Bumblebee SEOポイズニングの痕跡をDNSから探し出す

目次

要旨

Google広告やSEOポイズニングは、マルウェアを拡散するために脅威アクターが好んで使う手口です。ソフトウェアインストーラを装ったBumblebeeに関してSecureworksが行った最近の調査でも、そのことが改めて証明されました。

Bumblebeeは、現在最も広く普及しているエンタープライズアプリケーションのZoom、Cisco AnyConnect、ChatGPTおよびCitrix Workspaceを利用しています。そのため、数百万人のユーザーに影響を与える可能性があります。

Secureworksのレポートでは、2個のドメイン名と29個のIPアドレス、合計31個のセキュリティ侵害インジケーター（IoC）が特定されています。WhoisXML APIはこのIoCリストを拡張する形で、可能な限り多くの潜在的なBumblebee攻撃ベクトルを洗い出す調査を行いました。その結果、新たに以下を発見しました。

- IoCと同じIPホストを使用していた18個のドメイン名。そのうち2個は悪意あるドメイン名と確認
- IoCとして特定されたドメイン名の一つと同様の***appcisco***という文字列と、脅威アクターが悪用したソフトウェアの名前を表す***cisco***、***chatgpt***、***zoom***、***citrix***という文字列を含む1,955個のドメイン名。そのうち3つはマルウェアホストであることが判明

IoCの背後にあるもの

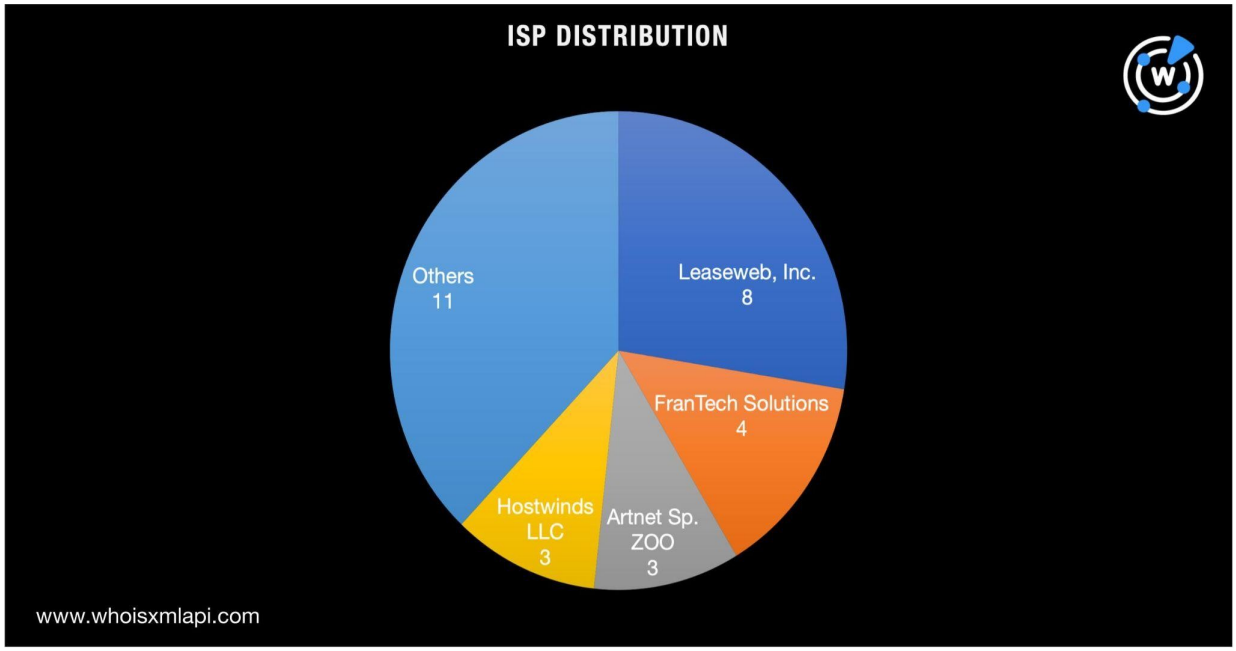
Secureworksの調査結果では、BumblebeeのIoCとして以下が挙げられています。

ドメイン名	IPアドレス
• appcisco[.]com • baveyek[.]com	• 173[.]44[.]141[.]131 • 23[.]82[.]140[.]131

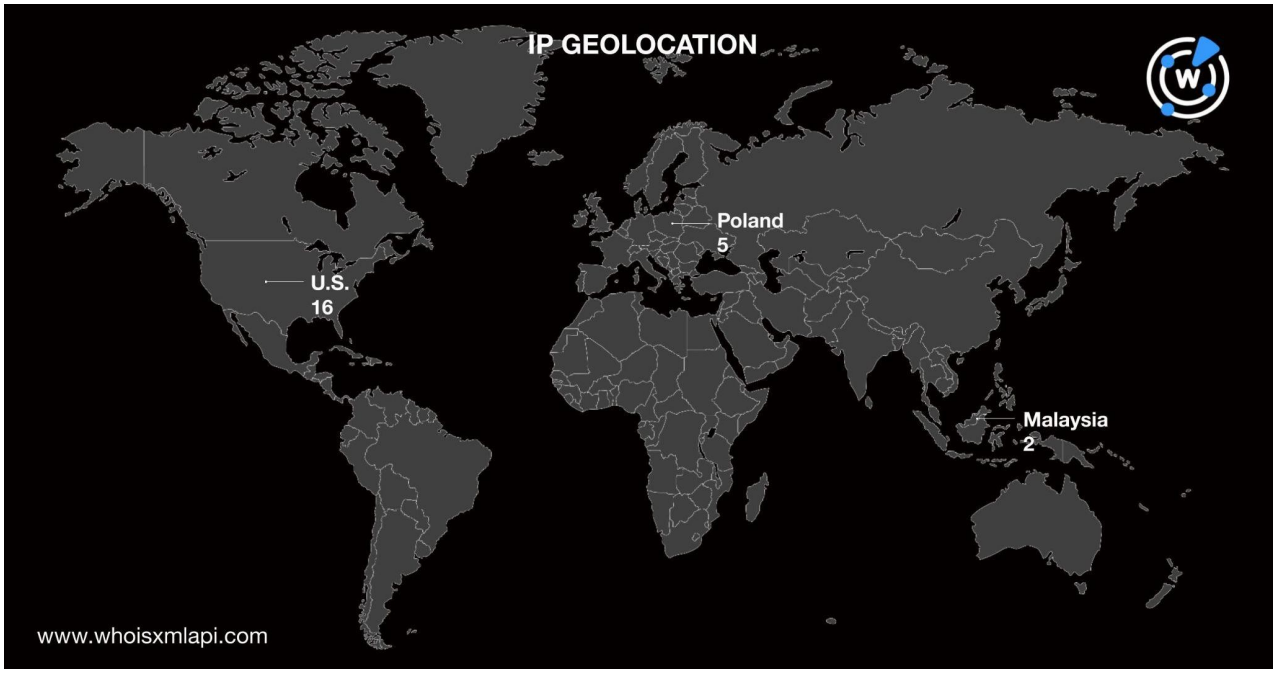
	• 172[.]93[.]193[.]3 • 23[.]81[.]246[.]22 • 95[.]168[.]191[.]134 • 104[.]168[.]175[.]78 • 172[.]93[.]193[.]46 • 157[.]254[.]194[.]104 • 37[.]28[.]157[.]29 • 23[.]106[.]124[.]23 • 194[.]135[.]33[.]182 • 54[.]38[.]139[.]94 • 192[.]119[.]65[.]175 • 107[.]189[.]8[.]58 • 205[.]185[.]114[.]241 • 104[.]168[.]171[.]159 • 103[.]144[.]139[.]159 • 91[.]206[.]178[.]204 • 198[.]98[.]58[.]184 • 172[.]241[.]27[.]120 • 23[.]106[.]223[.]197 • 23[.]108[.]57[.]83 • 54[.]37[.]131[.]232 • 23[.]82[.]128[.]11 • 160[.]20[.]147[.]91 • 103[.]175[.]16[.]10 • 45[.]61[.]187[.]225 • 91[.]206[.]178[.]68 • 193[.]109[.]120[.]252

上記の2つのドメイン名をWHOIS lookupsで検索したところ、2つともNamecheap, Inc.経由で2023年2月に購入されていたことがわかりました。また、どちらのドメイン名についても、アイスランドから登録されたものであることが判明しました。

また、上記の29個のIPアドレスをbulk IP geolocation lookupで調べた結果、そららのうち8つのIPアドレスを管理するLeaseweb, Inc.を筆頭に、10社のISPが管理していることがわかりました。FranTech Solutionsが14%のシェアでLeasewebに続いています。3位はArtnet Sp. ZOOとHostwinds LLCで、それぞれ10%のシェアでした。



IPアドレスのジオロケーション検索では、16個のアドレスが位置していた米国を筆頭に、9カ国に分布していることが明らかになりました。次に多かったのはポーランドとマレーシアで、それぞれ5つと2つのIPアドレスが位置していました。



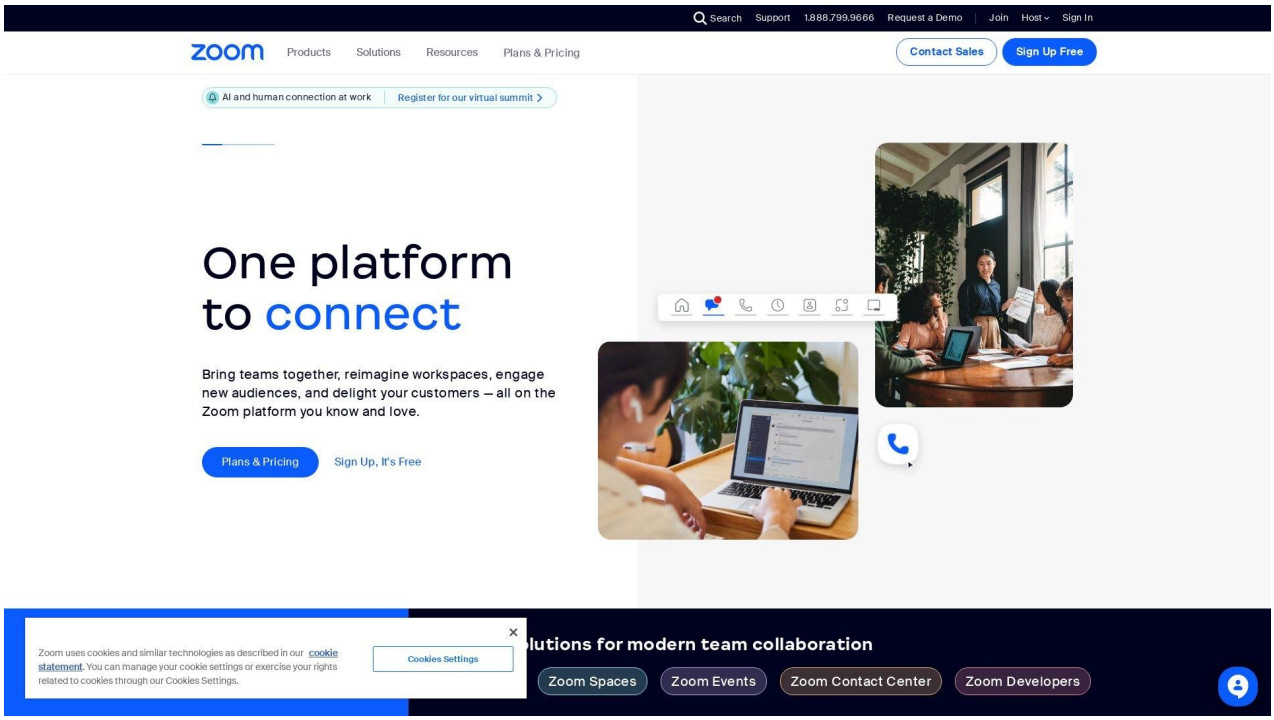
なお、ドメイン名登録者は自分の居住国としてアイスランドを指定していましたが、IoCとして特定されたIPアドレスのうち、アイスランドに位置するものはありませんでした。

BumblebeeのDNSにおけるつながり

次に、IoCとして特定されたIPアドレスをreverse IP lookupsで検索しました。その結果、18個のIPアドレスは解決せず、残りの11個は専用アドレスとわかりました。また、専用IPアドレスでホストされている18個のドメイン名が特定され、そのうちの2つは悪意あるドメイン名と確認されました。悪意あるドメイン名の一つであるnewsoftup[.]comは、以下のスクリーンショットように、ページのさらなる設定が必要ではあるものの、アクセス可能な状態になっていました。

newsoftup[.]comのスクリーンショット

Bumblebeeを詳細に分析したところ、4つのソフトウェアプロバイダの名前（Cisco、ChatGPT、Zoom、Citrix）の名前が悪用されていたことがわかりました。そこで、他の攻撃ベクターがないかを確かめるため、Domains & Subdomains Discoveryを使って、***cisco***、***chatgpt***、***zoom***、および***citrix***という文字列を含むドメイン名を探しました。その結果、1,955個のドメインが新たに発見されました。そのうちの3つはマルウェアのホストでした。本稿執筆時点で、appcisco[.]usはアクセス不能であり、zoom[.]cyouはパークドメインでした。また、zoom[.]com[.]deは有効なコンテンツをホストし続けていました。

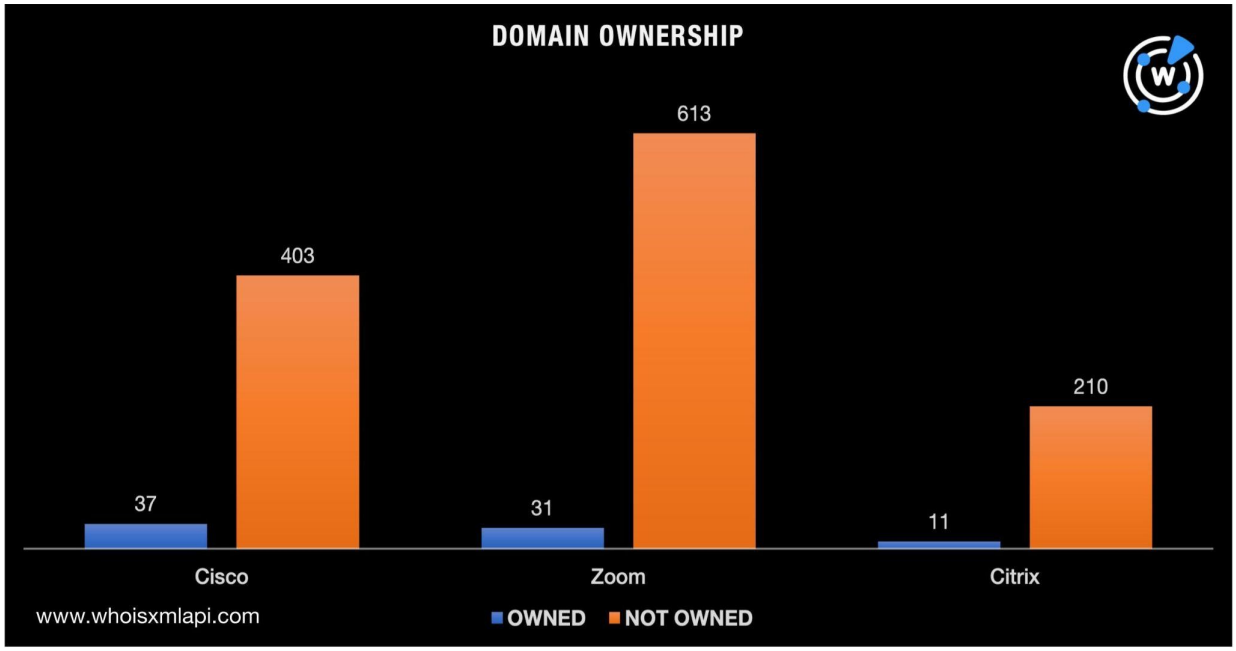


zoom[.]com[.]deのスクリーンショット

zoom[.]com[.]deは、Zoomの公式ウェブサイトで使われているドメイン名のzoom[.]comにそっくりですが、公開のWHOISレコードを見る限り、Zoomに帰属していることは確認できませんでした。

最後のステップとして、ブランドを含む1,900超のドメイン名のうち、名前が文字列に含まれている企業が実際に所有しているドメイン名がどれだけあるか調べました。なお、openai[.]com（ChatGPTの所有者）のWHOISレコードは一部が非公開にされているため、***chatgpt***を含むドメイン名はこの分析から除外しました。また、ドメイン名の所有者を特定するため、***cisco***および***citrix***を含むドメイン名には登録者のメールアドレスを、***zoom***を含むドメイン名には登録者の組織を使用して検索しました。

その結果、Cisco、Zoom、Citrixに帰属すると公表されているドメイン名は、ブランドを含むドメイン名全体のわずか6%に過ぎないことが判明しました。特に、Ciscoらしい1,305個のドメイン名のうち、Ciscoが実際に所有していたドメイン名は37個しかありませんでした。ZoomとCitrixが所有していたドメイン名はそれぞれ31個と11個にとどまりました。



—

Bumblebeeの例が示すように、見た目の似たドメイン名でホストされ、企業のロゴを表示しているサイトでも、その全てが信頼できるとは限りません。例えば、zoom[.]comとzoom[.]com[.]deのWHOISレコードを比較したところ、後者はサイバースクワッティングである可能性が高いことがわかりました。DNSの精査を進めれば、Cisco、Zoom、Citrixの所有であることが公開のWHOIS情報から確認できない1,200超のドメイン名についても、同様のことが確認される可能性があります。

同様の調査をご希望のお客様、または本調査のデーター式をご希望のお客様は、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

IoCと同じIPアドレスを使用していたドメイン名の例

- 157-254-194-104[.]plesk[.]page
- barnco-agricola[.]com
- d157029[.]artnet[.]gda[.]pl
- festive-cannon[.]157-254-194-104[.]plesk[.]page
- fs3vjo97f[.]dubbed1686[.]cf
- hollistechhelp[.]com
- hwsrv-1039376[.]hostwindsdns[.]com
- hwsrv-1040739[.]hostwindsdns[.]com
- hwsrv-1041841[.]hostwindsdns[.]com

- jovial-blackwell[.]157-254-194-104[.]plesk[.]page

IPアドレスを共用していた悪意あるドメイン名の例

- newsoftup[.]com

appcisco、*cisco*、*chatgpt*、*zoom*および*citrix*という文字列を含むドメイン名の例

- appcisco[.]us
- cisco[.]xn--io0a7i
- cisco[.]nyc
- cisco[.]cc
- cisco[.]xn--vuq861b
- cisco[.]space
- cisco[.]org[.]ru
- cisco[.]cymru
- cisco[.]pk
- cisco[.]ac[.]mw
- cisco[.]al
- cisco[.]off[.]ai
- cisco[.]net[.]pl
- cisco[.]gy
- cisco[.]lol
- cisco[.]org[.]ki
- cisco[.]co[.]tt
- cisco[.]security
- cisco[.]bar
- cisco[.]pics
- cisco[.]re
- cisco[.]pub
- cisco[.]moscow
- cisco[.]asia
- cisco[.]promo
- chatgpt[.]market
- chatgpt[.]media
- chatgpt[.]builders
- chatgpt[.]software
- chatgpt[.]pk
- chatgpt[.]loans
- chatgpt[.]cricket
- chatgpt[.]sexy
- chatgpt[.]org[.]uk
- chatgpt[.]diamonds
- chatgpt[.]clothing
- chatgpt[.]pro[.]vn
- chatgpt[.]vg
- chatgpt[.]wf
- chatgpt[.]moscow
- chatgpt[.]mg
- chatgpt[.]me[.]uk
- chatgpt[.]republican
- chatgpt[.]reviews
- chatgpt[.]soy
- chatgpt[.]hockey
- chatgpt[.]maison
- xn--chtgpt-jua[.]se
- chatgpt[.]jp
- chatgpt[.]zone
- zoom[.]football
- zoom[.]co[.]pl
- zoom[.]associates
- zoom[.]pictures
- zoom[.]mortgage
- zoom[.]czest[.]pl
- zoom[.]xn--5tzm5g
- zoom[.]sexy
- zoom[.]date
- zoom[.]moscow
- zoom[.]lighting
- zoom[.]realty

- zoom[.]salon
- zoom[.]accountants
- zoom[.]school
- zoom[.]review
- zoom[.]org[.]cn
- zoom[.]net
- zoom[.]co[.]gg
- zoom[.]yoga
- xn--oom-5ez[.]com
- xn--zom-1lz[.]com
- zoom[.]black
- zoom[.]industries
- zoom[.]photo
- citrix[.]wang
- citrix[.]ms
- citrix[.]pub
- citrix[.]ninja
- citrix[.]engineering
- citrix[.]nyc
- citrix[.]world
- citrix[.]cx
- citrix[.]agency
- xn--citr-oza8916b[.]com
- citrix[.]work
- citrix[.]fr
- citrix[.]se
- citrix[.]ae
- citrix[.]today
- citrix[.]llc
- citrix[.]si
- citrix[.]jobs
- citrix[.]io
- citrix[.]info
- citrix[.]ovh
- citrix[.]surf
- citrix[.]partners
- citrix[.]me
- citrix[.]tokyo

共通の文字列を含む悪意あるドメイン名の例

- appcisco[.]us
- zoom[.]com[.]de