MOVEitを悪用したCLOPの脅威ベクトルを DNSインテリジェンスで特定

目次

要旨

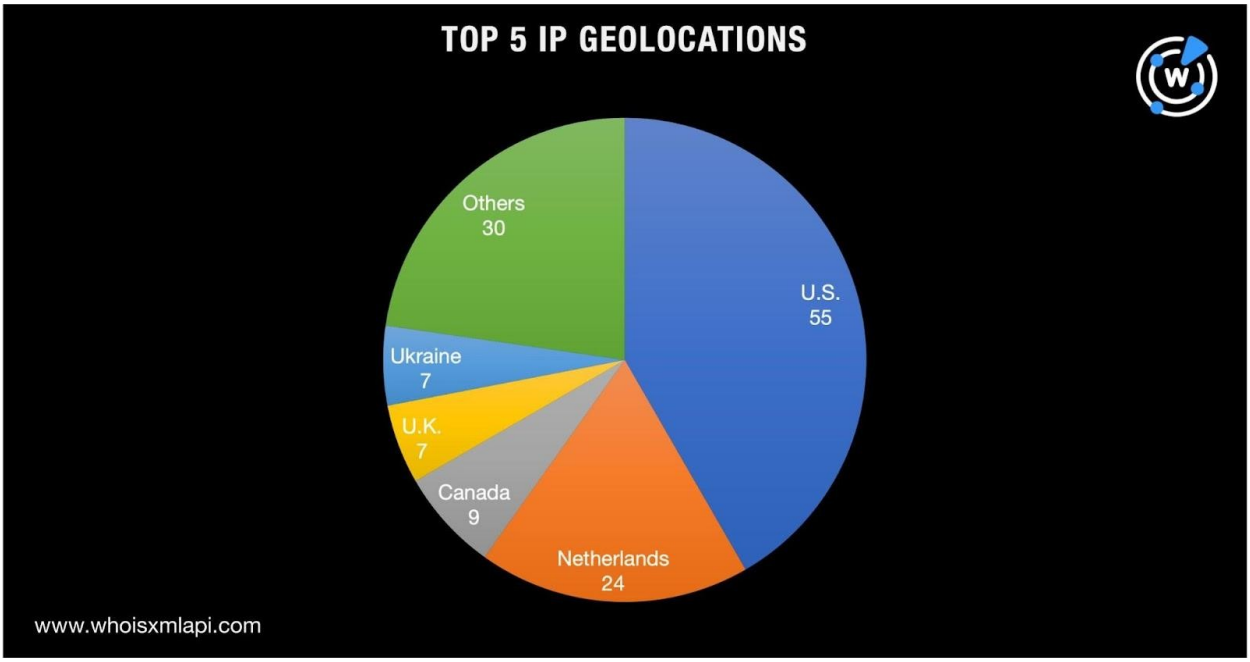
CleanINTERNETによると、2023年6月初旬に脆弱なMOVEitサーバーを標的とした複数のゼロデイ攻撃が発生し、機密データが流出しました。MOVEit Transfer は、ファイルやデータの交換をサポートするマネージドファイル転送ソフトウェアです。攻撃者はMOVEitの脆弱性を利用してデータベースにアクセスし、その構造や内容を推測することが可能になります。

その事件以降、MOVEit Transferの脆弱性を悪用したCLOPランサムウェア攻撃に関するレポートが、さまざまなセキュリティ企業の研究者により発表されています。そこで、WhoisXML APIでは、そうしたレポートからMOVEitを悪用したCLOPに関係する139のセキュリティ侵害インジケーター（IoC）のリストを入手し、DNSツールを使用してさらに分析を深めました。その結果、さらに以下が判明しました。

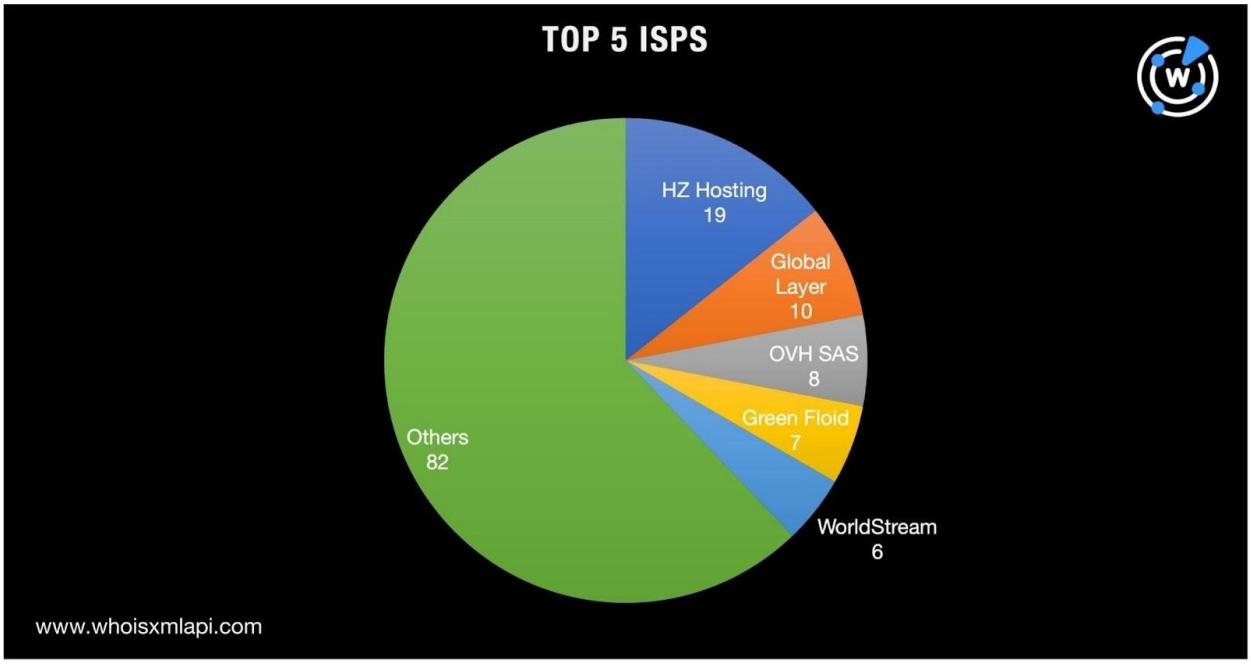
- IoCとして特定された専用IPアドレスに名前解決する34個のドメイン名。マルウェアチェックツールにより、そのうち 4個には悪意があることを確認
- IoCとして特定されたドメイン名の一部をホストしていた10個のユニークなIPアドレス。そのうち5個は専用であり、4個はマルウェアチェックツールによって悪意があるものと判明
- IoCとされた2つのドメイン名と同様に***zoom***という文字列を含んだ6,627個のドメイン名。そのうち56個はマルウェアチェックツールによってマルウェアホストと確認

IoCとして特定されたIPアドレスの詳細

MOVEitを使用したCLOPランサムウェア攻撃に関する詳細なレポートでは、132個のIPアドレスがIoCとして特定されました。それらをBulk IP Geolocation Lookupにかけたところ、米国（55個のIPアドレス）を筆頭に、オランダ（24個）、カナダ（9個）および英国とウクライナ（各7個）を含む16カ国に位置していることがわかりました。

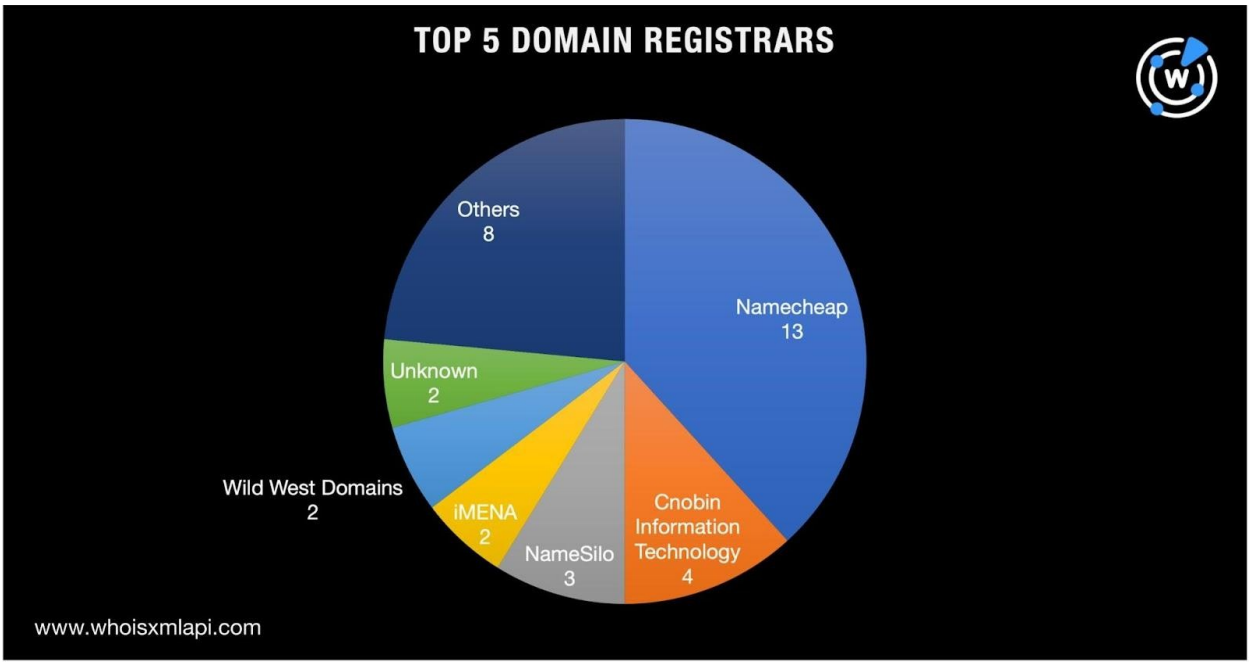


また、それらのIPアドレスIoCを管理していた50のISPが特定されました。上位5社は、HZ Hosting（19個のアドレス）、Global Layer（10個）、OVH SAS（8個）、Green Floid（7個）、WorldStream（6個）でした。



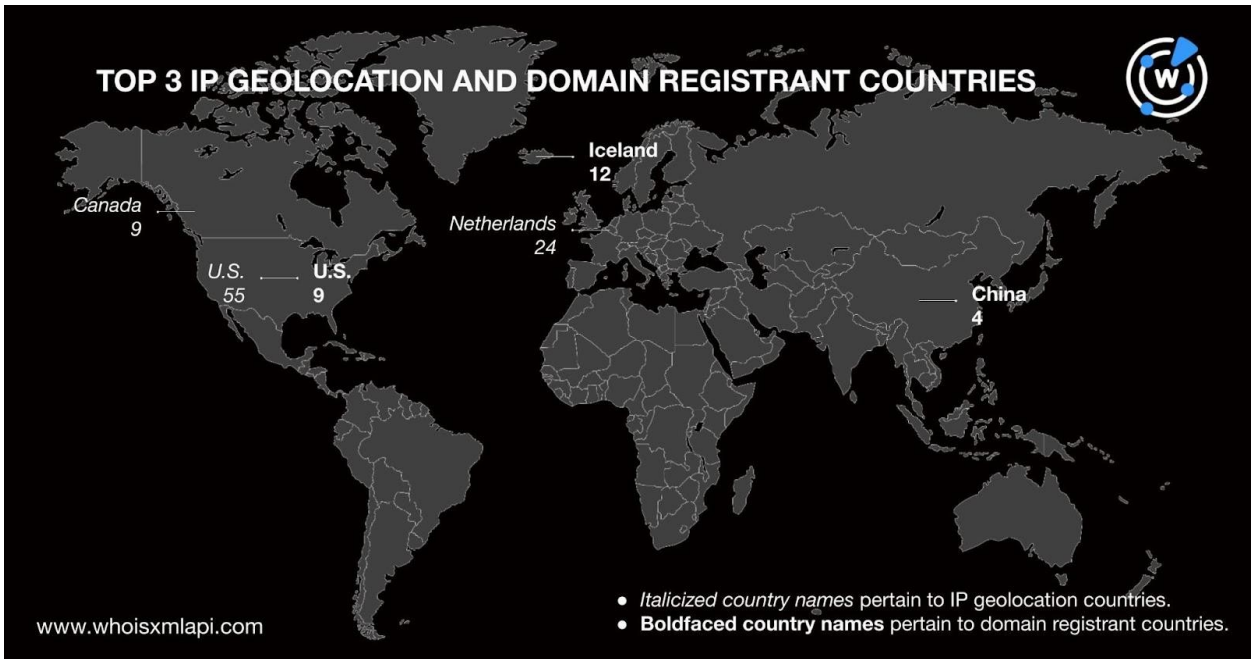
Reverse IP Lookupで検索したところ、132個のIPアドレスIoCうち17個が専用IPアドレスとわかりました。それらのIPアドレスは全部で34個のドメイン名をホストしており、うち4個のドメイン名は、マルウェアの一括チェックツールによって悪意があると判定されました。

次に、それらのドメイン名をBulk WHOIS Lookupで調べました。WHOISでレジストラの情報が公開されているドメイン名を見たところ、14社のレジストラが特定されました。管理ドメイン数が最も多かったのは13個を占めたNamecheapで、次いでCnobin Information Technology（4個）、NameSilo（3個）、iMENAとWild West Domains（各2個）がトップ5に入りました。



また、tube-plant[.]comというドメイン名については、登録者個人のメールアドレスがWHOISで一般に閲覧可能な状態になっていました。

そして、登録者の国が公開されているドメイン名を調べたところ、登録された国のトップはアイスランドで、同じIPアドレスを共用している12個のドメイン名が同国で登録されていました。なお、IPアドレスのジオロケーションを見たところ、アイスランドに位置するものはありませんでした。

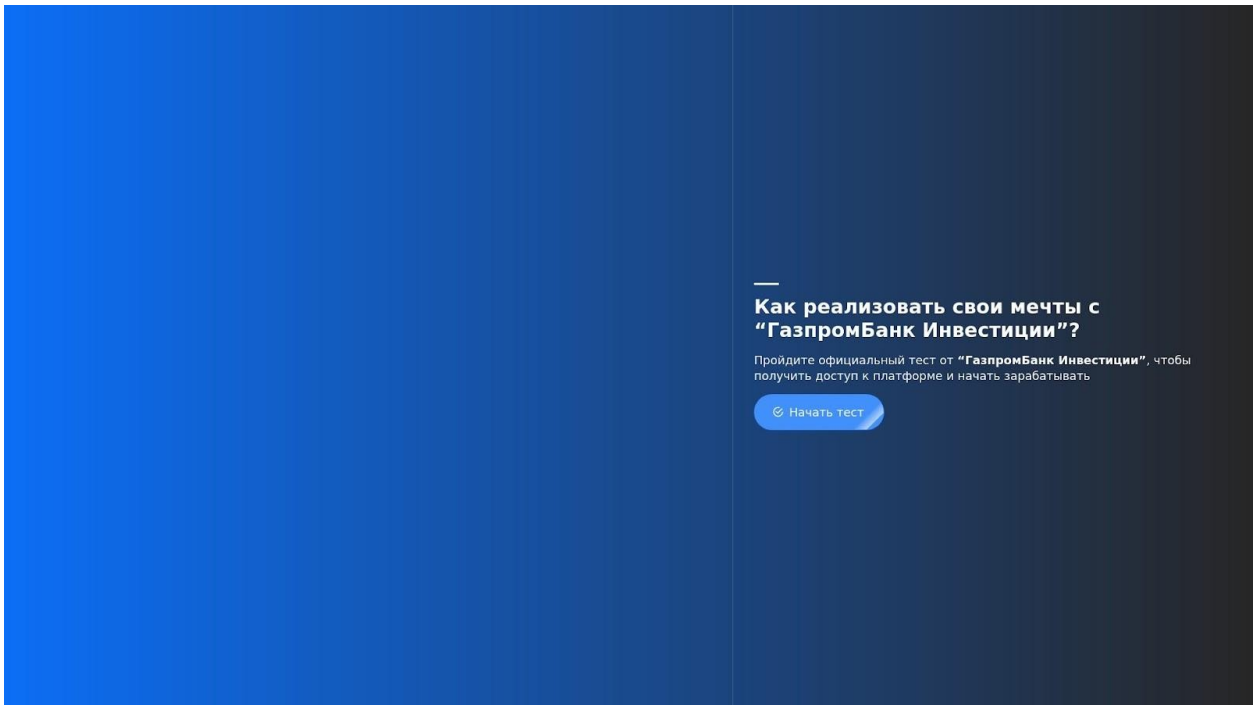


IoCとして特定されたドメイン名の詳細

MOVEitを悪用したCLOPランサムウェア攻撃に関するレポートでは、IoCとして7個のドメイン名も特定されていました。そのうちの2個は、***zoom***という文字列を含んでいます（connectzoomdownload[.]comとzoom[.]voyage）。しかし、この2つのドメイン名の現在のWHOISレコードには、zoom[.]comのWHOISレコードとの類似性が全くありませんでした。その2つは登録者の組織名が表示されず、レジストラはNameSiloでした。他方、zoom[.]comの登録組織名はZoom Video Communicationsと表示され、レジストラはMarkMonitor,Inc.を指していました。

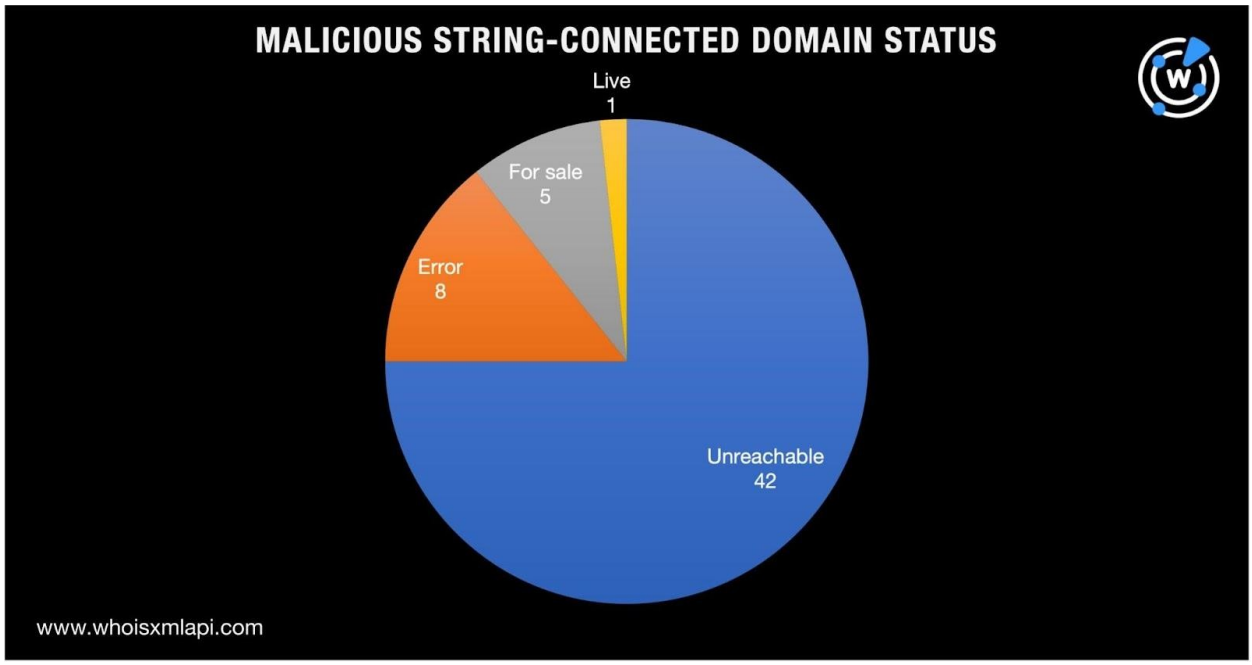
2つのドメイン名が2022年12月に新規登録されていたことから、当社ではさらに、***zoom***という文字列を含み、かつ2023年1月1日以降に新規登録された他のドメイン名を探しました。その結果、該当するドメイン名は6,627個見つかりました。WHOISレコードを取得できたそのうち6,609個について確認したところ、登録者の組織情報からZoom社に帰属していると確認できたものはありませんでした。

それらのドメイン名について一括マルウェアチェックを行った結果、56個はすでにマルウェアホストに分類されていたことがわかりました。そのうち1つだけがアクティブなコンテンツをホストし続けており、そのコンテンツはロシアの大手銀行とその投資プラットフォームに関連するものでした。なお、このドメイン名の文字列は「zoomplanet」ですが、コンテンツはZoomや地球とは何の関係もないようです。



*zoomplanet[.]online*のスクリーンショット

他の悪意あるドメイン名は、アクセス不能、販売中、またはエラーページに誘導されるものでした。



IoCとして特定されている7個のドメイン名をBulk WHOIS Lookupで一括検索すると、最も多い4つのドメイン名を管理しているレジストラはCnobin Information Technologyとわかりました。また、7個のうち6個は2022年に新規登録されたドメイン名で、残りの1個は1996年に作成されたかなり古いドメイン名でした。さらに、4個のドメイン名は中国、2個は米国、1個はカナダで登録されたものと判明しました。

これらのドメインIoCは10個のユニークなIPアドレスに解決しましたが、10個中4個は、公開されているIPアドレスIoCリストの一部でした。残りの6個のうち2個は、5個のドメイン名をホストする専用アドレスでした。マルウェアの一括チェックにより、その5個のドメイン名のうち4個には悪意があることが確認できました。いずれもアクティブなコンテンツはホストしていないものの、2個のドメイン名には***microsoft***という文字列が共通して含まれていました。

その2個（microsoftclouddownload[.]comおよびmlcrosoft[.]life）についてWHOIS Lookupを使って調べたところ、Microsoftへの帰属は確認できませんでした。Microsoft製品のユーザーを標的とした悪意あるキャンペーンで使われたのかもしれません。なお、microsoftclouddownload[.]com には、IoCとして特定されたconnectzoomdownload[.]com と同様に、***download***という文字列が含まれています。

—

MOVEitを悪用したCLOPランサムウェア攻撃の痕跡を求めてDNSを調査した結果、関与が疑われるドメイン名およびIPアドレスが合計6,600個あまり発見されました。

さらに深く掘り下げたところ、組織がブロックリストに含めることができる悪意あるアーティファクトが65個見つかりました。

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が特定したIoC

IPアドレス

- 84[.]234[.]96[.]104
- 209[.]222[.]103[.]170
- 198[.]27[.]75[.]110
- 96[.]44[.]181[.]131
- 96[.]10[.]22[.]178
- 92[.]118[.]36[.]249
- 92[.]118[.]36[.]213
- 92[.]118[.]36[.]210
- 91[.]223[.]227[.]140
- 91[.]222[.]174[.]68
- 88[.]214[.]27[.]101
- 88[.]214[.]27[.]100
- 82[.]117[.]252[.]97
- 82[.]117[.]252[.]142
- 82[.]117[.]252[.]141
- 81[.]56[.]49[.]148
- 79[.]141[.]173[.]94
- 79[.]141[.]161[.]82
- 76[.]117[.]196[.]3
- 74[.]218[.]67[.]242
- 68[.]156[.]159[.]10
- 54[.]39[.]133[.]41
- 54[.]184[.]187[.]134
- 50[.]7[.]118[.]90
- 5[.]34[.]178[.]31
- 5[.]34[.]178[.]30
- 5[.]34[.]178[.]28
- 5[.]34[.]178[.]27
- 5[.]188[.]206[.]76
- 5[.]149[.]252[.]51
- 5[.]149[.]250[.]90
- 45[.]182[.]189[.]229
- 45[.]182[.]189[.]228
- 45[.]182[.]189[.]200
- 44[.]206[.]3[.]111
- 3[.]101[.]53[.]11
- 23[.]237[.]56[.]234
- 23[.]237[.]114[.]154
- 216[.]144[.]248[.]20
- 213[.]121[.]182[.]84
- 209[.]222[.]98[.]25
- 208[.]115[.]199[.]25
- 20[.]47[.]120[.]195
- 198[.]245[.]13[.]4
- 198[.]199[.]74[.]207
- 198[.]137[.]247[.]10
- 195[.]38[.]8[.]241
- 185[.]81[.]113[.]156
- 185[.]80[.]52[.]230
- 185[.]33[.]87[.]126
- 185[.]33[.]86[.]225
- 185[.]174[.]100[.]17
- 185[.]117[.]88[.]2
- 185[.]104[.]194[.]134
- 173[.]254[.]236[.]131
- 172[.]71[.]134[.]76
- 166[.]70[.]47[.]90
- 162[.]158[.]129[.]79
- 15[.]235[.]83[.]73
- 15[.]235[.]13[.]184
- 148[.]113[.]159[.]213
- 148[.]113[.]159[.]146
- 143[.]31[.]133[.]99
- 142[.]44[.]212[.]178
- 141[.]101[.]68[.]166
- 141[.]101[.]68[.]154
- 107[.]181[.]161[.]207
- 104[.]200[.]72[.]149

- 100[.]21[.]161[.]34
- 93[.]190[.]142[.]131
- 91[.]229[.]76[.]187
- 91[.]222[.]174[.]95
- 91[.]202[.]4[.]76
- 89[.]39[.]105[.]108
- 89[.]39[.]104[.]118
- 84[.]234[.]96[.]31
- 79[.]141[.]160[.]83
- 79[.]141[.]160[.]78
- 66[.]85[.]26[.]248
- 66[.]85[.]26[.]234
- 66[.]85[.]26[.]215
- 63[.]143[.]42[.]242
- 62[.]182[.]85[.]234
- 62[.]182[.]82[.]19
- 62[.]112[.]11[.]57
- 5[.]34[.]180[.]48
- 5[.]34[.]180[.]205
- 5[.]252[.]25[.]88
- 5[.]252[.]23[.]116
- 5[.]188[.]87[.]27
- 5[.]188[.]87[.]226
- 5[.]188[.]87[.]194
- 5[.]188[.]86[.]250
- 5[.]188[.]86[.]114
- 5[.]149[.]250[.]92
- 5[.]149[.]250[.]74
- 5[.]149[.]248[.]68
- 45[.]56[.]165[.]248
- 45[.]227[.]253[.]82
- 45[.]227[.]253[.]6
- 45[.]227[.]253[.]50
- 45[.]227[.]253[.]147
- 45[.]227[.]253[.]133
- 209[.]97[.]137[.]33
- 209[.]127[.]4[.]22
- 209[.]127[.]116[.]122
- 206[.]221[.]182[.]106
- 198[.]12[.]76[.]214
- 194[.]33[.]40[.]104
- 194[.]33[.]40[.]103
- 193[.]169[.]245[.]79
- 188[.]241[.]58[.]244
- 185[.]185[.]50[.]172
- 185[.]183[.]32[.]122
- 185[.]181[.]229[.]73
- 185[.]181[.]229[.]240
- 185[.]174[.]100[.]250
- 185[.]174[.]100[.]215
- 185[.]162[.]128[.]75
- 185[.]117[.]88[.]17
- 185[.]104[.]194[.]40
- 185[.]104[.]194[.]24
- 185[.]104[.]194[.]156
- 179[.]60[.]150[.]143
- 162[.]244[.]35[.]6
- 162[.]244[.]34[.]26
- 148[.]113[.]152[.]144
- 146[.]0[.]77[.]183
- 146[.]0[.]77[.]155
- 146[.]0[.]77[.]141
- 138[.]197[.]152[.]201
- 104[.]194[.]222[.]107

ドメイン名

- zoom[.]voyage
- qweastradoc[.]com
- jirostrogud[.]com
- huntress[.]com
- hiperfdhaus[.]com
- guerdofest[.]com
- connectzoomdownload[.]com

IoCのIPアドレスを使っていたドメイン名の例

- 097[.]kh[.]ua
- 209-127-116-122[.]plesk[.]page
- 93-190-142-131[.]hosted-by-worldstream[.]net
- canismajor[.]site
- canisminor[.]life
- checkdrvms[.]com
- ciu1x8fy[.]ibxos[.]it
- cnetse[.]com
- cobaltrunner[.]net
- connectfillterdns[.]com
- crackpdud[.]pro
- ф2[.]myabandonware[.]com
- digiable[.]net
- fornax[.]life
- fuanshizmo[.]com
- ghustaderzk[.]com
- greenline[.]krd
- ideogencoo[.]vip

IoCのIPアドレスを使っていた悪意あるドメイン名の例

- cnetse[.]com
- digiable[.]net

IoCのドメイン名と同様に*zoom*という文字列を含むドメイン名の例

- zoomzoom[.]ga
- zoomzoom[.]cc
- zoomzoomz[.]ca
- zoomzoom[.]sbs
- zoomzoom[.]cyou
- zoomzoomllc[.]vg
- zoomzoom[.]co[.]de
- zoomtozoom[.]net
- zoomzoomies[.]de
- zoomzoom[.]click
- zoomzoom850[.]ru
- zoomzoomboom[.]ca
- zoomzoom[.]dating
- zoomzoombkk[.]com
- zoomzoomlab[.]com
- zoomzoommed[.]com
- zoomzoomads[.]com
- zoomifyzoom[.]com
- zoomzoomzurn[.]com
- zoomzoomwifi[.]com
- marrszoomzoom[.]com
- zoomzoomcars[.]shop
- zoombestzoom[.]shop
- airzoomzoom[.]click
- xn--oom-22a[.]de
- zoom[.]ac
- zoomzoomcaleb[.]com
- zoomzoomshoes[.]com
- zoomzoomdenton[.]com
- zoomzoomevents[.]com
- us04webzoomzoom[.]us
- nzoom[.]nl
- zooms[.]vg
- azoom[.]it
- zoomg[.]me
- zoomzoompets[.]com[.]br

- zoomm[.]ca
- xn--zm-8jaa[.]com
- zoomzoomcostume[.]com
- zoom5[.]us
- zoom1[.]vn
- zoomi[.]sk
- zoom[.]zip
- szoom[.]vg
- zooma[.]my
- zoomg[.]in
- ezoom[.]ga
- zoome[.]ga
- zoomg[.]de
- zoomc[.]ml
- szoom[.]ph
- zoomx[.]nl
- zooms[.]mx
- zoom3[.]cn
- zoomg[.]ga
- zoomc[.]ga
- zoomi[.]ch
- aculief-zoomzoom[.]com
- zoomer[.]ph
- zoom4d[.]in
- ipzoom[.]tv
- zoommc[.]ga
- kazoom[.]ch
- oazoom[.]uk
- zoomex[.]fr
- kkzoom[.]ru
- zoom47[.]tk
- zoomon[.]pl
- gazoom[.]me
- yjzoom[.]cn
- zoomag[.]kg
- zoomfr[.]vg
- izoom[.]fun
- zzoom[.]sbs
- ktzoom[.]xn--kprw13d
- zoomzl[.]cn
- zoomfs[.]vg
- vbzoom[.]vg
- edzoom[.]eu
- zoom47[.]ml
- zoome[.]mom
- zoomly[.]pl
- zoomit[.]ph
- zoomna[.]co
- zoom50[.]de
- zoom47[.]gq
- bizoom[.]ca
- mizoom[.]cn
- bgzoom[.]vg
- zooma5[.]ru
- bezoom[.]cn
- quzoom[.]de
- zoomat[.]us
- ezoom[.]app
- zoomzi[.]eu
- zoomik[.]ml
- zoomyx[.]co
- zoomat[.]eu
- x-zoom[.]us
- zoomie[.]ga

IoCのドメイン名と同様に*zoom*という文字列を含む悪意あるドメイン名の例

- zoomm[.]ca
- zoomad[.]us
- zoomupd[.]com
- myzoom[.]tech
- dzooms[.]site
- coudzoom[.]ru
- zoomify[.]pro
- zoomexhk[.]com

- zoom-docs[.]com
- legaczoom[.]com
- zoomchat[.]site
- quozoom[.]click
- zoomsender[.]in
- zoomexbit[.]com
- clientzoom[.]us
- zoomfile[.]tech
- zoom-conf[.]xyz
- zoom-meet[.]site
- zoomvideor[.]com
- zoomsetup[.]tech
- rulezoome[.]live
- zoompanel[.]site

IoCのドメイン名が名前解決したIPアドレスの例

- 193[.]42[.]33[.]206
- 92[.]118[.]36[.]213
- 88[.]214[.]27[.]101
- 216[.]239[.]34[.]21
- 216[.]239[.]32[.]21
- 216[.]239[.]36[.]21

IoCのドメイン名の専用IPアドレスでホストされていたドメイン名の例

- fastgotosasslst[.]online
- microsoftclouddownload[.]com
- mlcrosoft[.]life

IoCのドメイン名の専用IPアドレスでホストされていた悪意あるドメイン名の例

- microsoftclouddownload[.]com
- mlcrosoft[.]life