DNS情報からBECの潜在的媒体を発見

目次

要旨

脅威は、時間を追うごとに高度化する傾向にあります。SlashNextの記事によればビジネスメール詐欺（BEC）も同様で、年間数十億ドルの損失を企業に与えています。

FBIのInternet Crime Complaint Center（IC3）が受領する苦情件数が年々増加していることから、BECは今後も世界中のあらゆる組織に影響を与え続けるものと思われます。しかし、DNSツールの助けを借りて潜在的な脅威ベクトルを未然に特定すれば、組織は被害に遭うリスクを下げることができます。Microsoft 365の設計上の欠陥を悪用して企業の経営陣を攻撃した高度なBECについてMitigaが行った調査の報告に、その方法が示されています。

報告で特定された7つのセキュリティ侵害インジケーター（IoC）を出発点として、このほど当社でさらに調査を進めたところ、以下が判明しました。

- 一部のIoCが名前解決した5個のIPアドレス
- IoCのIPアドレスを共用していた761個のドメイン名。うち1個は悪意あるドメイン名と確認
- BECスキャマーがキャンペーンで詐称した会社の名称「***foobar***」を含む1,272個のドメイン名。うち8個はマルウェアホストであることを確認
- 被害者に署名させる文書を提供する際に脅威アクターが悪用した「***docusign***」という文字列を含む2,545個のドメイン名。うち43個は様々なマルウェアエンジンにより悪意あるものと分類
- BECメールの送信で脅威アクターが悪用した「***outlook***」という文字列を含む10,000個のドメイン名。うち30個はマルウェアホストと確認

これらのアーティファクトは全て、ここで取り上げた悪意のキャンペーンで将来使用され得るものです。

IoCに関する詳細を解明

前述の報告で指摘されたIoCには、4つのIPアドレスと3つのドメイン名（以下）が含まれていました。

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

この3つのドメイン名をWHOIS lookupsで検索したところ、2019年から2022年の間に新規登録されたドメイン名であることがわかりました。ドメイン名登録者の所在地については、web[.]appは米国、awin1[.]comは英国、lointree[.]comはアイスランドと、異なる国を示していました。

他方、4つのIPアドレスをIP geolocation lookupsで検索した結果、3つの国に所在していることが判明しました。すなわち、139[.]99[.]6[.]158はシンガポール、154[.]6[.]17[.]158と20[.]245[.]118[.]47は米国、5[.]31[.]10[.]180はアラブ首長国連邦にあるアドレスでした。

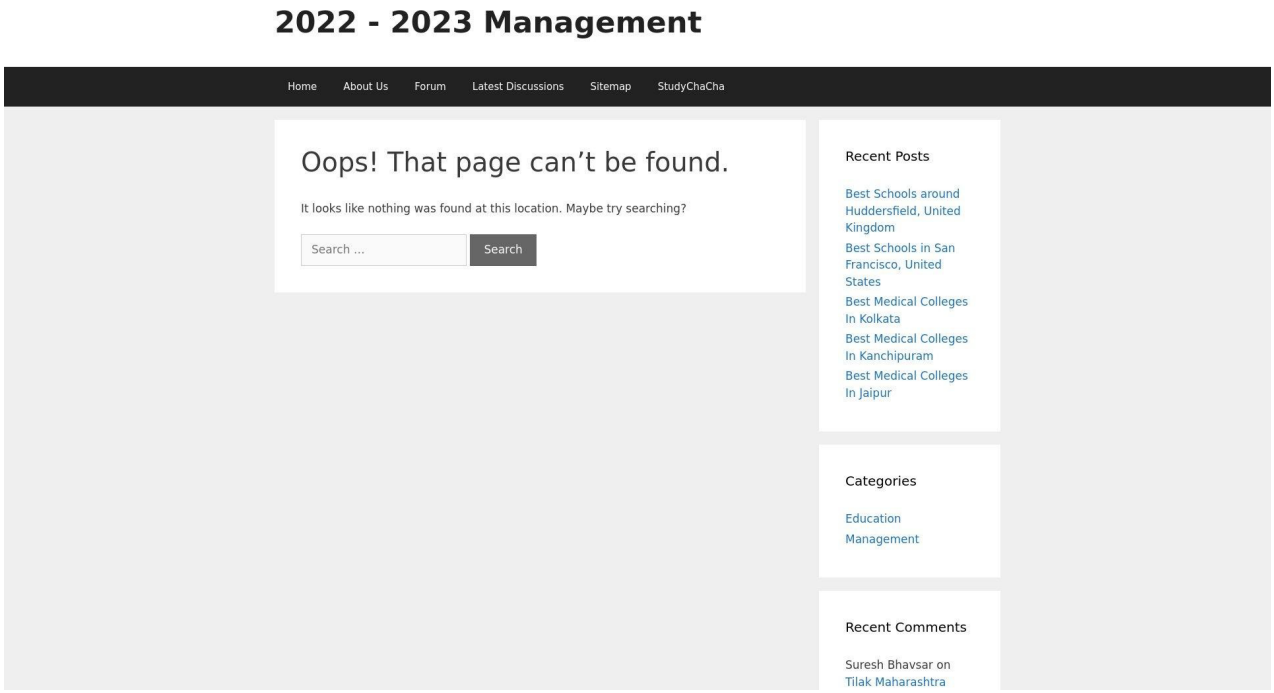
他の潜在的脅威ベクトルを特定

まず、IoCと特定された3つのドメイン名をDNS Lookupにかけました。その結果、元のIoCリストに含まれていなかった5つのIPアドレスを発見できました。これで、把握できたIPアドレスのIoCは合計9個となりました。追加で見つかった5つのIPアドレスは、2つの既存IoCと同様に米国内に位置していました。

合計9つのIPアドレスをReverse IP lookupsで検索したところ、3つは名前解決せず、1つは専用ホスト、残りの5つは共用ホストであることが判明しました。また、この検索で761個のドメイン名が見つかり、そのうち01lvnohlp0n[.]infoは悪意あるドメイン名と確認されました。

Mitigaの分析では、脅威アクターがFoobarという名前の会社になりすましたとしています。これを受け、当社は、今後BECで悪用されかねない***foobar***という文字列を含むドメイン名が既存のドメイン名の中にどれだけあるかを調べました。Domains & Subdomains Discoveryで検索したところ1,272個のドメイン名が見つかり、そのうち8つがマルウェアのホストであることが判明しました。うち3つは購入可能なパークドメイン、1つはすでに購入済みでウェブサイトを制作中でした。

Mitigaの報告では、脅威アクターがDocuSignを使用したことについても言及されています。そこで、***docusign***という文字列を含むドメイン名をDomains & Subdomains Discoveryで検索しました。その結果2,545個のドメイン名が特定され、うち43個が悪意あるドメイン名に分類されました。とりわけdocusignbusiness[.]comは、ページに関するエラーメッセージが表示されるものの、有効なコンテンツをホストし続けていました。

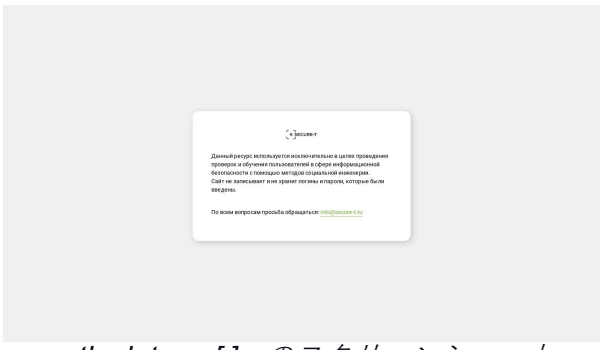


docusignbusiness[.]comの
スクリーンショット

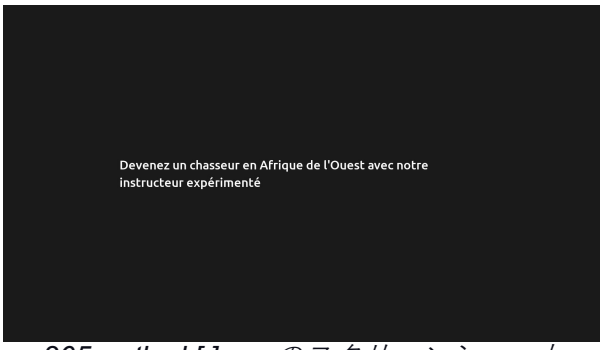
また、***docusign***を含むドメイン名のうちDocuSign, Inc.に帰属すると公開情報から確認できたのは、100個のみでした。残りの2,445個のドメイン名は潜在的なサイバースクワッティングドメインで、被害者に署名させる文書をホストするマルウェアの可能性があります。

さらに、BECスキャマーが悪意のキャンペーンでOutlook 365を悪用したとMitigaの報告では指摘されています。そこで***outlook***という文字列を含むドメイン名をDomains & Subdomains Discoveryで検索したところ、少なくとも10,000個のドメイン名が出てきました。そのうち30個はすでに悪意あるドメイン名としてタグ付けされたものでした。具体的には、22個のドメイン名がマルウェアのホスト、残りの8つのドメイン名がスパムの送信に使われたものです。

悪意のあるページはoutlook-team[.]ruやo365-outlook[.]comなどごくわずかでしたが、いずれもアクセス可能な状態でした。以下はそれぞれのスクリーンショットです。

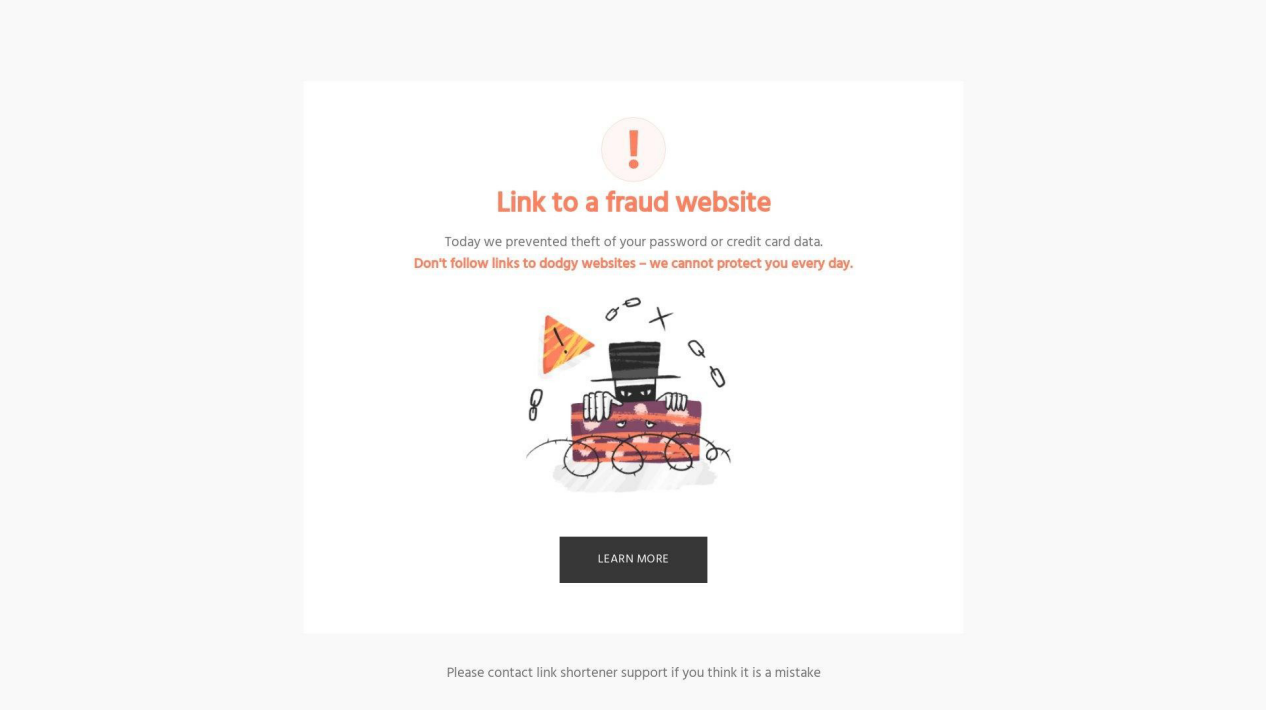


outlook-team[.]ruのスクリーンショット



o365-outlook[.]comのスクリーンショット

もう一つの悪意あるウェブサイトであるoutlooklive[.]orgは、訪問者に警告ページを表示するものでした。



outlooklive[.]orgのスクリーンショット

こうしたドメイン名のうちMicrosoftに帰属していることが公開情報から確認できたものは、117個にとどまりました。残りの9,883個のドメイン名については、脅威アクターがOutlook 365を利用する正規の企業になりすましてBECに使う可能性があります。

—

既存のIoCリストをもとに今回当社が特定したドメイン名は、BECやフィッシングの攻撃ベクトルになる可能性があります。いずれも疑わしい活動の兆候がないか注意深く監視する必要があるでしょう。

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

一部のIoCとIPアドレスを共用していたドメイン名の例

- 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

*Foobar*という文字列を含むドメイン名の例

- 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

*Foobar*を含む悪意あるドメイン名の例

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

*Docusign*という*文字列*を含むドメイン名の例

- 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

*Docusign*を含む悪意あるドメイン名の例

- 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
- docusigncxle[.]ml
- docusigndaps[.]ml
- docusignapp[.]org
- usdocusign[.]info
- docusigntwo[.]com
- docusignusa[.]com
- prodocusign[.]com

*Outlook*という文字列を含むドメイン名の例

- 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

*Outlook*を含む悪意あるドメイン名の例

- 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