DuckTail | ThreatLabz

By Sudeep Singh, Naveen Selvan

Published: 2023-08-30 · Archived: 2026-04-06 00:02:59 UTC

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.

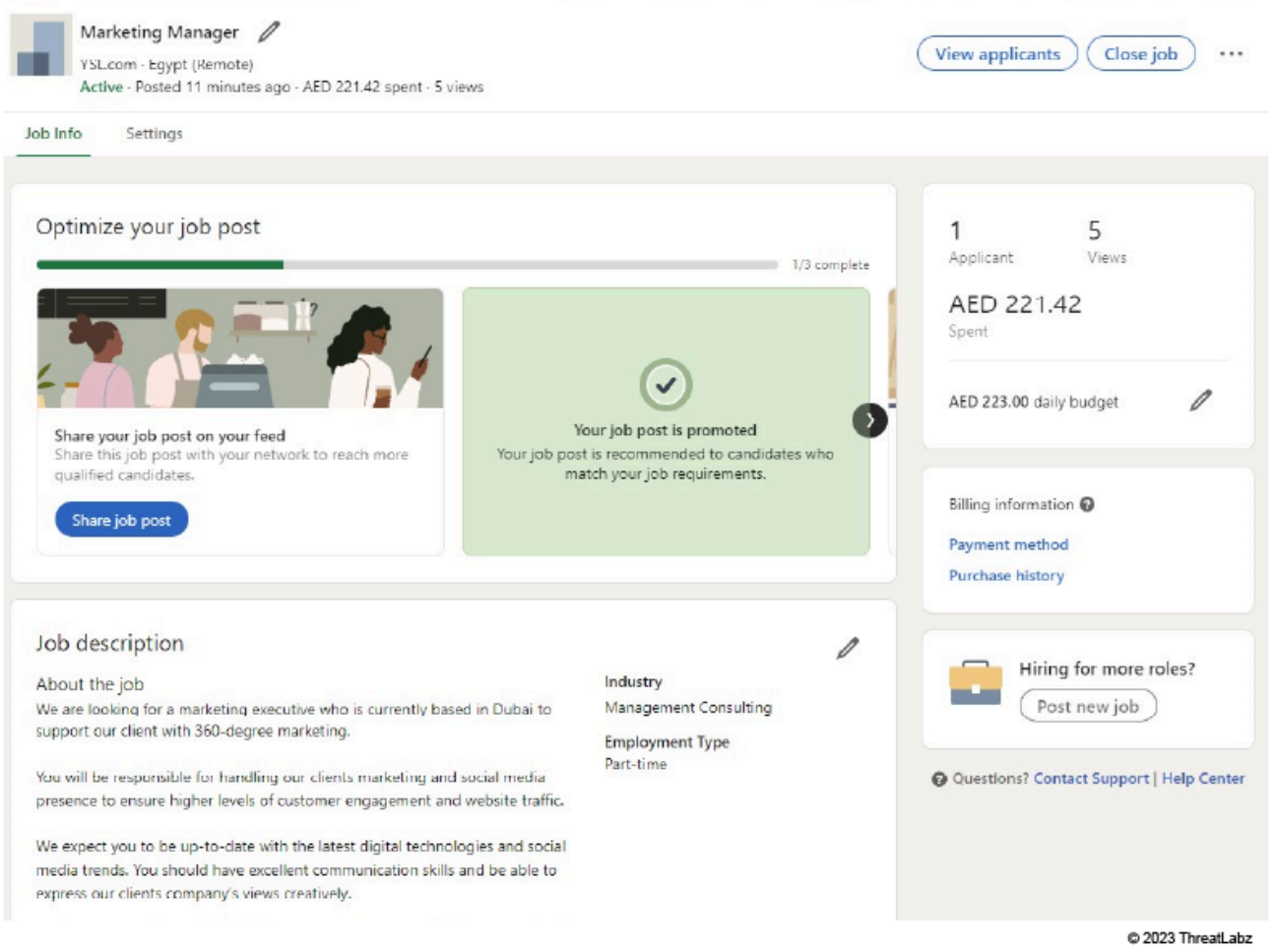

Figure 2: This is what the threat actor sees moments after setting up a fake marketing job post on LinkedIn. It's worth noting that the post is promoted.

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:

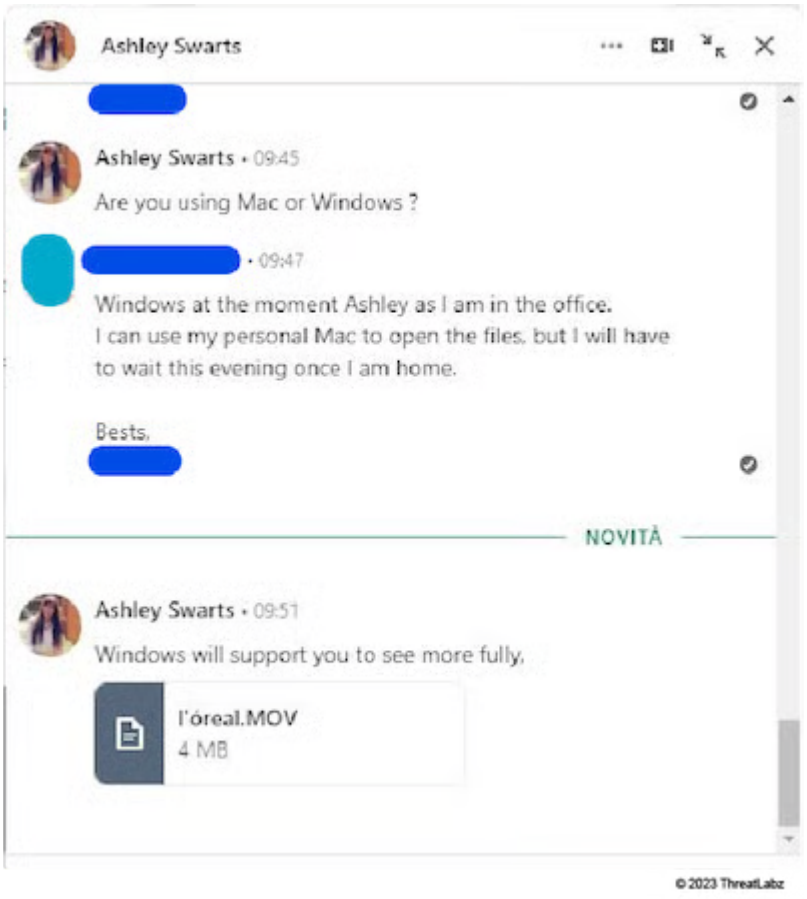

Figure 3: “Ashley Swarts” (a fake threat actor account) instructing a victim on how to open the fake job application package.

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.

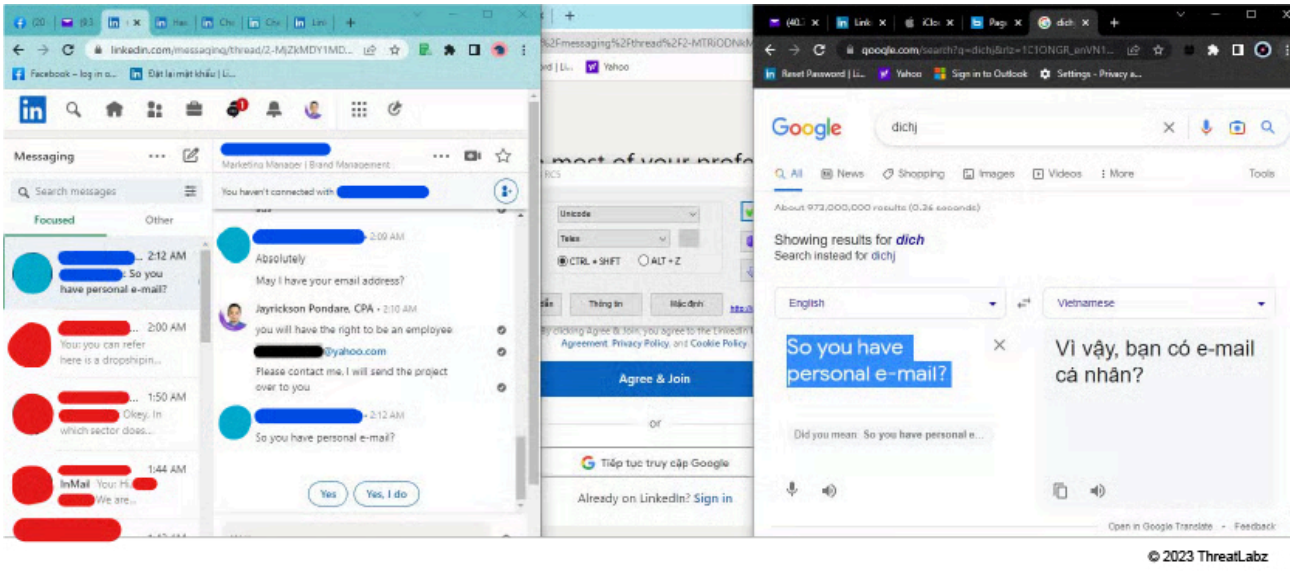

Figure 4: A threat actor using Google Translate to communicate in English while handling multiple fraudulent job application conversations on LinkedIn.

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

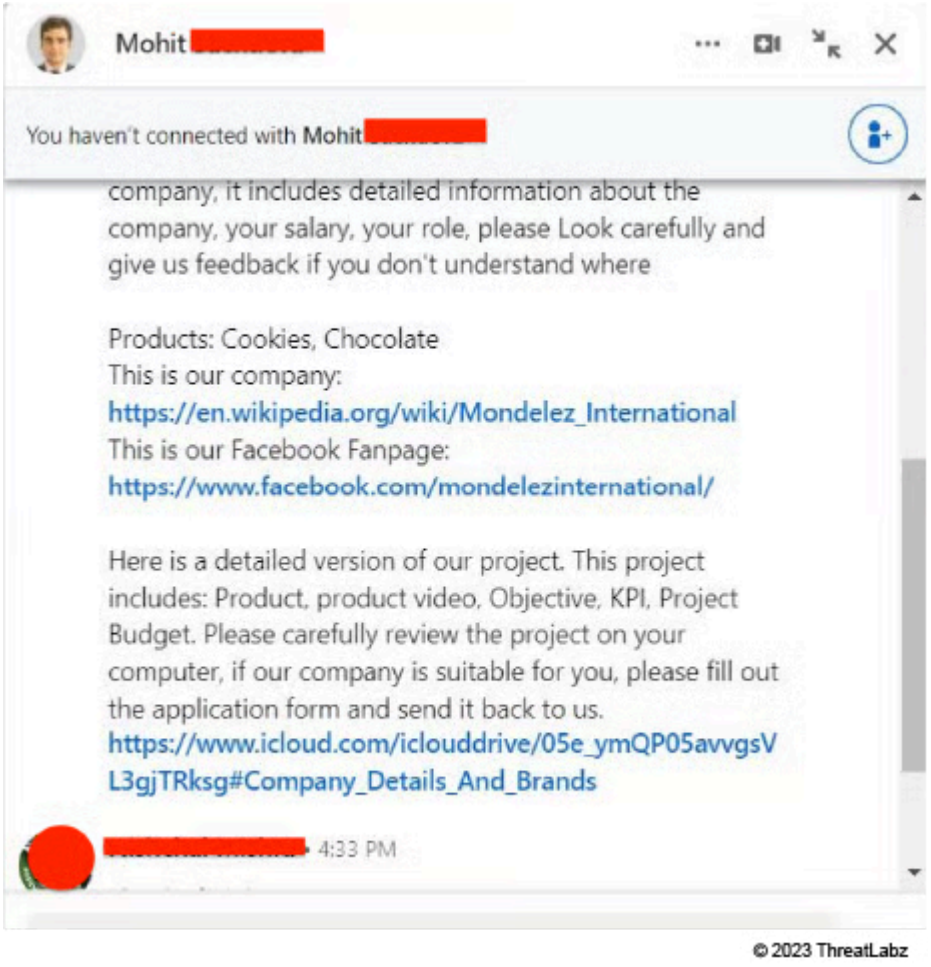

Figure 5: A threat actor messaging a victim on LinkedIn and impersonating a real company.

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.

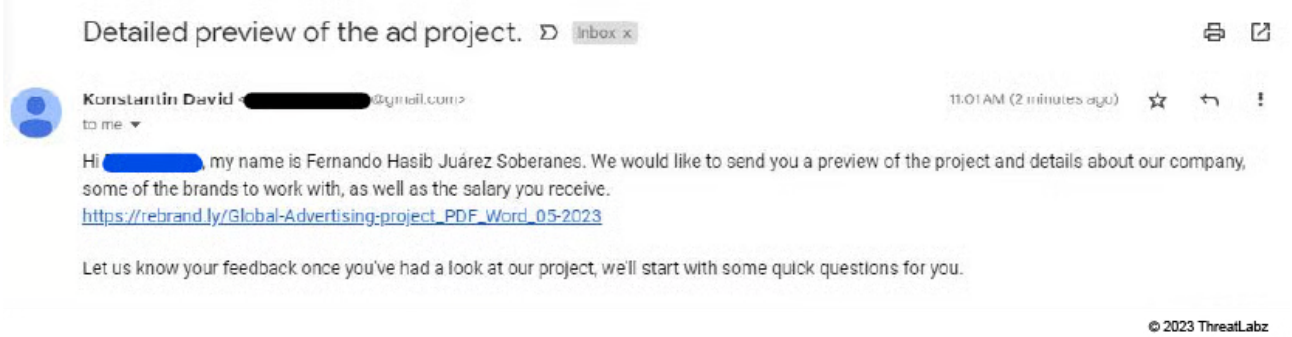

Figure 6: A spear phishing email sent to a victim containing the URL shortener link, which downloads the malicious archive file.

.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

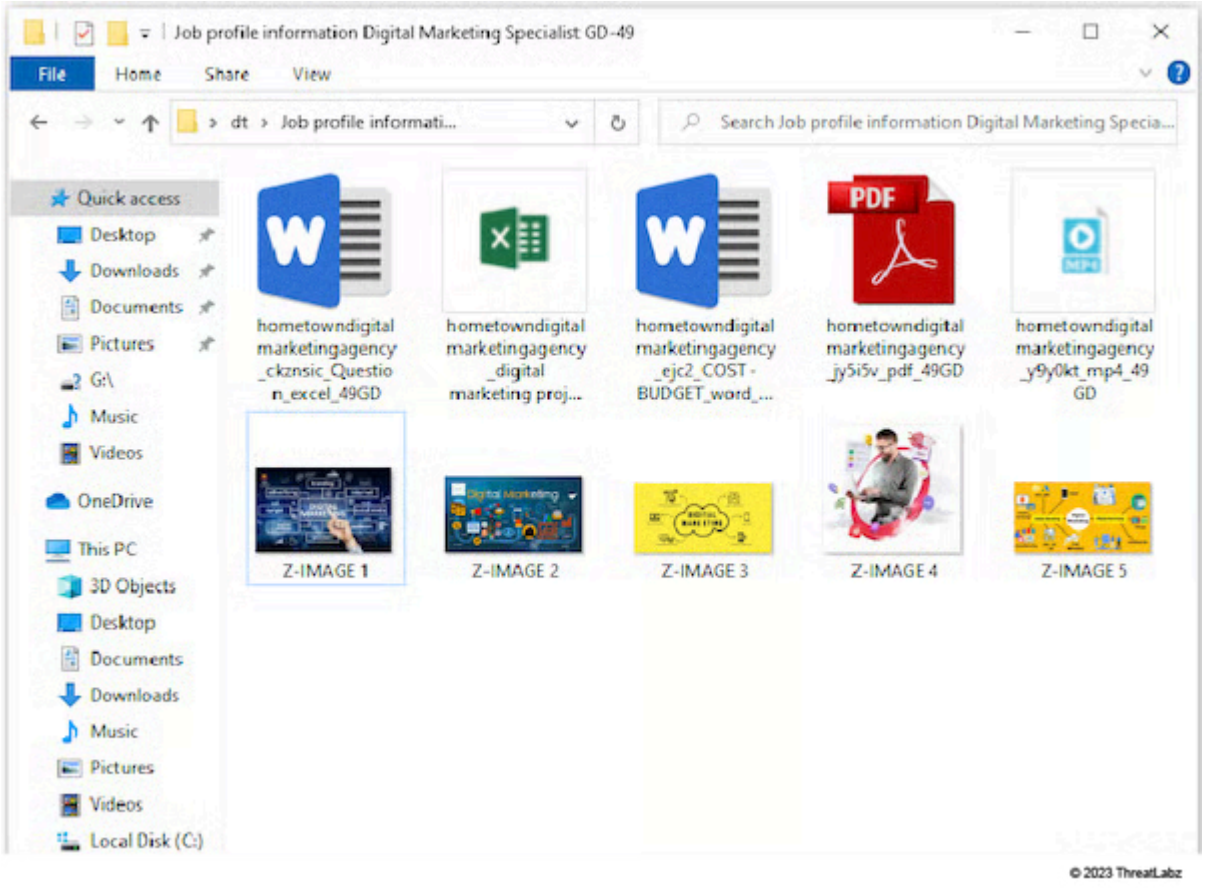

Figure 7: Type 1 Archive - .exe files with fake icons (first row), together with job-related images

Type 2 Archive

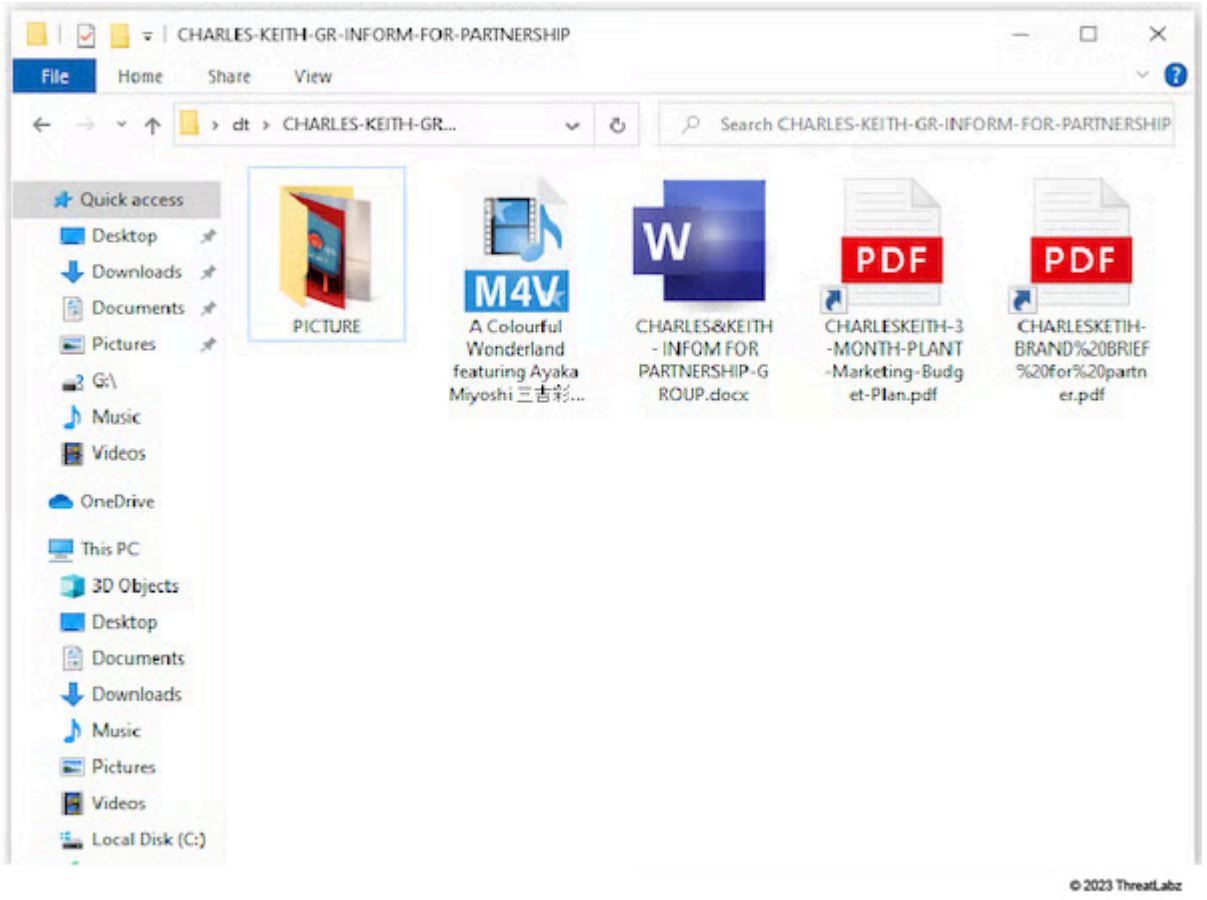

Figure 8: Type 2 Archive - .lnk files with PowerShell payloads, plus .scr executables, both obscured by double extensions (.pdf.lnk, .docx.scr), together with job-related images

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.

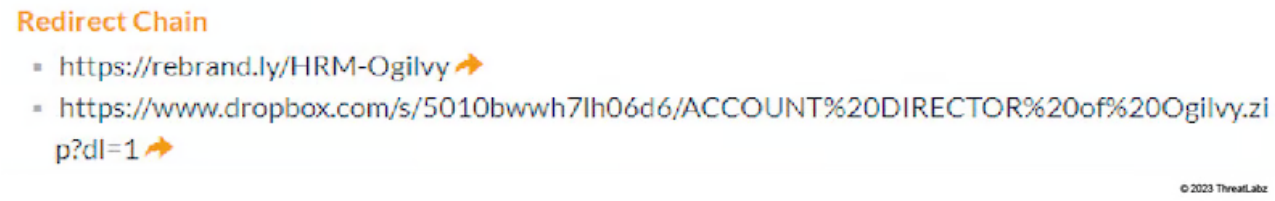

Figure 9: A redirection chain set up by the threat actor transforms a long, unfriendly Dropbox link into a short rebrand.ly link.

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.

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.

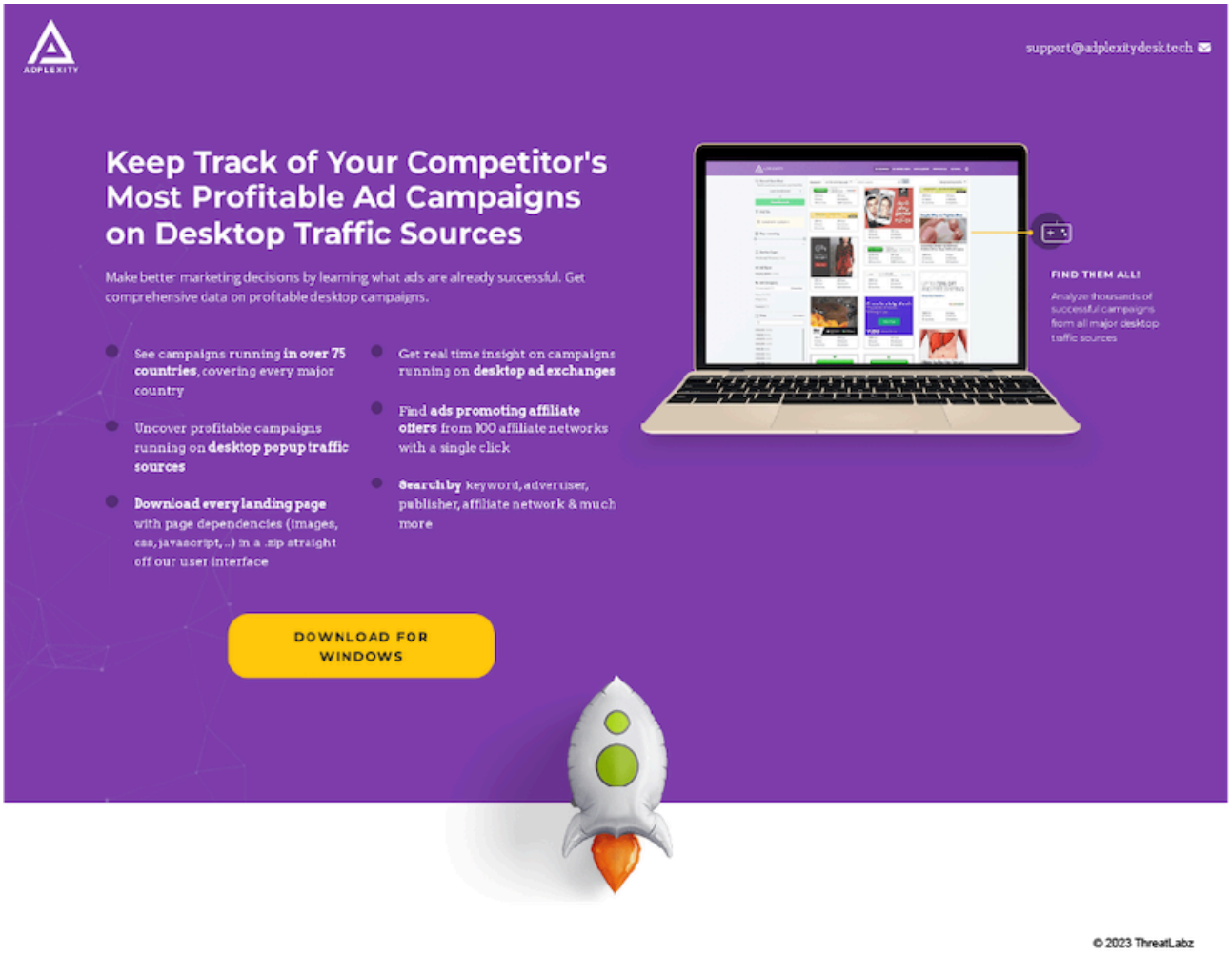

Figure 11: A screenshot of adplexitydesk[.]tech, a website set up by Ducktail impersonating Adplexity. The download button leads to a Ducktail infected archive.

Source: https://www.zscaler.com/blogs/security-research/look-ducktail