DNSインテリジェンスでChatGPTのフィッシングを発見

目次

要旨

2022年11月のサービス開始以来、ChatGPTの評判は利用者のみならず悪用者の間でも高まる一方です。Cybleの研究者が最近、ChatGPTと思われるサイトを利用して個人情報、特にクレジットカードのデータを盗み出すフィッシング攻撃を発見しました。

Cybleの研究では、セキュリティ侵害インジケーター（IoC）として、openai-pc-pro[.]online、chat-gpt-pc[.]online、chatgpt-go[.]online、rebrand[.]lyという4つのドメイン名が特定されました。当社ではこのほど、これらのIoCを出発点として調査を水平展開し、以下を発見しました。

- IoC が名前解決した 5 つの IP アドレス
- IoC と同じ IP アドレスを使用していた 303 個のドメイン名 。そのうち 1 つは悪意あるドメイン名と確認
- IoC と同様に ***openai***、***chatgpt*** または ***rebrand*** という文字列で始まる 1,142 個のドメイン名。 そのうち 11 個はマルウェアホストであることを確認
- ***chatgpt*** という文字列を含む,2,693 個のサブドメイン。そのうち 5 つはすでに悪意あるキャンペーンに関与している可能性あり

WHOISの繋がり

まず、4つのIoCをbulk WHOIS lookupで検索したところ、openai-pc-pro[.]online、chat-gpt-pc[.]online、chatgpt-go[.]onlineは最近新規登録されたドメイン名で、rebrand[.]lyは9年前に登録されたドメイン名であることが判明しました。また、これらをWHOISレコードで正規のドメイン名であるopenai[.]comおよびrebrand[.]comと比較したところ、4つのいずれも、ドメイン名の文字列として表示されている企業の所有ではないように見えました。具体的には、以下の結果が出ました。

- openai-pc-pro[.]online、chat-gpt-pc[.]online、chatgpt-go[.]onlineのレジストラと登録者の国は、openai[.]comのそれ（Gandi SAS、フランス）と異なる。
- Openai-pc-pro[.]onlineとchat-gpt-pc[.]onlineのレジストラはNamecheap, Inc.で、chatgpt-go[.]onlineのレジストラはPDR Ltd.。

- openai-pc-pro[.]onlineとchat-gpt-pc[.]onlineの登録者の国はアイスランドで、chatgpt-go[.]onlineの登録者の国はルーマニア。

DNSの繋がり

公表されていない他の関連性を見つけるためにIoCのDNSルックアップを行ったところ、69[.]12[.]73[.]19、104[.]21[.]21[.]135、172[.]67[.]199[.]21を含む5つのIPアドレスに名前解決しました。これらのIPアドレスのジオロケーション検索とIP/DNSの逆引きでは、以下が判明しました。

- 4つは米国、1つはベトナムのアドレス。
- 1つのIPアドレスはドメイン名に関連づけられていなかった。
- 2つは共用IPアドレス、もう2つはプライベートホストらしい。
- DNSの関連性を持っている4つのIPアドレスは、303個のドメインをホスト。そのうち1つ、denizyilbasiozel-taycan4s[.]comは、悪意のドメイン名と確認。

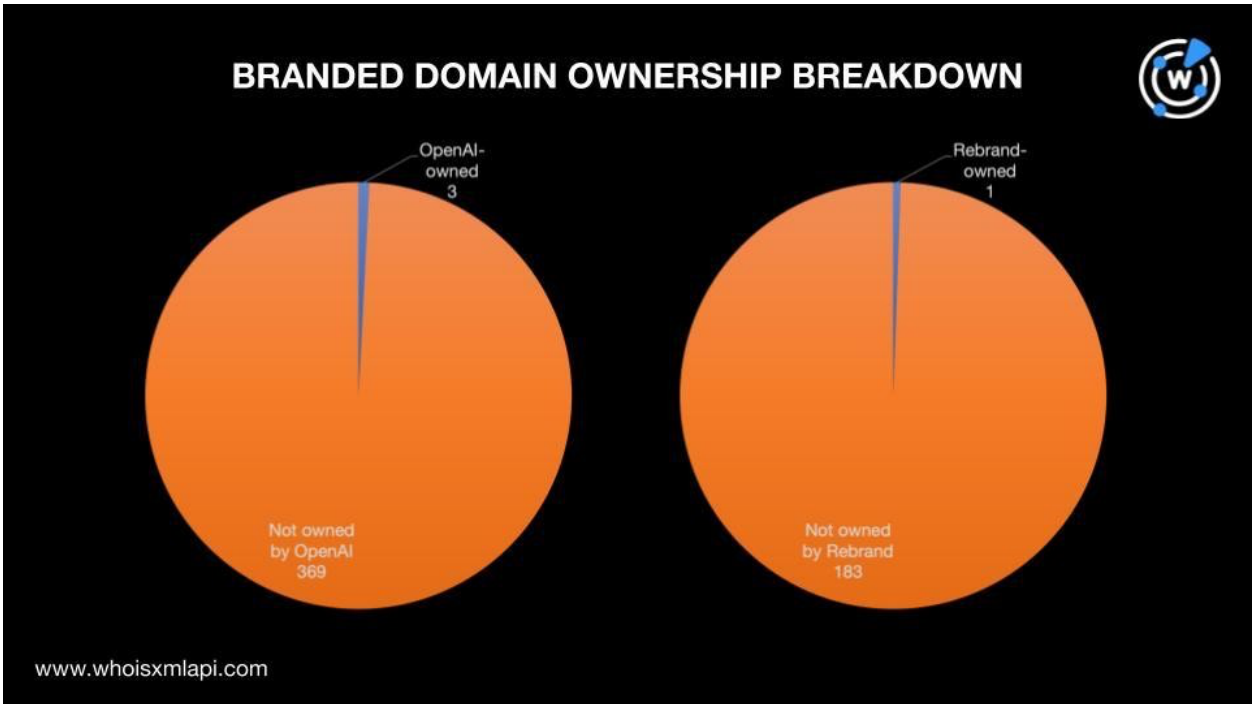
OpenAI、ChatGPT、Rebrandという3つのブランド名がIoCの中に見られました。***openai***、***chatgpt***、***rebrand***で始まり、***chatgpt***を含んでいる他のドメイン名がないか確認するため、これらの単語をキーワードにしてDomains & Subdomains Discoveryで検索しました。その結果、以下を発見しました。

- ***openai***、***chatgpt***、***rebrand***で始まる1,142個のドメイン名。そのうち11個は悪意あるドメイン名と確認
- ***chatgpt***を含む2,693個のサブドメイン。そのうち5つはマルウェアのホストと確認

その他の調査結果

さらに、共通の文字列を含むドメイン名とサブドメインのWHOISレコードを比較することで、次の興味深い結果が得られました。

- ***openai***で始まる372個のドメイン名のうち、OpenAIの登録者と同じレジストラを使い、同じ国で登録されたドメイン名は3つのみ。ただし、openai[.]comのWHOISレコードが非表示であったため、それらのドメイン名の所有権を正確には確認できず。
- ***rebrand***で始まる184個のドメイン名のうち、登録者のメールアドレスからRebrandが実際に所有しているとわかったのは1つのみ。
- ***chatgpt***で始まる589個のドメイン名のうち、レジストラおよび登録国がOpenAIのそれと同じものはなし。***openai***で始まるドメイン名のうち3つは、レジストラと登録国がOpenAIのそれと同じ。***rebrand***で始まるドメイン名のうちRebrandが所有していると思われるドメイン名は1つのみ。



- IoCに見られた文字列（***openai***、***rebrand***および***chatgpt***）を含むドメイン名において見られた文字列は、***chatgpt***のみ。
- ***chatgpt***という文字列はOpenAIに属する正規のドメイン名のサブドメインとしてのみ出現するため、***chatgpt***を含むサブドメインも調べました。WHOISレコードを調べた結果、***chatgpt***を含む2,693のサブドメインのうち、OpenAIが所有していると思われるものはありませんでした。

—

ChatGPTをテーマにしたフィッシングキャンペーンの存在が示すように、オンラインでの人気は諸刃の剣です。より多くのユーザーがこの技術とその利点を認識するようになる一方で、フィッシャーやその他のサイバー犯罪者がキャンペーンにこの名前を使用することも増えているのです。

同様の調査をご希望のお客様、またはこの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

Cybleが特定したChatGPT関連のIoC

- openai-pc-pro[.]online
- chat-gpt-pc[.]online

- chatgpt-go[.]online
- rebrand[.]ly

IoCが名前解決したIPアドレスの例

- 69[.]12[.]73[.]19
- 104[.]21[.]21[.]135
- 172[.]67[.]199[.]21

共通のIPアドレスを使っていたドメイン名の例

- 123movies[.]gr
- 147golkoop[.]buzz
- 1c[.]co[.]uk
- 1xslots-com8[.]buzz
- 22022140[.]xyz
- 33singapore[.]co
- 365doohd[.]com
- 404808909[.]com
- 414connecticut[.]com
- 50wmg1[.]cyou
- 607790[.]com
- a1plus[.]tk
- a4vn[.]com
- abcdbusiness[.]nz
- abergloranex[.]gq
- abzrszjv[.]tk
- accratursentipe[.]tk
- acnabupotoswolf[.]cf
- acnadesbau[.]gq
- adaldahamwhitsmall[.]makeup
- adthedemcaningder[.]ml
- afterburner[.]pics
- agnifipoundpo[.]tk
- airambulanceservicelist[.]life
- aircoolerportable[.]top
- akota-ket-new2022s[.]ru[.]com
- aleshaper[.]sa[.]com
- allweathertiresny[.]com
- almastrade[.]com
- almzoonsh[.]com
- alphabetacyber[.]com
- altidocana[.]gq
- alupnop[.]cf
- amazonitadesign[.]com[.]br
- amlicentrasto[.]ga
- anacovbarsono[.]tk
- anadconniditc[.]tk
- anadolumsigorta[.]online
- angle777899[.]com
- angp[.]uk
- anime-vn[.]net
- antiere[.]tk
- anupawogal[.]tk
- api[.]chciflek[.]cz
- aralinsmegwatch[.]tk
- armzzonm[.]com
- artherbivesithom[.]ga
- arubanci[.]cf
- aryamanadhikari[.]com[.]np
- asarpibersepi[.]ml

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

- denizyilbasiozel-taycan4s[.]com

openai、*chatgpt*、*rebrand*で始まるドメイン名の例

- openai[.]kz
- openai[.]ca

- openai[.]gay
- openai[.]vn
- openai[.]bzh
- openai[.]coffee
- openai[.]enterprises
- openai[.]one
- openai[.]net[.]co
- openai[.]plus
- openai[.]fun
- openai[.]team
- openai[.]solar
- openai[.]camp
- openai[.]icu
- openai[.]money
- openai[.]cloud
- openai[.]cash
- openai[.]fund
- openai[.]xn--fjq720a
- openai[.]watch
- openai[.]asia
- openai[.]uno
- openai[.]us
- openai[.]xyz
- openai[.]co[.]uk
- openai[.]careers
- openai[.]systems
- openai[.]city
- openai[.]moscow
- rebrand[.]guide
- rebrand[.]services
- rebrand[.]sk
- rebrand[.]fi
- rebrand[.]press
- rebrand[.]mba
- rebrand[.]one
- rebrand[.]io
- rebrand[.]asia
- rebrand[.]mobi
- rebrand[.]id
- rebrand[.]tech
- rebrand[.]biz
- rebrand[.]com[.]br
- rebrand[.]church
- rebrand[.]reviews
- rebrand[.]studio
- rebrand[.]com[.]au
- rebrand[.]com
- rebrand[.]moscow
- rebrand[.]fyi
- rebrand[.]ly
- rebrand[.]com[.]ph
- rebrand[.]ge
- rebrand[.]pro
- rebrand[.]dev
- rebrand[.]global
- rebrand[.]nyc
- rebrand[.]ru
- rebrand[.]kz
- chatgpt[.]house
- chatgpt[.]win
- chatgpt[.]parts
- chatgpt[.]yn[.]cn
- chatgpt[.]auction
- chatgpt[.]feedback
- chatgpt[.]adult
- chatgpt[.]singles
- chatgpt[.]surf
- chatgpt[.]koeln
- chatgpt[.]organic
- chatgpt[.]al
- chatgpt[.]be
- chatgpt[.]es
- chatgpt[.]xn--fiq228c5hs
- chatgpt[.]actor
- chatgpt[.]productions
- chatgpt[.]online
- chatgpt[.]party
- chatgpt[.]global
- chatgpt[.]vn
- chatgpt[.]tools

- chatgpt[.]exchange
- chatgpt[.]tg
- chatgpt[.]co[.]nz
- chatgpt[.]cleaning
- chatgpt[.]property
- chatgpt[.]id
- chatgpt[.]bike
- chatgpt[.]tennis
- chatgpt[.]kiwi
- chatgpt[.]doctor
- chatgpt[.]edu[.]pl
- chatgpt[.]futbol
- chatgpt[.]camera
- chatgpt[.]rent
- chatgpt[.]vodka
- chatgpt[.]sc[.]cn
- chatgpt[.]ong
- chatgpt[.]country

共通の文字列を含む悪意あるドメイン名の例

- chatgpt[.]run
- chatgpt[.]cruises
- chatgpt[.]xyz
- chatgpt[.]bargains
- chatgpt[.]love
- chatgpt[.]tf

*chatgpt*を含むサブドメインの例

- chatgpt[.]mevtic[.]ci
- chatgpt[.]dev[.]br
- chatgpt[.]tec[.]br
- chatgpt[.]eu[.]com
- chatgpt[.]cherishmoon[.]fun
- chatgpt[.]xbeibeix[.]com
- chatgpt[.]isning[.]ml
- chatgpt[.]senseidev[.]com
- chatgpt[.]everains[.]com
- chatgpt[.]askandgo[.]com[.]ua
- chatgpt[.]talhasultan[.]dev
- chatgpt[.]ciniugo[.]com
- chatgpt[.]xll[.]cc
- chatgpt[.]xrbzy[.]tk
- chatgpt[.]elitejoy[.]cn
- chatgpt[.]bellcousin[.]com
- chatgpt[.]zhuang-hu[.]com
- chatgpt[.]wrss[.]tk
- chatgpt[.]scld[.]cc
- chatgpt[.]esw[.]ink
- chatgpt[.]fjycnet[.]com
- chatgpt[.]0594codes[.]cn
- chatgpt[.]jingjiang[.]com
- chatgpt[.]realrohail[.]com
- chatgpt[.]devstage[.]com[.]ar
- chatgpt[.]astrodijitaldemo[.]com
- chatgpt[.]willieras[.]co[.]za
- chatgpt[.]oar6[.]com
- chatgpt[.]record2life[.]top
- chatgpt[.]dl-am[.]cn
- chatgpt[.]xinlab[.]fun
- chatgpt[.]ericcai[.]fun
- chatgpt[.]isaruxcloud[.]com
- chatgpt[.]imlam[.]com
- chatgpt[.]embery[.]com[.]au
- chatgpt[.]voidm[.]com
- chatgpt[.]shuzibaobao[.]com
- chatgpt[.]leyeeyle[.]net
- chatgpt[.]tvfans[.]top
- chatgpt[.]snsxiong[.]com
- chatgpt[.]gowd[.]tech
- chatgpt[.]aejson[.]com
- chatgpt[.]onionhealth[.]cn
- chatgpt[.]yoxix[.]com
- chatgpt[.]devcn[.]xyz
- chatgpt[.]ijike[.]wang

- chatgpt[.]wycwhj[.]ga
- chatgpt[.]somallq[.]com
- chatgpt[.]51meteor[.]com
- chatgpt[.]binishare[.]com
- chatgpt[.]ai-pro[.]org
- chatgpt[.]robotsfan[.]com
- chatgpt[.]wxyes[.]com
- chatgpt[.]lunatech-pro[.]net
- chatgpt[.]evertools[.]io
- chatgpt[.]malliavin[.]com
- chatgpt[.]helv[.]io
- chatgpt[.]geekershare[.]com
- chatgpt[.]exopidea[.]com
- chatgpt[.]hersecret[.]fi
- chatgpt[.]groro[.]io
- chatgpt[.]omithasan[.]com
- chatgpt[.]reddevs[.]net
- chatgpt[.]ru[.]com
- chatgpt[.]yuxy[.]cyou
- chatgpt[.]scholarcn[.]com
- chatgpt[.]teddysc[.]me
- chatgpt[.]1host[.]cn
- chatgpt[.]chaoyang[.]online
- chatgpt[.]360s[.]online
- chatgpt[.]haiying[.]co
- chatgpt[.]jswh[.]me
- chatgpt[.]bansoft[.]ru
- chatgpt[.]np-cloud[.]com
- chatgpt[.]zhaiwuxian[.]com
- chatgpt[.]2mb[.]xyz
- chatgpt[.]hackings[.]life
- chatgpt[.]ooo[.]ng
- chatgpt[.]gov6[.]net
- chatgpt[.]altervista[.]org
- chatgpt[.]545game[.]com
- chatgpt[.]qjidea[.]com
- chatgpt[.]print-rite[.]com
- chatgpt[.]em248[.]com
- chatgpt[.]num[.]la
- chatgpt[.]uk[.]net
- chatgpt[.]examhero[.]com
- chatgpt[.]3pixel[.]com[.]cn
- chatgpt[.]quickso[.]cn
- chatgpt[.]kribs[.]co[.]in
- chatgpt[.]autoadministrables[.]com
- chatgpt[.]uzi[.]co[.]in
- chatgpt[.]zx[.]al
- chatgpt[.]henanyaoneng[.]com
- chatgpt[.]vvxo[.]cn
- chatgpt[.]uibim[.]com
- chatgpt[.]next-step[.]asia
- chatgpt[.]eevv[.]ml
- chatgpt[.]gg740976583[.]monster
- chatgpt[.]paradise[.]ink

共通の文字列を含む悪意あるドメイン名の例

- chatgpt[.]easncdm[.]cf
- chatgpt[.]digitalhooked[.]com
- chatgpt[.]oxz[.]icu