Sifting for Digital Breadcrumbs Related to the Latest Zoom Attack

Table of Contents

Executive Report

Threat actors have been targeting Zoom and its users since the platform's launch, and it's easy to see why—the latest stats show it accounts for 3.3 trillion annual meeting minutes worldwide. It's not surprising, therefore, that cyber attackers trailed their sights yet again on the communication app.

Cyble researchers published a technical analysis of the IceID malware recently distributed via a massive Zoom attack. They identified three indicators of compromise (IoCs)—two domains and an IP address—related to the threat. WhoisXML API researchers, in an effort to identify as many potential attack vectors as possible to enable utmost user protection, expanded their list of IoCs and found:

- Two additional IP addresses that played host to the domains
- 299 domains that shared the IoCs' IP hosts
- Three domains that contained the string *explorezoom* as one IoC
- 20,000 domains and subdomains that contained the the string zoom, 31 of which turned out to be malicious

Uncovering DNS Connections

We began our deep dive by scouring through the IoCs' DNS records.

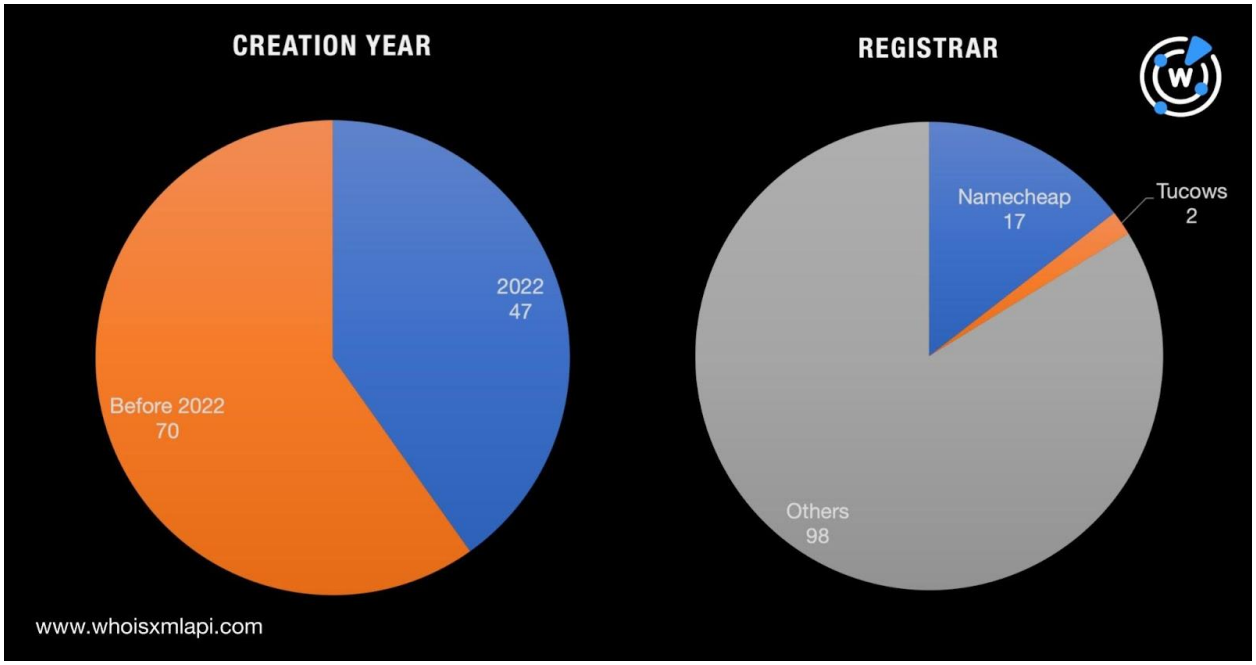
DNS lookups for the two domains identified as IoCs led to the discovery of two IP addresses that aren't in the Cyble report—172[.]67[.]163[.]25 and 104[.]21[.]15[.]157—both geolocated in the U.S. unlike the IoC 143[.]198[.]92[.]88, which traces its origin to Singapore.

To identify possible connections, we moved forward with reverse IP/DNS lookups for the three IP addresses. That provided 299 domains that shared the IoCs' IP hosts. While none of them

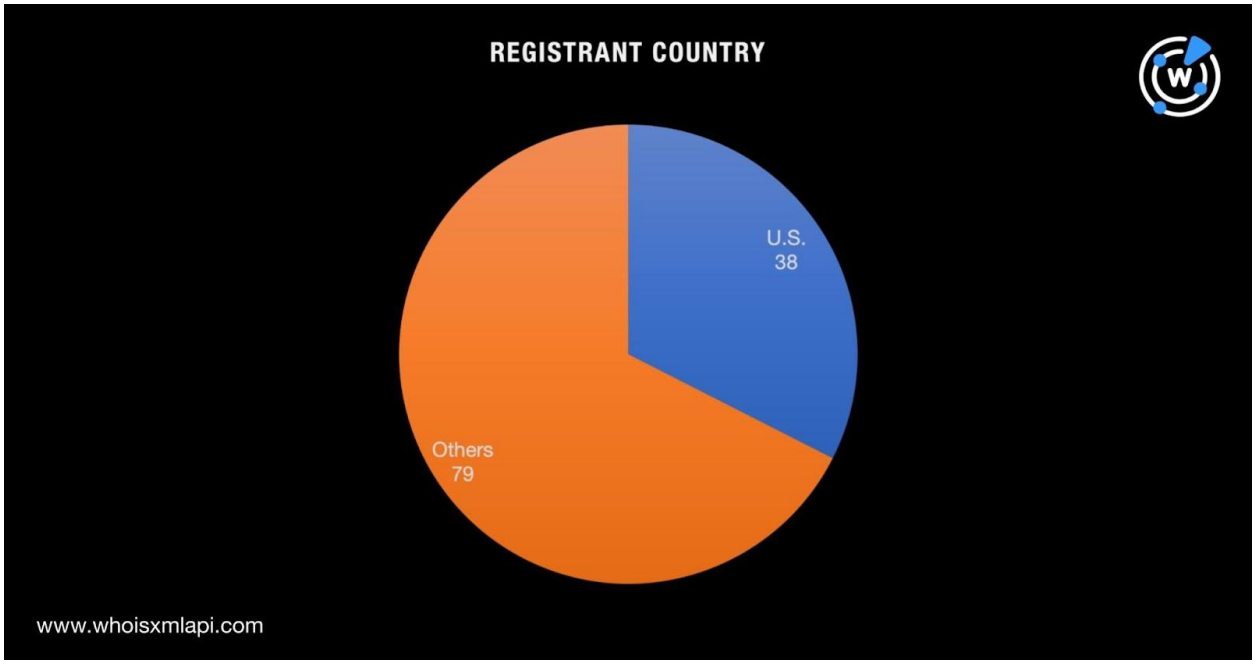
are being detected as malicious for now, sharing the IoCs' infrastructure makes them suspicious at the very least and, therefore, worth monitoring. Some of the additional domains we found shared interesting similarities with the IoCs, such as that 109 of them had the same name server (NS) host—Cloudflare.

Removing the Lid to Reveal WHOIS Ties

Next, we looked at the additional domains' WHOIS records and compared their details with those belonging to the IoCs. Of the 117 with retrievable WHOIS records, 47 shared the IoCs' creation year (2022) and 19 their registrars (17 for Namecheap, Inc. akin to explorezoom[.]com and two for Tucows, Inc. like trbiriumpa[.]com).



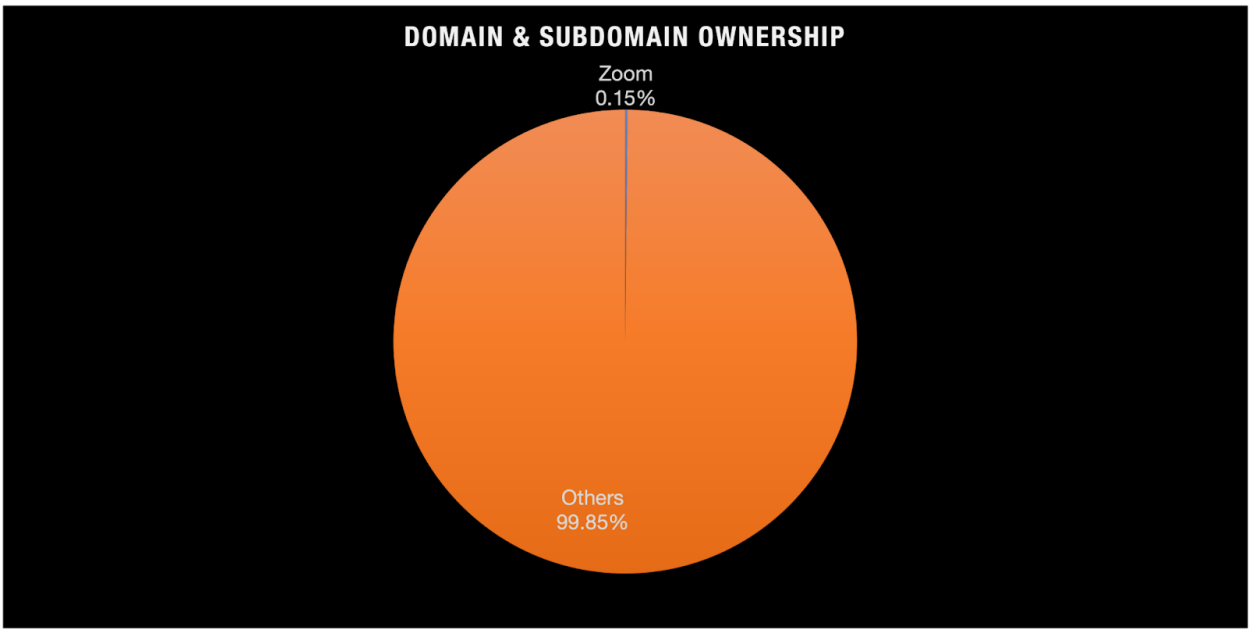
A total of 38, meanwhile, shared one of the IoCs' registrant countries—U.S. None of them indicated Singapore in their WHOIS records.



We then looked for other domains that contained the strings the threat actors used in their attack. Our search led to the discovery of three more domains containing the string *explorezoom*—explorezoom[.]us, explorezoom[.]fun, and explorezoom[.]rocks. As you can see, they only differed from the IoC in that they used different top-level domain (TLD) extensions. While none of them were considered malicious, they could easily serve as substitutes to explorezoom[.]com.

Finally, given Zoom's large global user base, we then sought to look for all domains and subdomains that contain the string *zoom* that could figure in future attacks against the platform and its users. Domains & Subdomains Discovery listed 20,000 additional web properties (10,000 domains and another 10,000 subdomains), 31 of which turned out to be malicious (30 were malware hosts and one was a confirmed spam source).

It's also interesting to note that a bulk WHOIS lookup for the *zoom*-containing domain and subdomain names showed that only 30 belonged to Zoom based on the organization name their registrants' indicated—Zoom Video Communications, Inc.



The remaining pages could thus serve as potential threat vectors if they get compromised or purchased then weaponized to distribute malware or spam targeting Zoom users.

Finally, apart from *zoom*, the domain and subdomain names also featured recurring strings, such as *web*, *site*, and *online*. The 10 most common strings found are shown in the following word map.

Many of these digital properties can host sites and pages mimicking the official Zoom download page, malware-laced Zoom tutorials, or publicly accessible prerecorded Zoom webcasts that may redirect to phishing or other malicious pages.

—

Any software or app with a huge user base is a prime cyber attack target. But avoiding the risks that threats targeting them pose is doable with a little help from WHOIS and DNS intelligence that can help security teams identify all potential attack entry points. Monitoring them for signs of malicious activity and blocking access to and from them are critical next steps.

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

Zoom Attack IoCs Identified by Cyble

- explorezoom[.]com
- trbiriumpa[.]com
- 143[.]198[.]92[.]88

Sample Zoom Attack IoC IP Address Resolution

- 172[.]67[.]163[.]25

Sample Zoom Attack IoC IP-Connected Domains

- 1000rbx[.]ml
- 123mkv[.]com
- 1xbet-tr[.]net
- 33rapzip[.]com
- 3d-futa-games[.]com
- 404quiz[.]net
- 610980[.]com
- 6523621[.]com
- 885cc[.]com
- 91avi30[.]com
- a-great-gel-antibacterial-go[.]fyi
- absgroup[.]online
- accountingoversightboard[.]us
- aconventionalwellness[.]com
- acuario[.]es
- adfarpyly[.]tk
- adilrchiv[.]ml
- adizinininer[.]tk
- adsbordkjgf[.]click
- adunbou[.]tk
- afrodisiaca[.]es
- agechaysqeeser[.]tk
- agischin[.]tk
- alahaa[.]com
- alaninmoithia[.]tk
- alasdair[.]mochi[.]ml

- alberguetexu[.]com
- alcoveworld[.]com
- algoy[.]com
- alinhul[.]ml
- allfree[.]co[.]il
- alrawnak[.]com
- aluminum-diamond[.]co[.]il
- alwaysabruin[.]com
- amalgawtlv[.]ru
- americangistflash[.]com
- amunracasino[.]net
- anaralanim[.]shop
- ansbperfume[.]com
- apcakerdia[.]gq
- apgrotdotiwordjor[.]tk
- api[.]vpnvastapp[.]com
- app[.]vpnvastapp[.]com
- appuiformation[.]fr
- areabpacompleci[.]ga
- arexas[.]ga
- arnecesmabizt[.]tk
- asabor[.]gq
- aspireperformancesystems[.]net
- assetmarketings[.]cf

Sample Zoom Attack IoC String-Connected Domains

- explorezoom[.]us
- explorezoom[.]fun

Sample *Zoom*-Containing Domains and Subdomains

DOMAINS	SUBDOMAINS
• zoomzoomzoomzoomzoomzoom[.]com • zoomzoomzoomzoomzoom[.]com • zoomzoomzoomzoom[.]com • zoomzoomzoom[.]co • zoomzoomzoom[.]uk • zoomzoomzoom[.]cn • zoomzoomzoom[.]ru • zoomzoomzoom[.]fr • zoomzoomzoom[.]org • zoomzoomzoom[.]com • zoomzoomzoom[.]net • zoomzoomzoom[.]xyz • zoomzoomzoom[.]info • zoomyzoomzoom[.]com • zoomazoomzoom[.]com • zoomzoomzoom01[.]tk • zoom-zoom-zoom[.]de • zoomzoom[.]nl • zoomzoom[.]ru • zoomzoomzoomba[.]com • zoomyzoomyzoom[.]com • zoomzoom[.]fr	• zoomzoomzoomzoomzoom[.]ytmnd[.]com • zoomzoomzoomzoom[.]ytmnd[.]com • zoomzoomzoom[.]ytmnd[.]com • zoomzoomzoom[.]myqnapcloud[.]com • zoomzoomzoom[.]muragon[.]com • zoomazoomzoom[.]ytmnd[.]com • zoom-zoom-zoom[.]urbanup[.]com • zoomzoom[.]teleport[.]sh • zoomzoom[.]freeboxos[.]fr • zoomzoom[.]gamezhero[.]com • zoomzoom[.]davaconsulting[.]com • zoomzoom[.]acars[.]ru • zoomzoom[.]carguru[.]ru • zoomzoom[.]mgpsolutions[.]mobi • zoomzoom[.]workers[.]dev • zoomzoom[.]summer-breath[.]com • zoomzoom[.]unblog[.]fr • zoomzoom[.]keenetic[.]link • zoomzoom[.]jadrianjohnson[.]com • zoomzoom[.]zoom[.]cab • zoomzoom[.]inbox[.]photo

- zoomzoom[.]eu
- zoomzoom[.]de
- zoomzoom[.]hu
- zoomzoom[.]jp
- zoomzoom[.]se
- zoomzoomzoom[.]co[.]uk
- zoomzoom[.]ro
- zoomzoom[.]us
- zoomzoom[.]sk
- zoom-zoom-zoom[.]icu
- zoomzoom[.]sg
- zoomzoom[.]la
- zoomzoom[.]me
- zoomzoom[.]tv
- zoomzoom[.]cn
- zoomzoom[.]no
- zoomzoom[.]ae
- zoomzoom[.]ca
- zoomzoom[.]ch
- zoomzoom[.]be
- zoomiezoomzoom[.]com
- zoomzoom[.]kr
- zoomzoom[.]uk
- zoomzoom[.]tk
- zoomzoom[.]co
- zoomzoom[.]pl
- zoomzoom[.]rs
- zoomzoom[.]cz
- zoomzoom[.]in
- zoomzoom[.]ir
- zoomzoom[.]dk
- zoomzoom[.]io
- zoomzoom[.]nu
- zoomzoom[.]it
- zoom-zoom-zoom[.]com
- zoomzoom[.]ng
- zoomzoom[.]at
- zoomzoom[.]nz
- zoomzoomzoom[.]camera
- zoom-zoom-zoom[.]info
- zoom-zoom[.]ba
- zoomzoom[.]icu
- zoom-zoom[.]hu
- zoomzoom[.]pro
- zoomzooms[.]ca
- zoomzoom[.]pickmyplaner[.]com
- zoomzoom[.]nannynannybooboo[.]com
- zoomzoom[.]carloparsons[.]com
- zoomzoom[.]ytmnd[.]com
- zoomzoom[.]aspiringeagles[.]com
- zoomzoom[.]igorsclouds[.]com
- zoomzoom[.]wildsight[.]ca
- zoomzoom[.]kyiv[.]ua
- zoomzoom[.]continu[.]nl
- zoomzoom[.]keenetic[.]pro
- zoomzoom[.]onedashten[.]com
- zoomzoom[.]plus[.]com
- zoomzoom[.]deviantart[.]com
- zoomzoom[.]claude-alain[.]com
- zoomzoom[.]synology[.]me
- zoomzoomzoomzoo[.]livejournal[.]com
- zoomzoom[.]asuscomm[.]com
- zoomzoom[.]homeserver[.]com
- zoomzoom[.]phpnet[.]us
- zoomzoom[.]dtjanaka[.]com
- zoomzooma[.]violity[.]auction
- zoomzoomj[.]tumblr[.]com
- zoom-zoom[.]lxpmz[.]com
- zoom-zoom[.]joerijansen[.]be
- zoomzoomb[.]eatnplaynlove[.]com
- zzoomzoom[.]loanforpeoplewithbadcredit[.]org
- zoom-zoom[.]ucsd[.]edu
- zoomzoom1[.]fortunecity[.]ws
- zoomzoomy[.]tumblr[.]com
- zoom-zoom[.]mazda[.]jp
- zoom8zoom[.]livejournal[.]com
- zoom[.]zoom[.]crepala[.]com
- zoom-zoom[.]financierabucareli[.]com[.]mx
- zoom-zoom[.]iapps4you[.]com
- zzoomzoom[.]olilaneb[.]info
- zoom-zoom[.]squarespace[.]com
- zoom-zoom[.]mazda[.]com
- zoom-zoom[.]us[.]com
- zoomzoom4[.]repl[.]co
- zoomwzoom[.]blogspot[.]com
- zoom[.]zoom[.]pagesperso-orange[.]fr

- zoomzoom[.]biz
- zoom-zoom[.]cz
- zoom-zoom[.]dk
- zoomzoom[.]fun
- zoom-zoom[.]pl
- zoomzoom[.]com
- zoom-zoom[.]jp
- zoom-zoom[.]no
- zoom-zoom[.]ch
- zoom-zoom[.]se
- zoomzoom[.]top
- zoom-zoom[.]eu
- zoom-zoom[.]de
- zoomzoom[.]xyz
- zoom-zoom[.]cn
- zoom-zoom[.]tv
- zoom-zoom[.]us
- zoom-zoom[.]be
- zoomzoom[.]net
- zoom-zoom[.]at
- zoom-zoom[.]fr
- zoom-zoom[.]su
- zoomzoom[.]app
- zoom-zoom[.]nl
- zoomzoom[.]nyc
- zoom-zoom[.]ro
- zoom-zoom[.]ru
- zoomzoom[.]vip
- zzoomzoom[.]us
- zoom-zoom[.]es
- zoom-zoom[.]ca
- zoomzoom[.]org
- zoomzoom[.]run
- zoomiezoomiezoom[.]com
- zoomzoomzoom-ing[.]com
- zoomzoom[.]club
- zoomzooms[.]com
- zoomzoom[.]shop
- zoominzoom[.]pl
- zoomxzoom[.]com
- zoomzooma[.]com
- zoomzoomz[.]com
- zoomzoom[.]taxi
- zoomzoomb[.]com
- zoomzoom[.]asia
- zoom-zoom[.]greenlist[.]kz
- zoom-zoom[.]con[.]ba
- zoomzoom7[.]blogspot[.]com
- zoom-zoom[.]yyaq[.]com
- zoomzooms[.]myshopify[.]com
- zoom-zoom[.]remotewebaccess[.]com
- zoomzoom2[.]xwx[.]co[.]il
- zoom-zoom[.]sakura[.]ne[.]jp
- zoom-zoom[.]udo[.]photo
- zoomxzoom[.]polyvore[.]com
- zoom-zoom[.]musicas[.]mus[.]br
- zoomxzoom[.]blogfa[.]com
- zoomwzoom[.]blogspot[.]com[.]ar
- zoomizoom[.]tablonaghashi[.]com
- zoom-zoomy[.]exteen[.]com
- zoomzoomit[.]cgttesting[.]com
- zoomzoom03[.]animepaper[.]net
- zoomzoom03[.]wordpress[.]com
- zoomzoomlj[.]asuscomm[.]com
- zoomzoom02[.]skyrock[.]com
- zoomzoomsg[.]thehopefultree[.]com
- zoom-zooms[.]urbanup[.]com
- zoomyzoom6[.]newgrounds[.]com
- zoomopzoom[.]ciderchat[.]com
- zoomzoom01[.]skyrock[.]com
- zoomazooma[.]foodpages[.]ca
- elzoomzoom[.]kroogi[.]com
- zoomzoommm[.]deviantart[.]com
- zoomzoomfr[.]7a7[.]fr
- zoom[.]zooms[.]kro[.]kr
- zoomzoom94[.]tumblr[.]com
- gozoomzoom[.]tomhintz[.]com
- vzoomvzoom[.]beul[.]digital
- zoom1[.]zoom[.]streamstorecloud[.]com
- lalalazoomzoomzoom[.]wordpress[.]com
- zoomzoom[.]fr[.]alouest[.]org
- zoomzoommag[.]edition-on[.]net
- zoezoomzoom[.]tumblr[.]com
- zoomzoomseo[.]blogspot[.]com
- zoomzoom345[.]tumblr[.]com
- zoomzoompie[.]newgrounds[.]com
- zoomzoombru[.]asuscomm[.]com

- zoomzoom[.]link
- zoomzoom[.]love
- zoomizoom[.]com
- zoomzoomi[.]com
- zoomzoom[.]wiki
- izoomzoom[.]com
- zoomzoom[.]live
- zoomyzoom[.]com
- zoom-zoom[.]net
- m6zoomzoom[.]cn
- zoomzoom[.]tech
- zoomzoom[.]fund
- vzoomvzoom[.]gr
- zoomzoom24[.]ru
- zoombyzoom[.]dk
- zoom4zoom[.]com
- zoomzoomin[.]xn--fiqz9s
- zoomazoom[.]com
- zoomzooms[.]net
- zoomzoom[.]mobi
- zoomzoom[.]work
- zoomazoom[.]net
- zoomzoom[.]cash
- zoomazooma[.]tk
- zoomnzoom[.]com
- zoomtozoom[.]eu
- zoomzoom[.]site
- zoomzoom[.]zone
- zoomzoom[.]info
- zoom-zoom[.]biz
- zoom-zoom[.]xyz
- zoom2zoom[.]com
- zoom-zoom[.]vip
- zoom-zoom[.]org
- zoom-zoom[.]com
- zoomzoomix[.]ru
- zoomzoomzoom-yacht[.]com
- zoomzoomzoomtowing[.]com
- zoomzoomzoomtowing[.]net
- zoombazoom[.]com
- zoomunzoom[.]com
- zoomtzoomt[.]com
- zoomitzoom[.]net
- zoomonzoom[.]com
- zoom-zoom[.]mobi
- zoomzoom[.]pl[.]w3snoop[.]com
- zooma1zooma[.]blogspot[.]com
- zoomzoomzoo[.]blogspot[.]com
- zoomzoomred[.]myds[.]me
- zooms[.]zooms[.]kro[.]kr
- zoomzoomhug[.]odotservice[.]com
- zoomzoomzem[.]blogspot[.]com
- iamzoomzoom[.]iq[.]pl
- zoomm-zoomm[.]exteen[.]com
- lolzoomzoom[.]ytmnd[.]com
- zoomzoom[.]cs[.]unc[.]edu
- vzoom-vzoom[.]blogspot[.]com
- zoomzoomemmy[.]polyvore[.]com
- gazoomgazoom[.]repl[.]co
- zoomzoomroom[.]livejournal[.]com
- zoomzoomwork[.]workers[.]dev
- zoomzoom[.]www[.]nn[.]ru
- zoomzoombubu[.]tumblr[.]com
- zoomzoom[.]dev[.]jivosite[.]com
- zoomzoomtown[.]zendesk[.]com
- zoomzoomclub[.]ganquedesigns[.]com
- autozoomzoom[.]mazdabatangas[.]com
- zoom-us-zoom[.]dlnow[.]co
- zoomzoom1341[.]wordpress[.]com
- zoominzoomin[.]blogspot[.]com
- bazoombazoom[.]showmax[.]com
- zoomzoomseal[.]ytmnd[.]com
- zoomzoomtour[.]zendesk[.]com
- www[.]zoomzoom[.]aspiringeagles[.]com
- zoom-us-zoom[.]mrdownload[.]com
- zoomzoom[.]bbs[.]fc2[.]com
- zoomzoomboom[.]myshopify[.]com
- cityzoomzoom[.]blogspot[.]com
- www[.]zoomzoom[.]onedashten[.]com
- zoomzoomclub[.]messageboard[.]nl
- zoom-us-zoom[.]descargar[.]gratis
- zoomzoomzeng[.]skyrock[.]com
- zoomzoom[.]geo[.]umass[.]edu
- zoomzoomicon[.]livejournal[.]com
- techzoomzoom[.]duckdns[.]org
- www[.]zoomzoom[.]pickmyplaner[.]com

- zoomzoomex[.]com
- zoomozoomo[.]com
- zoomzoom[.]cloud
- zoomzoom[.]today
- zoomzoom[.]pizza
- zoomzoomfx[.]com
- zoomzoomim[.]com
- zoomzoom[.]co[.]zw
- zoomzoomie[.]com
- zoomzoomme[.]com
- avzoomzoom[.]com
- zoomzoom[.]paris
- zoomzoom[.]photo
- zoomzoomfx[.]net
- zoomzoom[.]co[.]jp
- zoomzoom[.]in[.]ua
- gozoomzoom[.]com
- zoomzoomart[.]ca
- lezoomzoom[.]com
- zoombazoom[.]icu
- zoomzoomai[.]com
- zoomzoom-e[.]com
- zoomiezoom[.]com
- zoomszooms[.]com
- zoomerzoom[.]com
- zoomzoomkc[.]com
- zoomiszoom[.]com
- zoomzoomit[.]com
- zoomzoom83[.]com
- zoomtozoom[.]com
- zoomzoom[.]space
- zoomazooma[.]net
- zoomzoom[.]rocks
- zoomzoom[.]co[.]uk
- zoomzoommn[.]com
- zoomzoomfx[.]org
- izoom-zoom[.]com
- zoomzoomba[.]com
- zoom-zoom[.]club
- myzoomzoom[.]com
- zoomzoomtv[.]com
- zoomzoommag[.]ca
- zoomzoomtj[.]com
- runzoomzoom[.]de
- zoomzoomla[.]com
- www[.]zoomzoom[.]carloparsons[.]com
- zoomzoom-nao[.]muragon[.]com
- zoomzoom9238[.]continu[.]nl
- zoomzoomlane[.]kepowin[.]com
- zoom-us-zoom[.]dlnow[.]net
- zoomzoom9238[.]homeserver[.]com
- zoomzoom2012[.]polyvore[.]com
- zoombetazoom[.]instanthq[.]com
- zoomzoomtour[.]jejupassrent[.]com
- zoomzoomroom[.]livejounral[.]com
- zoomzoomlane[.]indoxbet[.]id
- zoomzoombali[.]bentamblyn[.]com
- zoomzoomluke[.]wordpress[.]com
- zoom-us-zoom[.]fileplanet[.]com
- zoom-us-zoom[.]uptodown[.]com
- zoomzoomlist[.]rebelbailey[.]com
- zoommoozzoom[.]tumblr[.]com
- www[.]zoom-zoom[.]financierabucarelli[.]com[.]mx
- zoomvmc1[.]zoom[.]msu[.]edu
- hazoom[.]hazoom[.]mixh[.]jp
- zoomzimmyzoom[.]booklikes[.]com
- zoomzoomzooom[.]kinja[.]com
- zoominzoomout[.]substack[.]com
- www[.]zoom-zoom[.]con[.]ba
- zoomzoommazda[.]blogspot[.]com
- zoomlarryzoom[.]tumblr[.]com
- zoominzoomout[.]connxusdemo[.]com
- zoomzoompartz[.]highwire[.]com
- zoom[.]meetzoom[.]daneesha[.]ml
- zoomzoom[.]demo[.]disco[.]co
- zoomzoombowen[.]bentamblyn[.]com
- zoomvmc2[.]zoom[.]msu[.]edu
- zoomin-zoomin[.]seesaa[.]net
- zoominzoomout[.]curseforge[.]com
- boonzzoomzoom[.]blogspot[.]com
- www[.]zoom-zoom[.]remotewebaccess[.]com
- www[.]zoom-zoom[.]udo[.]photo
- zoomzoomgroup[.]warner-co[.]com
- zoomzoomshell[.]tumblr[.]com
- www[.]zoomwzoom[.]blogspot[.]com
- zoomzoome[.]www[.]nn[.]ru

- zoomzoomzen[.]eu
- kazoomzoom[.]com
- zoomzoomzen[.]be
- zoommazoom[.]com
- zoominzoom[.]com
- zoomzoomer[.]com
- zoomzoomzen[.]fr
- zoomitzoom[.]com
- amazoomzoom[.]ru
- amazoomandazoomzoom[.]com
- zoomzoom[.]world
- zoombyzoom[.]com
- zoomzoom[.]co[.]il
- zoomzoomsg[.]com
- zoomzoomby[.]com
- zoomzoom[.]ninja
- zoomzoomaz[.]com
- zoomizoomi[.]com
- zoomzoomlaw[.]us
- zoomzoom[.]co[.]nz
- lezoomzoom[.]net
- zoombezoom[.]net
- zoomopzoom[.]com
- zoomyzoomy[.]com
- zoomzoom4k[.]com
- zoomhotzoom[.]tk
- zoomzoomsd[.]com
- zoomzoom[.]parts
- zoomezoome[.]com
- zoomzoomzoom[.]technology
- zoomzoom[.]party
- zoom-zoom[.]info
- zoomzoomin[.]com
- zzoomzzoom[.]com
- zoomzoomgo[.]com
- zoomazooma[.]com
- thezoomzoom[.]com
- nikzoomzoom[.]com
- airzoomzoom[.]com
- zoomzoombox[.]com
- zoomzoombaby[.]uk
- zoomtakezoom[.]ga
- zoomzoomtow[.]org
- zoomazoomer[.]com
- redzoomzoom[.]com
- zoomzoom-5202[.]myshopify[.]com
- www[.]zoom-zoom[.]joerijansen[.]be
- zoomblog-zoom[.]blogspot[.]com
- zoomzoomzooom[.]tumblr[.]com
- zoomzoomcarss[.]blogspot[.]com
- www[.]zoomzoomb[.]eatnplaynlove[.]com
- zoomzoomrider[.]blogspot[.]com
- gammazoomzoom[.]duckdns[.]org
- zoomzoomcarss[.]blogspot[.]hr
- zoomclus-zoom[.]blockedge[.]dev
- www[.]zoomizoom[.]tablonaghashi[.]com
- zoomzoomgirls[.]wixsite[.]com
- zoom-zoom-zoom[.]harunoya[.]mixh[.]jp
- zoom-zoom-zoom-for-kids[.]soft112[.]com
- zoom[.]sergioperezlissadini[.]com[.]uy
- zoom[.]bunda[.]co[.]id
- zoom[.]dc-market[.]kr
- zoom[.]nywx[.]org
- zoom[.]proyectodinaztia[.]com
- zoom[.]itstorque[.]com
- zoom[.]visperai[.]net
- zoom[.]romeobug[.]com
- zoom[.]cundari[.]us
- zoom[.]fahimyar[.]ir
- zoom[.]uaprom[.]net
- zoom[.]iluki[.]ru
- zoom[.]wayneming[.]com
- zoom[.]musicas[.]mus[.]br
- zoom[.]gotcore[.]net
- zoom[.]mysmsveri[.]com
- zoom[.]didivor[.]com[.]tr
- zoom[.]carloparsons[.]com
- zoom[.]collantes[.]me
- zoom[.]alexion[.]us
- zoom[.]skibamedia[.]de
- zoom[.]ercapps[.]com
- zoom[.]laacademia[.]com
- zoom[.]landmarkwisdomcgt[.]com
- zoom[.]jayenashar[.]org
- zoom[.]superall[.]ru
- zoom[.]bangorward[.]org

• zoomzoomkare[.]cf • zoomzoom[.]net[.]ua • zoomzoomfit[.]com	• zoom[.]bluetoothmicrophones[.]us • zoom[.]yudo[.]it • zoom[.]piscopoker[.]com • zoom[.]orderupcustomers[.]com • zoom[.]guillaumealla[.]in • zoom[.]ever[.]green • zoom[.]goonline[.]id • zoom[.]ipnetsupport[.]com • zoom[.]easyteach[.]co[.]il • zoom[.]kerese[.]co[.]uk • zoom[.]republictitle[.]com • zoom[.]chaignepain[.]org • zoom[.]worldtraderealty[.]com • zoom[.]sixprofit[.]com • zoom[.]on[.]fashion • zoom[.]danuma[.]online • zoom[.]propps[.]io • zoom[.]studiotecnicomc[.]it • zoom[.]paproperties[.]com[.]ph • zoom[.]activemax-2020[.]space • zoom[.]umybf[.]me • zoom[.]just-shared[.]top • zoom[.]ab-archive[.]net

Sample Malicious Zoom-Containing Domains and Subdomains

- zoom[.]cyou
- zoom-us[.]us
- zoomgel[.]ir
- lhzoom[.]com
- kazooms[.]us
- gmzoom[.]net
- zoomzoomclub[.]ganquedesigns[.]com
- zoom[.]fearlessnetpreneur[.]com
- zoom[.]netpreneur360[.]com
- zoom[.]fservingtech[.]com
- zoom[.]cosymie[.]com
- zoom[.]fusionysabor[.]cl
- zoom[.]sharechanneltv[.]com
- zoom[.]interface11[.]org
- zoom[.]opboysatbt[.]com
- zoom[.]xlalv[.]com
- zoom[.]clickhere[.]top
- zoom[.]clickablecard[.]top
- zoom[.]fourquarterseats[.]com
- zoom[.]ibrahim[.]az