WhoisXMLAPI
The Who Behind Domain, IP & Cyber Threat Intelligence

Hunting for DNS Traces of Hundreds of Malicious Google Play Apps

Table of Contents

Executive Report

Bitdefender uncovered a large-scale ad fraud campaign involving hundreds of malicious apps in Google Play that have been downloaded more than 60 million times. The apps displayed out-of-context ads and persuaded victims to give away their credentials and credit card information via phishing.

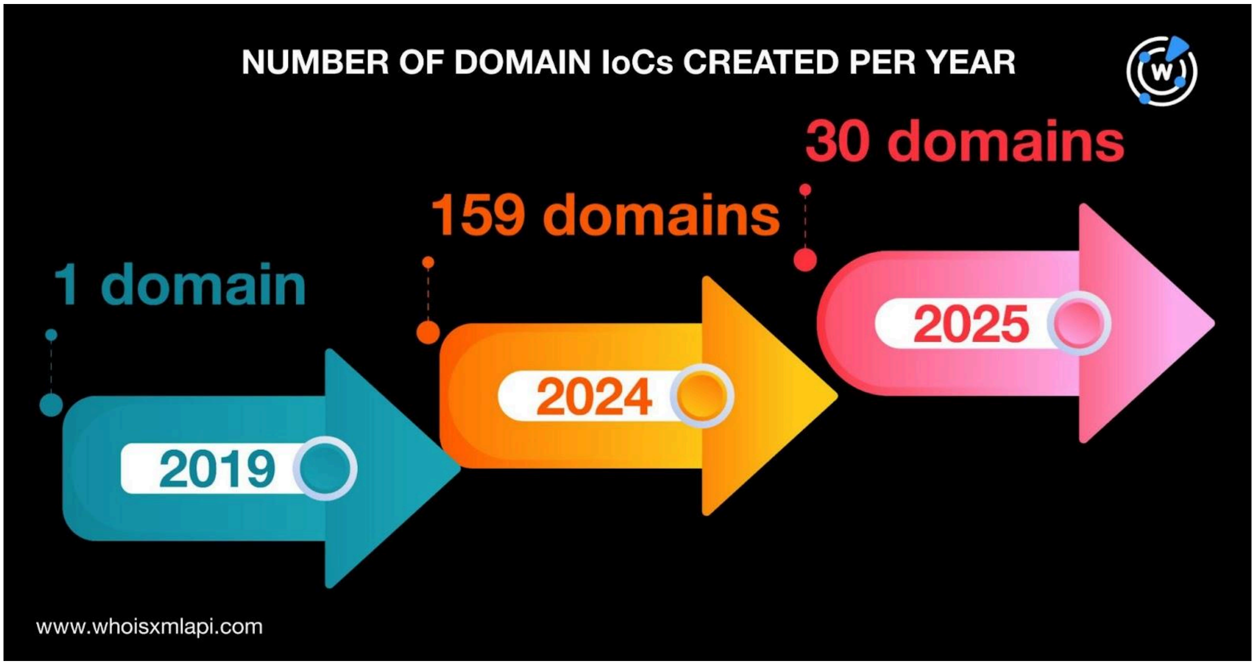
The security researchers identified 428 URLs as indicators of compromise (IoCs) that we extracted 197 unique domains from. Our expansion analysis of the 197 domains tagged as IoCs led to the discovery of:

- 145 email-connected domains, two of which were malicious
- 109 IP addresses
- 11 IP-connected domains
- 359 string-connected domains

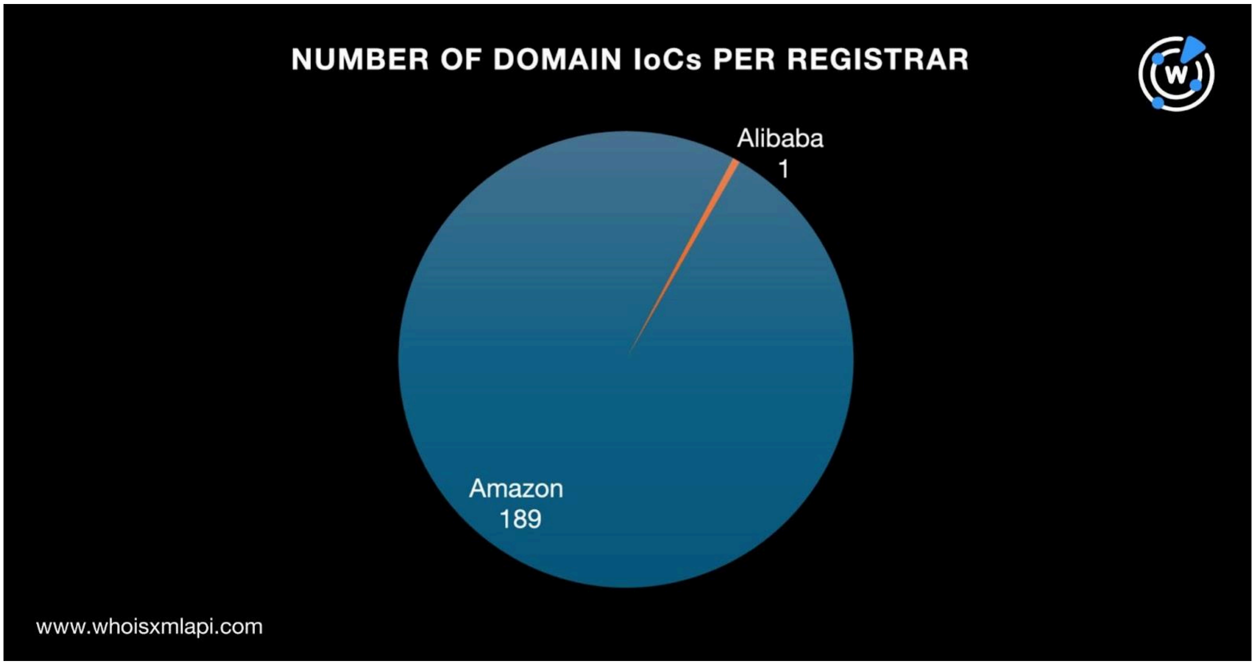
A Closer Look at the IoCs

We sought to find more information about the IoCs before diving into their DNS connections starting with a Bulk WHOIS API query for the 197 domains. We found that only 190 domains had current WHOIS records.

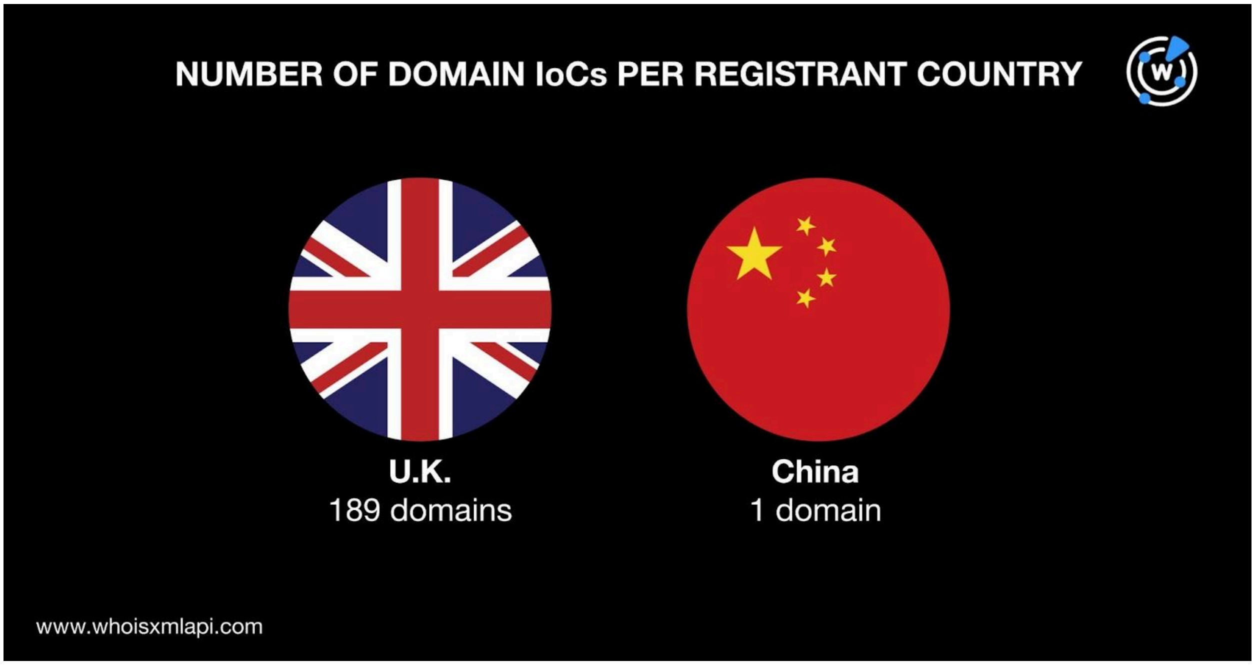
- The 190 domains were created between 2019 and 2025. Specifically, one domain was created in 2019, 159 in 2024, and 30 in 2025.



- The domains were administered by two registrars led by Amazon, which accounted for 189 domains. Alibaba administered one.



- The domains were registered in two countries led by the U.K., which accounted for 189 domains. One domain was registered in China.



We then queried the 197 domains identified as IoCs on DNS Chronicle API and discovered that 52 had historical domain-to-IP resolutions. In particular, the 52 domains had 3,303 resolutions over time. The domain inkpadnote[.]com posted the oldest resolution to IP address 199[.]115[.]115[.]118 on 9 October 2019. Take a look at five other examples below.

DOMAIN IoC	NUMBER OF IP RESOLUTIONS	FIRST IP RESOLUTION DATE
aquatrackergo[.]com	40	27 October 2024
bloodpressuretrackerapp[.]net	48	20 November 2024
cozybp[.]com	28	22 October 2024
disate[.]com	67	25 November 2019
fesder[.]com	2	10 October 2019

IoC List Expansion Analysis Findings

To uncover additional threat artifacts, we examined the DNS traces that the 197 domains tagged as IoCs left.

First, we queried the 197 domains on WHOIS History API and found that 188 had email addresses in their historical WHOIS records. We unearthed 233 email addresses in all after duplicates were filtered out and, upon closer examination, discovered that 16 were public email addresses.

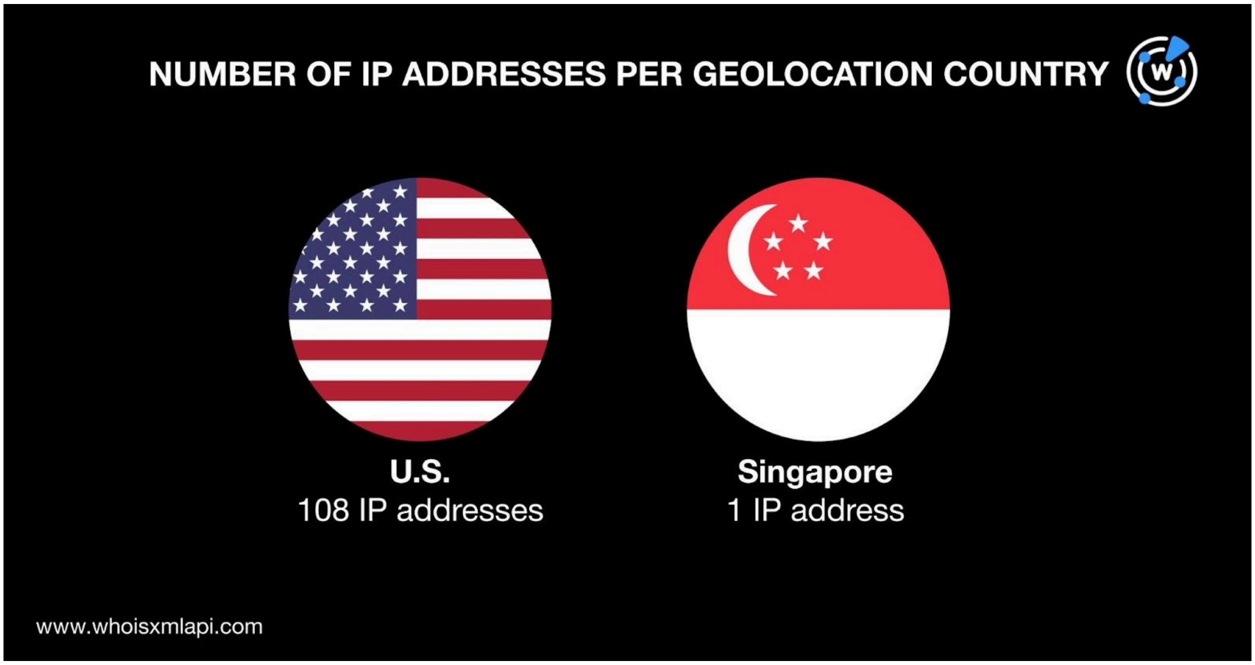
A Reverse WHOIS API query for the 16 public email addresses revealed that 13 appeared in the historical WHOIS records of other domains. All in all, the query led to the discovery of 145 email-connected domains after duplicates and those already identified as IoCs were filtered out.

We then queried the 145 email-connected domains on Threat Intelligence API and found that two have already figured in malicious campaigns. An example would be howtopickupgirlsontinder[.]com, which was attributed with malware distribution. Note, however, that the two malicious email-connected domains were offline as of this writing based on the results of our Screenshot API query earlier.

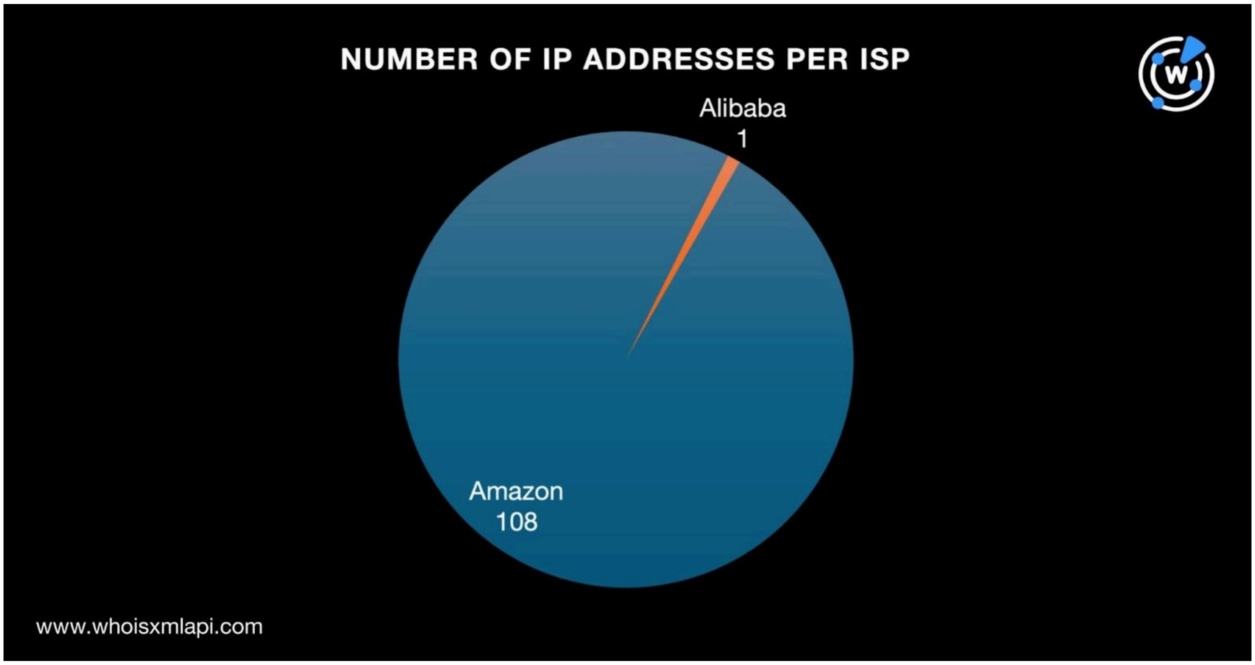
Next, we queried the 197 domains identified as IoCs on DNS Lookup API and discovered that 28 actively resolved to a total of 109 unique IP addresses.

A Bulk IP Geolocation Lookup for the 109 IP addresses showed that:

- They were split between two geolocation countries led by the U.S., which accounted for 108 IP addresses. One IP address was geolocated in Singapore.

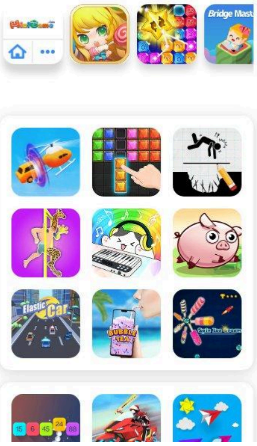


- Just like the IoCs, they were administered by two ISPs led by Amazon, which accounted for 108 IP addresses. One IP address was administered by Alibaba.

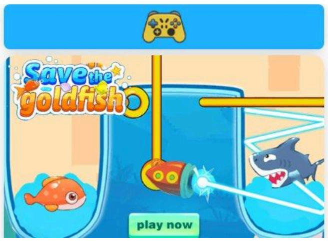


We also queried the 109 IP addresses on Reverse IP API and discovered that they all resolved to other domains. Upon closer examination, however, only one IP address could be a dedicated host. Specifically, the sole IP address hosted 11 IP-connected domains after duplicates, those already tagged as IoCs, and the email-connected domains were filtered out.

A Screenshot API query for the 11 IP-connected domains showed that all continued to host live content to this day. Take a look at two examples below.



Screenshot of IP-connected domain company[.]minigame[.]vip



Screenshot of IP-connected domain minigame[.]zone

Next, we took a closer look at the 197 domains identified as IoCs and found that they started with 196 unique text strings. We then performed Domains & Subdomains Discovery searches for the 196 text strings using the **Starts with** parameter and discovered that the 34 strings listed below appeared in other domains.

- auroralume.
- beautifuland.
- bloodpressuretrackerapp.
- bookanswers.
- btfdf.
- cardiapp.
- covboe.
- cutewallpaper.
- defea.
- dfcserwan.
- dilige.
- disate.
- drinksmart.
- fesder.
- minigame.
- moreagent.
- notenimbus.
- pennycharge.
- phmobi.
- photoah.
- robustdrink.
- scanblitz.
- scannertranslate.
- scribesphere.
- sigture.
- siphealth.
- spectrumnote.
- spritzy.
- terdpo.
- todaynote.
- vcdfcx.
- wallpapersave.
- wrdup.
- zoofv.

In total, we unearthed 359 string-connected domains that started with the 34 text strings above after duplicates, those already tagged as IoCs, and the email- and IP-connected domains were filtered out.

—

Our DNS deep dive into the 197 IoCs associated with the malicious Google Play apps led to the discovery of 624 connected threat artifacts comprising 145 email-connected domains, 109 IP addresses, 11 IP-connected domains, and 359 string-connected domains. We also discovered that so far, two of the artifacts we unearthed have already been weaponized for cyber attacks.

If you wish to learn more about the products used in this research, please don't hesitate to contact us.

Disclaimer: *We take a cautionary stance toward threat detection and aim to provide relevant information to help protect against potential dangers. Consequently, it is possible that some entities identified as "threats" or "malicious" may eventually be deemed harmless upon further investigation or changes in context. We strongly recommend conducting supplementary investigations to corroborate the information provided herein.*

Appendix: Sample Artifacts

Sample Email-Connected Domains

- 100legalfreemusicdownloads[.]com
- 808webhosting[.]com
- 96wallpaper[.]com
- abhinav[.]org
- alarmmonitoringservices[.]net
- alarmsystemsvancouver[.]net
- badcreditpersonalloanscanada[.]com
- badcreditpersonalloansusa[.]com
- bandtwins[.]com
- capdell[.]com
- capdell[.]org
- carleasetakeover[.]com
- dapeton[.]mobi
- datingcoachdirectory[.]com
- debtconsolidationloanscanada[.]com
- eliteadvising[.]com
- entrepreneurshipcoaches[.]com
- exploregadget[.]com
- forumcapdell[.]com
- freeipadwallpaper[.]com
- frontpointsecurityreview[.]com
- gayism[.]net
- globalvpnreviews[.]com
- gritnglory[.]us
- hitweet[.]com
- homesecurityalarm[.]systems
- homesecuritysystemsalabama[.]com
- in4ia[.]com
- in4ia[.]org
- indiacodes[.]com
- jaat[.]us
- javiermas[.]com
- keralawap[.]org
- keralwap[.]com
- killr[.]net
- latestproxysites[.]com
- lifestylesgreen[.]com
- livingarchinteriors[.]com
- manhoodlessons[.]com
- manulaosa[.]com
- marketingtrainingcourse[.]org
- nehu[.]org
- nylon[.]nyc
- nylon[.]tech
- onlinepaydayloanlenders[.]biz
- onlinetrainingcourses[.]biz
- ontariohairsalons[.]com
- pacocapdell[.]com
- pacocapdell[.]net
- phonesexoperators[.]net
- resourcesforadultfaith[.]com
- righthosts[.]com
- sarwagya[.]com
- securitycamerassystems[.]org
- shenlun[.]vip
- teachmeblog[.]com
- tecnologyworld[.]com
- temporaryemploymentagencies[.]net
- usecondom[.]org
- usemycomputer[.]org
- vancouvernightclubs[.]net
- vivolinks[.]com
- vpnselection[.]com
- wapday[.]net
- weboohost[.]com
- wheretomeetsingles[.]com
- youcookin[.]com
- zhongkaoshuxue[.]com

Sample IP-Connected Domains

- about[.]minigame[.]vip
- company[.]minigame[.]vip
- merge-number-puzzle[.]apps[.]minigame[.]com
- res[.]minigame[.]com
- sdk[.]minigame[.]com
- www[.]icplay[.]com

Sample String-Connected Domains

- auroralume[.]com
- auroralume[.]es
- auroralume[.]fr
- beautifuland[.]black
- beautifuland[.]com
- beautifuland[.]ga
- bloodpressuretrackerapp[.]com
- bookanswers[.]com
- bookanswers[.]org
- bookanswers[.]tk
- btfdf[.]loan
- btfdf[.]sbs
- btfdf[.]top
- cardiapp[.]cl
- cardiapp[.]co[.]uk
- cardiapp[.]com
- covboe[.]uk
- cutewallpaper[.]club
- cutewallpaper[.]co
- cutewallpaper[.]com
- defea[.]com
- defea[.]gr
- defea[.]hk
- dfcserwan[.]com
- dilige[.]cf
- dilige[.]com
- dilige[.]com[.]br
- disate[.]cf
- disate[.]cn
- disate[.]es
- drinksmart[.]app
- drinksmart[.]biz
- drinksmart[.]ca
- fesder[.]com[.]tr
- fesder[.]xyz
- minigame[.]ac[.]cn
- minigame[.]ai
- minigame[.]app
- moreagent[.]ai
- moreagent[.]com
- moreagent[.]xyz
- notenimbus[.]online
- pennycharge[.]com
- phmobi[.]com
- phmobi[.]tk
- phmobi[.]top
- photoah[.]co[.]uk
- photoah[.]ml
- photoah[.]ru
- robustdrink[.]com
- scanblitz[.]com
- scannertranslate[.]com
- scribesphere[.]ai
- scribesphere[.]com
- scribesphere[.]com[.]ng
- sigture[.]club
- siphealth[.]cn
- siphealth[.]com
- siphealth[.]in
- spectrumnote[.]loan
- spectrumnote[.]racing
- spectrumnote[.]science

- spritzy[.]au
- spritzy[.]be
- spritzy[.]biz
- terdpo[.]icu
- todaynote[.]co[.]kr
- todaynote[.]com
- todaynote[.]in
- vcdfcx[.]com
- wallpapersave[.]in
- wallpapersave[.]net
- wallpapersave[.]tk
- wrdup[.]co
- wrdup[.]co[.]nz
- wrdup[.]com
- zoofv[.]bid
- zoofv[.]icu
- zoofv[.]link