WhoisXMLAPI
The Who Behind Domain, IP & Cyber Threat Intelligence

GALLIUM APT Group and Other Threat Actors in Disguise

Table of Contents

Executive Report

Two cyber threats recently caught the attention of WhoisXML API researchers, primarily since parts of their infection chain hide behind legitimate services. This tactic is tricky for security teams because blocking the domains involved means blocking legitimate applications, too.

First is the GALLIUM APT Group, which was found using a new remote access Trojan (RAT). Indicators of compromise (IoCs) included 13 domains and 130 IP addresses. Three domains were hosted on a free dynamic DNS service with the domain publicvm[.]com. Another threat uses fake Facebook login pages, enabling actors to steal 1 million credentials in just four months. The first link victims clicked were subdomains of legitimate app deployment services, such as glitch[.]me, famous[.]co, and amaze[.]co.

This research focused on subdomains belonging to the legitimate root domains involved in the two threats mentioned above. Among our findings include:

- 14,000+ subdomains belonging to the four root domains added for all time, 63% of which are glitch[.]me subdomains added since 1 June 2022
- 3% of the total sample has been flagged as malicious by various malware engines
- Common text strings used in the malicious subdomains include those that invoke authority, such as “cpanel,” “cpcontacts,” “webdisk,” and “cpcalendars”
- Some subdomains hosted suspicious content, such as login and look-alike pages

Data Sample Distribution and Analysis

We uncovered 14,517 subdomains belonging to only four root domains—publicvm[.]com, glitch[.]me, famous[.]co, and amaze[.]co. A majority of the properties were under publicvm[.]com and glitch[.]me, 63% of which were new, having been added only since 1 June 2022.

Included in the data sample are 174 glitch[.]me subdomains that contain Facebook-related domains, such as “facebook,” “meta,” “instagram,” and “whatsapp.” Apart from these strings, some of the most common ones used in the subdomains were “cpanel,” “cpcontacts,” “webdisk,” “cpcalendars,” “login,” “webmail,” and “mail.” These are reflected in the word cloud below.

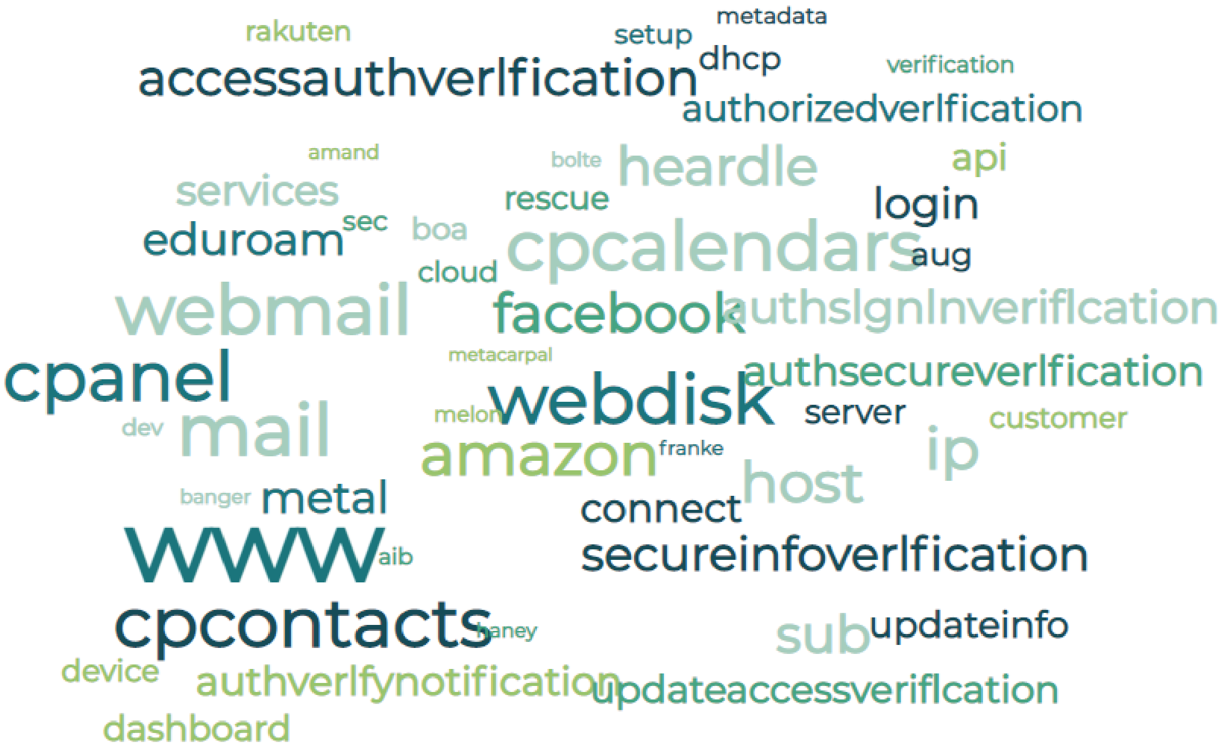


Image 1: *Word cloud showing the most common text strings used in the subdomains*

How Malicious Are the Subdomains?

We ran a bulk malware check on the data sample and found that 3.36% of the subdomains have been reported as malicious. Lexical analysis of these dangerous cyber resources yielded interesting results since most of the commonly used text strings also appeared in the nonmalicious subdomains.

The word cloud below shows similar strings found among the data sample, including “cpanel,” “cpcontacts,” “webdisk,” “cpcalendars,” “amazon,” and “login.”

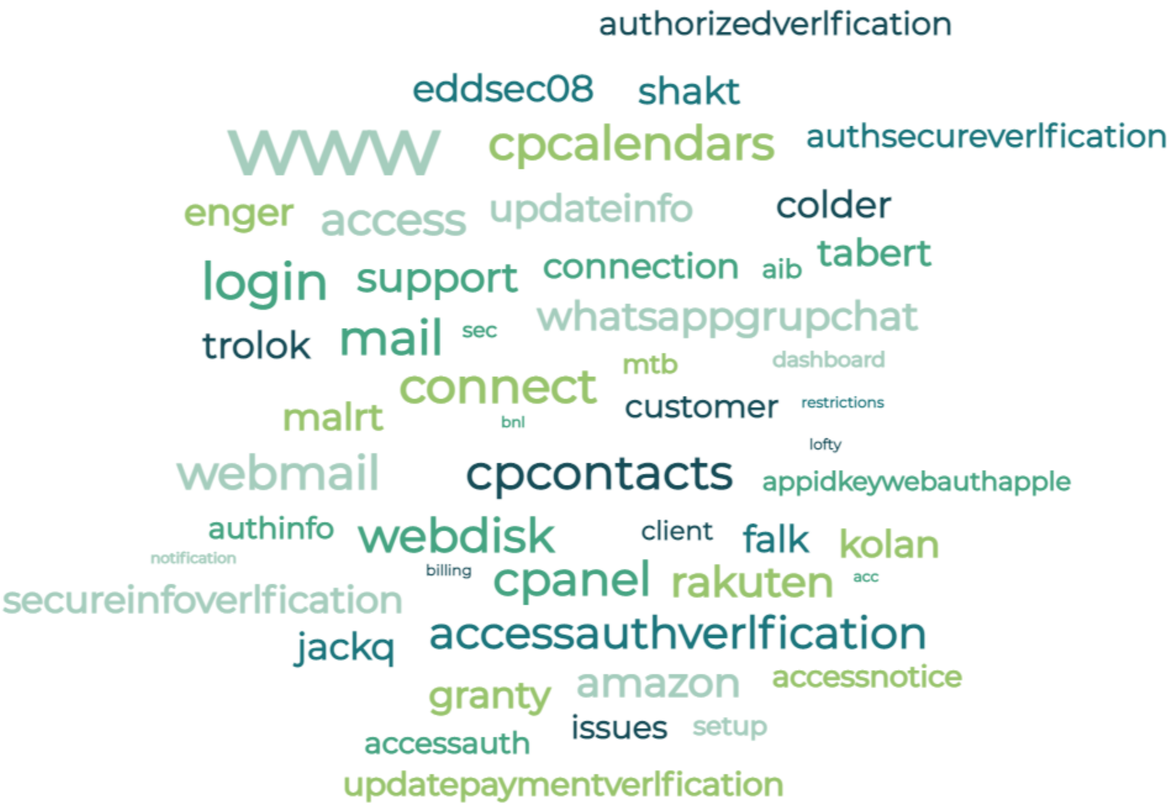
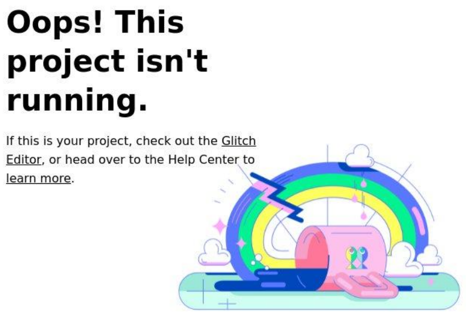
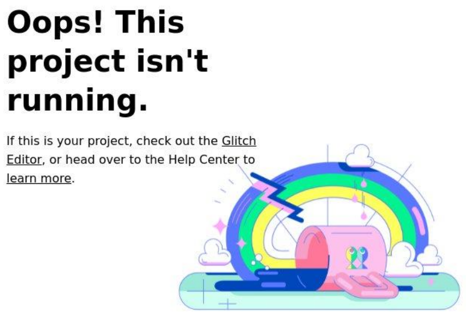
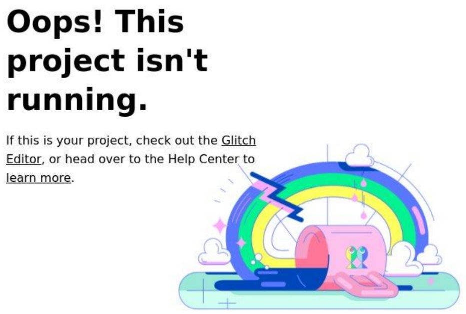
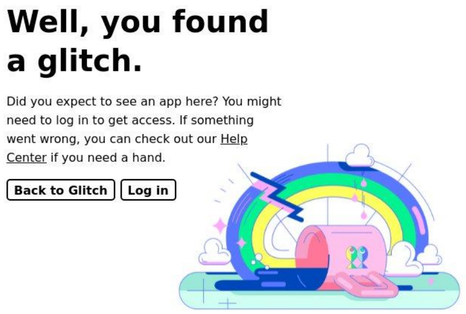


Image 2: *Word cloud showing the most common text strings used in the malicious subdomains*

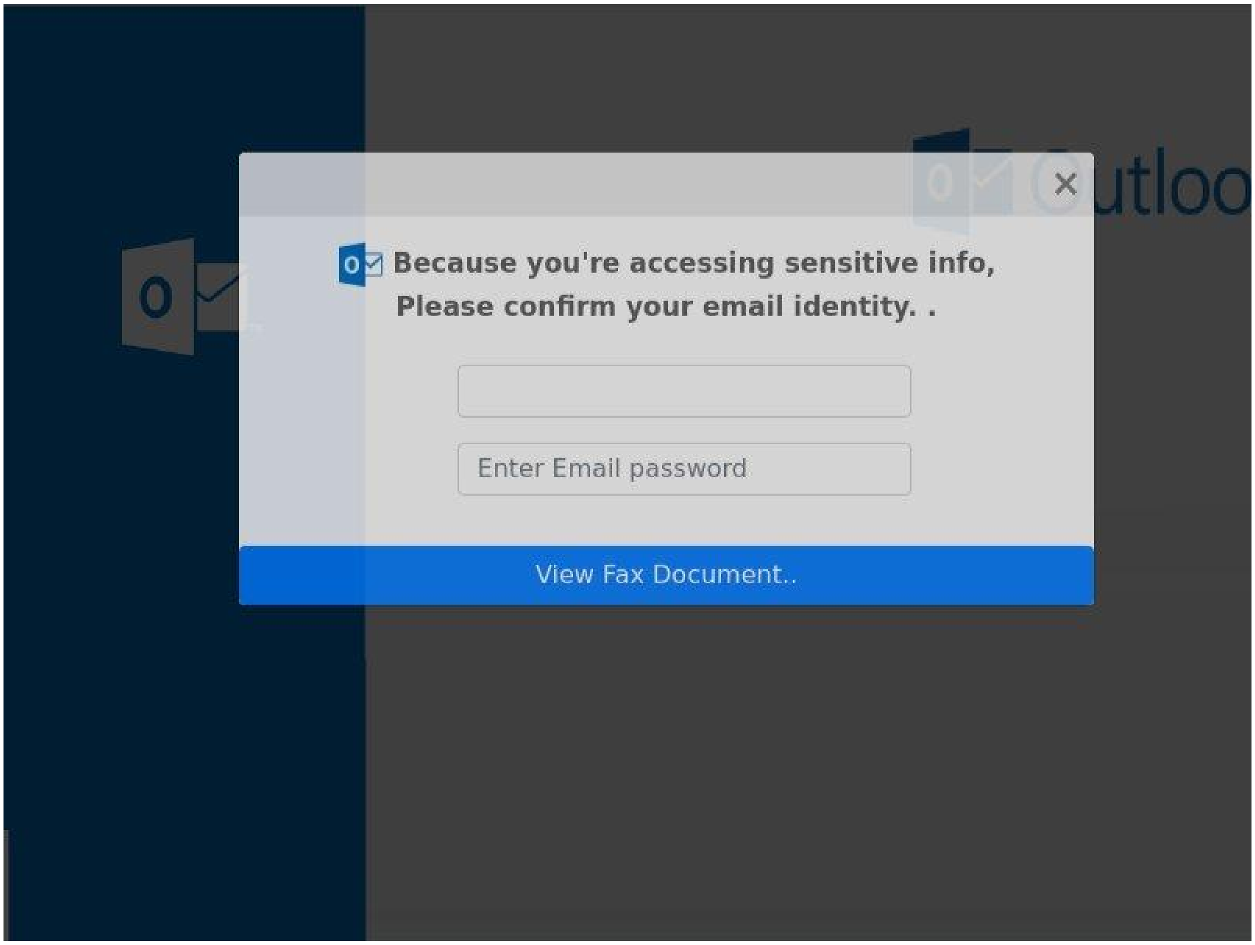
The findings brought to light the possibility of several unreported malicious subdomains.

What Types of Content Do the Properties Host?

Our screenshot analysis suggests that threat actors may be waiting for the right time to weaponize some of the properties. Or those may no longer be active, and possibly were already taken down by the subdomain addition service provider. For instance, the website screenshots of several Facebook-related glitch[.]me subdomains show they were linked to inactive projects. Some examples are shown below.

 **Oops! This project isn't running.** If this is your project, check out the Glitch Editor, or head over to the Help Center to learn more. *Screenshot of facebook9029*[.]*glitch*[.]*me*	 **Oops! This project isn't running.** If this is your project, check out the Glitch Editor, or head over to the Help Center to learn more. *Screenshot of facebook9032*[.]*glitch*[.]*me*
 **Oops! This project isn't running.** If this is your project, check out the Glitch Editor, or head over to the Help Center to learn more. *Screenshot of facebook409324*[.]*glitch*[.]*me*	 **Well, you found a glitch.** Did you expect to see an app here? You might need to log in to get access. If something went wrong, you can check out our Help Center if you need a hand. Back to Glitch Log in *Screenshot of facebook[.]boatneck-tamarillo-t8kh1ji2ev[.]glitch[.]me*

Other subdomains hosted Nextcloud, Roundcube, and other platforms' login pages. Some of these could be fronts for credential theft. An example is metal-absorbing-fly[.]glitch[.]me, which hosts a login page similar to that of Microsoft Outlook.

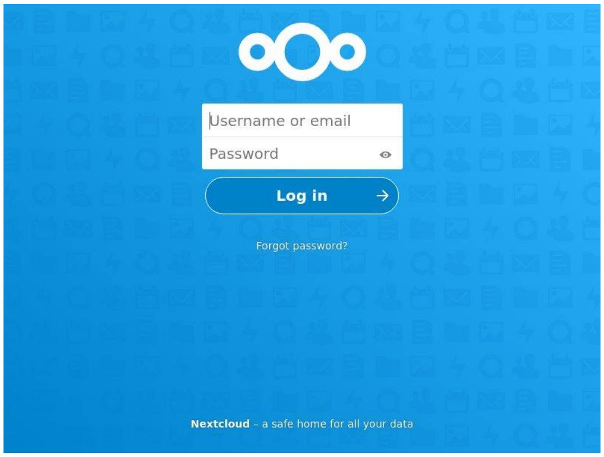
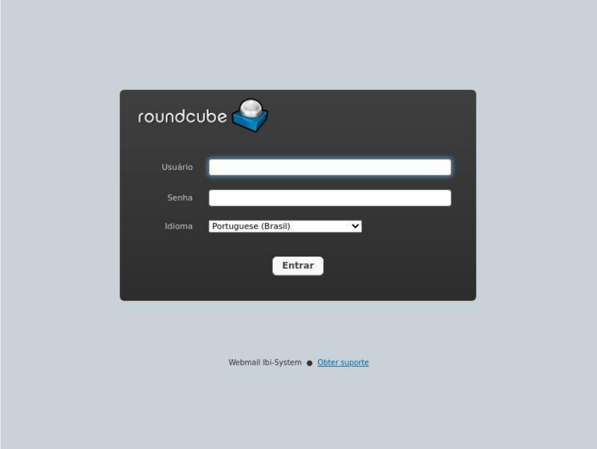


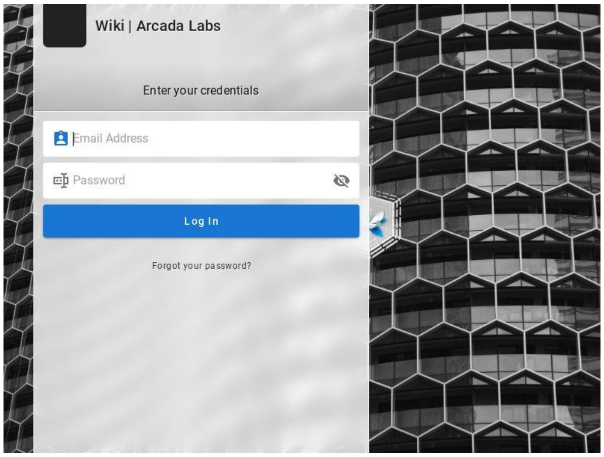
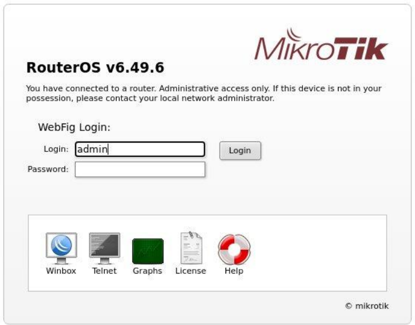
Because you're accessing sensitive info, Please confirm your email identity. .

Enter Email password

Screenshot of metal-absorbing-fly[.]glitch[.]me

On the other hand, other subdomains could be legitimate pages created by nonmalicious individuals and organizations. Even so, if these are services meant for internal network use, they could be vulnerable to brute force attacks. A few examples are shown below.

 Username or email Password Log in Forgot password? **Nextcloud** – a safe home for all your data	 roundcube Usuário Senha Idioma Portuguese (Brasil) Entrar Webmail Ibi-System ● Obter suporte

Screenshot of nextfigit[.]publicvm[.]com	*Screenshot of scuddcw[.]publicvm[.]com*
 Wiki | Arcada Labs Enter your credentials Email Address Password Log In Forgot your password? *Screenshot of www[.]lapess[.]publicvm[.]com*	 MikroTik RouterOS v6.49.6 You have connected to a router. Administrative access only. If this device is not in your possession, please contact your local network administrator. WebFig Login: Login: admin Password: Login Winbox Telnet Graphs License Help © mikrotik *Screenshot of www[.]casamiabodegon[.]publicvm[.]com*

There are many ways threat actors can lure victims into giving up their sensitive user information, but this almost always involves clicking a malicious link. That link could lead to cybersquatting domains, domain generation algorithm (DGA-) generated domains, or long-form URLs residing on legitimate root domains.

Comprehensive access to domain intelligence can help detect suspicious properties early and prevent threats, such as those posed by GALLIUM and the actors behind the massive Facebook user credential theft.

If you wish to perform a similar investigation or research, please don't hesitate to contact us. We're always on the lookout for potential research collaborations.

Appendix: Sample IoCs and Artifacts

GALLIUM APT Group IoCs

- df[.]micfkbeljacob[.]com
- t1[.]hinitial[.]com
- micfkbeljacob[.]com
- jack[.]micfkbeljacob[.]com
- hinitial[.]com
- v2[.]hinitial[.]com
- v3[.]hinitial[.]com
- v4[.]hinitial[.]com
- v5[.]hinitial[.]com
- goodjob36[.]publicvm[.]com
- goodluck23[.]jp[.]us
- helpinfo[.]publicvm[.]com

- mailedc[.]publicvm[.]com
- 5[.]181[.]25[.]55
- 92[.]38[.]135[.]62
- 5[.]8[.]71[.]97
- 92[.]38[.]135[.][.]62
- 101[.]36[.]102[.]34
- 101[.]36[.]102[.]93
- 101[.]36[.]114[.]167
- 101[.]36[.]123[.]191
- 103[.]116[.]47[.]65
- 103[.]179[.]188[.]93
- 103[.]22[.]183[.]131
- 103[.]22[.]183[.]138
- 103[.]22[.]183[.]141
- 103[.]22[.]183[.]146
- 103[.]51[.]145[.]143
- 103[.]61[.]139[.]71
- 103[.]61[.]139[.]72
- 103[.]61[.]139[.]75
- 103[.]61[.]139[.]78
- 103[.]61[.]139[.]79
- 103[.]78[.]242[.]62
- 118[.]193[.]56[.]130
- 118[.]193[.]62[.]232
- 123[.]58[.]196[.]208
- 123[.]58[.]198[.]205
- 123[.]58[.]203[.]19
- 128[.]14[.]232[.]56
- 152[.]32[.]165[.]70
- 152[.]32[.]203[.]199
- 152[.]32[.]221[.]222
- 152[.]32[.]245[.]157
- 154[.]222[.]238[.]50
- 154[.]222[.]238[.]51
- 165[.]154[.]52[.]41
- 165[.]154[.]70[.]51
- 167[.]88[.]182[.]166
- 176[.]113[.]71[.]62
- 2[.]58[.]242[.]230
- 2[.]58[.]242[.]231
- 2[.]58[.]242[.]235
- 202[.]87[.]223[.]27
- 212[.]115[.]54[.]54
- 37[.]61[.]229[.]104
- 45[.]116[.]13[.]153
- 45[.]128[.]221[.]61
- 45[.]128[.]221[.]66
- 45[.]136[.]187[.]98
- 45[.]14[.]66[.]230
- 45[.]154[.]14[.]132
- 45[.]154[.]14[.]164
- 45[.]154[.]14[.]188
- 45[.]154[.]14[.]254
- 45[.]251[.]241[.]74
- 45[.]251[.]241[.]82
- 45[.]76[.]113[.]163
- 47[.]254[.]192[.]79
- 92[.]223[.]30[.]232
- 92[.]223[.]30[.]52
- 92[.]223[.]90[.]174
- 92[.]223[.]93[.]148
- 92[.]223[.]93[.]222
- 92[.]38[.]139[.]170
- 92[.]38[.]149[.]101
- 92[.]38[.]149[.]241
- 92[.]38[.]171[.]127
- 92[.]38[.]176[.]47
- 107[.]150[.]127[.]124
- 118[.]193[.]56[.]131
- 176[.]113[.]71[.]168
- 185[.]239[.]227[.]12
- 194[.]29[.]100[.]173
- 2[.]58[.]242[.]236
- 45[.]128[.]221[.]182
- 45[.]154[.]14[.]191
- 47[.]254[.]250[.]117
- 79[.]133[.]124[.]88
- 103[.]137[.]185[.]249
- 103[.]61[.]139[.]74
- 107[.]150[.]112[.]211

- 107[.]150[.]127[.]140
- 146[.]185[.]218[.]65
- 152[.]32[.]221[.]242
- 165[.]154[.]70[.]62
- 176[.]113[.]68[.]12
- 185[.]101[.]139[.]176
- 188[.]241[.]250[.]152
- 188[.]241[.]250[.]153
- 193[.]187[.]117[.]144
- 196[.]46[.]190[.]27
- 2[.]58[.]242[.]229
- 2[.]58[.]242[.]232
- 37[.]61[.]229[.]106
- 45[.]128[.]221[.]172
- 45[.]128[.]221[.]186
- 45[.]128[.]221[.]229
- 45[.]134[.]169[.]147
- 103[.]170[.]132[.]199
- 107[.]150[.]110[.]233
- 152[.]32[.]255[.]145
- 167[.]88[.]182[.]107
- 185[.]239[.]226[.]203
- 185[.]239[.]227[.]34
- 45[.]128[.]221[.]169
- 45[.]136[.]187[.]41
- 137[.]220[.]55[.]38
- 45[.]133[.]238[.]234
- 103[.]192[.]226[.]43
- 92[.]38[.]149[.]88
- 5[.]188[.]33[.]237
- 146[.]185[.]218[.]176
- 43[.]254[.]218[.]104
- 43[.]254[.]218[.]57
- 43[.]254[.]218[.]98
- 92[.]223[.]59[.]84
- 43[.]254[.]218[.]43
- 81[.]28[.]13[.]48
- 89[.]43[.]107[.]191
- 103[.]123[.]134[.]145
- 103[.]123[.]134[.]161
- 103[.]123[.]134[.]165
- 103[.]85[.]24[.]81
- 212[.]115[.]54[.]241
- 43[.]254[.]218[.]114
- 89[.]43[.]107[.]190
- 103[.]123[.]134[.]139
- 103[.]123[.]134[.]240
- 103[.]85[.]24[.]121
- 103[.]169[.]91[.]93
- 103[.]169[.]91[.]94
- 45[.]121[.]50[.]230

Sample Subdomains Belonging to Legitimate Services

- 00j3azu[.]publicvm[.]com
- 0ffice365[.]publicvm[.]com
- 0t2q[.]glitch[.]me
- 1[.]janinakoeppen[.]publicvm[.]com
- 1spall[.]publicvm[.]com
- 1xty[.]glitch[.]me
- 26m1lk[.]publicvm[.]com
- 2ubu[.]glitch[.]me
- 3l0g17pan8l-dashboard-services87z[.]publicvm[.]com
- 3w[.]publicvm[.]com
- 4iegypt[.]publicvm[.]com
- 50[.]publicvm[.]com
- 89csach9w[.]publicvm[.]com
- 8nb6h6[.]publicvm[.]com
- 9pou[.]glitch[.]me
- abauuh[.]publicvm[.]com
- abbajabbadabba[.]publicvm[.]com
- accounts[.]amaze[.]co
- accounts[.]famous[.]co
- acrux[.]publicvm[.]com
- acruxdc2[.]publicvm[.]com

- adf[.]publicvm[.]com
- afpppn[.]publicvm[.]com
- ailp[.]glitch[.]me
- ale111[.]publicvm[.]com
- alisonbenz[.]publicvm[.]com
- alpha[.]jupiter-42[.]publicvm[.]com
- amazonureijapan[.]publicvm[.]com
- amazon-verifylogin[.]publicvm[.]com
- ambiguous-chamomile[.]glitch[.]me
- amp-filemetadata[.]glitch[.]me
- angry-cream-metatarsal[.]glitch[.]me
- ao7w8ge[.]publicvm[.]com
- api[.]amaze[.]co
- api[.]famous[.]co
- api-ben[.]famous[.]co
- api-qa[.]amaze[.]co
- api-rc[.]amaze[.]co
- apomail[.]publicvm[.]com
- app[.]famous[.]co
- app-ben[.]famous[.]co
- app-prod1[.]famous[.]co
- app-qa[.]amaze[.]co
- app-rc[.]amaze[.]co
- arjuna4m-instagram[.]glitch[.]me
- armus[.]publicvm[.]com
- asdewf[.]publicvm[.]com
- askaze[.]publicvm[.]com
- assets[.]famous[.]co
- astro000[.]publicvm[.]com
- aug-student-141-224-198-170[.]glitch[.]me
- authorlzeattempt-accessauth[.]publicvm[.]com
- avagallery2408vib[.]publicvm[.]com
- avaya-9611g-3[.]glitch[.]me
- ba1h[.]glitch[.]me
- babymetal-heardle[.]glitch[.]me
- banktrer[.]publicvm[.]com
- basenger[.]publicvm[.]com
- beaded-interesting-metal[.]glitch[.]me
- beryl-grand-metacarpal[.]glitch[.]me
- blog[.]amaze[.]co
- blog[.]famous[.]co
- blog[.]in[.]famous[.]co
- bocode-metadata[.]glitch[.]me
- bokepterbaruindonesia[.]publicvm[.]com
- bonaglia[.]publicvm[.]com
- bony-common-sphere[.]glitch[.]me
- boulder-slow-fortnight[.]glitch[.]me
- bqga4rxzguimrsh[.]publicvm[.]com
- bsgrd6he-supportverifyauth[.]publicvm[.]com
- bvaz[.]glitch[.]me
- cajkwr[.]publicvm[.]com
- carapino[.]publicvm[.]com
- chais12[.]publicvm[.]com
- chontra[.]publicvm[.]com
- christiancollections2408opc[.]publicvm[.]com
- chroma-fairy-metal[.]glitch[.]me
- citi-online[.]publicvm[.]com
- cl2020[.]publicvm[.]com
- claudioboscolo[.]publicvm[.]com
- cliente-credenziali-aggiornamento[.]publicvm[.]com
- closed-metal-chemistry[.]glitch[.]me
- cltbp[.]paperswriting[.]publicvm[.]com
- coiawuuu889ak9000beee[.]publicvm[.]com
- compras-vue[.]glitch[.]me
- conn[.]publicvm[.]com
- content[.]analytics[.]pendo[.]famous[.]co
- corporate[.]famous[.]co
- cpanel[.]accessauthverlfication-accessnotice[.]publicvm[.]com

- cpanel[.]authverlfynotification-updatenotice[.]publicvm[.]com
- cpanel[.]bavertt[.]publicvm[.]com
- cpanel[.]bolde[.]publicvm[.]com
- cpanel[.]jackq[.]publicvm[.]com
- cpanel[.]jiosl[.]publicvm[.]com
- cpanel[.]jonsuiwi[.]publicvm[.]com
- cpcalendars[.]anami[.]publicvm[.]com
- cpcalendars[.]api-usps5c-up-date[.]publicvm[.]com
- cpcalendars[.]authaccesslnformatlon-slgnln[.]publicvm[.]com
- cpcalendars[.]cayt[.]publicvm[.]com
- cpcalendars[.]eddsec08[.]publicvm[.]com
- cpcalendars[.]hame[.]publicvm[.]com
- cpcalendars[.]jakiy[.]publicvm[.]com
- cpcalendars[.]kolan[.]publicvm[.]com
- cpcalendars[.]malrt[.]publicvm[.]com
- cpcalendars[.]sba188sus[.]publicvm[.]com
- cpcalendars[.]secur05login[.]publicvm[.]com
- cpcontacts[.]03-rescue[.]publicvm[.]com
- cpcontacts[.]authverlfynotification-accessupdate[.]publicvm[.]com
- cpcontacts[.]bakerr[.]publicvm[.]com
- cpcontacts[.]bsgrd6he-supportverifyauth[.]publicvm[.]com
- cpcontacts[.]moliy[.]publicvm[.]com
- cpcontacts[.]paswold[.]publicvm[.]com
- cpcontacts[.]resafepay04[.]publicvm[.]com
- cpcontacts[.]resecedd04[.]publicvm[.]com
- cpcontacts[.]secureadmin03[.]publicvm[.]com
- cr[.]publicvm[.]com
- cream-galvanized-metacarpal[.]glitch[.]me
- daa-file-metadata-microservice[.]glitch[.]me
- darkogrbic[.]publicvm[.]com
- dashboard-pan7l-log1ngate[.]publicvm[.]com
- data[.]analytics[.]pendo[.]famous[.]co
- data[.]dfzbzv[.]publicvm[.]com
- deafmetal-heardle[.]glitch[.]me
- denethor[.]glitch[.]me
- design[.]famous[.]co
- dev-ghost[.]in[.]famous[.]co
- digibytewiki[.]publicvm[.]com
- dinolandgenes[.]glitch[.]me
- discordmetatricker[.]glitch[.]me
- dynamatic[.]publicvm[.]com
- ecm2[.]publicvm[.]com
- eddsec08[.]publicvm[.]com
- eduroam-173-221[.]glitch[.]me
- electric-metal-chip[.]glitch[.]me
- emx[.]publicvm[.]com
- energetic-solstice-metal[.]glitch[.]me
- enger[.]publicvm[.]com
- engert[.]publicvm[.]com
- essbit[.]publicvm[.]com
- etc-meiajpae[.]publicvm[.]com
- etc-meiajpan[.]publicvm[.]com
- etc-meicaoejp[.]publicvm[.]com
- etc-meisaicaojapan[.]publicvm[.]com
- etc-meisaiujapan[.]publicvm[.]com
- etc-meisavjapan[.]publicvm[.]com
- experienced-alkaline-metatarsal[.]glitch[.]me
- f2un4xc3l7a0-authappleid[.]publicvm[.]com
- facebook[.]blogoblog-aa[.]glitch[.]me

- facebook[.]bloom-sole[.]glitch[.]me
- facebook[.]bluehackteam[.]glitch[.]me
- facebook[.]boatneck-tamarillo-t8kh1ji2ev[.]glitch[.]me
- facebook[.]btschartdata[.]glitch[.]me
- facebook[.]btschartdata-spotify[.]glitch[.]me
- facebook[.]burclar-api[.]glitch[.]me
- facebook[.]carrybot[.]glitch[.]me
- facebook[.]casping-project[.]glitch[.]me
- facebook[.]chief-evergreen-green[.]glitch[.]me
- facebook[.]childlike-transparent-asterisk[.]glitch[.]me
- facebook[.]christina-wdd30[.]glitch[.]me
- facebook[.]chyperkodpaylasim[.]glitch[.]me
- facebook[.]colorful-burnt-psychiatrist[.]glitch[.]me
- facebook[.]colorful-meteor-saffron[.]glitch[.]me
- facebook[.]comfortable-glorious-titanium[.]glitch[.]me
- facebook[.]common-denominator[.]glitch[.]me
- facebook[.]common-rifle[.]glitch[.]me
- facebook[.]complimentererrrrwfdsf[.]glitch[.]me
- facebook[.]concise-colossal-flyaway[.]glitch[.]me
- facebook[.]confused-shake[.]glitch[.]me
- facebook[.]create-react-app-sample[.]glitch[.]me
- facebook[.]creative-developers[.]glitch[.]me
- facebook[.]crenw-bot[.]glitch[.]me
- facebook[.]cris2[.]glitch[.]me
- facebook[.]critical-computation-2020[.]glitch[.]me
- facebook333462683[.]glitch[.]me
- facebook409324[.]glitch[.]me
- facebook-433745558f452[.]glitch[.]me
- facebook-535-535386253[.]glitch[.]me
- facebook8734[.]glitch[.]me
- facebook9029[.]glitch[.]me
- facebook9030[.]glitch[.]me
- facebook9031[.]glitch[.]me
- facebook9032[.]glitch[.]me
- facebook948930[.]glitch[.]me
- facebook-debug[.]glitch[.]me
- facebook-log[.]glitch[.]me
- facebookpc[.]glitch[.]me
- facebook-witbot-lincolndu[.]glitch[.]me
- faiucjvhfhds2[.]publicvm[.]com
- famx[.]publicvm[.]com
- fasherie[.]glitch[.]me
- fate-perfect-station[.]glitch[.]me
- fcc-api-project-file-metadata-microservice[.]glitch[.]me
- fcc-be-filemetadata-sebek78[.]glitch[.]me
- fcc-file-metadata[.]glitch[.]me
- fcc-project-filemetadata-rms[.]glitch[.]me
- fiicontent[.]analytics[.]pendo[.]famous[.]co
- file-metadat[.]glitch[.]me
- file-metadata-microservice-marco[.]glitch[.]me
- fileshare[.]publicvm[.]com
- filmdrifter[.]publicvm[.]com
- floc-ot-meta[.]glitch[.]me

- flossy-periwinkle-metacarpal[.]glitch[.]me
- flower-scarce-muse[.]glitch[.]me
- foggeln[.]publicvm[.]com
- fordpasa[.]publicvm[.]com
- freckle-plump-metacarpal[.]glitch[.]me
- frien[.]publicvm[.]com
- frizz[.]publicvm[.]com
- functional-clear-rosemary[.]glitch[.]me
- fundacao-ibc[.]glitch[.]me
- gedx[.]glitch[.]me
- gimenezj-whatsapp-wave25[.]glitch[.]me
- git[.]in[.]amaze[.]co
- git[.]in[.]famous[.]co
- git[.]pb88[.]publicvm[.]com
- git-alt[.]in[.]famous[.]co
- git-old[.]in[.]famous[.]co
- git-priv[.]in[.]amaze[.]co
- glib-noisy-metacarpal[.]glitch[.]me
- grafana[.]cidashboard[.]publicvm[.]com
- gt19[.]glitch[.]me
- hangty[.]publicvm[.]com
- heather-metal-estimate[.]glitch[.]me
- hendlsofen[.]publicvm[.]com
- henmetaverse[.]glitch[.]me
- hgfh[.]publicvm[.]com
- hiltonpharma[.]publicvm[.]com
- hip-metal-tarantula[.]glitch[.]me
- homer-metaverse[.]glitch[.]me
- honed[.]publicvm[.]com
- hongry[.]publicvm[.]com
- hookk[.]publicvm[.]com
- huangguandailiw[.]glitch[.]me
- humdrum-metal-atom[.]glitch[.]me
- hyperion[.]publicvm[.]com
- icingdeath[.]publicvm[.]com
- iehun[.]publicvm[.]com
- in[.]amaze[.]co
- in[.]famous[.]co
- instagram2[.]glitch[.]me
- instagram-downloader[.]glitch[.]me
- instagram-photo-31patrykywatne[.]glitch[.]me
- instagrarn[.]glitch[.]me
- instagrat[.]glitch[.]me
- instaprivateopener[.]publicvm[.]com
- is-facebook-down[.]glitch[.]me
- itnesrasanpoalo[.]publicvm[.]com
- japanamazonsic[.]publicvm[.]com
- jealous-metal-hexagon[.]glitch[.]me
- jenkins[.]in[.]famous[.]co
- jocoamep[.]publicvm[.]com
- johnnieonl[.]publicvm[.]com
- jonsuiwi[.]publicvm[.]com
- jorgennas[.]publicvm[.]com
- jpamazondo[.]publicvm[.]com
- jpamazonfully[.]publicvm[.]com
- jpamazonot[.]publicvm[.]com
- juniper-splendid-rest[.]glitch[.]me
- karine[.]publicvm[.]com
- kolab[.]publicvm[.]com
- kws-www4[.]publicvm[.]com
- kylie[.]publicvm[.]com
- le4h[.]glitch[.]me
- lengkoas[.]publicvm[.]com
- limbus[.]publicvm[.]com
- linkactivepeymentsecurity[.]publicvm[.]com
- lions[.]publicvm[.]com
- lss[.]publicvm[.]com
- lydec[.]publicvm[.]com
- mail[.]amazon-services[.]publicvm[.]com
- mail[.]bsgrd6he-supportverifyauth[.]publicvm[.]com
- mail[.]haney[.]publicvm[.]com

- mail[.]poleru[.]publicvm[.]com
- makiodw[.]publicvm[.]com
- marbled-metal-rest[.]glitch[.]me
- material[.]supershopping[.]publicvm[.]com
- materialistic-sugary-acapella[.]glitch[.]me
- media-meta-theme-color[.]glitch[.]me
- mesquite-metal-fuel[.]glitch[.]me
- metacity[.]glitch[.]me
- metadata-microservice[.]glitch[.]me
- metafetish-white-label-teledildonics-server[.]glitch[.]me
- metahill[.]glitch[.]me
- metal-absorbing-fly[.]glitch[.]me
- metal-atom-list[.]glitch[.]me
- metal-boar[.]glitch[.]me
- metal-classic-cantaloupe[.]glitch[.]me
- metal-delightful-conchoraptor[.]glitch[.]me
- metal-diligent-fibre[.]glitch[.]me
- metal-familiar-magician[.]glitch[.]me
- metalheardle[.]glitch[.]me
- metal-heardle[.]glitch[.]me
- metal-helpful-silence[.]glitch[.]me
- metal-just-baker[.]glitch[.]me
- metallica-heardle[.]glitch[.]me
- metallic-planet-shader[.]glitch[.]me
- metal-makeup[.]glitch[.]me
- metal-organized-pineapple[.]glitch[.]me
- metal-profuse-arch[.]glitch[.]me
- metal-quark-panama[.]glitch[.]me
- metal-shard-factory[.]glitch[.]me
- metaphernbot[.]glitch[.]me
- meta-refresh-referer[.]glitch[.]me
- metasuncopoc[.]glitch[.]me
- metaverse-comic-booth-1[.]glitch[.]me
- metaverse-comic-festival[.]glitch[.]me
- mightymike[.]publicvm[.]com
- m-instagram[.]glitch[.]me
- minube[.]publicvm[.]com
- molerty[.]publicvm[.]com
- mountainous-metal-rosehip[.]glitch[.]me
- mpvon[.]publicvm[.]com
- msips1[.]publicvm[.]com
- muddy-scientific-tiger[.]glitch[.]me
- mx[.]amaze[.]co
- my[.]famous[.]co
- my-metaverse[.]glitch[.]me
- my-rc[.]amaze[.]co
- n1[.]publicvm[.]com
- n18y[.]glitch[.]me
- naf-nametags[.]glitch[.]me
- nextcloud[.]ideainox[.]publicvm[.]com
- nextcloud[.]mallet[.]publicvm[.]com
- nix[.]publicvm[.]com
- nuxt-routes-meta[.]glitch[.]me
- octagonal-possible-metacarpal[.]glitch[.]me
- olsdaa[.]publicvm[.]com
- omniscient-desert-vise[.]glitch[.]me
- ontoqav[.]publicvm[.]com
- open-metal-bull[.]glitch[.]me
- ordinary-metal-brass[.]glitch[.]me
- ostltd[.]publicvm[.]com
- ot-meta[.]glitch[.]me
- pixels-nft-metadata[.]glitch[.]me
- plastic-vaulted-metatarsal[.]glitch[.]me
- ppooc[.]publicvm[.]com
- premotion[.]glitch[.]me
- press[.]famous[.]co

- press[.]in[.]famous[.]co
- prober[.]publicvm[.]com
- publeer[.]publicvm[.]com
- puddle-metal-taxicab[.]glitch[.]me
- puiot[.]publicvm[.]com
- pushy-metal-gasoline[.]glitch[.]me
- pyrat[.]glitch[.]me
- reliable-efficient-metacarpal[.]glitch[.]me
- riverwest[.]publicvm[.]com
- royfroebel[.]publicvm[.]com
- sametaga[.]glitch[.]me
- sassw[.]publicvm[.]com
- science2[.]publicvm[.]com
- scottml[.]publicvm[.]com
- secawfv23[.]publicvm[.]com
- secure04-manageaccount[.]publicvm[.]com
- secureadmin03[.]publicvm[.]com
- secureinfoverlfication-authsignln[.]publicvm[.]com
- securityprimebillingupdate331[.]publicvm[.]com
- seen-whip-tilapia[.]glitch[.]me
- semihininstagramloginpagei[.]glitch[.]me
- sffsad[.]publicvm[.]com
- sharknetwork[.]publicvm[.]com
- shively[.]glitch[.]me
- sjcloud[.]publicvm[.]com
- standing-trite-metal[.]glitch[.]me
- stax-file-metadata[.]glitch[.]me
- students05[.]publicvm[.]com
- sulfuric-lizard-metatarsal[.]glitch[.]me
- sync-apple-surf-was705146[.]glitch[.]me
- t6i1[.]glitch[.]me
- tbgki[.]publicvm[.]com
- tilde-meta-instruments[.]glitch[.]me
- tismaz[.]publicvm[.]com
- tmpoqa[.]publicvm[.]com
- tor-node[.]publicvm[.]com
- torpid-metal-giraffe[.]glitch[.]me
- travis-kalanick-instagram-dungeon[.]glitch[.]me
- ttmobil[.]publicvm[.]com
- ttyulechengylcltcom[.]glitch[.]me
- tudy[.]publicvm[.]com
- ty-file-metadata[.]glitch[.]me
- ty-file-metadata-python[.]glitch[.]me
- usmomityt1984[.]publicvm[.]com
- viv[.]publicvm[.]com
- vonage-whatsapp-bot[.]glitch[.]me
- vpn[.]in[.]famous[.]co
- vpnattraction[.]publicvm[.]com
- vrify-chase[.]publicvm[.]com
- vynbh[.]publicvm[.]com
- w202sy2u3g[.]publicvm[.]com
- wealthy-metal-jam[.]glitch[.]me
- webaccesslnformationldactivity-authslgnln[.]publicvm[.]com
- webdisk[.]03-rescue[.]publicvm[.]com
- webdisk[.]banger[.]publicvm[.]com
- webdisk[.]dhsara[.]publicvm[.]com
- webdisk[.]jawdert[.]publicvm[.]com
- webdisk[.]polan33[.]publicvm[.]com
- webdisk[.]resafepay04[.]publicvm[.]com
- webdisk[.]sassw[.]publicvm[.]com
- webdisk[.]shakt[.]publicvm[.]com
- webmail[.]arsu[.]publicvm[.]com
- webmail[.]bolte[.]publicvm[.]com
- webmail[.]lokker[.]publicvm[.]com
- webmail[.]secur04login[.]publicvm[.]com
- webmail[.]secyb3[.]publicvm[.]com
- wellsfarg01terminal[.]publicvm[.]com

- whatsapp-cloud-api-echo-bot[.]glitch[.]me
- whatsapp-ui-clone[.]glitch[.]me
- whatsapp-web-api-lc[.]glitch[.]me
- whatsapp-webhook-setup[.]glitch[.]me
- wind-metal-sqirrel[.]glitch[.]me
- without-vp-meta[.]glitch[.]me
- with-vp-meta[.]glitch[.]me
- wp-famous[.]in[.]famous[.]co
- www[.]0ffice365[.]publicvm[.]com
- www[.]1x8klytn8xs7-webauthapple[.]publicvm[.]com
- www[.]3l0g17pan8l-dashboard-services87z[.]publicvm[.]com
- www[.]4if4arp7snsr[.]publicvm[.]com
- www[.]801901756[.]publicvm[.]com
- www[.]accessauthverlfication-authinfo[.]publicvm[.]com
- www[.]accessauthverlfication-authupdate[.]publicvm[.]com
- www[.]agetic[.]gob[.]bo[.]freweb[.]publicvm[.]com
- www[.]aib-authentic-setup-device[.]publicvm[.]com
- www[.]akamaitech[.]publicvm[.]com
- www[.]amazon-accesauth[.]publicvm[.]com
- www[.]amazon-updateaccounts[.]publicvm[.]com
- www[.]amazon-updateapps[.]publicvm[.]com
- www[.]authslgnlnveriflcation-updatenotice[.]publicvm[.]com
- www[.]authverlfynotification-updateinfo[.]publicvm[.]com
- www[.]basenger[.]publicvm[.]com
- www[.]bgwdv[.]publicvm[.]com
- www[.]bolde[.]publicvm[.]com
- www[.]boldv[.]publicvm[.]com
- www[.]bsgrd6he-supportverifyauth[.]publicvm[.]com
- www[.]darthsky[.]publicvm[.]com
- www[.]facebook[.]blog-clearlyelevated[.]glitch[.]me
- www[.]facebook[.]bloom-purple-hoof[.]glitch[.]me
- www[.]facebook[.]blossom-bush-flax[.]glitch[.]me
- www[.]facebook[.]bluehackteam[.]glitch[.]me
- www[.]facebook[.]bodalagmin[.]glitch[.]me
- www[.]facebook[.]bubble-mum[.]glitch[.]me
- www[.]facebook[.]bubbly-aspiring-polyester[.]glitch[.]me
- www[.]facebook[.]carras-io[.]glitch[.]me
- www[.]facebook[.]carras-io-publicc-deploy-prorcess-woodsmode-loader[.]glitch[.]me
- www[.]facebook[.]cashosys[.]glitch[.]me
- www[.]facebook[.]casping-project[.]glitch[.]me
- www[.]facebook[.]cherry-wealthy-dandelion[.]glitch[.]me
- www[.]facebook[.]chestlersss[.]glitch[.]me
- www[.]facebook[.]chia-startpage[.]glitch[.]me
- www[.]facebook[.]chief-lively-pharaoh[.]glitch[.]me
- www[.]facebook[.]childlike-transparent-asterisk[.]glitch[.]me
- www[.]facebook[.]christians-project[.]glitch[.]me
- www[.]facebook[.]chroke[.]glitch[.]me

- www[.]facebook[.]collapsa-ytdl[.]glitch[.]me
- www[.]facebook[.]colossal-rough-pamphlet[.]glitch[.]me
- www[.]facebook[.]cometchat-pro-javascript-react-chat-app-1[.]glitch[.]me
- www[.]facebook[.]comfortable-glorious-titanium[.]glitch[.]me
- www[.]facebook[.]comfortable-truthful-argon[.]glitch[.]me
- www[.]facebook[.]community-home-editor[.]glitch[.]me
- www[.]facebook[.]complementorr[.]glitch[.]me
- www[.]facebook[.]complete-tub[.]glitch[.]me
- www[.]facebook[.]credits[.]glitch[.]me
- www[.]facebook[.]crenw-bot[.]glitch[.]me
- www[.]facebook[.]critical-computation-2020[.]glitch[.]me
- www[.]facebook[.]crocodile-crew[.]glitch[.]me
- www[.]facebook[.]cropsafe-explore[.]glitch[.]me
- www[.]frakt-cache[.]publicvm[.]com
- www[.]hsecurewells08[.]publicvm[.]com
- www[.]jdhst[.]publicvm[.]com
- www[.]jorgennas[.]publicvm[.]com
- www[.]l0g7ngate-panel-ver7fy[.]publicvm[.]com
- www[.]l0g7ngate-sslscr-pan8l-services[.]publicvm[.]com
- www[.]lvyuanxian[.]publicvm[.]com
- www[.]magda-j[.]publicvm[.]com
- www[.]maomi[.]publicvm[.]com
- www[.]mwordonline[.]publicvm[.]com
- www[.]nanxing[.]publicvm[.]com
- www[.]no-reply-chaseonline[.]publicvm[.]com
- www[.]phongmata0958[.]publicvm[.]com
- www[.]planes[.]publicvm[.]com
- www[.]q07dwnxffmmi[.]publicvm[.]com
- www[.]qiwitask[.]publicvm[.]com
- www[.]qsgz2k4pzs[.]publicvm[.]com
- www[.]resecedd04[.]publicvm[.]com
- www[.]secure07c-auth-chase[.]publicvm[.]com
- www[.]stacom[.]publicvm[.]com
- www[.]unisonnetworks[.]publicvm[.]com
- www[.]updateaccessveriflcation-accessignln[.]publicvm[.]com
- www[.]updateaccessveriflcation-accessnotice[.]publicvm[.]com
- www[.]wcloud[.]publicvm[.]com
- www[.]webaccess01online[.]publicvm[.]com
- www[.]wfsecv07[.]publicvm[.]com
- www[.]whatsapp[.]net[.]grankikin2[.]publicvm[.]com
- ys888[.]publicvm[.]com
- yuguantou[.]publicvm[.]com
- yz[.]publicvm[.]com
- zahgt[.]publicvm[.]com
- zelolab-meta-tags[.]glitch[.]me
- zhadum[.]publicvm[.]com
- zhangxiaodong[.]publicvm[.]com
- zippy-verdant-meter[.]glitch[.]me

Malicious Properties Flagged during the Malware Check Dated 20 June 2022

- adaptable-charming-marionberry[.]glitch[.]me
- alert-peppermint-yard[.]glitch[.]me
- amazonureijapan[.]publicvm[.]com
- asdewf[.]publicvm[.]com
- authorlzeattempt-accessauth[.]publicvm[.]com
- basenger[.]publicvm[.]com
- boiling-tartan-roadrunner[.]glitch[.]me
- chiseled-hyper-earthworm[.]glitch[.]me
- cpanel[.]jackq[.]publicvm[.]com
- cpcalendars[.]eddsec08[.]publicvm[.]com
- cpcalendars[.]kolan[.]publicvm[.]com
- cpcalendars[.]malrt[.]publicvm[.]com
- curious-young-chance[.]glitch[.]me
- deciduous-forested-education[.]glitch[.]me
- dent-repeated-porpoise[.]glitch[.]me
- eddsec08[.]publicvm[.]com
- enger[.]publicvm[.]com
- etc-meiajpan[.]publicvm[.]com
- etc-meicaoejp[.]publicvm[.]com
- etc-meisaiujapan[.]publicvm[.]com
- fast-helix-snowstorm[.]glitch[.]me
- foggeln[.]publicvm[.]com
- foul-rose-opera[.]glitch[.]me
- https-mail-ionos-validate-ssli[.]glitch[.]me
- japanamazonsic[.]publicvm[.]com
- jpamazonot[.]publicvm[.]com
- lofty-better-pint[.]glitch[.]me
- login-mtb-server-connection[.]publicvm[.]com
- luck-kind-dianella[.]glitch[.]me
- merciful-bright-party[.]glitch[.]me
- mpaid[.]glitch[.]me
- opaque-magnificent-cereal[.]glitch[.]me
- petalite-creative-lupin[.]glitch[.]me
- ruby-lofty-hockey[.]glitch[.]me
- scientific-handsomely-tree[.]glitch[.]me
- secureinfoverlfication-authsignln[.]publicvm[.]com
- securityprimebillingupdate331[.]publicvm[.]com
- sincere-soapy-grade[.]glitch[.]me
- statuesque-soft-grasshopper[.]glitch[.]me
- succulent-truthful-supermarket[.]glitch[.]me
- tasteful-achieved-potential[.]glitch[.]me
- tidal-excellent-silk[.]glitch[.]me
- tree-freckle-swordfish[.]glitch[.]me
- vrify-chase[.]publicvm[.]com
- webdisk[.]shakt[.]publicvm[.]com
- wry-rustic-patch[.]glitch[.]me
- www[.]aib-authentic-setup-device[.]publicvm[.]com
- www[.]amazon-accesauth[.]publicvm[.]com
- www[.]bgwdv[.]publicvm[.]com
- www[.]hsecurewells08[.]publicvm[.]com