



WhoisXMLAPI

The Who Behind Domain, IP & Cyber Threat Intelligence

DNSでWoofLockerの実態を解明

目次

1. [要旨](#)
2. [付録：アーティファクトとIoCの例](#)

要旨

テクニカルサポート詐欺のツールキット「WoofLocker」は、2017年以降各所で大混乱を引き起こしています。その背後にいる脅威アクターはまだ活動を終わっておらず、むしろ脅威の耐性が増している可能性があります。侵害されたサイトを配布ベクトルとして使用する以外に、WoofLockerは[複雑なトラフィック配信スキーム](#)を使い始めました。

AlienVault OTXはこれまでに、346個のドメイン名と438個のIPアドレスを[WoofLockerのセキュリティ侵害インジケータ（IoC）](#)を収集しました。しかし、WoofLockerが8年もの間存在し続けていることから、見過ごされている未報告のウェブプロパティが他にあるかもしれません。

そこで、当社はこのほどDNSでWoofLockerを徹底的に調査し、以下を発見しました。

- IoCとして特定された一部のドメイン名が名前解決した、17個の未報告のIPアドレス
- IoCの専用IPホストの一部を共有していた1,194個の未報告のドメイン名
- マルウェア一括チェックで見つかった、共通のIPアドレスを使っている悪意ある18個のドメイン名

WoofLockerの隠れた実態

WoofLockerは8年の長きにわたり運用されてきました。そのため、様々なレジストラを使い、古いドメイン名と新規登録ドメイン名（NRD）を組み合わせ、世界中にインフラを展開しているように思えるかもしれません。しかし、本当にそうだったのでしょうか？それを確かめるため、当社はDNSを使ってWoofLockerの実態を解明することにしました。

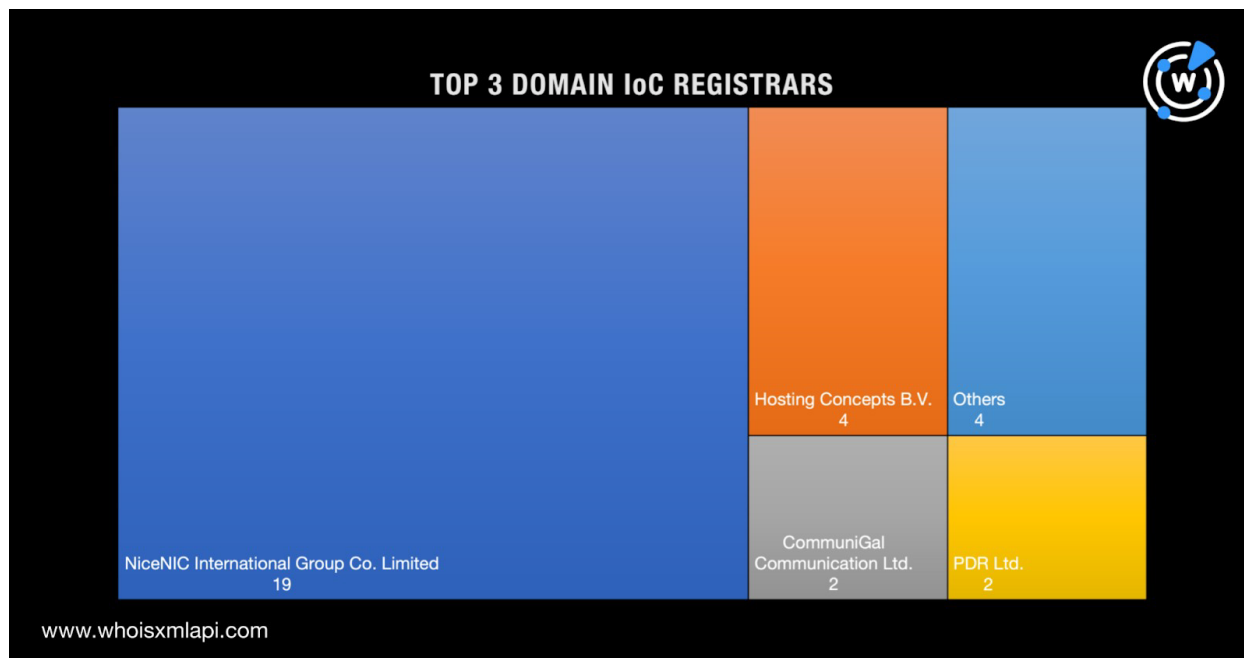
ドメインIoCの分析

まず、AlienVault OTX がIoCとして特定した346個のドメイン名（ドメインIoC）を[Bulk](#)

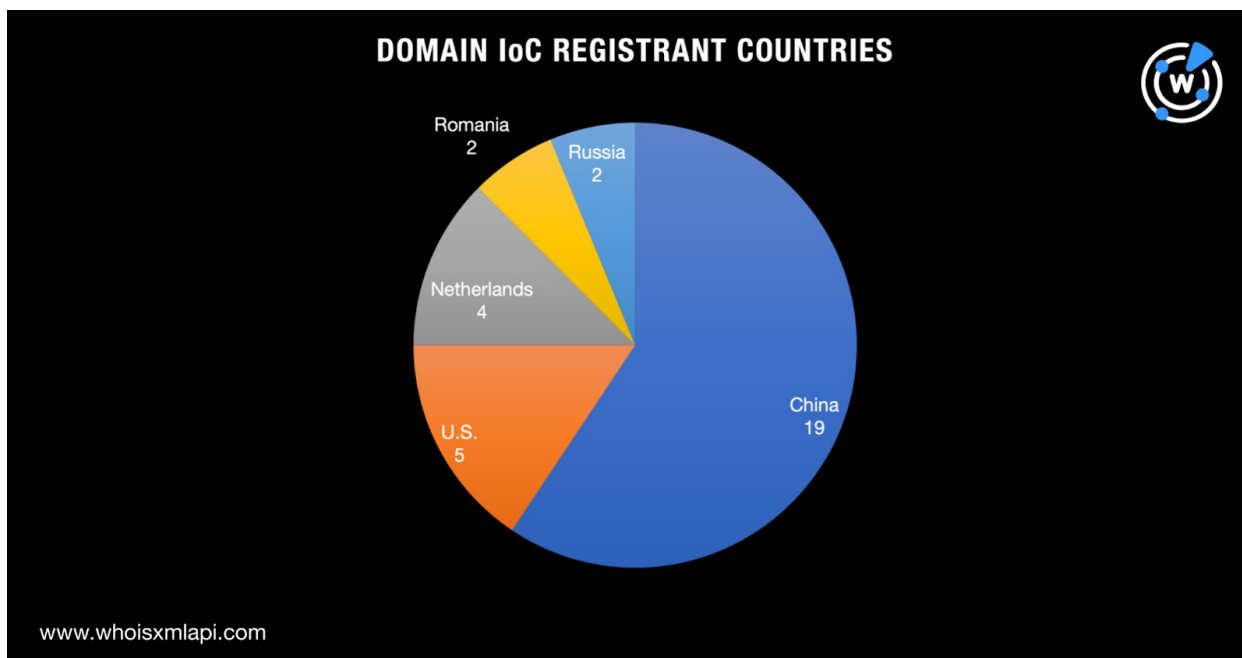


[WHOIS Lookup](#)で検索したところ、次のような発見がありました。

- 346個のうち、WHOISレコードが存在していたものは32個にとどまりました。そのうちの61%は、NiceNIC International Group Co. Limited（4個）、Hosting Concepts B.V.（4個）、CommuniGal Communication Ltd.（2個）、PDR Ltd.（2個）をレジストラとして使用していました。



- 78%はNRDで、19%は2021年と2022年に登録された新しいドメイン名でした。また、1個については、登録年月日の記録がありませんでした。
- 19個は中国で登録されたドメイン名でした。残りのドメイン名の登録国は4カ国に分散しており、米国（5個）、オランダ（4個）、ルーマニア（2個）、ロシア（2個）となっていました。

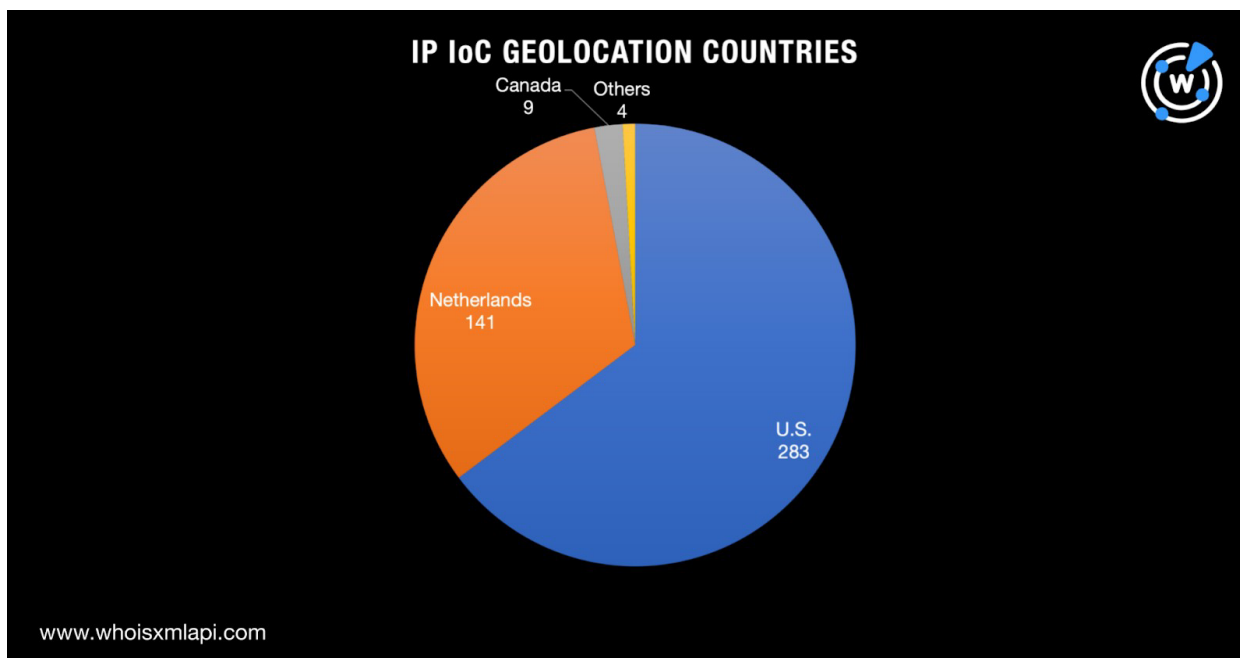


- ルーマニアで登録された2個のドメインIoC（mylandings[.jusとourlovestories[.jus）は登録者のメールアドレスが同じで、Gmailのものでした。このメールアドレスを [Reverse WHOIS Search](#) で検索したところ、10,000個を超えるドメイン名が共用していることがわかりました。この登録者はドメイナーなのかもしれません。

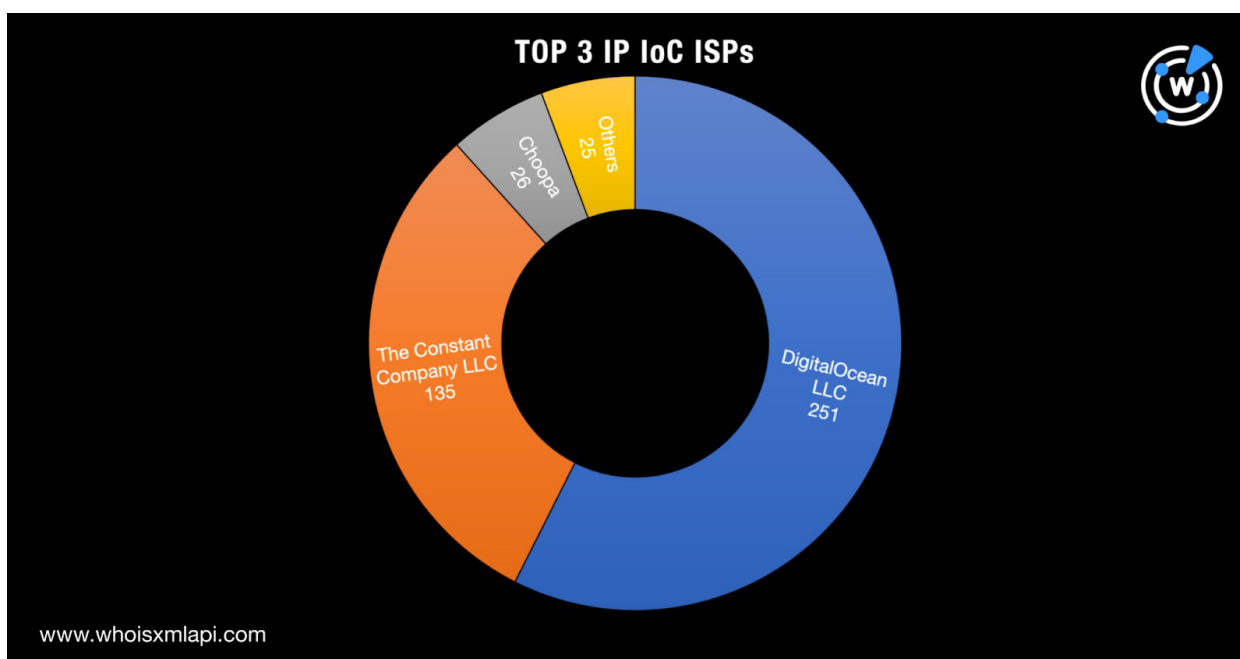
IP IoCの分析

次に、IoCとして特定されたIPアドレス（IP IoC）を [Bulk IP Geolocation Lookup](#) で精査したところ、以下のことが判明しました。

- 大半（283個）のIPアドレスが米国に位置していました。次に多かったIPジオロケーションは、オランダ（141個）とカナダ（9個）でした。



- IoCの管理ISPとして17社が特定されました。管理アドレス数が最も多かったのは DigitalOcean LLC (251個) で、これにConstant Company LLC (135個)、Choopa (26個) が続きました。



今回行ったドメインIoCおよびIP IoCの分析により、いくつかの疑問に対する答えを得ることができました。WoofLockerは長年運用されているにもかかわらず、使っていたレジストラとISPの数は限られていました(9社のレジストラと12社のISP)。また、346個のドメインIoCのうち、WHOISレコードが存在していたのはわずか32個であったことから、WoofLockerはNRDを好む傾向があるようです。WHOISレコードのないドメイン名は、意図的に失効または廃止させる目



的で放置されていた可能性があります。

また、WoofLockerのインフラは、限られた数カ国にあるようでした。ドメイン名の登録国は5カ国、IPアドレスのジオロケーションが指したのは8カ国にとどまりました。

WoofLockerのIoCをさらに調査

当社では、WoofLockerの内部の動きについても調査しました。

まず、この脅威が何年にもわたって存在していることを考慮し、未公開のアーティファクトがあるかどうかを調べました。ドメインIoCを[DNS Lookup](#)で検索したところ、17個のIPアドレス（12個のIPv4アドレスと5個のIPv6アドレス）を新たに発見しました。

これにより、脅威に関連しているIPアドレスの総数（IoCと今回見つかったIPアドレスの合計）は451個になりました。そこで、誤検出を抑制するために専用IPアドレスのみに焦点を絞って分析した結果、より深く調べるべきIPアドレスが104個残りました。

その104個のIPアドレスを[Reverse IP Lookup](#)で検索したところ、関連するドメイン名が1,194個見つかりました。それらのドメイン名に対して一括マルウェアチェックを実行した結果、19個が悪意あるドメイン名と確認されました。さらに、その悪意あるドメイン名のうち2個については、今も有効なコンテンツをホストし続けています。1つはニュースサイト、もう1つはブログのように見えます。



OXOFF.INFO EN CONTACTS CATEGORIES BLOVES OX417274 DAFUQ IS THIS? Q

EMPLOI **LE PORTAGE SALARIAL DANS SON MILIEU NATUREL**
 OxFF | 16 July 2021
 Après un comparatif des méthodes d'accès à l'emploi : CDI en interne, CDI en SSII/ESN (prestation de service), Freelance et Portage Salarial dans mon article intitulé Petit manuel [Read More](#)

EMPLOI **PETIT GUIDE DE LA FREELANCE (2023)**
 OxFF | 14 July 2021
 Dernière mise à jour : 24/02/2023 Bonjour jeune entrepreneur, toi aussi tu rêves de... Mais ta gueule putain ! Vous avez peut-être parcouru mon précédent papier Petit manuel d'auto-défense [Read More](#)

SECURITY **ADVANCED BUFFER OVERFLOW – BYPASS ASLR (32 BITS)**
 OxFF | 28 January 2021
 Dans le cours d'introduction aux Buffer Overflows et à GDB, je vous ai parlé de quelques sécurités système qui si elles n'empêchent pas d'exploiter ce type de vulnérabilités, compliquent [Read More](#)

VULNERABILITIES **ATTAQUE CÔTÉ CLIENT – XSS ET PHISHING**
 OxFF | 12 January 2021
 [Voix Off d'Enquête exclusive] Vol de mot de passe, création de bot-net, la vie sur internet est devenue une jungle. Si nos antivirus et nos pare-feux nous assurent [Read More](#)

SNIPPING/SPOOFING **MITM ET SPOIT BASIQUES EN PYTHON**
 OxFF | 3 January 2021
 Voici un petit article que j'écrivais traitant de reconnaissance réseau relatif à Infocur afin de faire des trucs nuls et de pouvoir voler les mots de passe et transmuter l'ip.

OxOff[.]infoのスクリーンショット

Dariamariposa

Privacy Policy telegram

Mindblown: a blog about philosophy.

Got any book recommendations?

[Get In Touch](#)

Dariamariposa

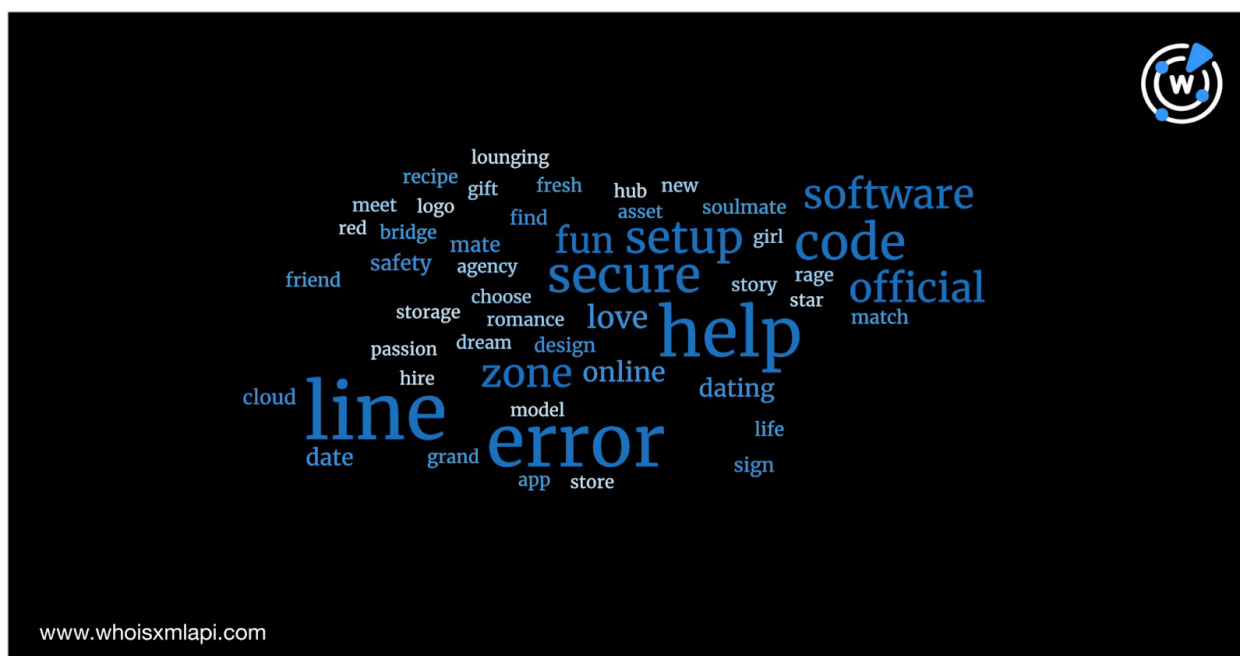
Proudly powered by [WordPress](#)

dariamariposa[.]comのスクリーンショット



また、アダルトサイトを詐欺の手段にするというWoofLockerの傾向にも注目しました。この傾向から、アダルトサイト以外のサイトは、気づかないうちに詐欺に加担してしまうことを心配しなくてもよいと言えるのでしょうか？

その答えを見つけるため、ドメインloCの中に含まれている文字列を特定することにしました。この作業の結果、51個のドメインloCに含まれる**official**を筆頭に、52種類の文字列を特定できました。2番目に多かったのは**zone**で、50個のドメインloCに含まれていました。3番目は**fun**で、41個に見られました。以下はこの分析結果を視覚的に表したものです。



errorhelpline24x7msofficialsoftwareerrorcodex16[.]monster、
errorhelpline24x7msofficialsoftwareerrorgh001[.]monsterおよび
errorhelpline24x7msofficialsoftwareerrornew06[.]monsterは、**official**、**error**、**help**を含んでいるドメイン名です。これらは全てMicrosoftのヘルプラインサイトと思われるものを指しているようでした。そうしたサイトでは、WoofLockerの手口であるテクニカルサポート詐欺が行われます。123個のドメインloCは、.monsterというTLDを使用していました。

また、WoofLockerがアダルトサイトを使う傾向にあることと関連しているかもしれませんが、約200個のドメイン名が出会い系サイトを指しているようでした。とはいえ、アダルト以外のサイト所有者が安全だということにはなりません。**cloud**、**design**、**logo**、**recipe**、**storage**といった文字列も特定されているためです。

—



今回当社が行った調査で、WoofLockerに関する興味深い事実が明らかになりました。WoofLockerは古くからある脅威ですが、その割には限られた場所で、限られた数のプロバイダーを使ってインフラを運用しています。また、キャンペーンにはNRDや新gTLDを好んで使用しているようです。そして、Wooflockerはアダルトサイトの侵害を好むことで知られているものの、クラウド、デザイン、ストレージサービス、料理サイトにも狙いを定めている可能性があります。

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。

免責事項： 当社は、潜在的な危険から企業を守るために役立つ情報の提供を目指しており、脅威の検出に対して厳格な姿勢で臨んでいます。そのため、当初「脅威」または「悪意がある」とみなされたエンティティが、さらなる調査やその後の状況の変化により最終的に無害と判断される可能性があります。ここで提供されている情報を確認する補足調査の実施を強くお勧めします。

付録：アーティファクトとIoCの例

AlienVault OTXが公開したWoofLockerのIoC

- 69chicks[.]site
- adsmyssecrettemptation[.]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
- datelikehilarity[.]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
- dezigndfrutto[.]fun
- dimensionalroute[.]fun
- dippystock[.]site
- divinelovertime[.]us
- e44o4-msg-co-1010100010110[.]cf
- elinorecyrusrosalind[.]site
- enduringlive[.]site
- errorhelpline24x7msofficialsoftwaree
rrorcodex16[.]monster
- errorhelpline24x7msofficialsoftwaree
rrorgh001[.]monster
- errorhelpline24x7msofficialsoftwaree
rrorgh002[.]monster
- errorhelpline24x7msofficialsoftwaree
rrorgh003[.]monster
- errorhelpline24x7msofficialsoftwaree
rrorgh004[.]monster
- errorhelpline24x7msofficialsoftwaree
rrorgh006[.]monster
- errorhelpline24x7msofficialsoftwaree
rrorgh008[.]monster
- errorhelpline24x7msofficialsoftwaree
rrorgh009[.]monster
- errorhelpline24x7msofficialsoftwaree
rrorgh012[.]monster
- errorhelpline24x7msofficialsoftwaree
rrorgh013[.]monster
- errorhelpline24x7msofficialsoftwaree
rrorgh015[.]monster
- errorhelpline24x7msofficialsoftwaree
rrorgh017[.]monster
- errorhelpline24x7msofficialsoftwaree
rrorgh018[.]monster
- errorhelpline24x7msofficialsoftwaree
rrorgh020[.]monster
- errorhelpline24x7msofficialsoftwaree
rrorgh021[.]monster
- errorhelpline24x7msofficialsoftwaree
rrorgh023[.]monster
- errorhelpline24x7msofficialsoftwaree
rrorgh024[.]monster
- errorhelpline24x7msofficialsoftwaree
rrorgh025[.]monster
- errorhelpline24x7msofficialsoftwaree
rrorgh028[.]monster
- errorhelpline24x7msofficialsoftwaree
rrorgh030[.]monster
- errorhelpline24x7msofficialsoftwaree
rrorgh033[.]monster
- errorhelpline24x7msofficialsoftwaree
rrorgh036[.]monster
- errorhelpline24x7msofficialsoftwaree
rrorgh037[.]monster
- errorhelpline24x7msofficialsoftwaree
rrorgh038[.]monster
- errorhelpline24x7msofficialsoftwaree
rrorgh039[.]monster
- errorhelpline24x7msofficialsoftwaree
rrorgh041[.]monster
- errorhelpline24x7msofficialsoftwaree
rrorgh044[.]monster
- errorhelpline24x7msofficialsoftwaree
rrorgh045[.]monster
- errorhelpline24x7msofficialsoftwaree
rrorgh046[.]monster
- errorhelpline24x7msofficialsoftwaree
rrorgh047[.]monster
- errorhelpline24x7msofficialsoftwaree
rrorgh048[.]monster
- errorhelpline24x7msofficialsoftwaree
rrorgh050[.]monster



- errorhelpline24x7msofficialsoftwaree
rrorgh051[.]monster
- errorhelpline24x7msofficialsoftwaree
rrorgh052[.]monster
- errorhelpline24x7msofficialsoftwaree
rrorgh053[.]monster
- errorhelpline24x7msofficialsoftwaree
rrorgh054[.]monster
- errorhelpline24x7msofficialsoftwaree
rrorgh055[.]monster
- errorhelpline24x7msofficialsoftwaree
rrorgh056[.]monster
- errorhelpline24x7msofficialsoftwaree
rrorgh057[.]monster
- errorhelpline24x7msofficialsoftwaree
rrorgh059[.]monster
- errorhelpline24x7msofficialsoftwaree
rrorgh061[.]monster
- errorhelpline24x7msofficialsoftwaree
rrorgh062[.]monster
- errorhelpline24x7msofficialsoftwaree
rrorgh063[.]monster
- errorhelpline24x7msofficialsoftwaree
rrorgh064[.]monster
- errorhelpline24x7msofficialsoftwaree
rrorgh065[.]monster
- errorhelpline24x7msofficialsoftwaree
rrorgh066[.]monster
- errorhelpline24x7msofficialsoftwaree
rrorgh067[.]monster
- errorhelpline24x7msofficialsoftwaree
rrorgh068[.]monster
- errorhelpline24x7msofficialsoftwaree
rrorgh069[.]monster
- errorhelpline24x7msofficialsoftwaree
rrorgh070[.]monster
- errorhelpline24x7msofficialsoftwaree
rrornew06[.]monster
- exoticrefreshment[.]site
- fantabulousfrils[.]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
- helpsecureity24x7errorcodehelpsoft
ware1[.]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
- pcmssecursetup24x7errorcodehel
plinezone1[.]monster
- pcmssecursetup24x7errorcodehel
plinezone10[.]monster
- pcmssecursetup24x7errorcodehel
plinezone11[.]monster
- pcmssecursetup24x7errorcodehel
plinezone12[.]monster
- pcmssecursetup24x7errorcodehel
plinezone14[.]monster
- pcmssecursetup24x7errorcodehel
plinezone15[.]monster
- pcmssecursetup24x7errorcodehel
plinezone2[.]monster
- pcmssecursetup24x7errorcodehel
plinezone3[.]monster
- pcmssecursetup24x7errorcodehel
plinezone4[.]monster
- pcmssecursetup24x7errorcodehel
plinezone5[.]monster
- pcmssecursetup24x7errorcodehel
plinezone7[.]monster
- pcmssecursetup24x7errorcodehel
plinezone8[.]monster
- pcmssecursetup24x7errorcodehel
plinezone9[.]monster
- pcmssecursetup24x7errorcodehel
plinezonedd16[.]monster
- pcmssecursetup24x7errorcodehel
plinezonedd17[.]monster
- pcmssecursetup24x7errorcodehel
plinezonedd18[.]monster
- pcmssecursetup24x7errorcodehel
plinezonedd19[.]monster
- pcmssecursetup24x7errorcodehel
plinezonedd20[.]monster
- pcmssecursetup24x7errorcodehel
plinezonedd21[.]monster
- pcmssecursetup24x7errorcodehel
plinezonedd22[.]monster
- pcmssecursetup24x7errorcodehel
plinezonedd24[.]monster
- pcmssecursetup24x7errorcodehel
plinezonedd25[.]monster
- pcmssecursetup24x7errorcodehel
plinezonedd26[.]monster
- pcmssecursetup24x7errorcodehel
plinezonedd29[.]monster
- pcmssecursetup24x7errorcodehel
plinezonedd30[.]monster
- pcmssecursetup24x7errorcodehel
plinezonedd33[.]monster
- pcmssecursetup24x7errorcodehel
plinezonedd34[.]monster
- pcmssecursetup24x7errorcodehel
plinezonedd38[.]monster
- pcmssecursetup24x7errorcodehel
plinezonedd39[.]monster
- pcmssecursetup24x7errorcodehel
plinezonedd40[.]monster
- pcmssecursetup24x7errorcodehel
plinezonedd43[.]monster
- pcmssecursetup24x7errorcodehel
plinezonedd44[.]monster
- pcmssecursetup24x7errorcodehel
plinezonedd45[.]monster
- pcmssecursetup24x7errorcodehel
plinezonedd46[.]monster
- pcmssecursetup24x7errorcodehel
plinezonedd47[.]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
- pcsecuresafety24x7errorcodez001[.]monster
- pcsecuresafety24x7errorcodez002[.]monster
- pcsecuresafety24x7errorcodez003[.]monster
- pcsecuresafety24x7errorcodez004[.]monster
- pcsecuresafety24x7errorcodez005[.]monster
- pcsecuresafety24x7errorcodez006[.]monster
- pcsecuresafety24x7errorcodez007[.]monster
- pcsecuresafety24x7errorcodez008[.]monster
- pcsecuresafety24x7errorcodez009[.]monster
- pcsecuresetup24x7errorcodehelpline01[.]monster
- pcsecuresetup24x7errorcodehelpline010[.]monster
- pcsecuresetup24x7errorcodehelpline011[.]monster
- pcsecuresetup24x7errorcodehelpline012[.]monster
- pcsecuresetup24x7errorcodehelpline02[.]monster
- pcsecuresetup24x7errorcodehelpline03[.]monster
- pcsecuresetup24x7errorcodehelpline04[.]monster
- pcsecuresetup24x7errorcodehelpline05[.]monster
- pcsecuresetup24x7errorcodehelpline06[.]monster
- pcsecuresetup24x7errorcodehelpline08[.]monster
- pcsecuresetup24x7errorcodehelpline09[.]monster
- pellamofloral[.]fun
- personalonline[.]xyz
- potraiture[.]site
- privys[.]site
- prophyrio[.]site
- puusssymate[.]xyz
- recipesonline365[.]com
- reliabilityassist[.]monster
- roasterrun[.]fun
- saledating[.]xyz



- sassysensations[.]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

IoCが名前解決したIPアドレス（今回の調査で発見）の例

- 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

共通のIPアドレスを使っていたドメイン名の例

- 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
- agroxxpro[.]com
- aike[.]shop
- airfundraiser[.]com
- akhtaboot[.]com
- aktivlizenz[.]de
- alda-ti[.]com
- alicelonergan[.]com
- aliciamariaa[.]com
- allfastag[.]com
- allkeys[.]online
- allkeyes[.]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



- `applianceclinic[.]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`

共通のIPアドレスを使っていた悪意あるドメイン名の例

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