アプリインストーラーの悪用に繋がる不審なダウンロードページを特定

目次

要旨

Windows 10の「アプリインストーラー」という機能は、このところ脅威アクターによく悪用されています。ランサムウェアの配布に繋がる可能性のあるこの悪用は、Storm-0569、Storm-1113、Sangria Tempest、Storm-1674といった金銭的な動機を持つアクターによって実行されたものと思われます。こうしたアクターは、Zoom、Microsoft OneDrive、Microsoft SharePoint、Microsoft Teamsなどの一般的なソフトウェアのランディングページを模倣し、標的にした被害者に悪意のあるインストーラーをダウンロードさせるよう仕向けます。

Microsoftはこれを受け、ms-appinstallerプロトコルハンドラを直ちにデフォルトで無効にすることで対応しました。他方、WhoisXML APIの研究者はこのほど、DNSに残された悪用の痕跡を探しました。

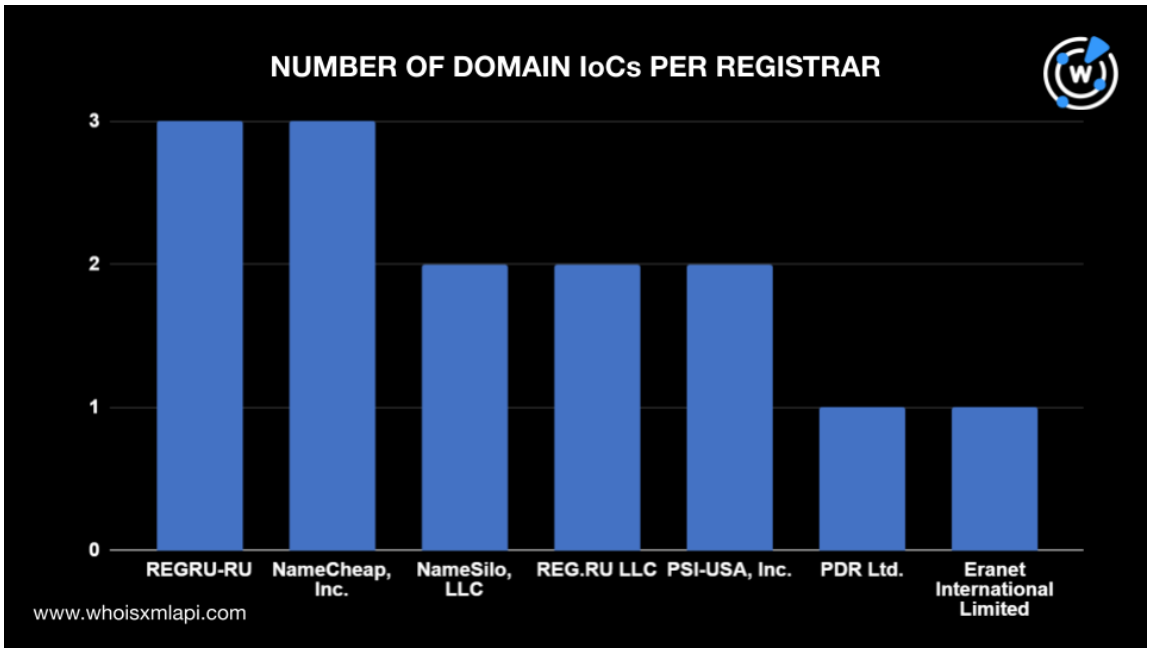
具体的には、Microsoftが公表した18個のサブドメインと14個のドメイン名（うち3個は18個のサブドメインから抽出したもの）からなるIoCリストをもとに、WhoisXML APIが誇るDNSインテリジェンスを駆使して関連アーティファクトを探しました。その結果、以下を検出するに至りました：

- ドメインIoCと同じメールアドレスを使って登録されたドメイン名4個
- IoCが名前解決したIPアドレス16個
- IoCが名前解決したIPアドレスによってホストされていたドメイン名127個
- ドメインIoCと同じ文字列を含むドメイン名401個
- サブドメインIoCと同じ文字列を含むサブドメイン596個

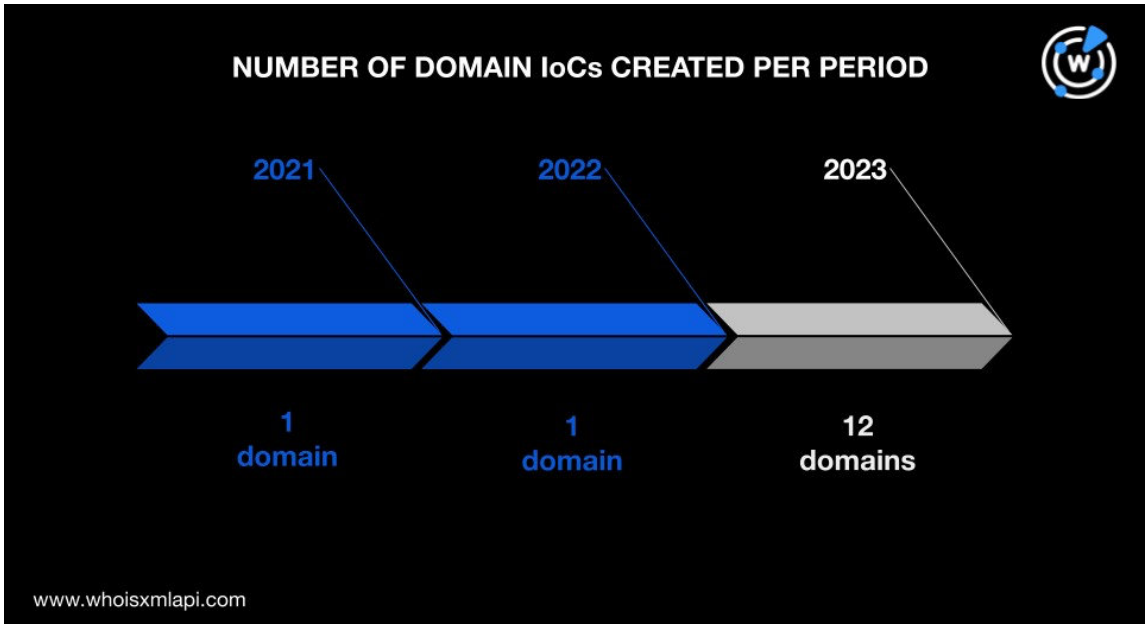
アプリインストーラー悪用のIoCを分析

まず、IoCとしてタグ付けされた前述の14個のドメイン名（以下「ドメインIoC」）をBulk WHOIS Lookupにかけました。その結果、WHOISレコードから以下の事実が判明しました：

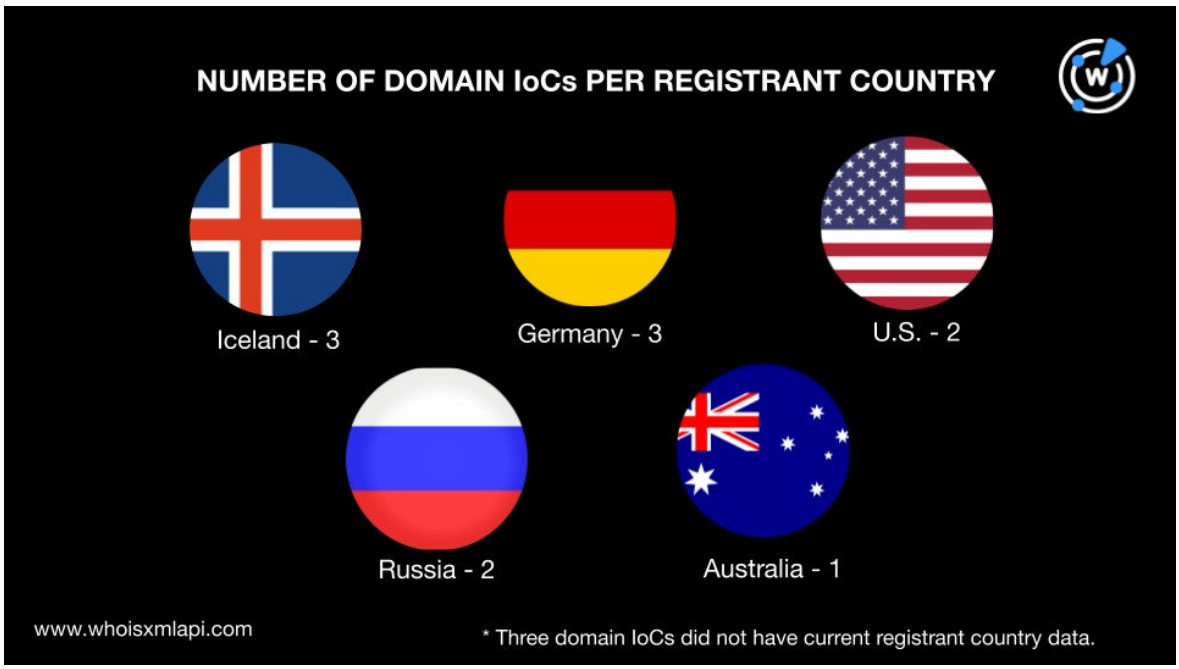
- 14個は7社の管理レジストラに分散していました。REGRU-RUとNameCheap, Inc.がそれぞれ3個、NameSilo LLC、REG.RU LLCおよびPSI-USA, Inc.がそれぞれ2個、PDR Ltd.とEranet International Limitedがそれぞれ1個のドメインIoCを管理していました。



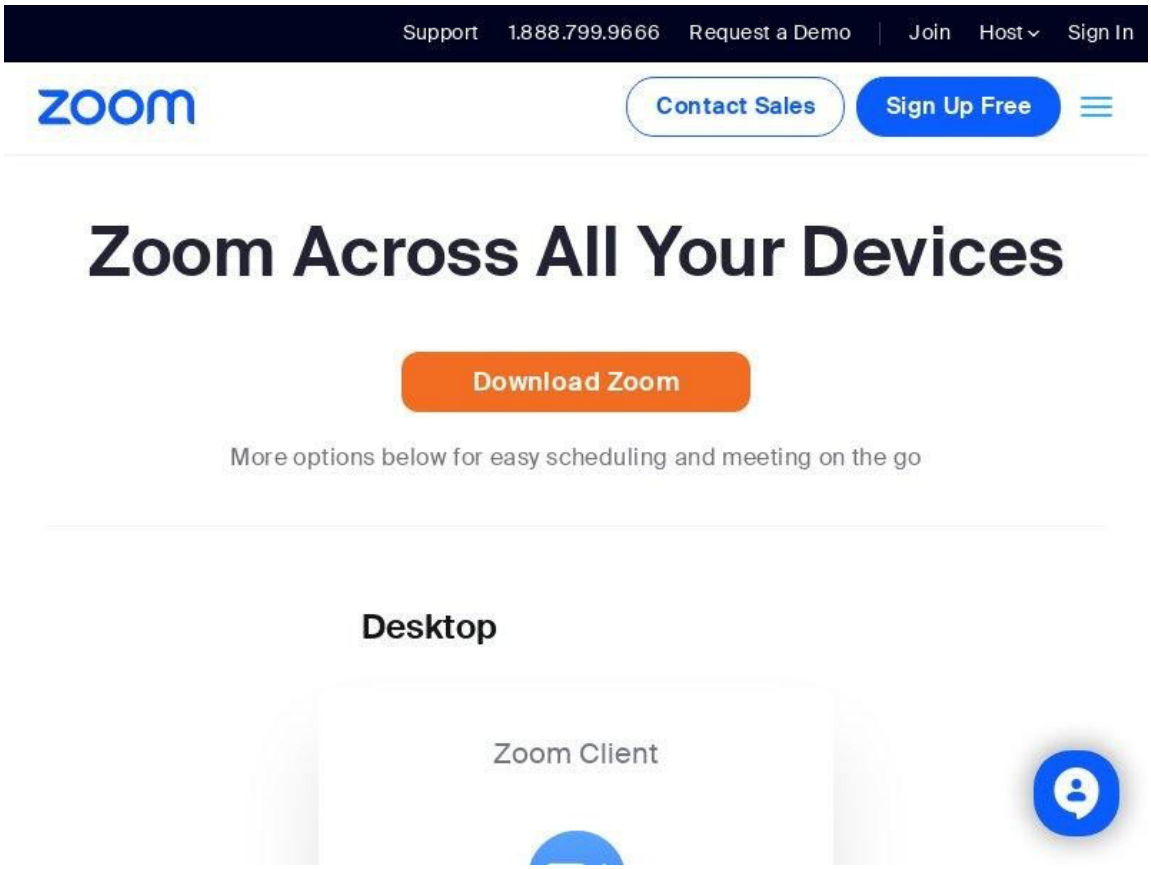
- 12個は2023年に新規登録されたドメイン名でした。また、2021年と2022年に新規登録されたものが1個ずつありました。



- ドメインIoCの登録地は5カ国に分散していました。アイスランドとドイツでそれぞれ3個、米国とロシアでそれぞれ2個、オーストラリアで1個が登録されていました。また、3個のドメインIoCについては、現在のレジストラの情報がWHOISにありませんでした。



次に、14個のドメインIoCのスクリーンショット分析を行ったところ、ZoomとMicrosoftのランディングページを表示する以下のウェブサイトを含め、有効なコンテンツをホストし続けているものがあることがわかりました。



Screenshot of the page hosted on domain IoC info-zoomapp[.]com

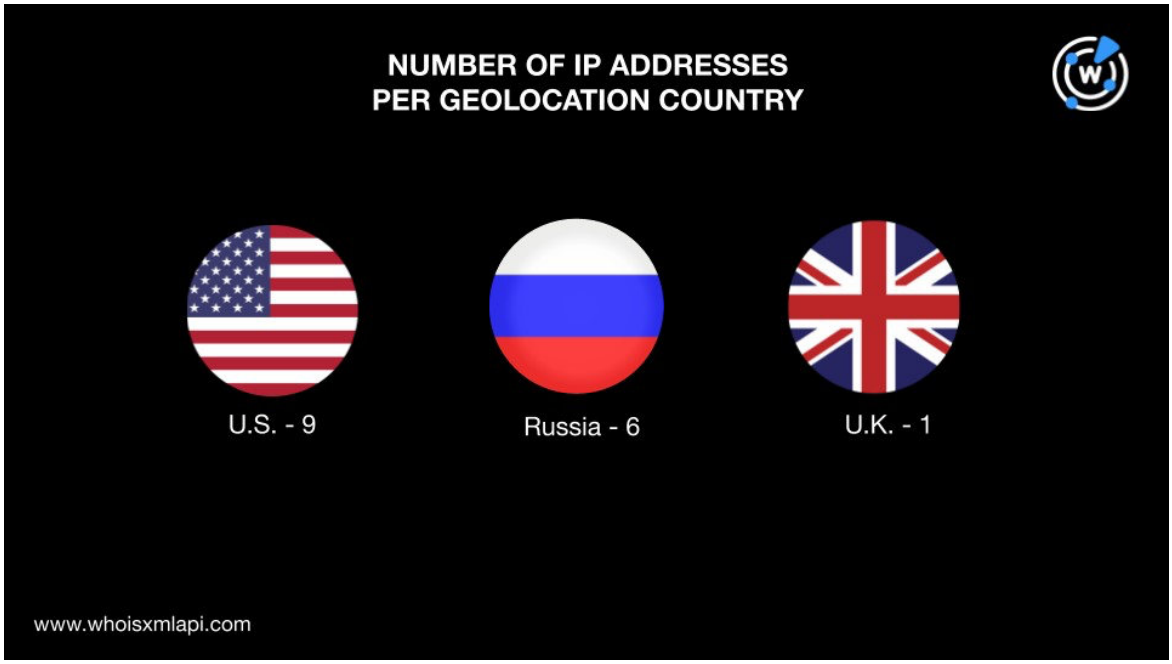
IoCと関連しているアーティファクトをDNSで探索

次のステップとして、アプリインストーラーの悪用で使われた既存IoC以外のドメイン名とサブドメインをDNSで探しました。

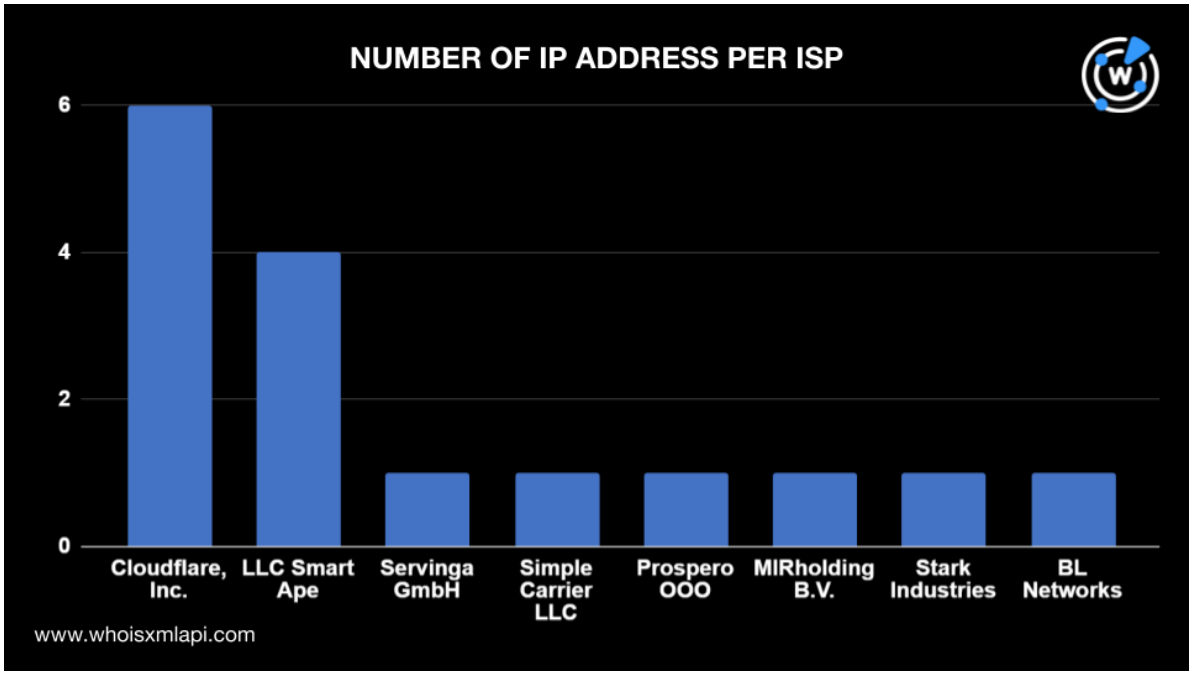
ドメインIoCをWHOIS History APIで問い合わせたところ、過去のWHOISレコードから12個のメールアドレスが検出されました。そして、そのうち5個は未編集のまま公開されていました。その5個の公開メールアドレスを使ってReverse WHOIS APIで逆引きした結果、それらが8,434個にのぼるドメイン名の現在のWHOISレコードに記載されていることが判明しました。ただし、1個は8,429ドメインの登録に使われていたことから、ドメイナーが大量登録に使ったメールアドレスと思われます。そのドメイナーが登録したらしいドメイン名と既存のIoCを除くと、ドメインIoCと同じメールアドレスを使って登録されたドメイン名は4個になりました。

次に、ドメインIoC 14個とIoCとして特定されたサブドメイン（以下「サブドメインIoC」）18個をDNS Lookupにかけたところ、合計16個の未報告のIPアドレスに名前解決しました。それらのIPアドレスの地理的位置をIP Geolocation Lookupで調べた結果、以下のことが判明しました：

- 9個は米国、6個はロシア、1個は英国を指していました。



- 8社の管理ISPが特定されました。Cloudflare, Inc.が6個、LLC Smart Apeが4個、Serving GmbH、Simple Carrier LLC、Prospero OOO、MIRholding B.V.、Stark Industries、BL Networksがそれぞれ1個を管理していました。



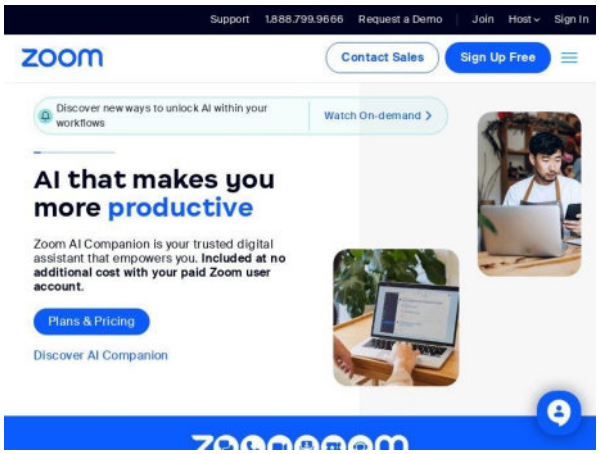
- Threat Intelligence APIを実行した結果、16個のうち9個は脅威と関連していることがわかりました。いくつかの例を以下に示します。

IPアドレス	関連する脅威の種類
185[.]196[.]8[.]246	Attack Command-and-control (C2) Malware
91[.]215[.]85[.]199	Attack Malware Spam
172[.]67[.]147[.]29	Generic Phishing
172[.]67[.]209[.]46	Generic Malware Phishing

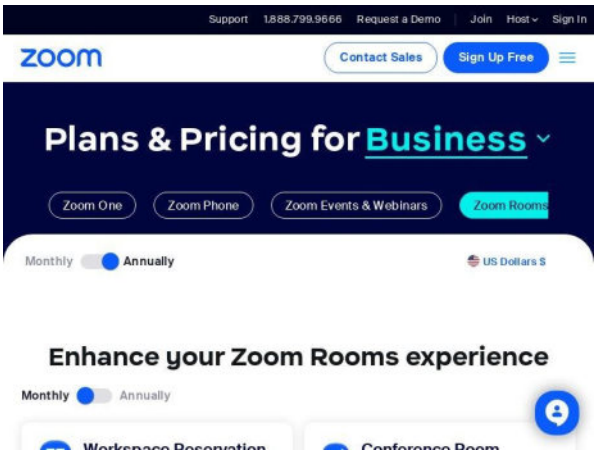
また、16個のIPアドレスを使ってReverse IP Lookupで検索したところ、9個は専用アドレスのようでした。そして、その9個のIPアドレスによってホストされているドメイン名が127個見つかりました（重複、既存IoC、ドメインIoCと同じメールアドレスを使って登録されたドメイン名を除く）。

さらに、上述の9個のIPアドレスがホストしているドメイン名についてスクリーンショット分析を行いました。その結果、本稿執筆時点で、アプリインストーラーの悪用に関与した悪意あるリソースと同じようにインストールページをホストしているドメイン名が多数あることが判明しました。

専用らしいIPアドレスがホストしているドメイン名「bitvarden-info[.]com」のスクリーンショット



専用らしいIPアドレスがホストしているドメイン名「biryaneehouse[.]com」のスクリーンショット



専用らしいIPアドレスがホストしているドメイン名「cotattoo[.]com」の　スクリーンショット

専用らしいIPアドレスがホストしているドメイン名「rextowingcarolinas[.]com」のスクリーンショット

最後に、Domains & Subdomains Discoveryを使ってIoCと同じテキスト文字列を含むドメイン名を探しました。以下の検索パラメータを指定してドメイン名を検索したところ、401個が該当しました。

- Starts with **scheta.**
- Starts with **tnetworks**
- Starts with **1204** and ends with **.ru**
- Starts with **gertefin**
- Starts with **septcn**
- Contains **-zoomapp**

- Starts with **storageplace**
- Starts with **sun1.**
- Starts with **tech-department**
- Starts with **kellyservices-**
- Starts with **ithr.**
- Starts with **meetlng**
- Starts with **webmicrosoft** and contains **system.**

他方、以下のパラメータを指定してサブドメインを検索した結果、596個のサブドメインが検出されました：

- Starts with **nixonpeabody**
- Starts with **amgreetings**
- Starts with **cbre.**
- Starts with **hubergroup**
- Starts with **formeld**
- Starts with **kelly** and contains **services** and **hr**
- Starts with **mckinsey** and contains **hr**
- Contains **support-my.**
- Starts with **zoonn**
- Starts with **amydeks**
- Starts with **abobe.**
- Starts with **amydesk**

401個のドメイン名と596個のサブドメインのスクリーンショットを分析したところ、不審なコンテンツをホストしているものが複数見つかりました。そうしたコンテンツの中には、本稿執筆時点でフィッシングのページと分類されているものもあります。

IoCと同じ文字列を含むサブドメイン「zoonn[.]meetlng[.]cn[.]com」のスクリーンショット

—

今回は、アプリインストーラー悪用のIoC（18個のサブドメインと14個のドメイン名。そのうち4個のドメイン名はサブドメインから抽出）を足がかりに調査を行いました。その結果、1,100を超える関連アーティファクト（ドメインIoCと同じメールアドレスを使って登録されたドメイン名4個、IoCが名前解決したIPアドレス16個、IoCが名前解決したIPアドレスによってホストされていたドメイン名127個、ドメインIoCと同じ文字列を含むドメイン名401個、サブドメインIoCと同じ文字列を含むサブドメイン596個）を特定することができました。

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：アーティファクトの例

ドメインIoCと同じメールアドレスを使って登録されていたドメイン名の例

- vmlian[.]top
- foodlian[.]top

IoCが名前解決したIPアドレスの例

- 188[.]127[.]224[.]193
- 188[.]127[.]254[.]229
- 188[.]127[.]235[.]18
- 91[.]219[.]150[.]24
- 80[.]77[.]23[.]210
- 185[.]196[.]8[.]246
- 91[.]215[.]85[.]199
- 193[.]233[.]22[.]126

IoCが名前解決したIPアドレスによってホストされていたドメイン名の例

- 500token[.]ru
- 001531[.]com
- 009987[.]com
- edd2ed2[.]online
- tservicessss[.]store
- accesutqymyiq[.]com
- meetlng[.]group
- admiai[.]com
- amjsecurityservices[.]com
- austinsmilecenter[.]com
- australiatvic[.]com
- autodesk-promo[.]com
- belaladel[.]com
- bestrealtorsindallas[.]com
- biblealways[.]com
- bibleandsouls[.]com
- bibleasoul[.]com
- biltwerdem-info[.]com
- birgletrossgolf[.]com
- biryaneehouse[.]com
- bitvarden-info[.]com
- bottletorque[.]com
- bouncebackbabyfat[.]com
- bouncebeast[.]com
- bugglesworth[.]com
- bundles2go[.]com
- buscorestaurante[.]com
- cannothide[.]com
- carepettips[.]com
- carnitasdelivery[.]com
- cartknoxxs[.]com
- challengermenu[.]com
- chicaespectaculos[.]com
- cotattoo[.]com
- creativedesignint[.]com
- cryptofindy[.]com
- crystalgemsfruit[.]com
- csritindia[.]com
- cualoland[.]com
- easyquickdinners[.]com
- enhanceexercise[.]com
- filmandfilmmaking[.]com
- fromge[.]com
- garypearlphotography[.]com
- gdaygym[.]com
- gdaygyms[.]com
- gdayreviews[.]com
- getmailgetpaid[.]com
- globalqualityparts[.]com
- globalwholesaleremanufacturing[.]com

ドメインIoCと同じ文字列を含むドメイン名の例

- scheta[.]info
- scheta[.]net
- scheta[.]moscow
- scheta[.]ru
- scheta[.]online
- scheta[.]com
- tnetworkperu[.]com
- tnetwork[.]cn
- tnetworkusa[.]com
- tnetworkmarketing[.]com
- tnetworks[.]com[.]au
- tnetworks[.]com[.]tr
- tnetwork[.]jp
- tnetwork[.]com[.]au
- tnetwork[.]cz
- tnetworkers[.]com
- tnetworkinc[.]com
- tnetworkservices[.]com
- tnetworksindo[.]com
- tnetwork[.]io[.]vn
- tnetwork[.]se
- tnetworkelsalvaldor[.]vg
- tnetworkdc[.]ws
- tnetworkworld[.]com
- tnetworkgroup[.]com
- tnetworks[.]df[.]gov[.]br
- tnetworksinc[.]com
- tnetwork[.]nl
- tnetworkinginc[.]ca
- tnetwork[.]co[.]kr
- tnetworkbd[.]net
- tnetwork[.]it
- tnetwork[.]co[.]jp
- tnetwork[.]de
- tnetwork[.]in
- tnetworks[.]xyz
- tnetwork[.]ca
- tnetworks[.]eu
- tnetworkyfl[.]top
- tnetworks[.]net
- tnetworkuk[.]info
- tnetworkasia[.]com
- tnetworkcn[.]com
- tnetwork[.]xyz
- tnetwork[.]com
- tnetworkmc[.]com
- tnetworksoftware[.]com
- tnetwork-system[.]online
- tnetworka[.]com
- tnetwork[.]dk

サブドメインIoCと同じ文字列を含むサブドメインの例

- nixonpeabody[.]careers[.]micronapps[.]com
- nixonpeabody-website[.]cmservicesltd[.]com
- nixonpeabody[.]vps[.]powersharkmbr[.]com
- nixonpeabody[.]introhive[.]com
- nixonpeabody[.]vmlstage[.]com
- nixonpeabody[.]zoom[.]us
- nixonpeabody[.]com[.]outerstats[.]com
- nixonpeabody[.]app[.]kirasystems[.]com
- nixonpeabody2[.]adobeconnect[.]com
- nixonpeabody[.]highq[.]com[.]origin[.]highq[.]com
- nixonpeabody[.]com[.]clearwebstats[.]com

- nixonpeabody[.]highq[.]com[.]cn[.]highq[.]com
- nixonpeabody[.]pixeldance[.]com
- nixonpeabody[.]searchfirm[.]micronapps[.]com
- nixonpeabody[.]highq[.]com
- nixonpeabody-sc102xm0-centralus-si[.]azurewebsites[.]net
- amgreetings[.]printercloud[.]com
- amgreetingscareers-com02i[.]mail[.]protection[.]outlook[.]com
- amgreetings[.]benefithub[.]com
- amgreetings[.]ui[.]quickbase[.]com
- amgreetings[.]walkertracker[.]com
- amgreetings[.]int[.]hubwoo[.]com
- amgreetingscareers-com[.]mail[.]protection[.]outlook[.]com
- amgreetings[.]mywbenefits[.]com
- amgreetings[.]dev[.]worksmartsuite[.]com
- amgreetings[.]jamfcloud[.]com
- amgreetingscareers-com02i[.]mail[.]protection[.]skribble[.]pro
- amgreetings-iphone-wifi[.]h6[.]xiaoeknow[.]com
- cbre[.]com[.]ve[.]us[.]cas[.]ms
- cbre[.]apps[.]dev[.]cf[.]thalesdigital[.]io
- cbre[.]ent[.]allianzim[.]com
- cbre[.]ent[.]syncsketch[.]dev
- cbre[.]campus[.]modelical[.]com
- cbre[.]account[.]recruitership[.]com
- cbre[.]referrals[.]connxusdemo[.]com
- cbre[.]referrals[.]fortnite[.]com
- cbre[.]referrals[.]yelp[.]com
- cbre[.]locator[.]zalora[.]com[.]ph
- cbre[.]myhse[.]wormhole[.]com
- cbre[.]ent[.]frontapp[.]com
- cbre[.]denver[.]brokers[.]business[.]ivirus[.]ru
- cbre[.]co[.]uk[.]mcas[.]ms
- cbre[.]ent[.]vk[.]cc
- cbre[.]at[.]ip4[.]bz
- cbre[.]genmills[.]liebi[.]com
- cbre[.]demo[.]tokopedia[.]com
- cbre[.]sandbox[.]joinmesa[.]com
- cbre[.]com[.]br[.]apescout[.]com
- cbre[.]referrals[.]miro[.]com
- cbre[.]myhse[.]speakap[.]com
- cbre[.]co[.]uk[.]eu2[.]cas[.]ms
- cbre[.]referrals[.]binance[.]com
- cbre[.]stage[.]movecloser[.]pl
- cbre[.]com[.]us[.]cas[.]ms
- cbre[.]ent[.]pulleyapp[.]com
- cbre[.]enterpriseqa[.]shakedeal[.]com
- cbre[.]pl[.]ipaddress[.]com
- cbre[.]co[.]uk[.]eu[.]cas[.]ms
- cbre[.]crmaxe[.]microsites02[.]redbull[.]com
- cbre[.]myhse[.]giftya[.]com
- cbre[.]qa7[.]monigle3[.]net
- cbre[.]referrals[.]spotifyforbrands[.]com
- cbre[.]bree[.]warnerbros[.]com
- cbre[.]ent[.]westhotel[.]web-6[.]hiltonbusinessonline[.]com
- cbre[.]referrals[.]selectminds[.]com
- cbre[.]ent[.]ya[.]ru
- cbre[.]pt[.]cutercounter[.]com
- cbre[.]com[.]tested[.]website
- cbre[.]ch[.]locatee[.]com
- cbre[.]dev[.]kodeks[.]no
- cbre[.]testing[.]myvolusion[.]com
- cbre[.]referrals[.]molinostuckyhilton[.]web-11[.]hiltonbusinessonline[.]com
- cbre[.]testing[.]canva-apps[.]com
- cbre[.]co[.]uk[.]admin-us[.]cas[.]ms
- cbre[.]fi[.]w3cdomain[.]com
- cbre[.]qa2[.]monigle3[.]net

- cbre[.]ent[.]williamhill[.]com
- cbre[.]com[.]tr[.]wenotify[.]net
- cbre[.]referrals[.]ardoq[.]com
- cbre[.]uk[.]yeahtic[.]com
- cbre[.]referrals[.]paydiant[.]com
- cbre[.]vo[.]llnwd[.]net
- cbre[.]ent[.]lucidstaging[.]app
- cbre[.]ent[.]fetlife[.]com
- cbre[.]referrals[.]robinhood[.]com
- cbre[.]genmills[.]litix[.]io
- cbre[.]magiceden[.]workers[.]dev
- cbre[.]referrals[.]williamhill[.]com
- cbre[.]com[.]ve[.]admin-us[.]cas[.]ms
- cbre[.]corprealestate[.]truist-api[.]com
- cbre[.]myhse[.]acc[.]mobilevikings[.]be
- cbre[.]ent[.]invisionapp[.]com
- cbre[.]a1[.]mailplus[.]nl
- cbre[.]saml[.]morganstanley[.]com
- cbre[.]ru[.]whoisbucket[.]com
- cbre[.]genmills[.]facilitiesdesk[.]com
- cbre[.]mirror[.]omnee[.]io
- cbre[.]ent[.]betsson[.]com
- cbre[.]ent[.]airbnbchicago[.]com