不正広告「UNC2975」のインフラを調査

目次

1. 要旨
2. 付録：アーティファクトとIoCの例

要旨

MandiantのManaged Defense Threat Hunting Teamは最近、「UNC2975マルバタイジングキャンペーン」と呼ばれるマルウェアの詳細な調査結果を発表しました。毒入りのスポンサー付き検索エンジンの検索結果やソーシャルメディアの投稿をクリックさせられたユーザーのコンピュータは、DANABOTまたはDARKGATEのバックドアに感染してしまいます。

Mandiantは、この脅威を詳細に分析した結果として、合計28個のセキュリティ侵害インジケーター（IoC）を特定しました。このIoCリストは、19個のドメイン名（以下「ドメインIoC」）と9個のIPアドレス（以下「IPアドレスIoC」）で構成されています。WhoisXML APIの研究チームはこれを受け、まだ特定されていない関連アーティファクトを洗い出すために、そのIoCリストの拡張を試みました。その結果、以下が検出されました：

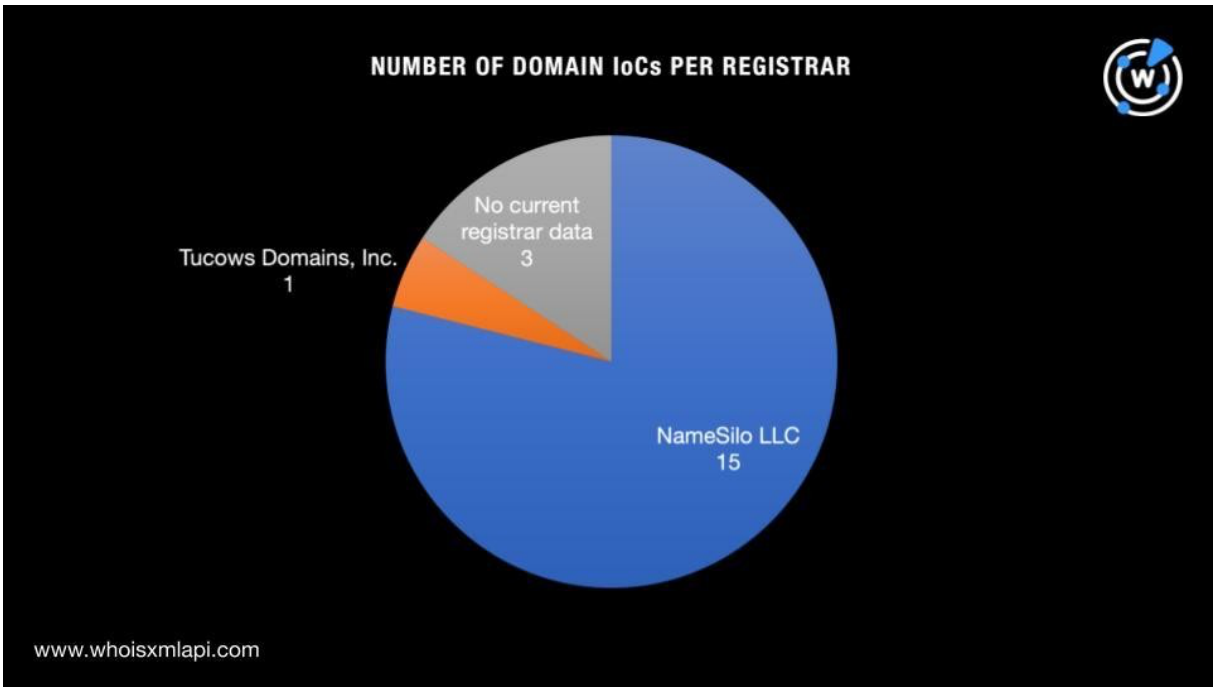
- ドメインIoCと同じメールアドレスを使用していた239個のドメイン名
- ドメインIoCが名前解決した13個のIPアドレス
- ドメインIoCの専用ホストを共用していた、またはIPアドレスIoCに名前解決した3個のドメイン名
- ドメインIoCと同じ文字列を含む2,772個のドメイン名

UNC2975のIoCにクローズアップ

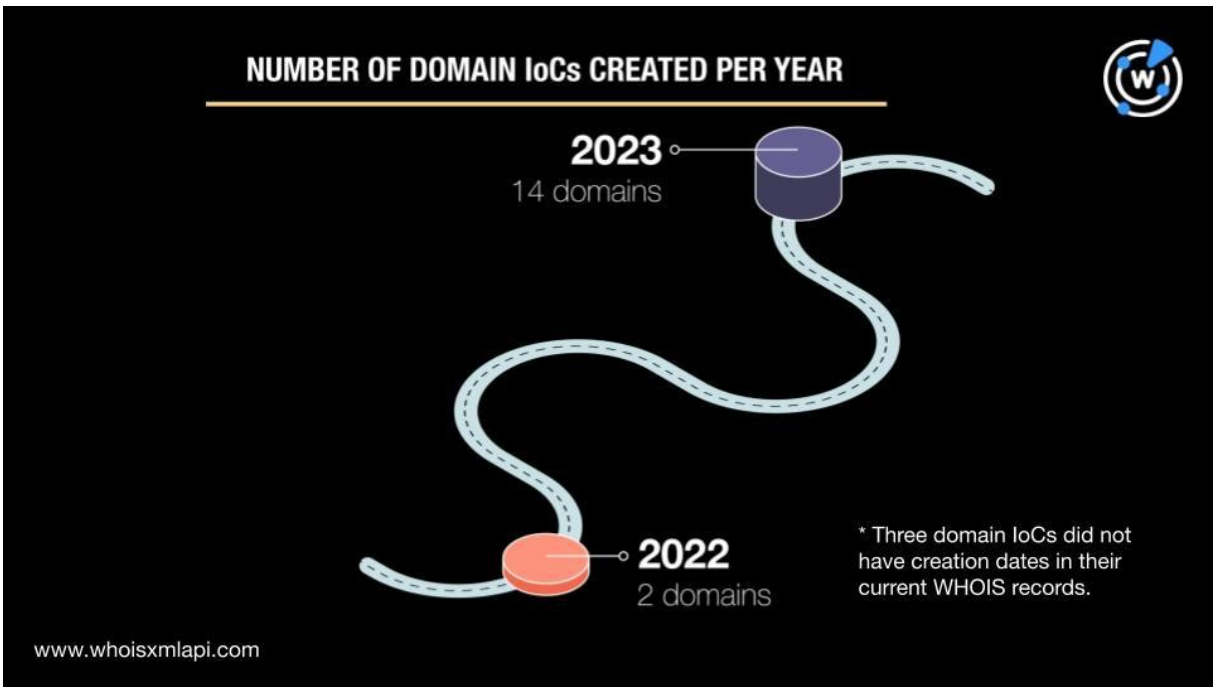
最初のステップとして、まずMandiantが特定したドメインIoCとIPアドレスIoCの詳細情報を探しました。

19個のドメインIoCについてBulk WHOIS Lookup を実行したところ、以下が判明しました：

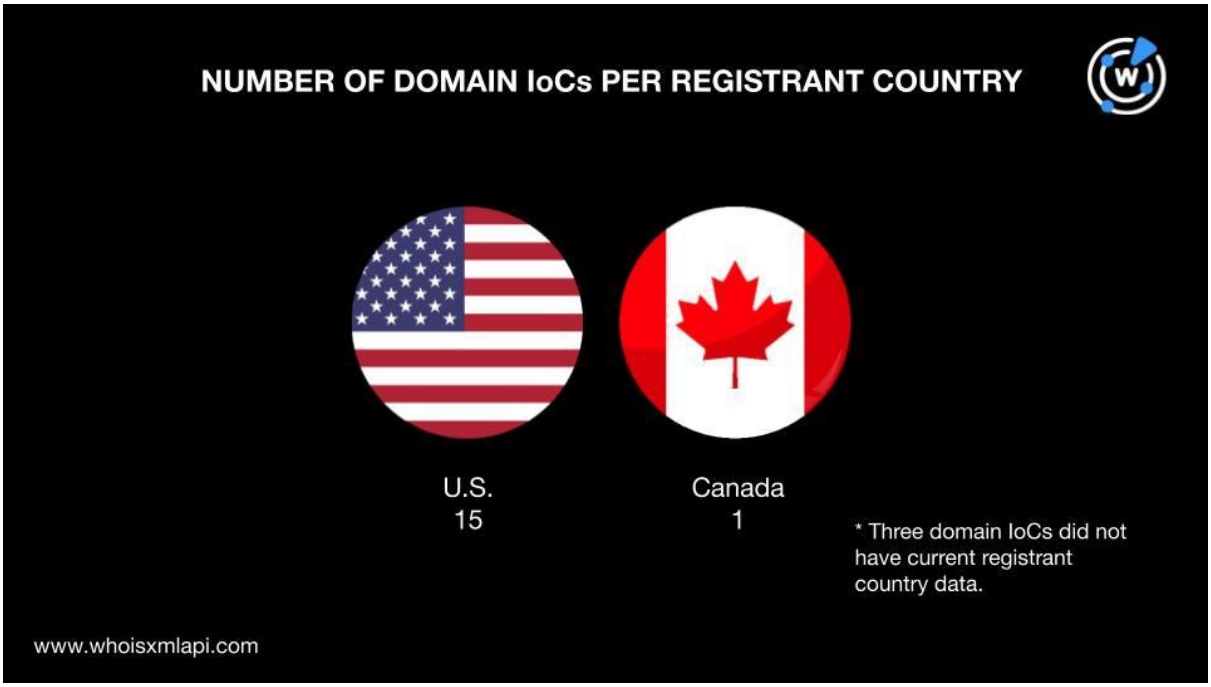
- 2社の管理レジストラが特定されました。15個のドメイン名はNameSilo LLCが、1個はTucows Domains, Incが管理していました。残りの3ドメインについては、現在のWHOISデータがありませんでした。



- 14個は2023年、2個は2022年に新規登録されたドメイン名でした。残りの3個のドメイン名については、現在のWHOISレコードから登録日を確認できませんでした。

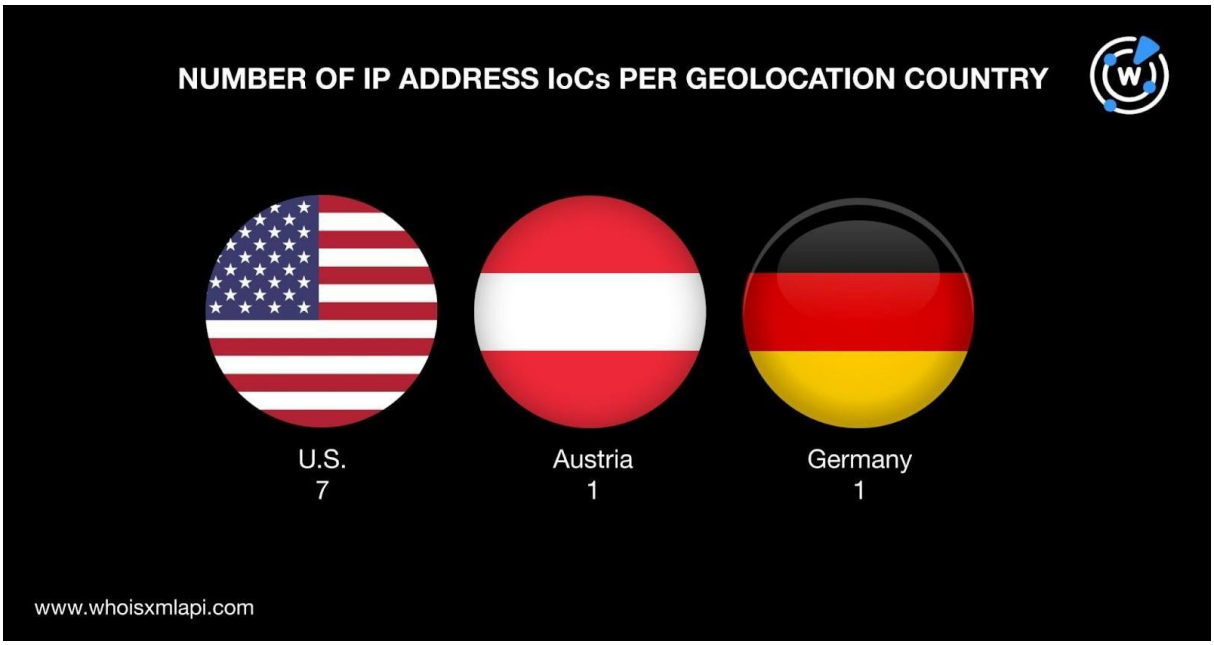


- 15個は米国、1個はカナダで登録されたと思われます。残り3個のドメイン名については、現在の登録者の国のデータがありませんでした。

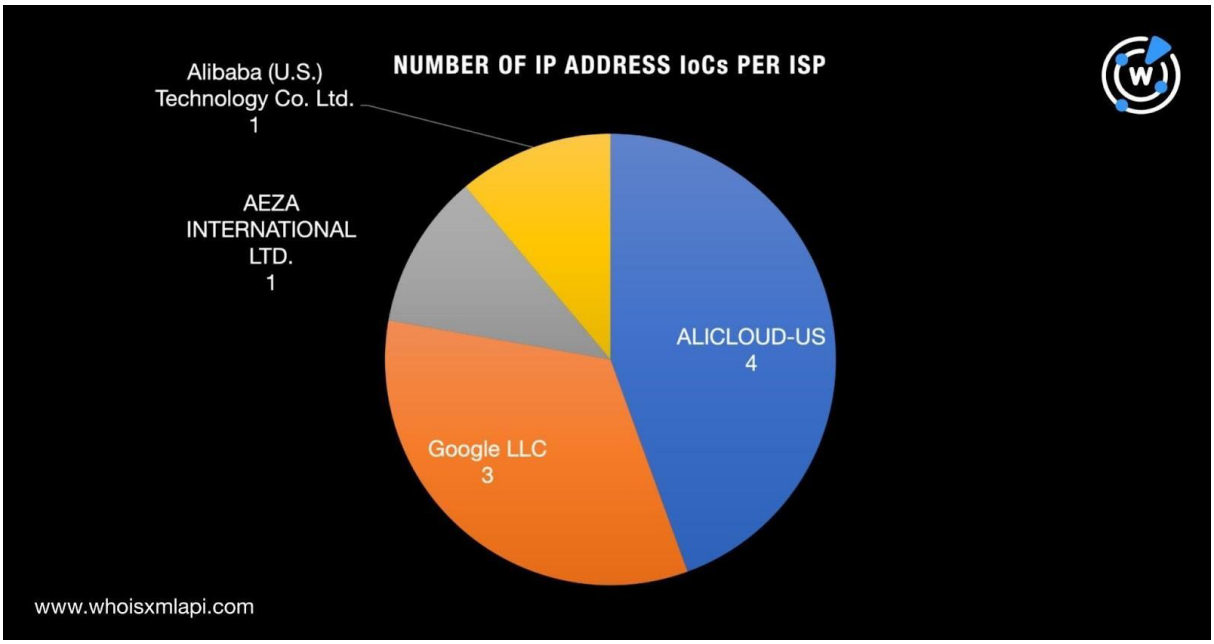


次に、9個のIPアドレスIoCをBulk IP Geolocation Lookupにかけたところ、以下のことがわかりました：

- 7個は米国に位置していました。そして、オーストリアとドイツを指すIPアドレスが1個ずつありました。



- ALICLOUD-USが4個のIPアドレスの管理ISPでした。この他、Google LLCが3個、AEZA INTERNATIONAL LTD.とAlibaba (U.S.) Technology Co. Ltd.がそれぞれ1個のIPアドレスを管理していました。



UNC2975のDNS上のつながり

UNC2975と関連している可能性のあるアーティファクトを可能な限り洗い出すため、まず19個のドメインIoCのWHOISレコードを調べました。

WHOIS History API検索の結果、19個のうち7個のWHOISレコードに合計15個のメールアドレスが表示されました。そのうち13個はパブリックなメールアドレスでした。

次に、その13個のメールアドレスに対してReverse WHOIS APIを実行したところ、重複とIoCを除外した後の状態で、5個のメールアドレスが別のドメイン名239個の現在のWHOISレコードに表示されました。

その239個のドメイン名をScreenshot APIで検索した結果、本稿執筆時点でアクティブなコンテンツをホストし続けているドメイン名が1個だけ特定されました（以下）。

Добро пожаловать на “Наше Радио”!

“Наше Радио” призывает всех к добру, позитиву и стремлению к миру. Наша миссия заключается в объединении всех, особенно представителей славянских народов. Мы отдаём дань уважения разнообразным культурным корням, которые прочно укоренились в Сакраменто, включая русских, украинцев, белорусов, узбеков, казахов, грузин, армян, латышей, литовцев, эстонцев, молдаван, азербайджанцев, киргизов, таджиков, туркмен и многих других.

Тем не менее, хотим обратить ваше внимание: не все мнения и высказывания, которые звучат в эфире нашей радиостанции, отражают позицию “Нашего Радио”. Мы предоставляем платформу для обмена различными взглядами, но не несем ответственности за мнения и высказывания наших гостей.

Мы верим в свободу слова, но также стремимся к конструктивному и уважительному диалогу.

メールアドレスを共有していたドメイン名nasheradio[.]usのスクリーンショット

次に、19個のドメインIoCをDNS Lookupにかけて重複と既存IoCを取り除いた後、10個のドメインIoCが13個のIPアドレスに名前解決することを確認しました。

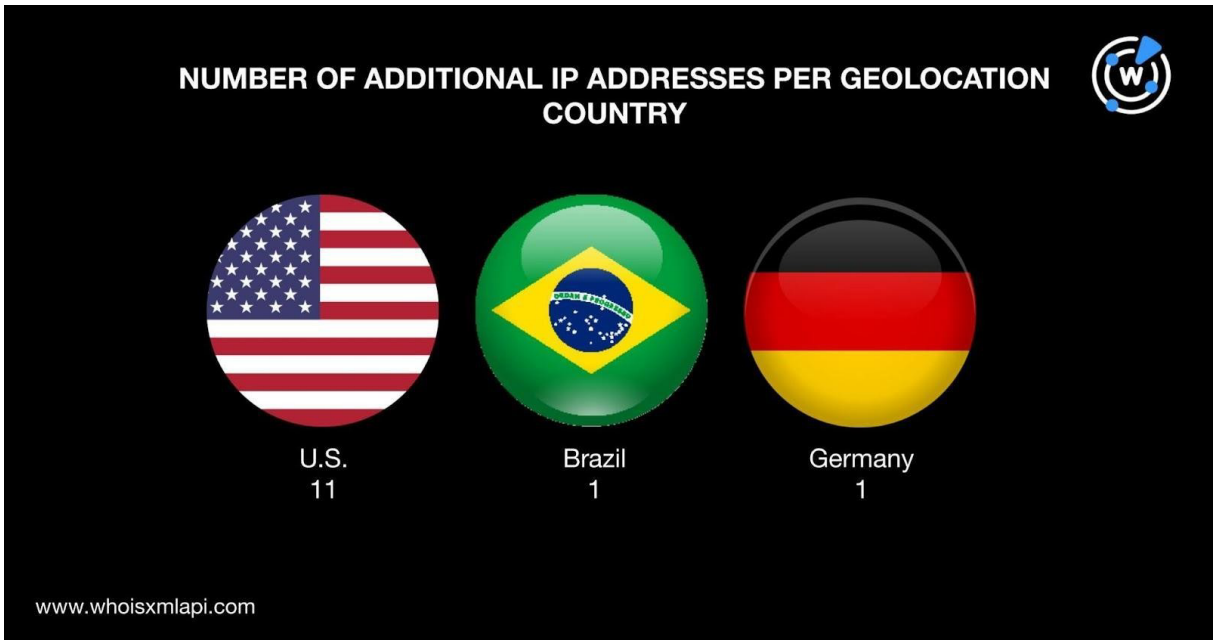
その13個のIPアドレスをThreat Intelligence APIで検索したところ、その全てがさまざまな脅威と関連していることがわかりました。具体的には、以下の通りです。

IPアドレス	関連する脅威の数	脅威の種類
104[.]21[.]29[.]244	3	Generic Phishing Malware
104[.]21[.]4[.]50	3	Malware Phishing Generic
104[.]21[.]43[.]177	3	Malware Phishing Generic
104[.]21[.]62[.]212	1	Malware
104[.]21[.]65[.]69	1	Malware
104[.]21[.]69[.]249	3	Phishing Malware Generic
172[.]67[.]131[.]172	3	Malware Phishing Generic
172[.]67[.]139[.]87	1	Malware
172[.]67[.]150[.]3	3	Generic Phishing Malware
172[.]67[.]182[.]165	3	Malware Phishing Generic
172[.]67[.]189[.]35	1	Malware

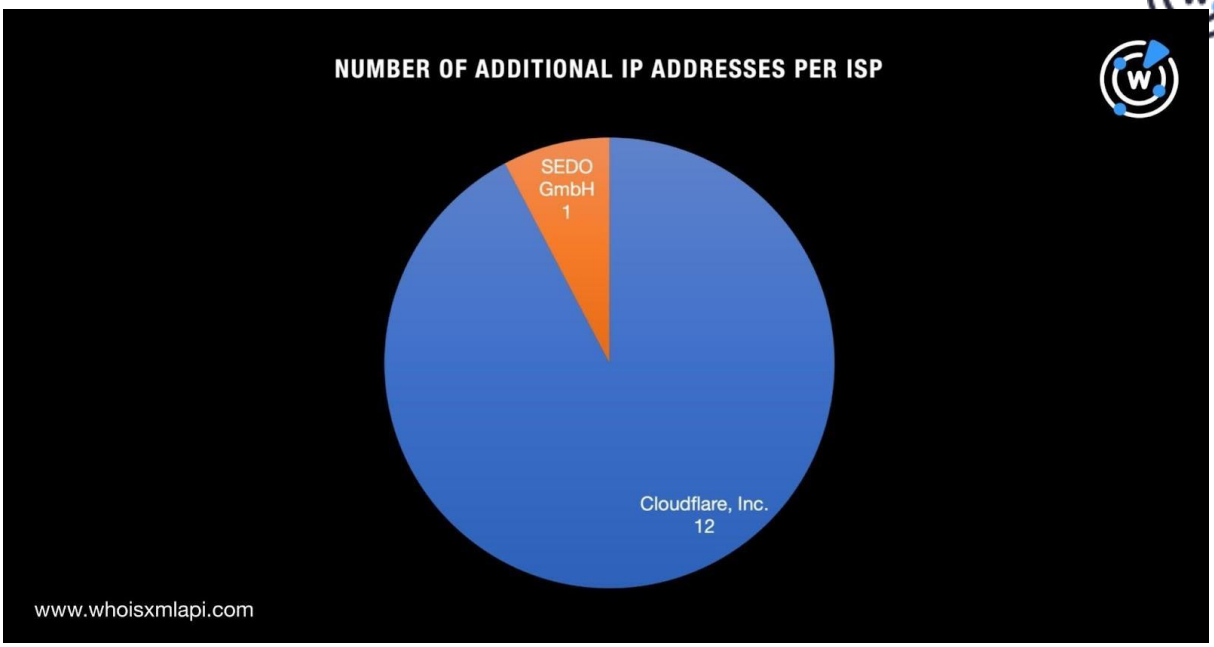
172[.]67[.]216[.]21	3	Phishing Malware Generic
91[.]195[.]240[.]12	5	Malware Phishing Generic Suspicious C2

その13個のIPアドレスについてBulk IP Geolocation Lookupによる一括検索を行ったところ、以下のことが判明しました：

- IPアドレスIoCと同様に、11個のIPアドレスは米国に位置しているようでした。また、ブラジルとドイツを指すIPアドレスが1個ずつありました。



- 12個のIPアドレスは、Cloudflare, Inc.によって管理されていました。また、1個はSEDO GmbHが管理しているアドレスでした。IPアドレスIoCと同じISPを使っているIPアドレスはありませんでした。

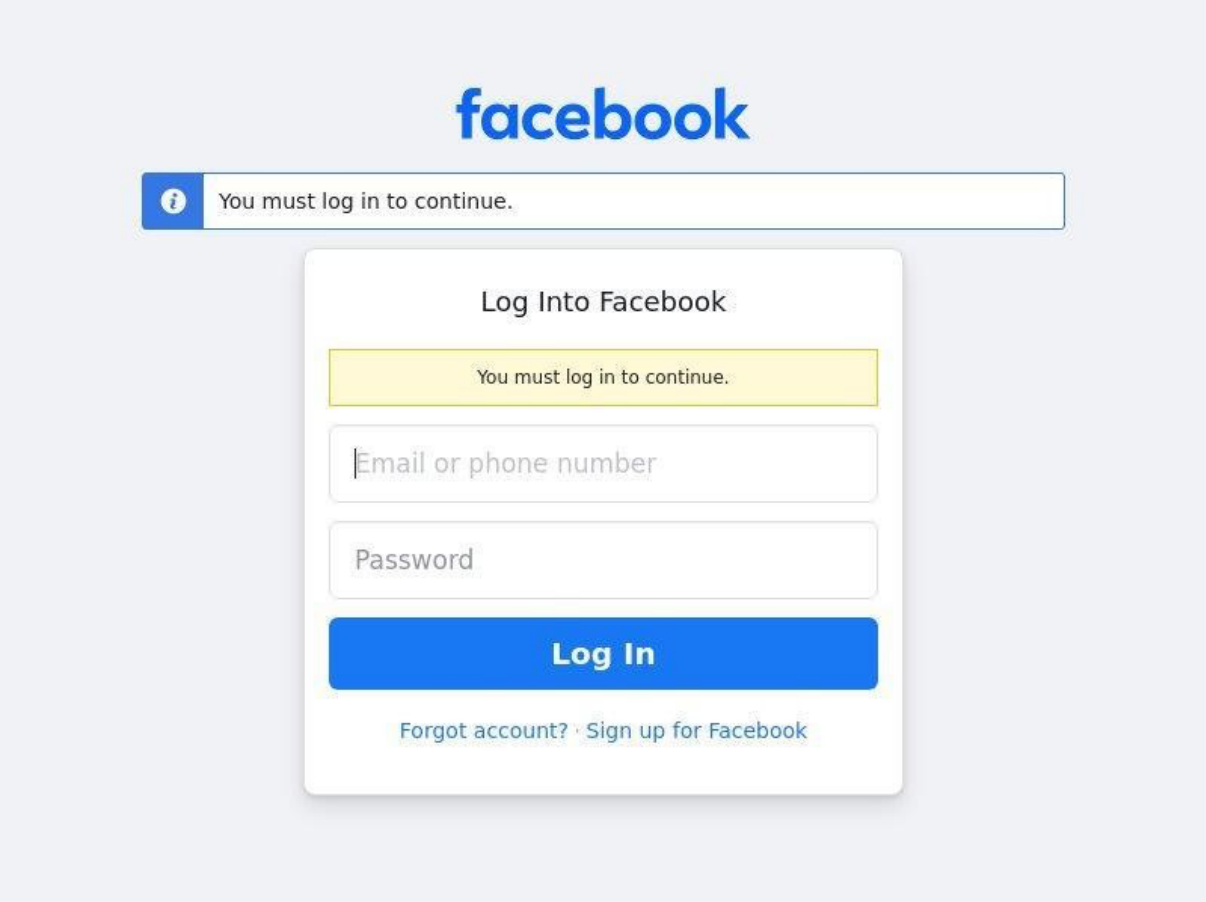


次に、22個のIPアドレス（9個のIPアドレスIoCと今回の調査で見つかった13個のIPアドレス）をReverse IP Lookupにかけたところ、3個は専用ホストらしいことがわかりました。重複、IoCおよび共通のメールアドレスを使用しているドメイン名を除外した後の状態で、それらは合計3個のドメイン名をホストしていました。

19個のドメインIoCをさらに精査し、重複、IoC、共通の文字列またはIPアドレスを使っているドメイン名を削除したところ、ドメインIoCに含まれている文字列が2,772個の別のドメイン名にも含まれていることがわかりました。ここでは、Domains & Subdomains Discoveryにおいて、**Starts with**パラメータを使って以下の文字列を検索しました：

- **assetfinder**
- **barracudas**
- **bikeontop**
- **capitalfinders**
- **claimprocessing**
- **claimunclaimed**
- **dreamteamup**
- **freelookup**
- **gfind**
- **halibut**
- **infocatalog**
- **lewru**
- **lugbara**
- **myunclaimedcash**
- **positivereview**
- **soulcarelife**
- **thebesttime**
- **treasurydept**
- **whatup**

同じ文字列を含むドメイン名をScreenshot Lookupで調べたところ、379個のドメイン名が今日まで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。興味深いことに、whatuptrepstars[.]comは、WHOISレコードからFacebookとの関連性を確認できないにもかかわらず、Facebookのログインページと思われるものに繋がりました。



whatuptrepstars[.]comのスクリーンショット

さらに、Threat Intelligence APIのチェック結果から、IoCと同じ文字列を含むドメイン名であるhalibut[.]siteが1件の脅威（マルウェア）に関与していることがわかりました。

—

UNC2975を当社で詳細に追跡した結果、メールアドレスまたはIPアドレスを共用しているドメイン名が3,027個特定されました。そのうち14個（IPアドレスを共用しているドメイン名13個とIoCと同じ文字列を含むドメイン名1個）は、何らかの脅威に関連しているか、または悪意あるドメイン名として確認済みのものでした。

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

UNC2975のIoC

ドメイン名	IPアドレス
assetfinder[.]org barracudas[.]sbs bikeontop[.]shop capitalfinders[.]org claimprocessing[.]org claimunclaimed[.]org dreamteamup[.]shop freelookup[.]org gfind[.]org halibut[.]sbs infocatalog[.]pics lewru[.]top lugbara[.]top myunclaimedcash[.]org positivereview[.]cloud soulcarelife[.]org thebesttime[.]buzz treasurydept[.]org whatup[.]cloud	34[.]16[.]181[.]0 35[.]203[.]111[.]228 35[.]247[.]194[.]72 47[.]252[.]33[.]131 47[.]252[.]45[.]173 47[.]253[.]141[.]12 47[.]253[.]165[.]1 8[.]209[.]99[.]230 94[.]228[.]169[.]143

共通のメールアドレスを使用していたドメイン名の例

- academic-advising[.]org
- admissionsrequirements[.]net
- alvincommunitycollege[.]net
- americanacademyofaudiology[.]org
- americanacademyofdermatology[.]org
- americanboardofpediatrics[.]org
- americanindiancollege[.]org
- americansocietyofradiologictechnologists[.]com
- associatedstudents[.]net
- athenstechnicalcollege[.]org
- athleticdept[.]org
- atlantadevelopmentauthority[.]com

- beaumontadultschool[.]com
- bentleycollege[.]org
- bethune-cookmancollege[.]com
- bethune-cookmanuniversity[.]com
- boblogan[.]us
- bollingairforcebase[.]com
- brownmackiecollege[.]org
- building-inspector[.]org
- bureauoflaborstatistics[.]org
- butlercountycommunitycollege[.]com
- cadlang[.]org
- californiavirtualcampus[.]com
- campus-security[.]org
- capitolcenterforthearts[.]com
- capt-kirk[.]org
- charter-school[.]org
- checkpageranking[.]org
- checkpagerankings[.]org
- chemicalphysics[.]net
- chemistryteacher[.]net
- choaterosemaryhall[.]org
- christian-college[.]org
- city-data[.]biz
- citycollegecoventry[.]com
- citycollegenorwich[.]com
- citydata[.]mobi
- citydatabase[.]org
- cityofaiken[.]org
- cityofakron[.]net
- cityofaventura[.]org
- cityofbathcollege[.]com
- cityofbend[.]org
- cityofkennewick[.]org
- cityoflubbock[.]net
- cityofpomona[.]org
- cityofrifle[.]com
- cityofsanford[.]net
- cityofunioncity[.]org

今回特定されたIPアドレスの例

- 104[.]21[.]29[.]244
- 104[.]21[.]4[.]50
- 104[.]21[.]43[.]177
- 104[.]21[.]62[.]212
- 104[.]21[.]65[.]69
- 104[.]21[.]69[.]249

IoCと同じ文字列を含むドメイン名の例

- assetfinder-rws[.]com
- assetfinder[.]biz
- assetfinder[.]cl
- assetfinder[.]club
- assetfinder[.]cn
- assetfinder[.]co
- assetfinder[.]co[.]uk
- assetfinder[.]com
- assetfinder[.]com[.]au
- assetfinder[.]de
- assetfinder[.]expert
- assetfinder[.]ie
- assetfinder[.]in
- assetfinder[.]info
- assetfinder[.]net
- assetfinder[.]net[.]au

- assetfinder[.]online
- assetfinder[.]services
- assetfinder[.]sh
- assetfinder[.]uk
- assetfinder[.]us
- assetfinder[.]xyz
- assetfinder02[.]com
- assetfinder02[.]ph
- assetfinder1[.]com
- assetfinder123[.]com
- assetfinder18[.]com
- assetfinder20[.]com
- assetfinder4[.]com
- assetfinder49[.]com
- assetfinder4u[.]com
- assetfinder4unow[.]com
- assetfinder56[.]com
- assetfinder56[.]ws
- assetfinder72[.]com
- assetfinder88[.]com
- assetfinderandrecovery[.]com
- assetfinderassociates[.]com
- assetfindercloud[.]com
- assetfinderco[.]com
- assetfinderconsultant[.]com
- assetfinderexperts[.]com
- assetfinderexperts[.]ws
- assetfindergroup[.]com
- assetfinderhub[.]com
- assetfinderllc[.]com
- assetfindernetwork[.]com
- assetfinderonline[.]com
- assetfinderonus[.]com
- assetfinderplus[.]com
- assetfinderpro[.]com
- assetfinderproject[.]com
- assetfinderpros[.]com
- assetfinderpros[.]net
- assetfinderr[.]com
- assetfinderrecovery[.]com
- assetfinders[.]biz
- assetfinders[.]com
- assetfinders[.]eu
- assetfinders[.]ie
- assetfinders[.]info
- assetfinders[.]net
- assetfinders[.]org
- assetfinders[.]us
- assetfinders007[.]com
- assetfinders123[.]com
- assetfinderservice[.]com
- assetfinderservices[.]com
- assetfindersgroup[.]com
- assetfindersinc[.]com
- assetfindersllc[.]com
- assetfindersllc[.]net
- assetfindersltd[.]com
- assetfindersnetwork[.]com
- assetfindersofamerica[.]com
- assetfindersofamerica[.]us
- assetfindersplus[.]com
- assetfindersrus[.]com
- assetfindersusa[.]com
- assetfindersusa1[.]com
- assetfinderteam[.]com
- assetfinderteam[.]info
- assetfinderteam[.]net
- assetfinderteam[.]org
- assetfindertoolkit[.]com
- assetfinderunlimited[.]com
- assetfinderunlimitedllc[.]com
- assetfinderusa[.]com
- assetfinderz[.]com
- barracudas-ambassadors[.]com
- barracudas-aquarama[.]co[.]za
- barracudas-aquarama[.]com
- barracudas-baseball[.]com
- barracudas-comms[.]co[.]uk
- barracudas-dive[.]ru
- barracudas-hotel[.]ru

- barracudas-hotel[.]xn--kprw13d
- barracudas-hotel[.]xn--kpry57d
- barracudas-hurricanes[.]dk
- barracudas-nue[.]de