Discovering Potential BEC Scam Vehicles through the DNS

Table of Contents

Executive Report

Threats tend to become more advanced over time. So is the case of business email compromise (BEC) scams, which according to a SlashNext post, cost companies billions of U.S. dollars in losses per year.

BEC scams are bound to continue affecting organizations worldwide, given the continued rise in the number of complaints the FBI IC3 receives with each passing year. But organizations can lessen their chances of ending up as victims by identifying potential threat vectors before they even get weaponized with the help of DNS tools. The following study by Mitiga on an advanced BEC scam targeting executives by exploiting a Microsoft 365 design flaw can demonstrate how.

Using the seven indicators of compromise (IoCs) identified in the report as expansion analysis jump-off points, we found an additional:

- Five IP addresses to which some of the IoCs resolved
- 761 domains that shared the IoCs' IP hosts, one of which turned out to be malicious
- 1,272 domains that contained ***foobar***, the company the BEC scammers spoofed in their campaign, eight of which turned out to be malware hosts
- 2,545 domains that contained ***docusign***, which the threat actors abused to supposedly host the document the victim needed to sign, 43 of which have been categorized as malicious by various malware engines
- 10,000 domains that contained **outlook**, which the threat actors abused to send out their BEC scam emails, 30 of which have been tagged as malware hosts

All these artifacts could serve as potential BEC scam vehicles specific to the featured campaign.

Uncovering Pertinent Details about the IoCs

The post about the recent BEC scam identified seven IoCs—four IP addresses and three domains, namely:

- 139[.]99[.]6[.]158
- 154[.]6[.]17[.]158
- 5[.]31[.]10[.]180
- 20[.]245[.]118[.]47
- awin1[.]com
- web[.]app
- lointree[.]com

WHOIS lookups for the three domains revealed that they were created between 2019 and 2022. Each domain registrant indicated a different country—the U.S. for web[.]app, the U.K. for awin1[.]com, and Iceland for lointree[.]com.

IP geolocation lookups, meanwhile, for the four IP addresses pointed to three countries—one (139[.]99[.]6[.]158) for Singapore, two (154[.]6[.]17[.]158 and 20[.]245[.]118[.]47) for the U.S., and one (5[.]31[.]10[.]180) for the U.A.E.

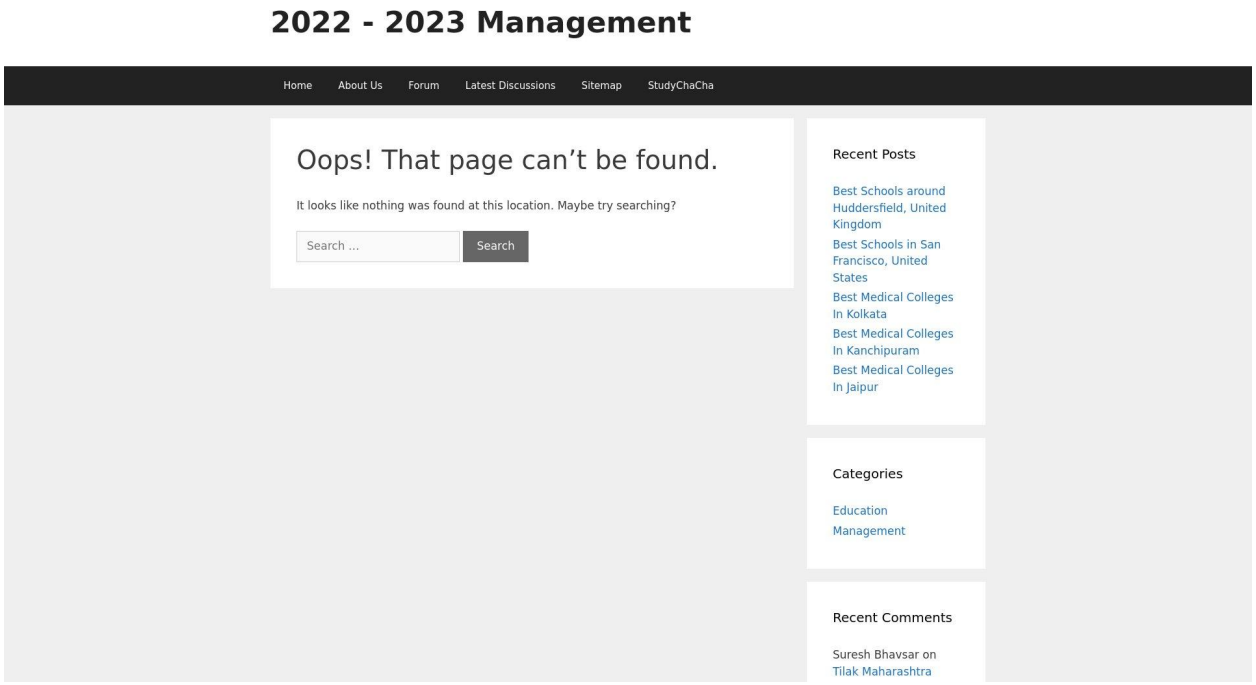
Identifying Other Potential Threat Vectors

We began our threat expansion by subjecting the three domains identified as IoCs to DNS lookups, which allowed us to identify five IP addresses that aren't part of the original IoC list, making our total number of IP hosts nine. All five additional IP addresses were geolocated in the U.S. like two of the IoCs.

Reverse IP lookups for the nine IP addresses revealed that three did not have resolutions, one was a dedicated host, and the remaining five were shared hosts. Said lookups also led to the discovery of 761 domains, one of which—01lvnohlp0n[.]info—turned out to be malicious.

The Mitiga analysis of the BEC scam stated the threat actors spoofed a company named Foobar in their campaign. We sought to identify how many existing domains contained the string ***foobar***, which may be weaponized for future use. Our Domains & Subdomains Discovery search uncovered 1,272 domains, eight of which turned out to be malware hosts. Three of them are currently parked and available for purchase while one has already been purchased and is undergoing website development.

The in-depth threat analysis also mentioned the threat actors' use of DocuSign. A Domains & Subdomains Discovery search for domains containing the string ***docusign*** led to the discovery of 2,545 domains, 43 of which have been categorized as malicious. Only one—docusignbusiness[.]com—continued to host live content despite the appearance of an error message regarding a specific page.

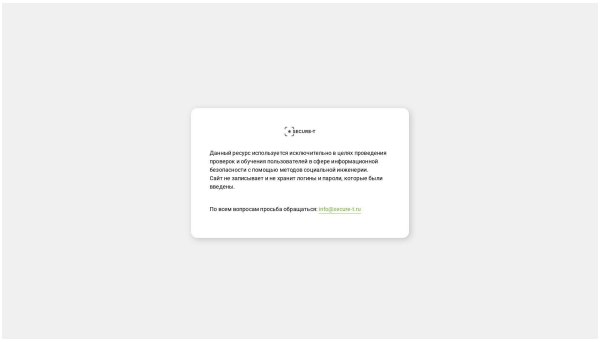


Screenshot of docusignbusiness[.]com

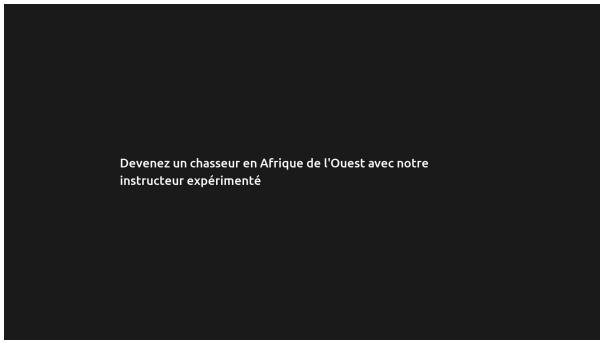
In addition, only 100 of the ***docusign***-containing domains could be publicly attributed to DocuSign, Inc. The remaining 2,445 domains could be cybersquatting and serve as potential hosts for supposed documents the victims need to sign that are actually malware.

The BEC scammers also reportedly abused Outlook 365 in their campaign. Another Domains & Subdomains Discovery search for domains containing the string ***outlook*** gave us a list of at least 10,000 domains, 30 of which have already been tagged as malicious. Specifically, 22 of the domains were malware hosts while the remaining eight were spam senders.

Very few of the malicious pages, such as outlook-team[.]ru and o365-outlook[.]com, remained accessible. Take a look at their screenshots below.

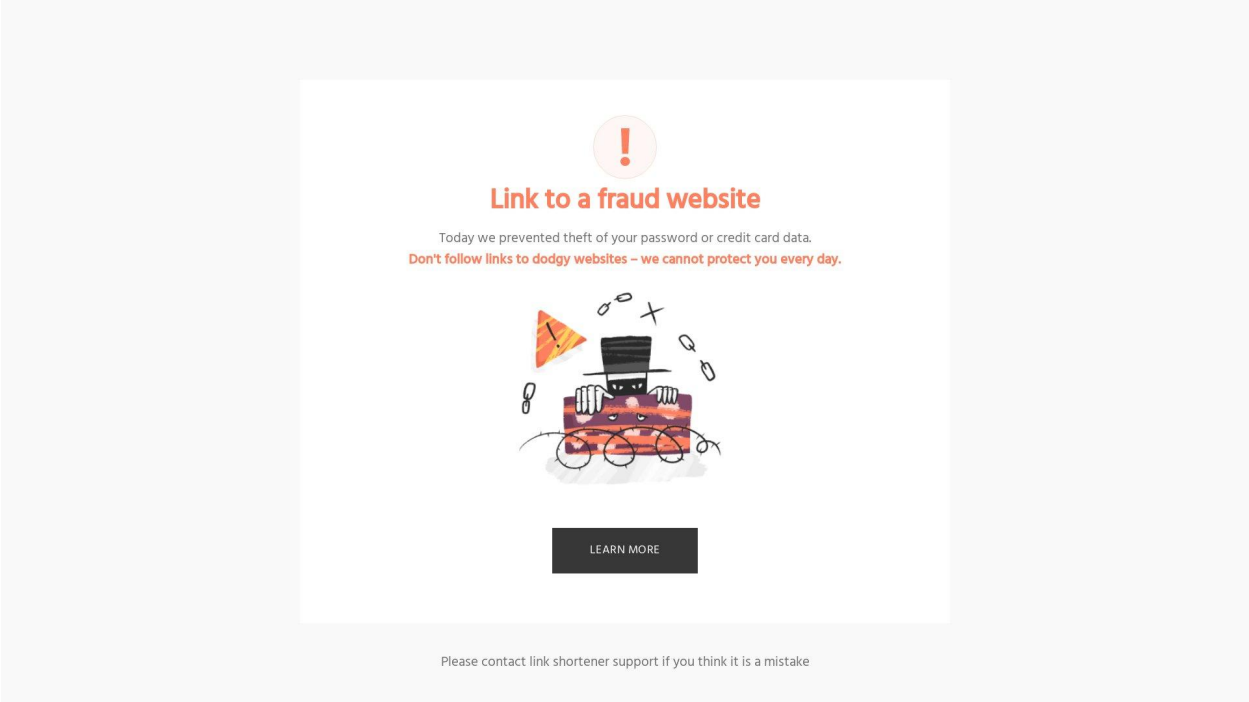


Screenshot of outlook-team[.]ru



Screenshot of o365-outlook[.]com

The third live malicious website—outlooklive[.]org—showed a warning page to potential visitors.



Screenshot of outlooklive[.]org

Additionally, only 117 of them could be publicly attributed to Microsoft. As such, threat actors could be using the remaining 9,883 domains to spoof legitimate companies using Outlook 365 for their BEC scams.

—

The domains that resulted from our IoC expansion could serve as potential BEC scam or phishing vectors that could be closely monitored for signs of suspicious activity.

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 That Shared Some of the IoCs' IP Hosts

- activefortress[.]com
- actrailersales[.]com
- adherocreative[.]com
- adkautumnfest[.]com
- adult69[.]app[.]link
- agavesociety[.]org
- alexjohn[.]link
- amandasstylebox[.]com
- amyswreaths[.]com
- analytics[.]rc4[.]note[.]com
- app[.]link
- appdim[.]com
- appspace9[.]com
- ari4l[.]app[.]link
- artbueno[.]com
- asmscript[.]xyz
- aswaaqgroup[.]surveysparrow[.]com
- attorneysusanoneal[.]com
- atzenhofferchevroletcadillac[.]com
- austinfulfillmentservices[.]com
- autobrowsers[.]net
- bb-pbc[.]mainroll[.]com
- beachguide[.]com
- benspottsbaseballcamps[.]com
- bestgiclinic[.]com
- bestplay88[.]xyz
- bl00m[.]co[.]uk
- bonusstoreexpress[.]com
- briannephotography[.]com
- bvrcs[.]app[.]link
- camtacan[.]com
- capitalfinancialregistration[.]com
- capitalnortherm[.]com
- careington500[.]net
- cc713c3a08aa473186b27b73aa55c856[.]cdomain[.]eu[.]itglue[.]com
- ccacwildcats[.]com
- ceicdata[.]com[.]hk
- chalkbeat[.]org
- chipestimate[.]org
- chrgup[.]io
- citysearch[.]com
- ck9hb[.]app[.]link
- click[.]15[.]delivery-chat-webview[.]bancointer[.]com[.]br
- clientportal[.]com
- cloudenly[.]com
- code1[.]paidvideocall[.]com
- codecat[.]shiftyhosting[.]com
- consultortrabalhista[.]com
- content[.]jpbooks[.]dev[.]nola-novel[.]com
- coziment[.]com
- craglify[.]com
- cresh[.]eu
- cuotasya[.]com
- d100jgbnjzmdv8[.]cloudfront[.]net
- d112qfbwadb3fn[.]cloudfront[.]net
- d11b3t5pow4ul5[.]cloudfront[.]net
- d11q8tb9qqr2lc[.]amplifyapp[.]com
- d11sxyoidq7egk[.]cloudfront[.]net
- d1342q7a08m7p3[.]cloudfront[.]net
- d13c7vv9s9gq96[.]cloudfront[.]net
- d15n1sls9pox8s[.]cloudfront[.]net

- d15t62zd1oya9g[.]cloudfront[.]net
- d15xre44fy3mdd[.]amplifyapp[.]com
- d16lr9u2n448hl[.]cloudfront[.]net
- d190f2pta1mwiw[.]cloudfront[.]net
- d19vqlxqcn3qsm[.]cloudfront[.]net
- d1aokzo5fveb53[.]cloudfront[.]net
- d1b25k8kmeefh2[.]cloudfront[.]net
- d1bngyt4qt6rm7[.]cloudfront[.]net
- d1d2qxgc5id4ge[.]cloudfront[.]net
- d1g2z620vyegl[.]cloudfront[.]net
- d1g4pmd66lwvwa[.]cloudfront[.]net
- d1gctvezfaa7it[.]cloudfront[.]net
- d1ggelqs9uz2n3[.]cloudfront[.]net
- d1gr0skykhkgkn[.]cloudfront[.]net
- d1gspfi9baxjaf[.]amplifyapp[.]com
- d1ilqbrrmeamck[.]cloudfront[.]net
- d1j6adv2fyge1t[.]cloudfront[.]net
- d1j99felrg6ka5[.]cloudfront[.]net
- d1ka64kmk3gx8q[.]cloudfront[.]net
- d1kefdaf6aet71[.]cloudfront[.]net
- d1kk7fxlt51jnm[.]cloudfront[.]net
- d1l32w8uvt14xy[.]cloudfront[.]net
- d1lmgk1bo4rsm9[.]cloudfront[.]net
- d1mb00r4rii9gb[.]cloudfront[.]net
- d1nwn1ue14gugb[.]cloudfront[.]net
- d1pwqqlyj1p4qh[.]cloudfront[.]net
- d1q6fcm2jqtj6r[.]cloudfront[.]net
- d1r66rke5dnyyg[.]cloudfront[.]net
- d1rw9nlgqq5ud2[.]cloudfront[.]net
- d1tdr53jb3ioeg[.]cloudfront[.]net
- d1ten4zq11dyzt[.]cloudfront[.]net
- d1w3gipqgli5xv[.]cloudfront[.]net
- d1whvokbqwjvf8[.]amplifyapp[.]com
- d1x9f7lsttbvmd[.]amplifyapp[.]com
- d1zvj6e1muw0v8[.]cloudfront[.]net
- d20tf7a9jedr93[.]cloudfront[.]net
- d21uzddoxtcip2[.]cloudfront[.]net
- d23pz3ig9khf3z[.]cloudfront[.]net
- d24alfwkr0j9al[.]cloudfront[.]net

Sample Domains Containing the String *foobar*

- foobarfoobar[.]xyz
- foobarfoobar[.]com
- foobar[.]rs
- foobar[.]me
- foobar[.]nu
- foobar[.]su
- foobar[.]co
- foobar[.]af
- foobar[.]be
- foobar[.]ee
- foobar[.]ca
- foobar[.]at
- foobar[.]sk
- foobar[.]de
- foobar[.]hu
- foobar[.]cd
- foobar[.]es
- xn--foobr-jra[.]ch
- foobar[.]xn--fiqs8s
- foobar[.]uk
- foobar[.]eu
- foobar[.]pw
- foobar[.]kr
- foobar[.]au
- foobar[.]cc
- foobar[.]cz
- foobar[.]ae
- foobar[.]tv
- foobar[.]xn--fiqz9s
- foobar[.]vc
- foobar[.]no
- foobar[.]to
- foobar[.]my
- foobar[.]si
- foobar[.]tk
- foobar[.]gg

- foobar[.]io
- foobar[.]nz
- foobar[.]fr
- foobar[.]in
- foobar[.]is
- foobar[.]cx
- foobar[.]gr
- foobar[.]tw
- foobar[.]cn
- foobar[.]it
- foobar[.]lu
- foobar[.]li
- foobar[.]fi
- foobar[.]se
- foobar[.]ga
- foobar[.]bz
- foobar[.]ws
- foobar[.]im
- foobar[.]sh
- foobar[.]nl
- foobar[.]st
- foobar[.]ru
- foobar[.]lv
- foobar[.]ro
- xn--foobr-jra[.]de
- foobar[.]cl
- foobar[.]dk
- foobar[.]us
- foobar[.]pl
- foobarbazfoobarbaz[.]xyz
- foobars[.]nl
- foobar[.]bet
- foobar[.]nyc
- foobars[.]jp
- foobar[.]top
- foobar[.]xin
- foobar[.]cat
- foobars[.]in
- ufoobar[.]xn--fiqz9s
- foobar[.]icu
- foobar[.]cam
- foobar2[.]de
- foobar[.]cfd
- foobar[.]ltd
- foobar[.]rip
- foobard[.]me
- foobar[.]one
- foobar[.]bid
- foobar[.]lol
- foobar[.]wtf
- foobar1[.]de
- foobar[.]run
- foobard[.]it
- foobar[.]net
- ifoobar[.]no
- foobar[.]ovh
- foobars[.]co
- foobar[.]win
- foobar[.]app
- foobarr[.]io
- foobar4[.]de
- foobar[.]dev
- foobar3[.]de
- kfoobar[.]se

Sample Malicious *foobar*-Containing Domains

- foobarbuz[.]com
- foobarinc[.]xyz
- foobarpig[.]top
- iknowfoobar[.]uk

Sample Domains Containing the String *docusign*

- docusign[.]cf
- docusign[.]at

- docusign[.]ci
- docusign[.]xn--kprw13d
- docusign[.]io
- docusign[.]ps
- docusign[.]tv
- docusign[.]lc
- docusign[.]dk
- docusign[.]nl
- docusign[.]ar
- docusign[.]eu
- docusign[.]bo
- docusign[.]tl
- docusign[.]gf
- docusign[.]ch
- docusign[.]cd
- docusign[.]am
- docusign[.]be
- docusign[.]no
- docusign[.]mx
- docusign[.]cc
- docusign[.]it
- docusign[.]ht
- docusign[.]se
- xn--dcusign-py4c[.]xn--fiqz9s
- docusign[.]dm
- docusign[.]in
- docusign[.]mn
- docusign[.]pt
- docusign[.]la
- docusign[.]id
- docusign[.]so
- docusign[.]ee
- docusign[.]af
- docusign[.]fm
- docusign[.]hk
- docusign[.]tk
- docusign[.]sk
- docusign[.]us
- docusign[.]sl
- docusign[.]cr
- docusign[.]ai
- docusign[.]ug
- docusign[.]dj
- docusign[.]ws
- docusign[.]je
- docusign[.]et
- docusign[.]gg
- docusign[.]xn--mxtq1m
- docusign[.]cz
- docusign[.]li
- docusign[.]mu
- docusign[.]es
- docusign[.]nu
- docusign[.]cm
- docusign[.]sc
- docusign[.]bi
- docusign[.]cn
- docusign[.]lt
- docusign[.]su
- docusign[.]xn--node
- docusign[.]sg
- docusign[.]ms
- docusign[.]kg
- docusign[.]cx
- docusign[.]lk
- docusign[.]ae
- docusign[.]ag
- docusign[.]tw
- docusign[.]de
- docusign[.]sx
- docusign[.]co
- docusign[.]ca
- docusign[.]by
- docusign[.]jp
- docusign[.]sn
- docusign[.]uz
- docusign[.]gr
- docusign[.]lu
- docusign[.]xn--fiqs8s
- docusign[.]rs

- docusign[.]uk
- docusign[.]nz
- docusign[.]uy
- docusign[.]qa
- docusign[.]ly
- docusign[.]hn
- docusign[.]kz
- docusign[.]im
- docusign[.]ie
- docusign[.]ng
- docusign[.]xn--fiqz9s
- docusign[.]ro
- docusign[.]pe
- docusign[.]gy
- docusign[.]gl
- docusign[.]me
- docusign[.]pl
- docusign[.]pw

Sample Malicious *docusign*-Containing Domains

- ydocusign[.]ml
- xn--docusgn-vfb[.]com
- docusignoi[.]cf
- gdocusign[.]com
- docusignoi[.]gq
- docusign-sa[.]us
- docusignin[.]xyz
- docusigndoc[.]co
- docusign[.]cloud
- docusigns[.]club
- docusignme[.]com
- docusigntur[.]cf
- docusignwork[.]ml
- docusign[.]net[.]in
- sbadocusign[.]com
- docusigncxie[.]ml
- docusigndaps[.]ml
- docusignapp[.]org
- usdocusign[.]info
- docusigntwo[.]com
- docusignusa[.]com
- prodocusign[.]com

Sample Domains Containing the String *outlook*

- outlookoutlook[.]pw
- outlook-outlook[.]de
- outlookoutlook[.]com
- outlook-outlooks[.]tk
- outlooksoutlook[.]com
- outlooksoutlooks[.]com
- pcoutlookoutlook[.]com
- outlookonoutlook[.]com
- outlookpcoutlook[.]com
- outlookoutlook365[.]com
- outlook[.]c
- outlook365outlook[.]com
- outlook[.]ro
- outlook[.]eu
- outlook[.]ms
- outlook[.]ma
- outlook[.]ax
- outlook[.]bz
- outlook[.]om
- outlook[.]pw
- outlook[.]ie
- outlook[.]jp
- outlook[.]tf
- outlook[.]ae
- outlook[.]la
- outlook[.]vg
- outlook[.]hk
- outlook[.]tl
- outlook[.]ao
- outlook[.]cc

- outlook[.]rs
- outlook[.]mx
- outlook[.]ge
- outlook[.]ee
- outlook[.]sg
- outlook[.]cn
- outlook[.]sc
- outlook[.]ws
- outlook[.]sk
- outlook[.]co
- outlook[.]do
- outlook[.]lt
- outlook[.]be
- outlook[.]fi
- outlook[.]ht
- outlook[.]xn--kprw13d
- outlook[.]im
- outlook[.]tn
- outlook[.]tc
- outlook[.]tk
- outlook[.]us
- outlook[.]hn
- outlook[.]xn--kpry57d
- outlook[.]gg
- outlook[.]sh
- outlook[.]uk
- outlook[.]nl
- outlook[.]hr
- outlook[.]nu
- outlook[.]mn
- outlook[.]ai
- outlook[.]re
- outlook[.]me
- outlook[.]xn--tckwe
- outlook[.]lv
- outlook[.]ca
- outlookstoreoutlook[.]com
- outlook[.]xn--fiqs8s
- outlook[.]ly
- outlook[.]cz
- outlook[.]ci
- outlook[.]ar
- outlook[.]tw
- outlook[.]lu
- outlook[.]ru
- outlook[.]fr
- outlook[.]am
- outlook[.]gs
- outlook[.]no
- outlook[.]pm
- outlook[.]md
- outlook[.]my
- outlook[.]ch
- xn--utlook-vxa[.]cf
- outlook[.]xn--vuq861b
- outlook[.]xn--fiqz9s
- outlook[.]gr
- outlook[.]cl
- outlook[.]is
- outlook[.]so
- outlook[.]cm
- outlook[.]by
- outlook[.]it
- outlook[.]su
- outlook[.]si
- outlook[.]to
- outlook[.]hu
- outlook[.]de
- outlook[.]pk
- outlook[.]bm
- outlook[.]li
- outlook[.]pl
- outlook[.]pt
- outlook[.]se
- outlook[.]es
- xn--outlk-muaa[.]de
- outlook[.]io
- outlook[.]dk
- outlook[.]tv
- outlook[.]kr

- outlook[.]in
- outlook[.]at
- outlook[.]bg
- outlookm[.]ca
- outlooke[.]ml
- outlook[.]cam
- moutlook[.]tk
- outlook2[.]me
- coutlook[.]co
- xn--utlook-hxa[.]xyz
- xoutlook[.]ga
- outlook1[.]gq
- xn--outlok-fxa[.]net
- outlooki[.]de
- outlooks[.]ru
- outlookk[.]gq
- outlooks[.]gq
- outlooke[.]de
- outlook1[.]ga
- moutlook[.]cn
- outlooke[.]gq
- xn--outlok-fxa[.]org
- outlookb[.]ml
- foutlook[.]ga
- zoutlook[.]tk
- outlookx[.]de
- outlook[.]onl
- xn--outook-5db[.]com
- outlooka[.]tk
- youtlook[.]me
- outlooke[.]tk
- outlooky[.]cf
- xn--otlook-3ya[.]net
- outlook[.]bio
- coutlook[.]cf
- xn--outlok-exa[.]com
- outlook2[.]ga
- outlook[.]net
- outlooks[.]tv
- aoutlook[.]es
- ooutlook[.]cf
- noutlook[.]tk
- outlook[.]ren
- outlook[.]dev
- poutlook[.]dk
- outlooks[.]me
- xn--otlook-pya[.]com
- outlooks[.]us
- outlook[.]com
- outlookk[.]es
- ioutlook[.]tk
- eoutlook[.]vg
- ioutlook[.]vg
- eoutlook[.]sk
- coutlook[.]ml
- eoutlook[.]cz
- outlook2[.]tk
- outlook[.]tel
- outlook1[.]ml
- outlook[.]org
- xn--outook-kcb[.]com
- outlook5[.]ga
- outlooku[.]me
- xn--utlook-hqc[.]net
- outlookk[.]tk
- foutlook[.]nl
- outlookk[.]co
- xoutlook[.]gq
- outlooks[.]eu
- xn--outlok-6wa[.]com
- outlooks[.]ch
- noutlook[.]cf
- xn--outlk-muaa[.]com
- outlooky[.]ga
- outlook[.]cat
- outlook2[.]ml
- outlook[.]nyc
- outlook4[.]ga
- outlookq[.]de
- outlook[.]llc

- outlook[.]srl
- houtlook[.]tk
- outlook[.]pub
- outlooks[.]ml
- outlooks[.]pw
- outlook1[.]tk
- xoutlook[.]cf
- outlook[.]how
- ooutlook[.]it
- outlookk[.]fr
- xn--outook-rq7b[.]com
- houtlook[.]fr
- outlook[.]xin
- ooutlook[.]fr
- outlook1[.]us
- outlook[.]bet
- outlook[.]one
- outlooks[.]at
- outlook[.]lol
- outlook[.]ist
- outlookb[.]ga
- outlook[.]gay
- moutlook[.]ml
- outlooks[.]de
- outlook[.]ink
- outlook[.]day
- xn--outlok-7wb[.]com
- outlook0[.]it
- xn--utlook-9wa[.]com
- ooutlook[.]tk
- outlook8[.]gq
- outlook7[.]gq
- outlookx[.]us
- xn--oulook-qkb[.]com
- outlook[.]fun
- xn--outlok-fxa[.]com
- outlook[.]con
- outlook[.]ooo
- outlooky[.]ml
- eoutlook[.]in
- outlook[.]app
- xn--utlook-9xa[.]com
- xn--outlok-mxa[.]com
- 9outlook[.]ca
- 5outlook[.]ca
- outlooks[.]uk
- outlookk[.]cm
- ioutlook[.]cn
- outlooka[.]ml
- outlooks[.]cf
- eoutlook[.]ru
- outlookk[.]it
- houtlook[.]it
- voutlook[.]cn
- outlook[.]xn--6qq986b3xl
- 1outlook[.]ru
- outlook2[.]uk
- outlookb[.]tk
- outlook1[.]uk
- outlook2[.]gq
- outlookc[.]ml
- boutlook[.]ga
- outlooks[.]it
- ooutlook[.]co
- outlook[.]lat
- outlook[.]bar
- outlooks[.]ga
- ioutlook[.]in
- xn--utlook-hxa[.]com
- outlook[.]sex
- outlooks[.]hk
- noutlook[.]ga
- outlooka[.]ae
- outlook2[.]ru
- outlooks[.]es
- houtlook[.]nl
- ioutlook[.]de
- outlook1[.]ru
- outlook9[.]cn
- outlooks[.]tk

- outlookk[.]me
- outlookl[.]it
- boutlook[.]tk
- xn--utlook-2wb[.]com
- outlookk[.]ml
- outlook[.]ovh
- outlookm[.]ml
- outlook[.]pro
- outlookk[.]ga
- outlook1[.]co
- soutlook[.]tk
- ooutlook[.]me
- outlooks[.]pl
- youtlook[.]us
- outlook[.]sbs
- outlook[.]red
- outlook[.]eus
- outlookt[.]de
- outlook[.]top
- outlookk[.]se
- outlooks[.]ir
- outlook3[.]ga
- outlookp[.]tk
- outlook[.]eco
- outlooky[.]gq
- outlooks[.]fr
- outlooks[.]nl
- poutlook[.]co
- loutlook[.]fr
- outlooks[.]ae
- houtlook[.]es
- outlookk[.]xn--node
- outlooko[.]th
- outlook[.]gal
- xn--utlook-ol8b[.]com
- outlook6[.]ga
- xn--outloo-1bb[.]com
- xn--utlook-hqc[.]com
- ioutlook[.]cm
- outlookk[.]in
- eoutlook[.]de
- outlook[.]xxx
- outlook[.]biz
- xn--outlok-exa[.]org
- woutlook[.]nl
- xn--outook-ycb[.]com
- outlook[.]mom
- outlook9[.]gq
- poutlook[.]cm
- outlooka[.]ph
- doutlook[.]co
- outlookl[.]fr
- moutlook[.]gq
- boutlook[.]gq
- xn--utlook-2wa[.]com
- outlooka[.]cf
- outlook[.]boo
- outlook1[.]de
- joutlook[.]pl
- outlook5[.]ru
- loutlook[.]cm
- xn--utlook-9fb[.]com
- houtlook[.]be
- aoutlook[.]de
- eoutlook[.]cn
- xoutlook[.]tk
- outlook[.]xyz
- outlook[.]icu
- outlook[.]nrw
- eoutlook[.]eu
- outlookk[.]cf
- outlooky[.]tk
- coutlook[.]ga
- outlook[.]fit
- zoutlook[.]cf
- ooutlook[.]ga
- noutlook[.]ml
- xn--utlook-oxa[.]com
- outlook[.]kim
- xn--oulook-j17b[.]com

- xn--otlook-iya[.]com
- outlook[.]new
- aoutlook[.]cn
- boutlook[.]ml
- outlook[.]vip
- outlook[.]frl
- outlooks[.]ca
- outlook03[.]cn
- outlook20[.]ca
- outlookk[.]app
- outlooks[.]fun
- xn--utlok-iuae[.]info
- hnoutlook[.]tw
- fxoutlook[.]ws
- woutlook[.]com
- outlookol[.]cn
- outlook[.]casa
- outlooksk[.]gq
- outlooks[.]one
- 78outlook[.]ws
- bhoutlook[.]us
- outlook[.]rest
- outlook24[.]de
- 40outlook[.]de
- outlookg[.]biz
- deoutlook[.]de
- outlooka[.]com
- outlooker[.]vg
- joutlook[.]com
- outlookexpresstooutlook[.]org
- scoutlook[.]ie
- rfoutlook[.]uk
- v-outlook[.]nl
- outlook21[.]ca
- outlook[.]page
- myoutlook[.]ch
- outlook3[.]com
- outlook[.]wiki
- outlooktv[.]ca
- 51outlook[.]cn
- outlookie[.]kr
- outlook[.]wang
- outlookpm[.]ca
- voutlook[.]com
- ooutlook[.]xyz
- outlookexpresstooutlook[.]net
- outlook24[.]dk
- outlook1[.]net
- outlookq[.]com
- outlook[.]comm
- outlookin[.]tk
- outlookb[.]com
- outlooki[.]top
- eoutlook[.]app
- houtlook[.]net
- outlooks[.]top
- outlook[.]name
- scoutlook[.]tv
- outlookco[.]kr
- 8outlook[.]com
- outlook[.]yoga
- gboutlook[.]co
- outlookv[.]com
- scoutlook[.]ca
- myoutlook[.]ir
- outlook[.]surf
- outlooktv[.]cn
- msoutlook[.]it
- outlook[.]info
- spoutlook[.]ga
- bdoutlook[.]es
- outlook2[.]xyz
- outlook[.]pink
- e-outlook[.]cz
- outlook4[.]xyz
- cloutlook[.]dk
- outlookx[.]com
- myoutlook[.]be
- outlook[.]mobi
- myoutlook[.]ga

- outlookcc[.]au
- hnoutlook[.]cn
- myoutlook[.]us
- 9outlook[.]com
- sdoutlook[.]cn
- outlook1[.]xyz
- troutlook[.]de
- outlook[.]band
- aboutlook[.]ru
- outlook[.]com3
- outlookz[.]xyz
- outlook[.]com0
- outlook2[.]com
- msoutlook[.]ms
- hroutlook[.]ca
- outlook[.]tech
- msoutlook[.]de
- outlook1[.]com
- myoutlook[.]tk
- myoutlook[.]de
- outlook88[.]cn
- 24outlook[.]us
- outlookm[.]org
- outlooked[.]ru
- outlook[.]kiwi
- outlooksw[.]uk
- rboutlook[.]be
- outlookis[.]ws
- outlook2[.]net
- cnoutlook[.]cn
- outlooks[.]biz
- outlook[.]sale
- outlookup[.]cn
- scoutlook[.]vg
- outlookde[.]ws
- outlooke[.]org
- doutlook[.]com
- goutlook[.]top
- outlook19[.]uk
- outlook[.]xn--com-9o0a
- outlookl[.]net
- outlookfp[.]uk
- outlooksa[.]tk
- m-outlook[.]es
- outlooks[.]icu
- gkoutlook[.]ru
- youtlook[.]net
- outlook[.]show
- outlook7[.]com
- scoutlook[.]co
- outlook[.]blue
- outlook5[.]com
- outlook5[.]net
- outlooksp[.]au
- outlookpc[.]ca
- outlookz[.]com
- outlook24[.]ch
- qoutlook[.]com
- outlookme[.]eu
- outlooki[.]com
- mioutlook[.]cl
- outlook5[.]org
- outlook24[.]cn
- hdoutlook[.]cn
- outlooker[.]in
- outlookk2[.]us
- toutlook[.]xyz
- cloutlook[.]nl
- msoutlook[.]cn
- outlook[.]scot

Sample Malicious *outlook*-Containing Domains

- outlook[.]sbs
- houtlook[.]es
- outlookl[.]com
- loutlook[.]com
- ssoutlook[.]ru
- 1outlook[.]com

- 11outlook[.]com
- outlookbox[.]me
- outlooks365[.]cz
- outlookpad[.]com
- outlookcdn[.]com
- outlook[.]nom[.]co
- outloutlook[.]com
- outlook-team[.]ru
- azureoutlook[.]cz
- outlooksslr[.]com