Own a Facebook Business? Beware of Ducktail

Table of Contents

Executive Report

WithSecure recently unveiled a malicious campaign dubbed "Ducktail," which trailed its sights on Facebook business owners and advertisers. Believed to be run by Vietnamese operators, Ducktail uses malware to steal data from victims and hijack vulnerable Facebook business properties.

The WithSecure report enumerated 1,885 indicators of compromise (IoCs). We used 1,747 of these (i.e., 1,739 email addresses and eight domains) as jump-off points for our IoC expansion exercise. Our deep dive aided by extensive WHOIS, IP, and DNS intelligence led to the following discoveries:

- Only 429 of the email addresses identified as IoCs were valid.
- Only one of the IoCs currently resolved to an IP address—ductai[.]xyz pointed to 58[.]158[.]177[.]102.
- At least 300 other domains shared ductai[.]xyz's IP host, 27 of which were malicious.
- A total of 170 domains contained the string "ductai," akin to two of the identified IoCs.

At First Glance

We began our investigation by observing the IoCs WithSecure identified.

We subjected the domains identified as IoCs to a bulk WHOIS lookup, which showed that only two of them had retrievable current WHOIS records—ductai[.]xyz and ductai90[.]com. Apart from the use of the string "ductai," though, they didn't share any other similarities, as evidenced by the following:

- Ductai[.]xyz's registrar is GoDaddy, LLC, while ductai90[.]com's was GMO Internet, Inc.
- Ductai[.]xyz was created way back on 14 May 2020, while ductai90[.]com was created on 24 November 2022.

- Only ductai90[.]com used a privacy protection service, specifically provided by Value-Domain. Ductai[.]xyz left its registrant email address field blank.
- Finally, ductai[.]xyz named the U.S. as its registrant country, while ductai90[.]com indicated Japan.

Next, we conducted DNS lookups for the domains and found that only one—ductai[.]xyz—resolved to a shared IP address, specifically 58[.]158[.]177[.]102. As with its WHOIS record, an IP geolocation lookup for this host showed Japan as its origin. A malware check revealed the host is malicious.

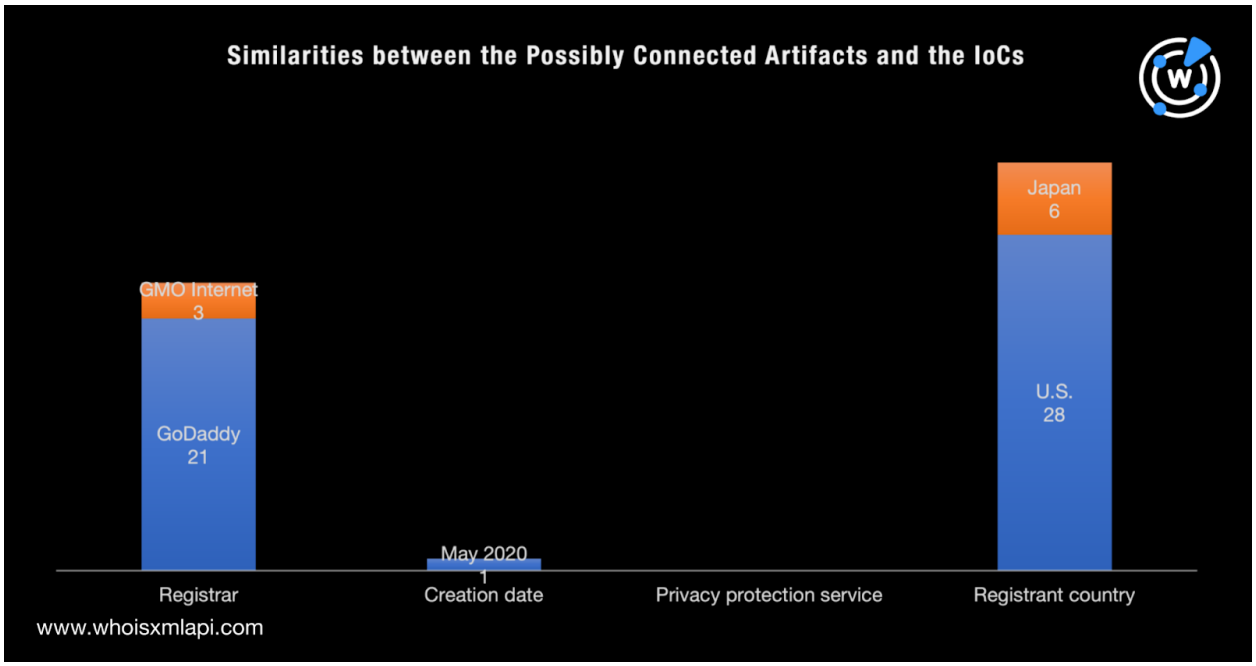
Finally, we subjected the email addresses identified as IoCs to a bulk email verification lookup and found that only 25% were valid. The remaining 75% all failed the Simple Mail Transfer Protocol (SMTP) check, which meant they can't send or receive messages.

The Deep Dive

We sought to find potentially connected artifacts and began by obtaining a list of IP-connected domains via DNS lookups. At least 300 domains shared the malicious IP address 58[.]158[.]177[.]102 as host. The high number of domains indicates the IP address is probably a shared host. However, a bulk malware check for these web properties showed that 27 were malicious.

Earlier, we noted the appearance of the text string "ducktai" in two of the IoCs. We used the string as a Domains & Subdomains Discovery search term to identify other potential threat vectors. That led to the discovery of 170 other domains. None of them are currently being detected by malware engines but we did notice similarities between the 66 with retrievable WHOIS records and the IoCs, including:

- A total of 24 additional domains (21 for GoDaddy and three for GMO Internet) shared the IoCs' registrars.
- One additional domain shared ductai[.]xyz's creation month (May 2020).
- Some 34 additional domains (28 for the U.S. and six for Japan) shared the IoCs' registrant countries.

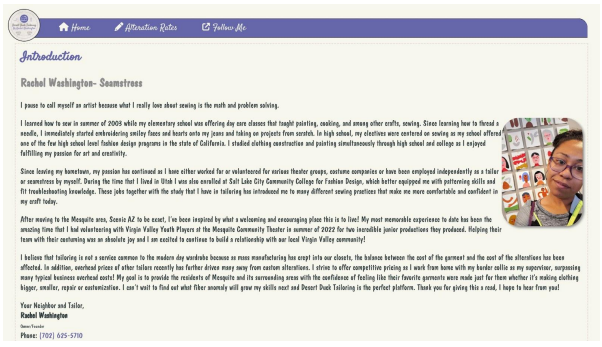


Screenshot lookups for the “ducktai”-containing domains also yielded interesting results, including:

- Ducktails-watusi[.]com looks like a Facebook business page, akin to Ducktail’s targets.

Screenshot of ducktails-watusi[.]com

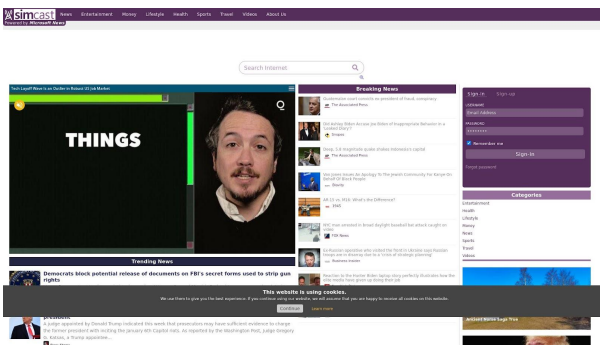
- The domains pointed to sites with common themes, including:
    - Tailoring services, clothing, and accessories



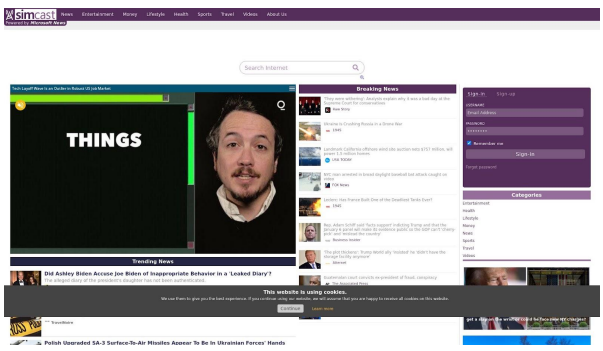
Screenshot of desertducktailoring[.]com

Screenshot of ducktail-jp[.]com

    - Simulated content

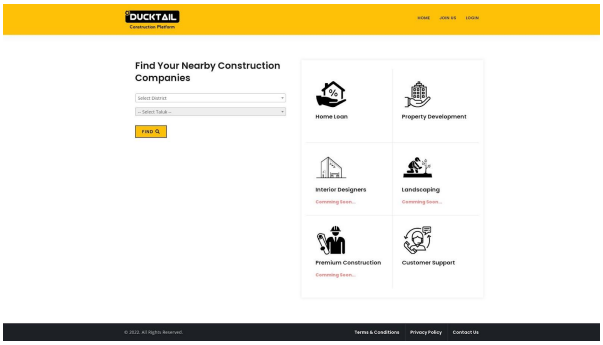


Screenshot of ducktail-jp[.]ph

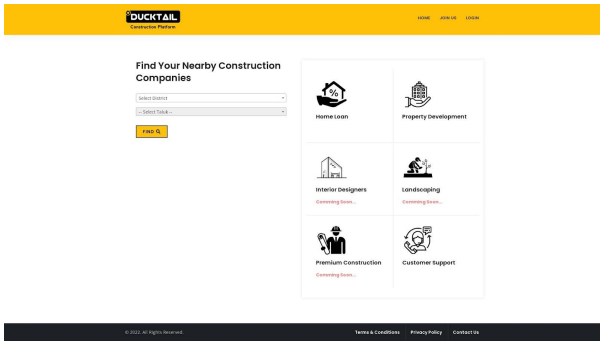


Screenshot of ducktailfox[.]ph

- Construction



Screenshot of ducktail[.]co[.]in



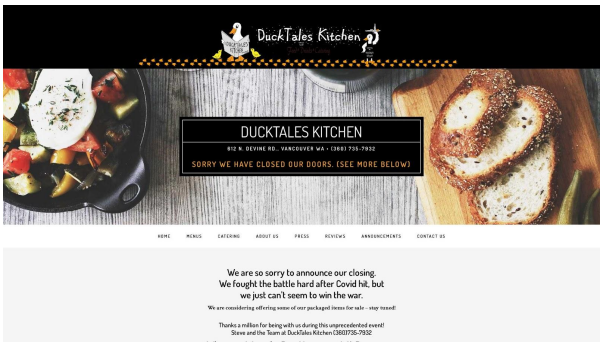
Screenshot of ducktail[.]in

- Cars and accessories

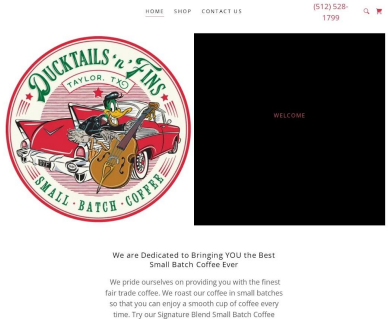
Screenshot of ducktailauto[.]co[.]za

Screenshot of ducktailautomotive[.]co[.]za

- Food, bars, restaurants, and events

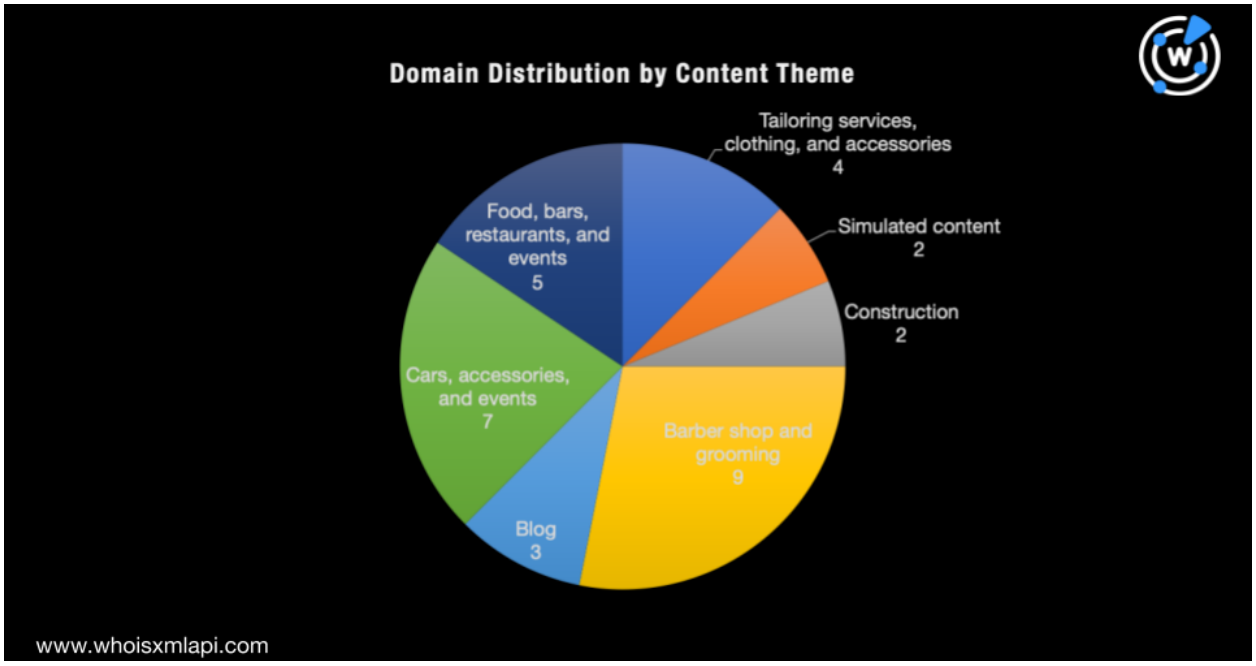


Screenshot of ducktailskitchen[.]com



Screenshot of ducktailsnfins[.]com

Note that none of the domains above are malicious, but given that they shared the threat's name, should any of them turn out to be vulnerable to exploitation, the threat actors may be tempted to use them for malicious campaigns. The diagram shows how many of the additional domains hosted content that fell under the various themes we identified above and other ones.



—

Our IoC expansion exercise allowed us to identify a malicious IP address and 27 malware-laden domains. We also identified nearly 500 additional artifacts.

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 Valid Email Addresses Identified as IoCs

- 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

Sample Domains That Shared One IoC's IP Host

- 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

Sample Domains Deemed Malicious

- 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

Sample Domains Containing the String “ducktai”

- 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