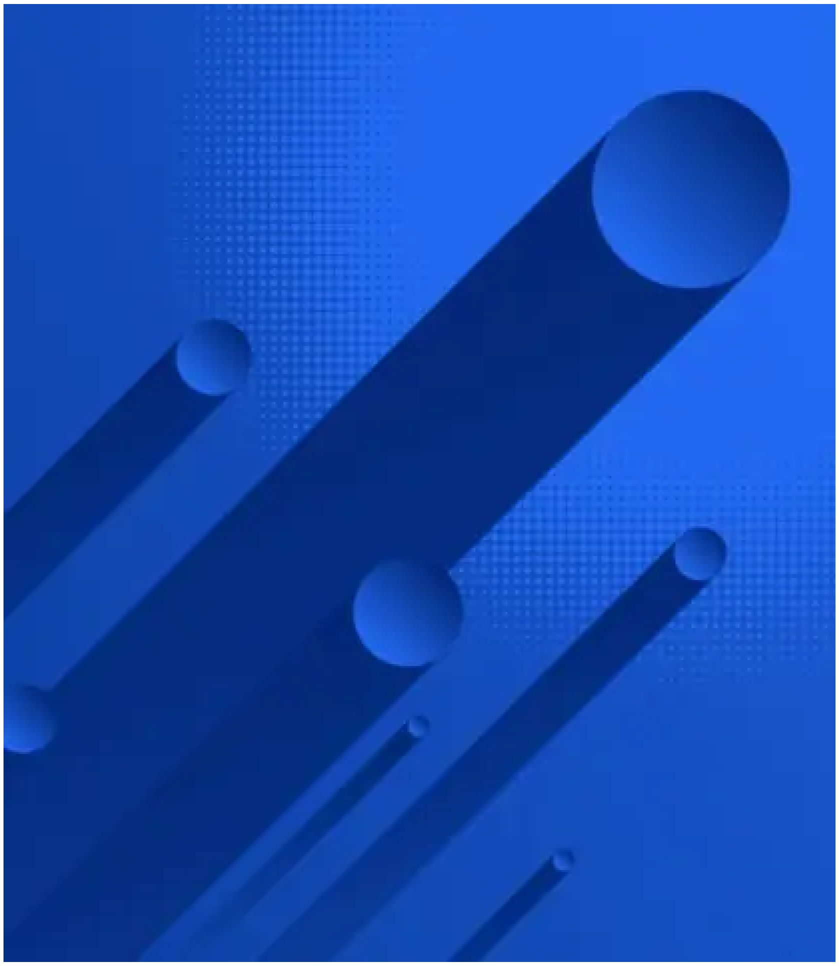
DuckTail | ThreatLabz

zscaler.com/blogs/security-research/look-ducktail

Sudeep Singh, Naveen Selvan



Introduction

In our persistent quest to decode DuckTail's maneuvers, Zscaler ThreatLabz began an intelligence collection operation in May 2023. Through an intensive three-month period of monitoring, we obtained critical details about DuckTail's operational framework. This expedition granted us unprecedented visibility into DuckTail's end-to-end operations, spanning the entire kill chain from reconnaissance to post-compromise.

Our team yielded valuable insights into DuckTail's intrusion techniques, compromise tactics, post-compromise procedures, and the underground economy. These insights, some of which have never been publicly documented, provide a panoramic view of their targets and an understanding of their strategic motives.

This report dives into the operational mechanics of DuckTail, dissecting the anatomy of their tactics, techniques and procedures (TTPs), and tracing the trajectory of stolen data.

Key Takeaways

- **Ideal Social Engineering Target:** DuckTail threat actors primarily target users working in the digital marketing and advertising space. Unfortunately, the tech layoffs occurring in 2022 and 2023 introduced more eager candidates into the digital market - meaning more prime targets for DuckTail.
- **Raiding Business and Ad Accounts:** DuckTail targets Facebook and TikTok business accounts, and Google ad accounts. Stolen social media business accounts feed an underground economy where these accounts are traded among other users in Vietnamese Telegram groups.
- **Social Engineering as the Distribution Method:** DuckTail's primary distribution vector continues to be social engineering through LinkedIn messaging. Threat actors set up fake LinkedIn recruiter profiles and fake job postings impersonating popular companies to lure unsuspecting victims looking for employment.
- **Expanding and Always Evolving:** DuckTail continues to expand the list of cloud services abused for hosting and distributing payloads.
- **Exploiting Themes of Innovative AI Online Tools:** DuckTail threat actors have successfully weaponized the recent popularity of generative AI platforms, such as ChatGPT and Google Bard AI, to lure victims to install malicious software.
- **Stealthy and Strategic Maneuvers:** DuckTail threat actors use private residential proxy services to log in to compromised social media business accounts to prevent raising any security alarms. In addition, they abuse the "Encrypted notifications" Facebook feature to prevent the victim from performing an account recovery.

Brief Overview

DuckTail is an operation that involves multiple Vietnam-based threat actors who share the same tactics, techniques, and procedures (TTPs). They also share the same motivation: gain access to social media business accounts, specifically ones belonging to digital marketers.

DuckTail malware steals saved session cookies from browsers, with code specifically tailored to take over Facebook business accounts.The malware is typically spread on LinkedIn, where threat actors post fake job descriptions to "recruit" potential victims.

The “products” of the operation (i.e. hacked social media accounts) feed an underground economy of stolen social media accounts, where numerous vendors offer accounts priced according to their perceived usefulness for malicious activity. The image below shows a high-level overview of how DuckTail threat actors abuse different cloud services and social media platforms in their whole operation:

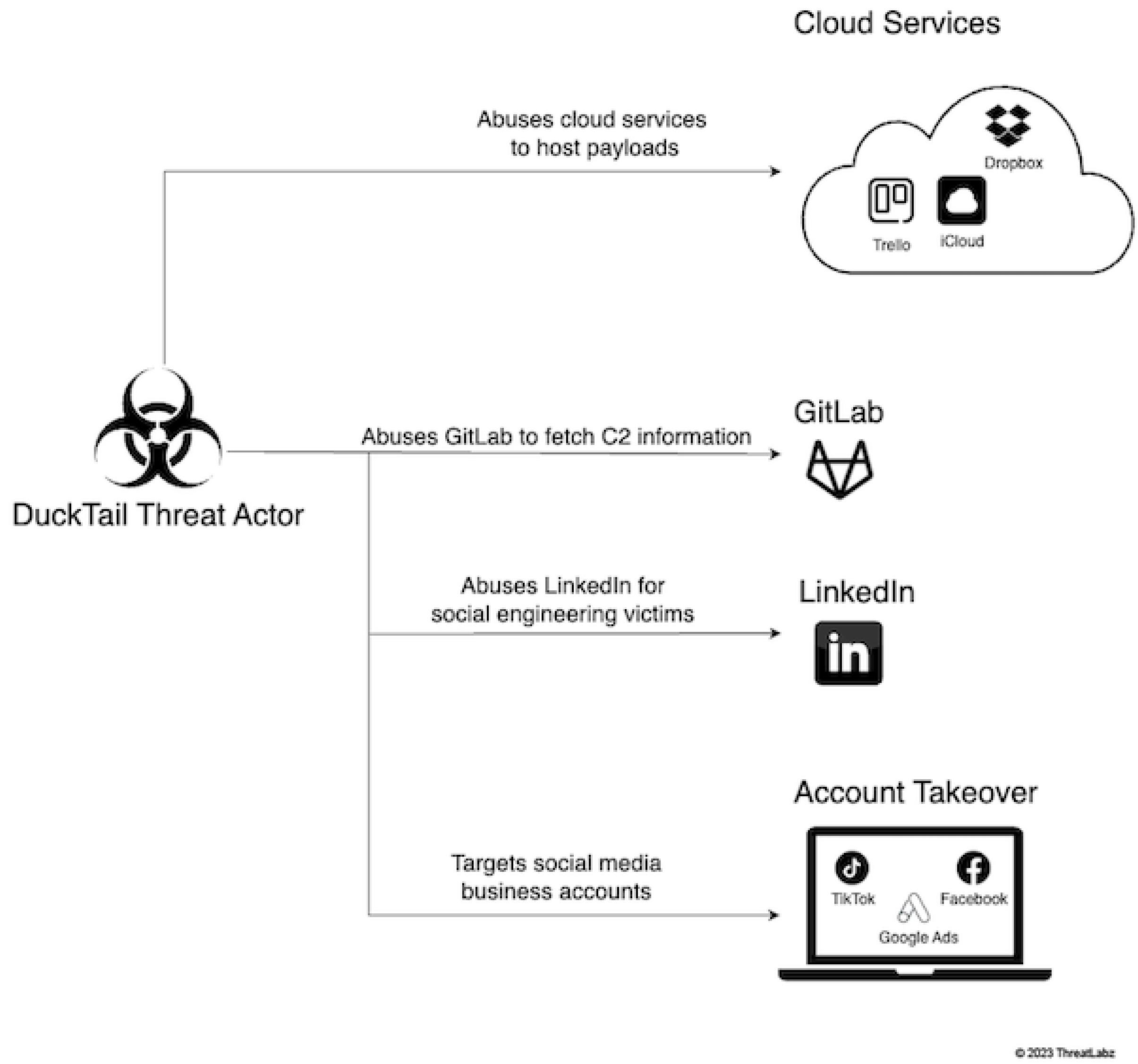

Cloud Services
Abuses cloud services to host payloads
Dropbox
Trello
iCloud
DuckTail Threat Actor
Abuses GitLab to fetch C2 information
GitLab
Abuses LinkedIn for social engineering victims
LinkedIn
Account Takeover
Targets social media business accounts
TikTok
Facebook
Google Ads
© 2023 ThreatLabz

Figure 1: Visual overview illustrating how DuckTail abuses social media and cloud platforms in different stages of their operation.

Unveiling DuckTail’s TTPs

Overview of the architecture

The threat research community is already abundant with great articles that address the technical details of DuckTail’s malware payload.

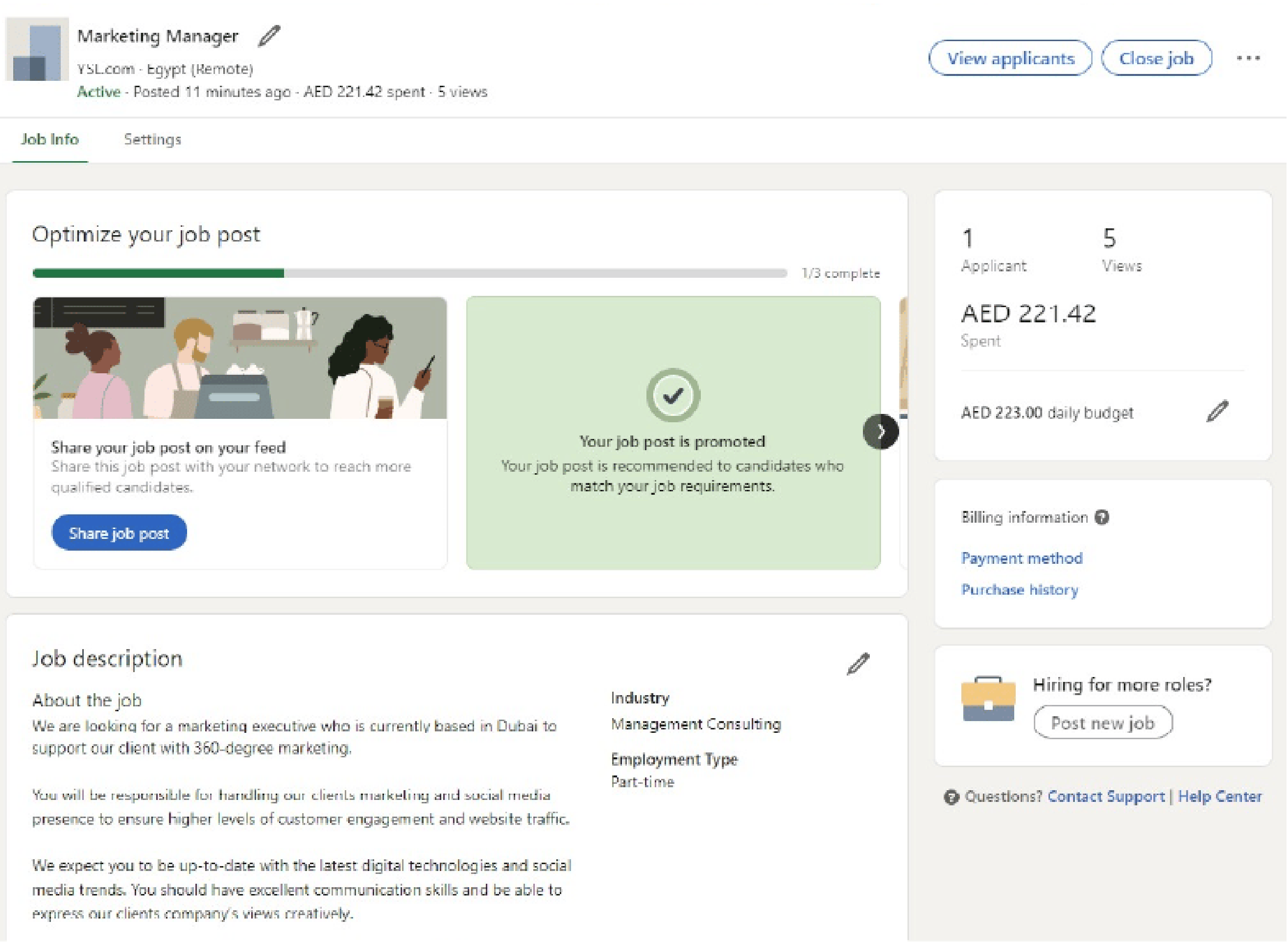
Distribution methods and techniques

The following sections break down:

- the infection vectors employed by Ducktail
- what those infection campaigns look like

Fake Job Posts on LinkedIn

DuckTail primarily reaches victims by posting fake marketing-related job listings on LinkedIn. The threat actors presume that the marketing professionals who apply likely have access to ad accounts. The image below is an example of a fake job post on LinkedIn used by Ducktail to lure an unsuspecting candidate.



Marketing Manager

YSL.com · Egypt (Remote)

Active · Posted 11 minutes ago · AED 221.42 spent · 5 views

Optimize your job post

1/3 complete

Share your job post on your feed

Share this job post with your network to reach more qualified candidates.

Your job post is promoted

Your job post is recommended to candidates who match your job requirements.

1 Applicant

5 Views

AED 221.42 Spent

AED 223.00 daily budget

Hiring for more roles?

Job description

About the job

We are looking for a marketing executive who is currently based in Dubai to support our client with 360-degree marketing.

You will be responsible for handling our clients marketing and social media presence to ensure higher levels of customer engagement and website traffic.

We expect you to be up-to-date with the latest digital technologies and social media trends. You should have excellent communication skills and be able to express our clients company's views creatively.

Industry

Management Consulting

Employment Type

Part-time

© 2023 ThreatLabz

Figure 2: This is what the threat actor sees moments after setting up a fake marketing job post on LinkedIn. It's worth noting that the post is promoted.

In addition to creating fake job posts on LinkedIn, threat actors also set up profiles on LinkedIn impersonating recruiters. To facilitate social engineering tactics, in some cases, threat actors add the “Hiring” banner to their LinkedIn profile picture. This catches the attention of users actively seeking a new job.

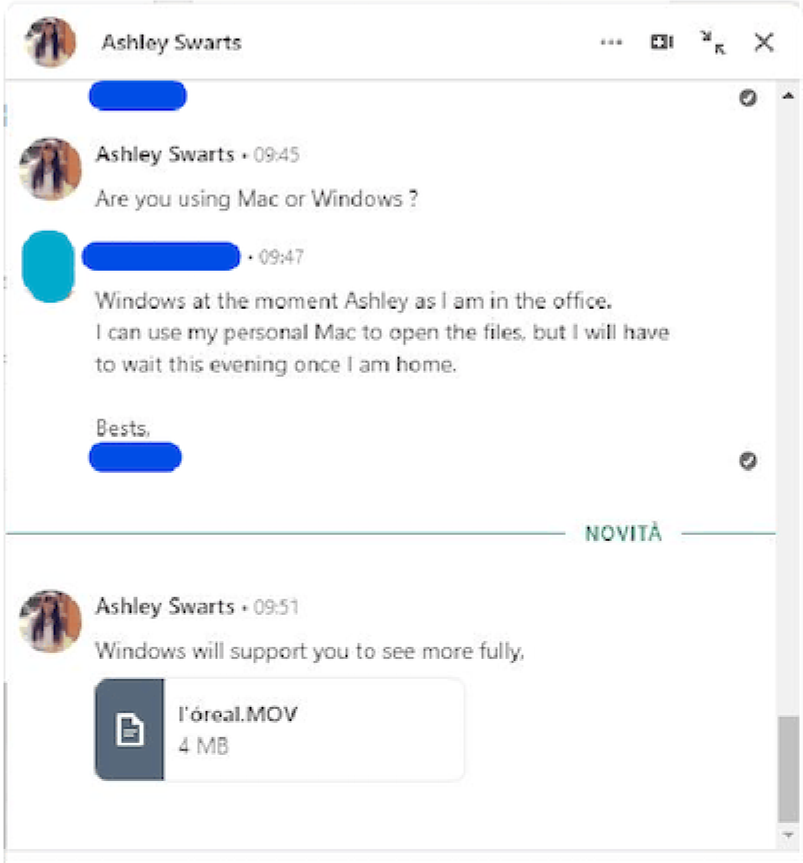
Once a potential victim responds to a bait post, the “recruiter” will send a message on LinkedIn.

How it works

The threat actors will ask the interested applicant to review the job application package by:

1. Downloading an archive
2. Opening it on a Windows machine
3. Double-clicking the executable (camouflaged as another type of file) inside it

To maximize their chance of infection, some threat actors create instructional videos showing victims how to “properly” infect their own devices. The image below shows this tactic in action:



Ashley Swarts

[redacted]

Ashley Swarts • 09:45
Are you using Mac or Windows ?

[redacted] [redacted] • 09:47
Windows at the moment Ashley as I am in the office.
I can use my personal Mac to open the files, but I will have to wait this evening once I am home.

Bests,
[redacted]

NOVITÀ

Ashley Swarts • 09:51
Windows will support you to see more fully.

l'óreal.MOV
4 MB

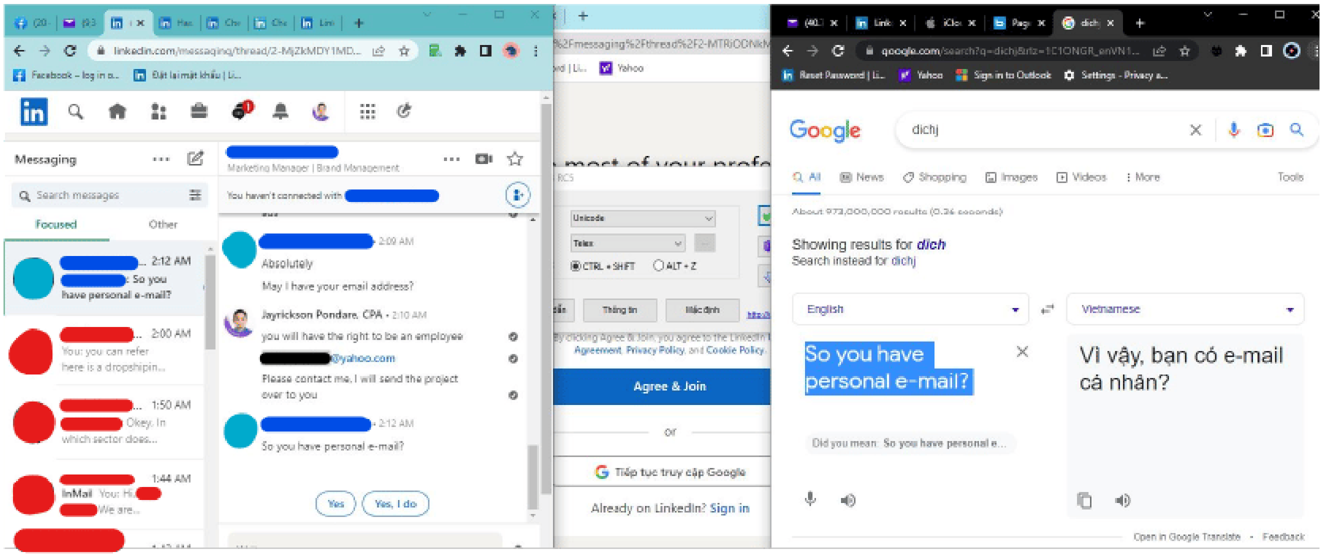
© 2023 ThreatLabz

Figure 3: “Ashley Swarts” (a fake threat actor account) instructing a victim on how to open the fake job application package.

The nuances of language

The threat actor’s English proficiency closely matches the English language skills of an average Vietnamese cybercriminal, not an American HR professional.

Our team observed threat actors using Google Translate to communicate with potential victims. The image below shows a threat actor translating messages from English to Vietnamese in real-time as they communicate with a victim. The predominant use of the Vietnamese language also supports our attributing DuckTail to Vietnamese threat actors.



[redacted] 2:12 AM
[redacted]: So you have personal e-mail?

[redacted] 2:00 AM
You: you can refer here is a dropshipin...

[redacted] 1:50 AM
[redacted] Okey. In which sector does...

[redacted] 1:44 AM
InMail You: Hi [redacted] We are...

[redacted]

You haven't connected with [redacted]

[redacted] • 2:09 AM
Absolutely
May I have your email address?

Jayrickson Pondare, CPA • 2:10 AM
you will have the right to be an employee
[redacted]@yahoo.com
Please contact me, I will send the project over to you

[redacted] • 2:12 AM
So you have personal e-mail?

About 973,000,000 results (0.36 seconds)

Showing results for *dịch*
Search instead for dichj

By clicking Agree & Join, you agree to the LinkedIn User Agreement, Privacy Policy, and Cookie Policy.

So you have personal e-mail?

Did you mean: So you have personal e...

Vì vậy, bạn có e-mail cá nhân?

© 2023 ThreatLabz

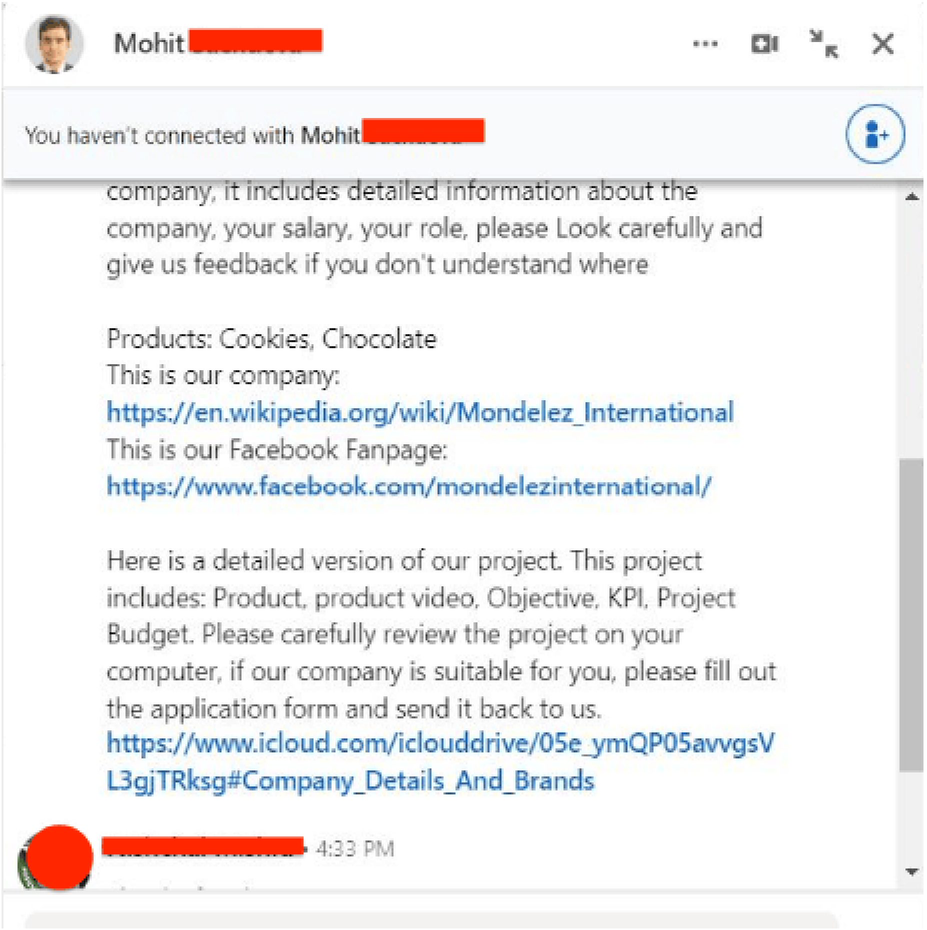
Figure 4: A threat actor using Google Translate to communicate in English while handling multiple fraudulent job application conversations on LinkedIn.

Impersonating real companies

DuckTail threat actors send job offers impersonating popular organizations and brands to entice job seekers.

In the image below, a threat actor leveraged a compromised LinkedIn account to message a victim with job opportunity details. While impersonating a real company called Mondelez International, this threat actor sent the following in their message:

- a link to the company's real Wikipedia and Facebook page
- an iCloud URL hosting an archive file containing the malware



Mohit [redacted]

You haven't connected with Mohit [redacted]

company, it includes detailed information about the company, your salary, your role, please Look carefully and give us feedback if you don't understand where

Products: Cookies, Chocolate
This is our company:
https://en.wikipedia.org/wiki/Mondelez_International
This is our Facebook Fanpage:
https://www.facebook.com/mondelezinternational/

Here is a detailed version of our project. This project includes: Product, product video, Objective, KPI, Project Budget. Please carefully review the project on your computer, if our company is suitable for you, please fill out the application form and send it back to us.
https://www.icloud.com/iclouddrive/05e_ymQP05avvgsVL3gjTRksg#Company_Details_And_Brands

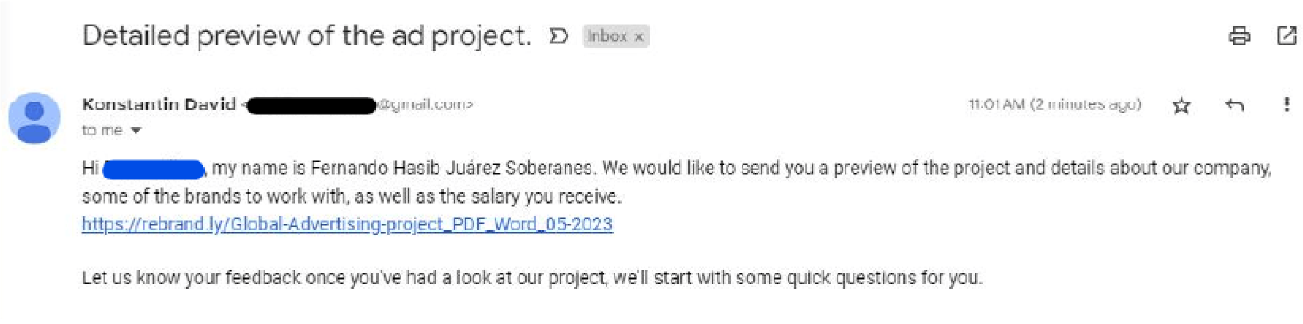
[redacted] [redacted] 4:33 PM

© 2023 ThreatLabz

Figure 5: A threat actor messaging a victim on LinkedIn and impersonating a real company.

Spear phishing emails

Our team also observed cases where threat actors sent infected archive links through email, after making initial contact on LinkedIn. The image below shows a spear phishing email example.



Detailed preview of the ad project.

Konstantin David <[redacted]@gmail.com>
to me

11:01 AM (2 minutes ago)

Hi [redacted], my name is Fernando Hasib Juárez Soberanes. We would like to send you a preview of the project and details about our company, some of the brands to work with, as well as the salary you receive.
https://rebrand.ly/Global-Advertising-project_PDF_Word_05-2023

Let us know your feedback once you've had a look at our project, we'll start with some quick questions for you.

© 2023 ThreatLabz

Figure 6: A spear phishing email sent to a victim containing the URL shortener link, which downloads the malicious archive file.

.NET executables as a common thread in DuckTail binaries

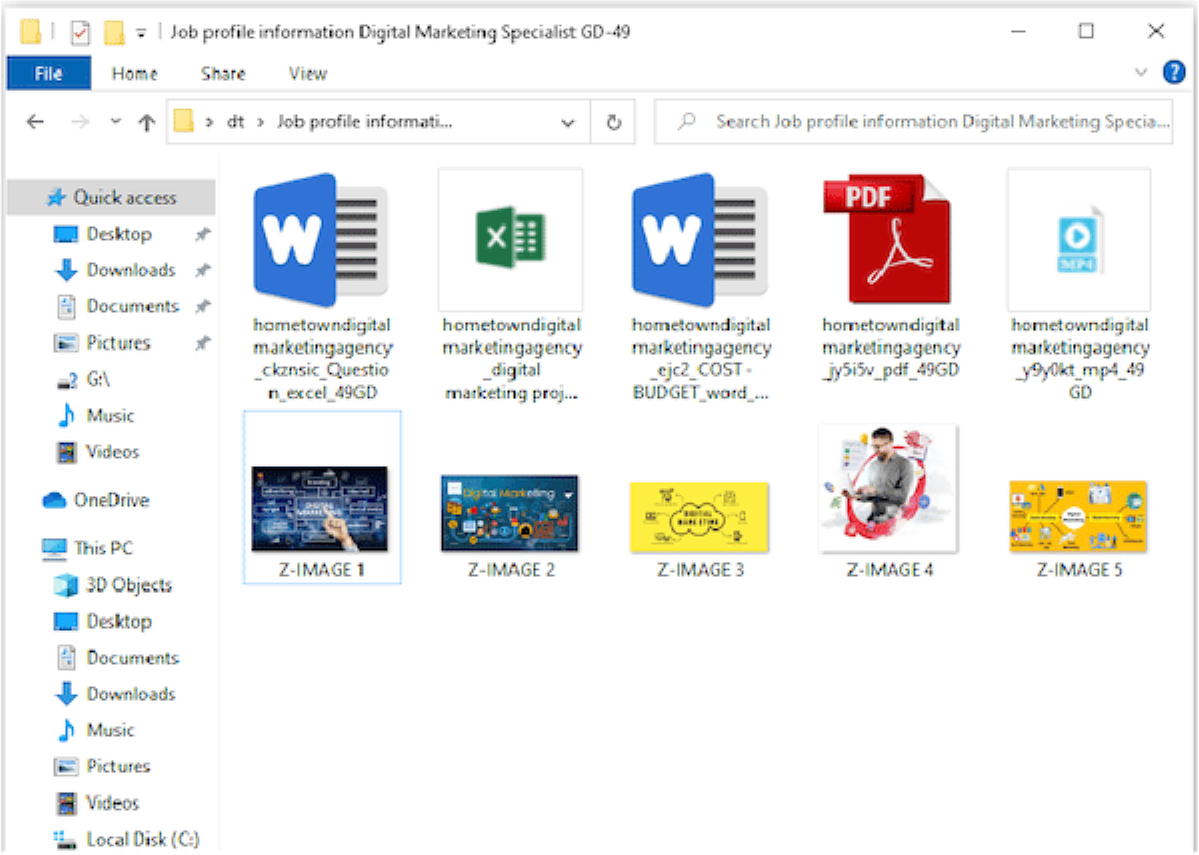
Most commonly, DuckTail's malware payload is a .NET executable, but this is not always the case. Some Ducktail payloads come in an Excel add-in or browser extension.

The .NET executables family associated with the Ducktail variants share the following attributes:

- Large file sizes, in most cases - around 70 MB or more
- Includes a fake Office or PDF document icon
- Contains a decoy document with details about the fake job offer/marketing advertisement, which opens right after execution
- Signed with valid code-signing certificates belonging to Vietnamese publishers (sometimes)
- Makes use of Telegram for C2 communications

The executable is usually delivered in an archive, together with image and video files. The images below depict two common archive variations.

Type 1 Archive


Job profile information Digital Marketing Specialist GD-49
File
Home
Share
View
dt › Job profile informati...
Search Job profile information Digital Marketing Specia...
Quick access
Desktop
Downloads
Documents
Pictures
G:\
Music
Videos
OneDrive
This PC
3D Objects
Desktop
Documents
Downloads
Music
Pictures
Videos
Local Disk (C:)
hometowndigitalmarketingagency_ckznsic_Question_excel_49GD
hometowndigitalmarketingagency_digital marketing proj...
hometowndigitalmarketingagency_ejc2_COST - BUDGET_word_...
hometowndigitalmarketingagency_jy5i5v_pdf_49GD
hometowndigitalmarketingagency_y9y0kt_mp4_49GD
Z-IMAGE 1
Z-IMAGE 2
Z-IMAGE 3
Z-IMAGE 4
Z-IMAGE 5

© 2023 ThreatLabz

Figure 7: Type 1 Archive - .exe files with fake icons (first row), together with job-related images

Type 2 Archive

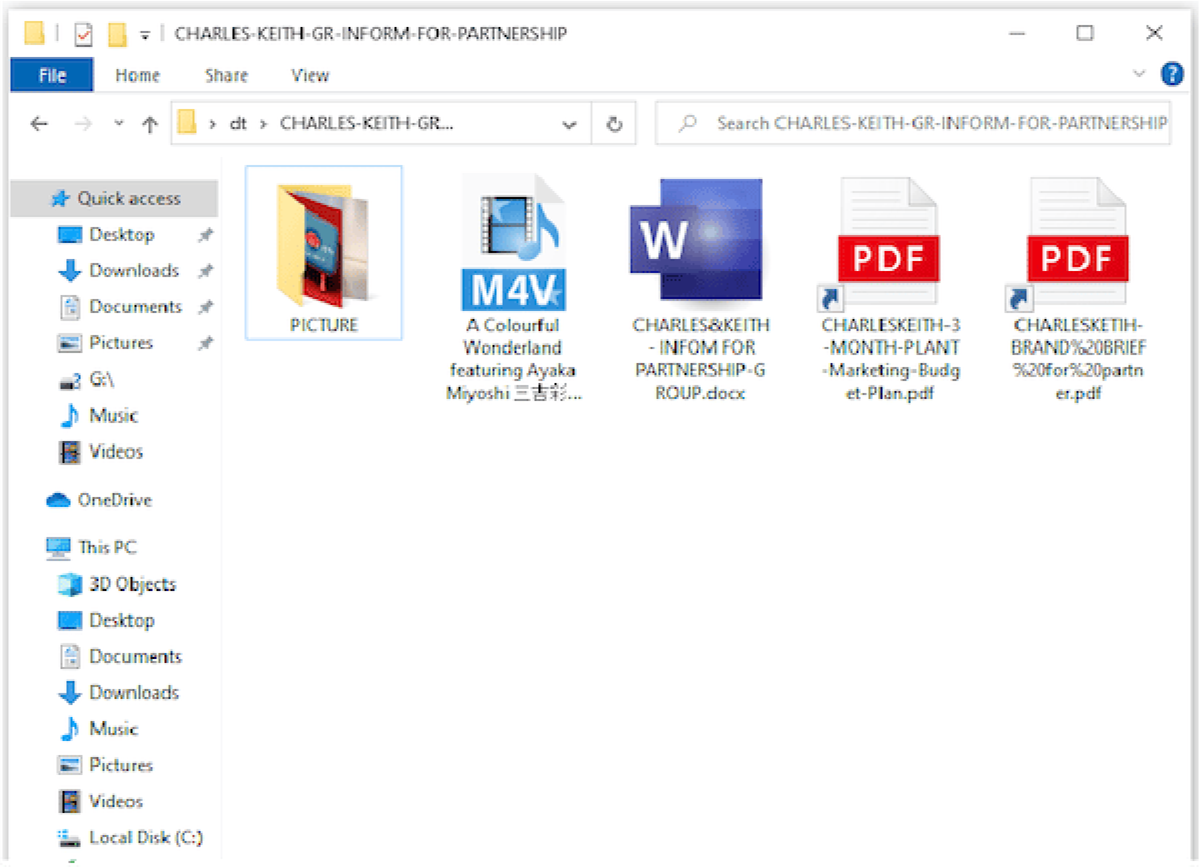
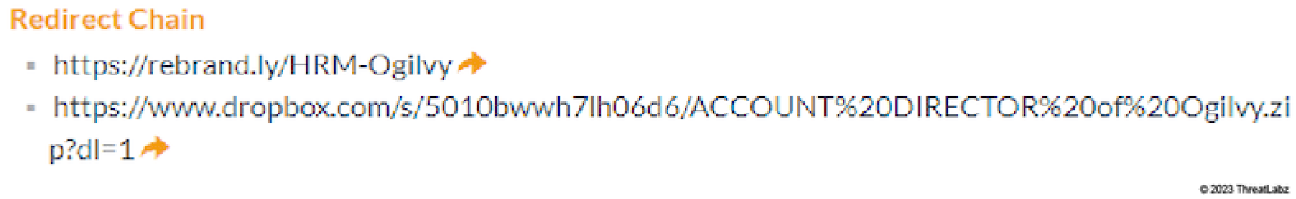

CHARLES-KEITH-GR-INFORM-FOR-PARTNERSHIP
File
Home
Share
View
dt > CHARLES-KEITH-GR...
Search CHARLES-KEITH-GR-INFORM-FOR-PARTNERSHIP
Quick access
Desktop
Downloads
Documents
Pictures
G:\
Music
Videos
OneDrive
This PC
3D Objects
Desktop
Documents
Downloads
Music
Pictures
Videos
Local Disk (C:)
PICTURE
A Colourful Wonderland featuring Ayaka Miyoshi 三吉彩...
CHARLES&KEITH - INFOM FOR PARTNERSHIP-GROUP.docx
CHARLESKEITH-3-MONTH-PLANT-Marketing-Budget-Plan.pdf
CHARLESKETIH-BRAND%20BRIEF%20for%20partner.pdf
© 2023 ThreatLabz

Figure 8: Type 2 Archive - .lnk files with PowerShell payloads, plus .scr executables, both obscured by double extensions (.pdf.lnk, .docx.scr), together with job-related images

Cloud hosting and URL shortening services

Our research team noticed the following patterns when investigating DuckTail's infrastructure:

- Malicious archives are often hosted on public cloud hosting services like iCloud, Google Drive, Dropbox, Transfer.sh, and OneDrive.
- In some cases, threat actors use Trello, a project management platform, as a cloud hosting service by uploading archives as attachments to Trello cards and providing victims with a direct download link to the card.
- Another widely abused platform is Rebrandly (rebrand.ly) - a URL shortener service. Threat actors spread download links generated by Rebrandly to give the download a more legitimate look. You can see the difference that Rebrandly makes in the image below.



Redirect Chain

- https://rebrand.ly/HRM-Ogilvy ➜
- https://www.dropbox.com/s/5010bwwh7lh06d6/ACCOUNT%20DIRECTOR%20of%20Ogilvy.zip?dl=1 ➜

© 2023 ThreatLabz

Figure 9: A redirection chain set up by the threat actor transforms a long, unfriendly Dropbox link into a short rebrand.ly link.

Newly registered domains used to host payloads

In addition to disguising links with Rebrandly, threat actors also registered many custom domains through Rebrandly, spreading shortened links with their own fake company name domains.

Most of these custom domains registered by the threat actor use TLDs like:

- .social
- .software
- .sale
- .click
- .news
- .agency
- .company

For a complete list of newly registered domains used by DuckTail, visit the **Indicators of Compromise (IOCs)** section at the bottom of this blog.

Marketing guides and AI tools

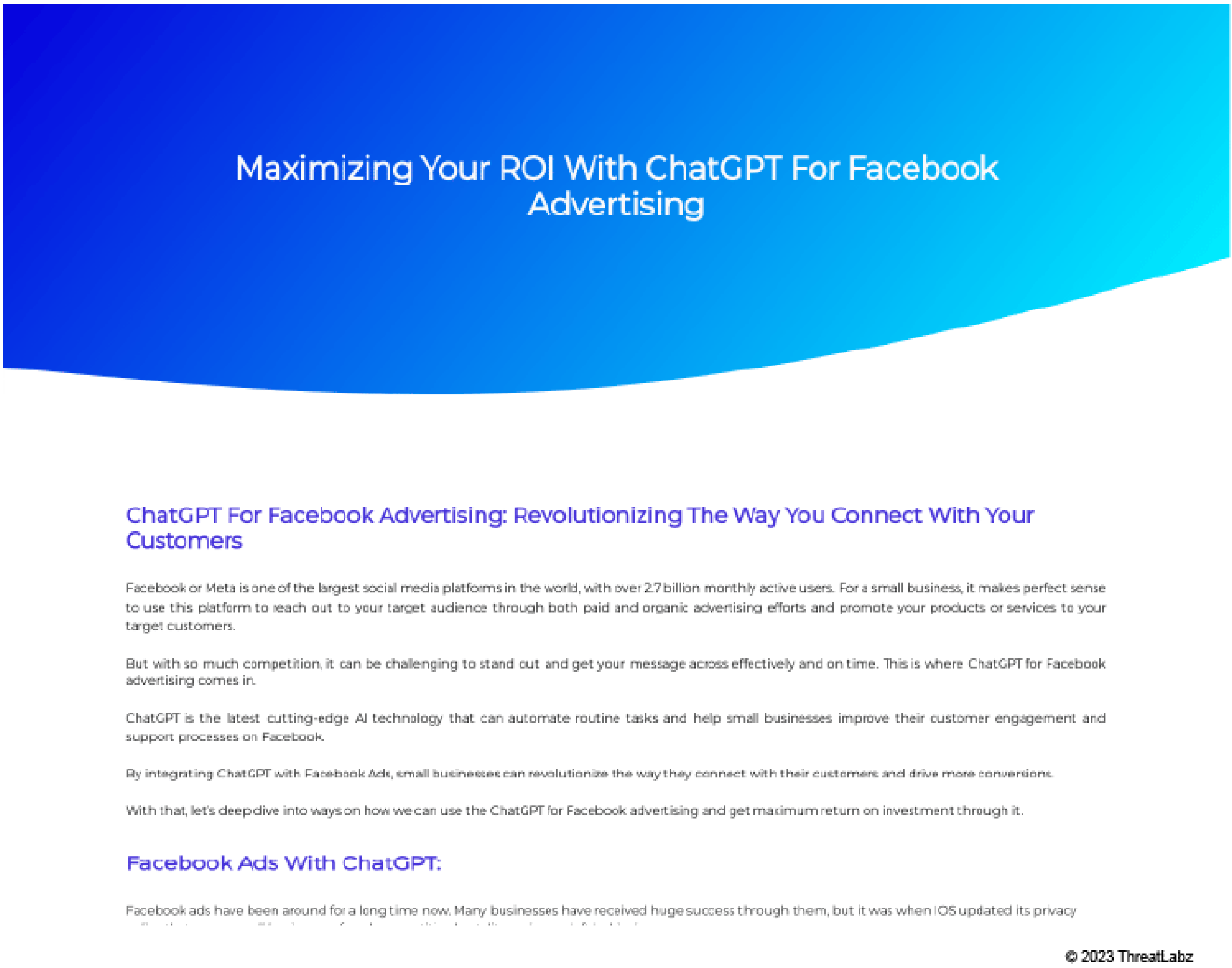
Another method of infection is the creation of web pages pretending to offer marketing guides and marketing software, but actually serving DuckTail malware.

We observed the following legitimate marketing and AI tools spoofed:

- Adplexity
- ClickMinded
- ChatGPT
- Google BardAI

Generative AI softwares, like ChatGPT, are prime targets because they are being increasingly utilized by professionals working in digital marketing, content creation, and advertising.

The image below shows a web page created by a threat actor leveraging ChatGPT for Facebook advertising.



Maximizing Your ROI With ChatGPT For Facebook Advertising

ChatGPT For Facebook Advertising: Revolutionizing The Way You Connect With Your Customers

Facebook or Meta is one of the largest social media platforms in the world, with over 2.7 billion monthly active users. For a small business, it makes perfect sense to use this platform to reach out to your target audience through both paid and organic advertising efforts and promote your products or services to your target customers.

But with so much competition, it can be challenging to stand out and get your message across effectively and on time. This is where ChatGPT for Facebook advertising comes in.

ChatGPT is the latest cutting-edge AI technology that can automate routine tasks and help small businesses improve their customer engagement and support processes on Facebook.

By integrating ChatGPT with Facebook Ads, small businesses can revolutionize the way they connect with their customers and drive more conversions.

With that, let's deepdive into ways on how we can use the ChatGPT for Facebook advertising and get maximum return on investment through it.

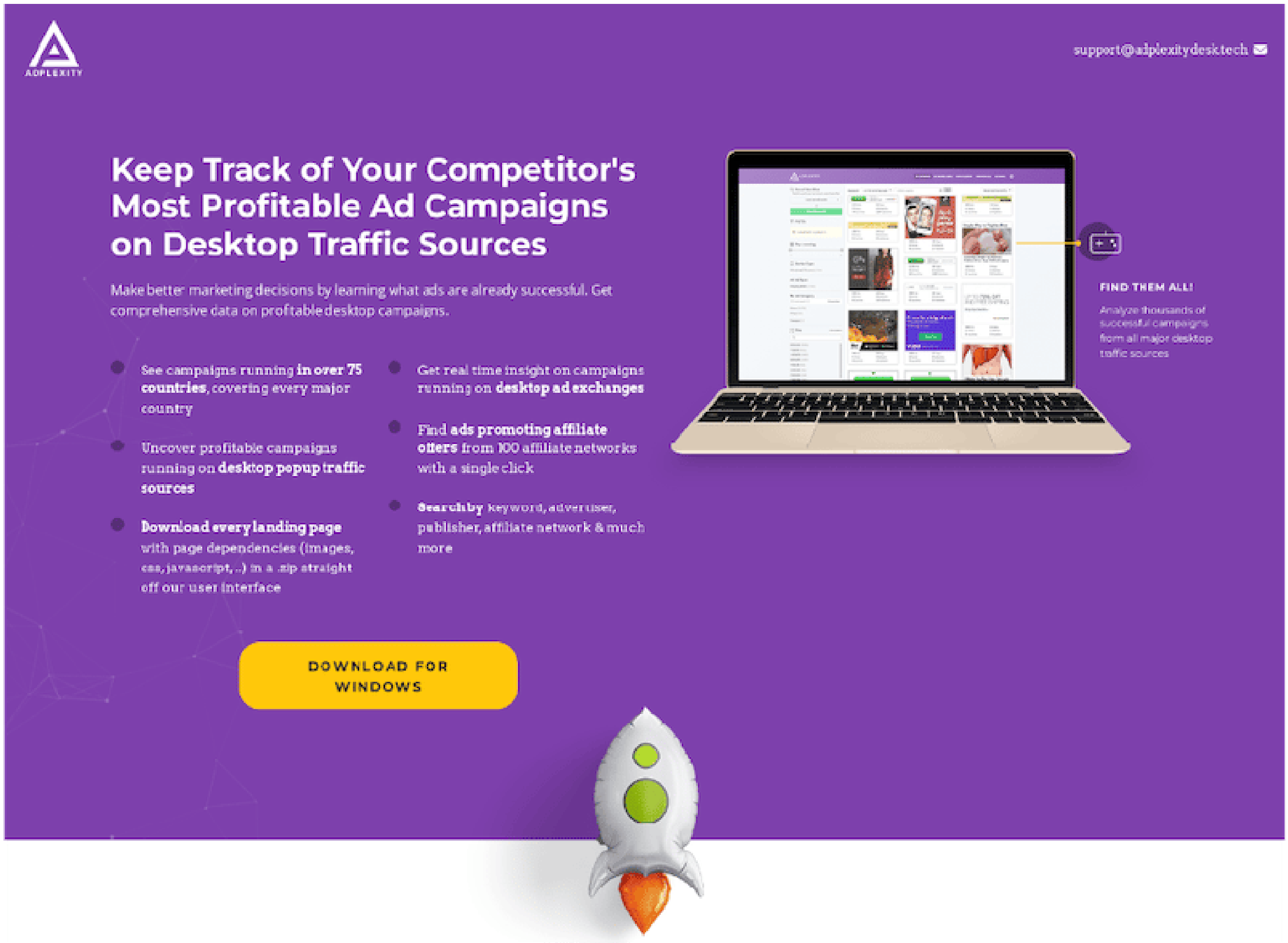
Facebook Ads With ChatGPT:

Facebook ads have been around for a long time now. Many businesses have received huge success through them, but it was when IOS updated its privacy

© 2023 ThreatLabz

Figure 10: A screenshot of newguide[.]tech, a website set up by Ducktail to leverage ChatGPT.

Below, there is another example of a website set up by a threat actor impersonating Adplexity.



Keep Track of Your Competitor's Most Profitable Ad Campaigns on Desktop Traffic Sources

Make better marketing decisions by learning what ads are already successful. Get comprehensive data on profitable desktop campaigns.

- See campaigns running **in over 75 countries**, covering every major country
- Uncover profitable campaigns running on **desktop popup traffic sources**
- **Download every landing page** with page dependencies (images, css, javascript,..) in a .zip straight off our user interface
- Get real time insight on campaigns running on **desktop ad exchanges**
- Find **ads promoting affiliate offers** from 100 affiliate networks with a single click
- **Search by** keyword, advertiser, publisher, affiliate network & much more

FIND THEM ALL!

Analyze thousands of successful campaigns from all major desktop traffic sources

© 2023 ThreatLabz

Figure 11: A screenshot of adplexitydesk[.]tech, a website set up by Ducktail impersonating Adplexity. The download button leads to a Ducktail infected archive.

Insights Gained

In the following sections, we share insights about the threat actors operating DuckTail and the strategies they employ.

Primary targets and industries

While Ducktail is mostly known for targeting Facebook users, we observed threat actors stealing and abusing access to victim accounts on other advertising platforms, namely TikTok Business and Google Ads. This ability to pilfer multiple platforms is due to Ducktail's general-purpose cookie stealing capabilities.

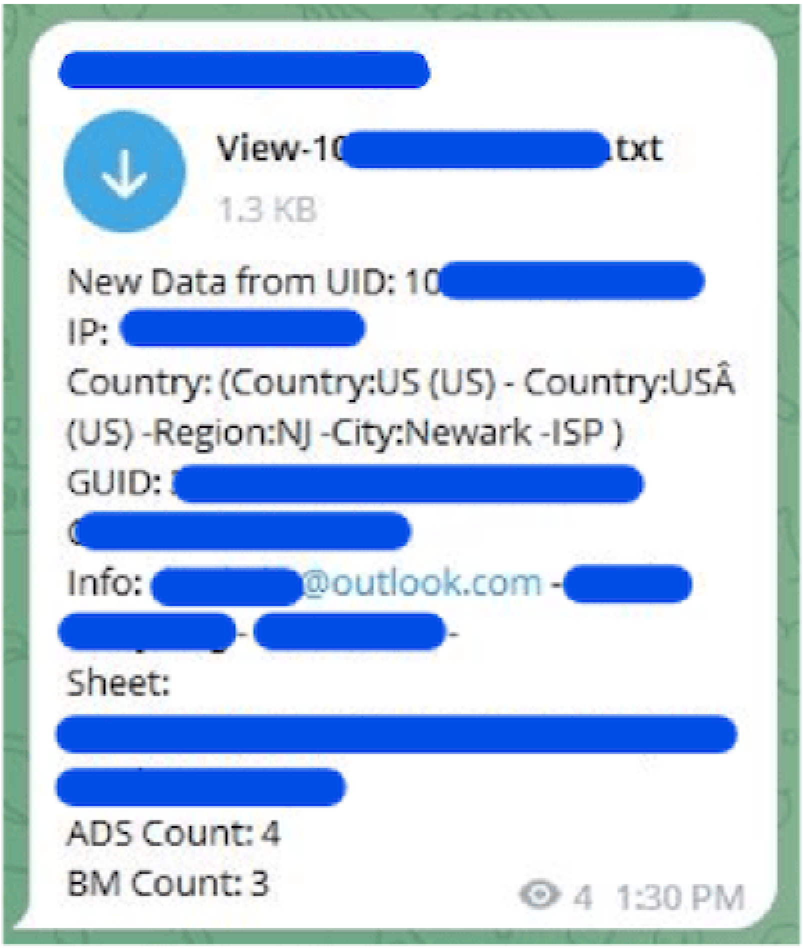
Communication channels and techniques

The threat actors use the following platforms to communicate and trade stolen information:

- Telegram
- Facebook
- Zalo (a Vietnamese messaging app)

The threat actors set up Telegram bots to automatically handle data arriving from new victims. This allows them to pinpoint the most important information, like:

- the victim's Facebook account information
- the number of detected ad accounts
- business manager accounts



[redacted]

View-10[redacted]txt
1.3 KB

New Data from UID: 10[redacted]
IP: [redacted]
Country: (Country:US (US) - Country:USÂ (US) -Region:NJ -City:Newark -ISP)
GUID: [redacted]
[redacted]
Info: [redacted]@outlook.com -[redacted]
[redacted]-[redacted]-
Sheet:
[redacted]
ADS Count: 4
BM Count: 3

4 1:30 PM

© 2023 ThreatLabz

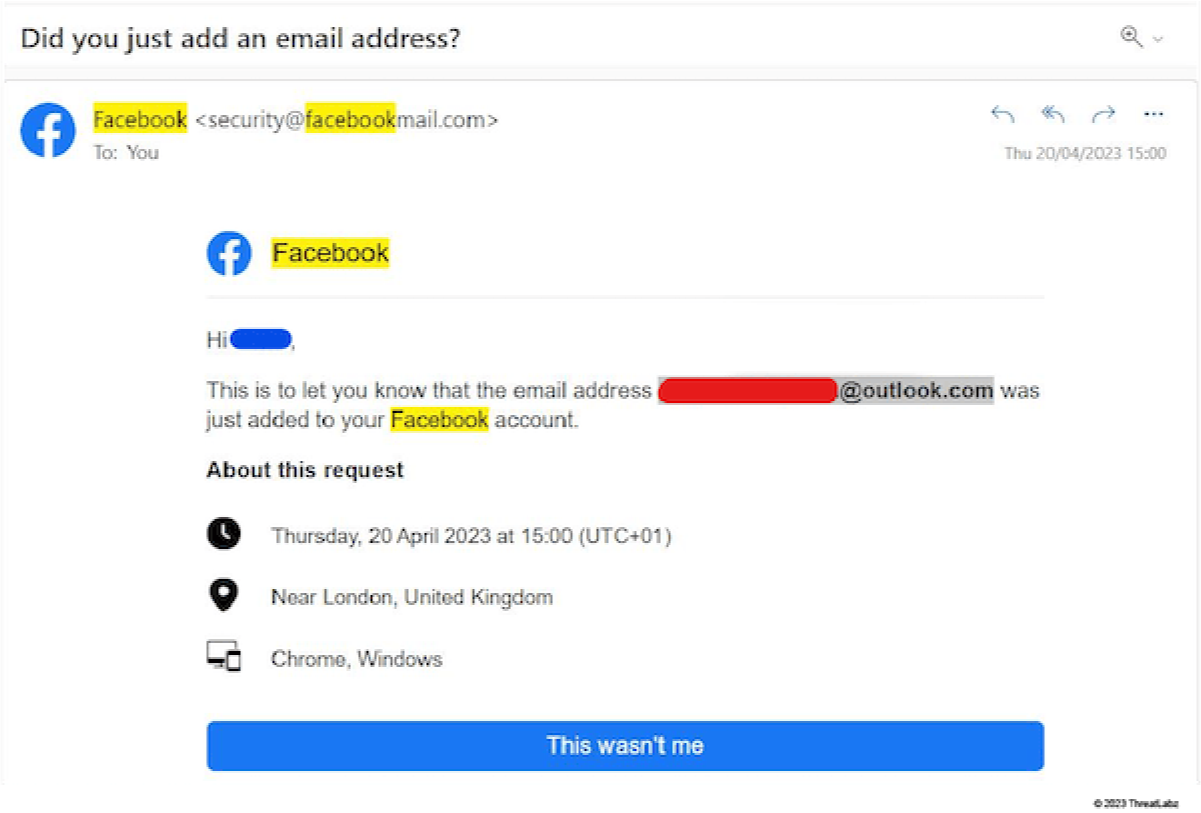
Figure 12: A bot introduces a new victim's Facebook profile. An American with control over four personal ad accounts and three business manager accounts.

Infiltration strategies

Adding threat actor email addresses to compromised accounts

One of the primary methods threat actors use to takeover a victim's compromised account is by adding their own email address to that account.

In the image below, Facebook emailed a security notification to a victim informing them that a threat actor has added an email address to their account.



Did you just add an email address?

Facebook <security@facebookmail.com>

To: You

Thu 20/04/2023 15:00

Facebook

Hi [redacted],

This is to let you know that the email address [redacted]@outlook.com was just added to your Facebook account.

About this request

Thursday, 20 April 2023 at 15:00 (UTC+01)

Near London, United Kingdom

Chrome, Windows

© 2023 ThreatLabz

Figure 13: This screenshot shows a security notification warning a victim about a new email address added to their account - indicating that a Ducktail threat actor has begun a takeover of their Facebook account.

Updating password and email for compromised accounts

DuckTail threat actors change the password and email address of a Facebook account during takeover.

Abusing Facebook Encrypted Notifications feature

We observed an instance where, after taking over a victim's Facebook account, the threat actor enabled the Encrypted Notifications setting. This way every Facebook email communication with the victim is encrypted - effectively preventing the victim from recovering their account.

Using compromised LinkedIn accounts for communication

While investigating communication between threat actors and victims on LinkedIn, we came across instances where threat actors contacted victims using compromised LinkedIn accounts.

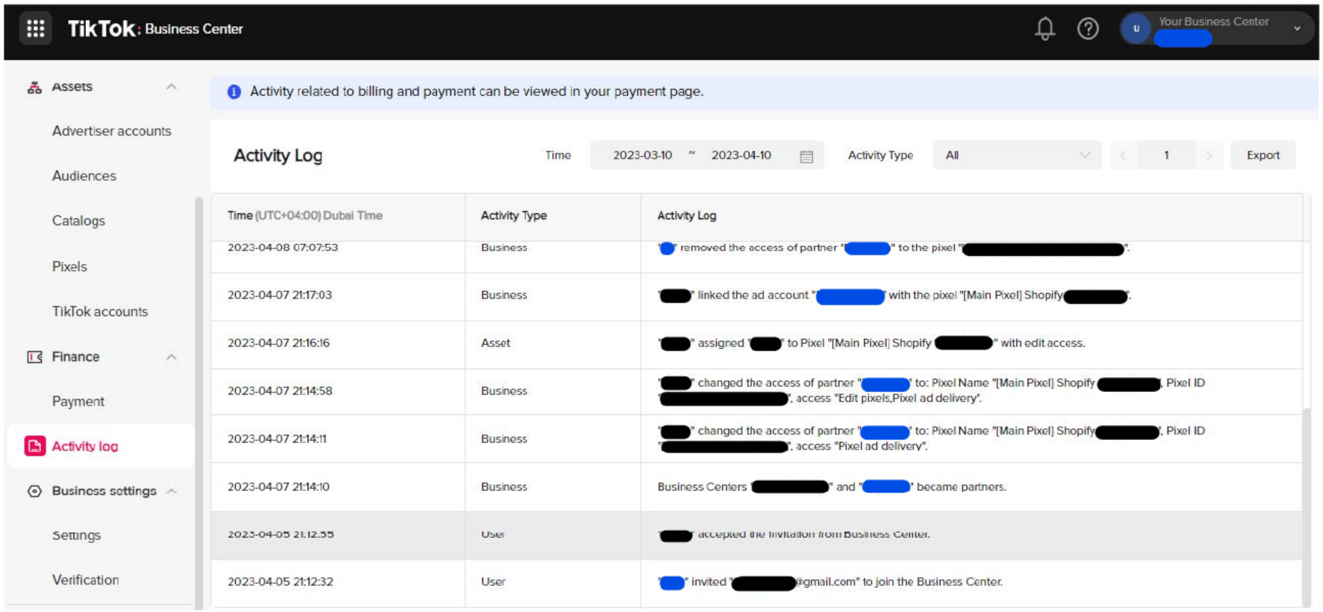
These compromised LinkedIn accounts belonged to users working in the digital marketing space. Some of the compromised LinkedIn accounts had more than 500 connections and 1000 followers. The high amount of connections/followers helped lend authenticity to the compromised accounts and facilitated the social engineering process for threat actors.

How are the threat actors compromising LinkedIn accounts?

- We believe, with a medium-confidence level, that some of these compromised LinkedIn accounts were purchased in underground markets by DuckTail threat actors. We discovered an internal budgeting spreadsheet used by the DuckTail team which details their revenue and expenditures. One of the entries in the spreadsheet corresponded to the purchase of LinkedIn accounts.
- We believe, with a high-confidence level, that threat actors are compromising the LinkedIn accounts of users who fell victim to DuckTail's initial attack where victims were enticed with fraudulent job posts and fake recruiters. We reached this conclusion after observing a conversation between members of the DuckTail group. One member directed another member to access a victim's Gmail account (using the stolen browser cookies), delete email entries related to LinkedIn (to clear traces), and change the account recovery email address to an attacker-controlled email.

Compromising TikTok business accounts

The image below shows the activity log page of a victim's compromised TikTok Business account. The log depicts the threat actor inviting themselves to control the account and then performing actions. After three days, the targeted business notices and revokes their access.



Activity related to billing and payment can be viewed in your payment page.

Activity Log

Time 2023-03-10 ~ 2023-04-10 Activity Type All 1 Export

Time (UTC+04:00) Dubai Time	Activity Type	Activity Log
2023-04-08 07:07:53	Business	"[redacted]" removed the access of partner "[redacted]" to the pixel "[redacted]".
2023-04-07 21:17:03	Business	"[redacted]" linked the ad account "[redacted]" with the pixel "[Main Pixel] Shopify [redacted]".
2023-04-07 21:16:16	Asset	"[redacted]" assigned "[redacted]" to Pixel "[Main Pixel] Shopify [redacted]" with edit access.
2023-04-07 21:14:58	Business	"[redacted]" changed the access of partner "[redacted]" to: Pixel Name "[Main Pixel] Shopify [redacted]", Pixel ID "[redacted]", access "Edit pixels,Pixel ad delivery".
2023-04-07 21:14:11	Business	"[redacted]" changed the access of partner "[redacted]" to: Pixel Name "[Main Pixel] Shopify [redacted]", Pixel ID "[redacted]", access "Pixel ad delivery".
2023-04-07 21:14:10	Business	Business Centers "[redacted]" and "[redacted]" became partners.
2023-04-05 21:12:55	User	"[redacted]" accepted the invitation from Business Center.
2023-04-05 21:12:32	User	"[redacted]" invited "[redacted]@gmail.com" to join the Business Center.

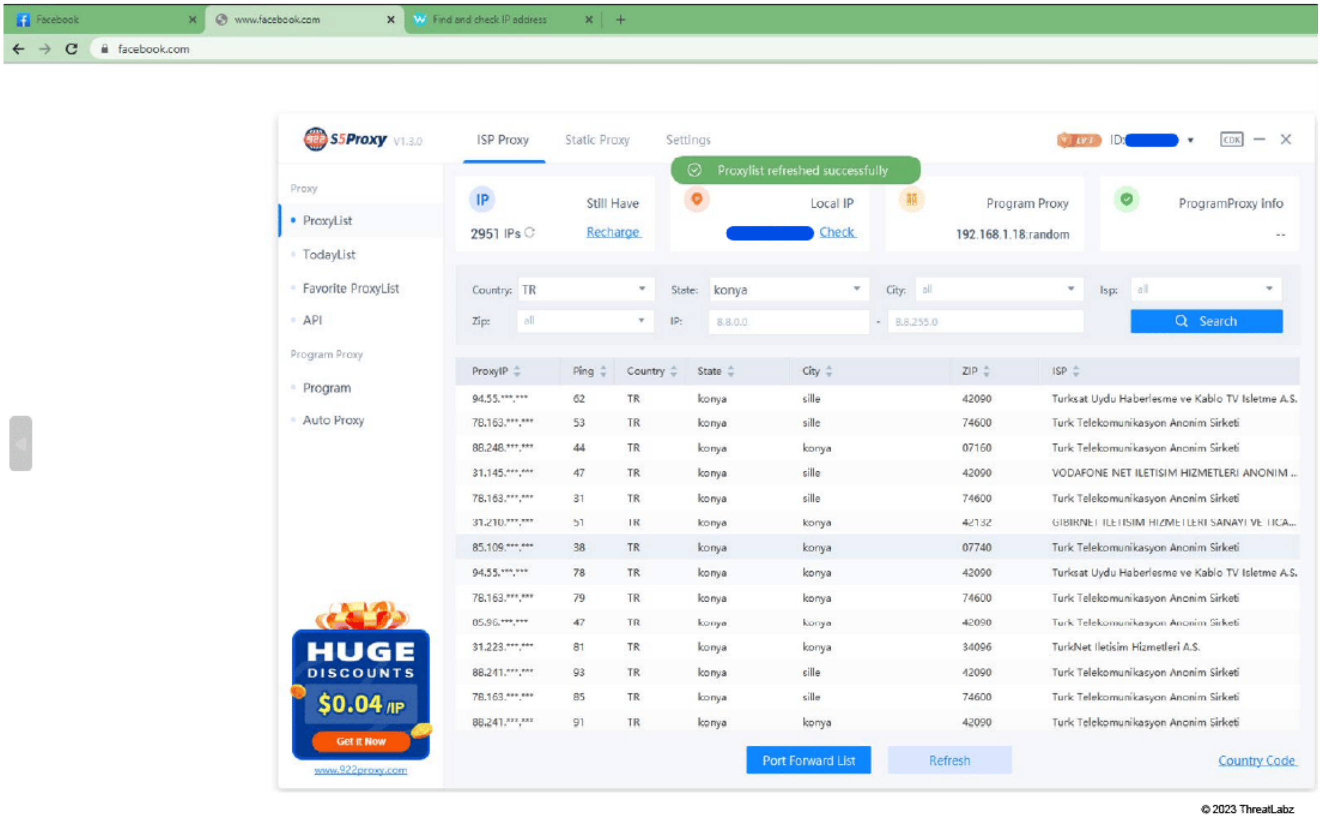
© 2023 ThreatLabz

Figure 14: This is a TikTok business center activity log for a compromised account, showing the actions executed by the threat actor.

Leveraging residential proxy services to access compromised accounts

Our team observed DuckTail threat actors using "Residential Proxy" services to circumvent Facebook account compromise detections.

In the image below, the attacker’s machine uses the “S5 Proxy” residential proxy service from the vendor - 922proxy.com. Interestingly, the UI also shows the threat actor’s own original IP address. We confirmed with an IP geolocation lookup that the threat actor’s original IP address maps to a city in Vietnam, further strengthening our theory that DuckTail is operated by Vietnam-based threat actors.



ID: [redacted]

Proxylist refreshed successfully

IP 2951 IPs Still Have Recharge

Local IP [redacted] Check

Program Proxy 192.168.1.18:random

ProgramProxy Info --

Country: TR State: konya City: all Isp: all

Zip: all IP: 8.8.0.0 - 8.8.255.0 Search

ProxyIP	Ping	Country	State	City	ZIP	ISP
94.55.***.***	62	TR	konya	sille	42090	Turksat Uydu Haberlesme ve Kablo TV Isletme A.S.
78.163.***.***	53	TR	konya	sille	74600	Turk Telekomunikasyon Anonim Sirketi
88.248.***.***	44	TR	konya	konya	07160	Turk Telekomunikasyon Anonim Sirketi
31.145.***.***	47	TR	konya	sille	42090	VODAFONE NET ILETISIM HIZMETLERI ANONIM ...
78.163.***.***	31	TR	konya	sille	74600	Turk Telekomunikasyon Anonim Sirketi
31.210.***.***	51	TR	konya	konya	42132	GIBIRNET ILETISIM HIZMETLERI SANAYI VE TICA...
85.109.***.***	38	TR	konya	konya	07740	Turk Telekomunikasyon Anonim Sirketi
94.55.***.***	78	TR	konya	konya	42090	Turksat Uydu Haberlesme ve Kablo TV Isletme A.S.
78.163.***.***	79	TR	konya	konya	74600	Turk Telekomunikasyon Anonim Sirketi
05.96.***.***	47	TR	konya	konya	42090	Turk Telekomunikasyon Anonim Sirketi
31.223.***.***	81	TR	konya	konya	34096	TurkNet Iletisim Hizmetleri A.S.
88.241.***.***	93	TR	konya	sille	42090	Turk Telekomunikasyon Anonim Sirketi
78.163.***.***	85	TR	konya	sille	74600	Turk Telekomunikasyon Anonim Sirketi
88.241.***.***	91	TR	konya	konya	42090	Turk Telekomunikasyon Anonim Sirketi

© 2023 ThreatLabz

Figure 15: This screenshot shows a threat actor connecting to a residential proxy in Konya, Turkey, before logging into the compromised Facebook account of a victim.

Stolen Credentials Enter Underground Market

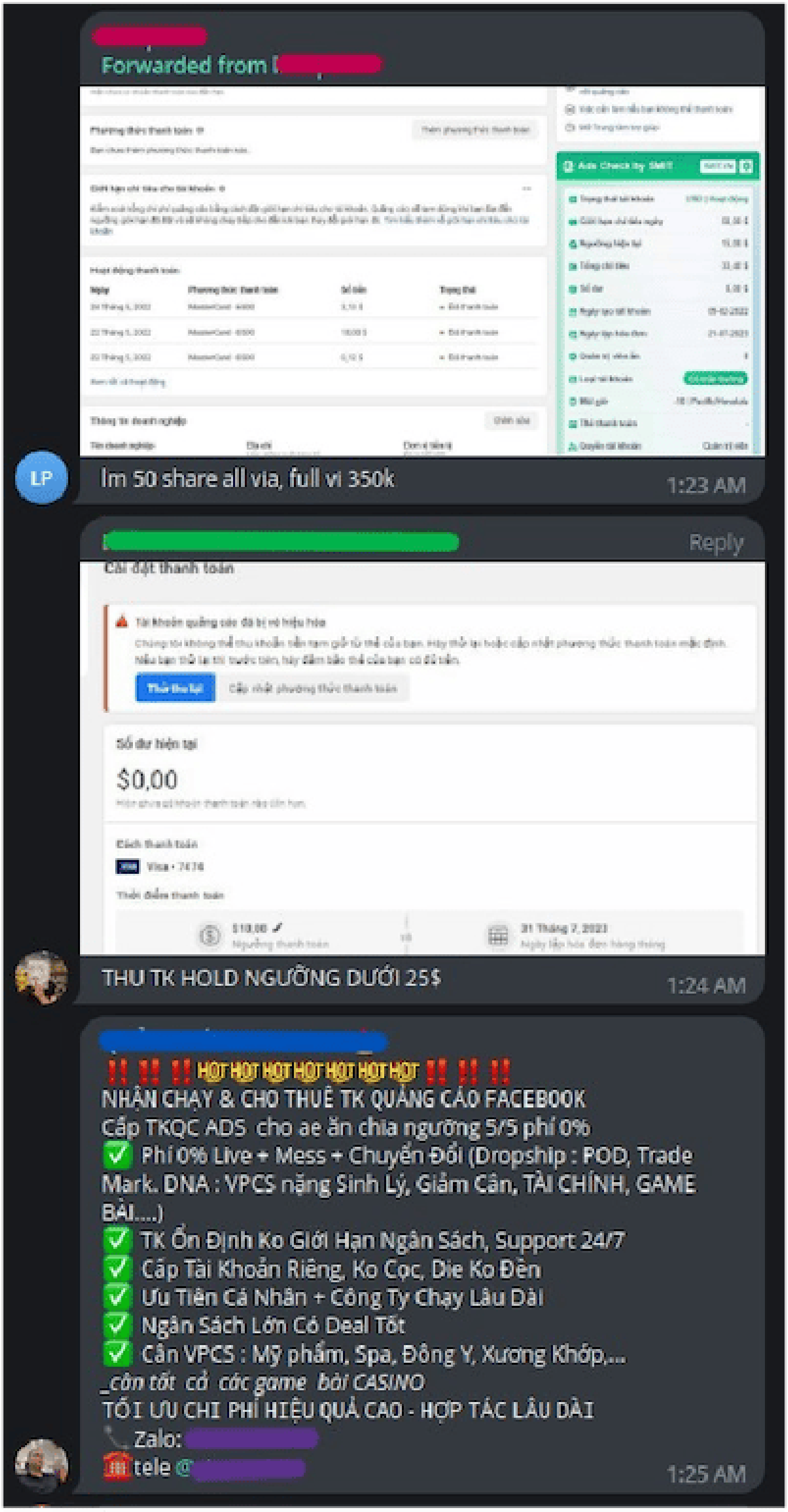
Social media ad accounts are constantly targeted for hacking. Threat actors, like those behind the Ducktail operation, collect massive amounts of hacked accounts. **But where do they end up?**

Hacked social media and ad accounts end up for sale in a busy Vietnamese-language underground market. Here is what we know about this market:

- Mainly Facebook accounts are sold
- It includes numerous publicly accessible Telegram groups
- DuckTail threat actors are active sellers

Despite the illicit nature of these groups, they are public and easily accessible. Although it may be difficult for a novice to interpret the jargon and abbreviations that are heavily used in the community.

Awareness of OPSEC among those involved appears to be be lacking or non-existent.



[redacted]
Forwarded from [redacted]

Im 50 share all via, full vi 350k
1:23 AM

[redacted] Reply

Cài đặt thanh toán

Tài khoản quảng cáo đã bị vô hiệu hóa

Chúng tôi không thể thu khoản tiền tạm giữ từ thẻ của bạn. Hãy thử lại hoặc cập nhật phương thức thanh toán mặc định. Nếu bạn thử lại từ trước tiền, hãy đảm bảo thẻ của bạn có đủ tiền.

Số dư hiện tại
$0,00

Cách thanh toán
Visa • 7478

Thời điểm thanh toán
$10,00 Ngưỡng thanh toán
31 Tháng 7, 2023 Ngày lập hóa đơn hàng tháng

THU TK HOLD NGƯỠNG DƯỚI 25$
1:24 AM

[redacted]
‼️ ‼️ ‼️ HOT HOT HOT HOT HOT HOT HOT ‼️ ‼️ ‼️
NHẬN CHẠY & CHO THUÊ TK QUẢNG CÁO FACEBOOK
Cấp TKQC ADS cho ae ăn chia ngưỡng 5/5 phí 0%
✅ Phí 0% Live + Mess + Chuyển Đổi (Dropship : POD, Trade Mark. DNA : VPCS nặng Sinh Lý, Giảm Cân, TÀI CHÍNH, GAME BÀI....)
✅ TK Ổn Định Ko Giới Hạn Ngân Sách, Support 24/7
✅ Cấp Tài Khoản Riêng, Ko Cọc, Die Ko Đền
✅ Ưu Tiên Cá Nhân + Công Ty Chạy Lâu Dài
✅ Ngân Sách Lớn Có Deal Tốt
✅ Cần VPCS : Mỹ phẩm, Spa, Đông Y, Xương Khớp,...
_còn tốt cả các game bài CASINO
TỐI ƯU CHI PHÍ HIỆU QUẢ CAO - HỢP TÁC LÂU DÀI
📞 Zalo: [redacted]
🏛 tele @[redacted]
1:25 AM

© 2023 ThreatLabz

Figure 16: In this screenshot, vendors offer access to hacked Facebook accounts on a Vietnamese Telegram group.

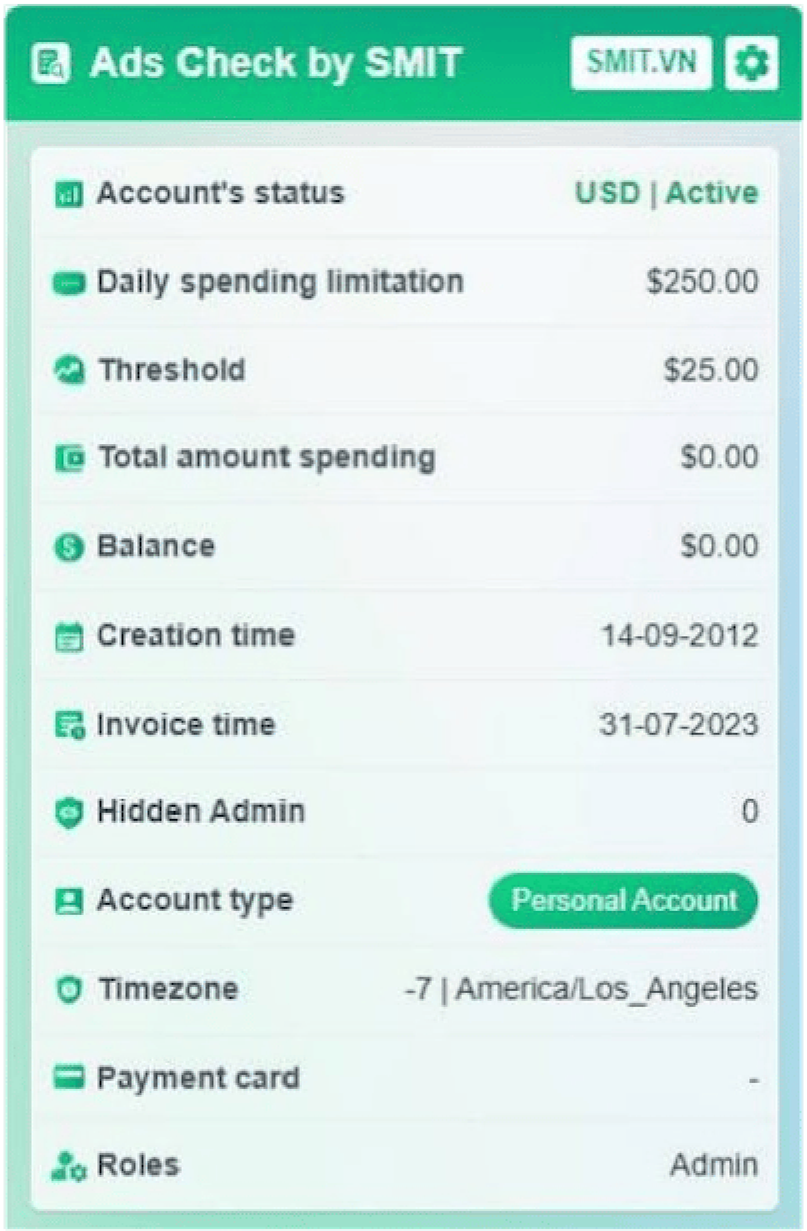
Threat actors target ad accounts so they can access ad budgets. High ad budgets and long-term accessibility to accounts are attractive characteristics to threat actors.

Facebook combats threat actors like Ducktail, who hack and abuse ad accounts on their platform, by automatically flagging suspicious accounts. Because of this, threat actors try to prolong the life of a compromised ad account. For this reason, hacked Facebook accounts are not interchangeable commodities. Depending on an account's properties, it may range from very valuable to almost useless to buyers.

Here are common properties that vendors and buyers check for in this underground market:

- The type of account (a personal ad account or a business manager account)
- The daily ad budget and payment threshold of an account
- The number of ad accounts a business manager account controls
- A successful business verification by Facebook
- If the account controls a page or profile with a verified badge
- The age of the account. Older accounts are more valuable than younger.
- The existence and validity of saved payment methods
- The account's successful payment history. More successful payments indicate a more valuable account.

We observed the following Vietnamese browser extension used for displaying account properties:



Ads Check by SMIT

Account's status	USD | Active
Daily spending limitation	$250.00
Threshold	$25.00
Total amount spending	$0.00
Balance	$0.00
Creation time	14-09-2012
Invoice time	31-07-2023
Hidden Admin	0
Account type	Personal Account
Timezone	-7 | America/Los_Angeles
Payment card	-
Roles	Admin

© 2023 ThreatLabz

Figure 17: A screenshot of the Vietnamese-designed browser extension used by threat actors to quickly assess social media business account details.

Payments and Transactions

We observed that an account deemed “low-grade” sells for around 350,000 Vietnamese dong (~$15 USD), while accounts considered valuable sell for around 8,000,000 Vietnamese dong (~$340 USD).

When a transaction is complete, the seller hands over control of the hacked account by:

- Adding/inviting the buyer to control the account through Facebook (business manager)
- Providing the victim’s login and password to the compromised account
- Providing the victim’s exported browser cookies, thus replicating their logged-in session

If the level of compromise is thorough, access to the victim’s email may be given on top of the above to maintain access even longer, and also be able to bypass MFA security measures.

Conclusion

In this blog, ThreatLabz provides a wealth of new insight for the research community. Understanding the operational methods and end-to-end journey of a threat actor like DuckTail is a form of protection. Because of our research team, we can confidently state:

- DuckTail is primarily run by Vietnamese-speaking cyber criminals who use Google Translate to communicate with potential victims over LinkedIn.
- DuckTail threat actors are abusing themes of popular AI tools, like ChatGPT, to infect devices.
- DuckTail threat actors take extra measures to prevent raising security alarms by using private residential proxy services to log in to compromised accounts.
- DuckTail threat actors use strategic account takeover methods which they routinely use in their post-compromise procedures to prevent any form of account recovery by victims
- Hacked and/or compromised social media business ad accounts enter a primarily Vietnamese-based underground market where they are sold based on their perceived value.
- You can take steps to minimize the impact of a hacker by managing your saved payment methods in business ad accounts and making use of safeguards like daily spending limits, payment thresholds, etc.

In addition to staying on top of these threats, Zscaler's ThreatLabz team continuously monitors for new threats and shares its findings with the wider community.

MITRE ATT&CK TTP Mapping

ID	TACTIC	TECHNIQUE
T1204.001	User Execution: Malicious Link	User executes the shortcut .lnk file
T1204.002	User Execution: Malicious File	User executes the attached compressed/executable file
T1027.001	Obfuscated Files or Information: Binary Padding	Binary inflated in order to avoid sandboxing
T1036.005	Masquerading: Match Legitimate Name or Location	Drops malicious binaries into legitimate paths

ID	TACTIC	TECHNIQUE
T1057	Process Discovery	Checks for well known security software analysis tools
T1567.002	Exfiltration Over Web Service: Exfiltration to Cloud Storage	Telegram API used to exfiltrate user data
T1070.006	Indicator Removal: Timestomp	PE’s Timestamp header value are tampered

Indicators of Compromise (IOCs)

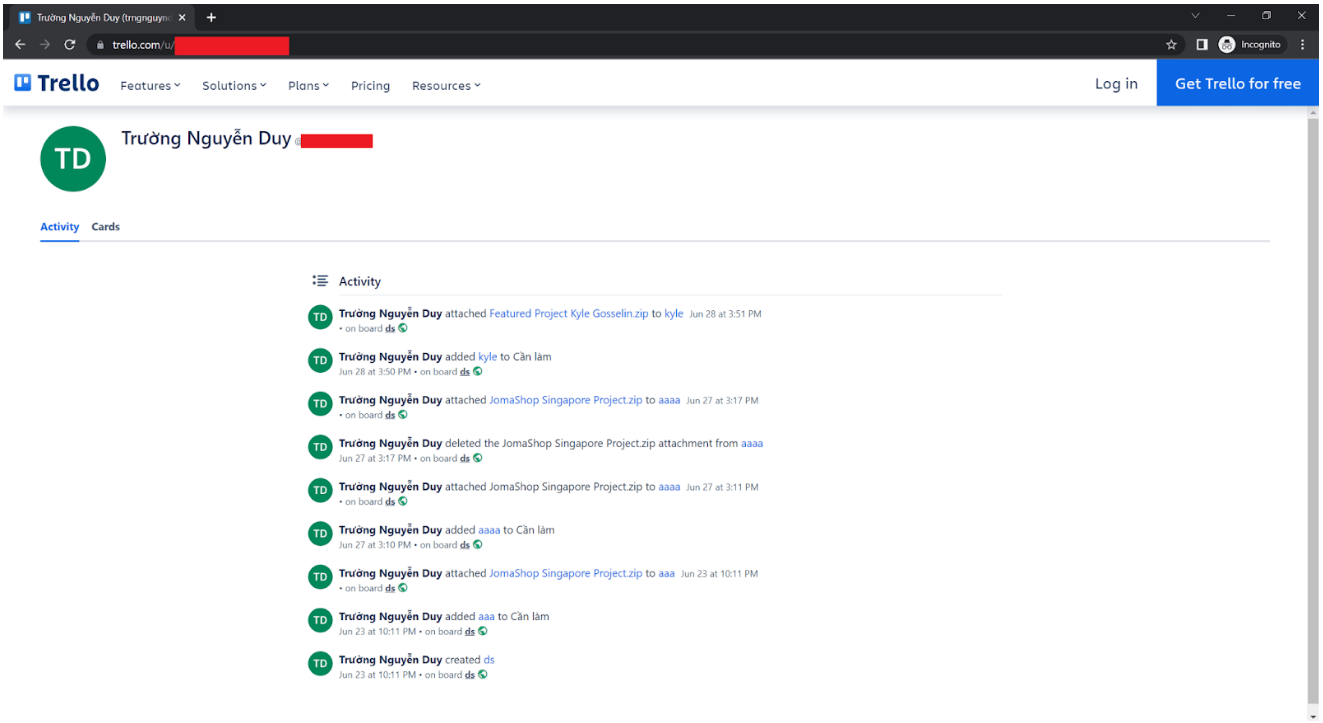
Fake sites set up by DuckTail threat actor

- marketingagency[.]social
- a1outreach[.]software
- mangogroup[.]sale
- la-roche-posay[.]click
- li-ning[.]agency
- li-ning[.]news
- hrm[.]social
- hrms[.]social
- mccann[.]fyi
- avalonorganics[.]work
- li-ningagency[.]news
- li-ningjod[.]news
- ogilvy[.]social
- narscosmetics[.]social
- yodo1game[.]software
- louisvuitton-social[.]news
- luoisviitton[.]news
- eucerin[.]work
- guessinc[.]work
- samsungagency[.]link
- brandresource[.]social
- recruiterofbrand[.]social
- brandrecruitment[.]social
- hrmmarketing[.]link
- marketingmanager[.]social
- recruitmentagency[.]social
- marketing-project[.]social
- nike-agency[.]link
- recuiter[.]company

- louisvuitton-agency[.]link
- louisvuitton-agencyjod[.]live
- mccann[.]expert
- ogilvysocial[.]company
- louisvuitton-hr[.]news
- louisvuitton-jod[.]chat
- hyundaimotorjob[.]social
- hyundaimotor[.]social
- hyundaimotorgroup[.]social
- adplexity[.]site
- adplexitydesk[.]tech
- fbadsguide[.]tech
- affiliateguide[.]tech
- newguide[.]tech
- businessmanagerads[.]tech
- businessmanager-update[.]info
- marketing-tool[.]info
- connectads[.]agency
- disruptiveadvertising[.]agency
- impressionagency[.]co
- themars[.]social
- ommmarketing[.]agency
- growmemarketing[.]agency
- ommmarketing[.]digital
- impressiondigitals[.]agency
- impressiondigital[.]info
- passions[.]agency
- brandstyle[.]agency
- brandstyle[.]digital

Appendix

Attacker-controlled Trello account



Trường Nguyễn Duy [redacted]

Activity

TD **Trường Nguyễn Duy** attached Featured Project Kyle Gosselin.zip to kyle Jun 28 at 3:51 PM • on board **ds**

TD **Trường Nguyễn Duy** added kyle to Cần làm
Jun 28 at 3:50 PM • on board **ds**

TD **Trường Nguyễn Duy** attached JomaShop Singapore Project.zip to aaaa Jun 27 at 3:17 PM • on board **ds**

TD **Trường Nguyễn Duy** deleted the JomaShop Singapore Project.zip attachment from aaaa
Jun 27 at 3:17 PM • on board **ds**

TD **Trường Nguyễn Duy** attached JomaShop Singapore Project.zip to aaaa Jun 27 at 3:11 PM • on board **ds**

TD **Trường Nguyễn Duy** added aaaa to Cần làm
Jun 27 at 3:10 PM • on board **ds**

TD **Trường Nguyễn Duy** attached JomaShop Singapore Project.zip to aaa Jun 23 at 10:11 PM • on board **ds**

TD **Trường Nguyễn Duy** added aaa to Cần làm
Jun 23 at 10:11 PM • on board **ds**

TD **Trường Nguyễn Duy** created ds
Jun 23 at 10:11 PM • on board **ds**

Figure 19: An attacker-controlled Trello account used to host the malicious files. Screenshot shows the activity log.

Thank you for reading

Was this post useful?

Get the latest Zscaler blog updates in your inbox

By submitting the form, you are agreeing to our privacy policy.