# DNS Snooping on Apple iOS 14 Zero-Click Spyware KingsPawn

## Table of Contents



## Executive Report

Last year, several governments reportedly used the NSO Group's spyware Pegasus to exploit a zero-day vulnerability in WhatsApp to spy on journalists, opposition politicians, and dissidents via their mobile devices. Apple quickly addressed the issue by launching more powerful data protection features.

This April, another zero-click spyware maker QuaDream surfaced in relation to ongoing espionage campaigns targeting anyone who owns an iOS device running iOS 14. The threat group's spyware dubbed "KingsPawn" exploits a zero-day vulnerability in the Calendar app.

Microsoft published an in-depth analysis of KingsPawn where they named 164 domains as indicators of compromise (IoCs). We added the string ***com.apple*** from the file and folder host names cited in the research. We then expanded the existing IoC list by identifying other possibly connected web properties through DNS connections, including:

- 19 IP addresses to which the IoCs resolved, 17 of which turned out to be malicious
- 2,101 additional domains that shared the IoCs' IP hosts, 11 of which turned out to be malware hosts
- 1,066 subdomains that contained the string ***com.apple***, 18 of which have been categorized as malicious

### KingsPawn IoC Facts

Despite being identified as KingsPawn IoCs, 40 of the domains Microsoft listed in their report weren't currently being detected as malicious. Half of them are:

- thetimespress[.]com
- thepila[.]com
- thenewsfill[.]com
- thegreenlight[.]xyz

- studyreaserch[.]com
- study-search[.]com
- studiesutshifts[.]com
- stockstiming[.]org
- stayle[.]co
- reloadyourbrowser[.]info
- redanddred[.]com
- novinite[.]biz
- nordmanetime[.]com
- newz-globe[.]com
- fosterunch[.]com
- ecologitics[.]com
- climatestews[.]com
- globepayinfo[.]com
- job4uhunt[.]com
- ctbgameson[.]com

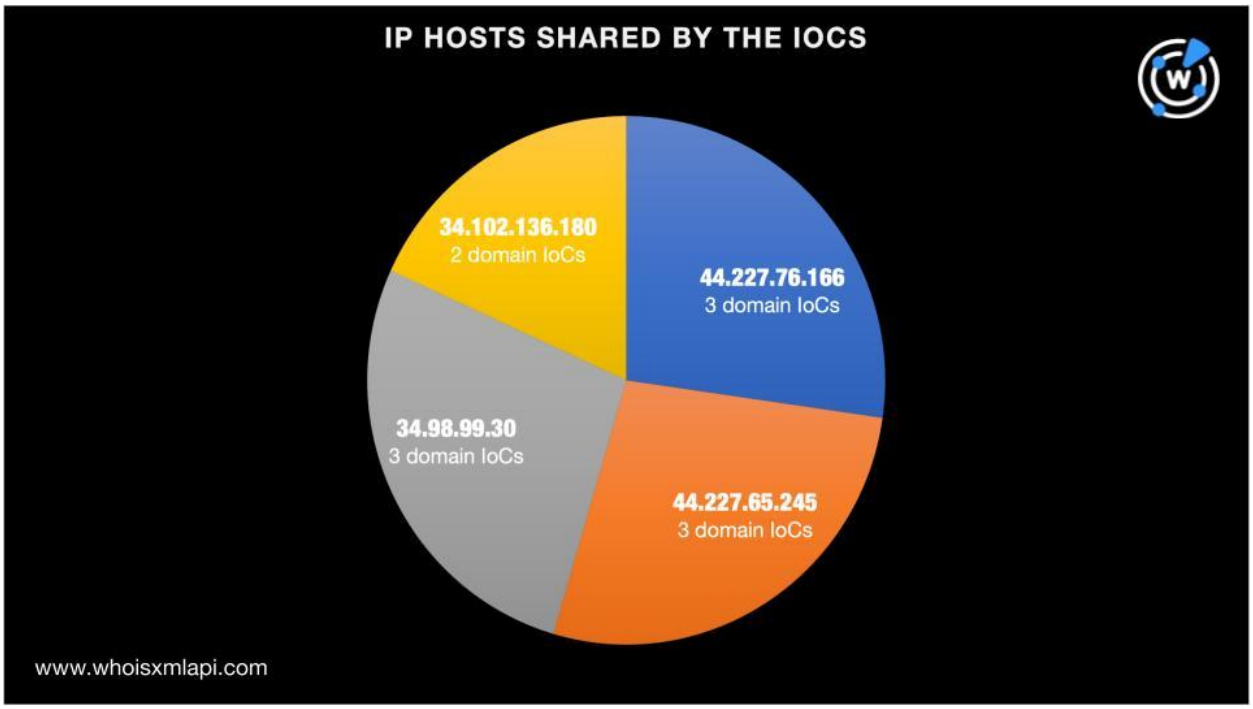
Of the 40 domains listed, 36 appeared to be unreachable. The remaining four IoCs are currently up for sale based on our screenshot lookups.

A bulk WHOIS lookup for the IoCs revealed they were created between 4 January 2022 and 3 April 2023, about 10 days before news about the KingsPawn attack broke. The 149 domains that had retrievable WHOIS records were spread across six registrars. Porkbun accounted for 78 of the web properties, followed by GoDaddy with 67 domains. 1API GmbH, Netim, Sav.com, and Xin Net Technology Corp., meanwhile, were responsible for one IoC each.

## KingsPawn IoC List Expansion Findings

To identify other KingsPawn-related artifacts, we subjected the IoCs to DNS lookups, which gave us 19 resolving IP addresses scattered across four countries led by the U.S. (16 IP addresses). The remaining three nations—France, Germany, and Switzerland—accounted for one IP address each. A bulk malware check for the IP hosts revealed that 11 of them were malicious.

Four of the IP hosts were each shared by a number of domains. 34[.]102[.]136[.]180, for instance, hosted nordmanetime[.]com and hotalsextra[.]com while 44[.]227[.]76[.]166 played host to zeebefg[.]com, topuprr[.]com, and koraliowe[.]com.




We then looked for domains hosted on the resolving IP addresses. Our reverse IP lookups uncovered 2,101 domains, 11 of which turned out to be malware hosts. Only one of them was up for sale while the remaining 10 were parked.

Microsoft's KingsPawn study also identified three host-based IoCs, namely:

- private/var/db/com[.]apple[.]xpc[.]roleaccountd[.]staging/subridged
- com[.]apple[.]avcapture
- /private/var/db/com[.]apple[.]xpc[.]roleaccountd[.]staging/PlugIns/fud[.]appex/

All three IoCs contained the string ***com.apple***, which we then used to search for potentially connected subdomains on Domains & Subdomains Discovery. Our inquiry led to the discovery of 1,066 such web properties.

While 421 of the subdomains contained Apple's legitimate domain name ***apple.com***, manual scrutiny of each showed none were likely owned by the company. Also, 19 of them, now unreachable, turned out to be malware hosts.

The string-connected subdomains fell under the five domains in the following table.

| DOMAIN | NUMBER OF MALICIOUS SUBDOMAINS |
|---|---|

| | |
|---|---|
| kinderramadan[.]com | 10 |
| ios-confirm[.]net | 3 |
| a-inc[.]tk | 2 |
| bijuprabhakar[.]com | 2 |
| tondi-asu[.]com | 1 |

Also, besides the legitimate Apple domain, other popular strings typically connected to the company and its products also appeared as strings in the subdomains. The string ***appleid*** and its variations, including those with typos, ***apple-id***, ***apple.id***, ***appleId***, and ***id-apple***, appeared most (442 subdomains). The string ***icloud***, meanwhile, was present in 131 subdomains. Capping the top 3 was ***appstore*** and its variation ***applestore***, which could be found in 31 subdomains. The nine remaining strings we observed were:

- ***applemusic***
- ***applecare*** or ***apple.care***
- ***findmy*** or ***find-my***
- ***iphone***
- ***ios***
- ***appletv*** or ***apple-tv***
- ***itunes*** or ***etunes***
- ***finder***
- ***siri***

Note, though, that some of the subdomains contained more than one of the Apple-specific strings above. Examples include icloud[.]com[.]apple[.]applecare-support[.]us, icloud[.]com[.]apple[.]id-identify[.]us, and icloud[.]com[.]apple[.]findmylphone[.]top.

—

Our IoC expansion analysis revealed that more than 3,000 domains and subdomains containing Apple's company, product, and service names already exist in the DNS. They could serve as hosts to zero-click spyware like KingsPawn.

***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

## KingsPawn IoCs Microsoft Identified

- zooloow[.]com
- zeebefg[.]com

- zedforme[.]com
- zebra-arts[.]com
- youristores[.]com
- womnbling[.]com
- wombatcash[.]com
- wildhour[.]store
- wilddog[.]site
- wikipedoptions[.]com
- whiteandpiink[.]com
- white-rhino[.]online
- wellnessjane[.]org
- vinoneros[.]com
- unitedyears[.]com
- treerroots[.]com
- transformaition[.]com
- topuprr[.]com
- tokenberries[.]com
- timeeforsports[.]com
- thetimespress[.]com
- thepila[.]com
- thenewsfill[.]com
- thegreenlight[.]xyz
- techpowerlight[.]com
- teachlearning[.]org
- takestox[.]com
- takebreak[.]io
- sunsandlights[.]com
- sunnyweek[.]site
- sunclub[.]site
- subcloud[.]online
- stylelifees[.]com
- styleanature[.]com
- studysliii[.]com
- studyshifts[.]com
- studyreaserch[.]com
- study-search[.]com
- studiesutshifts[.]com
- stockstiming[.]org
- stayle[.]co
- sseamb[.]com
- space-moon[.]com
- skyphotogreen[.]com
- sidelot[.]org
- shoppingeos[.]com
- shoplifys[.]com
- shoeszise[.]xyz
- sevensdfe[.]com
- setclass[.]live
- runningandbeyond[.]org
- retailmark[.]net
- rentalproct[.]com
- reloadyourbrowser[.]info
- redanddred[.]com
- recovery-plan[.]org
- recover-your-body[.]xyz
- razzodev[.]com
- projectoid[.]org
- powercodings[.]com
- playozas[.]com
- planningly[.]org
- planetosgame[.]com
- pennywines[.]com
- pachadesert[.]com
- nutureheus[.]com
- novinite[.]biz
- nordmanetime[.]com
- noraplant[.]com
- newz-globe[.]com
- fosterunch[.]com
- choccoline[.]com
- lateparties[.]com
- foundurycolletive[.]com
- jungelfruitime[.]com
- gameboysess[.]com
- healthcovid19[.]com
- codingstudies[.]com
- hoteluxurysm[.]com
- hotalsextra[.]com
- fullaniimal[.]com
- agronomsdoc[.]com

- eccocredit[.]com
- ecologitics[.]com
- climatestews[.]com
- aqualizas[.]com
- bgnews-bg[.]com
- mikontravels[.]com
- e-gaming[.]online
- betterstime[.]com
- goshopeerz[.]com
- countshops[.]com
- inneture[.]com
- mwww[.]ro
- bcarental[.]com
- kikocruize[.]com
- elvacream[.]com
- globepayinfo[.]com
- job4uhunt[.]com
- ctbgameson[.]com
- adeptary[.]com
- hinterfy[.]com
- biznomex[.]com
- careerhub4u[.]com
- furiamoc[.]com
- motorgamings[.]com
- aniarchit[.]com
- datacentertime[.]com
- kidzlande[.]com
- homelosite[.]com
- londonistory[.]com
- bestteamlife[.]com
- newsandlocalupdates[.]com
- gardenearthis[.]com
- fullstorelife[.]com
- incollegely[.]org
- codinerom[.]com
- gamingcolonys[.]com
- kidzalnd[.]org
- garilc[.]com
- fullmoongreyparty[.]org
- greenrunners[.]org
- gamezess[.]com
- luxario[.]org
- i-reality[.]online
- kidsfunland[.]org
- localtallk[.]store
- allplaces[.]online
- meehealth[.]org
- gameizes[.]com
- foodyplates[.]com
- designaroo[.]org
- designspacing[.]org
- hoteliqo[.]com
- deliverystorz[.]com
- forestaaa[.]com
- addictmetui[.]com
- earthyouwantiis[.]com
- navadatime[.]com
- careers4ad[.]com
- dressuse[.]com
- iwoodstor[.]xyz
- monvesting[.]com
- elektrozi[.]com
- hopsite[.]online
- bikersrental[.]com
- naturemeter[.]org
- goodsforuw[.]com
- eedloversra[.]online
- dsudro[.]com
- comeandpet[.]me
- brushyourteeth[.]online
- digital-mar[.]com
- homeigardens[.]com
- koraliowe[.]com
- newsbuiltin[.]online
- jyfa[.]xyz
- gosport24[.]com
- classiccolor[.]live
- cleanitgo[.]info
- enrollering[.]com
- newslocalupdates[.]com

- beendos[.]com
- linestrip[.]online

## Sample IoC IP Resolutions

- 185[.]101[.]158[.]113
- 185[.]26[.]105[.]244
- 198[.]58[.]118[.]167
- 3[.]64[.]163[.]50
- 34[.]102[.]136[.]180
- 34[.]98[.]99[.]30
- 44[.]227[.]65[.]245
- 44[.]227[.]76[.]166
- 45[.]56[.]79[.]23

## Sample Malicious IP Hosts

- 198[.]58[.]118[.]167
- 3[.]64[.]163[.]50
- 34[.]102[.]136[.]180
- 34[.]98[.]99[.]30
- 44[.]227[.]65[.]245
- 44[.]227[.]76[.]166
- 45[.]56[.]79[.]23
- 96[.]126[.]123[.]244
- 45[.]33[.]2[.]79

## Sample Domains That Shared the IoCs' IP Hosts

- 0--0[.]work
- 0--4[.]n4t[.]co
- 0-0-1pickle[.]com
- 0-0-2[.]club
- 0-0-2[.]online
- 0-0-2pickleball[.]com
- 0-0-serve[.]com
- 0-0-serve[.]net
- 0-0[.]academy
- 0-0[.]agency
- 1-4-all-4-1[.]ch
- 1-4-all-4-1[.]com
- 1-4-all-4-1[.]li
- 1-bank[.]ch
- 1-portal[.]ch
- 1-z[.]eu
- 1[.]mw
- 10-e-lotto[.]it
- 10[.]pm
- 100000349218345[.]paketzoll[.]de
- 2-2[.]eu
- 2-4-you[.]ch
- 2-for-t[.]com
- 2-m[.]eu
- 2-rad-zurich[.]ch
- 2[.]ie
- 2[.]mw
- 2[.]vg
- 20001214[.]xyz
- 200shopsin2025[.]africa
- 3-cloud[.]com
- 3-coins[.]com
- 3-coins[.]eu
- 3-rad-fahrzeug[.]ch
- 3-rad-fahrzeuge[.]ch
- 3-rad-vanderhall[.]ch
- 3-radfahrzeug-mieten[.]ch
- 3-radfahrzeuge[.]ch
- 3-wheeler-vanderhall[.]ch
- 3[.]ar
- 4-4-2[.]at
- 4-4-2[.]ch
- 4-4-2[.]de
- 4-4-2[.]eu

- 4-4-2[.]net
- 4-crypto[.]info
- 4-crypto[.]me
- 4-crypto[.]org
- 4-neid[.]eu
- 4-pfoten-dorfladen[.]ch
- 4wellenlaengenlaser[.]ch
- 4wellenlaengenlaser[.]com
- 4wellenlaengenlaser[.]de
- 4x[.]at
- 50w[.]ch
- 53-racing-team[.]ch
- 5303[.]ch
- 5304[.]ch
- 5408[.]ch
- 5415[.]ch
- 0-0[.]art
- 0-0[.]biz
- 0-0[.]buzz
- 0-0[.]bz
- 0-0[.]dev
- 0-0[.]host
- 0-0[.]studio
- 0-0[.]wine
- 0-08[.]example[.]com[.]exampl[.]com
- 0-09[.]example[.]com[.]exampl[.]com
- 0-096[.]com
- 0-0alc[.]com
- 0-0asia[.]com
- 0-0domain[.]com
- 0-0s[.]com
- 0-0start[.]com
- 0-0startpickleball[.]com
- 0-1-2-3-4-5-6-7-8-9-10[.]com
- 0-1[.]digital
- 0-1[.]nl
- 0-1[.]rocks
- 0-10[.]in
- 0-100[.]agency
- 0-100[.]in
- 0-100[.]xyz
- 0-100agency[.]com
- 0-100cars[.]com
- 0-100kcoach[.]com
- 0-100ksystem[.]com
- 0-100mph[.]com
- 0-100nft[.]com
- 0-100realquick[.]com
- 0-100subs[.]com
- 0-104[.]com
- 0-106[.]com
- 0-108-62-208-15[.]example[.]com[.]exampl[.]com
- 0-10k[.]co[.]uk
- 0-10k[.]com
- 0-10vdimmer[.]com
- 0-1219[.]com

## Sample Malicious IP-Connected Domains

- 0-o[.]club
- 000[.]network
- 0000[.]mx
- 0000000[.]xyz
- 0000048[.]com
- 00003692[.]xyz

## Sample Subdomains That Contained the String *com.apple*

- com[.]apple[.]driver[.]app
- com[.]apple[.]developer[.]ga
- com[.]apple[.]smb[.]se
- com[.]apple[.]home[.]group
- com[.]apple[.]fallguys-movie[.]net
- com[.]apple[.]fallguystwo[.]com

- com[.]apple[.]ferrerorondnoir[.]ch
- com[.]apple[.]pralinkyferrero[.]cz
- com[.]apple[.]mobilesms[.]com
- com[.]apple[.]fallguys2[.]com
- com[.]apple[.]nutellasnack[.]com[.]pl
- com[.]apple[.]kindercrazyfriends[.]com[.]pl
- com[.]apple[.]fallguysuniverse[.]com
- com[.]apple[.]appleid[.]co
- com[.]apple[.]nke[.]app
- com[.]apple[.]kindermilchschnitte[.]ch
- com[.]apple[.]kinderjoyzabawanacalego[.]eu
- com[.]apple[.]info-fmi[.]com
- com[.]apple[.]kpi[.]io
- com[.]apple[.]ios-confirm[.]net
- com[.]apple[.]services[.]fr
- com[.]apple[.]fallguysmania[.]com
- com[.]apple[.]private[.]audio
- com[.]apple[.]finhealth[.]fi
- com[.]apple[.]witajszkolonawesolo[.]net
- com[.]apple[.]8x8[.]uk
- com[.]apple[.]fallguysultimateknockout[.]net
- com[.]apple[.]preferences[.]in
- com[.]apple[.]power[.]la
- com[.]apple[.]dictionary[.]es
- com[.]apple[.]hydra[.]report
- com[.]apple[.]kinderbuenowhite[.]info
- com[.]apple[.]witaj-szkolo-na-wesolo[.]info
- com[.]apple[.]dictionary[.]fr
- com[.]apple[.]dz92d[.]com
- com[.]apple[.]news[.]link
- com[.]apple[.]nutella-biscuit[.]sk
- com[.]apple[.]fallguysmobile[.]com
- com[.]apple[.]kinderfriends[.]pl
- com[.]apple[.]xn--wesoypocztekszkoy-x7b76ina[.]com
- com[.]apple[.]fallguysbattle[.]com
- com[.]apple[.]kinderbuenowhite[.]com[.]pl
- com[.]apple[.]fallguys2d[.]com
- com[.]apple[.]fallguys[.]biz
- com[.]apple[.]kinderschokobons[.]com[.]pl
- com[.]apple[.]hydra[.]money
- com[.]apple[.]finder[.]plus
- com[.]apple[.]alisports[.]com
- com[.]apple[.]irregularcorporation[.]com
- com[.]apple[.]fallguysmusic[.]com
- com[.]apple[.]gamail[.]com
- com[.]apple[.]etunes[.]it
- com[.]apple[.]translate[.]ca
- com[.]apple[.]downloadfallguys[.]com
- com[.]apple[.]hydra[.]supply
- com[.]apple[.]pralinkiferrero[.]com
- com[.]apple[.]framework[.]co
- com[.]apple[.]stocks[.]help
- com[.]apple[.]withthegrid[.]com
- com[.]apple[.]fallguysrace[.]net
- com[.]apple[.]rocketpass[.]com
- com[.]apple[.]as[.]me
- com[.]apple[.]pkcs[.]store
- com[.]apple[.]fallguys-mobile[.]com
- com[.]apple[.]fallguys-shop[.]com
- com[.]apple[.]tips[.]tips
- com[.]apple[.]assistant[.]co
- com[.]apple[.]webkit[.]in
- com[.]apple[.]widget[.]com[.]apple[.]maps[.]ge
- com[.]applet[.]3d[.]com
- com[.]apple9[.]qirina[.]com
- rucom[.]apple[.]dt[.]do
- com[.]appleid[.]fallguystwo[.]com

- com[.]appleid[.]page-signin[.]top
- com[.]appleid[.]fallguys-show[.]com
- com[.]appleid[.]irregularcorporation[.]com
- com[.]appleid[.]kinderjoyroadshow[.]pl
- com[.]appleid[.]roadshowzabawanacalego[.]com
- com[.]apple-id[.]rocketpass[.]com
- com[.]apple-id[.]roadshowcrazyfriends[.]eu
- com[.]apple-id[.]fallguys-shop[.]com
- com[.]apple-id[.]downloadfallguys[.]com
- com[.]apple-id[.]fallguysultimateknockout[.]com
- com[.]apple[.]id[.]fallguysrace[.]net
- com[.]apple-id[.]propojse[.]cz
- com[.]apple-id[.]fallguys2[.]com
- ss[.]com[.]apple[.]driver[.]app
- com[.]apple-id[.]kinderdelice[.]ch
- com[.]appleton[.]listcrawler[.]com
- com[.]apple[.]id[.]fallguysultimateknockout[.]net
- com[.]apple-id[.]freshnow[.]org[.]pl
- www[.]com[.]apple[.]fallguys2[.]com
- www[.]com[.]apple[.]hydra[.]report
- www[.]com[.]apple[.]hydra[.]money
- www[.]com[.]apple[.]driver[.]app
- com[.]applejupp[.]qirina[.]com
- www[.]com[.]apple[.]finhealth[.]fi
- www[.]com[.]apple[.]nutellasnack[.]com[.]pl
- www[.]com[.]apple[.]kinderparadiso[.]sk
- www[.]com[.]apple[.]assistant[.]co

## Sample Malicious *com.apple*-Containing Subdomains

- com[.]apple[.]ios-confirm[.]net
- com[.]apple[.]ns95[.]kinderramadan[.]com
- apple[.]com[.]appleid[.]tondi-asu[.]com
- www[.]apple[.]com[.]apple[.]ns12[.]kinderramadan[.]com
- www[.]apple[.]com[.]apple[.]ns123[.]kinderramadan[.]com
- www[.]icloud[.]com[.]apple[.]ns21[.]kinderramadan[.]com
- www[.]icloud[.]com[.]apple[.]ns44[.]kinderramadan[.]com
- support[.]apple[.]com[.]apple-id[.]bijuprabhakar[.]com
- ca[.]appleid[.]mobile[.]com[.]apple[.]ios-confirm[.]net