



| Flash |

Australia Elections

F-2025-04-30a

Classification: TLP:CLEAR

Criticality: High

Intelligence Requirements: Geopolitical, Deep and Dark Web

April 30, 2025

Scope Note

ZeroFox Intelligence is derived from a variety of sources, including—but not limited to—curated open-source accesses, vetted social media, proprietary data sources, and direct access to threat actors and groups through covert communication channels. Information relied upon to complete any report cannot always be independently verified. As such, ZeroFox applies rigorous analytic standards and tradecraft in accordance with best practices and includes caveat language and source citations to clearly identify the veracity of our Intelligence reporting and substantiate our assessments and recommendations. All sources used in this particular Intelligence product were **identified prior to 7:00 AM (EDT) on April 29, 2025**; per cyber hygiene best practices, caution is advised when clicking on any third-party links.

| Flash | Australia Elections

| Key Findings

- Australia holds general elections on May 3, 2025, with final polls reporting a small lead for Anthony Albanese's incumbent Labor party over Peter Dutton's opposition Coalition.
- The policies of U.S. President Donald Trump have likely impacted voter candidate preferences in the Australian election, and there is evidence that Chinese-backed cyber threat actors have attempted to influence the election in support of current Prime Minister Anthony Albanese.
- The biggest cyber risks to the election come from financially motivated deep and dark web (DDW) actors selling compromised account credentials linked to voters and online election infrastructure.

| Geopolitics

On March 28, 2025, Australian Prime Minister Anthony Albanese of the Labor Party called general elections for May 3, 2025. Labor currently holds 77 of the 151 seats in the House of Representatives, with 19 additional seats held by cross-benchers. Albanese is running again for Prime Minister (PM); Peter Dutton of the opposition Coalition is his main rival.¹

¹<https://www.abc.net.au/news/2025-03-27/albanese-expected-to-call-federal-election-this-morning/105103954>

- PM Albanese will try to maintain his liberal Labor government in office, while opposition leader Peter Dutton aims to return his Coalition (a longstanding alliance of the conservative Liberal and National parties) to power.
- Tariffs and trade with China have been the two main geopolitical topics early on the campaign trail. Dutton had previously criticized Albanese for not establishing or maintaining a tariff exception apparently negotiated during the first Trump administration. A Labor representative responded that Dutton is hurting Australia's trading relationship with China.²
- Polling suggests a tight race between the two parties. The trend toward third-party voting in Australia could also result in the eventual winner being the party more able to ally with independent and smaller-party members of Parliament.³ Australia's use of ranked-choice voting makes third-party candidates much more viable than in countries that use first-past-the-post voting.
- The cost-of-living crisis—particularly unaffordable housing—has been the key domestic issue, while energy and mining policies are always important political issues in Australia.⁴

Like in Canada, the conservative Coalition was initially polling to win on economic issues and closer alliances with the United States. However, Labor has slowly risen in the polls since Trump's inauguration in January 2025 and now holds the presumptive advantage. Much of this shift can be attributed to an increase in negative perception of Dutton over the course of the campaign; Labor has worked hard to cast him as a Trumpian figure, and his approval has shifted from a +3 in December to a -12 today.⁵ Voters seem

2

[hXXps://www.rnz\[.\]co\[.\]nz/news/world/559240/dutton-names-china-as-biggest-threat-to-australia-s-security-as-leaders-faced-off-in-fiery-final-debate](https://www.rnz.co.nz/news/world/559240/dutton-names-china-as-biggest-threat-to-australia-s-security-as-leaders-faced-off-in-fiery-final-debate)

3

[hXXps://www.abc\[.\]net\[.\]au/news/2025-04-02/federal-election-2025-live-campaign-trail-wednesday-april-2-blog/105124752](https://www.abc.net.au/news/2025-04-02/federal-election-2025-live-campaign-trail-wednesday-april-2-blog/105124752)

4

[hXXps://www.abc\[.\]net\[.\]au/news/2025-04-29/election-2025-cost-of-living-campaign-politicians/105221010](https://www.abc.net.au/news/2025-04-29/election-2025-cost-of-living-campaign-politicians/105221010)

5

[hXXps://www.smh\[.\]com\[.\]au/national/nsw/donald-trump-s-clown-car-has-backfired-on-peter-dutton-again-20250428-p5lune.html](https://www.smh.com.au/national/nsw/donald-trump-s-clown-car-has-backfired-on-peter-dutton-again-20250428-p5lune.html)

increasingly disinclined to install Dutton as the head of a government, causing a decline in expected vote share for the Coalition.

That swing in voting may prove especially pronounced due to Australia's ranked-choice voting. Unlike in Canada, independent smaller parties play a major role in Australia's elections. The vote share for non-Labor and non-Coalition parties has been rising steadily for decades, and this year may well result in a Parliament where neither major party has a majority. The two most likely outcomes of the election are a Labor victory or a hung Parliament with no party gaining a majority.⁶ In the latter case, the party with the most seats will likely form a minority government, requiring them to negotiate with cross-benchers to pass legislation.

| Cyber Findings

The Australia Public Policy Institute observed what appears to be a concerted campaign by the People's Republic of China to influence the election in favor of incumbent Anthony Albanese. This campaign involves both Chinese-language and English-language efforts. As compared to Canada, the activity in Australia is more overt, involving state-run outlets pushing the same narrative—in this case, that opposition candidate Peter Dutton is Trump-aligned, will cause chaos in Australia, and is unreasonably critical of China. The researchers contrasted this effort to Chinese interference in Canada, where the campaign functioned primarily via WeChat and attempted to create the impression of organic public opinion.⁷

ZeroFox also investigated automated DDW marketplaces and paid-access DDW repositories, both of which contain compromised logins to online governmental portals related to the Australian federal election. The compromised credentials identified are used for both citizen-facing portals and access-controlled environments.

⁶

[hXXps://www.abc\[.\]net\[.\]au/news/2025-03-18/hung-parliament-independents-crossbenchers-election/105062236](https://www.abc.net.au/news/2025-03-18/hung-parliament-independents-crossbenchers-election/105062236)

⁷

[hXXps://www.aspistrategist\[.\]org\[.\]au/china-targets-canadas-election-and-may-be-targeting-australias/](https://www.aspistrategist.org.au/china-targets-canadas-election-and-may-be-targeting-australias/)

While some of the findings could be used to influence the election by changing voter registrations, the threat actors are most likely financially motivated, selling voter data that could then be used to commit financial fraud.

Compromised Credentials

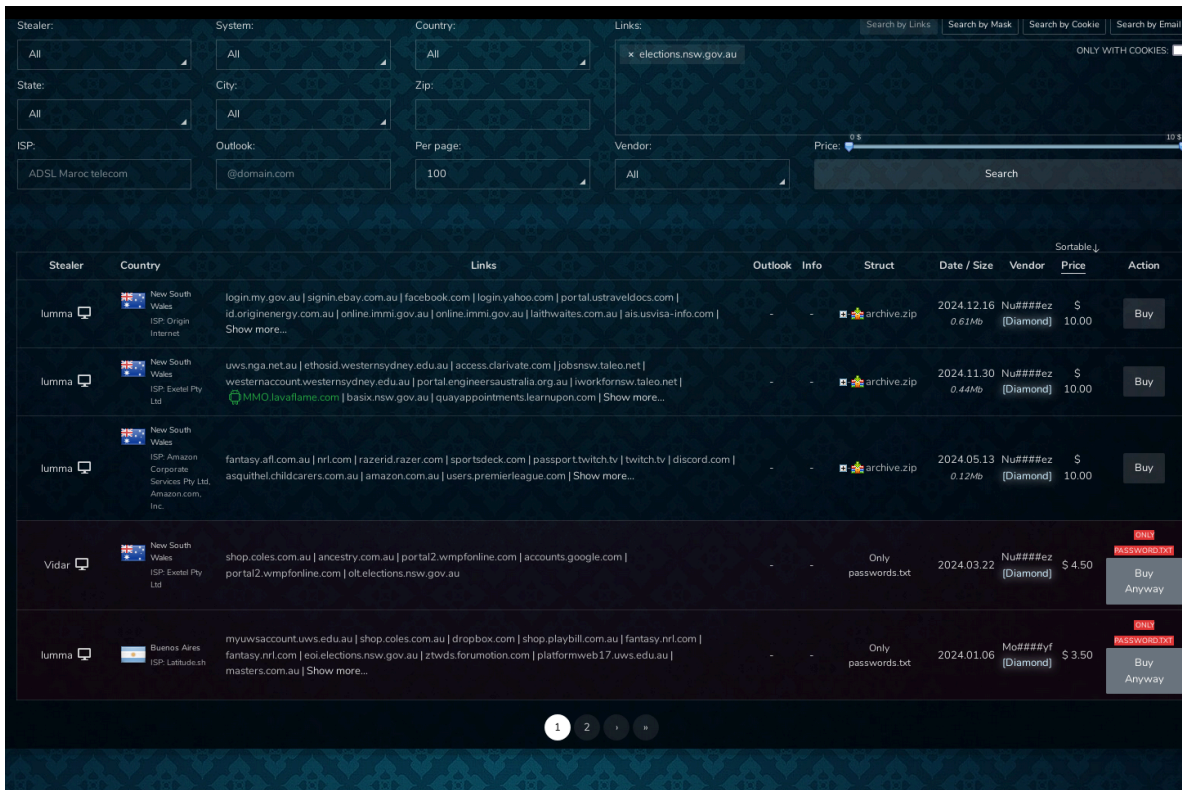
ZeroFox identified a number of login credentials on the deep web automated marketplace Russian Market that relate to governmental bodies in charge of administering the Australian elections; these are derived from the logs of stealer malware installed on compromised systems (AKA botnet logs).

- ZeroFox uncovered five logs uploaded in Russian Market that contain login credentials to elections.nsw[.]gov[.]au, the official election website of Australia's largest state by population, New South Wales. The most recent upload date associated with the logs listed for sale is December 16, 2024, while the oldest log dates back to January 6, 2024. The listings are traded for between USD 10-350, depending on the upload date. Four out of the five logs were captured by the Lumma infostealing malware strain.
- This website elections.nsw[.]gov[.]au is the official portal of the New South Wales Electoral Commission (NSWEC). ZeroFox assesses that this is a publicly accessible portal; however, authenticated users may engage in submitting sensitive personal information, such as full name, residential address, date of birth, contact information, and previous enrollment details. Capable actors may leverage such login details in order to manipulate voter registration by changing voters' addresses or by exploiting vulnerabilities associated with the New South Wales (NSW) online voting system. Affected resources include eoi.elections.nsw[.]gov[.]au and olt.elections.nsw[.]gov[.]au.

Some of the compromised data includes victims' cookies and additional system information linked to affected online resources, in addition to login credentials.

- This could allow a threat actor to mimic a victim's browser session and user agent, potentially allowing these actors to circumvent some multi-factor authentication (MFA) defenses and other anti-fraud measures.

- Most of the items provide full information from the bot, such as ID, browser history, browser cookies, system information on the victim's device, autofills, and payment information. Those logs are listed for up to USD 10 each.
- Some of the items are TXT files from the log that contain only usernames and passwords captured from the victim's device. In this case, the rest of the data is removed. Such password TXT files are cheaper than the full logs.



The screenshot shows a search interface for stolen data on the Russian Market. The search filters include Stealer (All), System (All), Country (All), Links (elections.nsw.gov.au), State (All), City (All), Zip (), ISP (ADSL Maroc telecom), Outlook (@domain.com), Per page (100), and Vendor (All). The search results are displayed in a table with columns: Stealer, Country, Links, Outlook, Info, Struct, Date / Size, Vendor, Price, and Action.

Stealer	Country	Links	Outlook	Info	Struct	Date / Size	Vendor	Price	Action
lumina	New South Wales ISP: Origin Internet	login.my.gov.au signin.ebay.com.au facebook.com login.yahoo.com portal.ustraveldocs.com id.originenergy.com.au online.immi.gov.au online.immi.gov.au laithwaites.com.au ais.usvisa-info.com Show more...	-	-	archive.zip	2024.12.16 0.61Mb	Nu####ez (Diamond)	\$ 10.00	Buy
lumina	New South Wales ISP: Exetel Pty Ltd	uws.nga.net.au ethosid.westernsydney.edu.au access.darivante.com jobsnsw.taleo.net westernaccount.westernsydney.edu.au portal.engineersaustralia.org.au workfor.nsw.taleo.net MMOJavaLume.com basix.nsw.gov.au quayappointments.learnupen.com Show more...	-	-	archive.zip	2024.11.30 0.44Mb	Nu####ez (Diamond)	\$ 10.00	Buy
lumina	New South Wales ISP: Amazon Corporate Services Pty Ltd, Amazon.com, Inc.	fantasy.afl.com.au nrl.com razerid.razer.com sportsdeck.com passport.twitch.tv twitch.tv discord.com asquithel.childcarers.com.au amazon.com.au users.premierleague.com Show more...	-	-	archive.zip	2024.05.13 0.12Mb	Nu####ez (Diamond)	\$ 10.00	Buy
Vidar	New South Wales ISP: Exetel Pty Ltd	shop.coles.com.au ancestry.com.au portal2.wmpfonline.com accounts.google.com portal2.wmpfonline.com olt.elections.nsw.gov.au	-	-	Only passwords.txt	2024.03.22	Nu####ez (Diamond)	\$ 4.50	Buy Anyway
lumina	Buenos Aires ISP: Latitude.sh	myuwsaccount.uws.edu.au shop.coles.com.au dropbox.com shop.playbill.com.au fantasy.nrl.com fantasy.nrl.com eoi-elections.nsw.gov.au ztwds.forumotion.com platformweb17.uws.edu.au masters.com.au Show more...	-	-	Only passwords.txt	2024.01.06	Mo####yf (Diamond)	\$ 3.50	Buy Anyway

Screenshot from Russian Market of available logs from elections.nsw[.]gov[.]au

Source: ZeroFox Intelligence

Stealer	Country	Links	Outlook	Info	Struct	Date / Size	Vendor	Price	Action
lumma	New South Wales ISP: Origin Internet	login.my.gov.au signin.ebay.com.au facebook.com login.yahoo.com portal.ustraveldocs.com id.originenenergy.com.au online.immi.gov.au online.immi.gov.au laithwaites.com.au ais.usvisa-info.com online.immi.gov.au auth.laithwaites.com.au opal.com.au vfglobal.ca sydneywater.com.au portal-portal-apps.cic.gc.ca atlasauth.b2dlogin.com signin.ebay.com.au repco.com.au eoi.elections.nsw.gov.au eoi.elections.nsw.gov.au login.my.gov.au login.live.com login.my.gov.au online.immi.gov.au online.immi.gov.au carsales.com.au ais.usvisa-info.com vfglobal.ca portal-portal-apps.cic.gc.ca atlasauth.b2dlogin.com portal.ustraveldocs.com atlasauth.b2dlogin.com laithwaites.com.au atlasauth.b2dlogin.com atlasauth.b2dlogin.com repco.com.au eoi.elections.nsw.gov.au login.live.com login.my.gov.au online.immi.gov.au online.immi.gov.au carsales.com.au auth.passports.gov.au auth.laithwaites.com.au login.service.nsw.gov.au atlasauth.b2dlogin.com atlasauth.b2dlogin.com login.service.nsw.gov.au atlasauth.b2dlogin.com atlasauth.b2dlogin.com login.yahoo.com id.originenenergy.com.au online.immi.gov.au online.immi.gov.au laithwaites.com.au ais.usvisa-info.com online.immi.gov.au auth.laithwaites.com.au opal.com.au vfglobal.ca sydneywater.com.au portal-portal-apps.cic.gc.ca atlasauth.b2dlogin.com signin.ebay.com.au repco.com.au eoi.elections.nsw.gov.au eoi.elections.nsw.gov.au login.my.gov.au login.live.com login.my.gov.au online.immi.gov.au online.immi.gov.au carsales.com.au auth.passports.gov.au login.service.nsw.gov.au				2024.12.16 0.61Mb	Nu####ez [Diamond]	\$ 10.00	Buy

Sample with the freshest log affecting elections.nsw[.]gov[.]au

Source: ZeroFox Intelligence

Similarly, ZeroFox observed 19 logs containing logins to the Australian Electoral Commission (AEC) website, aec[.]gov[.]au. The freshest log dates back to April 2, 2025, and the oldest one to August 20, 2023. They are traded for between USD 10–150, based on the upload date. Again, the bulk of the listings were captured by Lumma infostealing malware strain.

- ZeroFox assesses that aec[.]gov[.]au is the official AEC website, and it provides federal election-related services and information. Certain services—such as enrolling to vote or updating personal details—are accessed by registered voters. Sensitive information associated with those logins may include full names, dates of birth, addresses, and phone numbers.

ZeroFox investigated the Telegram-based compromised credentials repository "GoldPack Private" for any records affecting governmental bodies of interest. The precise origin of the leaks is not specified; however, ZeroFox operatives assess with high certainty that compromised credentials were sourced from botnet logs between April 8, 2024, and April 21, 2025.

- ZeroFox observed and extracted 267 records containing compromised credentials for eoi.elections.nsw[.]gov[.]au, the portal which serves individuals expressing interest in various election-related roles. Sensitive information associated with such applications may include full names, addresses, contact information, dates of birth, and employment history.

- Additionally, ZeroFox discovered 87 records containing compromised credentials associated with `olt.elections.nsw[.]gov[.]au` via the same Telegram source. This subdomain is likely associated with a learning environment designed for election workers. Sensitive information related to those logins may include electoral processes and staff training.
- ZeroFox also uncovered a single record affecting a login to `noms.elections.nsw[.]gov[.]au`. We assess that this subdomain serves as an official digital platform for submitting nominations for candidacy in NSW state and local government elections.
- A set of 13 official email addresses associated with the `elections.nsw[.]gov[.]au` domain is also present within the investigated source.
- Similarly, ZeroFox uncovered 142 official email addresses associated with the `vec.vic[.]gov[.]au` domain. This URL is related to an online platform of the Victorian Electoral Commission (VEC), a government portal that manages state elections and provides enrollment services to voters.
- A file containing 104 email addresses associated with the official `aec[.]gov[.]au` domain is attached to this report. We are also including a file containing 784 associated credentials for `aec[.]gov[.]au` subdomains.
- ZeroFox identified two plaintext passwords associated with a single email address related to the Tasmanian Electoral Commission (`tec.tas[.]gov[.]au`).
- ZeroFox also uncovered eight email addresses pertaining to the official domain of Western Australia's Electoral Commission, `waec.wa[.]gov[.]au`.

The amount of the leaked data ZeroFox identified poses significant risk to the affected entities, as threat actors can use it to facilitate account takeovers via credential stuffing attacks, create effective social engineering schemes, and conduct tailored phishing/spamming campaigns.

| Appendix A: Traffic Light Protocol for Information Dissemination

	Red	Amber
WHEN SHOULD IT BE USED?	Sources may use TLP:RED when information cannot be effectively acted upon by additional parties and could lead to impacts on a party's privacy, reputation, or operations if misused.	Sources may use TLP:AMBER when information requires support to be effectively acted upon but carries risks to privacy, reputation, or operations if shared outside of the organizations involved.
HOW MAY IT BE SHARED?	Recipients may NOT share TLP:RED with any parties outside of the specific exchange, meeting, or conversation in which it is originally disclosed.	Recipients may ONLY share TLP:AMBER information with members of their own organization and its clients, but only on a need-to-know basis to protect their organization and its clients and prevent further harm. Note that TLP:AMBER+STRICT restricts sharing to the organization only.
	Green	Clear
WHEN SHOULD IT BE USED?	Sources may use TLP:GREEN when information is useful for the awareness of all participating organizations, as well as with peers within the broader community or sector.	Sources may use TLP:CLEAR when information carries minimal or no risk of misuse in accordance with applicable rules and procedures for public release.
HOW MAY IT BE SHARED?	Recipients may share TLP:GREEN information with peers and partner organizations within their sector or community but not via publicly accessible channels.	Recipients may share TLP:CLEAR information without restriction, subject to copyright controls.

Appendix B: ZeroFox Intelligence Probability Scale

All ZeroFox intelligence products leverage probabilistic assessment language in analytic judgments. Qualitative statements used in these judgments refer to associated probability ranges, which state the likelihood of occurrence of an event or development. Ranges are used to avoid a false impression of accuracy. This scale is a standard that aligns with how readers should interpret such terms.

Almost No Chance	Very Unlikely	Unlikely	Roughly Even Chance	Likely	Very Likely	Almost Certain
1-5%	5-20%	20-45%	45-55%	55-80%	80-95%	95-99%