WhoisXMLAPI
The Who Behind Domain, IP & Cyber Threat Intelligence

The Business of Cybercrime: Does Malicious Campaign Planning Take as Long as Legitimate Marketing Campaign Planning?

Table of Contents

Executive Report

It has become customary for cybercriminals to ride on famous brands to make their nefarious campaigns work. The release of the world's most-awaited tech gadgets is no different. And given the public attention and techies' innate desire to be first to own the latest gadgets, threat actors will always zoom in on prospective buyers via the most ingenious scams.

We trailed our sights on 2022's most-sought-after tech releases in an effort to help users stay protected. Our investigation sought to determine if cybercriminals take just as long to prepare their campaigns as legitimate businesses do. Our key findings include:

- A total of 855 domains containing strings cybercriminals were likely to use in campaigns targeting the most-awaited gadgets' potential buyers were discovered.
- We uncovered 118 subdomains containing strings cybercriminals may employ in campaigns targeting the techies lying in wait for 2022's most-sought-after tech finds.
- Eight of the domains and subdomains containing the top 2022 products have been detected as malicious.
- Threat actors may have spent 3–29 weeks to prepare for their malicious campaign launches.
- The iPhone 14-related domain registration peaked in September, coinciding with its slated launch date.

Fishing for Clues in the DNS

We began our investigation by looking for domain registration-related clues via Domains & Subdomains Discovery. Using our list of 2022's most-awaited tech releases, we identified domain or subdomain strings that threat actors may plan to use for their scams (see the table below for details).

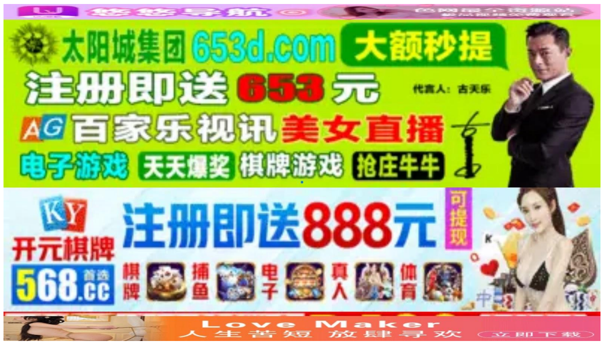
Most-Awaited Gadgets	Slated Release Date	Strings
Panic Playdate	18 April 2022	playdate playdate + console
Valve Steam Deck	25 February 2022	steam + deck valve + steam + deck
Rivian R1T	January 2022 (for all variants but originally released in September 2021)	rivian + r1t
Rivian R1S	June 2022	rivian + r1s
Magic Leap 2	September 2022	magicleap2
Meta Quest 3	October 2023 (delayed)	meta + quest3
Apple iPhone 14	16 September 2022	apple + iphone14 iphone14
Google Pixel Watch	13 October 2022	google + pixel + watch pixel + watch
Apple AR Glasses	January 2023 (delayed)	apple + arglasses
Chevy Silverado E	March 2023 (delayed)	chevy + silveradoe
Google AR Glasses	2023 or 2024 (delayed)	google + arglasses

To determine if cybercriminals spent as much time as marketers typically did on their campaign preparation (i.e., a year before the launch), we looked at the domain registration volume trends for each product a year before their slated releases. For the products originally slated to hit the market sometime in 2022, we began the tracking around two years before the new dates their manufacturers set.

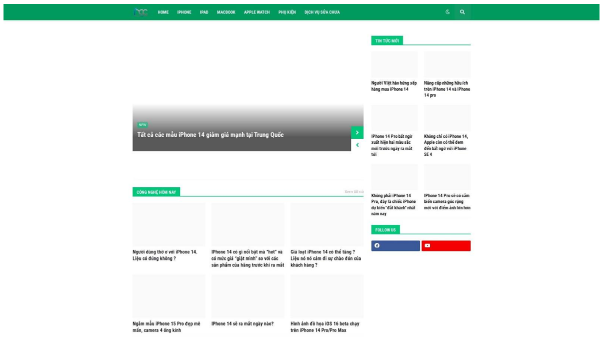
That led to the discovery of 855 domains. Note that obvious false positives like playdate-app[.]io, doggyplaydate[.]ws, and toddlerplaydate[.]com were removed from our list of "playdate"-containing domains given the string's generic nature. A bulk malware check showed that four of these are currently detected as malicious, namely:

- steamdecktouchtype[.]com
- apple-iphone14[.]in
- iphone14[.]biz
- 25iphone14pro[.]top

Only two—iphone14[.]biz and 25iphone14pro[.]top—continued to host live content but none had anything to do with selling iPhone 14 based on screenshot lookups nor owned by the manufacturers of the products named.



Screenshot of 25iphone14pro[.]top



Tất cả các mẫu iPhone 14 giảm giá mạnh tại Trung Quốc

Người dùng thờ ơ với iPhone 14. Liệu có đúng không ?

IPhone 14 có gì nổi bật mà "hot" và có mức giá "giật mình" so với các sản phẩm của hãng trước khi ra mắt

Giá loạt iPhone 14 có thể tăng ? Liệu nó nó cản đi sự chào đón của khách hàng ?

Ngắm mẫu iPhone 15 Pro đẹp mê mẩn, camera 4 ống kính

IPhone 14 sẽ ra mắt ngày nào?

Hình ảnh đồ họa iOS 16 beta chạy trên iPhone 14 Pro/Pro Max

Người Việt háo hứng xếp hàng mua iPhone 14

Nâng cấp những hữu ích trên iPhone 14 và iPhone 14 pro

IPhone 14 Pro bất ngờ xuất hiện hai màu sắc mới trước ngày ra mắt tới

Không chỉ có iPhone 14, Apple còn có thể đem đến bất ngờ với iPhone SE 4

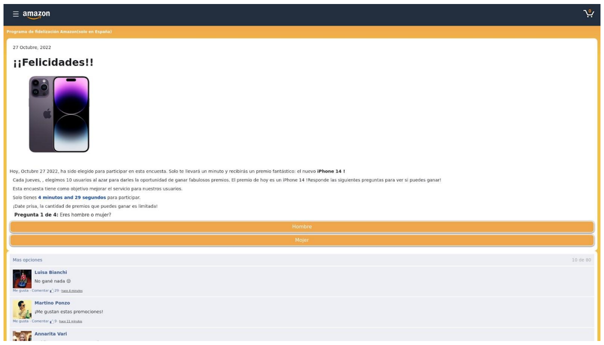
Không phải iPhone 14 Pro, đây là chiếc iPhone dự kiến "đắt khách" nhất năm nay

IPhone 14 Pro sẽ có cảm biến camera góc rộng mới với điểm ảnh lớn hơn

Screenshot of iphone14[.]biz

It's also interesting to note that only 41 of the 855 domains containing our predefined strings had unredacted registrant email addresses or were owned by the product manufacturers under scrutiny based on a bulk WHOIS lookup. Specifically, 24 indicated Apple, Inc. or Apple France as their registrant organization and three noted domains@apple[.]com as their registrant email address akin to domains the tech giant owned.

We followed the same steps for subdomains, leading to the discovery of 117 web properties bearing the strings identified earlier. Of these, four are currently classified as malware hosts—iphone14[.]pwr-lotterie1[.]tk, iphone14[.]issam[.]digital, www[.]iphone14[.]issam[.]digital, and iphone14metacollab[.]blogspot[.]com.


amazon
Programa de fidelización Amazon(solo en España)
Hombre
Mojer
Mas opciones
10 de 80
Me gusta · Comentar 29 · hace 4 minutos
Me gusta · Comentar 9 · hace 11 minutos

27 Octubre, 2022

¡¡Felicidades!!

Hoy, Octubre 27 2022, ha sido elegido para participar en esta encuesta. Solo te llevará un minuto y recibirás un premio fantástico: el nuevo **iPhone 14 !**

Cada Jueves, , elegimos 10 usuarios al azar para darles la oportunidad de ganar fabulosos premios. El premio de hoy es un iPhone 14 !Responde las siguientes preguntas para ver si puedes ganar!

Esta encuesta tiene como objetivo mejorar el servicio para nuestros usuarios.

Solo tienes **4 minutos and 29 segundos** para participar.

¡Date prisa, la cantidad de premios que puedes ganar es limitada!

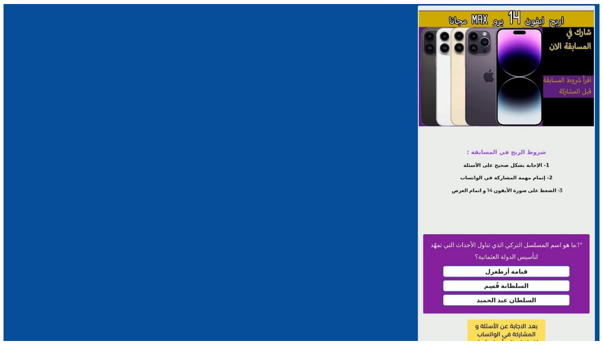
Pregunta 1 de 4: Eres hombre o mujer?

Luisa Bianchi
No gané nada ☹

Martino Ponzo
¡Me gustan estas promociones!

Annarita Vari

Screenshot of iphone14[.]pwr-lotterie1[.]tk



شروط الربح في المسابقة :

1- الإجابة بشكل صحيح على الأسئلة

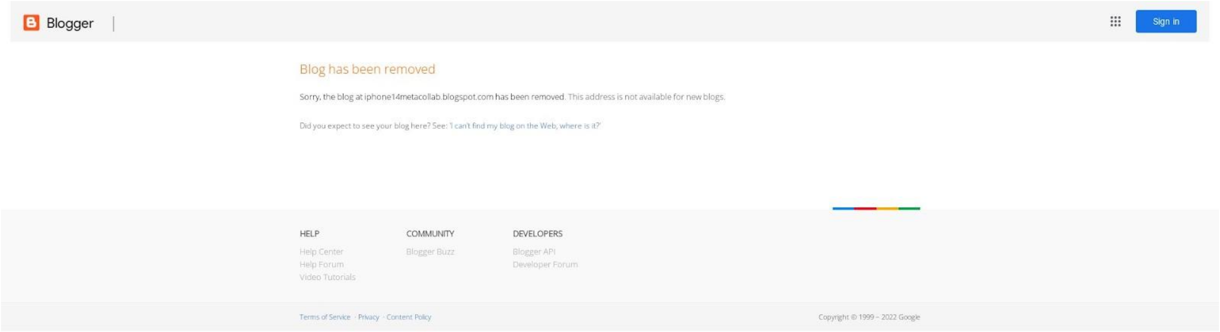
2- إتمام مهمة المشاركة في الواتساب

3- الضغط على صورة الأيفون 14 و اتمام العرض

1°:ما هو اسم المسلسل التركي الذي تناول الأحداث التي تمهّد لتأسيس الدولة العثمانية؟

بعد الاجابة عن الأسئلة و
المشاركة في الواتساب

Screenshot of iphone14[.]issam[.]digital and www[.]iphone14[.]issam[.]digital



Blog has been removed

Sorry, the blog at iphone14metacollab.blogspot.com has been removed. This address is not available for new blogs.

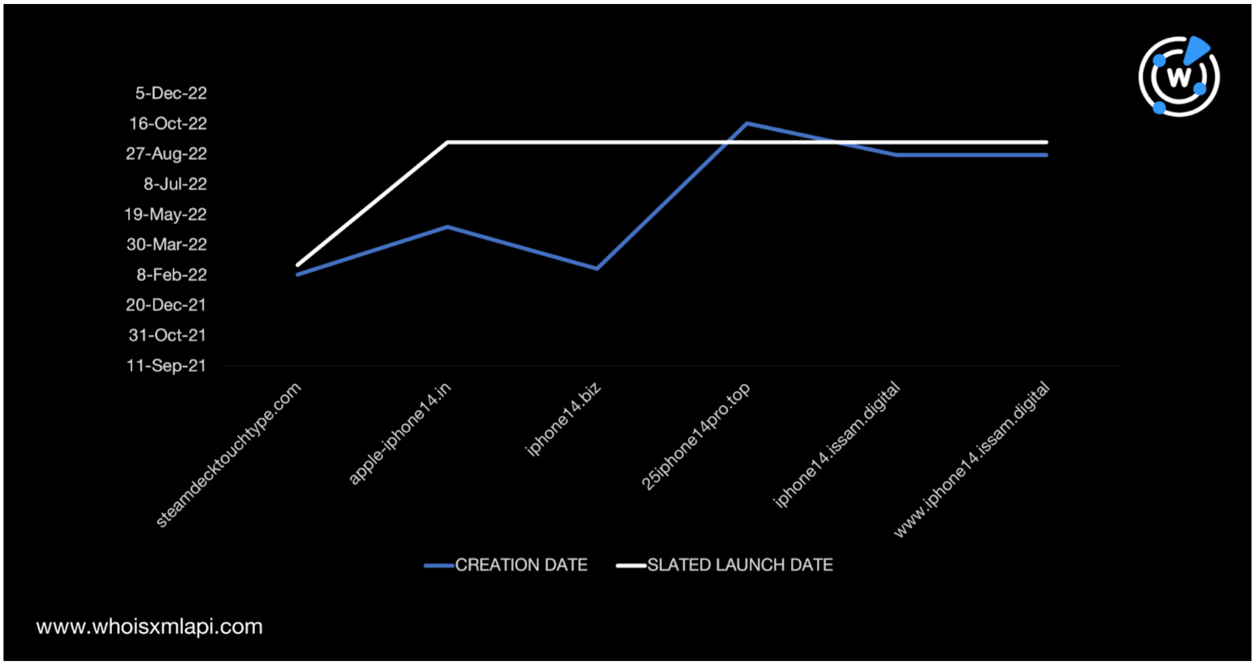
Did you expect to see your blog here? See: 'I can't find my blog on the Web, where is it?'

Screenshot of iphone14metacollab[.]blogspot[.]com

While all four pages remain live, Blogspot seemed diligent in removing the malicious blog from its platform. None of the subdomains were owned by the product manufacturers under study.

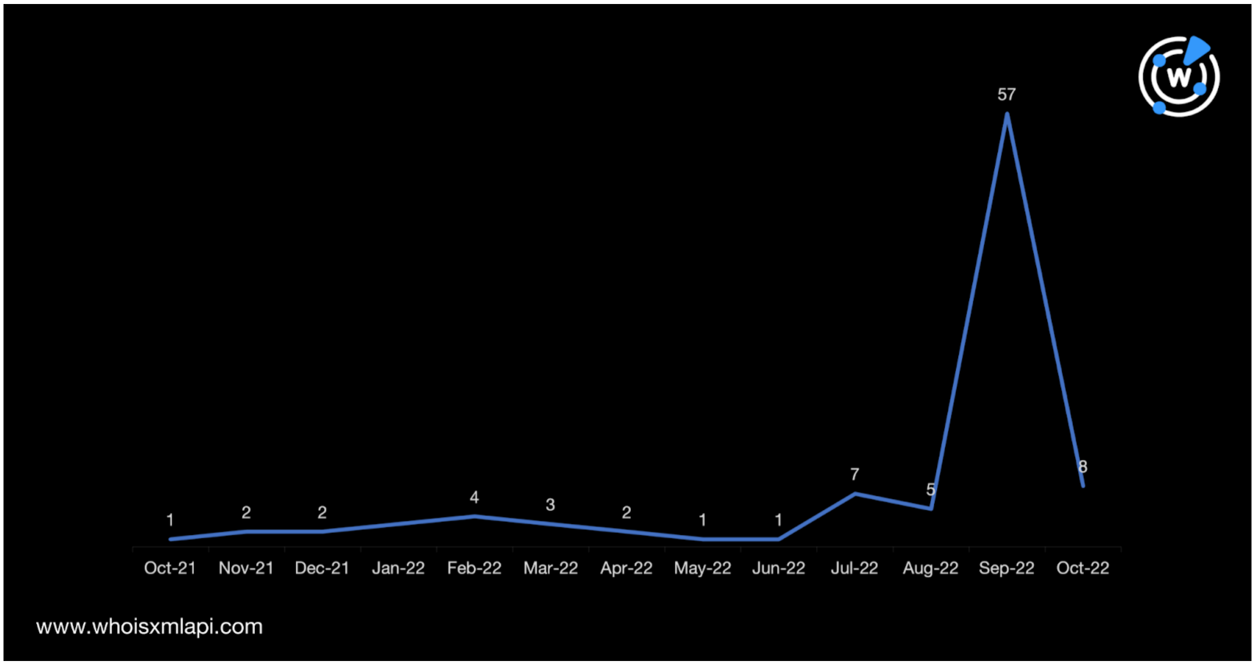
To know how much time threat actors spent on crafting their specially designed traps, we took a closer look at the malicious domains' and subdomains' (based on their root domains) WHOIS records. The malicious page iphone14metacollab[.]blogspot[.]com was, of course, excluded since anyone can create a blog on the platform.

Five of the malicious cyber resources were created between three and 29 weeks before their target products' launch dates. One, however, was created a week after the target gadget's release. Another—iphone14[.]pwr-lotterie1[.]tk—didn't have a creation date on record. The more detailed the site, as was the case with iphone14[.]biz, it seemed, the longer the preparation took.



The quick answer to our primary question then is that cybercrime may require weeks or months of planning. The more convincing a malicious website wishes to appear for greater chances of success, the more work and longer prep time required.

In addition, further investigation into the iPhone 14 domains showed that the related registration volume peaked in September, coinciding with the product's launch date. At present, domain registration has slowed down.



–

Cybercriminals and other threat actors are, as this study showed, aiming to gain the biggest profit. The time and effort they put into their campaigns and malicious sites could be expected to equate to their financial goals.

In the bad guys' case, the better the hoax, the greater the potential gain. The threats fake sites pose, however, is avoidable with the help of diligent WHOIS and DNS intelligence monitoring and consequent threat source blocking.

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

Sample Domains Containing Strings Threat Actors Would Likely Use in Their Malicious Campaigns

- buyplaydate[.]com
- shopplaydate[.]com
- playdate-console[.]ru
- playdatesoftware[.]com
- playdate-console[.]store
- steamdeckvr[.]com

- buysteamdeck[.]com
- getsteamdeck[.]com
- steamdeckmod[.]com
- steamdeckhax[.]com
- steamdecktrix[.]com
- steamdecktips[.]com
- steamdeckcase[.]com
- steamdeckcase[.]net
- steamdeckmods[.]net
- steamdeckblog[.]com
- steamdeck[.]support
- shop-steamdeck[.]ru
- steamdeckgames[.]de
- steamdeckmods[.]com
- steamdeckmodz[.]com
- steamdeckhack[.]com
- steamdeckshop[.]com
- steamdeckgame[.]com
- steamdeckhelp[.]com
- steamdeckgear[.]com
- steamdeckapps[.]com
- steamdeckstore[.]com
- storesteamdeck[.]com
- steamdeckguide[.]com
- valve-steamdeck[.]ru
- store-steamdeck[.]ru
- steamdeckgames[.]xyz
- steamdeckgames[.]com
- valvesteamdeck[.]com
- steamdeckhacks[.]com
- steamdeckforum[.]xyz
- promo-steamdeck[.]ru
- steamdeckforum[.]com
- steamdeckdeals[.]com
- steamdecklinux[.]com
- order-steamdeck[.]ru
- steamdecktweaks[.]com
- steamdeckforums[.]com
- steamdecktricks[.]com
- steamdeckgaming[.]com
- steamdeck-store[.]com
- steamdeck-forum[.]com
- steamdeckconsole[.]com
- gamingonsteamdeck[.]com
- rivianr1tparts[.]com
- rivianr1trental[.]com
- rivianr1trecall[.]com
- electric-rivian-r1t[.]com
- electric-rivian-r1t[.]co[.]uk
- rivianr1srental[.]com
- electric-rivian-r1s[.]com
- electric-rivian-r1s[.]co[.]uk
- electric-rivian-r1s-suv[.]com
- electric-rivian-r1s-suv[.]co[.]uk
- magicleap2[.]xyz
- metamagicleap2ar[.]com
- metaquest3[.]com
- metaquest3d[.]com
- metaquest3[.]co[.]uk
- metaquest3[.]quest
- metaquest360[.]com
- metaquest365[.]com
- metaquest3dsex[.]com
- metaquest3dporn[.]com
- appleiphone14[.]ru
- iphone14apple[.]com
- apple-iphone14[.]in
- appleiphone14[.]com[.]ua
- appleiphone14promax[.]com
- iphone14[.]co
- iphone14[.]be
- iphone14[.]uk
- iphone14[.]ca
- iphone14[.]in
- iphone14[.]pt
- pixelwatches[.]info

- pixelwatch[.]digital
- pixelwatchclub[.]com
- pixelwatches[.]co[.]uk
- mypixelwatch[.]co[.]uk
- pixelwatchbands[.]com
- hypixelscamwatch[.]ml
- pixelpigeonwatch[.]com
- pixelwatchrepair[.]com
- pixel-watch-loop[.]com
- pixel-watch-band[.]com
- watchbarspixelsme[.]com
- pixelwatchrepair[.]co[.]uk
- redditpixelwatchtouseold[.]pro
- luxewatchpixelspromotions[.]com
- applerealityarglasses[.]com
- chevysilveradoev[.]com
- chevysilveradoev[.]net
- be-us-chevy-silveradoes-ok[.]live
- googlearglasses[.]com

Sample Subdomains Containing Strings Threat Actors Would Likely Use in Their Malicious Campaigns

- playdategames[.]pages[.]dev
- panic-playdate[.]myshopify[.]com
- xboxplaydatesus[.]myspreadshop[.]com
- steamdeck[.]komodo[.]jp
- steamdeck[.]myjam[.]uk
- steamdeck[.]rf[.]gd
- steamdeck[.]bambusgaming[.]net
- steamdeck[.]techome[.]ro
- steamdeck[.]eu[.]com
- steamdeck[.]toiletbowlmartini[.]com
- steamsdeck[.]myshopify[.]com
- dans-rivian-r1t[.]eklickmedia[.]com
- www[.]dans-rivian-r1t[.]eklickmedia[.]com
- rivianr1s[.]direct[.]quickconnect[.]to
- apple-iphone14[.]netlify[.]app
- iphone14[.]lguplus[.]com
- iphone14[.]pages[.]dev
- iphone14[.]greensoft[.]vn
- iphone14[.]repl[.]co
- iphone14[.]re[.]kr
- iphone14[.]istockbd[.]com
- iphone14[.]datawithcar[.]com
- iphone14[.]pwr-lotterie1[.]tk
- iphone14[.]ddns[.]net
- iphone14[.]aufbau[.]cl
- iphone14[.]movie21new[.]my[.]id
- iphone14[.]selfiemobile[.]lk
- iphone14[.]spb[.]ru
- iphone14[.]sangmobile[.]com
- iphone14[.]aslowstory[.]com
- iphone14[.]simontait[.]com[.]au
- iphone14[.]issam[.]digital
- iphone14[.]tamnatt[.]com[.]au
- iphone14[.]minhtuanmobile[.]com
- iphone14[.]fastlinktraffic[.]com
- iphone14[.]ru[.]com
- iphone14[.]buihuy[.]tk
- iphone1437[.]zendesk[.]com
- jpiphone14[.]cho[.]ovh
- iphone14[.]be[.]scherpedeals[.]com
- iphone14pro[.]aufbau[.]cl
- www[.]iphone14[.]elinfor[.]com[.]br
- www[.]iphone14[.]movie21new[.]my[.]id
- freeiphone14[.]celltweak[.]com
- www[.]iphone14[.]aslowstory[.]com

- rifaiphone14[.]rendablackoficial[.]com[.]br
- www[.]iphone14[.]selfiemobile[.]lk
- iphone14gift[.]blogspot[.]com
- www[.]iphone14[.]simontait[.]com[.]au
- www[.]iphone14[.]datawithcar[.]com
- www[.]iphone14[.]issam[.]digital