# Detecting ChatGPT Phishing on Social Media with the Help of DNS Intelligence

## Table of Contents



## Executive Report

Since its launch last November, the ChatGPT hype has only increased not only among users but also abusers. Cyble researchers recently spotted phishing attacks using supposed ChatGPT sites to phish for personally identifiable information (PII), specifically credit card data.

The Cyble study identified four domains as indicators of compromise (IoCs)—openai-pc-pro[.]online, chat-gpt-pc[.]online, chatgpt-go[.]online, and rebrand[.]ly— that we used as jump-off points for an expansion analysis that led to the discovery of:

- Five IP addresses the IoCs resolved to
- 303 domains that shared the IoCs' IP hosts, one of which turned out to be malicious
- 1,142 domains that started with the strings ***openai.***, ***chatgpt.***, and ***rebrand.*** akin to two of the IoCs, 11 of which were confirmed malware hosts
- 2,693 subdomains that contained the string ***chatgpt***, five of which may have already figured in malicious campaigns

### WHOIS Connections

We began our analysis with a bulk WHOIS lookup for the IoCs that showed three of them were newly registered—openai-pc-pro[.]online, chat-gpt-pc[.]online, and chatgpt-go[.]online, while rebrand[.]ly was already nine years old. None of them seem to be owned by the companies whose names appeared as strings in them based on WHOIS record comparisons with the legitimate domains openai[.]com and rebrand[.]com. Specifically:

- The domains openai-pc-pro[.]online, chat-gpt-pc[.]online, and chatgpt-go[.]online didn't share openai[.]com's registrar Gandi SAS and registrant country France.
- Openai-pc-pro[.]online and chat-gpt-pc[.]online's registrar was Namecheap, Inc., while that of chatgpt-go[.]online was PDR Ltd.

- Also, openai-pc-pro[.]online and chat-gpt-pc[.]online's registrant country was Iceland, while that of chatgpt-go[.]online was Romania.

## DNS Ties

To find other connections that haven't been publicized, we performed DNS lookups on the IoCs that gave us five IP address resolutions, three of which are 69[.]12[.]73[.]19, 104[.]21[.]21[.]135, and 172[.]67[.]199[.]21. IP geolocation and reverse IP/DNS lookups for the IP hosts showed that:

- Four of them originated from the U.S., while one was from Vietnam.
- One IP address didn't have domain connections.
- Two were shared IP hosts, while another two appeared to be private hosts.
- The four IP addresses with existing DNS connections hosted 303 domains, one of which—denizyilbasiozel-taycan4s[.]com—turned out to be malicious.

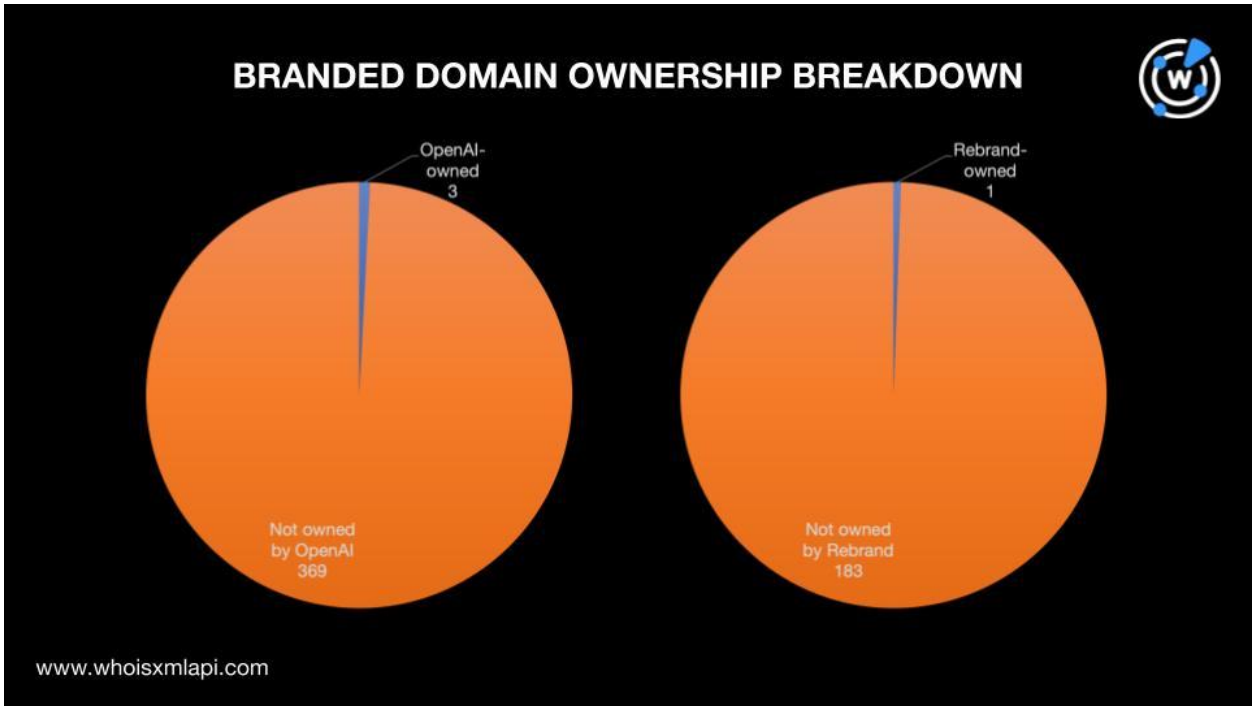
Three brand names—OpenAI, ChatGPT, and Rebrand—appeared in the IoCs. To determine if more domains started with ***openai.***, ***chatgpt.***, and ***rebrand.*** and contain ***chatgpt***, we used them as Domains & Subdomains Discovery search terms. That led to the discovery of:

- 1,142 domains that started with ***openai.***, ***chatgpt.***, and ***rebrand.***, 11 of which turned out to be malicious
- 2,693 subdomains that contained ***chatgpt***, five of which were confirmed malware hosts

## Other Findings

Additional WHOIS record comparisons of the string-connected domains and subdomains yielded interesting findings, such as:

- Only three of the 372 domains that started with ***openai.*** shared OpenAI's registrar and registrant country. We couldn't precisely confirm their ownership, though, since openai[.]com's WHOIS record was redacted.
- Only one of the 184 domains that started with ***rebrand.*** was owned by Rebrand based on its registrant email address.
- None of the 589 domains that started with ***chatgpt.*** shared OpenAI's registrar and registrant country. Three of the domains starting with ***openai.*** shared OpenAI's registrar and registrant country while only one domain beginning with ***rebrand.*** seemed to be owned by Rebrand.




- Among the domains that contained strings found among the IoCs (i.e., ***openai.***, ***rebrand.***, and ***chatgpt.***), only ***chatgpt.*** appeared in them.
- We also looked at subdomains that contained ***chatgpt*** since the string appeared only as a subdomain of the legitimate domain belonging to OpenAI. None of the 2,693 subdomains that contained ***chatgpt*** seemed to be owned by the company after careful scrutiny of their WHOIS record details.

—

Popularity online is a double-edged sword as the ChatGPT-themed phishing campaigns showed. While more and more users are becoming aware of the technology and its benefits, an increasing number of phishers and other cybercriminals are bound to use its name in their campaigns.

***If you wish to perform a similar investigation or get access to the full data behind this research, please don't hesitate to contact us.***

## Appendix: Sample Artifacts and IoCs

### ChatGPT-Related Attack IoCs Identified by Cyble Researchers

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

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

## Sample IP Addresses to Which the IoCs Resolved

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

## Sample IP-Connected Domains

- 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

## Malicious IP-Connected Domain

- denizyilbasiozel-taycan4s[.]com

## Sample Domains That Start with *openai.*, *chatgpt.*, and *rebrand.*

- 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

## Sample Malicious String-Connected Domains

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

## Sample Subdomains That Contain the String *chatgpt*

- 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

## Sample Malicious String-Connected Subdomains

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