iOS 14搭載のiPhoneを標的とするゼロクリックスパイウェア「KingsPawn」のDNSスヌーピング

目次

要旨

昨年、複数の国の政府がNSO GroupのスパイウェアPegasusを使ってWhatsAppのゼロデイ脆弱性を悪用し、ジャーナリスト、野党政治家および反体制派活動家をスパイしていたことが報じられました。この問題に対して、Appleはデータ保護機能を強化することで迅速に対処しました。

しかし、今年4月には、iOS 14搭載のiOSデバイスをターゲットにスパイ活動を行う別のゼロクリック・スパイウェアメーカー「QuaDream」が出現しました。このグループが作ったスパイウェアは「KingsPawn」と呼ばれ、カレンダーアプリのゼロデイ脆弱性を悪用します。

Microsoftが発表したKingsPawnの詳細な分析では、セキュリティ侵害インジケーター（IoC）として164個のドメイン名が挙げられました。当社は、その調査で引用されたファイルやフォルダのホスト名から***com.apple***という文字列をピックアップし、既存のIoCリストを拡張する形で、DNS情報からKingsPawnとの関連性が疑われる以下のウェブプロパティを新たに特定しました。

- IoCが名前解決した19個のIPアドレス。そのうち17個には悪意があることが判明
- IoCのIPホストを共用していた2,101個のドメイン名。うち11個はマルウェアホストと確認
- ***com.apple***という文字列を含む1,066個のサブドメイン。うち18個が悪意あるものと確認

KingsPawnのIoC

MicrosoftがKingsPawnのIoCとして挙げたドメイン名のうち40個については、現在のところ悪意が確認されていません。以下にその半分、20個のドメイン名を示します。

- 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

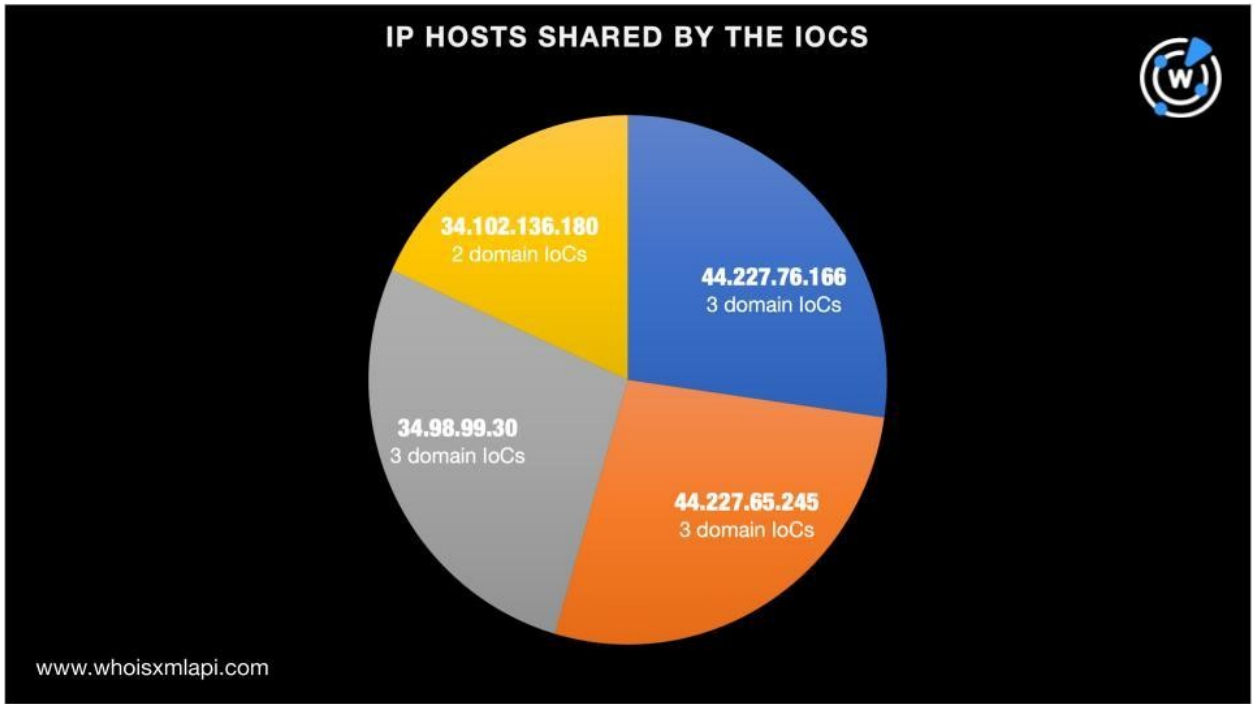
40個のドメインのうち、36個はアクセス不能のようでした。残りの4つは、当社のScreenshot Lookupによれば現在売りに出されています。

Bulk WHOIS LookupでIoCを一括検索したところ、2022年1月4日から2023年4月3日（KingsPawn攻撃が最初に報じられた日の約10日前）の間に新規登録されたものと判明しました。そのうちWHOISレコードを持つ149個のドメイン名は、6社のレジストラによって管理されていました。最も管理ドメイン数が多かったレジストラはPorkbunで、78個にのぼりました。次いで多かったのはGoDaddyで、67個でした。そして、1API GmbH、Netim、Sav.comおよびXin Net Technology Corp.が、それぞれ1個を管理していました。

KingsPawnのIoCリスト拡張でわかったこと

他のKingsPawn関連のアーティファクトを特定するために、IoCをDNS Lookupで検索しました。その結果、19個のIPアドレスが得られました。その地理的位置は米国が最も多く16個、残りはフランス、ドイツ、スイスに1個ずつ分散していました。それらのIPホストについてマルウェアチェックを行った結果、11個には悪意があることが判明しました。

そのうち4つのIPアドレスは、それぞれ複数のドメイン名で共用されていました。例えば、34[.]102[.]136[.]180はnordmanetime[.]comとhotalsextra[.]comをホストしており、44[.]227[.]76[.]166はzeebefg[.]com、topuprr[.]com、koraliowe[.]comをホストしていました。



次に、それらのIPアドレスでホストされているドメイン名を探しました。当社のReverse IP Lookupの結果2,101個のドメイン名が判明し、そのうち11個はマルウェアホストとわかりました。うち1個は売りに出されており、残りの10個はパークドメインでした。

MicrosoftのKingsPawn調査では、以下のホストベースのIoCも特定されました。

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

この3つのIoCには全て***com.apple***という文字列が含まれています。そこで、この文字列をDomains & Subdomains Discoveryにかけ、関連するサブドメインを検索しました。その結果、1,066個が該当しました。

421個のサブドメインはAppleの正規ドメイン名***apple.com***を含んでいましたが、手動で精査した結果、Appleが実際に所有していると思われるものはありませんでした。また、現在アクセスできない19個のサブドメインは、マルウェアのホストであることが判明しました。

以下の通り、そうした共通の文字列を含むサブドメインは5つのドメイン名の下にありました。

ドメイン名	悪意あるサブドメイン名の数

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

Appleの正規ドメイン名の他、Appleやその製品に関連する一般的な文字列もサブドメインに含まれていました。***appleid***およびそのタイポを含むバリエーションである***apple-id***、***apple.id***、***appleId***、***id-apple***が最も多く見られました（442個のサブドメイン）。また、***icloud***という文字列は131個のサブドメインに含まれていました。次に多かったのは***appstore***とそのバリエーションである***applestore***で、31個のサブドメインで見つかりました。それらに加え、以下の文字列が特定されました。

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

サブドメインの中には、上記のApple固有の文字列が複数含まれているものもあります。例えば、icloud[.]com[.]apple[.]applecare-support[.]us、icloud[.]com[.]apple[.]id-identify[.]us、icloud[.]com[.]apple[.]findmyIphone[.]topなどです。

—

当社が行ったIoCリスト拡張分析により、Appleの会社名、製品名、サービス名を含む3,000以上のドメイン名とサブドメインがすでにDNSに存在していることが判明しました。これらは、KingsPawnのようなゼロクリック・スパイウェアのホストになる可能性があります.

同様の調査をご希望のお客様、または本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

MicrosoftがKingsPawnのIoC

- 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

IoCが名前解決したIPアドレスの例

- 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

悪意あるIPホストの例

- 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

IoCのIPホストを共用していたドメイン名の例

- 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

IPアドレスを共用している悪意あるドメイン名の例

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

com.*apple* という文字列を含むサブドメインの例

- 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

com.*apple*という文字列を含む悪意あるサブドメインの例

- 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