Examining WoofLocker under the DNS Lens

Table of Contents

Executive Report

WoofLocker tech support scams have been wreaking havoc since 2017 but the threat actors behind it don't seem to be done yet. In fact, the threat may have become even more resilient. Apart from using compromised sites as distribution vectors, WoofLocker started employing a complex traffic direction scheme.

AlienVault OTX has identified 346 domains and 438 IP addresses as WoofLocker indicators of compromise (IoCs) to date. But given the threat's eight years of existence, how sure are we that no other web properties have fallen through the cracks? We sought to find out.

Our DNS deep dive into WoofLocker revealed:

- 17 unreported IP addresses to which some domains identified as IoCs resolved
- 1,194 unpublished domains that shared some of the IoCs' dedicated IP hosts
- 18 malicious IP-connected domains based on a bulk malware check

Under the WoofLocker Hood

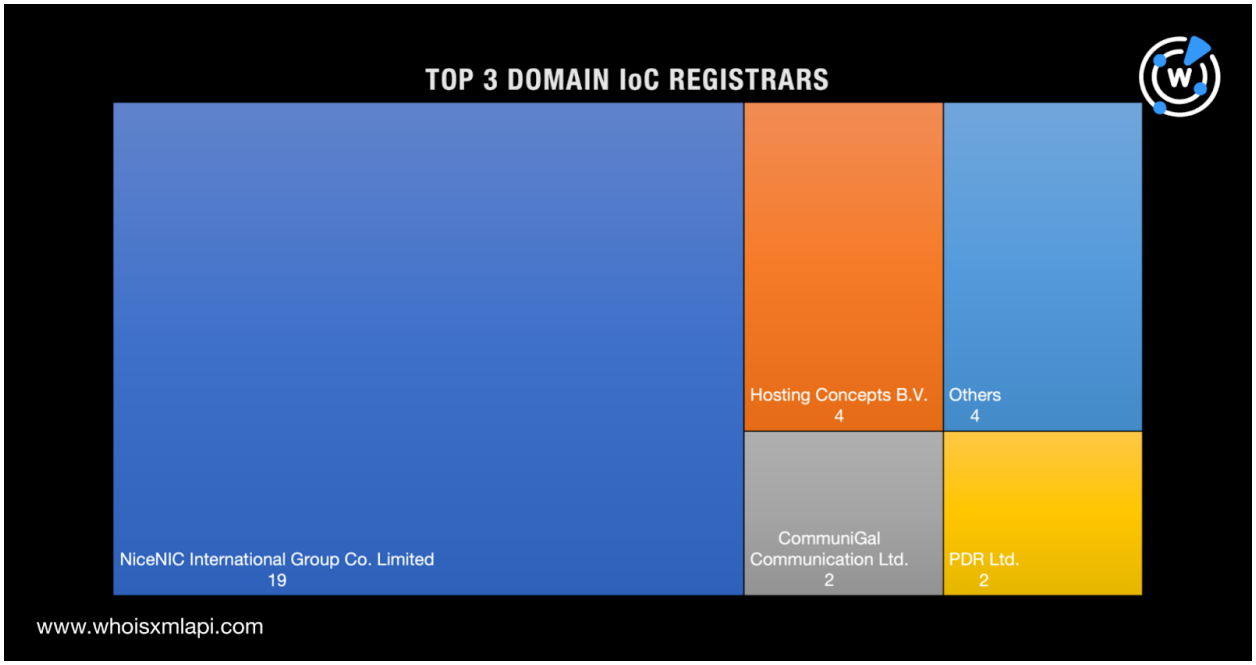
With eight years of operation and running in its belt, you would expect WoofLocker to have employed various registrars, a good mix of aged and newly registered domains (NRDs), and a widely spread out infrastructure worldwide. Was that the case, though? We trooped to the DNS to find out.

Domain IoC Analysis

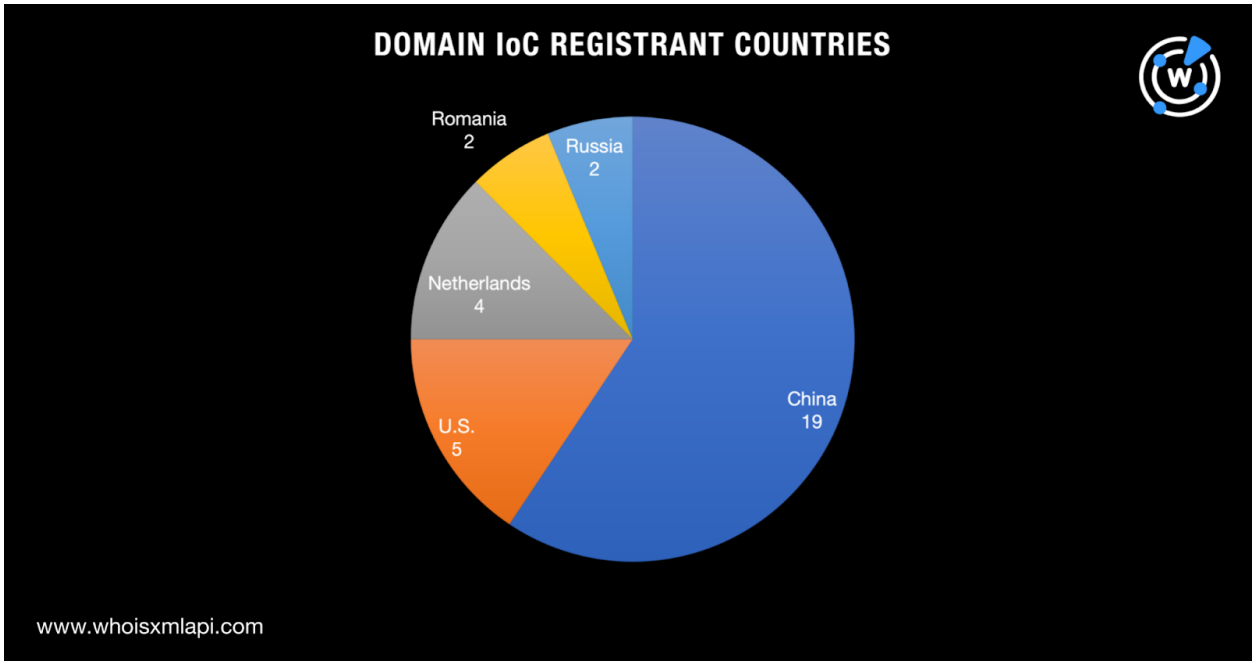
First off, we subjected the domains identified as IoCs to a bulk WHOIS lookup, which led to these discoveries:

- Only 32 of the 346 domains had current WHOIS records, 61% of which were administered by NiceNIC International Group Co. Limited, Hosting Concepts B.V. (four

IoCs) and CommuniGal Communication Ltd. and PDR Ltd. (two IoCs each) rounded out the top 3 registrars.



- A good number of the domains (78%) were NRDs while the remaining 19% were also fairly new, created in 2021 and 2022. One didn't have a recorded creation date.
- A majority of the IoCs (19 domains) were registered in China. The remaining were spread out across four other countries—five in the U.S., four in the Netherlands, and two each in Romania and Russia.

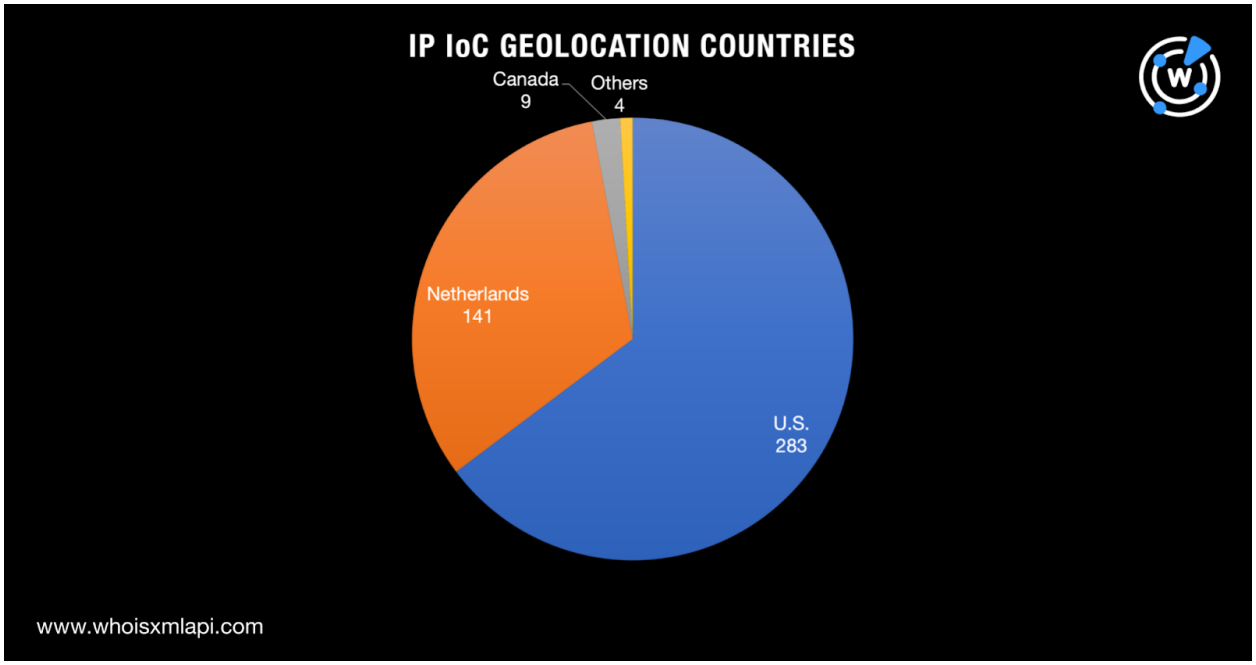


- The two domains registered in Romania—mylandings[.]us and ourlovestories[.]us—had the same public registrant Gmail email address. A reverse WHOIS search for the email address, however, turned up more than 10,000 domains, which could mean its owner was a domainer.

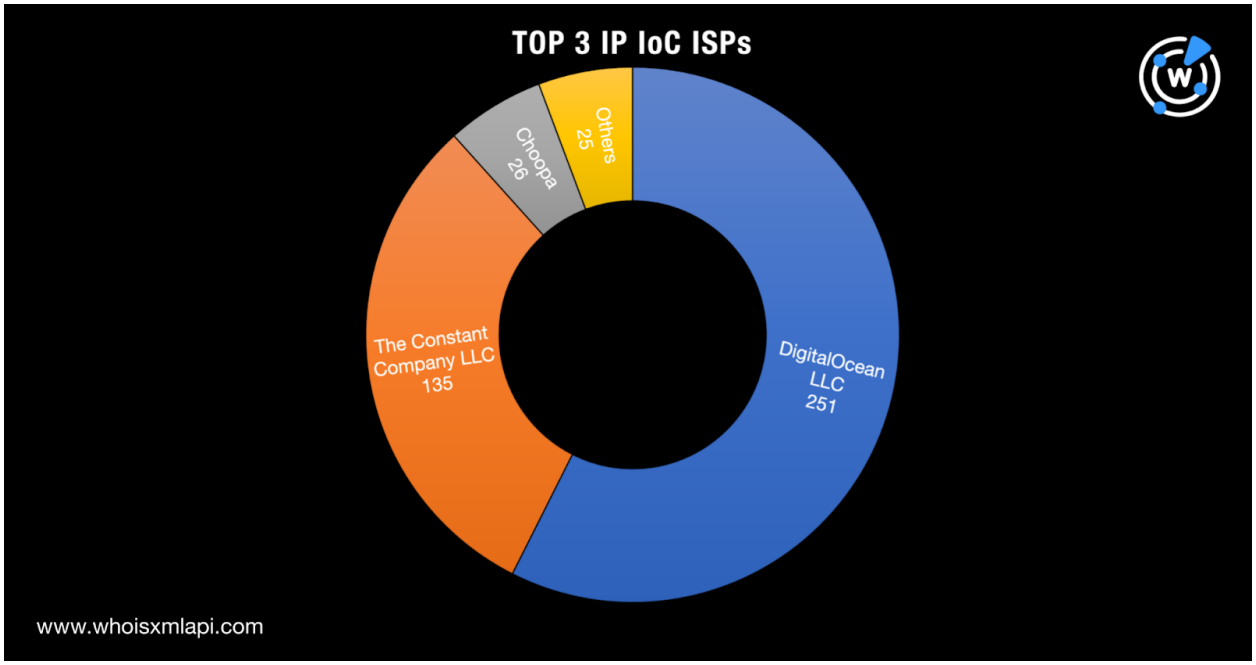
IP IoC Analysis

Next up, we scrutinized the IP addresses classified as IoCs via a bulk IP geolocation lookup, which uncovered:

- A majority of the IP addresses (283 IoCs) were geolocated in the U.S. The Netherlands (141 IoCs) and Canada (nine IoCs) rounded out the top 3 geolocation countries.



- The IoCs were spread out across 17 Internet service providers (ISPs) led by DigitalOcean LLC, which accounted for 251 IP addresses. The Constant Company LLC (135 IoCs) and Choopa (26 IoCs) completed the top 3.



Our domain and IP IoC analyses provided a few answers to the questions we posed earlier. Despite WoofLocker's long-running tech support ruse, the threat actors employed a limited

number of registrars (nine) and ISPs (12). Seemingly, they also showed a preference for NRDs, as only 32 out of 346 domains had current WHOIS records. It's possible that the domains without current WHOIS records were deliberately left to expire or taken down.

And finally, their infrastructure seemed to span only a few countries distributed across the world's continents—five current registrant countries and eight IP geolocation countries.

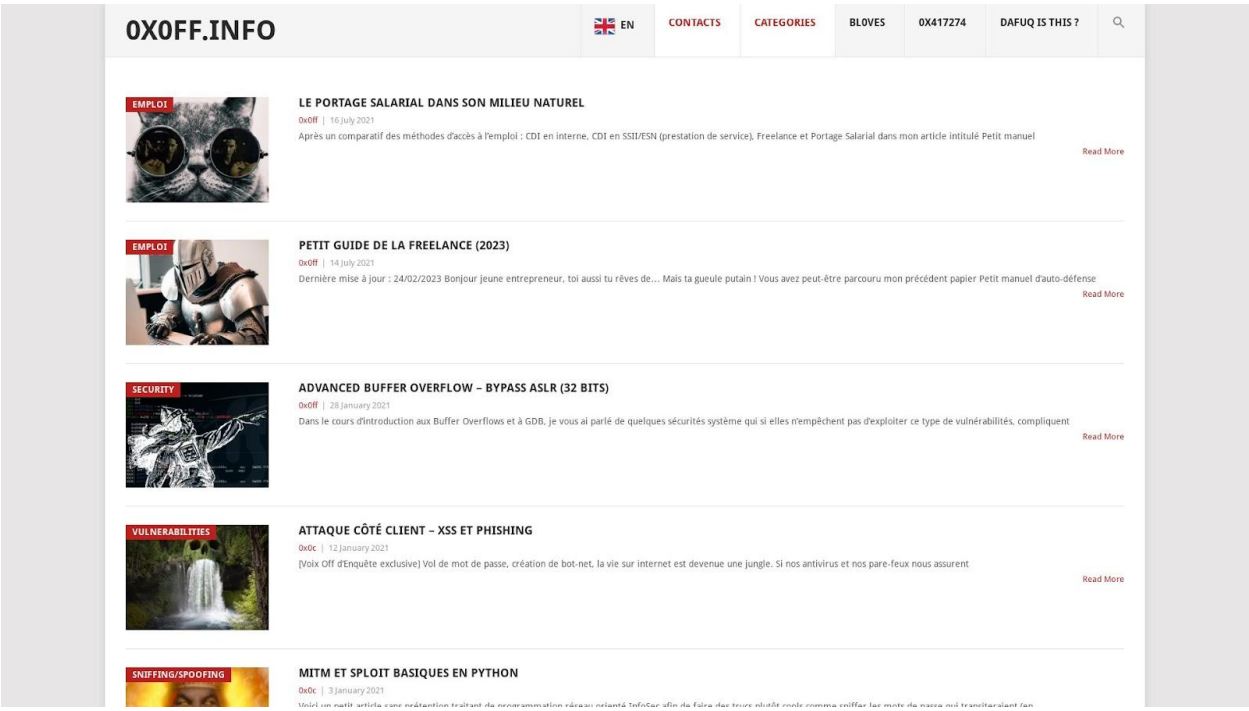
WoofLocker IoC Deep Dive

We also posed other questions regarding the inner workings of WoofLocker.

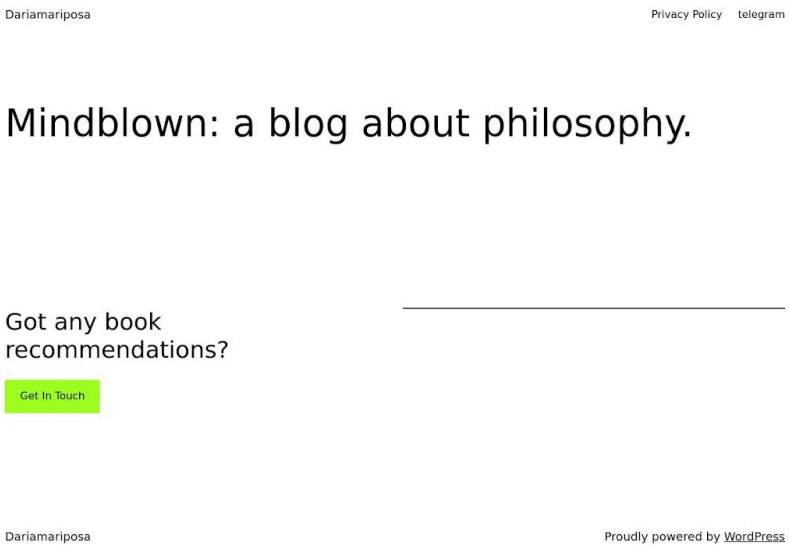
First, we wanted to find out if given the threat's years-long existence we could uncover unpublicized artifacts. DNS lookups for the domains identified as IoCs led to the discovery of 17 additional IP addresses—12 IPv4 and five IPv6 addresses.

That brought our total number of IP addresses (IoCs and artifacts combined) to 451. To limit false positives, we decided to focus only on those that were dedicated. That left us with 104 IP addresses to further analyze.

Reverse IP lookups for the 104 IP addresses led to the discovery of 1,194 connected domains. A bulk malware check showed that 19 of them were malicious. Two of the dangerous properties continue to host live content to this day, one looks to be a news site while the other appears to be a blog.



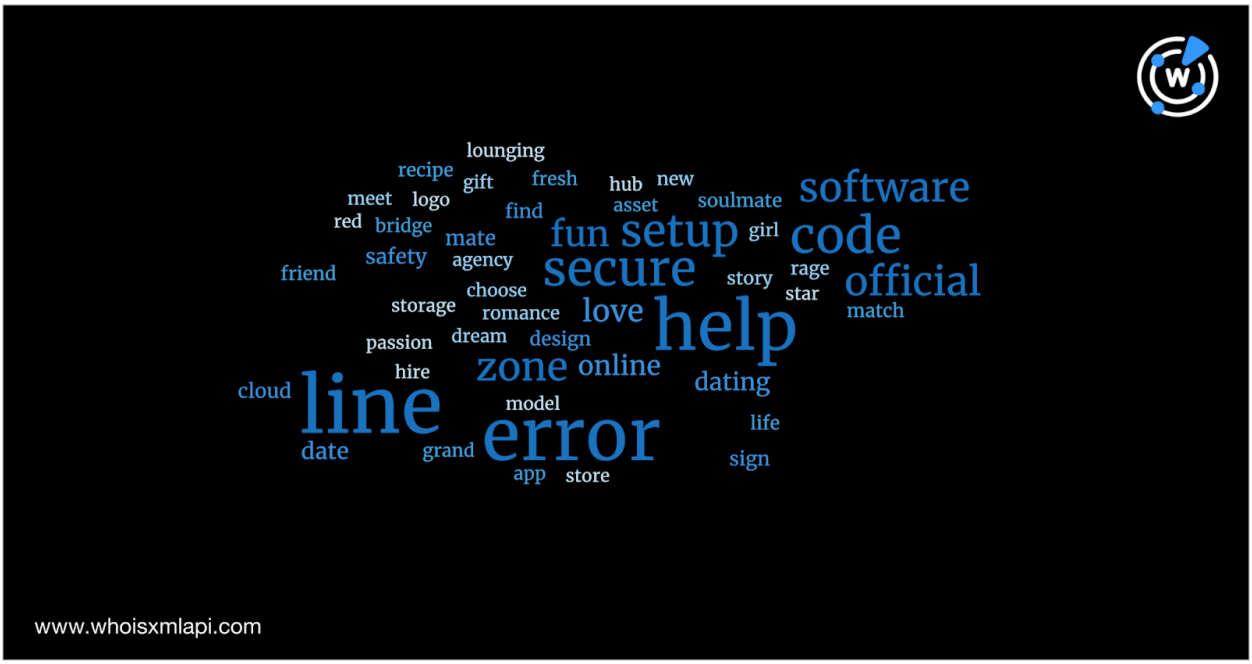
Screenshot of 0x0ff[.]info



Screenshot of dariamariposa[.]com

One tidbit about WoofLocker also caught our attention—the operators' penchant for compromising adult sites to serve as scam vehicles. Does that mean the owners of non-adult websites need not worry about becoming unwitting fraud participants?

To find out, we subjected the domains identified as IoCs to a closer examination. We sought to identify recurring text strings that appeared more than once among the IoCs. We named 52 strings led by **official**, which appeared in 51 domains. **Zone** closely followed in second place, appearing in 50 IoCs. **Fun**, seen in 41 domains, rounded out the top 3. Take a look at a visual representation of our text string analysis below.



The domains containing top 3 strings **official**, **error**, and **help**, such as errorhelpline24x7msofficialsoftwareerrorcodex16[.]monster, errorhelpline24x7msofficialsoftwareerrorgh001[.]monster, and errorhelpline24x7msofficialsoftwareerrornew06[.]monster, all seemed to point to supposed Microsoft helpline sites in support of WoofLocker's chosen tactic—tech support scams. Most of them (123 domains to be exact) also sported the .monster TLD.

Also, possibly in connection to WoofLocker's preference for adult sites, around 200 domains appeared to point to dating sites. That doesn't mean the owners of non-adult-related websites would remain safe, though. We also found other strings like **cloud**, **design**, **logo**, **recipe**, and **storage**.

—

Our WoofLocker IoC expansion analysis allowed us to answer questions that piqued our curious minds about the threat. Despite its age, the scammers limited their infrastructure components to a few providers and locations. They also seemingly favored employing NRDs and new gTLDs as campaign vehicles. Last but definitely not least, though they've been known to prefer compromising adult-related sites, they could also be trailing their sights on cloud, design, storage services, and cooking websites.

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

WoofLocker IoCs Compiled by AlienVault OTX

- 69chicks[.]site
- adsmysecrettemptation[.]com
- alouetteagency[.]site
- appcloudzedo[.]com
- aquireskill[.]site
- arrangemydate[.]site
- barustan[.]com
- beeronas[.]com
- besoliza[.]com
- blogspotnews[.]xyz
- bopiland[.]com
- bringstarsdownward[.]site
- cdncontentstorage[.]com
- cdnpictureasset[.]com
- choosetoupu[.]fun
- choosetozing[.]fun
- cloudcusersyn[.]com
- cloudgertopage[.]com
- cloudlogobox[.]com
- colourflames[.]site
- coloursoflove[.]us
- conventional[.]site
- corpusstimuli[.]site
- countour[.]site
- coupledatings[.]site
- csscloudstorage[.]com
- cumnow[.]site
- datacloudasset[.]com
- datefree[.]fun
- datelikehilary[.]site
- dateshookupseverything[.]life
- datesoulmate[.]site
- dateuse[.]xyz
- dating247[.]site
- datingagencies[.]site
- datinggirl[.]xyz
- datingglowy[.]fun
- datingholic[.]xyz

- datingloveever[.]website
- datingstre[.]site
- defolis[.]com
- deltadesignbrim[.]fun
- designercfode[.]fun
- designerdave[.]fun
- designersmart[.]fun
- designertone[.]fun
- dezigndoubles[.]fun
- dezignfrutto[.]fun
- dimensionalroute[.]fun
- dippystock[.]site
- divinelovemeet[.]us
- e44o4-msg-co-1010100010110[.]cf
- elinorecyrusrosalind[.]site
- enduringlive[.]site
- errorhelpline24x7msofficialsoftwareerrorcodex16[.]monster
- errorhelpline24x7msofficialsoftwareerrorgh001[.]monster
- errorhelpline24x7msofficialsoftwareerrorgh002[.]monster
- errorhelpline24x7msofficialsoftwareerrorgh003[.]monster
- errorhelpline24x7msofficialsoftwareerrorgh004[.]monster
- errorhelpline24x7msofficialsoftwareerrorgh006[.]monster
- errorhelpline24x7msofficialsoftwareerrorgh008[.]monster
- errorhelpline24x7msofficialsoftwareerrorgh009[.]monster
- errorhelpline24x7msofficialsoftwareerrorgh012[.]monster
- errorhelpline24x7msofficialsoftwareerrorgh013[.]monster
- errorhelpline24x7msofficialsoftwareerrorgh015[.]monster
- errorhelpline24x7msofficialsoftwareerrorgh017[.]monster
- errorhelpline24x7msofficialsoftwareerrorgh018[.]monster
- errorhelpline24x7msofficialsoftwareerrorgh020[.]monster
- errorhelpline24x7msofficialsoftwareerrorgh021[.]monster
- errorhelpline24x7msofficialsoftwareerrorgh023[.]monster
- errorhelpline24x7msofficialsoftwareerrorgh024[.]monster
- errorhelpline24x7msofficialsoftwareerrorgh025[.]monster
- errorhelpline24x7msofficialsoftwareerrorgh028[.]monster
- errorhelpline24x7msofficialsoftwareerrorgh030[.]monster
- errorhelpline24x7msofficialsoftwareerrorgh033[.]monster
- errorhelpline24x7msofficialsoftwareerrorgh036[.]monster
- errorhelpline24x7msofficialsoftwareerrorgh037[.]monster
- errorhelpline24x7msofficialsoftwareerrorgh038[.]monster
- errorhelpline24x7msofficialsoftwareerrorgh039[.]monster
- errorhelpline24x7msofficialsoftwareerrorgh041[.]monster
- errorhelpline24x7msofficialsoftwareerrorgh044[.]monster
- errorhelpline24x7msofficialsoftwareerrorgh045[.]monster
- errorhelpline24x7msofficialsoftwareerrorgh046[.]monster
- errorhelpline24x7msofficialsoftwareerrorgh047[.]monster
- errorhelpline24x7msofficialsoftwareerrorgh048[.]monster
- errorhelpline24x7msofficialsoftwareerrorgh050[.]monster

- errorhelpline24x7msofficialsoftwareerrorgh051[.]monster
- errorhelpline24x7msofficialsoftwareerrorgh052[.]monster
- errorhelpline24x7msofficialsoftwareerrorgh053[.]monster
- errorhelpline24x7msofficialsoftwareerrorgh054[.]monster
- errorhelpline24x7msofficialsoftwareerrorgh055[.]monster
- errorhelpline24x7msofficialsoftwareerrorgh056[.]monster
- errorhelpline24x7msofficialsoftwareerrorgh057[.]monster
- errorhelpline24x7msofficialsoftwareerrorgh059[.]monster
- errorhelpline24x7msofficialsoftwareerrorgh061[.]monster
- errorhelpline24x7msofficialsoftwareerrorgh062[.]monster
- errorhelpline24x7msofficialsoftwareerrorgh063[.]monster
- errorhelpline24x7msofficialsoftwareerrorgh064[.]monster
- errorhelpline24x7msofficialsoftwareerrorgh065[.]monster
- errorhelpline24x7msofficialsoftwareerrorgh066[.]monster
- errorhelpline24x7msofficialsoftwareerrorgh067[.]monster
- errorhelpline24x7msofficialsoftwareerrorgh068[.]monster
- errorhelpline24x7msofficialsoftwareerrorgh069[.]monster
- errorhelpline24x7msofficialsoftwareerrorgh070[.]monster
- errorhelpline24x7msofficialsoftwareerrornew06[.]monster
- exoticrefreshment[.]site
- fantabuluousfrils[.]site
- findlovelife[.]fun
- findlovestory[.]fun
- findmymatch[.]us
- findsoulmates[.]fun
- flexsterreep[.]site
- florenciacurreyaretina[.]club
- foodfreshrecipe[.]com
- freshrecipe[.]xyz
- fuckherin69[.]site
- fuckin69[.]site
- fundatingservices[.]com
- funsexwebcams[.]com
- furakelw[.]com
- genersok[.]xyz
- getdateus[.]com
- getgiftfortrad[.]site
- getmedate[.]us
- getpitcuresque[.]site
- giftyrootpour[.]site
- ginnilovellmatazzoni[.]club
- goldenfriendshipp[.]com
- gomoyad[.]com
- gopilofan[.]com
- gustyhouled[.]fun
- helpsecureity24x7errorcodehelpsoftware1[.]monster
- hiredatingagency[.]site
- hiremodels[.]site
- howdydrakon[.]site
- ilovedating[.]site
- jenniferlovehewit[.]site
- klassycafe[.]fun
- letsdate[.]website
- letsminglelove[.]fun
- letssee[.]click
- lobosixt[.]com
- logosvault[.]com
- lounging[.]website
- lovebeyondtruth[.]website
- lovecolours[.]site

- lovedatingg[.]fun
- lovefinder[.]site
- loveromances[.]fun
- loveyourlife[.]fun
- loyalgirlfriendships[.]com
- makelovestory[.]site
- makemecum[.]site
- malubana[.]com
- manageanddate[.]site
- mateclassicstuff[.]site
- meedtdate[.]site
- meetdreamdate[.]site
- meetnearyou[.]xyz
- midnightfriendships[.]com
- mightiestdream[.]site
- miniassetcloud[.]com
- molesanu[.]com
- mprospect[.]site
- mybokingdip[.]site
- mycircle[.]website
- myclichepic[.]site
- mydishlove[.]site
- mydustyhair[.]site
- myfebyacht[.]site
- myfudgesweet[.]site
- mygoggyrusk[.]site
- mygrandfun[.]site
- mygrandmoves[.]site
- mygrandtricks[.]site
- myhandytuff[.]site
- myhoggytool[.]site
- myhuggystore[.]site
- mylandings[.]us
- mylinkcards[.]xyz
- mylounging[.]site
- mylovebirdsmatch[.]com
- mylovebridge[.]site
- myloverage[.]site
- mylovescene[.]site
- mylovescoop[.]site
- mylovestory[.]website
- mymatelove[.]site
- mymatestayed[.]site
- mymodelling[.]site
- myonlinegrond[.]site
- myonlineneeds[.]site
- myonlinesignh[.]site
- myonlinestors[.]site
- myonlinetheme[.]site
- mypalebag[.]site
- mypaperstore[.]site
- mypecttystub[.]site
- mypeggybridge[.]site
- mypeppywok[.]site
- myphasebloom[.]site
- myradius[.]site
- mysangstroke[.]site
- mysoulmates[.]site
- mytottyfiks[.]site
- mytroyup[.]site
- new-recipe[.]xyz
- nextlevels[.]fun
- onlinecollenging[.]fun
- onlinecraig[.]fun
- onlinedisky[.]fun
- onlinegappo[.]fun
- onlinekate[.]fun
- onlinelovest[.]site
- onlinemacraigs[.]site
- onlinemapornhub[.]site
- onlinemasarcg[.]site
- onlinerug[.]fun
- onlinesclean[.]fun
- onlinescope[.]fun
- onlinesoughtfor[.]fun
- onlinetrips[.]fun
- ourdating[.]site
- ourloveline[.]life
- ourloveromance[.]fun
- ourloveromance[.]site

- ourlovestories[.]us
- ourredmarket[.]site
- oursdate[.]site
- oursnapshot[.]fun
- ourwellformed[.]site
- outfitsdome[.]fun
- papputhesailor[.]site
- passiondating[.]ml
- passiondating[.]xyz
- pastyourtime[.]site
- pcmssecuresetup24x7errorcodehelplinezone1[.]monster
- pcmssecuresetup24x7errorcodehelplinezone10[.]monster
- pcmssecuresetup24x7errorcodehelplinezone11[.]monster
- pcmssecuresetup24x7errorcodehelplinezone12[.]monster
- pcmssecuresetup24x7errorcodehelplinezone14[.]monster
- pcmssecuresetup24x7errorcodehelplinezone15[.]monster
- pcmssecuresetup24x7errorcodehelplinezone2[.]monster
- pcmssecuresetup24x7errorcodehelplinezone3[.]monster
- pcmssecuresetup24x7errorcodehelplinezone4[.]monster
- pcmssecuresetup24x7errorcodehelplinezone5[.]monster
- pcmssecuresetup24x7errorcodehelplinezone7[.]monster
- pcmssecuresetup24x7errorcodehelplinezone8[.]monster
- pcmssecuresetup24x7errorcodehelplinezone9[.]monster
- pcmssecuresetup24x7errorcodehelplinezonedd16[.]monster
- pcmssecuresetup24x7errorcodehelplinezonedd17[.]monster
- pcmssecuresetup24x7errorcodehelplinezonedd18[.]monster
- pcmssecuresetup24x7errorcodehelplinezonedd19[.]monster
- pcmssecuresetup24x7errorcodehelplinezonedd20[.]monster
- pcmssecuresetup24x7errorcodehelplinezonedd21[.]monster
- pcmssecuresetup24x7errorcodehelplinezonedd22[.]monster
- pcmssecuresetup24x7errorcodehelplinezonedd24[.]monster
- pcmssecuresetup24x7errorcodehelplinezonedd25[.]monster
- pcmssecuresetup24x7errorcodehelplinezonedd26[.]monster
- pcmssecuresetup24x7errorcodehelplinezonedd29[.]monster
- pcmssecuresetup24x7errorcodehelplinezonedd30[.]monster
- pcmssecuresetup24x7errorcodehelplinezonedd33[.]monster
- pcmssecuresetup24x7errorcodehelplinezonedd34[.]monster
- pcmssecuresetup24x7errorcodehelplinezonedd38[.]monster
- pcmssecuresetup24x7errorcodehelplinezonedd39[.]monster
- pcmssecuresetup24x7errorcodehelplinezonedd40[.]monster
- pcmssecuresetup24x7errorcodehelplinezonedd43[.]monster
- pcmssecuresetup24x7errorcodehelplinezonedd44[.]monster
- pcmssecuresetup24x7errorcodehelplinezonedd45[.]monster
- pcmssecuresetup24x7errorcodehelplinezonedd46[.]monster
- pcmssecuresetup24x7errorcodehelplinezonedd47[.]monster

- pcmssecuresetup24x7errorcodehelplinezonedd48[.]monster
- pcmssecuresetup24x7errorcodehelplinezonedd49[.]monster
- pcmssecuresetup24x7errorcodehelplinezonedd51[.]monster
- pcmssecuresetup24x7errorcodehelplinezonedd52[.]monster
- pcmssecuresetup24x7errorcodehelplinezonedd53[.]monster
- pcmssecuresetup24x7errorcodehelplinezonedd55[.]monster
- pcmssecuresetup24x7errorcodehelplinezonedd56[.]monster
- pcmssecuresetup24x7errorcodehelplinezonedd58[.]monster
- pcmssecuresetup24x7errorcodehelplinezonedd59[.]monster
- pcmssecuresetup24x7errorcodehelplinezonedd62[.]monster
- pcmssecuresetup24x7errorcodehelplinezonedd63[.]monster
- pcmssecuresetup24x7errorcodehelplinezonedd64[.]monster
- pcmssecuresetup24x7errorcodehelplinezonedd65[.]monster
- pcmssecuresetup24x7errorcodehelplinezonedd66[.]monster
- pcmssecuresetup24x7errorcodehelplinezonedd67[.]monster
- pcseсuresafety24x7errorcodez001[.]monster
- pcseсuresafety24x7errorcodez002[.]monster
- pcseсuresafety24x7errorcodez003[.]monster
- pcseсuresafety24x7errorcodez004[.]monster
- pcseсuresafety24x7errorcodez005[.]monster
- pcseсuresafety24x7errorcodez006[.]monster
- pcseсuresafety24x7errorcodez007[.]monster
- pcseсuresafety24x7errorcodez008[.]monster
- pcseсuresafety24x7errorcodez009[.]monster
- pcseсuresetup24x7errorcodehelpline01[.]monster
- pcseсuresetup24x7errorcodehelpline010[.]monster
- pcseсuresetup24x7errorcodehelpline011[.]monster
- pcseсuresetup24x7errorcodehelpline012[.]monster
- pcseсuresetup24x7errorcodehelpline02[.]monster
- pcseсuresetup24x7errorcodehelpline03[.]monster
- pcseсuresetup24x7errorcodehelpline04[.]monster
- pcseсuresetup24x7errorcodehelpline05[.]monster
- pcseсuresetup24x7errorcodehelpline06[.]monster
- pcseсuresetup24x7errorcodehelpline08[.]monster
- pcseсuresetup24x7errorcodehelpline09[.]monster
- pellamofloral[.]fun
- personalsonline[.]xyz
- potraiture[.]site
- privys[.]site
- prophyrio[.]site
- puusssymate[.]xyz
- recipesonline365[.]com
- reliabilityassist[.]monster
- roasterrun[.]fun
- saledating[.]xyz

- sassysenssations[.]com
- sebasong[.]com
- semilupa[.]com
- showelritetrak[.]site
- simplecorp[.]site
- somalics[.]com
- somawan[.]com
- spongteens[.]site
- stardomforus[.]site
- stemloves[.]com
- straightbreak[.]site
- superbmatch[.]site
- superbmatch[.]xyz
- surrounds[.]site
- swayamhubs[.]com
- swiftfling[.]online
- talentagent[.]website
- tastebuds[.]site
- terminalrope[.]site
- thetruefriendships[.]com
- toasterbroom[.]site
- triostagunite[.]site
- truesoulmate[.]fun
- tubbingduo[.]site
- underthebridge[.]site
- universality[.]site
- vedopixt[.]com
- vulidoc[.]com
- xepilondi[.]com
- zemolist[.]com
- 104[.]131[.]126[.]138
- 104[.]131[.]172[.]154
- 104[.]131[.]21[.]130
- 104[.]131[.]40[.]163
- 104[.]131[.]41[.]112
- 104[.]131[.]46[.]187
- 104[.]131[.]61[.]228
- 104[.]156[.]226[.]32
- 104[.]156[.]227[.]254
- 104[.]207[.]129[.]181
- 104[.]207[.]132[.]221
- 104[.]207[.]158[.]235
- 104[.]248[.]114[.]189
- 104[.]248[.]197[.]131
- 104[.]248[.]207[.]211
- 104[.]248[.]207[.]250
- 104[.]248[.]227[.]194
- 104[.]248[.]228[.]231
- 104[.]248[.]236[.]157
- 104[.]248[.]49[.]33
- 104[.]248[.]86[.]105
- 104[.]248[.]90[.]146
- 107[.]191[.]36[.]143
- 107[.]191[.]39[.]78
- 107[.]191[.]40[.]6
- 108[.]61[.]132[.]82
- 108[.]61[.]155[.]209
- 108[.]61[.]158[.]112
- 108[.]61[.]159[.]18
- 108[.]61[.]191[.]117
- 108[.]61[.]195[.]183
- 108[.]61[.]23[.]249
- 108[.]61[.]89[.]254
- 118[.]98[.]239[.]134
- 128[.]199[.]14[.]231
- 128[.]199[.]52[.]70
- 128[.]199[.]57[.]140
- 128[.]199[.]58[.]252
- 128[.]199[.]63[.]45
- 134[.]122[.]113[.]145
- 134[.]122[.]27[.]114
- 134[.]122[.]61[.]100
- 134[.]122[.]63[.]113
- 134[.]209[.]197[.]200
- 134[.]209[.]198[.]14
- 134[.]209[.]198[.]5
- 134[.]209[.]205[.]101
- 134[.]209[.]82[.]1
- 134[.]209[.]83[.]211
- 134[.]209[.]87[.]97

- 134[.]209[.]88[.]3
- 134[.]209[.]93[.]111
- 136[.]244[.]107[.]160
- 136[.]244[.]108[.]147
- 136[.]244[.]94[.]125
- 137[.]184[.]100[.]175
- 137[.]184[.]101[.]140
- 137[.]184[.]102[.]204
- 137[.]184[.]130[.]246
- 137[.]184[.]131[.]200
- 137[.]184[.]138[.]98
- 137[.]184[.]156[.]41
- 137[.]184[.]20[.]109
- 137[.]184[.]209[.]34
- 137[.]184[.]210[.]96
- 137[.]184[.]219[.]167
- 137[.]184[.]23[.]156
- 137[.]184[.]29[.]90
- 137[.]184[.]31[.]128
- 137[.]184[.]49[.]232
- 137[.]184[.]51[.]182
- 137[.]184[.]52[.]27
- 137[.]184[.]76[.]63
- 137[.]184[.]89[.]152
- 137[.]220[.]32[.]176
- 137[.]220[.]32[.]55
- 137[.]220[.]35[.]174
- 137[.]220[.]35[.]55
- 137[.]220[.]39[.]254
- 137[.]220[.]41[.]210
- 137[.]220[.]51[.]151
- 137[.]220[.]51[.]34
- 137[.]220[.]55[.]51
- 138[.]197[.]13[.]94
- 140[.]82[.]0[.]140
- 140[.]82[.]11[.]161
- 140[.]82[.]13[.]174
- 140[.]82[.]15[.]186
- 140[.]82[.]4[.]73
- 140[.]82[.]42[.]75
- 140[.]82[.]5[.]77
- 140[.]82[.]56[.]193
- 140[.]82[.]57[.]201
- 140[.]82[.]60[.]100
- 142[.]93[.]143[.]66
- 142[.]93[.]226[.]124
- 142[.]93[.]229[.]200
- 142[.]93[.]235[.]33
- 142[.]93[.]246[.]79
- 142[.]93[.]250[.]114
- 142[.]93[.]59[.]110
- 142[.]93[.]64[.]88
- 143[.]110[.]148[.]174
- 143[.]110[.]233[.]61
- 143[.]198[.]101[.]247
- 143[.]198[.]113[.]111
- 143[.]198[.]113[.]140
- 143[.]198[.]119[.]136
- 143[.]198[.]119[.]143
- 143[.]198[.]121[.]101
- 143[.]198[.]125[.]180
- 143[.]198[.]134[.]73
- 143[.]198[.]235[.]102
- 143[.]198[.]72[.]5
- 143[.]244[.]152[.]212
- 143[.]244[.]163[.]177
- 143[.]244[.]163[.]249
- 143[.]244[.]167[.]196
- 143[.]244[.]177[.]185
- 143[.]244[.]183[.]127
- 144[.]202[.]12[.]108
- 144[.]202[.]13[.]10
- 144[.]202[.]14[.]205
- 144[.]202[.]15[.]60
- 144[.]202[.]2[.]55
- 144[.]202[.]3[.]218
- 144[.]202[.]48[.]17
- 144[.]202[.]81[.]178
- 144[.]202[.]81[.]49
- 144[.]202[.]81[.]57

- 144[.]202[.]85[.]126
- 144[.]202[.]86[.]232
- 144[.]202[.]89[.]64
- 144[.]202[.]90[.]185
- 144[.]202[.]91[.]76
- 144[.]217[.]29[.]118
- 147[.]182[.]175[.]121
- 147[.]182[.]191[.]68
- 147[.]182[.]235[.]74
- 147[.]182[.]248[.]110
- 149[.]248[.]32[.]46
- 149[.]248[.]45[.]2
- 149[.]28[.]15[.]3
- 149[.]28[.]15[.]96
- 149[.]28[.]196[.]108
- 149[.]28[.]232[.]53
- 149[.]28[.]237[.]61
- 149[.]28[.]246[.]223
- 149[.]28[.]33[.]205
- 149[.]28[.]37[.]87
- 149[.]28[.]42[.]55
- 149[.]28[.]43[.]180
- 149[.]28[.]48[.]200
- 149[.]28[.]51[.]176
- 149[.]28[.]55[.]76
- 149[.]28[.]62[.]48
- 151[.]106[.]96[.]195
- 155[.]138[.]133[.]94
- 155[.]138[.]134[.]120
- 155[.]138[.]136[.]95
- 155[.]138[.]144[.]219
- 155[.]138[.]214[.]143
- 155[.]138[.]243[.]167
- 155[.]138[.]247[.]177
- 155[.]138[.]247[.]81
- 157[.]245[.]139[.]184
- 157[.]245[.]163[.]74
- 157[.]245[.]243[.]253
- 157[.]245[.]253[.]141
- 157[.]245[.]70[.]195
- 157[.]245[.]74[.]238
- 157[.]245[.]75[.]164
- 157[.]245[.]94[.]232
- 159[.]203[.]170[.]218
- 159[.]203[.]189[.]241
- 159[.]203[.]38[.]172
- 159[.]203[.]68[.]96
- 159[.]223[.]0[.]190
- 159[.]223[.]109[.]76
- 159[.]223[.]112[.]225
- 159[.]223[.]125[.]238
- 159[.]223[.]129[.]254
- 159[.]223[.]144[.]9
- 159[.]223[.]151[.]27
- 159[.]223[.]158[.]160
- 159[.]223[.]158[.]168
- 159[.]223[.]162[.]10
- 159[.]223[.]162[.]184
- 159[.]223[.]163[.]124
- 159[.]223[.]164[.]54
- 159[.]223[.]189[.]88
- 159[.]223[.]2[.]87
- 159[.]223[.]3[.]141
- 159[.]223[.]99[.]17
- 159[.]65[.]196[.]90
- 159[.]65[.]198[.]22
- 159[.]65[.]206[.]250
- 159[.]65[.]233[.]177
- 161[.]35[.]108[.]165
- 161[.]35[.]117[.]134
- 161[.]35[.]150[.]7
- 161[.]35[.]153[.]122
- 161[.]35[.]157[.]74
- 161[.]35[.]63[.]32
- 161[.]35[.]86[.]33
- 161[.]35[.]93[.]228
- 161[.]35[.]95[.]168
- 162[.]0[.]209[.]253
- 162[.]241[.]148[.]226
- 162[.]241[.]194[.]45

- 162[.]255[.]119[.]170
- 162[.]255[.]119[.]38
- 162[.]255[.]119[.]82
- 164[.]90[.]194[.]238
- 164[.]90[.]194[.]65
- 164[.]90[.]195[.]41
- 164[.]90[.]196[.]19
- 164[.]90[.]200[.]163
- 164[.]90[.]201[.]242
- 164[.]90[.]206[.]154
- 164[.]90[.]206[.]84
- 164[.]92[.]213[.]153
- 164[.]92[.]213[.]90
- 164[.]92[.]215[.]232
- 164[.]92[.]216[.]249
- 164[.]92[.]217[.]5
- 164[.]92[.]220[.]71
- 164[.]92[.]221[.]102
- 164[.]92[.]221[.]18
- 164[.]92[.]222[.]171
- 164[.]92[.]222[.]233
- 164[.]92[.]223[.]22
- 164[.]92[.]73[.]33
- 164[.]92[.]77[.]118
- 164[.]92[.]92[.]201
- 165[.]22[.]206[.]176
- 165[.]227[.]202[.]86
- 165[.]227[.]80[.]180
- 165[.]227[.]95[.]73
- 165[.]232[.]137[.]23
- 165[.]232[.]140[.]203
- 165[.]232[.]159[.]232
- 165[.]232[.]84[.]97
- 165[.]232[.]86[.]116
- 167[.]71[.]104[.]9
- 167[.]71[.]13[.]32
- 167[.]71[.]15[.]227
- 167[.]71[.]5[.]46
- 167[.]71[.]9[.]102
- 167[.]99[.]14[.]167
- 167[.]99[.]210[.]124
- 167[.]99[.]216[.]66
- 167[.]99[.]218[.]140
- 167[.]99[.]221[.]22
- 167[.]99[.]221[.]41
- 167[.]99[.]222[.]254
- 167[.]99[.]237[.]232
- 167[.]99[.]34[.]35
- 167[.]99[.]38[.]47
- 167[.]99[.]43[.]137
- 167[.]99[.]45[.]97
- 167[.]99[.]8[.]56
- 173[.]199[.]117[.]36
- 174[.]138[.]3[.]95
- 178[.]128[.]238[.]16
- 178[.]128[.]241[.]243
- 178[.]128[.]245[.]227
- 178[.]128[.]246[.]10
- 178[.]128[.]248[.]103
- 178[.]128[.]251[.]153
- 178[.]62[.]192[.]240
- 178[.]62[.]232[.]220
- 178[.]62[.]249[.]65
- 18[.]216[.]200[.]4
- 185[.]224[.]138[.]122
- 185[.]224[.]138[.]142
- 185[.]224[.]138[.]82
- 185[.]92[.]223[.]145
- 188[.]166[.]101[.]190
- 188[.]166[.]108[.]203
- 188[.]166[.]113[.]213
- 188[.]166[.]113[.]239
- 188[.]166[.]115[.]176
- 188[.]166[.]118[.]105
- 188[.]166[.]118[.]128
- 188[.]166[.]123[.]200
- 188[.]166[.]127[.]169
- 188[.]166[.]13[.]60
- 188[.]166[.]146[.]47
- 188[.]166[.]29[.]92

- 188[.]166[.]37[.]189
- 188[.]166[.]4[.]148
- 188[.]166[.]44[.]48
- 188[.]166[.]55[.]207
- 188[.]166[.]57[.]179
- 188[.]166[.]68[.]130
- 188[.]166[.]76[.]28
- 188[.]166[.]8[.]176
- 188[.]166[.]81[.]132
- 188[.]166[.]84[.]173
- 188[.]166[.]86[.]14
- 188[.]166[.]88[.]70
- 188[.]166[.]91[.]52
- 188[.]166[.]99[.]12
- 192[.]64[.]119[.]168
- 192[.]81[.]208[.]159
- 198[.]211[.]104[.]93
- 198[.]211[.]105[.]172
- 198[.]211[.]113[.]166
- 198[.]54[.]114[.]241
- 198[.]54[.]115[.]71
- 198[.]54[.]126[.]79
- 199[.]247[.]29[.]235
- 204[.]48[.]23[.]61
- 206[.]189[.]101[.]174
- 206[.]189[.]104[.]71
- 206[.]189[.]107[.]195
- 206[.]189[.]108[.]197
- 206[.]189[.]108[.]237
- 206[.]189[.]110[.]173
- 206[.]189[.]233[.]104
- 206[.]189[.]8[.]141
- 207[.]148[.]1[.]20
- 207[.]148[.]19[.]99
- 207[.]148[.]2[.]195
- 207[.]148[.]24[.]47
- 207[.]148[.]25[.]47
- 207[.]148[.]31[.]131
- 207[.]148[.]31[.]47
- 207[.]148[.]4[.]136
- 207[.]148[.]6[.]134
- 207[.]246[.]121[.]31
- 207[.]246[.]122[.]39
- 207[.]246[.]85[.]73
- 207[.]246[.]92[.]251
- 207[.]246[.]94[.]212
- 207[.]246[.]95[.]249
- 207[.]246[.]97[.]240
- 208[.]109[.]20[.]245
- 208[.]167[.]233[.]119
- 209[.]222[.]10[.]96
- 209[.]250[.]248[.]222
- 209[.]250[.]249[.]168
- 216[.]128[.]134[.]108
- 216[.]128[.]140[.]3
- 216[.]128[.]144[.]231
- 216[.]128[.]179[.]100
- 216[.]155[.]135[.]21
- 3[.]137[.]33[.]235
- 3[.]20[.]160[.]170
- 3[.]22[.]184[.]46
- 45[.]32[.]185[.]190
- 45[.]32[.]194[.]190
- 45[.]32[.]85[.]181
- 45[.]63[.]14[.]130
- 45[.]63[.]16[.]80
- 45[.]63[.]17[.]110
- 45[.]63[.]17[.]88
- 45[.]63[.]18[.]121
- 45[.]63[.]20[.]236
- 45[.]63[.]36[.]129
- 45[.]63[.]39[.]11
- 45[.]63[.]64[.]43
- 45[.]63[.]8[.]44
- 45[.]76[.]11[.]88
- 45[.]76[.]13[.]69
- 45[.]76[.]242[.]180
- 45[.]76[.]243[.]204
- 45[.]76[.]245[.]54
- 45[.]76[.]246[.]180

- 45[.]76[.]3[.]106
- 45[.]76[.]4[.]16
- 45[.]76[.]5[.]118
- 45[.]76[.]58[.]172
- 45[.]76[.]9[.]149
- 45[.]77[.]100[.]188
- 45[.]77[.]104[.]230
- 45[.]77[.]111[.]147
- 45[.]77[.]115[.]214
- 45[.]77[.]147[.]68
- 45[.]77[.]151[.]151
- 45[.]77[.]158[.]197
- 45[.]77[.]201[.]205
- 45[.]77[.]205[.]14
- 45[.]77[.]209[.]147
- 45[.]77[.]209[.]156
- 45[.]77[.]209[.]181
- 45[.]77[.]210[.]111
- 45[.]77[.]220[.]154
- 45[.]77[.]96[.]163
- 45[.]77[.]99[.]43
- 63[.]209[.]33[.]25
- 64[.]225[.]11[.]4
- 64[.]225[.]55[.]61
- 64[.]225[.]79[.]111
- 64[.]227[.]108[.]73
- 64[.]227[.]30[.]224
- 64[.]227[.]65[.]96
- 64[.]227[.]68[.]126
- 64[.]227[.]74[.]136
- 64[.]227[.]74[.]28
- 64[.]227[.]78[.]76
- 64[.]227[.]9[.]231
- 66[.]135[.]2[.]224
- 66[.]135[.]6[.]180
- 66[.]135[.]7[.]191
- 66[.]42[.]67[.]122
- 66[.]42[.]72[.]138
- 66[.]42[.]72[.]177
- 66[.]42[.]74[.]81
- 66[.]42[.]74[.]9
- 66[.]42[.]75[.]27
- 66[.]42[.]77[.]176
- 66[.]55[.]159[.]68
- 67[.]205[.]136[.]29
- 67[.]205[.]148[.]146
- 67[.]205[.]182[.]148
- 68[.]183[.]0[.]123
- 68[.]183[.]101[.]96
- 68[.]183[.]113[.]63
- 68[.]183[.]116[.]65
- 68[.]183[.]12[.]221
- 68[.]183[.]121[.]19
- 68[.]183[.]125[.]152
- 68[.]183[.]129[.]45
- 68[.]183[.]13[.]175
- 68[.]183[.]130[.]50
- 68[.]183[.]30[.]111
- 68[.]183[.]7[.]67
- 68[.]183[.]98[.]80
- 68[.]65[.]122[.]208
- 68[.]65[.]123[.]186
- 78[.]141[.]221[.]1
- 92[.]249[.]44[.]180
- 92[.]249[.]44[.]58
- 92[.]249[.]44[.]74
- 95[.]179[.]133[.]25
- 95[.]179[.]137[.]38
- 95[.]179[.]167[.]232

Sample Additional IP Resolutions

- 2001:678:f08:2:61:83:10:100
- 78[.]128[.]113[.]74
- 2001:678:f08:2:89:e9:38:a0
- 78[.]128[.]113[.]86

- 204[.]11[.]56[.]48
- 2001:678:f08:2:123:43:12:da
- 78[.]128[.]113[.]228
- 35[.]241[.]18[.]84
- 3[.]18[.]7[.]81

Sample IP-Connected Domains

- 01laden[.]de
- 0x0ff[.]info
- 123912891251[.]xyz
- 157rivobahis[.]com
- 169rivobahis[.]com
- 1951923123[.]online
- 23456734[.]xyz
- 2951923123[.]online
- 300knots[.]me
- 380manbetx[.]com
- 3dben[.]com
- 41234546[.]xyz
- 4951923123[.]online
- 51234546[.]xyz
- 61234546[.]xyz
- 7644sqn[.]org[.]uk
- 88fortunesslots[.]net
- abdul-wasay[.]com
- abi-not-barbie[.]com
- abiclarke[.]com
- abinotbarbie[.]com
- ablo[.]shop
- adams-premium[.]com
- adamspainting[.]us
- adog[.]shop
- adventuresteam[.]online
- afroresearch[.]com
- agaciaabril[.]com
- agetune[.]com
- agomglobal[.]com
- agrow-tek[.]com
- agroxpro[.]com
- aike[.]shop
- airfundraiser[.]com
- akhtaboot[.]com
- aktivlizenz[.]de
- alda-ti[.]com
- alicelonergan[.]com
- aliciamariaa[.]com
- allfastag[.]com
- allkeys[.]online
- allkeyses[.]online
- almadinahalalmeat[.]us
- altosales[.]com
- altotrends[.]com
- alwayshealthy[.]club
- amantescalientes[.]co
- amazingshopgh[.]com
- amentian[.]com
- amigotextile[.]com
- andreasmasis[.]com
- andymiciula[.]com
- angelachetina[.]com
- animlist[.]com
- anke[.]shop
- annakristinwebber[.]com
- anosa[.]uk
- ansiora[.]com
- anti-social-network[.]ca
- antiquecarpetdealer[.]com
- antiquerugschicago[.]net
- antiquerugsgeorgia[.]com
- antiquerugsindiana[.]com
- antiquerugsmichigan[.]com
- antiquerugsnewjersey[.]com
- ap1ds[.]com
- api[.]mbarete[.]cl
- apkhackvip[.]online

- appliancemedic[.]com[.]au
- arb[.]lat
- archimedes-advisors[.]com
- archimedesadvisors[.]com
- arikamacaalay[.]ca
- aserve[.]nl
- ashleyrich[.]rocks
- asianparent[.]website
- assumption[.]us
- assumptionhighschoolnairobi[.]com
- atoto[.]online
- augcrystal[.]com
- augustlakerecords[.]art
- automatedspace[.]co[.]uk
- autopaus[.]online
- autoposter[.]org
- avou[.]shop
- aw0005[.]com
- awhtrading[.]com
- awizemedia[.]com
- ayrcare[.]com
- badalwalagame[.]pro
- balaji-grocery[.]com
- bdvtx[.]com
- bdvtx[.]net
- beanheaditsolutions[.]com
- beetwise[.]com
- belbrandsusaa[.]com
- benefitsbureau[.]com
- berzunza[.]com
- best-sportscodes[.]com
- bestdealsalert[.]in

Sample Malicious IP-Connected Domains

- 0x0ff[.]info
- 123912891251[.]xyz
- 1951923123[.]online
- 23456734[.]xyz
- 2951923123[.]online
- 4951923123[.]online
- 61234546[.]xyz
- breakingnews20[.]beauty
- breakingnews30[.]beauty