LockBitランサムウェアの痕跡をDNSでたどる

目次

要旨

ReliaQuestは、現在最も効果的で、最も多発しているランサムウェアの1つとしてLockBitを挙げています。実際、ReliaQuestが発表している四半期ごとのランサムウェアリストでは、2022年に引き続き、2023年1〜3月期においてもLockBitが首位を獲得しました。

LockBitは昨年、SocGholishの感染を通じて配布されて研究者の関心を集めました。今日では、LockBitの運用者はランサムウェア・アズ・ア・サービス（RaaS）モデルを採用するようになっています。

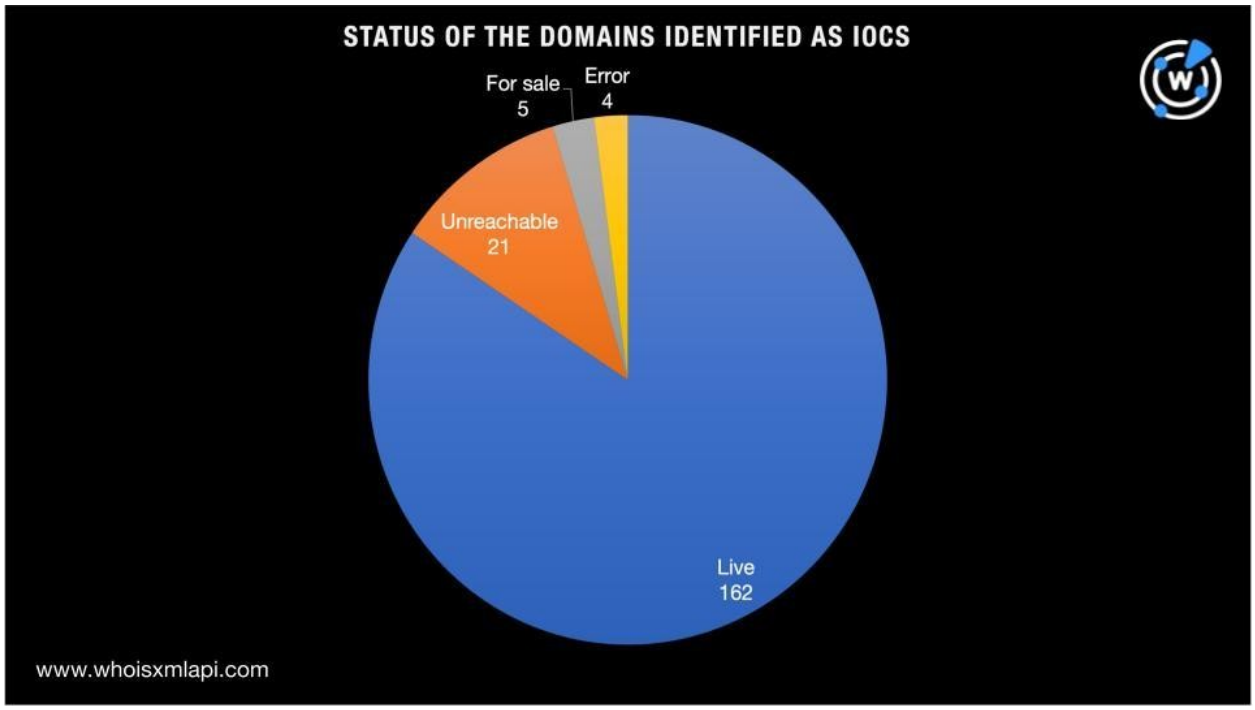
WhoisXML APIでは、インターネットの安全性と透明性を高めるというミッションのもと、一般に公開されているLockBitのIoCのリストを拡張し、関連性が疑われる他のアーティファクトを特定することにしました。そして、この調査の結果、以下を発見しました。

- IoCとして特定されたドメイン名が名前解決した226個のIPアドレス。そのうち20%には悪意があることが判明
- IoCが使うIPホストの一部を共用している6,066個のドメイン名。うち16個はマルウェアホストと確認

LockBitのIoC

AlienVault OTXは先般、LockBitのIoCとして195個のドメイン名と3個のIPアドレスを公表しました。本レポートの付録にその例を収録しています。

そこで、当社はまずScreenshot Lookupを使い、IoCとして特定されたドメイン名のうちどれが有効な状態にあるかを把握することにしました。その結果、162個がアクティブなコンテンツをホストし続けていることがわかりました。



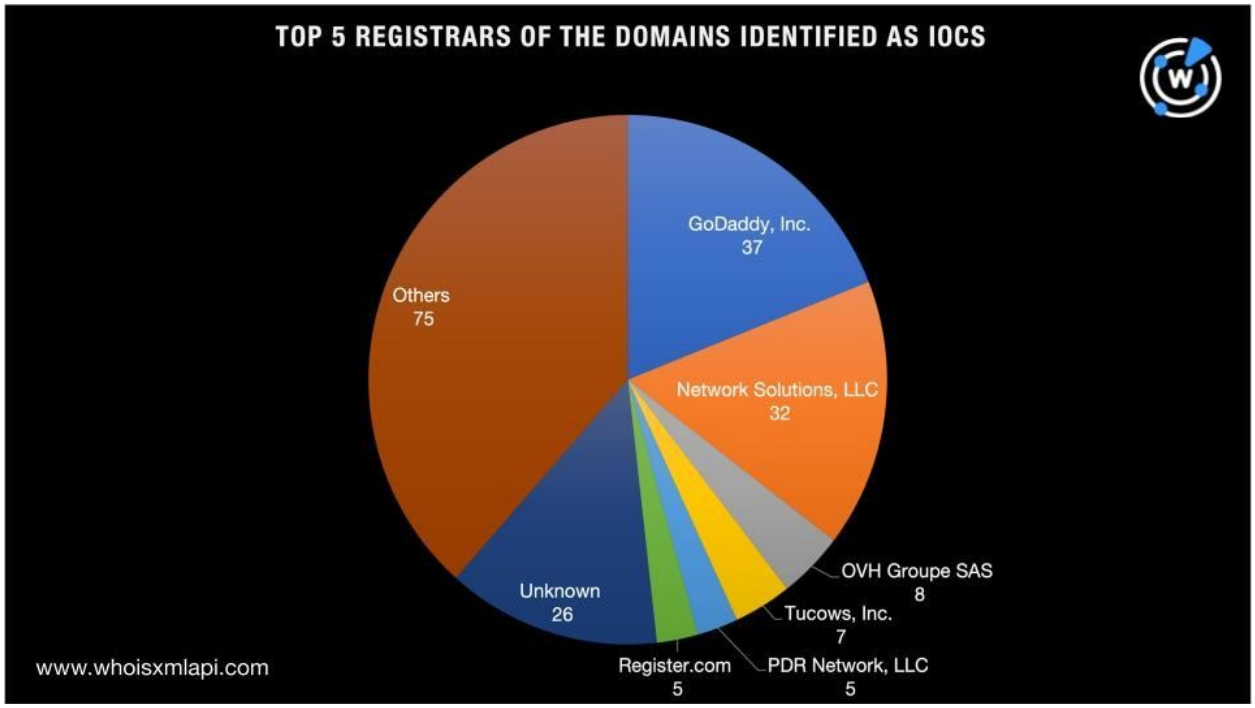
一般に、悪意あるドメイン名は検出されると閉鎖されます。しかし、中には閉鎖されずに残っているものもあります。それらは合法的なドメイン名ではあるものの、不正利用されたことがあるものです。例えば、LockBitのIoCリストに含まれているtiger[.]jpはタイガー魔法瓶株式会社の正規のドメイン名です。このドメイン名に対してマルウェアチェックをしたところ、その時点では悪意があると見なされていませんでした。

Screenshot of tiger[.]jp

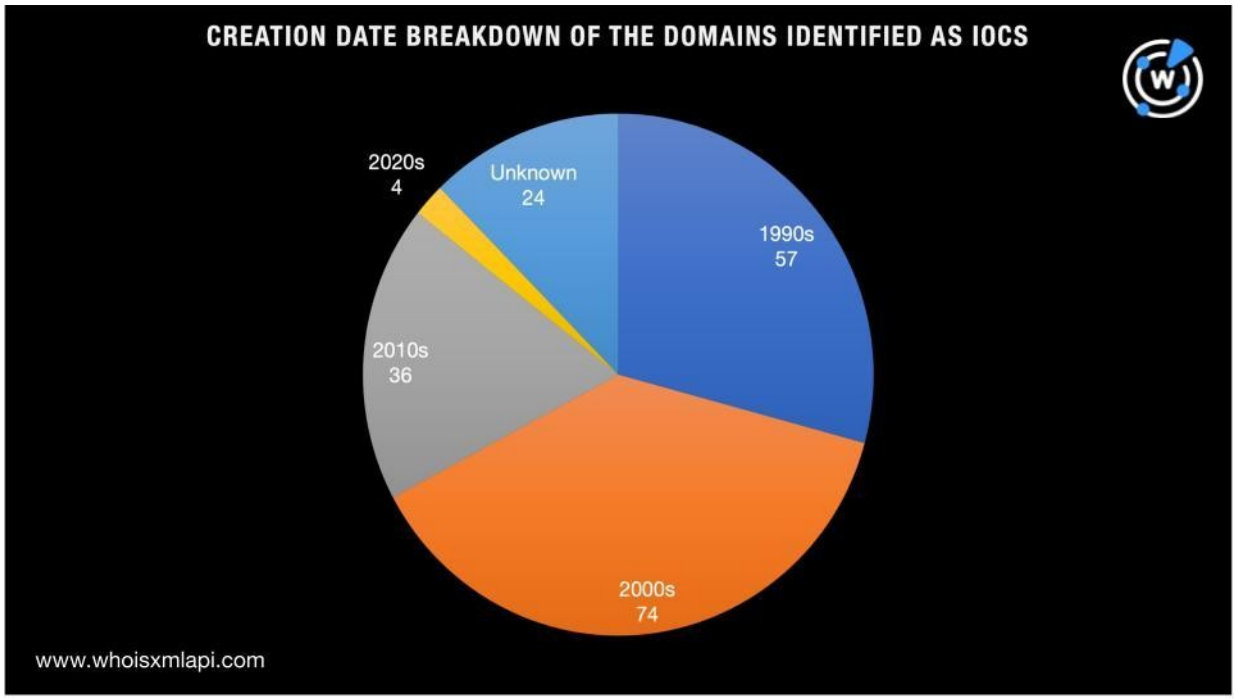
もう一つのドメインIoCであるgrupcovesa[.]comについては、ドメイン名の登録者がFord Motor Companyの公式ドメイン名ford[.]comの登録者とは異なっていました。それにもかかわらず、grupcovesa[.]comでホストされているサイトではFordのロゴを使用していました。これは、Fordの知名度を利用したサイバースクワッティングかもしれません。Fordの顧客をルアーに誘い込み、無意識のうちにLockBitをコンピューターにダウンロードさせるために使われた可能性があります。ただし、IoCの中でサイバースクワッターの可能性があったのはgrupcovesa[.]comのみでした。

Screenshot of grupcovesa[.]com

公開されているドメインIoCをbulk WHOIS lookupで一括検索したところ、GoDaddy（37ドメイン）、Network Solutions（32ドメイン）、OVH Groupe SAS（8ドメイン）、Tucows（7ドメイン）、PDR NetworkとRegister.com（各5ドメイン）をトップとする58のレジストラに分散して管理されていることもわかりました。



また、LockBitの運用者は古いドメイン名と新しいドメイン名の両方を混ぜて使用しており、ドメイン名の年齢という点では特に区別していないらしいことも確認されました。

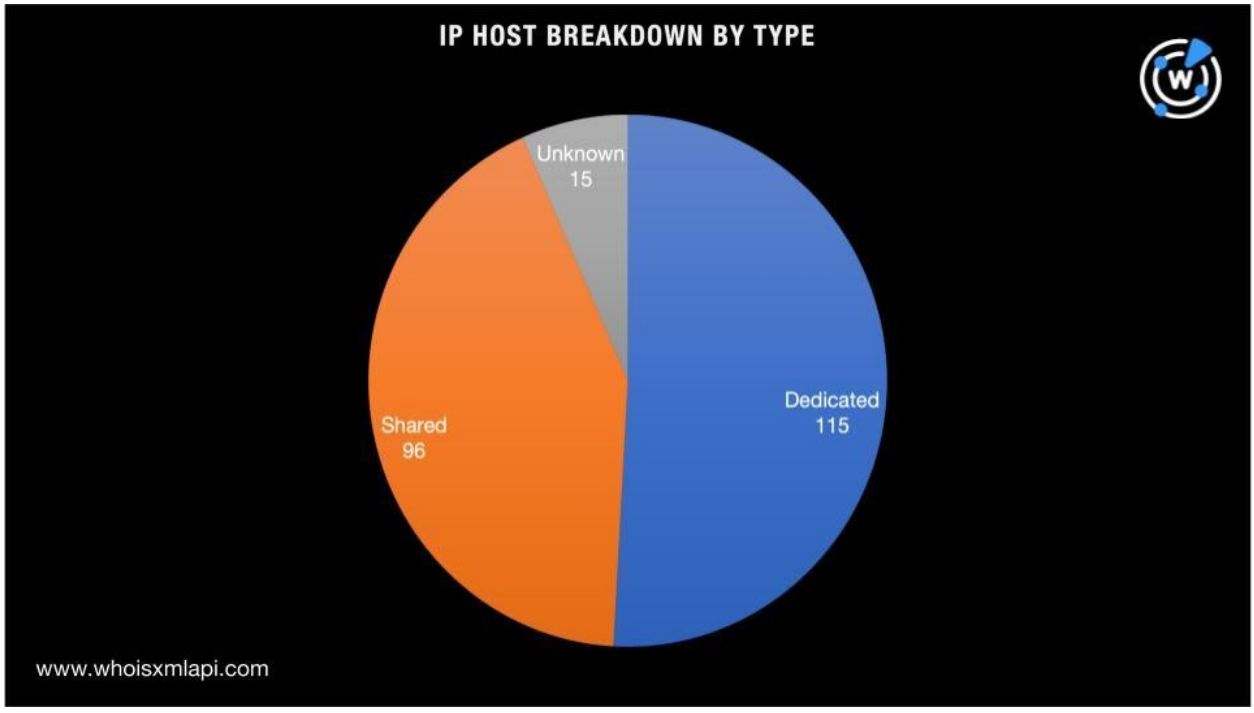


その一方で、IoCとして特定された3つのIPアドレスをbulk IP geolocation lookupで検索したところ、2つのISPに分散していたものの、全てシンガポールを指していることが判明しました。Constant Companyが2つを管理し、残りの1つはChoopaが管理していました。

LockBitのIoCリストの拡張

LockBitのインフラとその運用者についてできるだけ多くの情報を収集するため、IoCとして特定されたドメイン名をDNS Lookupで検索しました。その結果、195個のドメイン名は226個のユニークなIPアドレスに解決しました。

次に、IoCとしてすでに特定されている3つのIPアドレスと当社のDNS Lookupで見つかった226個のIPアドレスをReverse IP Lookupにかけてみました。51%のIPアドレスは関連付けられたドメイン名が300に満たないことから、専用ホストと思われます。他方、42%は300超の関連ドメイン名があることから共用ホストのようでした。残りの7%は、ドメイン名に関連づけられていませんでした。



専用IPアドレスのうち9つは悪意のあるアドレスと判明しました。また、それらの地理的位置を一括検索したところ、4つは米国にあることが確認されました。

また、当社のReverse IP Lookupの結果、一部のIoCの専用IPホストを共用している6,066個のドメイン名も特定されました。マルウェアチェックにより、そのうちの16個には悪意があることが判明しました。

LockBitが過去にSocGholishと関係していたことから、この2つのマルウェアで発見されたアーティファクトがDNSに同じような痕跡を残しているかどうかを調べました。その結果の概要は以下の通りです。

- 共通のIPアドレスを使っていたSocGholish関連のアーティファクトのほとんどはロシアを指していました。他方、最新のLockBitキャンペーンのホストは米国に集中していました。当社が発見したLockBitのIPアドレスIoCとアーティファクトのうち、地理的にロシアに位置しているものはありませんでした。
- SocGholishの主たるISPはSelectelでしたが、LockBitの主要ISPはAmazonでした。LockBitのIPアドレスIoCとアーティファクトの中にSelectelの管理下にあるものはありませんでした。

したがって、LockBitの最新の亜種とSocGholishの関連性は、ReliaQuestの研究者が考えていた通り、現在は存在しないのかもしれません。

—

包括的なDNSインテリジェンスに基づくIoCリストの拡張分析は、特定の脅威との関連が疑われるアーティファクトを洗い出す効果的な手段です。また、脅威グループのインフラの特徴を知る上でも役立ちます。例えば今回のLockBitの調査では、その運用者が新規登録ドメイン名を使用するのではなく、既存の正規のドメイン名を侵害するやり方を好んでいた可能性が示されました。また、ランサムウェア配布の戦術が変化しているという他のセキュリティ研究者の主張も裏付けられました。最新のLockBitの亜種は、もはやSocGholishと結びついていません。

同様の調査をご希望のお客様、または本調査で使用された当社の商品にご興味をお持ちのお客様は、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

LockBitのIoCとして特定されたドメイン名の例

- 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

IoCとして特定されたIPアドレスの例

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

IoCとして特定されたドメイン名が名前解決したIPアドレスの例

- 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

悪意あるIPホストの例

- 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

IoCの専用IPホストと同じIPアドレスに名前解決したドメイン名の例

- 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
- aaaaaaaaaaaaaaaaaaaaaaacmbbtiaaaaaaaayaaaa[.]shard-3[.]pop-iad-2[.]cf[.]hls[.]row[.]aiv-cdn[.]net
- aaaaaaaaaaaaaaaaaaaaaaacv3daiaaaaaaaayaaaa[.]shard-2[.]pop-iad-2[.]cf[.]hls[.]row[.]aiv-cdn[.]net
- aaaaaaaaaaaaaaaaaaaaaaacybc3iaaaaaaaayaaaa[.]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

共通のIPアドレスを使用していた悪意あるドメイン名の例

- 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