Headquarters
New Zealand Defence Force
Defence House
Private Bag 39997
Wellington Mail Centre
Lower Hutt 5045
New Zealand

OIA-2023-4658

28 March 2023

[redacted]
[redacted]@stuff.co.nz

Dear [redacted]

I refer to your email of 3 March 2023 requesting, under the Official Information Act 1982 (OIA), *a copy of the November 2, 2022 directive to personnel regarding TikTok, a copy of the risk assessment that informed this directive, and any over policy work regarding TikTok in the past year.*

A copy of the Chief Information Security Officer Directive regarding TikTok is provided at Enclosure 1. This is the New Zealand Defence Force policy regarding TikTok. Where indicated, information is withheld under sections 6(a) and 9(2)(k) of the OIA. The risk assessment that informed the directive is withheld in full under section 6(a) of the OIA.

You have the right, under section 28(3) of the OIA, to ask an Ombudsman to review this response to your request. Information about how to make a complaint is available at www.ombudsman.parliament.nz or freephone 0800 802 602.

Please note that responses to official information requests are proactively released where possible. This response to your request will be published shortly on the NZDF website, with your personal information removed.

Yours sincerely

AJ WOODS
Air Commodore
Chief of Staff HQNZDF

Enclosure:
1. Chief Information Security Officer Directive 01/2022

Released under the Official Information Act

Headquarters NZDF
Defence House
34 Bowen Street
Wellington 6011
NEW ZEALAND

1 Nov 2022

See distribution

CISO DIRECTIVE 01/2022

REMOVAL OF TIKTOK APPLICATION ON NZDF ISSUED DEVICES

Authority

1. Issued by the Chief Information Security Officer.

Applicability

2. This Directive constitutes a general instruction to the Chief Information Officer (CIO).

Purpose

3. The purpose of this Directive is to provide direction to the CIO regarding the removal of the TikTok application from all NZDF issued devices and a restriction on accessing the TikTok Website from any NZDF issued device via the internet (access to the internet is via Internet to the Desktop (ITD)). The expectation is that this will be done at the close of ten working days from the publication of this directive.

Background

4. TikTok is owned by ByteDance, who are headquartered in Beijing. Numerous cyber security experts have raised concerns with the security of the TikTok App and the ability of threat actors to access data collected by TikTok. TikTok reportedly collects significant amounts of user data, such as contact lists, calendars, the contents of a person's hard drive, and can geolocate a user's device on an hourly basis.

5. s.6(a) [redacted]

Context

6. s.6(a) [redacted]

Released under the Official Information Act

7. s.6(a) [redacted]

8. The Cyberspace Administration of China (CAC) requires Chinese companies to register Internet Information Service Algorithms under the auspices of improving security governance and promoting CCP socialist values.

9. s.6(a) [redacted]

Risk to the NZDF

10. s.6(a) [redacted]

11. s.6(a) [redacted]

12. Among the many opportunities TikTok data presents to threat actors, the following items are highlighted as part of this report:

    a. User and device data can be used to create unique 'fingerprints' to track user activity on the platform, and across other Internet services. This can enable targeting for intelligence operations, and highlight opportunities for software and device exploitation. It can also be used to discover associated users, which could include other NZDF members.

    b. Video media is rich in biometric data that can be used for facial and voice recognition, invaluable for building biometric databases, and training recognition algorithms. These could be abused to correlate data and activity on TikTok with other external sources, enabling identification and tracking of current and future NZDF members. Data could also be used to generate high quality deep fake media to impersonate individuals and spread disinformation.

Threat to be avoided

13. TikTok uses a proprietary algorithm for content curation which analyses data on user activity and behaviours, to promote engaging content and make recommendations on the platform. The algorithm will likely evolve further to meet the demands of increasing digital commerce activity. s.6(a) [redacted]

Released under the Official Information Act

14. While initially the assessment of the TikTok platform presents no immediate disruptive cyber threat to the NZDF specifically, s.6(a) [redacted]

15. There is a realistic possibility cyber threat actors will exploit TikTok software vulnerabilities to target users of the application. A plausible scenario for targeting NZDF members is the use of zero-click[1] and one-click[2] exploits by threat actors, using bespoke or commercially procured malware, to conduct cyber espionage against high value targets.

16. TikTok encourages the re-use of posted video content. A threat actor could edit and re-post any NZDF content to undermine messages, or spread dis- and misinformation, potentially being viewed more than NZDF's original content.

17. Exemptions to this policy are to be made on a case by case basis through Defence Information Security (DIS) to the Chief Information Security Officer for consideration. Exemptions to this policy will be managed and reviewed regularly through DIS, and included in the regular security assurance reporting to the Security Reference Group.

Accountabilities and responsibilities

18. The CIO is to have the TikTok application removed from all NZDF provided devices immediately, prevent future downloading of the application and restrict access to the TikTok website via ITD.

Cancellation and disposal instructions

19. This Directive is to remain in force until the CISO determines it can be cancelled or its contents are moved to another publication.

s.9(2)(k) [redacted]

J LICHT
Mr
Chief Information Security Officer

Distribution

OCDF

OVCDF

CA

CN

CAF

[1] (U) Zero-click vulnerability exploits target applications which will execute the malicious code automatically.
[2] (U) One-click vulnerability exploits target users who will allow malicious code to execute by granting permission.

Released under the Official Information Act

CPO

CFO

CJDS

CDI

COMLOG

CIO