EevilcorpをDNSインテリジェンスで解き明かす

目次

1. 要旨
2. 付録：アーティファクトとIoCの例

要旨

フィッシングは、かねてより企業や個人のネットワークにとって最大の脅威のひとつです。実際、今日のデータ漏洩の3分の1以上がフィッシングに関係したものです。

「芸術は自然を模倣する」とアリストテレスは言いましたが、サイバーセキュリティの世界では、その逆もまた真なりです。Eコープ（「Evil Corp」の略称）はテレビ番組「Mr. Robot」の中だけの存在ではありません。現在、「Eevilcorp」として知られる実在のフィッシンググループが、世界中の組織や個人を大混乱に陥れているのです。

Vadeの脅威インテリジェンス・レスポンスセンター（TIRC）の研究者が最近、「Eevilcorpフィッシングキャンペーン」とその犯人が使用したマルウェアを詳細に分析しました。そして、以下のドメイン名とサブドメインをIoCとして特定しました。

- periodic-checker[.]glitch[.]me
- scan-verified[.]glitch[.]me
- transfer-with[.]glitch[.]me
- air-dropped[.]glitch[.]me
- precise-share[.]glitch[.]me
- monthly-payment-invoice[.]glitch[.]me
- monthly-report-check[.]glitch[.]me
- eevilcorp[.]online
- ultimotempore[.]online

WhoisXML APIでは今回、この公開IoCリストをもとに調査を深め、さらに以下を発見しました。

- IoCとして識別されたドメイン名とサブドメインが名前解決した9個のユニークなIPアドレス
- IoCの専用ホストを共用していた可能性のある579個のドメイン名。そのうち13個はマルウェアの一括チェックにより悪意があると確認
- **microsoft + outlook**または**adobe + document + cloud**という文字列で始まる20個のドメイン名。そのうち6個は一括マルウェアチェックで悪意あるドメイン名に分類

- **microsoft + outlook**または**adobe + document + cloud**という文字列を含んだ715個のサブドメイン。一括マルウェアチェックで、そのうち8個には悪意があることを確認

EevilcorpのIoC

Vade TIRCの研究者は、Eevilcorpが少なくとも2つの主要なテクノロジー製品（Microsoft OutlookとAdobe Document Cloud）に狙いを定めていることを発見しました。Eevilcorpはまた、glitch[.]meプラットフォームを悪用して、特別に細工された7つのサブドメインをホストし、別の2つのドメイン名を継続的なキャンペーンに使用していました。

当社ではまず、IoCとして特定された9個のドメイン名を当社のBulk WHOIS Lookupにかけてみました。その結果、WHOISレコードが利用可能だったのはeevilcorp[.]onlineとultimotempore[.]onlineのみとわかりました。どちらもレジストラはHostinger Operations, UABであり、またプライバシー保護サービスのPrivacy Protect, LLCを使ってWHOISレコードを非公開にしていました。両方とも2023年初めの2カ月以内に作成された比較的新しいドメイン名で、登録地は米国でした。

Website categorization lookupsで9個のドメイン名を検索したところ、以下の表の通り、興味深い事実が明らかになりました。

ドメイン名	Website Categorization Lookupでの分類
eevilcorp[.]online	フィッシングまたはその他の詐欺行為
ultimotempore[.]online	フィッシングまたはその他の詐欺行為
periodic-checker[.]glitch[.]me	フィッシングまたはその他の詐欺行為
scan-verified[.]glitch[.]me	フィッシングまたはその他の詐欺行為
transfer-with[.]glitch[.]me	フィッシングまたはその他の詐欺行為
air-dropped[.]glitch[.]me	フィッシングまたはその他の詐欺行為
precise-share[.]glitch[.]me	フィッシングまたはその他の詐欺行為
monthly-payment-invoice[.]glitch[.]me	フィッシングまたはその他の詐欺行為
monthly-report-check[.]glitch[.]me	フィッシングまたはその他の詐欺行為

Eevilcorp IoCの調査結果

次に、すでにEevilcorpのIoCとして特定されているもの以外に避けるべきドメイン名があるかどうかを判断するため、当社のDNSインテリジェンスを駆使してIoCリストを拡張することにしました。

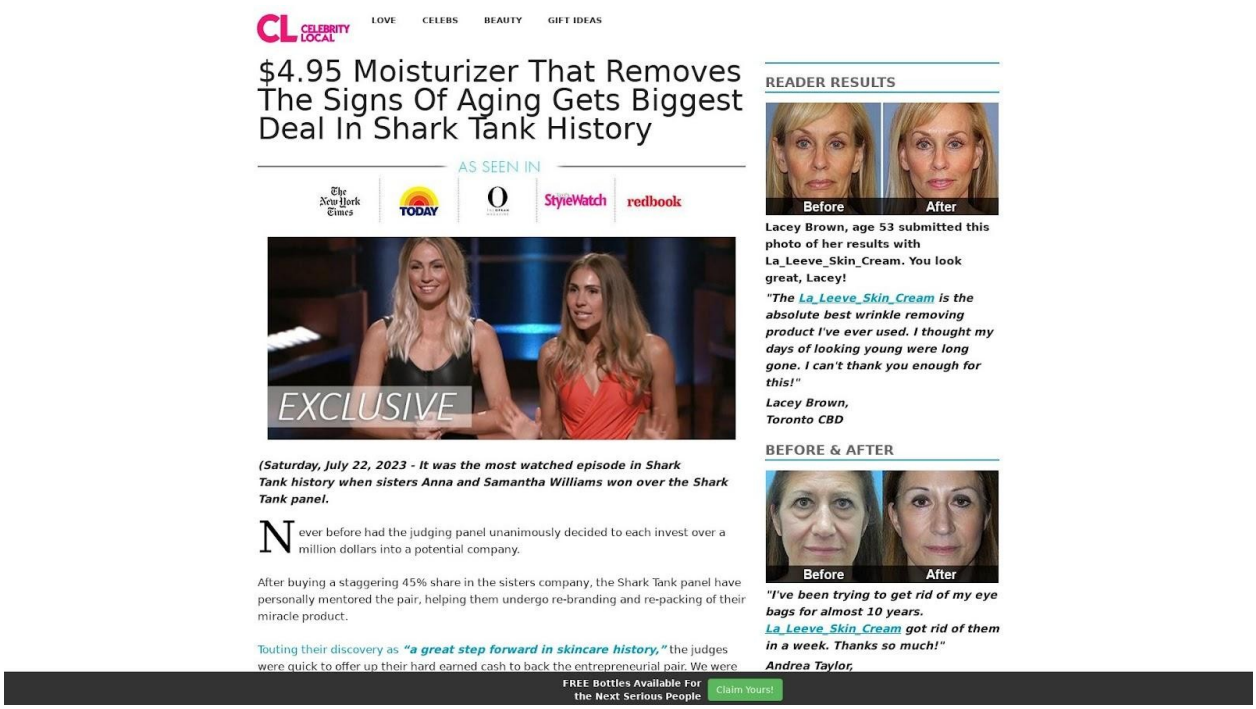
IoCとされたドメイン名は、合計9個のユニークなIPアドレスに名前解決しました。しかし、Bulk IP Geolocation Lookupの結果、検索可能なAレコードを持っていることが確認できたIPアドレスはそのうち8個にとどまりました。また、4個はAmazon、残りはCloudflareが管理するIPアドレスでした。名前解決する8個のIPアドレスは、全て米国内に位置していました。

また、IoCをDNS Lookupで検索したところ、それらの多く、特にglitch[.]meでホストされているIoCは、4個の共用IPアドレス（3[.]212[.]249[.]142、44[.]198[.]62[.]156、54[.]144[.]28[.]217、54[.]235[.]167[.]164）を使用していることがわかりました。

さらに、Reverse IP Lookupにかけた結果、残りの4個のIPアドレスは専用アドレスの可能性があり、既存の公開IoCリストにはない合計579個のドメイン名をホストしていることが判明しました。同じIPアドレスを使っているドメイン名を対象にマルウェアの一括チェックを行った結果、13個は悪意あるドメイン名と判定されました。

その13個の悪意あるドメイン名のうち5個は、Screenshot Lookupの結果から、アクティブなコンテンツをホストし続けていることが確認されました。また、そのうち2個は、マルウェアのホストとして検出された上、ドメイン名の文字列が表現しているものとコンテンツが一致しませんでした。

nutritionfactsforfree[.]onlineはセレブに関するニュースサイトのようでした。他方、perjakatoto[.]net（perjakatotoはマレー語で「女の子」の意味）とvldb2009[.]orgは、ギャンブルのサイトにつながりました。

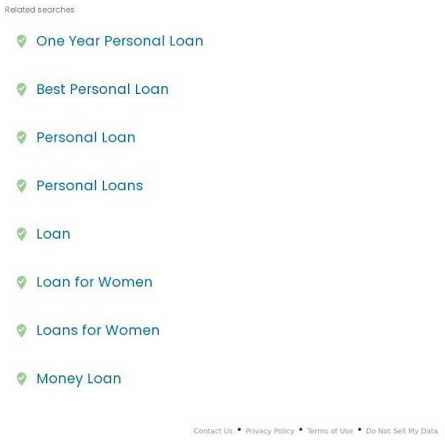


nutritionfactsforfree[.]onlineのスクリーンショット

perjakatoto[.]netのスクリーンショット

vldb2009[.]orgのスクリーンショット

なお、悪意あるドメイン名のpersonal-loan-look-seeks[.]todayは、その文字列が表現している通り、ローン関連の検索リストを表示するページをホストしていました。



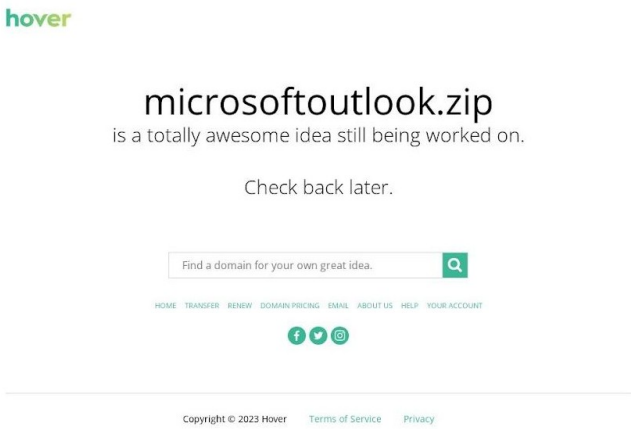
personal-loan-look-seeks[.]todayのスクリーンショット

次に、MicrosoftとAdobeの人気ブランドを攻撃者が悪用したことをふまえ、今後他のドメイン名やサブドメインを悪用したキャンペーンが行われる可能性があるかどうかも調査しました。

Domains & Subdomains Discovery を使って**microsoft + outlook**という文字列で始まるドメイン名または**microsoft + outlook**を含んだサブドメインを調べたところ、今年に作成されたばかりのドメイン名20個およびサブドメイン715個が検出されました。その一方で、**adobe + document + cloud**で始まるドメイン名とその文字列を含むサブドメインを同様に検索したところ、11個のドメイン名と15個のサブドメインがヒットしました。

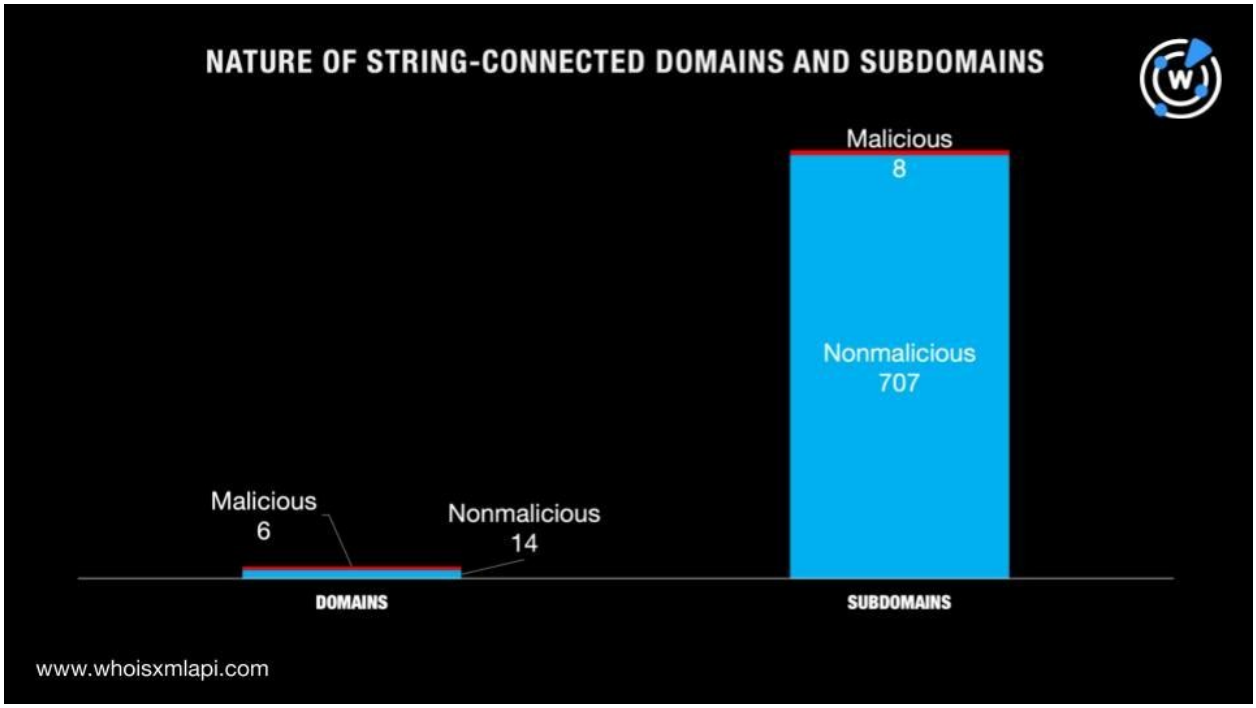
当社が発見した全てのドメインをBulk WHOIS Lookupで一括検索したところ、MicrosoftとAdobeに帰属することが公開のWHOIS情報から確認できるドメインはありませんでした。また、登録者のメールアドレスやその他のWHOIS情報も、microsoft[.]comとadobe[.]comのものとは異なっていました。

他方、共通の文字列を含むドメインについてマルウェアの一括チェックを行ったところ、6個は悪意あるものとして分類されました。その大半はアクセス不能でしたが、1個のドメイン名は、以下の通り製作中のサイトにつながりました。



microsoftoutlook[.]zipのスクリーンショット

また、共通の文字列を含むサブドメインをマルウェアの一括チェックにかけたところ、8個のサブドメインはマルウェアのホストとわかりました。そのうちアクセス可能な状態に維持されていたのは3つで、1つは空白のページを、2つはエラーページを表示しました。



—

今回、公開IoCリストをもとに当社でDNSを深掘りした結果、Eevilcorpが意図せずに残した可能性のある、1,300を超える関連プロパティが新たに特定されました。Eevilcorpが現在行っているフィッシング・キャンペーンに直接関係しているかどうかにかかわらず、この調査で発見した合計27個の悪意あるプロパティは、組織や個人に対してリスクをもたらす可能性があります。

同様の調査をご希望のお客様、または本調査で使用された当社の商品にご興味をお持ちのお客様は、こちらまでお気軽にお問い合わせください。

免責事項： *当社は、潜在的な危険から企業を守るために役立つ情報の提供を目指しており、脅威の検出に対して厳格な姿勢で臨んでいます。そのため、当初「脅威」または「悪意がある」とみなされたエンティティが、さらなる調査やその後の状況の変化により最終的に無害と判断される可能性があります。ここで提供されている情報を確認する補足調査の実施を強くお勧めします。*

付録：アーティファクトとIoCの例

IoCが名前解決したIPアドレスの例

- 104[.]21[.]62[.]191
- 172[.]67[.]138[.]168

- 172[.]67[.]184[.]21
- 104[.]21[.]59[.]213

共通のIPアドレスを使用していたドメイン名の例

- 01server01[.]sbs
- 100seoer[.]com
- 10powerpro[.]club
- 123cendoldawet[.]xyz
- 1bar[.]uk
- 1za8a1q[.]bar
- 2023keeoxezyxaz[.]cyou
- 2biizhug[.]xyz
- 2winph[.]com
- 333tron[.]live
- 3b9n3t1[.]work
- 3y3coin[.]shop
- 4g7ye8[.]cyou
- 4hg333[.]com
- 60ok[.]it
- 637glorietta[.]com
- 69xx1019[.]xyz
- 69xx1671[.]xyz
- 7512289[.]com
- 8crafts[.]cyou
- 96dg[.]in
- 97or3[.]com
- 9se123[.]xyz
- a-prime-drive[.]zone
- actiontreeservicesa[.]com
- actor2athlete[.]com
- addvancestudio[.]com
- adgokanroreva[.]tk
- administrise[.]one
- adriannabialobrzeska[.]pl
- aefr47[.]shop
- agenciab2be[.]com[.]br
- agrcolicener[.]tk
- alassautdusida[.]live
- aljanabdshop[.]com
- allied-esports[.]com
- altukosjaupiccia[.]cf
- aminsamad[.]cf
- amkhatar[.]cf
- ankarapastirma[.]com
- aquavenatus[.]com
- aradiginajans[.]com
- aranex-provider[.]de
- arbbnb[.]net
- architecte[.]asia
- areweeatingfishyfood[.]com
- arirealinon[.]cf
- arshanmedia[.]ir
- artofhome[.]com
- asfwebcamchat[.]ru
- asix88[.]net
- assystengenharia[.]com[.]br
- atasehirdeyim[.]com
- aurumx[.]io
- auswideframeless[.]com[.]au
- avatka[.]ru
- azino777-gv[.]top
- azuremoonstone[.]xyz
- baguette-academy[.]in
- ballspromotion[.]com
- barrettcommunity[.]com
- bbbnoordenveld[.]nl
- bearmtnband[.]com
- benebolton[.]space
- bhaitea[.]sg
- bigcupbrassale[.]com
- bitquickls[.]com
- blazercomaposta[.]icu
- blypw[.]me
- bocoranslotonlinegacor[.]com
- bocphot[.]xyz
- boitier-ethanol[.]net

- bordobet[.]buzz
- bpw2u0[.]cfd
- brain2train[.]net
- brandtchiroclinic[.]com
- brunflohus4[.]com
- bubbelsenjets[.]nl
- bubblegumheaven[.]com
- budget-locksmith-albuquerque[.]com
- buildengineers[.]com
- bulgariangambler[.]com
- buxtonshop[.]com
- buywithccm[.]com
- calivaria[.]org
- campingartikel-neu[.]com
- carshowsigns[.]com
- casapestera[.]ro
- cashofferli[.]com
- cashup[.]me
- cddgc63[.]top
- cemmaresme[.]com
- cen95996[.]com
- centralestagio[.]com
- ceyokahealth[.]com
- chinapo[.]org
- chinesedreamsisgone[.]com
- chloesavageembroidery[.]com
- circuscasino[.]rs
- citizenshipcourtesy[.]cn

共通のIPアドレスを使用していた悪意あるドメイン名の例

- mpsconsultingcorp[.]com
- nutritionfactsforfree[.]online
- perjakatoto[.]net
- personal-loan-look-seeks[.]today
- tamilprint23[.]bio
- vldb2009[.]org
- wecindia[.]in

共通の文字列を含むドメイン名の例

- microsoftoutlook[.]cn
- microsoftoutlook[.]zip
- microsoft365outlook[.]de
- microsoftoutlook[.]com[.]de
- microsoftoutlookonline[.]xn--ngbrx
- adobedocumentscloud[.]ml
- adobedocumentscloud[.]ga
- adobeclouddocument[.]com
- adobedocumentscloud[.]tk
- adobe-documentscloud[.]ml
- adobe-documentscloud[.]cf

共通の文字列を含む悪意あるドメイン名の例

- microsoftoutlook[.]zip
- adobedocumentscloud[.]ga
- adobeclouddocument[.]com

共通の文字列を含むサブドメインの例

- microsoftoutlook[.]com[.]xyz
- microsoftoutlook[.]com[.]com
- microsoft-outlook[.]oculusvr[.]com
- microsoft-outlook[.]williamhill[.]com
- microsoft-outlook[.]attcorona[.]com
- microsoft-outlook[.]onelink[.]me

- outlook-microsoft[.]42web[.]io
- microsoft-outlook[.]just-eat[.]co[.]uk
- microsoft-outlook[.]as[.]me
- microsoftoutlooks[.]intactsolutions[.]net
- outlook[.]microsoft[.]user-login[.]online
- microsoft-outlook[.]hitta[.]se
- outlook[.]microsoft[.]techgyaanii[.]com
- microsoft-outlook[.]quizlet[.]com
- microsoft-outlook[.]menulog[.]co[.]nz
- outlook[.]microsoft[.]vdwal[.]xyz
- microsoft-outlook[.]larksuite[.]com
- microsoft-outlook[.]planningcenteronline[.]com
- microsoft-outlook[.]climedo[.]de
- microsoft-outlook[.]verily[.]com
- microsoft-outlook[.]paydiant[.]com
- microsoft-outlook[.]betsson[.]com
- microsoft-outlook[.]wolf-of-wilderness[.]com
- microsoft-outlook[.]syncsketch[.]dev
- microsoft-outlook[.]staging-airtableblocks[.]com
- microsoft-outlook[.]jfrog[.]com
- microsoft-outlook[.]yelp[.]com
- microsoft-outlook[.]nextdoor[.]de
- microsoft-outlook[.]cyna[.]io
- microsoft-outlook[.]unfold[.]com
- microsoft-outlook[.]connxusdemo[.]com
- microsoft-outlook[.]emotient[.]com
- microsoft-outlook[.]smashfly[.]com
- microsoft-outlook[.]twilio[.]com
- microsoft-outlook[.]wistia[.]com
- outlook[.]microsoft[.]integra-group[.]cz
- microsoft-outlook[.]duolingo[.]com
- microsoft-outlook[.]binance[.]com
- microsoft-outlook[.]acuityscheduling[.]com
- microsoft-outlook[.]withgoogle[.]com
- outlook[.]microsoft[.]demstronic[.]com
- microsoft-outlook[.]yelptop100[.]com
- microsoft-outlook[.]snowflakecomputing[.]com
- microsoft-outlook[.]netlify[.]app
- microsoft-outlook[.]recko[.]io
- microsoft-outlook[.]realtime[.]email
- microsoft-outlook[.]miro[.]com
- outlook[.]microsoft[.]sec-line[.]xyz
- microsoft-outlook[.]litix[.]io
- microsoft-outlook[.]vivy[.]com
- adobeclouddocument[.]lpages[.]co
- adobedocumentcloud[.]ormimas[.]com
- adobedocumentcloud[.]aqualunub[.]com
- adobe-document-cloud[.]webflow[.]io
- www[.]adobedocumentcloud[.]aqualunub[.]com
- adobe-document-cloud[.]en[.]mercadopago[.]com[.]pe
- adobe-document-cloud[.]en[.]humio[.]cloud
- adobe-document-cloud[.]en[.]foodpanda[.]my
- adobe-document-cloud[.]en[.]structure[.]app
- adobe-document-cloud[.]en[.]datad0g[.]com
- adobe-document-cloud[.]en[.]foodpanda[.]ph
- adobe-document-cloud[.]en[.]tccalling[.]net

- documentcloud[.]adobe[.]com[.]i[.]edgekey[.]net
- documentcloud-adobe-com-s[.]vpn2[.]aufe[.]edu[.]cn
- adobefreeuserschannel[.]na1experiencecloud[.]documents[.]adobe[.]com
- outlookmicrosoft-la[.]4lima[.]de
- microsoftoutlook[.]id[.]cghub[.]com
- microsoftoutlook[.]nl[.]mongodb[.]com
- microsoftoutlook[.]en[.]tagomi[.]com
- microsoftoutlook[.]de[.]fortnite[.]com
- microsoftoutlook[.]ro[.]tidalhi[.]fi
- outlook[.]microsoft[.]outlook[.]com[.]bogston[.]com
- microsoft-outlook[.]en[.]8x8pilot[.]com
- microsoft-outlook[.]en[.]ncplatform[.]net
- microsoft-outlook[.]nl[.]bolt[.]com
- microsoft-outlook[.]nl[.]fbsbx[.]com
- microsoft-outlook[.]en[.]affinity[.]co
- microsoft-outlook[.]en[.]netlify[.]app
- microsoft-outlook[.]nl[.]animalfriends[.]co[.]uk
- microsoft-outlook[.]nl[.]8x8pilot[.]com
- microsoft-outlook[.]nl[.]32red[.]com
- microsoft-outlook[.]th[.]canvaslms[.]com
- microsoft-outlook[.]nl[.]climedo[.]de
- microsoft-outlook[.]nl[.]miro[.]com
- microsoft-outlook[.]en[.]cloudinary[.]com
- microsoft-outlook[.]en[.]hitta[.]se
- microsoft-outlook[.]nl[.]caesars[.]com
- microsoft-outlook[.]en[.]claiming[.]com[.]au
- microsoft-outlook[.]en[.]nextdoor[.]nl
- microsoftoutlook1337[.]zendesk[.]com
- microsoft-outlook[.]nl[.]exploretock[.]com
- microsoft-outlook[.]en[.]guildwars2[.]com
- microsoft-outlook[.]en[.]staging-airtableblocks[.]com
- microsoft-outlook[.]en[.]shopkeep-staging[.]com
- microsoft-outlook[.]en[.]goodrx[.]com
- microsoft-outlook[.]en[.]fortnite[.]com
- microsoft-outlook[.]en[.]small-improvements[.]com
- microsoft-outlook[.]en[.]connxusdemo[.]com
- microsoft-outlook[.]en[.]attcorona[.]com
- microsoft-outlook[.]nl[.]slackb[.]com

共通の文字列を含む悪意あるサブドメインの例

- microsoftoutlook[.]zip
- adobedocumentscloud[.]ga
- adobeclouddocument[.]com