貴社のイントラネットは大丈夫ですか？
DNSにおけるイントラネットのなりすましを調査

目次

要旨

Redditは2023年2月10日、フィッシングによってネットワークのイントラネットゲートウェイを模したウェブサイトに同社の従業員が誘導される、というセキュリティインシデントが発生したと発表しました。被害者が認証情報と二要素認証（2FA）トークンを入力したことで、内部のコード、ドキュメントおよび業務システムに対して攻撃者がアクセスできるようになったといいます。これは高度な標的型攻撃です。脅威アクターは、Redditのイントラネットアドレスが何なのか、どのように動作するのか、どのように見えるのかを知っていました。

この発表を受け、WhoisXML APIの研究者は、攻撃ベクトルとして使用され得るイントラネット関連のドメイン名を調べました。このレポートでは、2023年1月1日から3月20日の間に新規登録されたウェブプロパティに焦点を当て、Redditのインシデントと同様のフィッシングの手段になる可能性を明らかにしました。主な調査結果は以下の通りです。

- 最も人気のある20のイントラネットソフトウェアを標的にした800超のサイバースクワッティングドメイン
- 文字列***intranet***を含む220超のドメイン名
- サイバースクワッティングドメインのうち、標的になった正規のソフトウェアベンダーに実際に帰属するドメインは1%未満
- イントラネット関連ドメイン名の3.4%は悪意あるドメイン名と確認。その一部は2023年3月21日現在もフィッシングサイトをホスト
- 一般に公開されたログインページをホストしていた60超のイントラネット関連ドメイン名

イントラネットの人気ソフトを標的にしたサイバースクワッティングドメイン

この調査ではまず、Domains & Subdomains Discoveryでの検索により、20の人気ソフトウェアのブランド名を文字列として含む、最近登録されたドメイン名を814個特定しました。また、同時期に登録された**intranet**という言葉を含むドメイン277個を発見し、ドメイン名の合計数が1,091個となりました。

ドメイン名の属性

次に、Bulk WHOIS Lookupを使用し、イントラネットソフトウェアの公式ドメイン名とサイバースクワッティングの可能性があるプロパティのWHOISレコードを取得しました。その結果、814個のサイバースクワッティングドメインのうち、公式ドメイン名と同じ登録者データを共有しているドメイン名は5個しかないことが判明しました。

また、IPアドレスをチェックするため、公式ドメイン名とサイバースクワッティングドメインをbulk IP geolocation lookupsにかけてみたところ、サイバースクワッティングドメインのうち正規ドメイン名のIPアドレスに名前解決したのは2個にとどまりました。

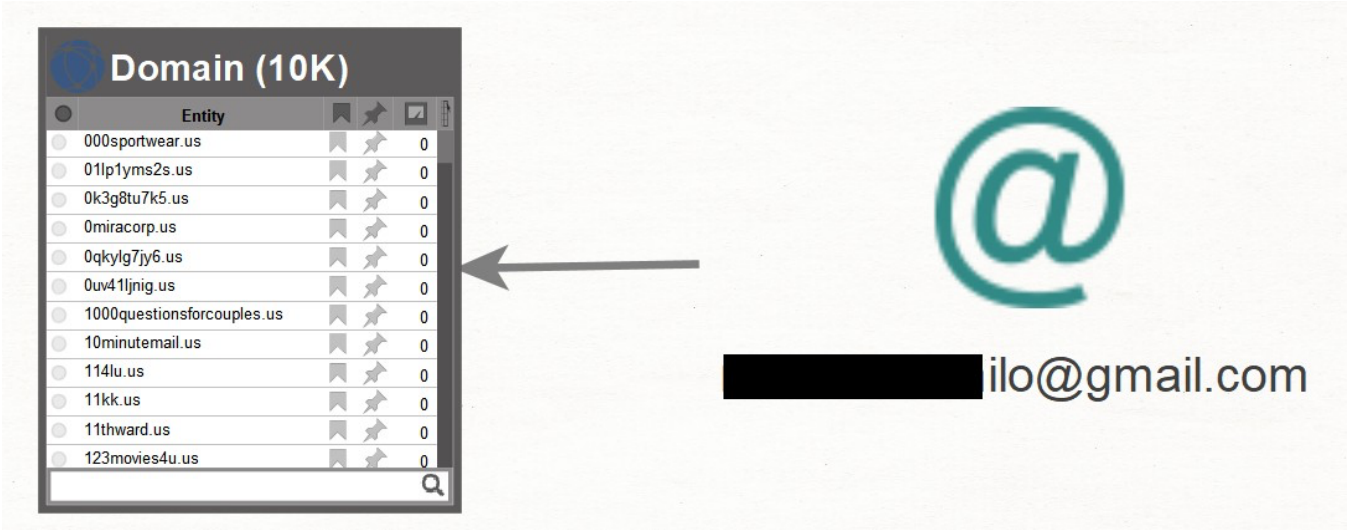
全体として、サイバースクワッティングドメインのうち正規のソフトウェアベンダーに帰属すると公に確認できたものは1%未満であり、ほとんどのドメイン名が未知の存在の支配下に置かれていることがわかりました。.

イントラネット関連ドメイン名のWHOISインフラ

サイバースクワッティングドメインのうち、正規のソフトウェアベンダーに帰属するドメインがほとんどなかったため、次に登録数の詳細について分析することにしました。ほとんどのドメイン名ではWHOISレコードが非公開となっていましたが、37個のドメイン名の登録者データは公開されていました。そこから登録者のメールアドレスが32個判明しましたが、そのほとんどがGmailアドレスでした。

それらのメールアドレスをReverse WHOIS Searchで検索したところ、10,611個のドメイン名と関連していることが判明しました。そして、そのうち数十個は、今回取り上げたイントラネットソフトウェアのいくつかを狙ったサイバースクワッティングドメインでした。

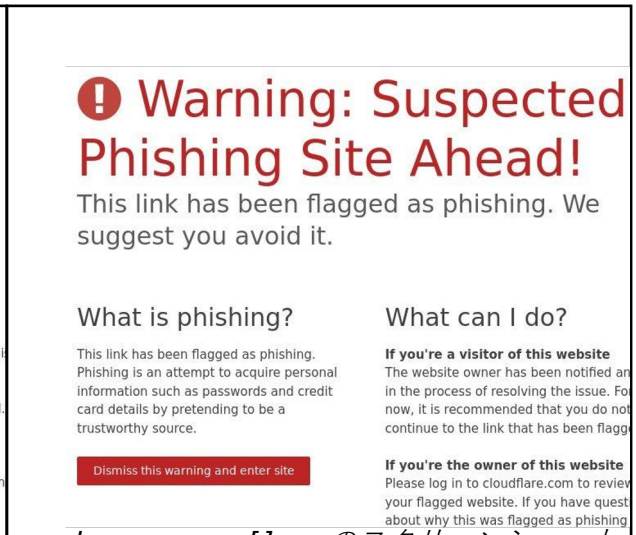
さらに、1つのGmailアドレスが関連性のある10,000個のドメイン名の登録メールアドレスとして使われていることがわかりました。ドメイン投資家のポートフォリオの一部である可能性があります。以下は、関連性をMaltegoで確認した結果のスクリーンショットです。



サイバースクワッティングドメインの悪意ある不審な利用

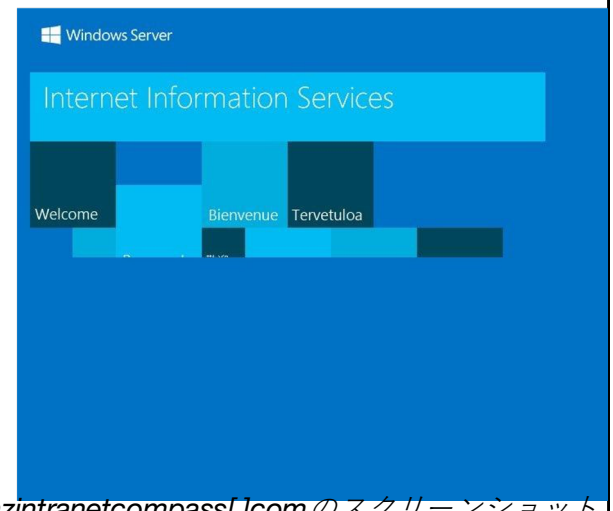
一部のドメイン名は組織のイントラネットのゲートウェイとして使われている可能性がありますが、2023年3月21日時点で、サイバースクワッティングドメインの約3.4%が悪意あるキャンペーンに利用されています。中には、以下のようなフィッシングサイトのホスティングを続けているドメイン名もあります。

wvv-basecamp-us[.]comのスクリーンショット

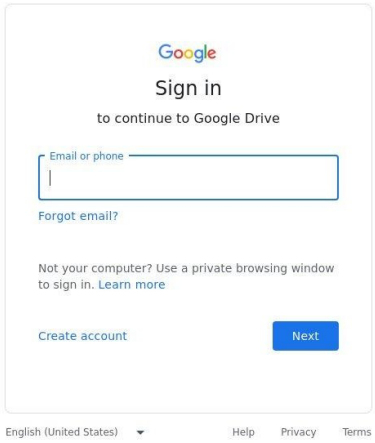


www-basecamp-us[.]comのスクリーンショット

Windows Serverのページをホストするnzintranetcompass[.]comや、Googleドライブにリダイレクトするjohnsonandwilsonintranet[.]comなど、フラグのないドメインにも疑わしいコンテンツがホストされているものがありました。これらのサイトのスクリーンショットは以下の通りです。



nzintranetcompass[.]comのスクリーンショット



johnsonandwilsonintranet[.]comのスクリーンショット

イントラネットゲートウェイの潜在的脆弱性

先述の通り、本調査で特定したイントラネット関連ドメイン名には、正規のイントラネットゲートウェイかもしれないものが含まれていました。例えば、スクリーンショット分析の結果、401、forbiddenまたはunauthorized accessといった警告ページに行き着くドメイン名がいくつか見られました。

とはいえ、ログインページをホストしているサイバースクワッティングドメインも存在していました。これらが正規のものであれば、標的とする組織のイントラネットゲートウェイを模倣する基点を脅威アクターに与えてしまう可能性があります。また、ブルートフォース攻撃に対して脆弱かもしれません。他方、これらのドメイン名が正規のイントラネットゲートウェイでない場合、標的にされた組織の従業員1人が罠にかかるだけで陥落することもあります。

—

Redditのセキュリティインシデントが示すように、イントラネットは標的の公式ゲートウェイを模倣するだけで攻撃ベクトルとして機能できます。脅威ベクトルが増加し、組織のアタックサーフェスがかつてないほど広がっている今、積極的な監視と脆弱性スキャンが肝要です。

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

イントラネットのサイバースクワッティングドメインの例

- aihcltech[.]com
- aunily[.]cf
- aunily[.]ga
- aunily[.]ml
- axero[.]me
- axero[.]work
- axeroc[.]net
- axeroc[.]org
- basecamp[.]ga
- basecamp[.]rest
- basecamp[.]sbs
- basecampbv[.]co
- basecampost[.]de
- basecamptw[.]co
- basecampv[.]ca
- bempulsa[.]shop
- circlinked[.]com
- clinked[.]ai
- clinked[.]com[.]au
- clinked-in[.]org
- cplworkvivo[.]com
- diejostle[.]com
- doclinked[.]nl
- elaxero[.]cn
- empuls[.]at
- empuls[.]cn
- empuls[.]com[.]cn
- empulsar[.]de
- empuls-ems[.]de
- flagstaffbasecamppt[.]com

- gaxero[.]net
- gclinked[.]com[.]au
- gempulsa[.]xyz
- happeon[.]fr
- happeon[.]shop
- happeon[.]store
- haystack[.]fi
- haystacka7a[.]shop
- haystackex[.]com
- haystacks[.]capital
- hcltech[.]co[.]kr
- hcltech[.]com[.]pl
- hcltechsw[.]cz
- hcltechsw[.]de
- hcltechsw[.]eu
- hirayammer[.]com
- iclinked[.]com[.]cn
- igloosoftwares[.]ws
- it-hcltech[.]com
- jesterjostler[.]com
- jostle[.]app
- jostled[.]io
- jostle-presidency[.]com
- jostlesuccess[.]me
- mangoappsfun[.]com
- maryammerlin[.]com
- maxero[.]pl
- metaworkplace[.]de
- metaworkplace[.]ml
- metaworkplace[.]mp
- metaworkplace[.]pa
- metaworkplace[.]ph
- metaworkplace[.]pk
- metaworkplace[.]tk
- networkvivor[.]com
- networkvivor[.]xyz
- onthesamepage[.]club
- ryunilyan[.]ml
- samepage[.]cafe
- samepage[.]church
- samepage[.]fyi
- samepageacademy[.]com
- samepagemeeting[.]net
- samepagesports[.]org
- sharepointaa[.]com
- sharepointlab[.]ir
- sharepointsf[.]ga
- sharepointxs[.]nl
- sharepointxz[.]ml
- staffbase[.]cn
- staffbase[.]com[.]cn
- staffbase[.]me
- staffbase[.]online
- staffbase[.]studio
- sunily[.]co[.]in
- syammerijaya[.]com
- thoughtfarmerdev[.]vg
- unilya[.]com
- usehaystack[.]fyi
- usehaystack[.]us
- usehaystack[.]xyz
- workvivo[.]de
- workvivome[.]com
- wssharepoint[.]de
- wwwmangoapps[.]com
- wwwstaffbase[.]com
- wwwunily[.]com
- yammer-blog[.]com
- yammergram[.]io
- yammerindia[.]vg
- yammers[.]lol
- ysharepoint[.]net
- zoho[.]hair
- zohobraincenter[.]com
- zohogermany[.]de
- zohohoist[.]vg
- zohomailbox[.]eu
- zohoz[.]com[.]pe
- zohoz[.]de

Intranetという文字列を含むドメイン名の例

- aicintranet[.]ht
- aocintranet[.]org
- ascintranet[.]ws
- azintranet[.]vg
- bcintranet[.]com
- bintranet[.]de
- btintranet[.]ga
- cintranet[.]net
- dd-intranet[.]de
- ecintranet[.]ph
- escintranet[.]ws
- faintranet[.]co
- hdintranet[.]org
- hhdintranet[.]vg
- ids-intranet[.]de
- intranet[.]arab
- intranet[.]cfd
- intranet[.]mba
- intranet[.]nyc
- intranet3[.]fr
- intranet365[.]vg
- intranetapp[.]it
- intranet-bs[.]ch
- intranetey[.]com
- intranetgun[.]vg
- intranet-gw[.]ws
- intranet-ivt[.]de
- intranet-old[.]ws
- intranetpsw[.]vg
- intranetrd[.]vg
- intranets[.]shop
- intranetsa[.]net
- intranetsma[.]com
- jul-intranet[.]de
- lbg-intranet[.]nl
- mtgintranet[.]vg
- nvcintranet[.]xn--node
- oelcintranet[.]ca
- oi-intranet[.]fr
- pintranet[.]pl
- qmcintranet[.]ws
- skintranet[.]be
- smuintranet[.]vg
- spcintranet[.]ws
- spintranet[.]ws
- tcaintranet[.]org
- tccintranet[.]gq
- wb-intranet[.]de
- wbuintranet[.]vg
- ww-intranet[.]nl

2023年3月21日時点の悪意あるサイバースクワッティングドメインの例

- 1sharepointprofile[.]com
- apagcosyst-sharepoint[.]com
- astridenterprise-sharepoint[.]net
- basecampadventurepakistan[.]com
- basecampuscom[.]top
- basecampus-com[.]top
- findauthorizationsharepoint[.]com
- info-sharepoint[.]top
- info-sharepoints[.]top
- intranetey[.]com
- irisintranet[.]dev
- mysharepoint-onedrive[.]com
- sharepointnote[.]cfd
- sharepoint-payment-invoice[.]ml
- websharepoint[.]sbs
- wvv-basecamp-us[.]com
- wvv-basecamp-us[.]top
- wvw-basecamp-us[.]com
- zohoc[.]net
- zoho-hero[.]com