Blurring the Lines between APTs and Cybercrime: Cobalt Mirage Uses Ransomware to Target U.S. Organizations

Table of Contents

Executive Report

In the past, security experts typically made a distinction between a cybercrime and an advanced persistent threat (APT). While cybercrime focused on obtaining financial gain, APTs trailed their sights on specific organizations, often to steal nation-state secrets. Cobalt Mirage recently seems to have blurred the lines with recent attacks on U.S.-based targets using BitLocker and DiskCryptor.

In an effort to keep organizations safe through transparency, we delved deeper into the threat to identify more artifacts that could put them at risk. Our analysis revealed:

- Three unredacted email addresses used to register some of the domains (11 in total) AlienVault identified as indicators of compromise (IoCs)
- 72 domains that used the same registrant email addresses
- 3 IP address resolutions of the domain IoCs
- 600 domains that shared the domain IoCs' IP hosts (5 in total)
- 2 out of the 672 domains found turned out to be malicious
- 23,875 domains that contained similar strings or string combinations as the domain IoCs, none of which belonged to Microsoft and only two were Symantec-owned, and 1,568 of which were dubbed "malicious"

What the Public Knows So Far

SecureWorks researchers uncovered the threat earlier this month and, like AlienVault, publicized domain names as IoCs. AlienVault also identified two IP addresses as IoCs.

Domain IoCs	IP Address IoCs
• winstore[.]us • update[.]us • tcp443[.]org • symantecserver[.]co • service-management[.]tk • onedriver-srv[.]ml • newdesk[.]top • my-logford[.]ml • msupdate[.]us • microsoft-updateserver[.]cf • aptmirror[.]eu	• 198[.]12[.]65[.]175 • 107[.]173[.]231[.]114

SecureWorks also went on to identify the ransomware variants Cobalt Mirage used in their attacks—BitLocker and DiskCryptor. BitLocker is a built-in Microsoft encryption feature that cybercriminals abused to lock targets out of their systems in November 2021. DiskCryptor, meanwhile, is an open-source encryption tool also compromised by cybercriminals to launch what came to be known as Mamba ransomware attacks in April 2021.

What Our Deep Dive Revealed

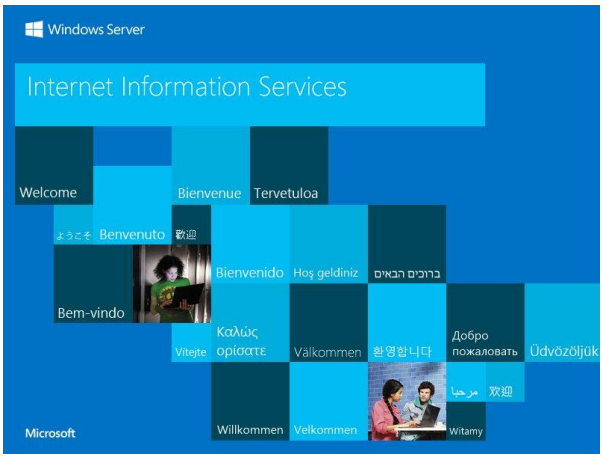
Using the publicized IoCs as jump-off points, we began by subjecting the 11 domain IoCs to a bulk WHOIS lookup, which led to the discovery of three unredacted email addresses. Subjecting those registrant email addresses to historical reverse WHOIS searches let us uncover 72 domains.

Reverse IP lookups for five IP addresses (2 identified by AlienVault as IoCs and 3 revealed by DNS lookups for the additional 72 domains) that played host to the domain IoCs provided an additional 600 domains. Interestingly, one of the three additional IP hosts we uncovered—54[.]39[.]78[.]148—seemed to be a dedicated IP address.

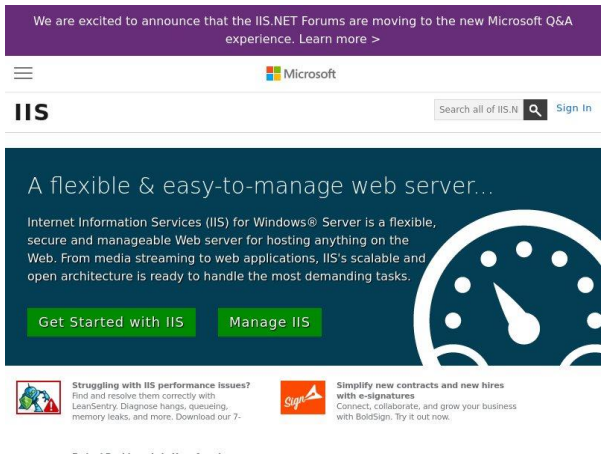
A bulk malware check on the Threat Intelligence Platform on all the additional domains and IP addresses identified through our analysis showed that organizations should probably block access to and from two specific domains—001lab[.]com and agrisecurv-supc[.]ml—as they have been dubbed “malicious” by various malware engines.

What Else Can Put Organizations at Risk?

Screenshot lookups for the domain IoCs showed that one remained accessible—my-logford[.]ml. A side-by-side comparison with the official Windows Server Internet Information Services (IIS) site—iis[.]net—shows they do not even remotely look alike.



Screenshot of my-logford[.]ml, which seems to be mimicking Microsoft's IIS site



Screenshot of iis[.]net, the official Microsoft IIS site

A closer look at the domain IoCs also showed close ties to known Microsoft brands like Windows, OneDrive, and Microsoft. One also seemed to be mimicking U.S.-based security solution provider Symantec. Using the strings and string combinations "win + store," "onedrive," "ms + update," "microsoft + update," and "symantec" as Domains & Subdomains Discovery search terms, we identified 23,875 additional domain artifacts. Note, though, that there may be a number of false positives given short strings like "win" and "ms."

None of the 22,280 domains carrying Microsoft-owned brands actually belonged to the company based on the details on their WHOIS records. In addition, only two out of the 1,595 web properties containing Symantec's name were under its control. A bulk malware check also showed that 1,568 of them were malicious.

—

Organizations should avoid accessing any of the 1,570 domains identified as malware hosts to avoid joining the slew of Cobalt Mirage victims to date. And given the recent change in APT groups' modus operandi—adding the use of cybercrime tools into the mix—monitoring emerging threat trends is also necessary.

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

Unredacted Registrant Email Addresses

- spie*****@yahoo[.]com
- thu*****@protonmail[.]com
- amirbit*****@gmail[.]com

Domains Registered Using the Unredacted Email Addresses

- update[.]us
- vrs[.]us
- avn[.]us
- tradevisitor[.]com
- ajn[.]fr
- 1pagecheckout[.]com
- vennootschapsbelasting[.]com
- task[.]us
- onecoincreditcard[.]com
- primacoupons[.]com
- directoryphon[.]com
- pocketfolio[.]com
- selfmadewealth[.]net
- onecoindebitcards[.]com
- onecoindebitcard[.]com
- onecoincreditcards[.]com
- onecoinmerchants[.]com
- onecoinmerchant[.]com
- omniacoins[.]com
- knowledgebusiness[.]com

IP Addresses the Domain IoCs Resolved To

- 52[.]58[.]78[.]16
- 195[.]20[.]55[.]179
- 54[.]39[.]78[.]148

Domains That Shared the IoCs' IP Hosts

- a2a4yw[.]ga
- a2om64[.]ga
- a70i2[.]gq
- abahasoxov[.]cf
- abandoned104[.]ga
- abduganiev[.]ml
- abehysaboqivilo[.]ml
- abezobuxix[.]ga
- abfilajase[.]ga
- abinitcommie[.]gq
- abirvan[.]ml
- abitganbove[.]gq
- abmercanonis[.]cf
- abrinqs[.]gq
- abshar[.]cf
- abunimyvysol[.]ga

- abusomexne[.]ml
- acapprovim[.]ml
- acawedebikuguci[.]ml
- acayiwuzecocuzi[.]gq
- acayulemysobyve[.]cf
- accountalerto2a[.]cf
- acehiqupug[.]cf
- acfiticrema[.]gq
- acincetca[.]ml
- acinev[.]gq
- acitoltravri[.]ga
- acizredmingwolf[.]gq
- acmantho[.]ga
- acodstuppomvict[.]cf
- acolutuborix[.]cf
- acovfo[.]gq
- acperroen[.]gq
- acsterporapicsand[.]gq
- activity-mobilelegendsproject562[.]gq
- actwinterrauthic[.]ga
- acwangolfwracfo[.]ga
- acwogo[.]ga
- ad94iwipux[.]ga
- ada004[.]ga
- adaberrega[.]gq
- adamtnx-zone[.]ga
- adanefab[.]ml
- adattronrop[.]cf
- adcnkcfu[.]ml
- adcresnycyguc[.]ml
- adesgoo[.]gq
- adetawymyvav[.]ga
- adethcajam[.]ml
- adflexchiefifa[.]gq
- adigactodi[.]gq
- adinat[.]gq
- admenfo[.]ml
- admin-recovery-1000000123459869586800003 57[.]ml
- admirandga[.]cf
- adobe2020[.]cf
- adolopeeroooswe[.]cf
- adonepeq[.]ga
- adonosalor[.]gq
- adoodssq[.]ga
- adpatirella[.]cf
- adqwedqwd[.]ga
- adrarona[.]ga
- adrehsonbekend[.]cf
- adtybomma[.]ml
- adulenbio[.]ga
- adultwaterslidedyr[.]ml
- adunlebir[.]ga
- adylamsnot[.]ga
- adymawic[.]gq
- aestroburger[.]ga
- afekiguqal[.]cf
- afertala[.]ga
- afexcatinum[.]ga
- afexemit[.]gq
- affixationej[.]ga
- afigatonil[.]ga
- aflamnews[.]ga
- afodedomaf[.]cf
- afohifileg[.]ml
- africare[.]gq
- afunewbritex[.]cf
- afuricymapir[.]cf
- afybogohyful[.]ml
- afyricitif[.]gq
- agalfloun[.]cf
- agamobafovoh[.]ml
- agangeptiging[.]cf
- agct[.]ml
- agedifegusyko[.]cf

- agerdo[.]ml
- aggonxiacocan[.]ml
- aggregate654dr[.]cf
- agifuk[.]ml
- agiyygelykujac[.]ga
- agohahuquj[.]ga
- agrisecurv-supc[.]ml
- agtonade[.]cf
- agtrujzelecsa[.]cf
- agynzamisuszo[.]gq
- ahagigidan[.]gq

Domains That Contained the Same Strings or String Combinations as the IoCs

- onedrive[.]ro
- onedrive[.]ca
- onedrive[.]jp
- onedrive[.]es
- onedrive[.]us
- onedrive[.]be
- onedrive[.]no
- onedrive[.]la
- onedrive[.]by
- onedrive[.]mx
- onedrive[.]ee
- onedrive[.]pm
- onedrive[.]to
- onedrive[.]cm
- onedrive[.]fi
- onedrive[.]xn--vuq861b
- onedrive[.]me
- onedrive[.]ie
- onedrive[.]hu
- onedrive[.]pw
- onedrive[.]fr
- onedrive[.]cn
- onedrive[.]pt
- onedrive[.]in
- onedrive[.]sc
- onedrive[.]dk
- onedrive[.]ir
- onedrive[.]io
- onedrive[.]ru
- onedrive[.]ai
- onedrive[.]xn--tckwe
- onedrive[.]do
- onedrive[.]gr
- onedrive[.]sk
- onedrive[.]tw
- onedrive[.]cl
- onedrive[.]su
- onedrive[.]co
- onedrive[.]eu
- onedrive[.]tv
- onedrive[.]cz
- onedrive[.]it
- onedrive[.]pl
- onedrive[.]hn
- onedrive[.]uk
- onedrive[.]tk
- onedrive[.]nl
- onedrive[.]ae
- onedrive[.]at
- onedrive[.]sg
- onedrive[.]ge
- onedrive[.]se
- onedrive[.]nu
- onedrive[.]de
- onedrive-onedriveadmin[.]net
- onedrivefiles-onedrive[.]com

- onedrivee[.]ml
- onedrive[.]org
- onedrivel[.]ga
- onedriver[.]tk
- onedrive[.]wtf
- onedrive[.]lol
- onedrives[.]ru
- onedrive[.]top
- onedrive[.]ooo
- onedrive[.]ovh
- monedrive[.]cf
- onedriver[.]ch
- onedrive7[.]tk
- onedrive[.]run
- onedriver[.]fr
- onedriver[.]es
- gonedrive[.]tk
- onedrivel[.]pw
- onedriven[.]us
- onedrives[.]it
- onedrive[.]one
- onedrive[.]xin
- onedrive[.]dev
- onedriver[.]gq
- onedrivex[.]ml
- onedrives[.]cf
- zonedrive[.]ru
- onedrive[.]sbs
- onedriver[.]kz
- xn--onedrve-cza[.]com
- onedrive[.]cab
- xn--oedrive-p13c[.]com
- xn--oedrive-kkb[.]com
- monedrive[.]gq
- onedrive[.]how
- onedrive[.]ren
- onedrivee[.]us
- monedrive[.]tk
- xn--onedrve-kza[.]com
- xn--onedrve-vfb[.]com
- onedrive[.]tel
- onedrive[.]pet
- onedrive[.]xyz
- onedriver[.]dk
- onedrive[.]moe
- onedrive7[.]ru
- onedrive[.]ltd
- onedrive[.]fun
- onedriver[.]pw
- onedrive[.]red
- onedriver[.]de
- onedrives[.]me
- onedrivex[.]ru
- onedrivet[.]pw
- onedriver[.]ru
- onedriven[.]me
- onedriven[.]tk
- xn--ondrive-ss4c[.]com
- onedriver[.]ec
- onedrive4[.]us
- onedrives[.]co
- xn--nedrive-k0a[.]com
- onedrive[.]pub
- onedrive[.]app
- conedrive[.]co
- onedrive[.]biz
- onedrive[.]cam
- onedriver[.]pt
- monedrive[.]ml
- zonedrive[.]su
- onedrive[.]fit
- onedrive[.]pro
- onedrives[.]cc
- xn--ondriv-cpce[.]com
- onedrives[.]ca
- monedrive[.]ga

- xn--onedriv-xya[.]com
- xn--onedrve-3ya[.]com
- onedrive[.]vip
- onedrive4[.]me
- onedrivep[.]pw
- onedrive[.]kim
- onedrives[.]nl
- onedrive[.]com
- conedrive[.]us
- onedrives[.]us
- onedriver[.]co
- onedrives[.]cn
- onedrive[.]ink
- onedrives[.]tk
- onedrive[.]sex
- onedrive5[.]ru
- conedrive[.]cn
- onedrivee[.]tk
- onedrive[.]net
- onedrive1[.]ru
- onedriver[.]it
- onedrive[.]uno
- onedriver[.]ga
- onedrivefolders-onedrive[.]com
- 1onedrive[.]org
- onedrivepe[.]ga
- dronedrive[.]ru
- onedrive1[.]xyz
- onedrivee[.]icu
- clonedrive[.]ru
- rwonedrive[.]cf
- onedriven[.]org
- ononedrive[.]tk
- lonedrive[.]com
- onedriver[.]one
- zonedrive[.]com
- onedrive[.]pics
- uonedrive[.]com
- onedrive[.]land
- wonedrive[.]biz
- onedrivebn[.]tk
- phonedrive[.]nl
- onedrive[.]qpon
- dronedrive[.]kr
- zonedriver[.]su
- onedrivex1[.]ru
- onedriver[.]cab
- onedriveau[.]ml
- onedriveau[.]tk
- onedrivean[.]pw
- onedrives[.]com
- onedrive[.]guru
- onedrive[.]game
- onedrive1[.]top
- onedriveap[.]pw
- onedrivens[.]pw
- onedrive[.]mobi
- lsonedrive[.]tk
- bonedriven[.]ph
- tonedrive[.]com
- onedrive[.]team
- onedrive[.]best
- onedrive[.]plus
- onedrivepe[.]gq
- onedriveds[.]cf
- onedrive[.]asia
- onedrive4[.]com
- onedrivez7[.]tk
- onedriveai[.]pw
- onedrivevn[.]co
- onedrive[.]tips
- onedrive25[.]ru
- onedrivebc[.]ml
- onedrive[.]porn
- myonedrive[.]us
- zonedriver[.]ru

- dronedrive[.]eu
- onedrive[.]menu
- onedrivesd[.]tk
- onedrive[.]fail
- onedrive[.]limo
- onedrive[.]name
- aonedrive[.]com
- onedrive[.]chat
- onedriver[.]fun
- zonedrive[.]org
- s-onedrive[.]tk
- nonedrive[.]xyz
- onedriveuk[.]tk
- onedriveaq[.]pw
- onedriveac[.]pw
- onedrivel[.]com
- bonedrive[.]com
- onedrive[.]show
- onedrive4[.]biz
- onedrive[.]tech
- zonedriver[.]tk
- gonedrive[.]com
- clonedrive[.]de
- onedrivers[.]ml
- onedriveeu[.]gq
- zonedrive[.]net
- onedrivepe[.]cf
- onedrivebn[.]cf
- onedriver[.]net
- onedrive[.]news
- ononedrive[.]gq
- onedriver[.]com
- onedrive[.]site
- onedrivenw[.]ml
- onedriver[.]biz
- onedriveuk[.]cf
- onedrivebn[.]gq
- onedriveus[.]tk
- onedrivee[.]net
- onedrivex7[.]ru
- onedrivern[.]pw
- onedrive3[.]top
- phonedrive[.]fr
- onedriverl[.]pw
- onedrive[.]work
- onedrives[.]pro
- wonedrive[.]org
- honedrive[.]com
- onedrivebn[.]ml
- onedrivebc[.]ga
- onedrivenz[.]ga
- onedrivepe[.]ml
- onedriveeu[.]cf
- onedrive[.]auto
- onedrive[.]gold
- fonedrive[.]com
- dronedrive[.]tk
- ponedrive[.]com
- onedrivesd[.]ml
- onedrive[.]info
- onedrivex5[.]ru
- myonedrive[.]nl
- eonedrive[.]com
- myonedrive[.]gq
- onedrivenz[.]ml
- xonedrive[.]com
- onedrive[.]camp
- donedrive[.]com
- onedrivers[.]tk
- onedrivez[.]com
- econedrive[.]fr
- dronedrive[.]it
- onedrive[.]host
- onedriveeu[.]ml
- onedrivex6[.]ru
- onedrives[.]app

- onedrivepe[.]tk
- conedrive[.]net
- onedrivers[.]ga
- onedrivee[.]xyz
- onedrive[.]buzz
- onedriven[.]net
- clonedrive[.]ir
- onedrives[.]net
- onedrivep[.]fun
- onedriveau[.]gq
- onedrivevn[.]ga
- onedriveuk[.]ml
- onedrivenz[.]tk
- msonedrive[.]at
- onedrivead[.]pw
- myonedrive[.]ph
- onedrived[.]xyz
- myonedrive[.]ml
- sonedrive[.]com
- onedrive[.]wang
- wonedrive[.]net
- s-onedrive[.]ml
- cnonedrive[.]ga
- onedrivee[.]org
- 5onedrive[.]com
- onedrive3[.]com
- nonedrive[.]com
- onedrives[.]top
- onedrive[.]fans
- onedriveau[.]cf
- onedrivevn[.]ml
- wonedrive[.]com
- onedrivee[.]biz
- monedrive[.]com
- myonedrive[.]ga
- 1onedrive[.]com
- ononedrive[.]cf
- conedrive[.]com
- onedrive[.]live
- onedrivevn[.]gq
- onedrivems[.]pw
- phonedrive[.]ru
- onedrivemb[.]pw
- onedriveds[.]ga
- onedrive[.]love
- onedrivee[.]com
- clonedrive[.]tk
- ononedrive[.]ml
- onedrivex[.]com
- onedrive[.]casa
- onedrivew[.]com
- onedrive[.]help
- onedriveds[.]tk
- onedriveal[.]pw
- onedrivevn[.]tk
- onedriveau[.]ga
- phonedrive[.]ga
- msonedrive[.]ml
- onedrive[.]club
- onedrive[.]wiki
- s-onedrive[.]ga
- ronedrive[.]com
- onedriver[.]org
- onedrivev[.]com
- onedrivebn[.]ga
- onedrivebc[.]cf
- onedriverv[.]pw
- onedrive[.]link
- ionedrive[.]com
- onedrive[.]life
- onedrivex[.]xyz
- onedrives[.]xyz
- onedrivecn[.]cn
- dronedrive[.]pl
- phonedrive[.]ml
- onedrivess[.]pw

- onedrives[.]biz
- onedriver[.]ovh
- zonedriver[.]us
- onedrivex3[.]ru
- phonedrive[.]cf
- onedrivebc[.]gq
- myonedrive[.]cf
- onedrive[.]blog
- onedrives[.]org
- nonedrive[.]net
- aonedriver[.]ca
- onedriver[.]app
- onedriver[.]top
- onedriveds[.]ml
- onedrivex9[.]ru
- onedrivem[.]com
- onedriveeu[.]ga
- onedrivevn[.]cf
- onedrivec[.]com
- phonedrive[.]ir
- onedriver[.]xyz
- onedriven[.]com
- onedrivem[.]xyz
- dronedrive[.]co
- onedrivecf[.]cf
- onedrive[.]shop
- onedrived[.]com
- oonedrive[.]com
- onedrive4business-onedrive[.]com
- kbonedrive[.]com
- onedrive[.]sucks
- onedriveps[.]fun
- onedrivems[.]com
- onedrivepro[.]nl
- grponedrive[.]ml
- onedrive[.]audio
- onedriverv[.]fun
- hronedrive[.]com
- onedrivene[.]icu
- fonedriver[.]com
- onedrive[.]store
- onedrive365[.]de
- bhonedrive[.]com
- onedrivedoc[.]us
- stonedrives[.]uk
- onedriveyun[.]tk
- onedrives19[.]ml
- onedrive1[.]tech
- onedrive-cn[.]cf
- onedrive-x7[.]ru
- wonedrives[.]net
- onedrive[.]co[.]ke
- onedriveaus[.]tk
- onedriveuk[.]top
- honedriven[.]com
- onedrive5t[.]com
- onedrives[.]host
- onedrivego[.]com
- onedrive-x3[.]ru
- msonedrive[.]icu
- onedriveapp[.]me
- onedriver0[.]xyz
- royonedrive[.]tk
- onedriveto[.]com
- onedrive423[.]ga
- lonedrivers[.]tk
- onedrives[.]live
- onedrivelr[.]top
- onedrive5t[.]top
- msonedrive[.]com
- onedrivee[.]live
- onedriveie[.]com
- onedriveos[.]fun
- onedrive897[.]tk
- onedrive[.]pp[.]ua
- myonedrive[.]net

- onedrivees[.]icu
- onedrive1x[.]xyz
- oneonedrive[.]co
- zonedriver[.]org
- wonedrives[.]biz
- onedrivedvr[.]ru
- onedrivesg[.]top
- msnonedrive[.]ru
- onedrive[.]gripe
- onedrivedoc[.]cf
- myonedrive[.]org
- clonedrive[.]net
- onedrive423[.]ml
- onedrive010[.]tk
- iphonedrive[.]nl
- newonedrive[.]pt
- onedrivecli[.]gq
- aonedriver[.]com
- onedrivedoc[.]ml
- aonedrivers[.]ca
- onedriverv[.]com
- zonedrive[.]info
- onedrivevn[.]top
- onedriveaus[.]ga
- aonedrives[.]com
- ononedrive[.]org
- onedrive[.]co[.]nz
- ozonedrive[.]com
- onedriveee[.]com
- nonedriver[.]com
- inonedrive[.]com
- onedrivebm[.]icu
- onedrive365[.]ca
- conedrivee[.]com
- onedriveis[.]fun
- atonedrive[.]com
- onedrivenp[.]top
- ecoonedrive[.]vg
- 5gonedrive[.]com
- onedrivee[.]host
- onedrive[.]email
- onedrive[.]media
- onedrivejo[.]com
- onedrivepan[.]gq
- dronedriver[.]ru
- onedrive-co[.]ml
- onedriveoff[.]ml
- proonedrive[.]uk
- onedrivecdn[.]tk
- onedrive[.]click
- gzonedrive[.]com
- onedrivevn[.]xyz
- onedrivehk[.]com
- msonedrive[.]top
- i-onedrive[.]xyz
- onedrive[.]house
- onedrivers[.]xyz
- zonedriver[.]com
- onedrive[.]group
- wonedrives[.]com
- iconedrive[.]com
- zonedriver[.]net
- phonedrive[.]com
- tonedriven[.]com
- onedrivesp[.]com

Malicious Domains Containing Similar Strings or String Combinations as the IoCs

- ewiner[.]store
- mywinstore[.]ru
- howstores[.]win
- winskin[.]store
- com-win[.]store
- darwinn[.]store
- fly-store[.]win
- winkzstore[.]com
- wf-restore[.]win
- snowings[.]store
- mswindstore[.]xyz
- goodwinjp[.]store
- twinstoresz[.]com
- restore-win[.]com
- window-store[.]ru
- windowstore[.]xyz
- baldwinstore[.]xyz
- windsoestore[.]com
- adbeadsstore[.]win
- micwindstore[.]xyz
- wingatestore[.]com
- winplaystore2[.]ga
- windowstore[.]live
- windowshop[.]store
- softwindstore[.]xyz
- storesd-apple[.]win
- winashopcam[.]store
- stores-icloud[.]win
- amazing-win[.]store
- verdictwing[.]store
- wingclaimstore[.]xyz
- swisswinners[.]store
- shapkiwinter[.]store
- winstoreonline[.]com
- windowsfanstore[.]ga
- wintriprodiet[.]store
- winnerstorey[.]racing
- windowsappstore[.]net
- onedrive[.]pw
- xn--onedrve-cza[.]com
- onedriven[.]tk
- ononedrive[.]gq
- msonedrive[.]at
- onedriver[.]xyz
- dronedrive[.]co
- onedrivenus[.]uk
- onedrivee[.]info
- onedrives[.]site
- gkonedrive[.]xyz
- onedrivelive[.]nl
- onedriveaus[.]icu
- myonedrive[.]live
- onedrive-pdf[.]ga
- onedrivemsw[.]bid
- onedrivers[.]live
- onedrivesave[.]gq
- onedrivefile[.]tk
- phonedriven[.]com
- onedrive0000[.]cf
- phonedrivers[.]ru
- onedrivenet[.]xyz
- onedrivemail[.]gq
- onedrive-ms[.]com
- onedrive-eu[.]com
- onedrivedocs[.]xyz
- onedrivesales[.]tk
- onedriveinc[.]info
- onedrive-pl[.]cyou
- onedriveflow[.]com
- int-onedrive[.]com
- onedrivefile[.]xyz
- onedrivecom[.]live
- onedriveview[.]com
- m365onedrive[.]com
- onedrivemail[.]xyz
- onedrivemgb[.]live

- onedrive-cn[.]live
- onedrivelive[.]org
- onedrive-sdn[.]com
- onmsonedrive[.]com
- onedrivedrive[.]ml
- onedriver-srv[.]ml
- mcsftonedrive[.]org
- lusrionedrive[.]com
- onedriveadmin[.]pro
- onedrivems[.]online
- onedriveonline[.]tk
- onedrivefiles[.]icu
- onedrivelogin[.]app
- onedrive-login[.]tk
- cloudonedrive[.]com
- onedrive-folder[.]cf
- onedrive-asia[.]cyou
- officeonedrive[.]xyz
- onedrive-lives[.]com
- onedriveservice[.]ga
- onedrivesharei[.]com
- trustonedrives[.]com
- onedrive-secure[.]tk
- theonedrive[.]online