FOCUSNET TECHNOLOGY

cyber@focusnet.com.au
1300 077 777
focusnet.com.au

Certified System — Quality ISO 9001

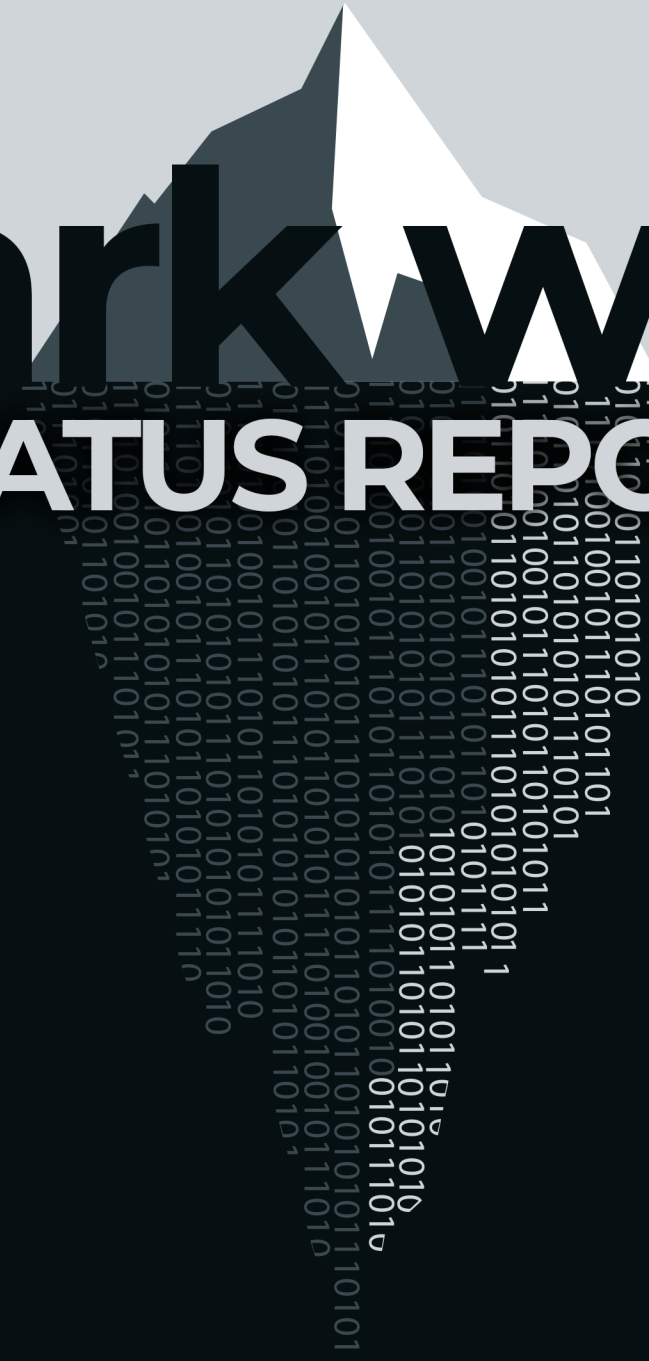
Certified System — Information Security ISO 27001

OFFENSIVE SECURITY CERTIFIED OSCP

OFFENSIVE SECURITY CERTIFIED OSEP

dark signal

dark web STATUS REPORT



CONFIDENTIAL

Audit Type: Dark Web Status Review
Completed For: **No-one In Particular**

Date Completed: **22/10/2025**
Report Produced By: **David Baines** (Cyber Security Specialist)
QA By: **Luke Ide** (Sales & Marketing Executive)

Background

What is the Darkweb?

The Dark Web functions as a cyber black market where stolen information is traded. Cybercriminals profit by selling previously breached data to other criminals, who then go on to sell this aggregated data to others, or openly abuse it themselves. As their activities remain lucrative, breaches and phishing scams persist, leaving employee data and entire organisations vulnerable.

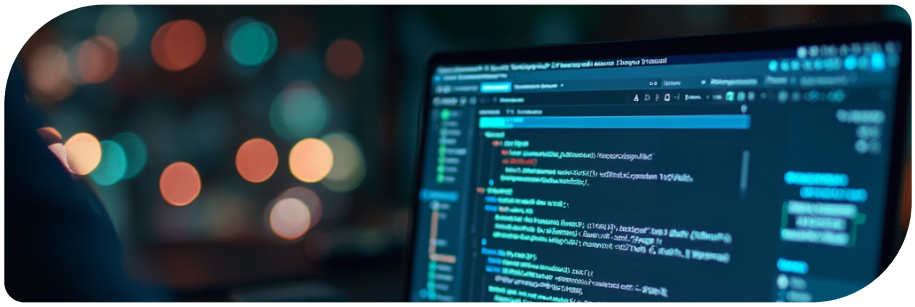
What you should know

Information found on the dark web is often used to launch targeted attacks, including phishing, impersonation, and fraud. Stolen credentials can lead to unauthorised access, data breaches, and financial loss. Even without a current breach, the risk is ongoing and requires constant vigilance.

Purpose of this report

The purpose of this report is to empower your organisation to take control of its cyber risk. By identifying whether your company's data or employee credentials have appeared on the dark web, this report provides you with the critical insight needed to act before attackers do.

Use this information to immediately secure any compromised accounts, strengthen your internal security practices, and educate your staff about the latest threats. Don't wait for a breach to happen—let this report be your catalyst for proactive defence and ongoing vigilance in an ever-changing threat landscape.



Results

Note: The results below exclude breaches or exposures classified as sensitive. Actual total exposure may exceed the values shown..

Breached Service	Breach Date	Exposed Data
admin@no-one.com.au		**2 Breaches**
VerificationsIO	25/02/19	Email Addresses, Names
OnlinerSpambot	28/08/17	Email Addresses, Passwords
manager@no-one.com.au		**8 Breaches**
QuestionPro	21/05/22	Email Addresses
LinkedInScrape	08/04/21	Email Addresses, Names
Nitro	28/09/20	Email Addresses, Names, Passwords
PDL	16/10/19	Email Addresses, Names
Canva	24/05/19	Email Addresses, Usernames, Names, Passwords
OnlinerSpambot	28/08/17	Email Addresses, Passwords
Adobe	04/10/13	Email Addresses, Usernames, Passwords
LinkedIn	05/05/12	Email Addresses, Passwords

What's the actual impact?

Breached Passwords

When breached account credentials like email address and passwords become available on the dark web, they can be used to access that account, steal information, or access additional accounts that may use the same credentials.

Organisation Exposure

2 email addresses tested

2	9	10
Email Addresses Exposed.	Breached services found.	Breaches involving your organisation.

Spear Phishing

Even if passwords weren't compromised on the dark web, the email address, physical address, or other personally identifiable information can be used to craft specific and convincing phishing emails that could put your business at future risk.

Network Access

If the credentials compromised are the same credentials used to access your business network or sensitive customer information, criminals could use this information for unauthorised access to your network where they can wreak havoc.

⚠ Data associated with your organisation has been found on the dark web. This means that either your business or one of your employees has been affected by a third-party data breach, potentially exposing your organisation to increased cyber risk. Take this as an opportunity to strengthen your defences—review the details in this report and follow the recommended actions to proactively reduce your exposure to future threats.

Who is FocusNet?

FocusNet is a cybersecurity and IT services provider dedicated to protecting Australia's small and medium-sized enterprises (SMEs). We deliver tailored, cost-effective solutions that balance strong security with system performance.

With deep cybersecurity expertise and a practical, business-first mindset, we help organisations uncover vulnerabilities, reduce risk, and build sustainable security strategies. Cyber protection doesn't have to be complicated or costly — it just needs to be done right.

In a climate where 60% of Australian SMEs that experience a serious cyber incident shut down within 12 months, FocusNet delivers the technical insight and guidance needed to keep businesses resilient and operational.

Our Cyber Suite offers a wide range of services designed to meet the growing security needs of modern businesses:

E8 Cyber Health Checks

Comprehensive Cyber review of your business based on the ACSC Essential Eight maturity model and NIST standards. Includes detailed findings and recommended mitigations.

CIS M365 Benchmark Assessment

A comprehensive assessment of your Microsoft 365 tenancy, benchmarking its configuration against CIS hardening guidelines to enhance your cyber resilience and safeguard your business.

Cyber Advisory & Risk Mitigation

Expert Cyber advisory is a critical support service for every modern-day business - Cyber incident prevention, cyber risk management, cyber incident response.

Penetration Testing

Internal stress testing of your IT environment to expose any cyber risks and recommend strategies to be implemented to reinforce your cyber posture.

Staff Security Awareness Training

A training platform designed to reduce staff's risky online behavior via Phishing simulations, training content, cyber policy management and effective reporting.

The Next Step

Your credentials have been found on the Dark Web.
What you do next is important.

- **You're a target.**
  Cybercriminals don't just go after big companies—any business can be at risk.
- **Leaked data = open door.**
  Exposed credentials can lead to phishing, fraud, and unauthorized access.
- **Urgent action is key.**
  Don't wait for an attack—proactive steps now can prevent major losses.
- **Review your security:**
  - > Change passwords for affected accounts
  - > Enable multi-factor authentication
  - > Educate your team about phishing and scams
- **Get an expert review.**
  Even if you have IT support, an independent cyber health check can reveal hidden risks.
- **Cyber insurance isn't enough.**
  Prevention and awareness are your best defence.

Feel free to reach out to me if you have any questions or need further assistance.

Dave Baines
Msc. Cyber Security, OSCP, OSEP
Cyber Security Specialist
david.baines@focusnet.com.au
(08) 6500 0505

Appendix - Breach Details

QuestionPro

May 21, 2022 *1 email reference*

In May 2022, the survey website QuestionPro was the target of an extortion attempt relating to an alleged data breach. Over 100GB of data containing 22M unique email addresses (some of which appear to be generated by the platform), are alleged to have been extracted from the service along with IP addresses, browser user agents and results relating to surveys. QuestionPro would not confirm whether a breach had occurred (although they did confirm they were the target of an extortion attempt), so the data was initially flagged as "unverified". Subsequent verification by impacted HIBP subscribe...

LinkedInScrape

April 8, 2021 *1 email reference*

During the first half of 2021, LinkedIn was targeted by attackers who scraped data from hundreds of millions of public profiles and later sold them online. Whilst the scraping did not constitute a data breach nor did it access any personal data not intended to be publicly accessible, the data was still monetised and later broadly circulated in hacking circles. The scraped data contains approximately 400M records with 125M unique email addresses, as well as names, geographic locations, genders and job titles. LinkedIn specifically addresses the incident in their post on An update on report o...

Nitro

September 28, 2020 *1 email reference*

In September 2020, the Nitro PDF service suffered a massive data breach which exposed over 70 million unique email addresses. The breach also exposed names, bcrypt password hashes and the titles of converted documents. The data was provided to HIBP by dehashed.com.

PDL

October 16, 2019 *1 email reference*

In October 2019, security researchers Vinny Troia and Bob Diachenko identified an unprotected Elasticsearch server holding 1.2 billion records of personal data. The exposed data included an index indicating it was sourced from data enrichment company People Data Labs (PDL) and contained 622 million unique email addresses. The server was not owned by PDL and it's believed a customer failed to properly secure the database. Exposed information included email addresses, phone numbers, social media profiles and job history data.

Canva

May 24, 2019 *1 email reference*

In May 2019, the graphic design tool website Canva suffered a data breach that impacted 137 million subscribers. The exposed data included email addresses, usernames, names, cities of residence and passwords stored as bcrypt hashes for users not using social logins.

VerificationsIO

February 25, 2019 *1 email reference*

In February 2019, the email address validation service verifications.io suffered a data breach. Discovered by Bob Diachenko and Vinny Troia, the breach was due to the data being stored in a MongoDB instance left publicly facing without a password and resulted in 763 million unique email addresses being exposed. Many records within the data also included additional personal attributes such as names, phone numbers, IP addresses, dates of birth and genders. No passwords were included in the data. The Verifications.io website went offline during the disclosure process, although an archived copy...

OnlinerSpambot

August 28, 2017 *2 email references*

In August 2017, a spambot by the name of Onliner Spambot was identified by security researcher Benkow mo?u?q. The malicious software contained a server-based component located on an IP address in the Netherlands which exposed a large number of files containing personal information. In total, there were 711 million unique email addresses, many of which were also accompanied by corresponding passwords. A full write-up on what data was found is in the blog post titled Inside the Massive 711 Million Record Onliner Spambot Dump.

Adobe

October 4, 2013 *1 email reference*

In October 2013, 153 million Adobe accounts were breached with each containing an internal ID, username, email, encrypted password and a password hint in plain text. The password cryptography was poorly done and many were quickly resolved back to plain text. The unencrypted hints also disclosed much about the passwords adding further to the risk that hundreds of millions of Adobe customers already faced.

LinkedIn

May 5, 2012 *1 email reference*

In May 2016, LinkedIn had 164 million email addresses and passwords exposed. Originally hacked in 2012, the data remained out of sight until being offered for sale on a dark market site 4 years later. The passwords in the breach were stored as SHA1 hashes without salt, the vast majority of which were quickly cracked in the days following the release of the data.