windowstearns[.]com
- max[.]cornm100[.]io
- s[.]livelyhellp[.]chat
- files[.]amazonawsgarages[.]com
- 8[.]219[.]76[.]37

WhoisXML API の研究者は、IP アドレス、DNS および WHOIS データを徹底的に調べることで上記の IoC リストを広げ、潜在的にターゲットとなり得る組織が侵害を防ぐ手助けをしたいと考えました。こうして行った当社の調査で、以下のことが明らかになりました。

- C&C サーバのドメイン名が名前解決したのは 9 個の IP アドレス。
- C&C サーバのものと同じ IP ホストを共有していたドメイン名は 306 件。
- C&C サーバーのドメイン名に含まれる文字列と同じ文字列を持つドメイン名が 4 件、サブドメインが 32,822 件判明、そのうちの 81 件は悪意があると確認。
- 2022 年に最も多く利用されたチャットアプリ 10 種の名称を文字列の中に含んでいる 660 件のドメイン名のうち、それら製品名の帰属する企業自身が登録していると確認できたものは、わずか 2%。8 件は悪意あるドメイン名であることが判明。

IoC リストの拡張分析でわかったこと

当社ではまず、C&C サーバのドメイン名を DNS lookups で検索し、まだ公開されていない 9 つの IP アドレスを発見しました。そのうちの 4 つを以下に紹介します。

- 47[.]243[.]117[.]16
- 8[.]219[.]76[.]37
- 47[.]243[.]85[.]219
- 47[.]242[.]253[.]75

発見した IP アドレスを当社の Reverse IP Lookups で検索したところ、別の 306 件のドメイン名に共有されていることがわかりました。315 のウェブプロパティのうち悪意があると認められたものはありませんでしたが、IP アドレスのマルウェアチェックをした結果、それらの全てに SSL（Secure Sockets Layer）の設定上の問題があると判明しました。

前述の IoC には他のドメイン名やサブドメインの文字列になっている可能性のある特定の名称が含まれており、同一または類似の脅威の媒介となる可能性があります。下表のユニークな文字列をキーワードとして、Domains & Subdomains Discovery で検索してみました。その際、「Starts with」パラメータを使って、IoC と最もよく似たものに結果を絞り込みました。

ドメイン名の検索文字列	サブドメインの検索文字列
livehelp100services	*services.*
livehelpl00service	*service.*
livelyhellp	*max.*
cornm100	*files.*
amazonawsgarages	*analysis.*
windowstearns	*analyze.*
s3amazonbucket	

この検索により、追加で 4 件のドメイン名、32,822 件のサブドメインが明らかになりました。マルウェアのチェックを一括して行ったところ、81 件がさまざまなマルウェアエンジンによって悪意あるものと分類されていました。

悪意あるサブドメインを詳細に調査した結果、Amazon、Google、PayPal、Apple といった人気ブランドの名称が IoC に含まれる文字列と並んで表記されていることがわかりました。下図は、その結果を反映したワードクラウドです。

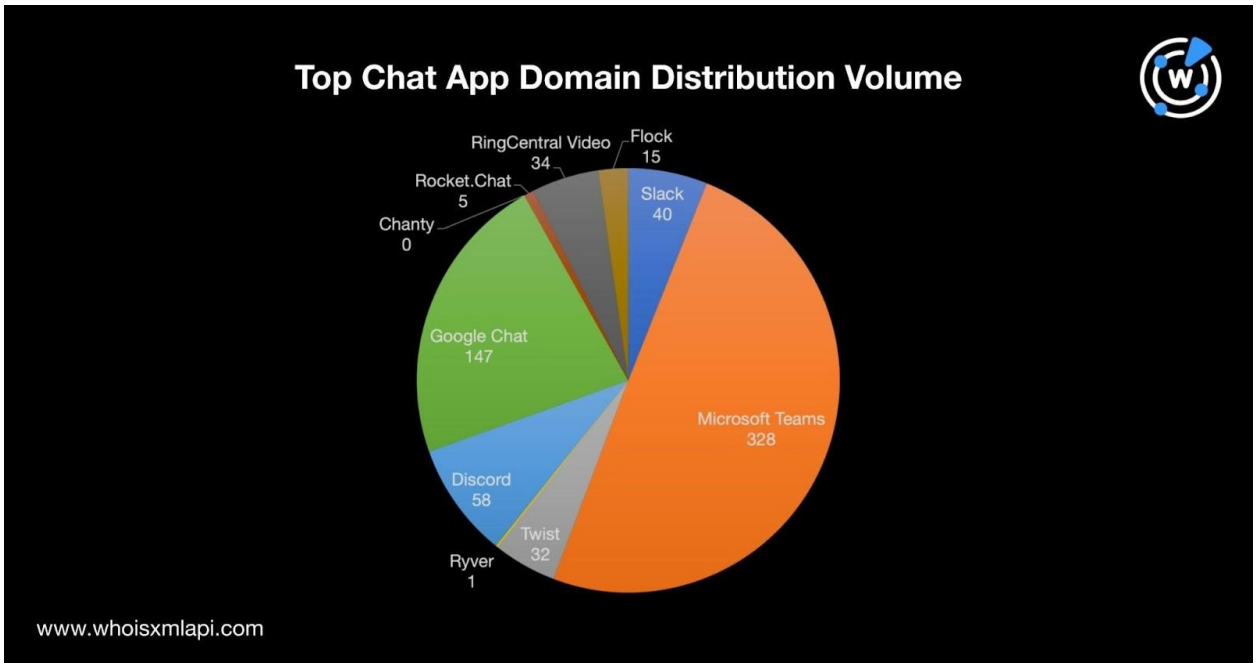
悪意あるサブドメインの大半に「runescape」が含まれ、「paypal」と「apple」がそれに次いで多いことがわかります。

他のチャットアプリやそのユーザーも危険にさらされている？

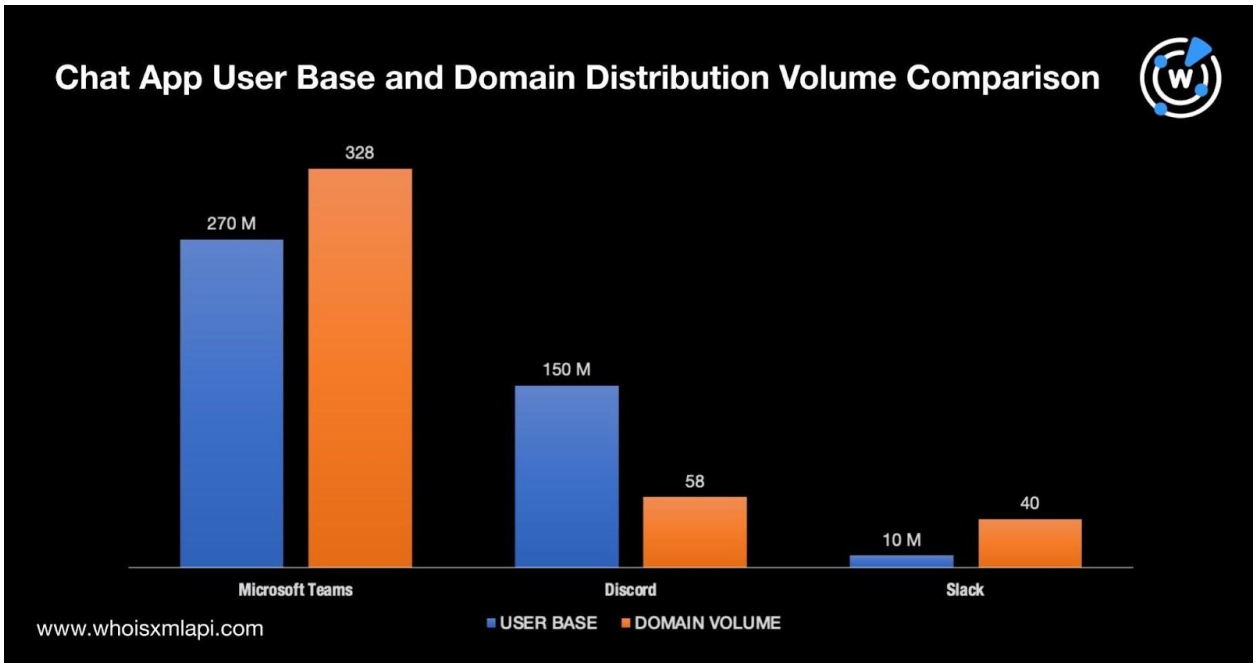
他のチャットアプリやそのユーザーが同様の脅威の標的となる可能性があるかどうか判断するため、2022 年の人気チャットアプリトップ 10 のリストを入手しました。そして、当社の Domains & Subdomains Discovery によってドメインを限定し、下表の文字列を使用して調査を行いました。

チャットアプリ	使用文字列
Slack	*slack + chat*
Microsoft Teams	*microsoft + teams*
Twist	*twist + chat*
Ryver	*ryver + chat*
Discord	*discord + chat*
Google Chat	*google + chat*
Chanty	*chanty + chat*
Rocket.Chat	*rocket.chat*
RingCentral Video	*ringcentral + video*
Flock	*flock + chat*

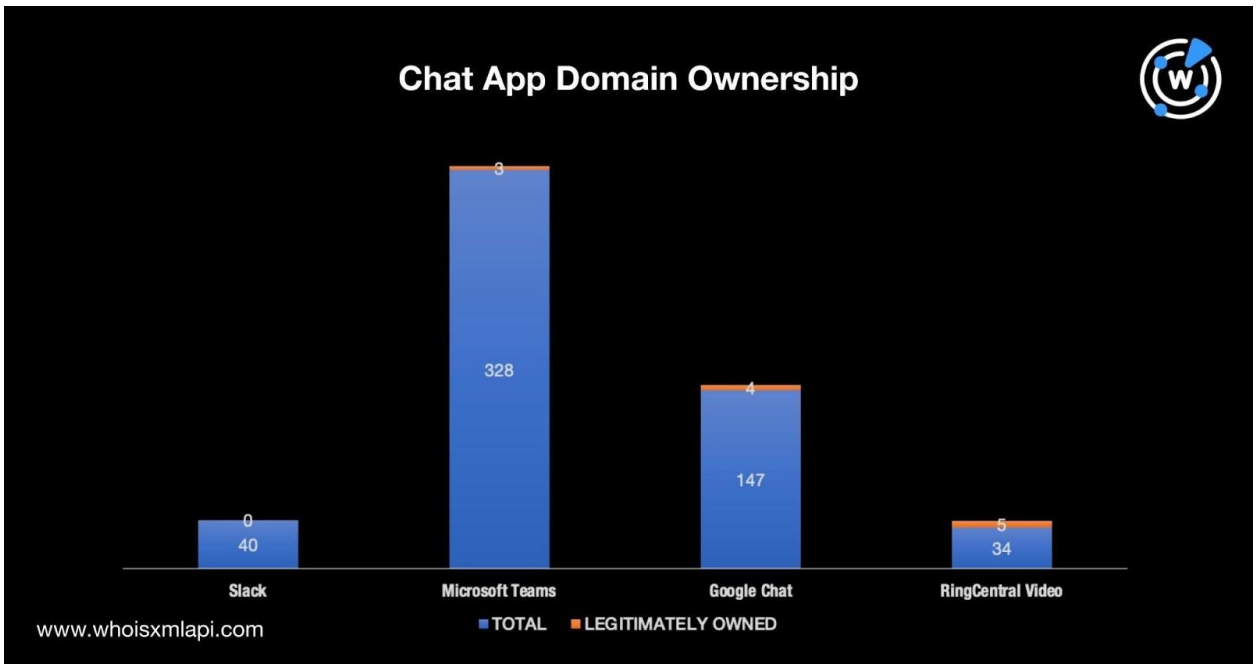
今回の検索では、「chanty + chat」を含むドメインは見つからなかったものの、それでも660件のドメイン名が該当しました。チャットアプリ別のドメイン数の内訳は以下の通りです。



Microsoft Teamsの利用者が世界で2億7千万人と最も多いことを考えれば、この結果は驚くことではありません。上位3つのアプリの利用者数とドメイン名数の分布を比較してみましょう。



追加で見つかったドメイン名の WHOIS データを一括検索したところ、ブランド名を文字列に含んでいるドメイン名のうち正規の企業に属しているものがどれだけあるかを特定できました。ただし、これは WHOIS で登録者の情報が公開されているもの、すなわち Slack、Microsoft Teams、Google Chat、RingCentral Video に限定した結果です。比較を以下のグラフで示します。



全体を見ると、チャットアプリのドメインのうち、正規の企業に属していると確認できたものはわずか 2%（549 件中 12 件）でした。そのうちの 8 件は悪意あるものとして分類されました。例として 4 つを以下に示します。

- microsoftteams[.]fun
- microsoftteams[.]top
- discord-chatbot[.]tk
- discordchatterscommunity[.]com

—

企業、とりわけ巨大なグループ会議に対応したチャットアプリを必要とする企業は、今回確認した悪意あるドメインに注意する必要があります。脅威アクターは、こうした不正なウェブプロパティを利用して、組織に同じようなサプライチェーン攻撃を仕掛ける可能性があります。

If 同様の調査をご希望のお客様、またはこの調査の全データをご希望のお客様は、こちらまでお気軽にお問い合わせください。

付録：アーティファクトと IoC の例

C&C サーバのドメイン名が名前解決した IP アドレスの例

- 47[.]243[.]117[.]16
- 8[.]219[.]76[.]37
- 47[.]243[.]85[.]219
- 47[.]242[.]253[.]75

C&C サーバの IP アドレスを共有していたドメイン名の例

- 0--i[.]com
- 0-0-0-7[.]com
- 0-24[.]top
- 0-it[.]com
- 0-lesbienne[.]com
- 0-y[.]in
- 000[.]email
- 000[.]irish
- 000[.]one
- 000[.]reisen
- 000000[.]best
- 0000020[.]xyz
- 00001test[.]com
- 00002test[.]com
- 00003test[.]com
- 000106[.]xyz
- 000111[.]xyz
- 000117[.]xyz
- 0001210[.]xyz
- 0001230[.]xyz
- 000126[.]xyz
- 000129[.]xyz
- 000132[.]xyz
- 000133[.]xyz
- 000134[.]xyz
- 000135[.]xyz
- 000136[.]xyz
- 000137[.]xyz
- 000138[.]xyz
- 000139[.]xyz
- 000141[.]xyz
- 000142[.]xyz
- 000144[.]xyz
- 000146[.]xyz
- 000147[.]xyz
- 000148[.]xyz

- 000149[.]xyz
- 000151[.]xyz
- 000152[.]xyz
- 000153[.]xyz
- 000154[.]xyz
- 000157[.]xyz
- 000158[.]xyz
- 000159[.]xyz
- 000161[.]xyz
- 000162[.]xyz
- 000164[.]xyz
- 000165[.]xyz
- 000167[.]xyz
- 000169[.]xyz

C&C サーバのドメインと同じ文字列を含むドメインとサブドメインの例

- livehelp100services[.]com
- livehelp100servicestandby[.]com
- services[.]dev[.]dev01[.]foodi[.]fr
- services[.]staging[.]escale[.]com[.]br
- services[.]wifi[.]mhyuan[.]dev[.]usa[.]cloud[.]watchguard[.]com
- services[.]eps2[.]metlife[.]com
- services[.]test[.]sctv[.]ch
- services[.]prod-aws[.]pizzahut[.]com
- services[.]wp[.]dvlp[.]es[.]cloud[.]vt[.]edu
- services[.]dev2[.]api[.]bluestreamsinsurance[.]com
- services[.]bcom-185[.]tbe[.]zeus[.]fds[.]com
- services[.]vacheron[.]dev2[.]utopix[.]ch
- services[.]swift[.]state[.]mn[.]us
- services[.]www[.]wdesk[.]ca
- services[.]etatcivil[.]gouv[.]qc[.]ca
- services[.]clg-frederic-montenard[.]ac-nice[.]fr
- services[.]dev[.]helthjem[.]no
- services[.]bcom-098[.]tbe[.]zeus[.]fds[.]com
- services[.]49d811904d21887de83bca4b34a60a2f[.]dancefloor[.]dev
- services[.]ews[.]admin[.]ch
- services[.]loki[.]business[.]crxt[.]io
- services[.]bcom-103[.]tbe[.]zeus[.]fds[.]com
- services[.]71612c3be8a501099904d679f00520dd[.]dancefloor[.]dev
- services[.]e63e5fa3491b460f82b69e2dbb402887[.]dancefloor[.]dev
- services[.]02d48f21bddf02c1eeb3d6a2f91c9a45[.]dancefloor[.]dev
- services[.]staging02[.]alfredstaging[.]com
- services[.]alec[.]dev[.]kolab[.]io
- services[.]1acb2f454f8fe76fd1893929c785e178[.]dancefloor[.]dev
- services[.]stg[.]spreadsimple[.]com
- services[.]mcom-166[.]tbe[.]zeus[.]fds[.]com
- services[.]dr[.]reputation-manager[.]it
- services[.]cc202e087fa83c34b0c738876aab7643[.]dancefloor[.]dev
- services[.]bcom-199[.]tbe[.]zeus[.]fds[.]com
- services[.]zingle[.]medallia[.]com
- services[.]calendar[.]events[.]ubc[.]ca
- services[.]runescape[.]rs-qw[.]xyz
- services[.]web01-prod[.]dak[.]xsarus[.]net
- services[.]data[.]dtenv[.]acceptatiedomein[.]nl

- services[.]external[.]s3-paris[.]vcp[.]vzwops[.]com
- services[.]sandbox[.]bcb[.]systems
- services[.]mpuk[.]baswareqa[.]com
- services[.]external[.]s11-branchburg[.]vcp[.]vzwops[.]com
- services[.]astoria[.]gexcp[.]com
- services[.]pinang-mikro[.]dev[.]rayain[.]net
- services[.]solutionforum[.]ntt-east[.]co[.]jp
- services[.]financeadm[.]bradesco[.]com[.]br
- services[.]runescape[.]com-rsp[.]cf
- services[.]meet[.]scaling[.]just1not2[.]org
- services[.]staging[.]lunchboxpos[.]io
- services[.]4c3710150869c1342aca82ba1d93c697[.]dancefloor[.]dev
- services[.]dclark[.]vero[.]dev[.]chakrayuk[.]co
- services[.]63ae9dc4cce3d0e3e6ff4dfc13d93419[.]dancefloor[.]dev
- services[.]f1ccd8009bdf20a1d43a65ec30bee696[.]dancefloor[.]dev
- services[.]jewelcandle[.]c[.]korekontrol[.]net
- services[.]waterapp[.]innovationm[.]com
- services[.]7eb48fcc1b2d3bbfa6c44e8907e13150[.]dancefloor[.]dev
- services[.]8396eea93334094b4531d82c6b9653c0[.]dancefloor[.]dev
- services[.]1cd9dd39338728a51fd2a5d06e97bb84[.]dancefloor[.]dev
- services[.]iot[.]kimclark[.]com
- services[.]uat-ext[.]vt[.]cnb[.]com
- services[.]1690c3275162cf69ea8ef93779dea7a3[.]dancefloor[.]dev
- services[.]250e4613b94f1f5e3bae73533559c4e4[.]dancefloor[.]dev
- services[.]39579624744c31fb69aa309b468cf2a3[.]dancefloor[.]dev
- services[.]prices[.]tctc[.]se
- services[.]east[.]eco[.]cloud[.]att[.]com
- services[.]cfaa1bf8b7927fb0542ae261809aa622[.]dancefloor[.]dev
- services[.]ca55aabff5a42c2840ac672a84d622c7[.]dancefloor[.]dev
- services[.]doh[.]rtsclients[.]com
- services[.]83a4b82652a016d96d4394a7a706394c[.]dancefloor[.]dev
- services[.]c04cbd1aa3d2310f6dd43256589e38cc[.]dancefloor[.]dev
- services[.]34084e181dc430522b592854028f449c[.]dancefloor[.]dev
- services[.]ikmz[.]uzh[.]ch
- services[.]2c9db8820fd607cc6a9c28a81085fa57[.]dancefloor[.]dev
- services[.]anz[.]virtusa[.]dev
- services[.]amazon[.]sellercentrass1[.]ddnsfree[.]com
- services[.]qa1ydl2[.]registeredsite[.]com
- services[.]dev02-magento[.]comune[.]askhuron[.]co
- services[.]amazon[.]sellersigseasdseller[.]camdvr[.]org
- services[.]amazon[.]ind778221[.]myddns[.]rocks
- services[.]cdn[.]jwplatform[.]com
- services[.]pl[.]marc-cain[.]com
- services[.]qld[.]gov[.]au[.]us3[.]cas[.]ms
- services[.]amer[.]staging[.]forcepoint[.]io
- services[.]journals[.]lww[.]com

- services[.]amazon[.]isdn213[.]giize[.]com
- services[.]amazon[.]asersellercentrals[.]kozow[.]com
- services[.]mpm[.]mp[.]br
- services[.]mkb[.]hu[.]tsok[.]cloudns[.]ph
- services[.]5[.]feature[.]trader[.]avus[.]io
- services[.]mcom-004[.]tbe[.]zeus[.]fds[.]com
- services[.]ekompas[.]dfm[.]nl
- services[.]xte1[.]klm[.]com
- services[.]test1[.]pc-rnd[.]salesforce[.]com
- services[.]staging[.]autoleague[.]io
- services[.]back[.]glap[.]h0st1ng[.]com
- services[.]la[.]utexas[.]edu
- services[.]external[.]dev[.]era[.]nih[.]gov
- services[.]chris-test4[.]nonprod[.]shorttrack[.]dev
- services[.]runescape[.]ca-in[.]cz
- services[.]runescape[.]com-ka[.]top
- service[.]com[.]lottery-tactics[.]com
- service[.]end-to-end-kpksx[.]xor[.]inpher[.]io
- service[.]stage[.]emcd[.]io
- service[.]api[.]us-west-2[.]devquinnn[.]events[.]aws[.]a2z[.]com
- service[.]ccd[.]woa[.]com
- service[.]end-to-end-hmoib[.]xor[.]inpher[.]io
- service[.]preprod[.]fbplatform[.]co[.]uk
- service[.]e2e-ewoyu[.]xor[.]inpher[.]io
- service[.]preview[.]ride2go[.]com
- service[.]managedstorage[.]sebollin[.]shock[.]games[.]aws[.]a2z[.]com
- service[.]forrester-staging[.]evidanza[.]cloud
- service[.]giftbox[.]kt[.]co[.]kr
- service[.]e2e-nefqp[.]xor[.]inpher[.]io
- service[.]management[.]business[.]avnisheshop[.]com
- service[.]external[.]anspacher[.]com
- service[.]lc-news[.]delmed[.]org
- service[.]interview[.]qagr[.]io
- service[.]staging[.]jiveworld[.]com
- service[.]old[.]alumeco[.]structtest[.]dk
- service[.]cleverest[.]martian[.]services
- service[.]open-platform[.]cs[.]shopee[.]com
- service[.]delta[.]tu-dortmund[.]de
- service[.]stronganswer[.]uclockit[.]com
- service[.]eu[.]prod[.]network-feasibility-authority[.]scot[.]a2z[.]com
- service[.]streetgovernerpilot[.]co[.]za[.]host-za[.]com
- service[.]e2e-ninfx[.]xor[.]inpher[.]io
- service[.]xgb-rgsw9[.]xor[.]inpher[.]io
- service[.]production[.]1673603712[.]us[.]east[.]1[.]elb[.]silevosolar[.]com
- service[.]apb[.]con[.]la
- service[.]stg[.]mungo[.]konekti[.]xyz
- service[.]e2e-kfcse[.]xor[.]inpher[.]io
- service[.]gcd[.]com[.]59259[.]com
- service[.]secure[.]buva[.]nl
- service[.]gcd[.]com[.]75216[.]com
- service[.]gcd[.]com[.]28636[.]com
- service[.]gcd[.]com[.]37989[.]com
- service[.]gcd[.]com[.]55606[.]com
- service[.]map02[.]wirelesscity[.]jp
- service[.]gcd[.]com[.]37709[.]com
- service[.]gcd[.]com[.]96551[.]com
- service[.]dev[.]dxl-vf[.]de

- service[.]lab7[.]cpsudevops[.]com
- service[.]hb[.]10086[.]cn
- service[.]coprint-t[.]eu-central-1[.]aws[.]cloud[.]bmw
- service[.]app[.]agakura[.]io
- service[.]kdr-group[.]od[.]ua
- service[.]bp[.]tasdemo[.]xyz
- service[.]dev[.]cpt[.]firstam[.]com
- service[.]mpn[.]minienm[.]nl
- service[.]clc[.]telnet[.]sk
- service[.]subject[.]cqvip[.]com
- service[.]messaging[.]feature01[.]dnevnik[.]ru
- service[.]mantle-mgmt[.]stp[.]hmlr[.]zone
- service[.]plantproductivity[.]henkelgroup[.]cloud
- service[.]privacy-bbva[.]aiwin[.]co
- service[.]app[.]render[.]com
- service[.]us-east-1[.]discovery[.]gg[.]amazon[.]dev
- service[.]api[.]sample[.]dev[.]carrier[.]io
- service[.]hipaa[.]datalot[.]com
- service[.]logging[.]workingsystems[.]com
- service[.]stage[.]tripmakery[.]com
- service[.]qa[.]enduranceapi[.]com
- service[.]console[.]ubutouch[.]com
- service[.]eu[.]teamretro[.]sandbox[.]groupmap[.]com
- service[.]msp[.]dev[.]ec[.]sulzer-us[.]com
- service[.]stormsystems[.]brandshake[.]nl
- service[.]ocrm[.]student[.]bcschool[.]cn
- service[.]student[.]bcschool[.]cn
- service[.]um-leak[.]office[.]almaware[.]net
- service[.]8238[.]mold-corponews[.]pics
- service[.]bnym[.]xor[.]inpher[.]io
- service[.]qq[.]com[.]hongransunny[.]com
- service[.]ngok[.]techsoupglobal[.]org
- service[.]alpha[.]elkhorn[.]ec2[.]aws[.]dev
- service[.]preview[.]standaard[.]be
- service[.]pdpm[.]mojoerp[.]com
- service[.]tst[.]devopstest[.]konekti[.]xyz
- service[.]demo[.]ashiaap[.]com
- service[.]dev[.]nanai[.]amihan[.]net
- service[.]sd[.]10086[.]cn[.]c[.]cdn[.]chinamobile[.]com
- service[.]ekata[.]preprod[.]esprinumerique[.]fr
- service[.]test[.]dexswipe[.]com
- service[.]paypal[.]com[.]secureservice09[.]information82[.]lpsashokvihar[.]com
- service[.]modern[.]cv[.]ua
- service[.]c52dddf4a9ec499d992a[.]westeurope[.]aksapp[.]io
- service[.]sign[.]accounit[.]magassecurityyz[.]me
- service[.]qa[.]menards[.]com
- service[.]mcs[.]preprod[.]tafenswtest[.]edu[.]au
- service[.]bjoerngit[.]evidanza[.]cloud
- service[.]delta[.]lg[.]ua
- service[.]paulngyn[.]alpha[.]mindil[.]dubai[.]aws[.]dev
- service[.]crm-bulk-update[.]dev[.]office[.]n360[.]io
- service[.]blogs[.]rub[.]de
- service[.]agent[.]foxylion11[.]com
- service[.]abr[.]lazio[.]it

- service[.]b7c6b33[.]pr[.]accredion[.]com
- service[.]bank[.]islandsbanki[.]forgerock[.]financial
- service[.]c04567f[.]pr[.]accredion[.]com
- service[.]babyhood35[.]hasura-app[.]io
- service[.]broadcast[.]bit[.]te[.]ua
- max[.]sch[.]bme[.]hu
- max[.]on[.]friday[.]lottery-tactics[.]com
- max[.]boot[.]oyuncuhaberler[.]xyz
- max[.]demo[.]odoo[.]niboo[.]ovh
- max[.]guerrero[.]basic[.]space
- max[.]v2202005217271189 81[.]ultrasrv[.]de
- max[.]test[.]wizjanet[.]pl
- max[.]wmrose[.]mtcdevserver6[.]com
- max[.]bx17959[.]rdock[.]ru
- max[.]anz[.]eu[.]cas[.]ms
- max[.]dev[.]vavoo[.]net
- max[.]amm[.]ru[.]ac[.]za
- max[.]auch[.]simplon[.]me
- max[.]bi[.]fraunhofer[.]de
- max[.]cc-com[.]affrc[.]go[.]jp
- max[.]chemie[.]hu-berlin[.]de
- max[.]cms[.]hu-berlin[.]de
- max[.]dci[.]pomona[.]edu
- max[.]dorm6[.]nccu[.]edu[.]tw
- max[.]dynamic[.]ucsd[.]edu
- max[.]ece[.]ufl[.]edu
- max[.]graz[.]inode[.]at
- max[.]hex[.]dev[.]splinestudio[.]com
- max[.]iic[.]hokudai[.]ac[.]jp
- max[.]informatik[.]tu-ilmenau[.]de
- max[.]infr[.]tawherotech[.]nz
- max[.]ist[.]flinders[.]edu[.]au
- max[.]ma[.]utexas[.]edu
- max[.]main[.]tpu[.]ru
- max[.]mpi-klsb[.]mpg[.]de
- max[.]staging[.]small2big[.]com
- max[.]state[.]ia[.]us
- max[.]nyw[.]gupiao3158[.]cn
- max[.]paedgymge[.]hf[.]uni-koeln[.]de
- max[.]papy[.]uni-heidelberg[.]de
- max[.]pjl[.]ucalgary[.]ca
- max[.]qui[.]uam[.]es
- max[.]sinp[.]msu[.]ru
- max[.]storage[.]msn-ppe[.]com
- max[.]tka[.]mfwdk[.]com
- max[.]webid[.]jolocom[.]de
- max[.]wordpress[.]oxiddemo[.]com
- max[.]www[.]23369[.]tw
- max[.]www[.]2502969[.]loan
- max[.]www[.]4742866[.]loan
- max[.]www[.]6247011[.]loan
- max[.]www[.]7084173[.]loan
- max[.]www[.]7719115[.]loan
- max[.]www[.]7795872[.]loan
- max[.]www[.]8226258[.]loan
- max[.]www[.]95245[.]tw
- max[.]www[.]dzi4jzy[.]tw
- max[.]www[.]gdbwol[.]loan
- max[.]www[.]lrinzb[.]top
- max[.]www[.]lzczof[.]top
- max[.]www[.]pc[.]2158129[.]loan
- max[.]www[.]pc[.]9200918[.]loan
- max[.]www[.]wsetml[.]top
- max[.]www[.]xrcevy[.]top
- max[.]www[.]yeari2o[.]tw
- max[.]www[.]ygvklj[.]top
- max[.]xyz[.]xyz2014[.]info
- max[.]zay[.]wajin13[.]com
- max[.]zoom[.]to[.]ivirus[.]ru
- max[.]celebration[.]larosarealty[.]com
- max[.]fsim[.]paleto[.]de
- max[.]www[.]19549964[.]cn

- max[.]www[.]1650872[.]loan
- max[.]www[.]1361002[.]loan
- max[.]ioc[.]fiocruz[.]br
- max[.]demo[.]filetransit[.]com
- max[.]public[.]edrd2[.]int10h[.]net
- max[.]tour[.]nacnot[.]com
- max[.]sta[.]mode[.]io
- max[.]mytendays[.]shamaazi[.]io
- max[.]dev[.]my-prtg[.]com
- max[.]dawson[.]lab[.]go4labs[.]net
- max[.]educa[.]madrid[.]org
- max[.]exlog[.]mtcdevserver5[.]com
- max[.]schon[.]jelgava[.]dsl[.]microlink[.]lv
- max[.]earth[.]orderbox-dns[.]com
- max[.]www[.]love[.]odnoklassniki[.]armworld[.]ru
- max[.]strathmore-foods[.]mtcdevserver6[.]com
- max[.]dev[.]boyzinthecloud[.]nl
- max[.]di[.]diedasweb[.]at
- max[.]staging4[.]emperium[.]net
- max[.]paalvast[.]flexvakken[.]nl
- max[.]dev[.]gametailors[.]com
- max[.]mueller[.]fls-hi[.]shop
- max[.]acc[.]coronacheck[.]nl
- max[.]lubor[.]qa[.]odkarla[.]cz
- max[.]beta3[.]qa[.]odkarla[.]cz
- max[.]development[.]uk[.]syrahost[.]com
- max[.]www[.]iwpndw[.]loan
- max[.]www[.]0452095[.]loan
- max[.]hubstores[.]mulgoapastoral[.]net
- max[.]shadow[.]ctmers[.]io
- max[.]student[.]8x8[.]uk
- max[.]book[.]118[.]cl
- max[.]anew[.]does-it[.]net
- files[.]hazgo[.]test[.]digitaltalents[.]be
- files[.]engage[.]voc[.]cloud
- files[.]jozefien[.]dco2[.]robovision[.]ai
- files[.]bakkerijkenis[.]preview[.]digitaltalents[.]be
- files[.]javateam[.]intranet[.]beone-group[.]com
- files[.]shop201548[.]inventshop[.]cz
- files[.]pfwall[.]linkpc[.]net
- files[.]pr-1234[.]preview[.]smythcasting[.]co
- files[.]beatrice[.]k313[.]xyz
- files[.]www[.]vissen[.]tv
- files[.]lotta-fra-brakmakergata[.]webnode[.]com
- files[.]darkxweb[.]co[.]cc
- files[.]parrocchiacrespellano[.]webnode[.]it
- files[.]strednygemer[.]webnode[.]sk
- files[.]f[.]myname[.]life
- files[.]africanstudies[.]webnode[.]com
- files[.]urshaberstroh[.]webnode[.]com
- files[.]tombruins[.]webnode[.]com
- files[.]ampaortegaygasset[.]webnode[.]es
- files[.]cultural-intertexts[.]webnode[.]com
- files[.]iespabloneruda[.]webnode[.]es
- files[.]ctau[.]webnode[.]tw
- files[.]autoconfig[.]old[.]qiantaiweb[.]pjinbfskfund[.]xyz
- files[.]thelodge[.]geoconsensus[.]com
- files[.]public[.]sitebuilder[.]systems
- files[.]designer[.]loginserver[.]ch
- files[.]picturebox[.]bpglobal[.]com
- files[.]dev[.]cvcreate[.]culteer[.]com
- files[.]qa[.]mailstoretest[.]com
- files[.]home[.]hiems[.]net
- files[.]erp[.]vntm[.]vn

- files[.]edubbs[.]duckdns[.]org
- files[.]anacibg[.]coriweb[.]it
- files[.]cdn[.]croak[.]me
- files[.]dev[.]design-bureau[.]ru
- files[.]politielrhwebshop[.]test[.]qustomized-beta[.]be
- files[.]api[.]test[.]computo[.]io
- files[.]notes[.]sysctl[.]io
- files[.]instance6[.]grandus[.]sk
- files[.]services[.]redsmart[.]group
- files[.]sharptooth[.]synology[.]me
- files[.]locipo[.]com[.]id159[.]jocdn[.]jp
- files[.]monstersinc[.]ghosthost[.]live
- files[.]autodiscover[.]zqq0512[.]test[.]shopplus[.]vip
- files[.]geease[.]com[.]w[.]kunlunpi[.]com
- files[.]4creative[.]4tech[.]mobi
- files[.]bd[.]dev[.]repon[.]io
- files[.]preprod-ru[.]adc-lv[.]io
- files[.]staging2[.]sorting[.]tech
- files[.]integration[.]sellergeni[.]com
- files[.]wbk[.]ch-dns[.]net
- files[.]up[.]melem[.]at
- files[.]stage[.]therapy[.]khealth[.]com
- files[.]aph[.]austintexas[.]gov
- files[.]vimyfoundation[.]ca[.]s3[.]amazonaws[.]com
- files[.]schnauzer[.]ipolos[.]nl
- files[.]azure[.]chomba[.]xyz
- files[.]kjarvis[.]duckdns[.]org
- files[.]lursa[.]imposter[.]cz
- files[.]shop201659[.]inventshop[.]cz
- files[.]imaginelife[.]keenetic[.]pro
- files[.]translation-studies[.]webnode[.]ro
- files[.]pkf3[.]webnode[.]es
- files[.]biercontract-nl8[.]webnode[.]nl
- files[.]biogrundl2[.]webnode[.]es
- files[.]news[.]ontario[.]ca[.]s3-website-us-east-1[.]amazonaws[.]com
- files[.]schrijfmotoriek-com[.]webnode[.]nl
- files[.]fpoe-badischl-info[.]webnode[.]com
- files[.]labtopope[.]webnode[.]com
- files[.]athletes-celebrities[.]tseworld[.]com
- files[.]cayetanoarroyo[.]webnode[.]com
- files[.]biblioteca-espaco-digital1[.]webnode[.]com
- files[.]pb-2661[.]qa[.]gpblog[.]com
- files[.]phite[.]cn[.]w[.]kunlunca[.]com
- files[.]gameplayer[.]games[.]dmm[.]com
- files[.]local[.]echo[.]tn
- files[.]hjlx[.]jiauxuan[.]com
- files[.]hok[.]lobby2[.]app
- files[.]hok[.]tripleplay[.]ai
- files[.]api[.]pactima[.]com
- files[.]show[.]51minsheng[.]com
- files[.]tyler[.]lobby2[.]app
- files[.]storage[.]ibmz[.]awan[.]io
- files[.]ysg[.]dao991[.]com
- files[.]intranet[.]abnahme[.]dvag
- files[.]int[.]cxmgmt[.]ai
- files[.]nfter[.]eu[.]org
- files[.]5mot[.]neacon[.]eu
- files[.]coinframe[.]secreate[.]dev
- files[.]bus-en-coach[.]digitalstock[.]be
- files[.]vs-web[.]net[.]vs-dn09[.]net
- files[.]flbbzh[.]hopto[.]org
- files[.]jade[.]indgo[.]com[.]br
- files[.]jabba[.]dscloud[.]me
- files[.]c12net[.]tapras[.]jp
- files[.]forms[.]api[.]labq[.]com
- files[.]tenant-sa-1[.]oneclick[.]es

- files[.]gamerdad[.]ghosthost[.]live
- files[.]sitebuilder[.]baukasten[.]at
- files[.]help[.]bloomgrowth[.]com
- analysis[.]internal[.]cajalneuro[.]com
- analysis[.]dev[.]bloomberg[.]com
- analysis[.]mortgage[.]suggestsoft[.]com
- analysis[.]it[.]gwu[.]edu
- analysis[.]tomato[.]vocinno[.]com
- analysis[.]sp[.]dqmp[.]jp
- analysis[.]biol[.]uvic[.]ca
- analysis[.]tuanimg[.]com[.]wscdns[.]com
- analysis[.]78[.]46[.]83[.]200[.]xip[.]io
- analysis[.]aomygod[.]com[.]wswebpic[.]com
- analysis[.]checkout[.]teste[.]tray[.]net[.]br
- analysis[.]stg[.]zamby[.]jp
- analysis[.]freeware[.]filetransit[.]com
- analysis[.]cn[.]chowis[.]com
- analysis[.]blog-sign[.]mixh[.]jp
- analysis[.]cn-hangzhou[.]alipay-cdn[.]aliyun-inc[.]com
- analysis[.]shadow[.]ctmers[.]io
- analysis[.]gamma[.]diffypop[.]hweng[.]aws[.]dev
- analysis[.]live[.]sumelongenterprise[.]com
- analysis[.]stg[.]vcrm[.]dev
- analysis[.]ext-1[.]test[.]co[.]egym[.]coffee
- analysis[.]sp[.]am[.]whill[.]cloud
- analysis[.]mcm[.]skoda-auto[.]com
- analysis[.]databaseforyou[.]cerved[.]com
- analysis[.]us[.]lastline[.]com
- analysis[.]intech[.]gdinsight[.]com
- analysis[.]ces[.]nexpando[.]com
- analysis[.]afgslb[.]afreecatv[.]com
- analysis[.]platformservices[.]co[.]uk[.]edgekey[.]net
- analysis[.]kist[.]re[.]kr
- analysis[.]stage[.]volleymetrics[.]com
- analysis[.]narzissmus[.]zortify[.]com
- analysis[.]lastline[.]com[.]maloneyproperties[.]com
- analysis[.]med[.]realbio[.]cn
- analysis[.]flights[.]localadventures[.]io
- analysis[.]dev[.]bmw[.]evotrq[.]com
- analysis[.]opti[.]suedcode[.]de
- analysis[.]252776298826[.]beta[.]diffypop[.]hweng[.]aws[.]dev
- analysis[.]api[.]rosepetal[.]ai
- analysis[.]amaula[.]dev[.]kubioscloud[.]com
- analysis[.]gl-8[.]test[.]co[.]egym[.]coffee
- analysis[.]math[.]ualberta[.]ca
- analysis[.]interlabs[.]spb[.]ru
- analysis[.]node2[.]hellohey[.]top
- analysis[.]path-neuro[.]med[.]uni-goettingen[.]de
- analysis[.]tyai[.]tyc[.]edu[.]tw
- analysis[.]50[.]116[.]84[.]142[.]sslip[.]io
- analysis[.]kostat[.]go[.]kr
- analysis[.]oxfordjournals[.]org[.]ezproxy[.]baylor[.]edu
- analysis[.]see-port[.]intage[.]co[.]jp
- analysis[.]southindia[.]cloudapp[.]azure[.]com
- analysis[.]suborbital[.]dfrc[.]nasa[.]gov
- analysis[.]hnr[.]cn[.]wsssec[.]com
- analysis[.]crocker[.]ucdavis[.]edu
- analysis[.]group[.]iteye[.]com
- analysis[.]ameriquest[.]suggestsoft[.]com

- analysis[.]mesothelioma[.]suggestsoft[.]com
- analysis[.]dev[.]vatlab[.]com
- analysis[.]backup[.]rangni[.]cn
- analysis[.]dev[.]drbfm[.]toyota[.]com
- analysis[.]stg-1[.]qa[.]gcp[.]netpulse[.]com
- analysis[.]np-4[.]qa[.]gcp[.]netpulse[.]com
- analysis[.]travelmentor[.]in[.]net
- analysis[.]qa[.]ceon-dev[.]io
- analysis[.]univer[.]kharkov[.]ua
- analysis[.]test[.]bmw[.]evotrq[.]com
- analysis[.]trusk[.]com[.]s[.]strikinglydns[.]com
- analysis[.]gl-3[.]test[.]co[.]egym[.]coffee
- analysis[.]linyi[.]ftagricloud[.]com
- analysis[.]release[.]impect[.]com
- analysis[.]openvpn[.]stevensbeek[.]com
- analysis[.]preview[.]archerdx[.]com
- analysis[.]sts[.]apiad[.]cs[.]scania[.]com
- analysis[.]lon[.]prod[.]theplatform[.]eu
- analysis[.]sub2[.]rikunabi[.]com
- analysis[.]rads[.]optum[.]com
- analysis[.]dev[.]zamby[.]jp
- analysis[.]api[.]huichiyo[.]com
- analysis[.]repgrid[.]dev[.]rotecag[.]com
- analysis[.]agent[.]aishitui[.]cn
- analysis[.]crowdsense-eu[.]teratrace[.]net
- analysis[.]dic[.]cit[.]nihon-u[.]ac[.]jp
- analysis[.]am[.]nttdata-sec[.]com
- analysis[.]legacy[.]notprod[.]dq[.]homeoffice[.]gov[.]uk
- analysis[.]ericrobinson[.]repl[.]run
- analysis[.]expertwitness[.]freereferral[.]com
- analysis[.]qa[.]manceon[.]io
- analysis[.]tam[.]test[.]ricetec[.]com
- analysis[.]cloud[.]dev[.]asoc[.]argus-sec[.]com
- analysis[.]pms[.]vara[.]ai
- analysis[.]dyt[.]connxusdemo[.]com
- analysis[.]aws[.]forum[.]ibood[.]com
- analysis[.]us-east-1[.]alpha[.]fleet-advisor[.]nautilus[.]aws[.]dev
- analysis[.]prod[.]fleet-advisor[.]nautilus[.]aws[.]dev
- analysis[.]service[.]makarxr[.]cn
- analysis[.]math[.]unibas[.]ch
- analysis[.]software[.]filedudes[.]com
- analysis[.]groups[.]newsvine[.]com
- analysis[.]notprod[.]dq[.]homeoffice[.]gov[.]uk
- analysis[.]sa-east-1[.]prod[.]fleet-advisor[.]nautilus[.]aws[.]dev

C&C サーバのドメイン名と同じ文字列を持つ悪意あるドメインとサブドメインの例

- services[.]runescape[.]com-kz[.]top
- services[.]ird[.]govt[.]nz[.]pahaditrails[.]com
- services[.]cash[.]app-account-support[.]dispute-ticket[.]de
- services[.]runescape[.]rs-er[.]xyz

- services[.]ui-my773[.]is-certified[.]com
- services[.]a99372ama88zo23n[.]webhop[.]info
- services[.]myargoscard[.]tintbyrita[.]com
- services[.]runescape[.]com-i[.]cz
- services[.]runescape[.]com-sup[.]xyz
- services[.]myappbilling[.]configured[.]presencecopration[.]com
- services[.]google[.]com[.]brunocpa[.]com
- services[.]runescape[.]com-r[.]ws
- services[.]u7558345ef[.]ha004[.]t[.]justns[.]ru
- services[.]amazon[.]co[.]uk[.]nongchokfci[.]com
- services[.]runescape[.]com-fr[.]cz
- services[.]swiftalmahid[.]mavsm[.]com
- services[.]onligne[.]sherock-online[.]com
- services[.]runescape[.]com-re[.]xyz
- services[.]runescape[.]com-j[.]ws
- services[.]runescape[.]com-un[.]cc

2022 年の人気ビジネスチャットアプリのブランド名が含まれているドメイン名の例

- slack[.]chat
- slackchat[.]me
- slackchat[.]us
- unslack[.]chat
- slacker[.]chat
- slackchat[.]tk
- slackchat[.]io
- slackcat[.]chat
- slackchat[.]com
- chatslack[.]com
- slackchat[.]dev
- slackoff[.]chat
- slackchat[.]net
- slackchat[.]host
- slackchats[.]com
- slackchats[.]net
- slackychat[.]com
- chat-slack[.]com
- slackchat[.]info
- chatslacker[.]com
- slacktochat[.]com
- slackchats[.]blog
- slackerchat[.]com
- slackandchat[.]com
- slackchatter[.]com
- chatbotslack[.]com
- slackchatbot[.]com
- slacklivechat[.]com
- hipchatvslack[.]com
- slackchatbots[.]com
- slackimation[.]chat
- slackchatroom[.]com
- slackfakechat[.]xyz
- slackchatrooms[.]com
- slackvshipchat[.]com
- hipchatvsslack[.]com
- slackchatpodcast[.]com
- arelrajchatoslack[.]tk
- ecommerceslackchat[.]com
- slackchatconfessional[.]com
- microsofteams[.]ir
- microsofteams[.]tk
- microsofteams[.]cn
- microsofteams[.]au
- microsofteams[.]nl
- microsofteams[.]ga

- microsoftteams[.]uk
- microsoftteams[.]ru
- microsoftteams[.]ws
- microsoftteams[.]it
- teamsmicrosoft[.]ml
- microsoftteams[.]fr
- microsoftteams[.]in
- microsoftteams[.]us
- microsoftteams[.]se
- microsoftteams[.]me
- microsoftteams[.]cz
- microsofteams[.]com
- microsoftteams[.]ie
- microsoftteams[.]co
- microsoftteams[.]ca
- teamsmicrosoft[.]cf
- teamsmicrosoft[.]ru
- microsoftteams[.]io
- microsoftteams[.]nl
- microsoftteams[.]dk
- teamsmicrosoft[.]uk
- microsoftteams[.]es
- microsoftteams[.]ir
- microsoftteams[.]cc
- teamsmicrosoft[.]se
- teamsmicrosoft[.]co
- microsoftteams[.]de
- microsoft-teams[.]co
- teams-microsoft[.]fr
- microsoftteams[.]fun
- microsoft-teams[.]cz
- microsoft-teams[.]es
- microsoftteams[.]xyz
- microsoft-teams[.]nl
- teamsmicrosoft[.]net
- microsoft-teams[.]in
- teams-microsoft[.]ru
- teamsmicrosoft[.]com
- microsoft-teams[.]fr
- teams-microsoft[.]pl
- microsoft-teams[.]de
- microsoft-teams[.]eu
- microsoftteams[.]dev
- xn--mcrosoft-teams-0lb[.]me
- microsoft-teams[.]ch
- microsoftteams[.]top
- teams-microsoft[.]ga
- microsofteams[.]team
- teams-microsoft[.]nl
- microsoftteams[.]app
- microsoft-teams[.]gq
- microsoft-teams[.]pl
- microsoftteams[.]org
- microsoft-teams[.]ml

2022 年の人気ビジネスチャットアプリのブランド名が含まれている悪意あるドメインの例

- microsoftteams[.]fun
- microsoftteams[.]top
- discord-chatbot[.]tk
- discordchatterscommunity[.]com