What Are the DNS Artifacts Associated with APT36 or Earth Karkaddan?

APT36 or Earth Karkaddan is an advanced persistent threat (APT) actor group targeting various government entities, most especially those based in India. The web properties they use for campaigns include only a few domains and IP addresses along with related malware hashes as indicators of compromise (IoCs).

Organizations that wish to block all possibly related domains, email addresses, and IP addresses may find it difficult. Tracking all those web assets down is tedious and time-consuming, not to mention likely impossible, for entities without dedicated cybersecurity teams or the resources to do so.

WhoisXML API researchers have attempted to uncover APT36's digital footprint in this study, which found:

- An unredacted domain registrant email address that led to the discovery of at least 10,000 possibly connected domains
- Two IP address resolutions that helped uncover another 599 domains that could be connected to the threat
- 69 of the potentially related domains dubbed "dangerous" by various malware engines

What Publicly Available Resources Have Told Us So Far

At least two of the published reports on APT36 or Earth Karkaddan (by Trend Micro and AlienVault) provided two domains and IP addresses each related to the threat. We used those malicious web properties as search terms for various WHOIS, IP, DNS, and other threat intelligence tools to get our more in-depth investigation going.

What You May Not Know about the Threat

We began by looking at the WHOIS records of the two domain IoCs. That led to the discovery of an unredacted domain registrant email address.

Using that email address as a reverse WHOIS search term uncovered at least 10,000 domains that could have ties to APT36 or Earth Karkaddan. These digital properties include:

- afropill[.]com
- elkmthomeschool[.]com
- golf-together[.]com
- hasil[.]net
- ivoryboards[.]com
- maternalfetalmed[.]com
- orphaleesmith[.]com
- selfhelpseo[.]com
- trustnews-24[.]com
- webmendi[.]com

A bulk malware check on Threat Intelligence Platform (TIP) revealed that 68 of these possibly connected domains are dubbed “dangerous” by various malware engines. Examples are:

- arbtimes[.]com
- databaseebook[.]com
- esotericworldnews[.]com
- facetbook[.]com
- help-2020[.]com
- indiaclassifiedonline[.]com
- lxnewstv[.]com
- mischiefmagazine[.]com
- officeproduces[.]com
- politicallimit[.]com

Note the usage of common search terms people at work may use. Employees searching for general news or information may unknowingly land on pages that host CapraRAT or Android RAT, the malware APT36 or Earth Kardakkan actors use to infiltrate their target networks. Those who mistype facebook[.]com or who wish to know more about Microsoft Office products can easily fall victim too.

Those were, however, not the only potentially connected artifacts we found. Subjecting the two domain IoCs to DNS lookups gave us their IP address resolutions—204[.]11[.]56[.]48 and 205[.]144[.]171[.]198. Using these as reverse IP search terms led us to discover an additional 599 possibly connected domains. Examples include:

- alephpublications[.]email

- booksthatmakeyouthink[.]com
- cancercentersupport[.]net
- doublep[.]com
- enews[.]iiaonline[.]in
- flight-jobs[.]net
- gladministracion[.]com[.]ar
- howtoreadthebiblebook[.]com
- icspakistan[.]com[.]pk
- jdholmes[.]net

While none of them are currently tagged “malicious,” the fact that they share the domain IoCs’ IP addresses means they are at least worth monitoring to ensure utmost security.

—

As this study showed, no IoC list is ever complete or as exhaustive as we may think. It’s always worth exerting extra effort to dig deeper into publicized IoCs because they can lead to the discovery of thousands or other web properties that could put your network at great risk of becoming the next APT36 or Earth Kardakkan victim in this case.

If you wish to perform a similar investigation, please don’t hesitate to contact us. We’re always on the lookout for potential research collaborations.

APPENDIX IOC and Artifacts Samples

2 domains and 2 IP addresses identified by Trend Micro and AlienVault as threat IoCs

DOMAINS	IP ADDRESSES
sharingmymedia[.]com	209[.]127[.]19[.]241
iiaonline[.]in	185[.]136[.]161[.]124

Sample from the 10,000 domains that shared a public registrant email address of sharingmymedia[.]com (one of the domain IoCs)

CONNECTED DOMAINS
maternalfetalmed[.]com
hasil[.]net
ivoryboards[.]com
integritygracehealth[.]com
metart[.]net
golf-together[.]com
selfhelpseo[.]com
trustnews-24[.]com
afropill[.]com
hashtaggadgets[.]com
shuttershackphoto[.]com
orphaleesmith[.]com
elkmthomeschool[.]com
webmendi[.]com
travel-gazette[.]com
leisuredivecanada[.]com
bioapplicant[.]com
viyo-elite[.]com
vocaloidp3[.]com
visithola[.]com
vintagemarketlist[.]com
win-women-networking[.]com
mycodepilot[.]com
worldjetinc[.]com

thepandapost[.]com
smartfundata[.]com
rexstatefarm[.]com
redc[.]net
yourownsunrise[.]com
nocost-forum[.]com
thedovesstudio[.]com
nationalhotelottawa[.]com
monarchwebwork[.]com
sletv[.]com
nodisponible[.]com
wrayvw[.]com
solarpoweryourworld[.]com
expandmymind[.]com
huntwebsite[.]com
mytopideas[.]com
live-broadcast-equipment[.]com
gallery-vip[.]com
fksdl[.]com
drfakhar[.]com
rapcity[.]com
129082[.]com
digitalengr[.]com
gftp[.]net
thesilverant[.]com
missiontreatment[.]com
androidfilmy[.]com
904849[.]com
followthetraveler[.]com
marshallautomation[.]com
raleighrealifestyle[.]com
wespank[.]net
propertybuzzonline[.]com
dresscleaner[.]com
renwoods[.]com
theclickhost[.]com
toner-skincare[.]com
space-cctv[.]com
reviewslaptop[.]com
respondedreports[.]com
sappmtraining[.]com
marchedugamer[.]com

komsomolskayapravda[.]com
therevelernyc[.]com
spicyeats[.]com
lilianasdrapes[.]com
muslimprisoners[.]com
sapindia[.]com
areyoupro[.]com
pineatix[.]com
miprimermundo[.]com
midtownkalamazoo[.]com
dentallord[.]com
instantcomputersolution[.]com
websellhosting[.]com
it1684[.]com
cocofist[.]com
sapcloudsoft[.]com
sydneymutual-bank[.]com
studenthubtv[.]com
teachertaban[.]com
oedysee[.]com
kidzpartyzonecoventry[.]com
tampatradebrokers[.]com
pinkcourtyard[.]com
okmsar[.]com
oneandonlyproducts[.]com
viaacost[.]com
universalboy[.]com
torealtor[.]com
titansparkplugs[.]com
pcsitx[.]com
orangecashcow[.]com
realbin-at[.]com
photolabtrading[.]com
politicallimit[.]com
petrolheadgurus[.]com
oldfortyfives[.]com
drunkenmonkbrewery[.]com
delivery-email[.]com
skyconstructionwa[.]com
japanese2018[.]com
inretailconsultants[.]com
mailmink[.]com

lorebeasts[.]com
kbcc[.]net
meetnewgadgets[.]com
mejobs99[.]com
cowboysex[.]com
fauke[.]com
aromacamp[.]com
aromaidea[.]com
areawidemarketplace[.]com
anointedfighternutrition[.]com
animeroompic[.]com
clear-viewpoint[.]com
addissquare[.]com
389367[.]com
389012[.]com
389375[.]com
portlens[.]net
newsfrompolitics[.]com
morethanaphotograph[.]com
condoslasvegasnv[.]com
marinelens[.]net
osteoarthritis-pain[.]com
lactails[.]com
wehostex[.]com
pretext[.]net
dadhour[.]com
banncor[.]com
animation-backgrounds[.]com
academiaconvexa[.]com
ihavemunchies[.]com
slackex[.]com
hugbots[.]com
gaithertech[.]com
finesttop100[.]com
emergenzanimali[.]com
intranet-pioneer[.]com
corona-virus-map[.]com
cjgarland[.]com
cheapbookingonline[.]com
guil[.]net
goyardus[.]com
bookcrm[.]com

benefitssoul[.]com
baylinefire[.]com
groupbuff[.]com
discountaffordablehomes[.]com
greencards4u[.]com
1simplehack[.]com
designmill[.]com
forabsentfriends[.]com
crisppros[.]com
clouddra[.]com
cochinfood[.]com
colhomes[.]com
butlerwick[.]com
blinqui[.]net
ewingcity[.]com
everyvpn[.]com
indonanospray[.]net
imarketingltd[.]com
7figureskier[.]com
louisep[.]com
2md[.]net
guestblast[.]com
200live[.]com
arhack[.]net
19thmile[.]com
hustleislandmail[.]com
earningmoneyuk[.]com
orgasmodamulher[.]net
myshareinvestment[.]com
8620399[.]com
becksbirdfeeders[.]com
inachinashop[.]com
articleonpad[.]com
uscoalinc[.]com
freeonlinegamesgames[.]com
lightmagazineafrica[.]com
homesuganda[.]com
queenport[.]com
loftypurpleray[.]com
greenspirehome[.]com
businessdirectorytampa[.]com
unorthodoxluv[.]com

pokyshop[.]com
newjurnal[.]com
ecellstreet[.]com
cultporn[.]com
a1digitalservices[.]com
topnotchdatingtips[.]com
dght[.]net
vamera-studio[.]com
dongshankeji[.]com
postpaidtravel[.]com
mostbet-az[.]com
worldtoptrending[.]com
tyfa[.]net
beautybooty411[.]com
adulttubemovies[.]com
bindasrent[.]com
techseaa[.]com
lucidboomer[.]com
sostencapri[.]com
planettancalifornia[.]com
herues[.]com
throughmagnifyingglass[.]com
worldpoliticsnow[.]com
cheapconsumer[.]com
lvhypnosis[.]com
bayasweets[.]com
pacificaerospacegroup[.]com
theathea[.]com
dignitythroughart[.]com
caaainfo[.]net
criterionassets[.]com
ampdiscount[.]com
airkingelectronics[.]com
discoverbeijingtours[.]com
dessertpin[.]com
clasysassynvrtrashy[.]com
campbulls[.]com
chargedgbh[.]com
diveca[.]com
christiangeology[.]com
aswolves[.]com
antiochichurch[.]com

aflfanzone[.]com
allgoodroads[.]com
alldelightedpeople[.]com
onetruereason[.]com
jobautocad[.]com
escedu[.]com
costahd[.]com
clinicadentalgirard[.]com
chinesegamesfree[.]com
alterbud[.]com
activetrader-links[.]com
shuunen[.]com
peliculasi[.]com
jokerfiles[.]com
elizabethlaprelle[.]com
byproof[.]com
boutiquecoupons[.]com
92topwin[.]com
barakavoice[.]com
2eyepickle[.]com
rigorousdevelopment[.]com
njpoppunk[.]com
mindyourmanna[.]com
memberat[.]com
messyprogress[.]com
megaconcerto[.]com
matchswift[.]com
malayachronicles[.]com
manhuavn[.]com
laviedetergents[.]com
humorisus[.]com
fullserialcrack[.]com
freshclicksmedia[.]com
furioustakedown[.]com
filipinosforlife[.]com
ecommercemasterycourses[.]com
82topwin[.]com
763255[.]com
2lionsllc[.]com
2012portal[.]com
17cube[.]com
anteldata[.]com

bluenoteevents[.]com
be-me-up[.]com
digitalsigngraphics[.]com
ashbath[.]com
adventureswithus[.]com
juvenews[.]net
hostingcros[.]net
gossiphotnews[.]com
galsdays[.]com
shift2inbound[.]com
pareabistro[.]com
pageindustrialinc[.]com
partystylebeads[.]com
northgatewebsolutions[.]com
newlifewv[.]com
nadirasworld[.]com
magweeks[.]com
mamogames[.]com
hiiiilog[.]com
hiphopcommunication[.]com
hostalsantamarta[.]com
healthylandethic[.]com
golatheme[.]com
elektrogame[.]com
britainplaces[.]com
bullhornnews[.]com
bosskeytrip[.]com
1000gtr[.]com
deliversto[.]com
nobs3d[.]com
hauntingnews[.]com
burstscam[.]com
bornwildoutdoors[.]com
bethlehemretreatcentre[.]com
986185[.]com
6791777[.]com
amusicalshoppe[.]com
amanaah[.]com
lovelifefamilytravels[.]com
lilwaynesite[.]com
interfig[.]com
iforan[.]com

ljkhlkjkljkljkljlkjklj[.]com
lincolnserviceparts[.]com
luggageshippers[.]com
learningfact[.]com
keycreativeworks[.]com
perathai[.]com
pussymeat[.]com
iptvvatan[.]com
usafreeclassifiedads[.]com
selimasfar[.]com
violetlashes[.]com
vaporsir[.]com
tropicalcocktails[.]com
supernetcargo[.]com
swipepet[.]com
strainedmuscle[.]com
sunflower-service[.]com
yyltz[.]com
solofulldvd[.]com
sheistheend[.]com
wheeledu[.]com
bet8001[.]com
makinglifemerry[.]com
mda-data[.]com
7lv5[.]com
desirablevillas[.]com
meetmust[.]com
misinformationclaims[.]com
leaguerehabilitation[.]com
koponyab[.]com
ladycyber[.]com
japanesesushifood[.]com
hostpython[.]com
hqbullies[.]com
home-kitchen-appliances[.]com
by250[.]com
provorealestateagents[.]com
pricesspy[.]com
domainsreal[.]com
dolphinozoneate[.]com
ecoursepro[.]com
eagerhotel[.]com

529772[.]com
708081[.]com
722426[.]com
77pmpm[.]com
395418[.]com
181040[.]com
213998[.]com
impane[.]com
ittybittymedia[.]com
inwelcomes[.]com
getithost[.]com
fansubfoda[.]com
enetwebsolutions[.]com
outstore[.]net
realchat[.]net
photodelusions[.]com
pears-project[.]com
philly-guild[.]com
pdatad[.]com
urbanolive[.]net
locusbayblog[.]com
mobilemediaminds[.]com
groundfl[.]com
corporaciongrvpoterra[.]com
alasifur[.]com
pen-tool[.]com
styleandform[.]com
tiresarena[.]com
socialims[.]com
jillianolita[.]com
thecorporationinc[.]com
zine6[.]com
7decorideas[.]com
thepeppar[.]com
gsbsportsconference[.]com
daythreesoftware[.]com
jackmedialondon[.]com
ais-tech[.]com
miramelapolla[.]com
grabrightnews[.]com
zooperstar[.]com
stayonpoker[.]com

readlongform[.]com
themainengine[.]com
todomay[.]com
washingtonethical[.]com
treasurechestgiftshop[.]com
shopsolonfirst[.]com
shoppersbill[.]com
rusexvids[.]com
robustdiet[.]com
robothangari[.]com
reviewofthis[.]com
parscove[.]com
judgewhite[.]com
coolmetier[.]com
purlan[.]com
videokeralam[.]com
thursdaysfortlauderdale[.]com
orangedotinc[.]com
oppositeleaks[.]com
thehauntingfilm[.]com
cat-friends[.]com
toner10[.]com
qstat[.]net
airblock[.]net
birthdayclubtime[.]com
capitalvillageproperties[.]com
badcondos[.]com
087918[.]com
070714[.]com
109349[.]com
mymindit[.]com
incoginvestigator[.]com
21doctor[.]com
177store[.]com
youihome[.]com
wholenessintherapy[.]com
whitecountertops[.]com
sunnydaynow[.]com
garofaloobgyn[.]com
vinfriends[.]com
fyss[.]net
070644[.]com

mmotales[.]com
tutorfrog[.]com
watchingheroes[.]com
first2die[.]com
fitnessorange[.]com
dictionnairedesreves[.]com
dicle-fm[.]com
twinsoup[.]com
usadailytime[.]com
pupsquest[.]com
fancypix[.]com
easyinternetdeals[.]com
ryanfamilyamusements[.]com
pullionflooring[.]com
rihosts[.]com
listmamablog[.]com
i37raceway[.]com
goldmovs[.]com
tech-tickets[.]com
traveltracker[.]net
topguncostume[.]com
smart-button[.]com
sommersonntag[.]com
soscome[.]com
erizn[.]com
sonnolenta[.]com
greenethanolfireplaces[.]com
gistmee[.]com
hungtang[.]com
gettysburgstuff[.]com
gladesauction[.]com
goblackamerica[.]com
edu-cons[.]com
debbiecastillo[.]com
decaturfirstbank[.]com
smokingface[.]com
timgrubu[.]com
rvdealerlinks[.]com
knownproduct[.]com
jerkyfarm[.]com
adderconsulting[.]com
abluftanlage[.]com

abhiwebs[.]com
546235[.]com
oceanographyrace[.]com
nova4x4projects[.]com
contentwritingseo[.]com
craftsunrise[.]com
cqza[.]net
videoseogo[.]com
kokuyou[.]com
superblogseo[.]com
magmablog[.]com
wickedpaint[.]net
ehbl[.]net
beargay[.]net

END OF SAMPLE

2 IP addresses that the domain IoCs resolved to

DOMAINS	IP ADDRESSES
sharingmymedia[.]com	204[.]11[.]56[.]48
iiaonline[.]in	205[.]144[.]171[.]198

Sample from the 599 domains that shared the IP hosts of the domain IoCs

DOMAINS
0-0-kz-ehr[.]yogamonkeyfitness[.]com
0-0[.]info
0-03-seconds[.]iapps4you[.]com
0-100edu[.]com
0-24life[.]com
0-afternic-e2e[.]org
0-foods[.]com
0-nachalnik[.]xelpost[.]com
0-nachalnik[.]yogamonkeyfitness[.]com
0-nachalnik[.]youflexing[.]com
0-rublejj-porno[.]xelpost[.]com
0-rublejj-porno[.]yogamonkeyfitness[.]com

0-rublejj-porno[.]youflexing[.]com
0-vision[.]com
0[.]0-127[.]57[.]39[.]24[.]in-addr[.]arpa
0[.]0-255[.]157[.]51[.]204[.]in-addr[.]arpa
0[.]0-255[.]180[.]204[.]173[.]in-addr[.]arpa
0[.]0-255[.]203[.]51[.]204[.]in-addr[.]arpa
0[.]0-255[.]215[.]51[.]204[.]in-addr[.]arpa
0[.]0-27[.]250[.]86[.]65[.]in-addr[.]arpa
0[.]0-31[.]51[.]112[.]65[.]in-addr[.]arpa
0[.]0[.]typehair[.]com
0[.]0234022491810393[.]anycastloop[.]com
0[.]041876[.]com
0[.]060758[.]com
0[.]0730s[.]com
0[.]10avs[.]com
0[.]112956[.]com
0[.]114196[.]com
0[.]118911265330887[.]anycastloop[.]com
0[.]11hehe[.]com
0[.]126705008112957[.]anycastloop[.]com
0[.]134349094407963[.]anycastloop[.]com
0[.]141837772707493[.]anycastloop[.]com
0[.]151826856100453[.]anycastloop[.]com
0[.]156428[.]com
0[.]162748[.]com
0[.]164748[.]com
0[.]165148[.]com
0[.]165748[.]com
0[.]170277737215038[.]anycastloop[.]com
0[.]173548[.]com
0[.]191280687384133[.]anycastloop[.]com
0[.]19405042394035[.]anycastloop[.]com
0[.]203497328447252[.]anycastloop[.]com
0[.]204862646426772[.]anycastloop[.]com
0[.]212430240711619[.]anycastloop[.]com
0[.]226826244300344[.]anycastloop[.]com
0[.]229891440005325[.]anycastloop[.]com
0[.]260343393731656[.]anycastloop[.]com
0[.]267351[.]com
0[.]267899239002411[.]anycastloop[.]com
0[.]271788756809102[.]anycastloop[.]com
0[.]291927605711852[.]anycastloop[.]com

0[.]292862159093151[.]anycastloop[.]com
0[.]2sectionlogistics[.]com
0[.]330502[.]com
0[.]34642121524568[.]anycastloop[.]com
0[.]350614874122058[.]anycastloop[.]com
0[.]375186[.]com
0[.]393895095178976[.]anycastloop[.]com
0[.]395893973588972[.]anycastloop[.]com
0[.]403677378830938[.]anycastloop[.]com
0[.]429971514642816[.]anycastloop[.]com
0[.]444828844534666[.]anycastloop[.]com
0[.]447815[.]com
0[.]460439771137167[.]anycastloop[.]com
0[.]48753667171674[.]anycastloop[.]com
0[.]48ddd[.]com
0[.]491695093311719[.]anycastloop[.]com
0[.]5002688[.]com
0[.]51field[.]com
0[.]52106213383761[.]anycastloop[.]com
0[.]560930[.]com
0[.]561514975890482[.]anycastloop[.]com
0[.]571578543049359[.]anycastloop[.]com
0[.]600078160620559[.]anycastloop[.]com
0[.]663077137562702[.]anycastloop[.]com
0[.]66hehe[.]com
0[.]687115433030826[.]anycastloop[.]com
0[.]690140875585765[.]anycastloop[.]com
0[.]702077148011384[.]anycastloop[.]com
0[.]702907[.]com
0[.]756962449922497[.]anycastloop[.]com
0[.]758582[.]0[.]758582[.]com
0[.]758582[.]com
0[.]765821238967344[.]anycastloop[.]com
0[.]769185065790175[.]anycastloop[.]com
0[.]773914028167479[.]anycastloop[.]com
0[.]7mangas[.]com
0[.]80[.]64[.]62[.]tnps[.]net
0[.]812215221430304[.]anycastloop[.]com
0[.]816781[.]0[.]816781[.]com
0[.]816781[.]com
0[.]820168[.]com
0[.]820886[.]com

0[.]830258[.]com
0[.]831366206899922[.]anycastloop[.]com
0[.]842078[.]com
0[.]863348[.]com

END OF SAMPLE

Sample from the 69 connected domains dubbed "dangerous" by various malware engines

CONNECTED DOMAINS
2069brackets[.]com
22-4[.]com
3d-list[.]com
allfilesfree[.]com
americaentry[.]com
arbtimes[.]com
arbtoon[.]com
awarfaregaming[.]com
baliplantation[.]com
bitsgroove[.]com
bmcary[.]com
boost-my-game[.]com
cabe2beca[.]com
dapengcnc[.]com
databaseebook[.]com
debugdatalab[.]com
drunkenmonkbrewery[.]com
esotericworldnews[.]com
facetbook[.]com
firemanstream[.]com

END OF SAMPLE