

Cybersecurity Digest

Bi-Weekly Update by the O/o
CISO of Meghalaya Rural Bank

Date: 16.09.2026

Ducktail



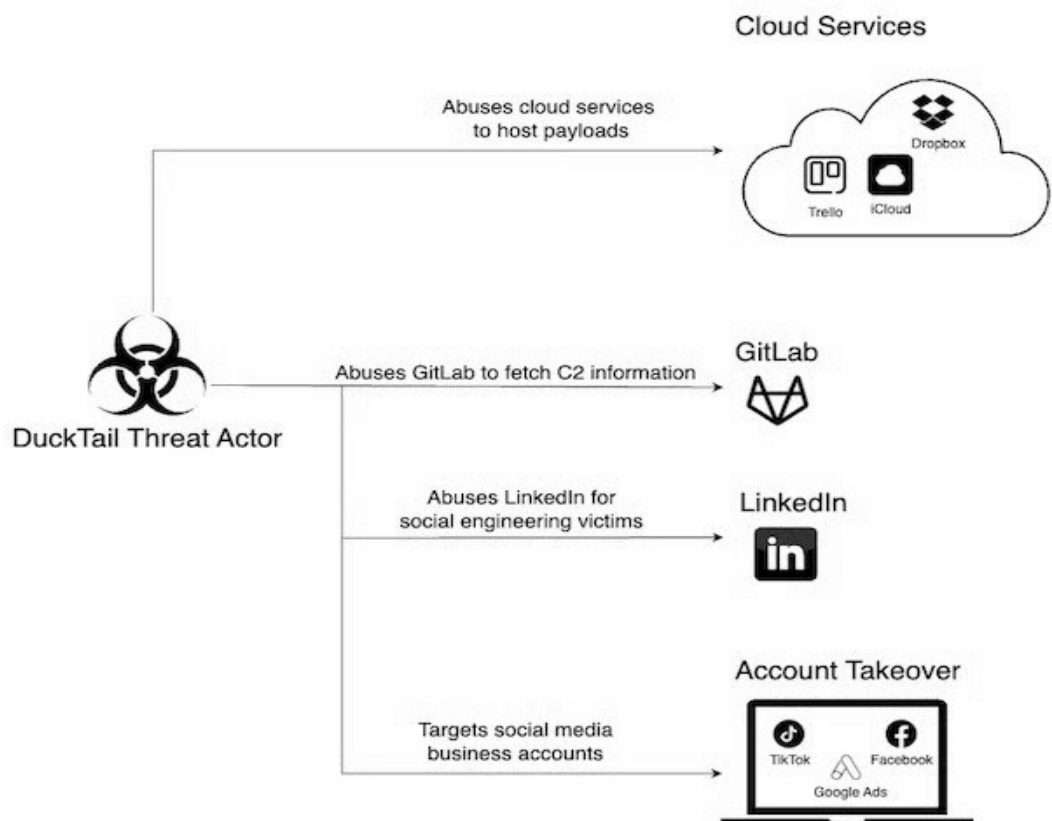
DuckTail is an operation that involves multiple Vietnam-based threat actors who share the same tactics, techniques, and procedures (TTPs). They also share the same motivation: gain access to social media business accounts, specifically ones belonging to digital marketers.

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:

Cybersecurity best practices

Do not open suspicious emails and unknown links.
Keep software and hardware up to date.
Avoid using public networks.
Always check HTTPS on websites.
Backup your sensitive data.
Use secure file sharing only.
Always scan external storage devices.
Handle passwords carefully.



How to protect ourselves from Ducktail malware

Although Ducktail malware is highly adaptive, which makes it difficult to establish a specific protection protocol to address this threat, there are ways to protect against an attack. We outline several methods below:

- **Employee training:** Corporate cybersecurity often starts with the employees. In this case, they play a critical role in ensuring precautions are taken to avoid falling victim to this attack, which is why companies should invest in training so that workers can identify fraudulent activity. This boosts awareness among teams and serves as the first step towards protecting organizations.

- **Use of firewalls:**

Although prevention is key, in the event of a potential threat we must also have a system in place that blocks a malicious agent from entering the system. Installing a firewall to prevent the spread of any malware is an essential part of shielding an organization's devices and internal systems.

- **Implementing a unified cybersecurity system:** Installing a firewall is the foundation of an effective cybersecurity protocol but complementing this measure with other solutions can really make the difference when it comes to protecting your organization. Combining cybersecurity systems such as



XDR functionality to ensure detection and response to the presence of threat actors, the aforementioned use of firewalls, and endpoint security helps cover any potential gaps in data protection, thus unifying the cybersecurity protocol and making it more effective.

Key Takeways

- **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 Tele-

gram 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 In-**

- **novative 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 Ma-**

neuvres: 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.



DUCKTAIL MALWARE

**Looks harmless.
Steals your data.**



Through suspicious
emails and links



Via fake software,
cracked apps or files



By exploiting
security loopholes

Think Safe | Stay Aware | Stay Secure