# Scanning for LockBit Ransomware DNS Traces

## Table of Contents



## Executive Report

ReliaQuest named LockBit one of the most effective and undoubtedly most prolific currently active ransomware groups today. In fact, the malware topped their latest ransomware quarterly list for the first three months of 2023, a continuation of their 2022 observation.

LockBit initially piqued researchers' interest when it was distributed via SocGholish infections last year. Today, the ransomware operators have taken to employing the ransomware-as-a-service (RaaS) model.

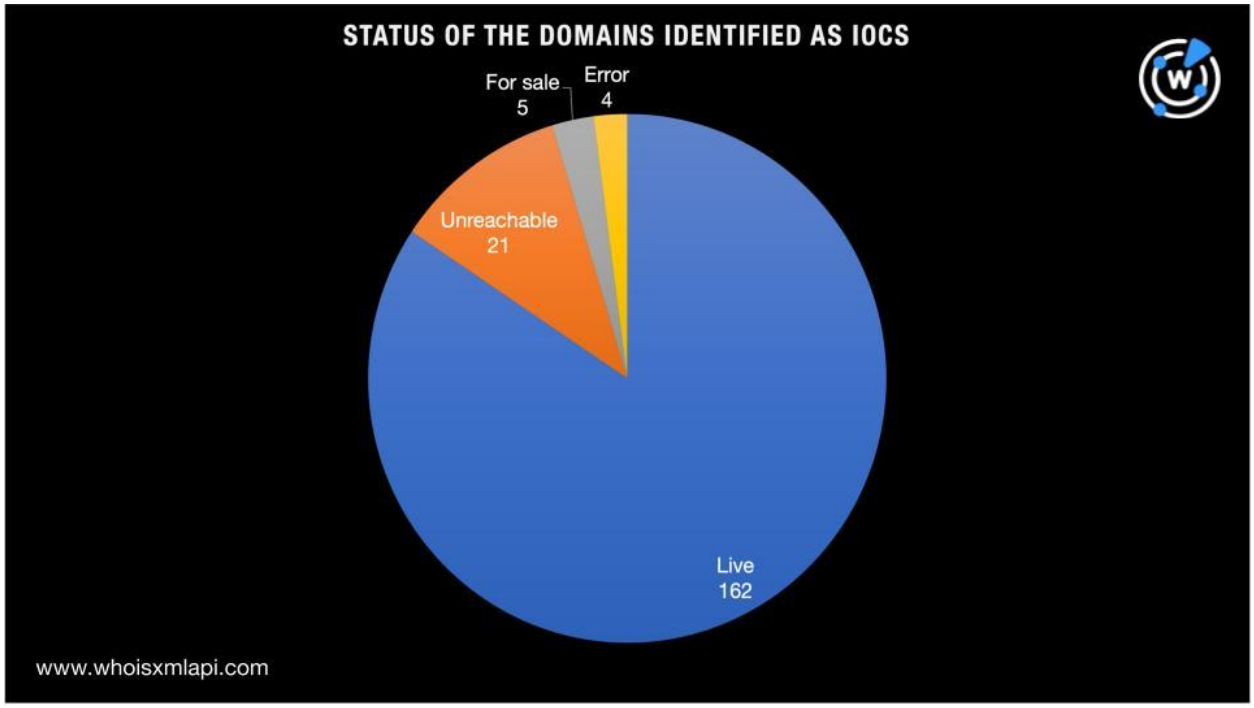
In line with our goal of making the Internet safer and more transparent, we sought to expand a publicly available list of LockBit IoCs to uncover other potentially connected artifacts. Our analysis found:

- 226 IP addresses to which the domains identified as IoCs resolved, 20% of which turned out to be malicious
- 6,066 additional domains that shared some of the IoCs' dedicated IP hosts, 16 of which turned out to be malware hosts

### LockBit IoC Facts

AlienVault OTX publicized 198 LockBit IoCs, specifically 195 domains and three IP addresses. See a sampled list in the Appendix.

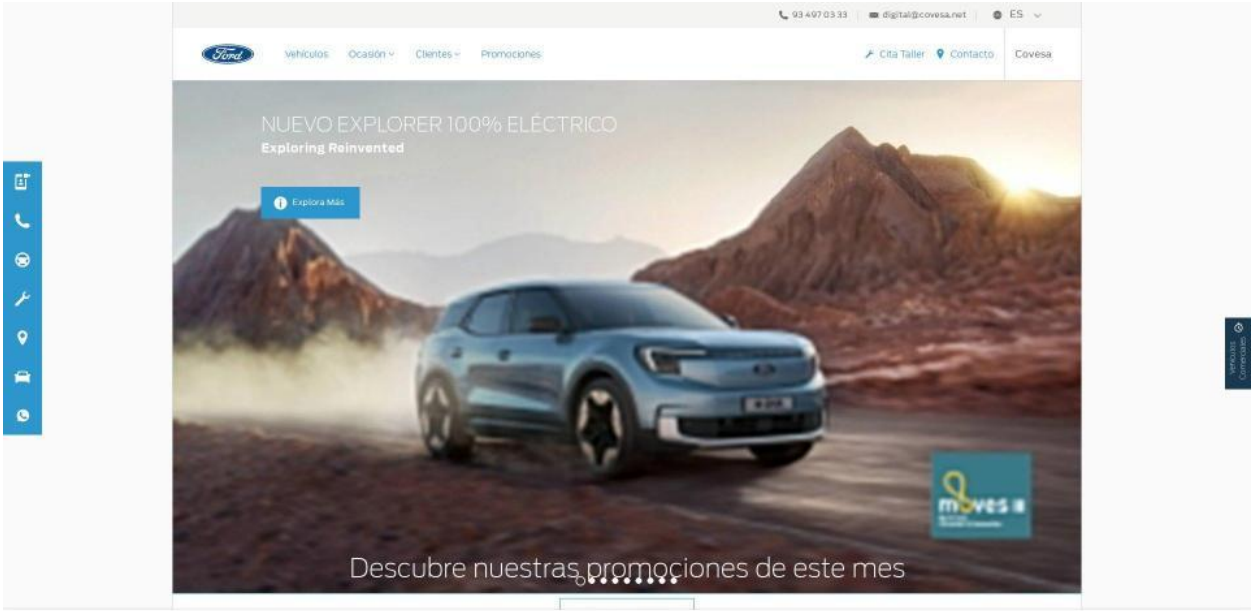
We began our investigation by determining which of the domains identified as IoCs remained live via screenshot lookups. A majority, 162 to be exact, continued to host live content.




While it's a common practice to take down malicious domains once detected, some may remain up because they are actually legitimate but have been compromised. An example would be tiger[.]jp, a legitimate domain of Tiger Corporation. A malware check for it, in fact, shows that it's not currently considered malicious.

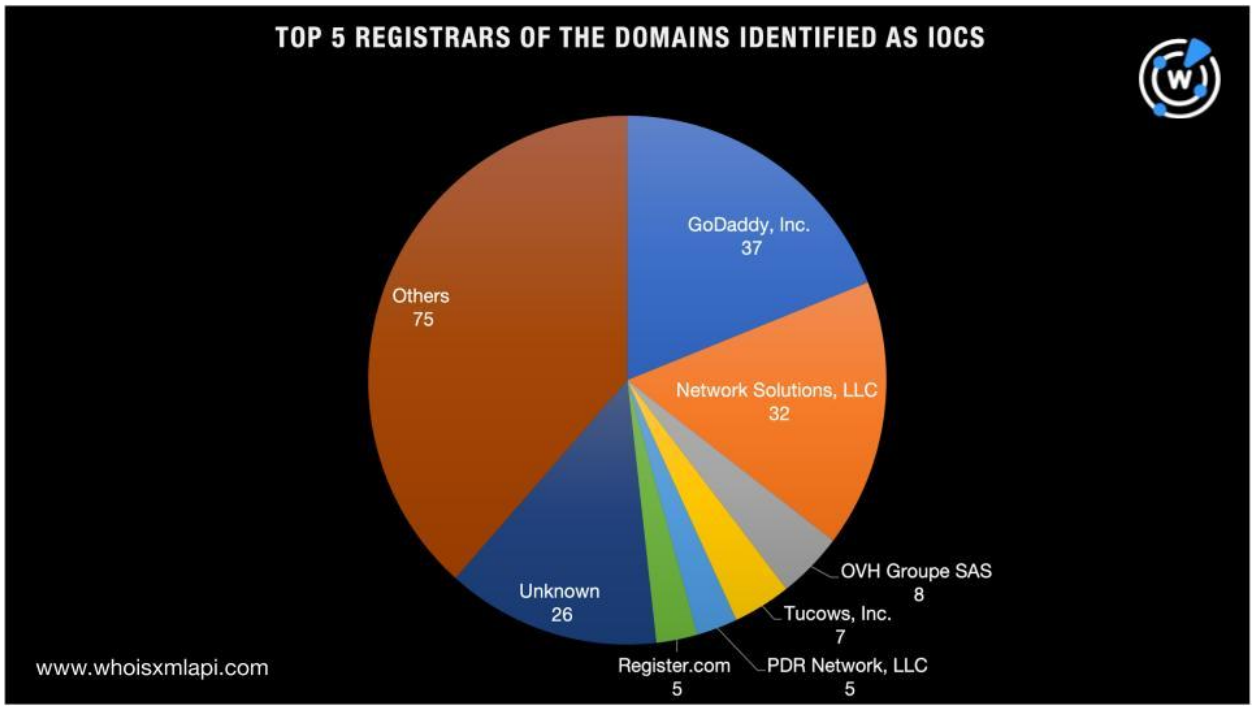

***Screenshot of tiger[.]jp***

It's also interesting to note that the site hosted on the IoC grupcovesa[.]com sported the Ford logo even if its registrant isn't the same as that of ford[.]com, Ford Motor Company's official website, based on a WHOIS lookup. It could be cybersquatting on the car manufacturer's popularity and may have been used to lure in Ford customers to unknowingly download LockBit onto their computers. Grupcovesa[.]com was, however, the only one among the IoCs that could be categorized as a potential cybersquatter.

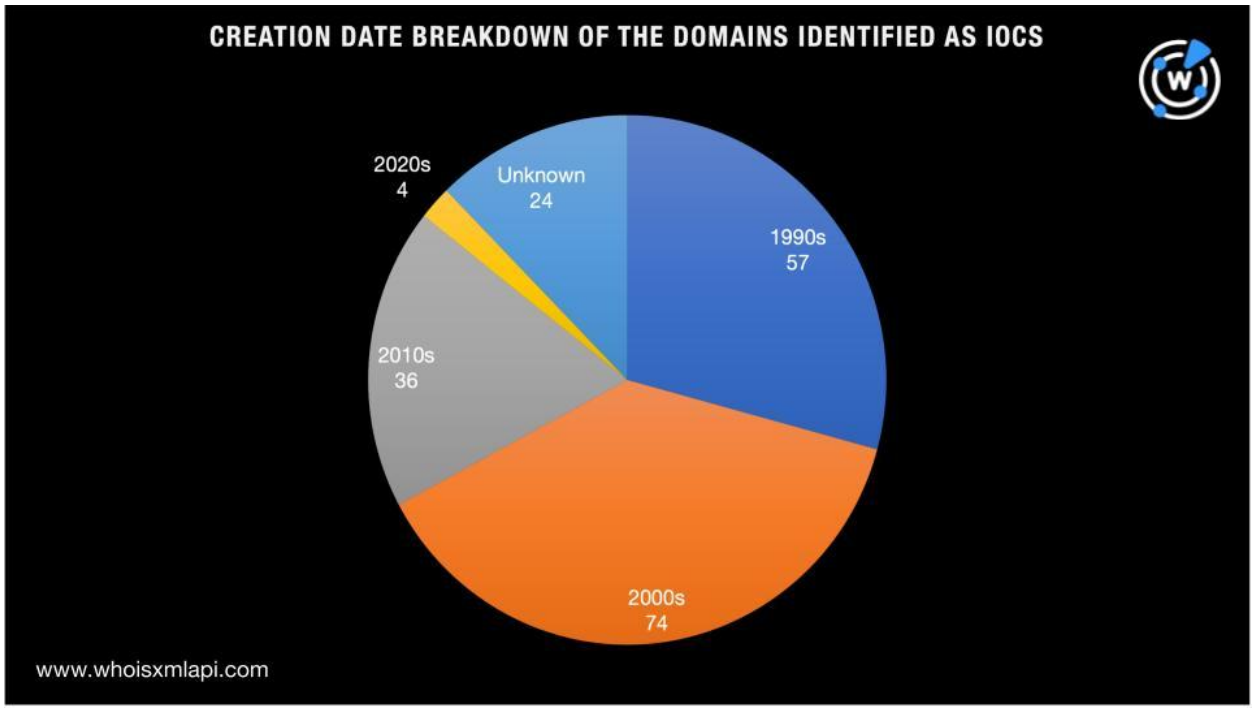



***Screenshot of grupcovesa[.]com***

A bulk WHOIS lookup for the domain IoCs also showed they were spread across 58 registrars topped by GoDaddy (37 domains); Network Solutions (32 domains); OVH Groupe SAS (8 domains); Tucows (7 domains); and PDR Network and Register.com (5 domains each).




The LockBit operators also didn't seem to discriminate in terms of domain age since they used a mix of both old and new domains.

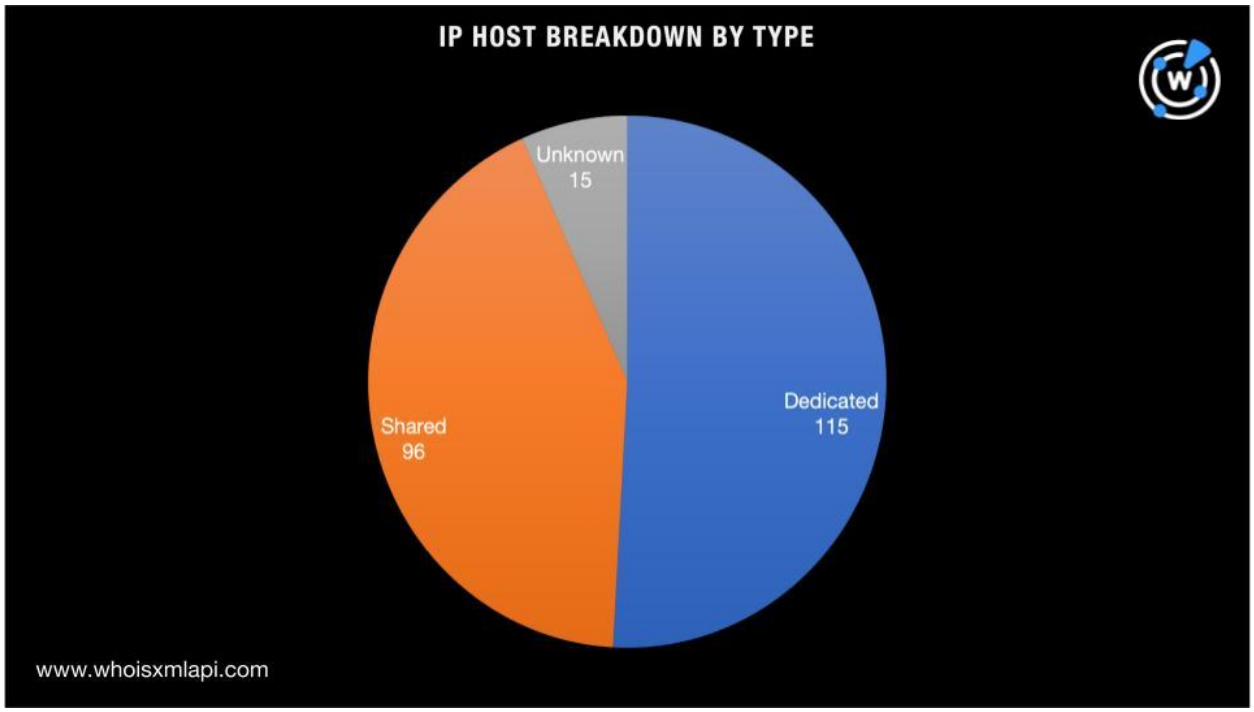


A bulk IP geolocation lookup for the three IP addresses identified as IoCs, meanwhile, revealed that they all pointed to a single country—Singapore—even if they were distributed across two ISPs. The Constant Company managed two of the hosts while the remaining one was under Choopa's control.

## LockBit IoC List Expansion Analysis Findings

To gather as much intelligence on LockBit's infrastructure and its operators, we performed DNS lookups on the domains identified as IoCs. The 195 domains resolved to 226 unique IP addresses.

We then subjected the 229 IP addresses—the three that have been identified as IoCs and the additional 226 from our DNS lookups—to reverse IP lookups. A majority of the IP hosts (51%) were seemingly dedicated as they each had less than 300 connected domains while 42% were shared hosts for having more than 300 connected domains each. The remaining 7% of the IP addresses didn't appear to have connected domains.




Nine of the dedicated IP hosts turned out to be malicious. A bulk IP geolocation lookup for them revealed that most, four to be exact, were geolocated in the U.S.

In addition to the IP host types, our reverse IP lookups also found 6,066 domains that shared the dedicated IP hosts of some of the IoCs. Malware checks then revealed that 16 of them were malicious.

Due to LockBit's aforementioned connection to SocGholish in the past, we sought to determine if the artifacts we discovered for the two malware left similar DNS traces, if any. Here's a summary of our comparison.

- While the SocGholish IP-connected artifacts mostly pointed to Russia, the latest LockBit campaign artifact hosts were concentrated in the U.S. None of the LockBit IP IoCs and artifacts we found were, in fact, geolocated in Russia.
- SocGholish's primary ISP was Selectel while that of LockBit was Amazon. As with the geolocation country, none of the LockBit IP IoCs and artifacts belonged to Selectel.

Overall, therefore, the latest LockBit variant's connection to SocGholish could be just as the ReliaQuest researchers thought—now nonexistent.

—

IoC expansion analyses aided by comprehensive DNS intelligence are effective means to identify as many possibly connected artifacts to specific threats as possible. They can also help determine the scale of a specific threat groups' infrastructure. Our LockBit investigation, for instance, showed that its operators may have favored compromising legitimate domains instead of using newly registered domains (NRDs). It also supported other security researchers' claim regarding a change in the ransomware group's distribution tactic. The latest LockBit variant no longer has ties to SocGholish.

***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.***

# Appendix: Sample Artifacts and IoCs

## Sample Domains Identified as LockBit IoCs

- abilways[.]com
- b2gi[.]fr
- cdcbmestihl[.]com
- dcashpro[.]com
- eds-automotive[.]de
- fabeckarchitectes[.]lu
- garrottbros[.]com
- handrhealthcare[.]com
- id-logistics[.]com
- jams[.]edu[.]jo
- k-toko[.]com
- lsa-international[.]com
- mandirisekuritas[.]co[.]id
- nicklaus[.]com
- omegaservicos[.]com[.]br
- peachtree-medical[.]com
- rbroof[.]com
- sabena-engineering[.]com
- tdtu[.]edu[.]vn
- uhloans[.]com
- vcclawservices[.]com
- waldogeneral[.]com
- xpresscargoinc[.]com

## Sample IP Addresses Identified as IoCs

- 139[.]180[.]184[.]147
- 45[.]32[.]108[.]54

## Sample IP Addresses to Which the Domains Identified as IoCs Resolved

- 100[.]24[.]208[.]97
- 101[.]53[.]19[.]99
- 103[.]18[.]244[.]112
- 103[.]233[.]0[.]178
- 103[.]27[.]74[.]13
- 103[.]3[.]246[.]76
- 104[.]196[.]146[.]230
- 104[.]196[.]197[.]188
- 104[.]196[.]224[.]135
- 104[.]198[.]14[.]52
- 104[.]21[.]14[.]148
- 104[.]21[.]14[.]29
- 104[.]21[.]19[.]159
- 104[.]21[.]22[.]165
- 104[.]21[.]25[.]97
- 104[.]21[.]4[.]215
- 104[.]21[.]59[.]94
- 104[.]21[.]8[.]88
- 104[.]26[.]4[.]120
- 104[.]26[.]5[.]120
- 104[.]26[.]6[.]184
- 104[.]26[.]6[.]32
- 104[.]26[.]7[.]184
- 104[.]26[.]7[.]32
- 104[.]26[.]8[.]140
- 104[.]26[.]9[.]140
- 107[.]180[.]29[.]216
- 109[.]234[.]165[.]67
- 110[.]232[.]143[.]1
- 119[.]59[.]100[.]50
- 120[.]89[.]55[.]86
- 122[.]10[.]113[.]13
- 122[.]248[.]237[.]25
- 128[.]199[.]197[.]201
- 130[.]185[.]85[.]230
- 130[.]255[.]187[.]120
- 134[.]119[.]101[.]242
- 135[.]181[.]45[.]80
- 138[.]201[.]201[.]163
- 140[.]227[.]106[.]120
- 141[.]193[.]213[.]10
- 141[.]193[.]213[.]11
- 143[.]125[.]244[.]236
- 146[.]148[.]118[.]17
- 146[.]148[.]53[.]236
- 148[.]62[.]1[.]241
- 15[.]197[.]142[.]173
- 151[.]101[.]1[.]91
- 151[.]101[.]129[.]91
- 151[.]101[.]130[.]159

## Sample Malicious IP Hosts

- 100[.]24[.]208[.]97
- 103[.]27[.]74[.]13
- 104[.]198[.]14[.]52
- 107[.]180[.]29[.]216
- 141[.]193[.]213[.]10
- 141[.]193[.]213[.]11
- 15[.]197[.]142[.]173
- 151[.]101[.]1[.]91
- 151[.]101[.]130[.]159
- 151[.]101[.]65[.]91
- 162[.]210[.]97[.]218
- 185[.]230[.]63[.]107

- 185[.]230[.]63[.]171
- 185[.]230[.]63[.]186
- 185[.]31[.]40[.]13
- 192[.]124[.]249[.]161
- 192[.]124[.]249[.]18
- 192[.]124[.]249[.]3
- 192[.]169[.]220[.]85
- 192[.]185[.]129[.]96

## Sample Domains That Shared the IoCs' Dedicated IP Hosts

- 057c4dfec7a7496b9cb15480164e49c6[.]emt[.]cf[.]ww[.]aiv-cdn[.]net
- 0937987567[.]com[.]tw
- 0982508849[.]com[.]tw
- 1[.]141[.]208[.]35[.]bc[.]googleusercontent[.]com
- 1[.]ohla[.]org
- 1000weststorage[.]com
- 1012properties[.]com
- 101na[.]com
- 108equity[.]com
- 113[.]109[.]206[.]35[.]bc[.]googleusercontent[.]com
- 119[.]108[.]209[.]35[.]bc[.]googleusercontent[.]com
- 119taipei[.]org[.]tw
- 12p[.]com[.]tw
- 135[.]224[.]196[.]104[.]bc[.]googleusercontent[.]com
- 135network[.]com
- 144[.]26[.]89[.]34[.]bc[.]googleusercontent[.]com
- 15[.]169[.]202[.]35[.]bc[.]googleusercontent[.]com
- 1501health[.]com
- 163[.]200[.]74[.]97[.]host[.]secureserver[.]net
- 17[.]118[.]148[.]146[.]bc[.]googleusercontent[.]com
- 177[.]208[.]185[.]35[.]bc[.]googleusercontent[.]com
- 178[.]208[.]51[.]169[.]static[.]hosted[.]by[.]combell[.]com
- 184[.]210[.]208[.]35[.]bc[.]googleusercontent[.]com
- 188[.]197[.]196[.]104[.]bc[.]googleusercontent[.]com
- 19-clean[.]ca
- 196[.]23[.]117[.]34[.]bc[.]googleusercontent[.]com
- 1e[.]1f[.]3da9[.]ip4[.]static[.]sl-reverse[.]com
- 1fcbocholt[.]de
- 1gainesville[.]com
- 1r2chat[.]com
- 1r2tchat[.]com
- 1seulclic[.]com
- 1sixoneeight[.]com
- 1stclassmortgageservice[.]com
- 1stopcomputerservice[.]com
- 203[.]72[.]215[.]35[.]bc[.]googleusercontent[.]com
- 20clinic[.]com[.]tw
- 20il[.]co[.]il
- 20il[.]co[.]il
- 20il[.]co[.]il
- 210-65-88-201[.]hinet-ip[.]hinet[.]net
- 230[.]146[.]196[.]104[.]bc[.]googleusercontent[.]com
- 236[.]53[.]148[.]146[.]bc[.]googleusercontent[.]com
- 25hours[.]com[.]tw
- 26medias[.]com
- 29[.]129[.]208[.]35[.]bc[.]googleusercontent[.]com
- 2h-ailleurs[.]com
- 2ndwind[.]org

- 2solvit[.]com
- 3-werf[.]com
- 3[.]227[.]12[.]198[.]host[.]secureserver[.]net
- 360business[.]uk[.]com
- 37northrealtygroup[.]com
- 39wq6ua[.]impervadns[.]net
- 3alex[.]eu
- 3d-hipmas[.]eu
- 3d-hipmas[.]eu
- 3dcncafrica[.]co[.]za
- 3pedras[.]com
- 3rspresentes[.]com
- 3v3uflh[.]impervadns[.]net
- 420partytours[.]com
- 444dirt[.]com
- 4bcloud[.]io
- 4t5films[.]com
- 4wallsnh[.]com
- 50lu-710n-v3l0[.]fr
- 55181c9863f54a2e98f4afc07917f051[.]emt[.]cf[.]ww[.]aiv-cdn[.]net
- 59[.]194[.]62[.]50[.]host[.]secureserver[.]net
- 5vp53i5[.]impervadns[.]net
- 647f[.]com
- 666-gogo[.]com
- 666-gogo[.]com
- 72cndrx[.]impervadns[.]net
- 786club[.]org
- 7fm-fmea[.]com
- 7steps6figures[.]com
- 813seniors[.]com
- 8bp4ny6[.]impervadns[.]net
- 94oggi8[.]impervadns[.]net
- 95[.]30[.]120[.]34[.]bc[.]googleusercontent[.]com
- 99investment[.]com[.]na
- a11ysyllabus[.]site
- a2z-consulting[.]com[.]pt
- a2z[.]pt
- a6autos[.]com
- a7ym8po[.]x[.]incapdns[.]net
- aaaaaaaaaaaaaaaaaaaaaaciwxkoaaaaaaaayaaaa[.]shard-3[.]pop-iad-2[.]cf[.]hls[.]row[.]aiv-cdn[.]net
- aaaaaaaaaaaaaaaaaaaaaacmbbtiaaaaaaaayaaaa[.]shard-3[.]pop-iad-2[.]cf[.]hls[.]row[.]aiv-cdn[.]net
- aaaaaaaaaaaaaaaaaaaaaacv3daiaaaaaaaayaaaa[.]shard-2[.]pop-iad-2[.]cf[.]hls[.]row[.]aiv-cdn[.]net
- aaaaaaaaaaaaaaaaaaaaaacybc3iaaaaaaaayaaaa[.]shard-3[.]pop-iad-2[.]cf[.]hls[.]row[.]aiv-cdn[.]net
- aaronlomax[.]com
- aaronlomax[.]com
- aaronscottyoung[.]com
- ab7nsp3[.]impervadns[.]net
- abadiacar[.]com
- abalone-services[.]com
- abarthmarcosautomocion[.]com
- abas-software[.]in
- abas-thailand[.]com

## Sample Malicious IP-Connected Domains

- 1e[.]1f[.]3da9[.]ip4[.]static[.]sl-reverse[.]com
- atlantis[.]com[.]na
- coastalimports[.]com[.]na
- dphenam[.]com
- ecapturetech[.]com
- everclean[.]com[.]na
- expressnam[.]com
- healingphysiohands[.]com