Facebook のビジネスアカウントをお持ちですか？ Ducktail にご注意を

目次

1. 要旨
2. 付録：アーティファクトと IoC の例

要旨

WithSecure が最近、Facebook ビジネスアカウントのオーナーや広告主を狙った「Ducktail」と呼ばれる不正行為の情報を公開しました。Ducktail はベトナムの事業者が運営していると思われ、マルウェアを使って被害者からデータを盗み、脆弱な Facebook ビジネスアカウントを乗っ取ります。

WithSecure のレポートには、1,885 件の IoC（セキュリティ侵害インジケーター）が列挙されています。当社では、このうち 1,747 件（1,739 件の電子メールアドレスと 8 件のドメイン名）を IoC 拡張調査の出発点として分析しました。WHOIS、IP アドレス、DNS の広範な情報を駆使して深く掘り下げることで、以下のことがわかりました。

- IoC として特定されたメールアドレスのうち、有効なものは 429 件のみ。
- IP アドレスに名前解決する IoC は 1 つ（ductai[.]xyz が 58[.]158[.]177[.]102 を指す）。
- 300 件以上のドメイン名が ductai[.]xyz の IP ホストを共有、そのうち 27 件は悪意あるドメイン名。
- 特定された IoC のうち 2 件と同じく、合計 170 件のドメイン名に「ductai」という文字列が含まれている。

当社の分析で得られた追加のアーティファクトのサンプルは、当社ウェブサイトからダウンロードしていただけます。

調査の糸口をつかむ

当社の調査ではまず、WithSecure が特定した IoC を観察することから始めました。

IoC と判定されたドメイン名の Bulk WHOIS Lookup（WHOIS の一括検索）を行ったところ、現在有効な WHOIS レコードが出力されたのは ductai[.]xyz と ductai90[.]com のみでした。しかし、以下で示すように、「ductai」という文字列が使われていること以外に、2 つのドメイン名に共通点はありませんでした。

- ductai[.]xyz のレジストラは GoDaddy, LLC、ductai90[.]com のレジストラは GMO インターネット。

- ductai[.]xyz の新規登録日は 2020 年 5 月 14 日、ductai90[.]com の新規登録日は 2022 年 11 月 24 日。
- ductai90[.com]のみ、Value-Domain が提供する個人情報保護サービスを利用。ductai[.]xyz では、ドメイン名登録者のメールアドレス欄が空白。
- ductai[.]xyz の登録者の所在国は米国、ductai90[.]com の登録者の所在国は日本。

次に 2 つのドメイン名の DNS 検索を行ったところ、ductai[.]xyz は共用 IP アドレス、具体的には 58[.]158[.]177[.]102 に解決されました。この IP アドレスを IP Geolocation Lookup で検索した結果、WHOIS レコードと同様、起源が日本にあることが示されました。また、マルウェアチェックにより、このホストに悪意があることが判明しました。

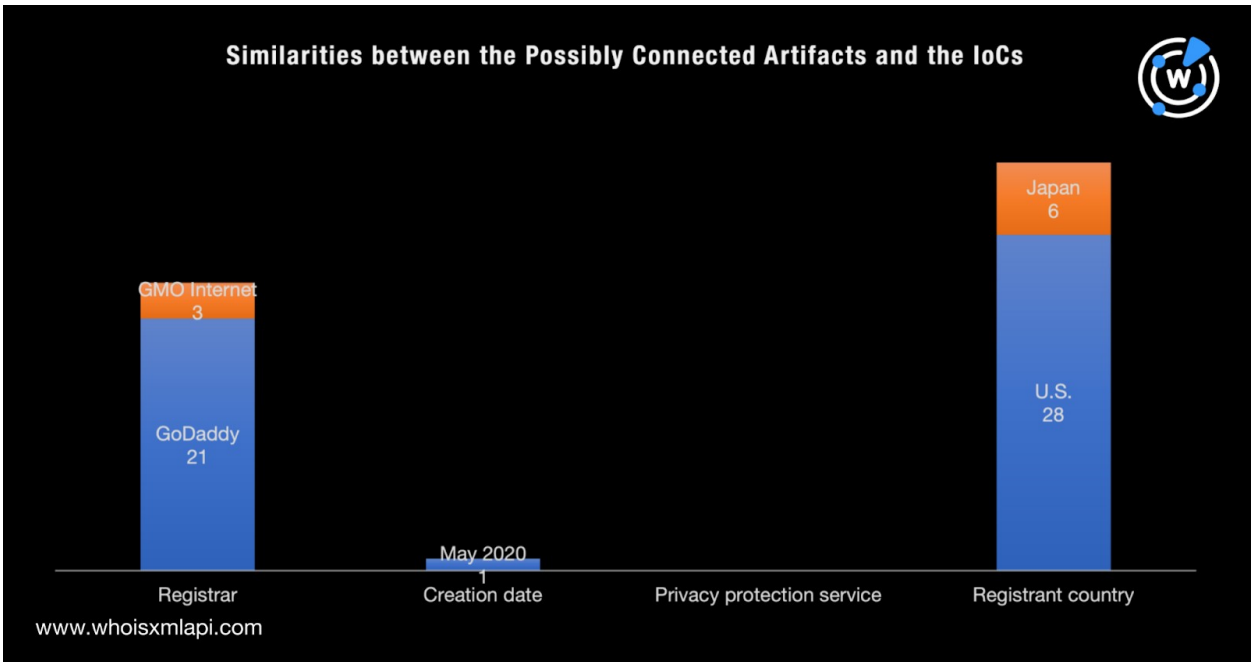
そして、IoC と認識されたメールアドレスを Bulk Email Verification Lookup（一括メール検証検索）にかけたところ、有効なメールアドレスは 25%しかありませんでした。残りの 75%はすべて SMTP（Simple Mail Transfer Protocol）チェックに失敗し、メッセージの送受信ができないことを示しました。

さらに調査を拡大

さらに調査を広げ、関連している可能性のある他のアーティファクトを見つけるため、同じ IP アドレスに結びついたドメイン名のリストを DNS Lookup で取得しました。その結果、少なくとも 300 件のドメイン名が悪意ある IP アドレス 58[.]158[.]177[.]102 をホストとして使っていることがわかりました。関連づけられたドメイン名の数が多いことから、この IP アドレスは共用ホストと思われます。しかし、これらのウェブプロパティについて一括マルウェアチェックをかけたところ、悪意あるものが 27 件検出されました。

また、前述の 2 つの IoC に含まれていた 「ducktai」という文字列を Domains & Subdomains Discovery で検索し、他の潜在的脅威ベクトルがないか探してみました。その結果、170 件のドメイン名が特定されました。いずれも現在マルウェアエンジンで検出されないものですが、WHOIS レコードが取得可能な 66 件のドメイン名とその 2 つの IoC の間に、以下の類似性があることがわかりました。

- 24 件のドメイン名（GoDaddy：21、GMO インターネット：3）が 2 つの IoC と同じレジストラを利用している。
- ductai[.]xyz が新規に登録された月（2020 年 5 月）と同じタイミングで新規登録されたドメイン名がもう 1 つある。
- 34 のドメイン名（米国：28、日本：6）が上記の IoC と同じ国で登録されている。

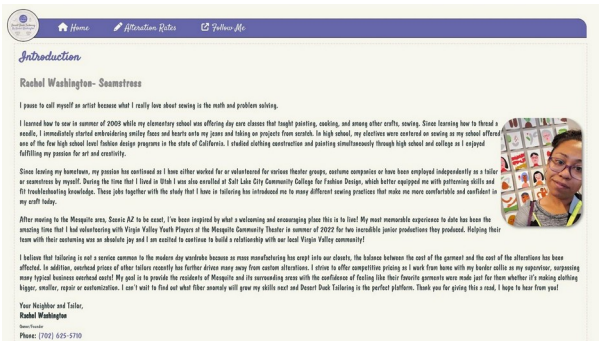


「ducktai」を含むドメイン名の Screenshot Lookup でも、以下の興味深い結果が出ました。

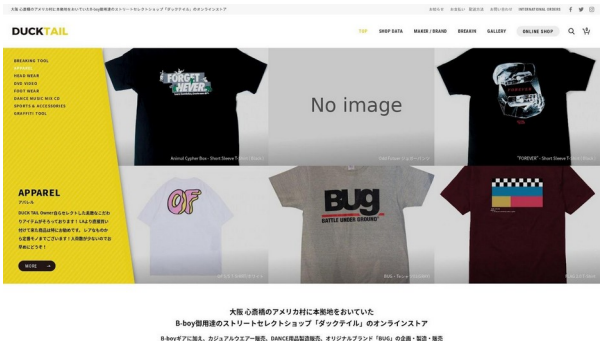
- Ducktails-watusi[.]com の見た目は Facebook ビジネスアカウントのページで、Ducktail の標的に似ている。

ducktails-watusi[.]com のスクリーンショット

- それらのドメイン名は、以下を含む共通のテーマを持ったサイトを指している。
    - 仕立てサービス、衣料品、アクセサリー

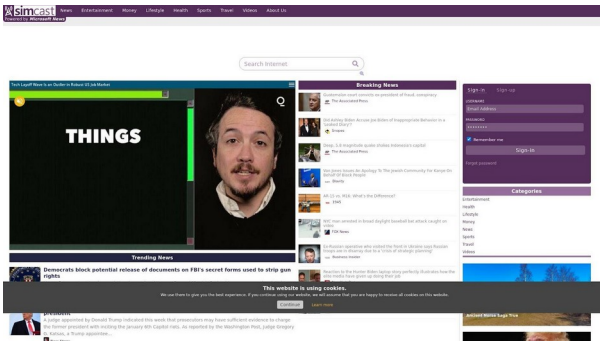


desertducktailoring[.]com のスクリーンショット

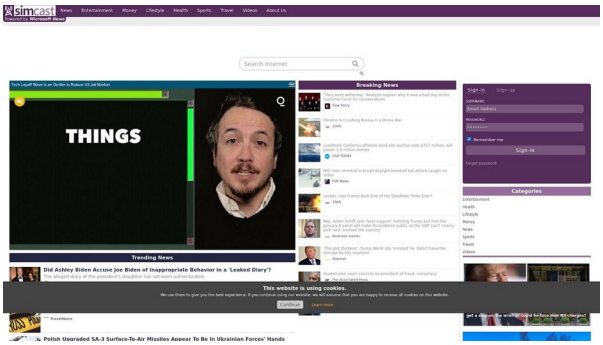


ducktail-jp[.]com のスクリーンショット

- コンテンツのシミュレーション

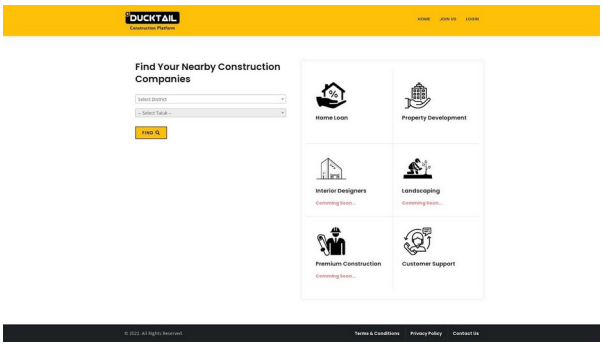


ducktail-jp[.]ph のスクリーンショット

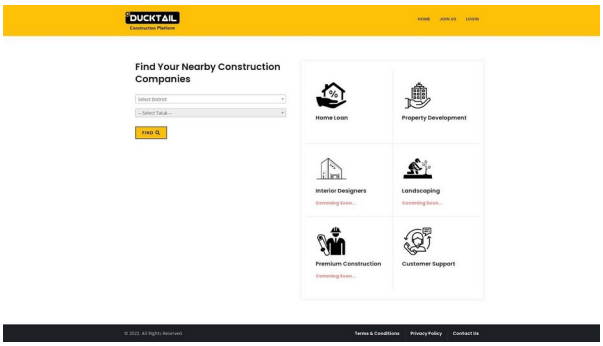


ducktailfox[.]ph のスクリーンショット

- 建設



ducktail[.]co[.]in のスクリーンショット



ducktail[.]in のスクリーンショット

- 自動車、カー用品

ducktailauto[.]co[.]za のスクリーンショット

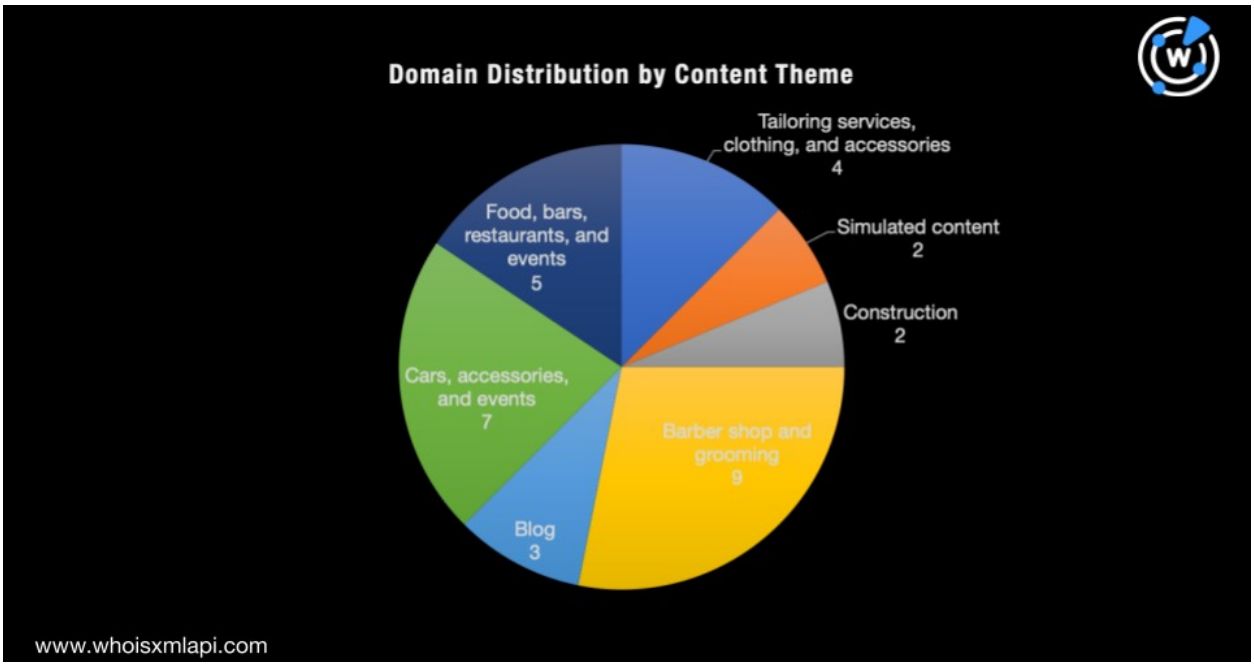
ducktailautomotive[.]co[.]za のスクリーンショット

- 食品、バー、レストラン、イベント

ducktailskitchen[.]com のスクリーンショット

ducktailsnfins[.]com のスクリーンショット

上記のドメイン名はいずれも悪意あるものではありませんが、脅威の名前を文字列として含んでいます。そのため、こうしたドメイン名のいずれかが悪用されやすいとわかれば、脅威アクターはそれを不正行為に利用しようとするかもしれません。下の図は、各種テーマのコンテンツをホストしているドメイン名の数を示しています。



—

当社の IoC 拡張調査により、悪意ある IP アドレス 1 件とマルウェアを含んだドメイン名 27 件を特定しました。また、さらに 500 近くのアーティファクトを確認できました。

同様の調査をご希望のお客様、または本調査の全データをご希望のお客様は、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

IoC として識別された有効なメールアドレスの例

- albertandrew[.]facebook@gmail[.]com
- alice32lor@hotmail[.]com
- bangthangsfatr@gmail[.]com
- buttjerry[.]facebook@gmail[.]com
- chrisjamees[.]facebook@gmail[.]com
- enecildne@gmail[.]com
- erichenderson[.]facebook@gmail[.]com
- jessicca[.]facebook@gmail[.]com
- larmincessdf@gmail[.]com
- louisnathan[.]facebook@gmail[.]com
- luatquysvat@gmail[.]com
- paulettec9iij@hotmail[.]com
- saingghuy@gmail[.]com
- thomsonemily[.]facebook@gmail[.]com
- trinan95fe@hotmail[.]com
- uthertyiiu@gmail[.]com
- worstaustadny@gmail[.]com
- a13sella@hotmail[.]com
- addieu1sarah@hotmail[.]com
- adell_cs159[.]ejzc@outlook[.]com
- adellmarieux@hotmail[.]com

- agnes_cc63[.]lbw@outlook[.]com
- alana_xm90[.]rmu@outlook[.]com
- alberta_sz903[.]zths@outlook[.]com
- alda_pt368[.]vmf@outlook[.]com
- alda_rr461[.]hop@outlook[.]com
- alice237sophie@hotmail[.]com
- alice23werin@hotmail[.]com
- alicealdaovp3@hotmail[.]com
- alicia_pk31[.]ohwk@outlook[.]com
- alyce_as34[.]eeb@outlook[.]com
- alyssa_no325[.]zxh@outlook[.]com
- alyssaemeliaykxy@hotmail[.]com
- amy_mf014[.]zfrv@outlook[.]com
- amycoq2y@hotmail[.]com
- amylorrilj@hotmail[.]com
- ana_zf559[.]avf@outlook[.]com
- anan8ylottie@hotmail[.]com
- andrea_dq67[.]sjhn@outlook[.]com
- andrea_mv955[.]qham@outlook[.]com
- anjelica_ou55[.]pjui@outlook[.]com
- anjene04y@hotmail[.]com
- ann_do361[.]wojl@outlook[.]com
- anna_ev878[.]fwo@outlook[.]com
- antmubessie@hotmail[.]com
- antoinette_es312[.]lpap@outlook[.]com
- antoinetteczm10@hotmail[.]com
- antoinetteshvpp@hotmail[.]com
- april_fh88[.]tpc@outlook[.]com
- arlenersssdenise@hotmail[.]com

ある IoC の IP アドレスと同じ IP アドレスに名前解決するドメイン名の例

- 10080[.]site
- 1685810[.]com
- 1cake[.]top
- 44740[.]xyz
- 4k[.]chemscalere[.]com
- 58x158x177x102[.]ap58[.]ftth[.]ucom[.]ne[.]jp
- 8788912[.]com
- 9awi[.]pw
- a[.]chemscalere[.]com
- abiesvc[.]com
- abiesvc[.]info
- ac[.]chemscalere[.]com
- account[.]chemscalere[.]com
- accountforuser[.]website
- ace[.]1cake[.]top
- acebookmap[.]top
- acessonet[.]chemscalere[.]com
- acpzamakmz[.]com
- ad[.]chemscalere[.]com
- add[.]1cake[.]top
- admindirector[.]com
- ado[.]1cake[.]top
- adobephotostage[.]com
- adp[.]1cake[.]top
- adq[.]1cake[.]top
- adr[.]1cake[.]top
- ads[.]1cake[.]top
- adserver[.]doesntexist[.]org
- adserver[.]dyndns-free[.]com
- adsl[.]chemscalere[.]com
- adslgp[.]chemscalere[.]com
- adt[.]1cake[.]top
- adu[.]1cake[.]top
- adv[.]1cake[.]top
- advanceorthocenter[.]com
- adw[.]1cake[.]top
- adx[.]1cake[.]top
- ady[.]1cake[.]top
- aea[.]1cake[.]top
- aeb[.]1cake[.]top
- aebankonline[.]com
- aec[.]1cake[.]top
- aef[.]1cake[.]top
- aeg[.]1cake[.]top
- aei[.]1cake[.]top
- aek[.]1cake[.]top
- aeternam[.]me

- afghannewsnetwork[.]com
- agent[.]chemscalere[.]com
- ahaizyb86[.]com

悪意があると判定されたドメイン名の例

- 10080[.]site
- 1685810[.]com
- 1cake[.]top
- admindirector[.]com
- aeternam[.]me
- asphspes[.]com
- benjamiilliams[.]icu
- benzerold[.]com
- bhomes[.]cc
- cardchsk[.]com
- cardkuys[.]com
- careerhuawei[.]net
- cargisite[.]com
- cloudistcdn[.]com
- congci[.]info
- dangquanwatch[.]com
- dataupdates[.]live
- devguardmap[.]org
- diplomatsign[.]com
- eofficeupdating[.]com

「ducktai」という文字列を含むドメイン名の例

- ducktail[.]com
- ducktails[.]uk
- ducktail[.]xyz
- ducktails[.]biz
- ducktails[.]org
- educktail[.]com
- ducktails[.]xyz
- ducktail[.]blog
- mrducktail[.]uk
- ducktails[.]com
- ducktails[.]net
- ducktail2[.]com
- ducktailen[.]net
- ducktail[.]co[.]uk
- rsducktail[.]com
- ducktails[.]info
- ducktail[.]store
- ducktail-jp[.]ph
- ducktailmr[.]com
- ducktailfox[.]ph
- ducktailbar[.]de
- ducktailen[.]com
- ducktail33[.]com
- ducktailor[.]com
- mrducktail[.]com
- ducktailfox[.]de
- ducktail[.]co[.]in
- ducktails[.]farm
- ducktail888[.]jp
- ducktailfx[.]com
- ducktailinc[.]com
- harducktail[.]com
- ducktails[.]co[.]uk
- theducktails[.]it
- ducktailrun[.]com
- ducktail[.]online
- ducktailfox[.]com
- ducktails[.]co[.]za
- ducktail-jp[.]com
- ducktail[.]events
- ducktailsoap[.]com
- hardducktail[.]com
- ducktainment[.]com
- ducktailshop[.]com
- ducktailfarm[.]biz
- mrducktail[.]co[.]uk
- ducktailhair[.]com
- rajaducktail[.]com
- ducktailsemb[.]net
- ducktails-bar[.]de