CYBLE®

REPORT

Threat Landscape Report 2024

Region: **ANZ**

Table of **Contents**

Executive Summary

The cybersecurity landscape in the Australia and New Zealand (ANZ) region is experiencing unprecedented challenges, with a significant uptick in high-profile cyber incidents targeting critical sectors such as finance, healthcare, government, and infrastructure. Recent attacks have exploited critical software vulnerabilities, utilized Ransomware-as-a-Service (RaaS) models, and conducted ideologically motivated Distributed Denial-of-Service (DDoS) campaigns. This surge in cyber threats is largely attributed to financially motivated cybercriminals and geopolitically driven actors, underscoring the urgent need for robust, sector-specific security measures and proactive defenses.

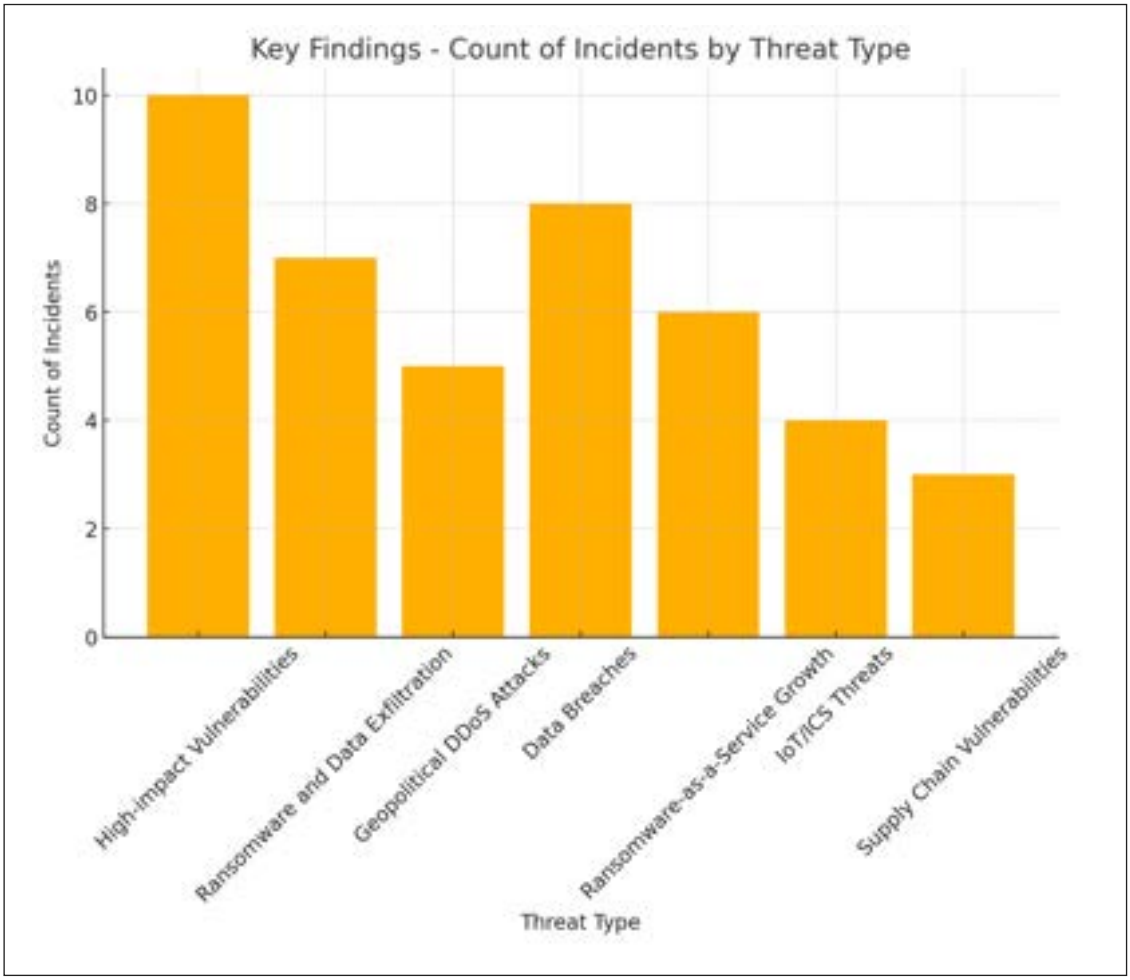
Key vulnerabilities, including the recently disclosed CVE-2024-21887, have allowed attackers to deploy malware, execute unauthorized code, and disrupt essential services. As a result, sectors dependent on secure, uninterrupted operations—such as healthcare and financial services—face heightened risks. Attackers continue to exploit newly identified weaknesses in critical systems, risking data exposure, service disruptions, and regulatory challenges.

Geopolitical factors have amplified the threat landscape, with ideologically motivated groups such as People's Cyber Army and Mysterious Team Bangladesh targeting government websites, financial institutions, and infrastructure, particularly in retaliation for Australia's global political alignments. These attacks often aim to disrupt public services, influence public perception, and pressure government resources.

A significant rise in data breaches has exposed sensitive information across sectors, with stolen records often sold on the dark web or exploited for further attacks. RaaS models, like the recently introduced SpiderX, enable a broader range of threat actors to carry out ransomware attacks, expanding the threat landscape and increasing the likelihood of incidents. Additionally, increased supply chain vulnerabilities are leaving organizations exposed to third-party threats through malicious software packages and compromised services.

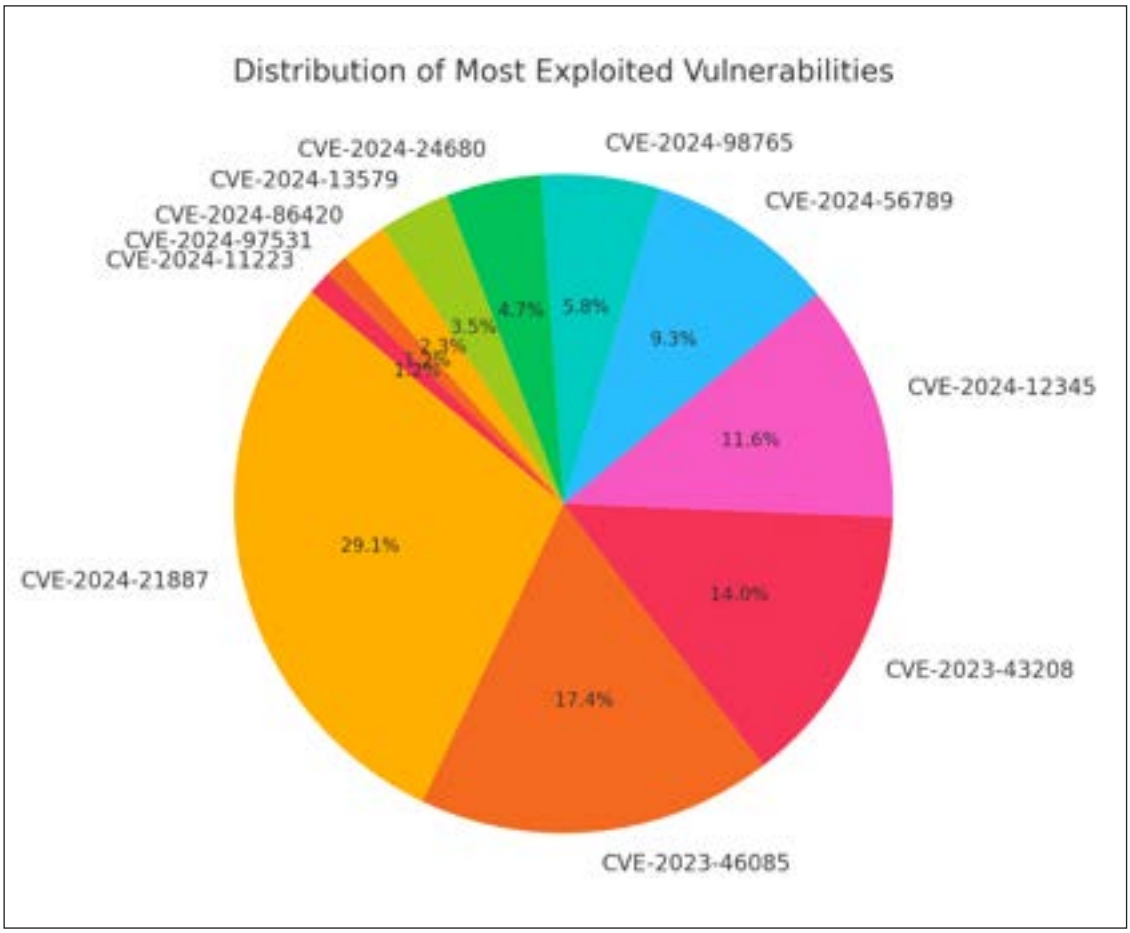
In response to these escalating threats, Cyble offers a comprehensive suite of cybersecurity solutions tailored to the unique challenges faced by organizations in the ANZ region. Cyble's offerings include advanced attack surface management (ASM), dark web monitoring, and threat intelligence services designed to proactively identify and mitigate risks. Notably, Cyble has introduced capabilities such as deepfake detection, physical security intelligence, and cloud security posture management, providing organizations with the tools necessary to enhance their cybersecurity posture and protect valuable assets in an increasingly complex threat environment.

Key Findings



- Persistent exploitation of high-impact vulnerabilities, such as CVE-2024-21887.
- Rising ransomware and data exfiltration incidents targeting finance, healthcare, and government.
- Surge in geopolitically motivated DDoS attacks, disrupting critical infrastructure.
- Data breaches across sectors, exposing customer, employee, and financial information.
- Growth in RaaS offerings, enabling less sophisticated actors to launch ransomware attacks.
- Increased threats to IoT and ICS systems, risking operational disruptions.
- Escalating supply chain vulnerabilities and more sophisticated phishing campaigns.

Most Exploited Vulnerabilities



Cyber attackers continue to exploit critical software and infrastructure vulnerabilities, impacting a range of sectors globally. Notable vulnerabilities such as CVE-2024-21887, affecting Ivanti systems, and flaws in cloud platforms, IoT devices, and popular software applications have emerged as key attack vectors. Exploitation of these vulnerabilities allows attackers to deploy malware, execute unauthorized code, and disrupt services, underscoring the urgency for organizations to prioritize timely patching and security updates.

- **CVE-2023-46085:** A critical vulnerability in certain applications, allowing attackers to deploy destructive malware like WhisperGate. The Australian Cyber Security Centre (ACSC) issued a high alert regarding this vulnerability.
- **CVE-2024-21887:** A critical flaw affecting ICS (9.x, 22.x) and IPS systems, potentially leading to unauthorized access and data breaches. The ACSC highlighted the urgency of patching this vulnerability.
- **CVE-2023-43208:** A high-severity vulnerability in NextGen Mirth Connect's Java XStream, predominantly impacting healthcare organizations. Exploitation could result in unauthorized code execution.
- **CVE-2024-12345:** A critical zero-day vulnerability in widely used financial software, leading to unauthorized transactions. Financial institutions in the ANZ region reported significant incidents related to this flaw.

- **CVE-2024-56789:** A severe vulnerability in cloud service platforms, allowing attackers to gain administrative control over virtual machines. Several ANZ businesses experienced data breaches due to this exploit.
- **CVE-2024-98765:** A critical flaw in popular content management systems, enabling remote code execution. Numerous websites in the ANZ region were defaced or compromised.
- **CVE-2024-24680:** A high-severity vulnerability in network infrastructure devices, leading to widespread service disruptions. The ACSC issued alerts urging immediate patching.
- **CVE-2024-13579:** A critical vulnerability in mobile banking applications, exposing user credentials. Banks in the ANZ region implemented emergency updates to mitigate risks.
- **CVE-2024-86420:** A severe flaw in IoT devices used in industrial settings, allowing attackers to disrupt operations. Manufacturing sectors in the ANZ region reported incidents linked to this vulnerability.
- **CVE-2024-97531:** A critical vulnerability in widely used email servers, facilitating phishing campaigns. Organizations in the ANZ region faced increased phishing attacks exploiting this flaw.
- **CVE-2024-11223:** A high-severity vulnerability in VPN solutions, leading to unauthorized network access. Several businesses in the ANZ region reported breaches due to this exploit.

Among the listed vulnerabilities, **CVE-2024-21887** stands out as the most critical, with a CVSS score of 9.1. This command injection vulnerability affects Ivanti Connect Secure (ICS) versions 9.x and 22.x, as well as Ivanti Policy Secure (IPS). Exploitation allows authenticated administrators to execute arbitrary commands on the appliance, potentially leading to unauthorized access and data breaches.

The Australian Cyber Security Centre (ACSC) emphasized the urgency of patching this vulnerability due to its severe implications.

Major Cybersecurity Incidents targeting ANZ Region

The ANZ region has witnessed a surge in high-profile cyber incidents, with organizations in sectors such as finance, healthcare, and critical infrastructure facing attacks from a variety of threat actors. Recent breaches have included data exfiltration, DDoS attacks, and ransomware deployments by actors motivated by financial gain, ideological causes, and political retaliation. These incidents illustrate the broad vulnerability landscape and the pressing need for robust cybersecurity measures across industries.

Incident: Source codes of 'Baby Steps' video game on sale
Actor: IntelBroker, EnergyWeaponUser
Impact: Exfiltration of source codes
Details: Source codes for PS5 and PC versions stolen from co-developer's Bitbucket, offered for $50K.

Incident: DDoS attacks on Australian infrastructure
Actor: People's Cyber Army
Impact: DDoS attacks on Australian critical infrastructure
Details: Attacks targeted government website, telecom, and port in retaliation for Ukraine support.

Incident: Compromise of Funlab Holdings Pty Limited
Actor: Lynx
Impact: Compromise of entertainment company
Details: Threat actors posted proof of compromise via sample folders.

Incident: Data from Caleb & Brown's live chat support system
Actor: Chow
Impact: Exfiltration of data from cryptocurrency brokerage
Details: Live chat data involving AI agent discussions offered for sale for 1 BTC.

Incident: DDoS attack against Bank of Sydney
Actor: RipperSec
Impact: DDoS attack on bank
Details: DDoS motivated by support for Palestinian cause using MegaMedusa tool.

Incident: Exfiltration of data from Ultra Tune Australia Pty Ltd
Actor: FOG
Impact: Exfiltration of customer and HR data
Details: 3 GB of data claimed to be stolen without posting proof.

Incident: DDoS attacks on Australian airports
Actor: Mysterious Team Bangladesh
Impact: DDoS attacks on airports
Details: DDoS attacks in response to Australia's support for Israel.

Incident: Acloan's database leak
Actor: markitto35
Impact: Database leak containing loan agreements and personal data
Details: Files include loan agreements and personal information.

Incident: DDoS attack on Bisalloy Steels
Actor: Liquid Blood
Impact: DDoS attack on steel manufacturer
Details: DDoS attack on steel provider supporting defense industry.

Incident: Attack on Compass Group (Australia)
Actor: Medusa
Impact: Compromise and exfiltration of data from corporate entity
Details: Ransom demanded with data leak threat in 8 days.

Incident: Evolution Mining cyber incident
Actor: Not specified
Impact: Contained cyber incident
Details: Incident reported to ACSC with limited information available.

Incident: Database theft from Early Settler Group
Actor: Worry
Impact: Database theft containing customer data
Details: Database contains customer records, stolen in July 2024.

Incident: Attack on Engedi Inc.
Actor: Rhysida
Impact: Exfiltration of personal identification details
Details: Sensitive identification documents leaked with ransom demand.

Incident: Database theft from Adreno Scuba Diving
Actor: Worry
Impact: Database theft containing customer records
Details: Database includes customer info without price quoted.

Incident: Compromise of Australian Department of Justice
Actor: Pysa
Impact: Compromise of South African government department
Details: Compromise of justice department with significant data loss.

Incident: Unauthorized access to BlueScope Steel Limited
Actor: IntelBroker
Impact: Unauthorized SSH access for sale
Details: Access to manufacturing company SSH listed for sale.

Incident: Stake gambling platform data breach
Actor: Taken
Impact: Data breach of notable individuals
Details: Breach from 2022 advertised in 2024.

Incident: Trojanized jQuery npm campaign
Actor: Various (not specified)
Impact: Malicious npm packages for supply chain attacks
Details: Malicious npm packages for supply chain attacks.

Incident: Data from Opaxe Pty Ltd on sale
Actor: Tanaka
Impact: Database exfiltrated and put on sale
Details: Database containing millions of rows and user data.
Incident: Ransomware attack on Harry Perkins Institute
Actor: Medusa
Impact: Exfiltration of video recordings
Details: Camera recordings exfiltrated without proof.

Incident: Exfiltration of data from Reward Supply Co Pty Ltd
Actor: Black Suit
Impact: Sensitive document theft with no proof provided
Details: Sensitive document theft with no proof provided.

Incident: Ransomware attack on Insula Group Pty Ltd
Actor: BianLian
Impact: Exfiltration of source code and sensitive data
Details: Source codes and sensitive data exfiltrated without proof.

Incident: Microsoft employee data leak
Actor: 888
Impact: PII leak of Microsoft employees
Details: PII records of employees leaked from third-party breach.

Incident: Ransomware attack on Brett Slater Solicitors
Actor: Akira
Impact: Compromise of legal documents
Details: Legal document compromise disclosed publicly.

Incident: Introduction of SpiderX RaaS
Actor: phant0m
Impact: Ransomware-as-a-Service offering
Details: SpiderX includes encryption and data exfiltration for $150 BTC.

Incident: Ransomware attack on Herron Todd White Pty Ltd
Actor: Black Suit
Impact: Exfiltration of property advisory data
Details: Property advisory data exfiltrated by ransomware group.

Incident: Data theft from SSS Australia
Actor: Hunters International
Impact: Exfiltration of medical supplier data
Details: Medical supplier data with publication threat.

Incident: Cybercrime analysis of April 2023 incidents
Actor: Multiple actors
Impact: Diverse cyber threats analysis
Details: Overview of 22 incidents covering ransomware, data breaches, and financial fraud.

Incident: Database leak from DancingAngel Productions
Actor: redcoat
Impact: Media company database leak
Details: Database leak from a New Zealand media company.

Incident: Data sale from Rave Build Management Ltd
Actor: adre
Impact: Construction software database sale
Details: Data put up for sale containing customer information.

Incident: Database leak from University of Western Australia
Actor: sarah_jackson
Impact: Leak of university data
Details: Database leak from an Australian university.

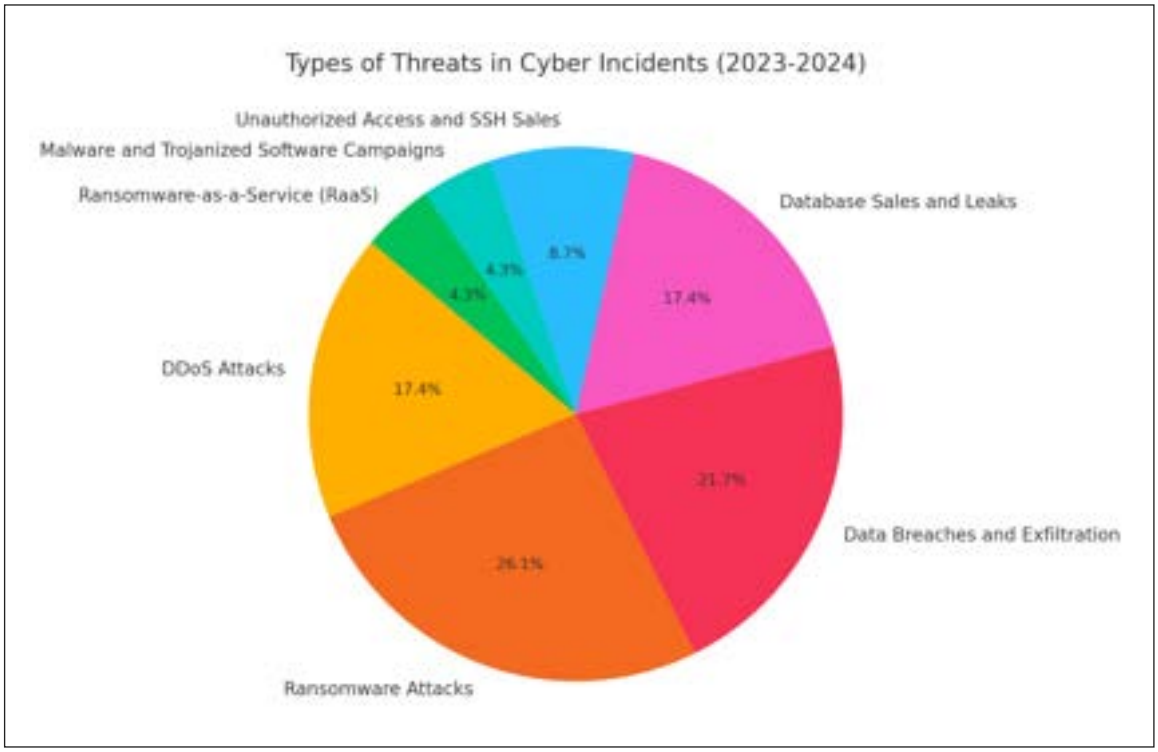
Incident: Leak of 40k Australia Database Leads
Actor: PIRATE04
Impact: Leak of database with PII and financial data
Details: Data leak affecting 40k Australian leads.

Incident: Data leak from unidentified shipping company
Actor: biskut
Impact: Medium risk database leak
Details: Data leak from an Australian shipping company.

Incident: Data leak from Australian Academic Centre
Actor: B33N
Impact: Database leak
Details: Database leak

Threat Types

Cyber threats affecting the ANZ region encompass a diverse range of tactics, including DDoS, ransomware, data breaches, unauthorized access, and emerging ransomware-as-a-service offerings. Key actors, often driven by political, financial, and strategic motives, have targeted critical infrastructure, financial institutions, and retail organizations. The persistent nature of these threats emphasizes the need for sector-specific security strategies to defend against increasingly sophisticated cyber attacks.



DDoS Attacks

- **Targeted Entities:** Government websites, telecom companies, banks, airports, and steel manufacturers.
- **Notable Actors:** People's Cyber Army, RipperSec, Mysterious Team Bangladesh, Liquid Blood.
- **Motivations:** Political retaliation (e.g., support for Ukraine or Israel) or ideological causes (support for Palestine).
- **Impact:** Temporary disruption of services in sectors like banking, transportation, and logistics, affecting critical infrastructure.
-

Ransomware Attacks

- **Targeted Entities:** Australian companies in sectors such as property advisory, medical supply, entertainment, and government agencies.
- **Notable Actors:** Medusa, Lynx, FOG, Akira, Rhysida, Black Suit, BianLian.
- **Impact:** Exfiltration of sensitive data (employee info, financial records, and personal identification documents) and ransom demands.
- **Unique Cases:** Medusa demanded a ransom of 2 million dollars from Compass Group, and data from Harry Perkins Institute and Engedi Inc. were also exfiltrated.

Data Breaches and Exfiltration

- **Targeted Entities:** Various sectors, including gambling platforms, customer databases, cryptocurrency brokerages, loan service companies, and academic institutions.
- **Notable Actors:** Chow, markitto35, Taken, Tanaka, Worry, Pysa, B33N.
- **Impact:** Leaks of PII (Personally Identifiable Information), financial data, healthcare data, and customer records.
- **Examples:** Microsoft employee data leak (888 actor), Stake gambling platform breach, and the Australian Academic Centre database leak.

Database Sales and Leaks

- **Targeted Entities:** Financial services, healthcare, educational institutions, construction management software, and media.
- **Notable Actors:** Various BreachForum actors such as redcoat, adre, and PIRATE04.
- **Impact:** Exposure of customer information, loan agreements, PII, and business records.
- **Examples:** Database leaks from Early Settler Group, Adreno Scuba Diving, and the University of Western Australia.

Unauthorized Access and SSH Sales

- **Targeted Entities:** Manufacturing and large enterprises.
- **Notable Actors:** IntelBroker.
- **Impact:** Unauthorized access (e.g., SSH access to BlueScope Steel) offered for sale, potentially allowing further compromise or ransomware deployment.
- **Example:** IntelBroker listed SSH access for sale, targeting BlueScope Steel for USD 20,000.

Malware and Trojanized Software Campaigns

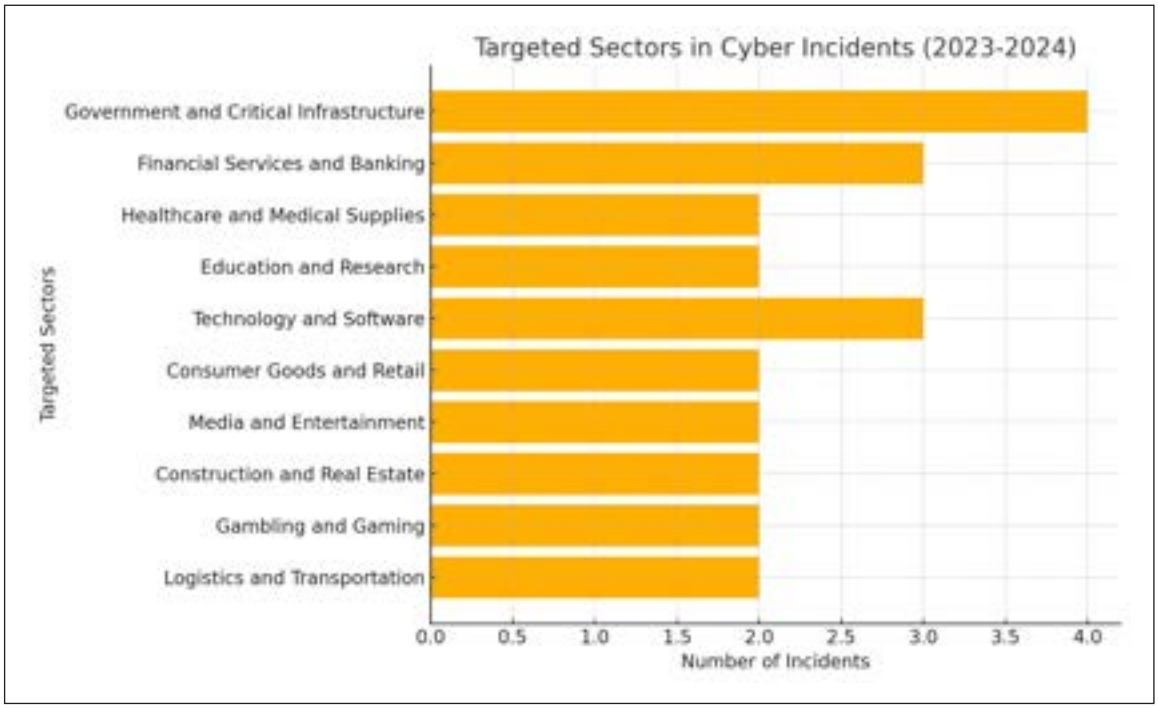
- **Details:** Focus on supply chain threats with malicious npm packages (e.g., trojanized jQuery npm packages).
- **Impact:** Potential infiltration into supply chains, affecting software users globally, with a high risk to Windows users.
- **Example:** Various actors published malicious npm packages designed for supply chain attacks.

Ransomware-as-a-Service (RaaS)

- **Example:** Introduction of SpiderX RaaS by phant0m, offering features like data encryption and exfiltration at a low cost.
- **Impact:** Increased access to ransomware capabilities for smaller threat actors, spreading potential threats.
- **Unique Features:** ChaCha20-256 encryption and data storage on MegaNz.

Sectoral Analysis

Various sectors, from government to financial services and healthcare, have experienced targeted cyber attacks in the ANZ region, each with unique impacts and motivations. Government entities face ideologically driven DDoS and ransomware attacks, while financial and healthcare sectors are increasingly targeted for sensitive data theft and financial extortion. The focus on sector-specific vulnerabilities highlights the strategic importance of tailoring cybersecurity defenses to the unique challenges each sector faces.



1. Government and Critical Infrastructure

- **Threat Types:** DDoS attacks, ransomware, unauthorized access.
- **Notable Incidents:**
  - **Australian Prime Minister's Website:** Targeted by People's Cyber Army in a DDoS attack.
  - **South African Department of Justice:** Compromised by the Pysa ransomware group.
  - **BlueScope Steel (Manufacturing):** Unauthorized SSH access offered for sale by IntelBroker.
- **Impact:** Disruptions to essential services, exposure of sensitive government or critical infrastructure data, and potential vulnerabilities in system access.
- **Motivation:** Political retaliation and ideological reasons.

2. Financial Services and Banking

- Threat Types: DDoS attacks, data breaches, ransomware.
- **Notable Incidents:**
  - **Bank of Sydney:** DDoS attack by RipperSec.
  - **Caleb & Brown (Cryptocurrency Brokerage):** Exfiltration of customer chat data by Chow.
  - **Acloan (Financial Services):** Data leak involving customer loan agreements.

- **Impact:** Service disruptions affecting financial transactions, exposure of sensitive financial data, and potential reputational damage.
- **Motivation:** Political and financial gains, targeting high-value and high-visibility entities.

3. Healthcare and Medical Supplies

- **Threat Types:** Ransomware, data breaches.
- **Notable Incidents:**
  - **SSS Australia (Medical Supplier):** Data exfiltration by Hunters International.
  - **Top End Allied Health Services:** Data breach exposing healthcare and payroll information.
- **Impact:** Compromise of personal healthcare data, financial information, and potential regulatory consequences.
- **Motivation:** Financial extortion and data theft for resale.

4. Education and Research

- **Threat Types:** Data leaks, ransomware.
- **Notable Incidents:**
  - **University of Western Australia:** Data leak affecting university records.
  - **Harry Perkins Institute:** Exfiltration of 4.6 TB of data by Medusa ransomware group.
- **Impact:** Exposure of academic and research data, sensitive identification details, and potential disruptions to ongoing research.
- **Motivation:** Financial extortion, potential exploitation of academic information for resale or further cyber attacks.

5. Technology and Software

- **Threat Types:** Data leaks, malware campaigns, RaaS offerings.
- **Notable Incidents:**
  - **Microsoft:** Employee data leaked, including PII.
  - **Trojanized jQuery npm Campaign:** Targeted at software users in a supply chain attack.
  - **SpiderX RaaS:** Ransomware service promoted for cybercriminals.
- **Impact:** Compromise of sensitive employee data, risk to supply chains through software dependencies, and increased threat landscape from accessible RaaS.
- **Motivation:** Financial incentives, facilitation of cyber attacks via supply chains, and lowering barriers for cybercrime.

6. Consumer Goods and Retail

- **Threat Types:** Ransomware, data leaks.
- **Notable Incidents:**
  - **Early Settler Group (Retail):** Database theft containing 1.1 million customer records.
  - **Reward Supply Co Pty Ltd:** Exfiltration of 385 GB of sensitive documents by Black Suit ransomware.
- **Impact:** Exposure of customer data, potential identity theft, and reputational damage.
- **Motivation:** Financial extortion, sale of customer data on black markets.

7. Media and Entertainment

- **Threat Types:** Data leaks, unauthorized access.
- **Notable Incidents:**
  - **Funlab Holdings Pty Limited (Entertainment):** Compromised by Lynx, leaking sample folders and financial documents.
  - **DancingAngel Productions:** Data breach involving New Zealand-based media company.
- **Impact:** Exposure of sensitive business data, potential leak of intellectual property, and reputational harm.
- **Motivation:** Financial gain, data theft for resale, and disruption of operations.

8. Construction and Real Estate

- **Threat Types:** Data leaks, ransomware.
- **Notable Incidents:**
  - **Herron Todd White Pty Ltd (Property Advisory):** Ransomware attack resulting in 300 GB of exfiltrated data.
  - **Rave Build Management Ltd (Construction Software):** Data sale involving customer information.
- **Impact:** Leak of property advisory data and construction management information, compromising client confidentiality and trust.
- **Motivation:** Financial incentives, sale of industry-specific data.

9. Gambling and Gaming

- **Threat Types:** Data breaches.
- **Notable Incidents:**
  - **Stake Gambling Platform:** Data breach exposed notable individuals' details.
  - **Baby Steps Video Game Source Codes:** Theft of source codes offered for sale.
- **Impact:** Exposure of customer details, intellectual property loss, and financial repercussions.
- **Motivation:** Financial gain, resale of stolen IP, and targeting high-profile clientele.

10. Logistics and Transportation

- **Threat Types:** DDoS attacks, data leaks.
- **Notable Incidents:**
  - breach exposed notable individuals' details.
  - des offered for sale.
- **Impact:** Service disruptions in transportation, exposure of operational data, and potential logistical delays.
- **Motivation:** Political retaliation, financial gain, and operational disruption of critical transportation services.

Geopolitical Influence and Cybersecurity Implications

Global political dynamics have increasingly influenced the nature and frequency of cyberattacks, where geopolitical tensions have direct implications for cybersecurity. Cyber actors, whether state-sponsored groups or ideologically motivated individuals, often use cyberattacks as a vehicle to express dissent, retaliate against political stances, or destabilize adversaries. Australia, for instance, has faced a surge in cyber incidents as a result of its support for Ukraine and Israel, which has triggered retaliatory attacks from various politically motivated threat actors.

A notable example includes Distributed Denial of Service (DDoS) attacks carried out by groups like the People's Cyber Army and Mysterious Team Bangladesh. These attacks targeted Australian government websites, telecommunications firms, and airports, intentionally disrupting critical services and infrastructure. These DDoS campaigns not only aimed to cripple essential systems but also served as a form of protest, expressing disagreement with Australia's geopolitical alignment. For these threat groups, the objective goes beyond financial gain; it's about making a statement and creating political pressure by impacting public perception and government resources.

Additionally, Australia's Department of Justice was compromised in incidents linked to international threat actors, further demonstrating the global nature of modern cyber threats. This breach, like many others, underscores how quickly political and diplomatic tensions can evolve into cyber conflicts. For countries like Australia, the stakes are high as these cyber incidents threaten national security, disrupt critical services, and may even influence government policy. Such attacks can destabilize regions, erode public trust, and create vulnerabilities that could be exploited further by adversarial nations or groups.

Motivations Behind Cyberattacks

Cyberattacks are driven by a range of motivations, from political ideology to financial incentive and even strategic espionage. Below are the primary motivations that underlie these cyber incidents:

1. **Political Retaliation and Ideological Causes:** Politically motivated threat actors are increasingly using cyberattacks to make ideological statements or retaliate against nations whose policies they oppose. For instance, DDoS attacks by groups like RipperSec and Mysterious Team Bangladesh were motivated by political reasons, notably in response to Australia's support for Ukraine and Israel. The People's Cyber Army, a collective with a history of politically driven cyber activities, was responsible for attacks on Australian infrastructure, seeking to disrupt essential services as a form of digital protest. These attacks are less about financial extortion and more about causing public disruption and sending a political message to both the targeted government and its allies. Such cyber campaigns often align with global events, where international stances on geopolitical matters spur a cascade of digital confrontations.

2. **Financial Gain:** Financial motivation remains one of the most prevalent drivers behind cybercrime, with ransomware attacks at the forefront. Groups like Medusa and Black Suit have targeted sectors with sensitive, high-value data, such as healthcare, finance, and retail. These sectors are often vulnerable due to their critical reliance on data and operational uptime, making them prime targets for ransomware. Attackers exfiltrate sensitive data, including patient records, financial information, and proprietary business details, then demand ransoms to prevent public disclosure. In many cases, the cost of downtime and data recovery incentivizes organizations to consider paying the ransom, which perpetuates the cycle of financially motivated attacks. These threat actors are increasingly sophisticated, leveraging Ransomware-as-a-Service (RaaS) models to distribute tools to a broader range of attackers. This allows even less technically skilled individuals to carry out attacks, thus broadening the threat landscape and raising the likelihood of financially motivated incidents.

3. **Data Theft and Espionage:** Cyber espionage has emerged as a significant motivation behind many data breaches and unauthorized access incidents, especially in sectors with valuable intellectual property or sensitive personal information. Incidents like the unauthorized access to BlueScope Steel and the leak of Microsoft employee data exemplify attacks driven by data theft and espionage. State-sponsored groups and cybercriminals alike seek proprietary information, research data, and personnel records, which can be exploited for economic gain or political leverage. For example, a breach involving proprietary manufacturing processes could provide an advantage to competing industries, while access to employee records might enable further social engineering attacks or provide intelligence on high-value targets within organizations. Unlike financially motivated ransomware attacks, espionage-driven incidents tend to be stealthier, with attackers often remaining undetected for extended periods to maximize data collection efforts.

Forecast and Expected Trends

As cybersecurity threats evolve, organizations can anticipate a rise in ransomware, supply chain attacks, and data breaches, driven by both geopolitical tensions and the pursuit of financial gains. Critical sectors, such as healthcare, finance, and government, may see heightened risks from increasingly accessible RaaS platforms, intensified exploitation of software vulnerabilities, and sophisticated phishing campaigns. Preparing for these trends is essential as the cybersecurity landscape continues to grow in complexity and scale

1. **Increased Exploitation of Critical Vulnerabilities:** Attackers are likely to intensify efforts to exploit recently identified critical vulnerabilities, such as CVE-2024-21887, which affects Ivanti Connect Secure (ICS) and Ivanti Policy Secure (IPS) systems. Organizations that have not yet applied necessary patches may face heightened risks of unauthorized access and data breaches.

2. **Surge in Ransomware Attacks:** Ransomware groups, including Medusa, Lynx, and Black Suit, are expected to continue targeting sectors like healthcare, education, and finance. These attacks may involve data exfiltration followed by ransom demands, potentially leading to operational disruptions and financial losses.

3. **Escalation of DDoS Attacks Motivated by Geopolitical Tensions:** Distributed Denial-of-Service (DDoS) attacks, such as those executed by groups like People's Cyber Army and Mysterious Team Bangladesh, are anticipated to rise, particularly against government websites, financial institutions, and critical infrastructure. These attacks are often driven by political motives and can result in significant service disruptions.

4. **Proliferation of Data Breaches and Unauthorized Access:** Threat actors are expected to continue targeting organizations across various sectors to exfiltrate sensitive data, including personally identifiable information (PII) and financial records. Industries such as retail, education, and technology may be particularly vulnerable to these breaches.

5. **Emergence of New Ransomware-as-a-Service (RaaS) Offerings:** The introduction of services like SpiderX RaaS indicates a trend toward more accessible ransomware tools for cybercriminals. This development could lead to an increase in ransomware attacks by less sophisticated actors, expanding the threat landscape.

6. **Targeted Attacks on Supply Chains:** Supply chain attacks, including the distribution of trojanized software packages, are expected to rise. Organizations relying on third-party software and services should exercise increased vigilance to prevent such compromises.

7. **Focused Attacks on Financial Institutions:** Given the critical nature of financial data, banks and financial services are likely to remain prime targets for cybercriminals seeking financial gain through data breaches, ransomware, or unauthorized transactions.

8. **Heightened Threats to Healthcare and Medical Sectors:** The healthcare industry may face increased cyber threats, including ransomware attacks and data breaches, potentially compromising patient data and disrupting essential services.

9. **Continued Exploitation of IoT and Industrial Control Systems:** Vulnerabilities in Internet of Things (IoT) devices and Industrial Control Systems (ICS) may be increasingly targeted, leading to potential operational disruptions in manufacturing and critical infrastructure sectors.

10. **Amplified Phishing and Social Engineering Campaigns:** Cybercriminals are expected to enhance phishing and social engineering tactics, leveraging current events and exploiting human vulnerabilities to gain unauthorized access to systems and data.

Regional Overview of Cybersecurity Developments

The Australia and New Zealand (ANZ) region is undergoing significant transformations in its cybersecurity landscape, driven by escalating cyber threats and proactive governmental measures. Both nations have introduced strategic initiatives, increased budget allocations, and enacted new legislation to fortify their cybersecurity frameworks. This report examines the current threat environment and offers actionable insights for mitigating risks in high-priority sectors, including finance, healthcare, government, and infrastructure. Key areas of focus encompass leveraging government directives, capitalizing on regional budget enhancements, and adhering to recent cybersecurity regulations to counteract the growing sophistication of cybercriminals and politically motivated threat actors.

Australia's Cybersecurity Initiatives

In response to the evolving cyber threat landscape, Australia has implemented significant measures to strengthen its cybersecurity posture:

- **2023–2030 Australian Cyber Security Strategy:** Released on 22 November 2023, this comprehensive roadmap aims to position Australia as a world leader in cybersecurity by 2030. The strategy emphasizes protecting Australians through enhanced legislative frameworks and increased funding for cybersecurity initiatives.
- **Cyber Security Legislative Package 2024:** Introduced in October 2024, this package aims to implement seven initiatives under the 2023–2030 strategy, addressing legislative gaps to align Australia with international best practices. It includes measures such as the Cyber Security Bill 2024 and amendments to the Security of Critical Infrastructure Act.

New Zealand's Cybersecurity Efforts

New Zealand has also taken steps to enhance its cybersecurity resilience:

- **National Cyber Security Centre (NCSC) Strategy:** The NCSC has been instrumental in supporting nationally significant organizations to improve their cybersecurity resilience. Its strategy to 2024 guides the delivery of services aimed at protecting the nation's wellbeing and prosperity through trusted cybersecurity services.
- **Advancement of Cybercrime Legislation:** In October 2024, New Zealand advanced its cybercrime legislation with the first reading of new laws aimed at protecting citizens from increasing digital fraud and cybercrime. This legislative effort seeks to align New Zealand's legal framework with international standards, enhancing the country's defenses against cyber threats.

Key Regional Insights

1. Government Budget Enhancements:

- **Australia:** The 2024–25 federal budget reflects a strong commitment to cybersecurity, with significant allocations including $206 million to improve the cybersecurity of regulators and registers, $288.1 million to expand Australia's Digital ID system, and $472 million invested in quantum computing. These investments underscore the government's dedication to bolstering national cybersecurity infrastructure.
- **New Zealand:** While specific budget figures are less prominently reported, New Zealand continues to invest in cybersecurity through initiatives led by the NCSC and other governmental bodies, focusing on enhancing national resilience against cyber threats.

2. New Cyber Codes and Legislation:

- **Australia:** The Cyber Security Legislative Package 2024 aims to implement seven initiatives under the 2023–2030 Australian Cyber Security Strategy. This package addresses legislative gaps to align Australia with international best practices and includes measures such as the Cyber Security Bill 2024 and amendments to the Security of Critical Infrastructure Act.
- **New Zealand:** In October 2024, New Zealand advanced its cybercrime legislation with the first reading of new laws aimed at protecting citizens from increasing digital fraud and cybercrime. This legislative effort seeks to align New Zealand's legal framework with international standards, enhancing the country's defenses against cyber threats.

3. Sector-Specific Cyber Threats:

- **Healthcare:** The healthcare sector faces heightened risks from ransomware attacks and data breaches, as evidenced by incidents targeting medical suppliers and health services. Protecting patient data and ensuring the continuity of critical services are paramount.
- **Finance:** Financial institutions are prime targets for cybercriminals seeking financial gain through data breaches, ransomware, and unauthorized transactions. Strengthening defenses against these threats is crucial to maintaining trust and stability in the financial system.
- **Government and Infrastructure:** Government entities and critical infrastructure are susceptible to ideologically motivated attacks, including Distributed Denial-of-Service (DDoS) campaigns. Implementing robust security measures is essential to safeguard national security and public services.

How Cyble is Addressing Cybersecurity Challenges in the ANZ Region

Cyble provides a robust suite of cybersecurity solutions tailored to meet the unique challenges faced by organizations in the Australia and New Zealand (ANZ) region. These solutions encompass **Attack Surface Management (ASM), Brand Intelligence, Dark Web Monitoring, Advanced Threat Intelligence**, and cutting-edge capabilities in **Executive Monitoring, Physical Security Intelligence, Cloud Security Posture Management**, and more.

Key Offerings

1. Attack Surface Management (ASM)

- **Comprehensive Visibility:** Cyble's ASM tools identify and mitigate threats across an organization's entire digital footprint, ensuring protection against vulnerabilities.
- **Proactive Security:** Enables organizations to uncover hidden risks, providing actionable intelligence to stay ahead of cyber threats.

2. Brand Intelligence

- **Protect Brand Integrity:** Safeguard against impersonation, phishing attacks, and fraudulent domains to maintain trust and credibility in the digital space.
- **Online Abuse Mitigation:** Ensure your brand remains uncompromised across various platforms.

3. Cyber Threat Intelligence

- **Actionable Insights:** Aggregates data from diverse sources, helping organizations detect and mitigate threats in real time.
- **Enhanced Response Times:** Reduces the need for manual monitoring, streamlining threat detection and response.

4. Dark Web Monitoring

- **Continuous Vigilance:** Scans millions of websites, forums, and marketplaces in real time, identifying threats specific to the ANZ region.
- **Custom Alerts:** Set up personalized notifications to enable swift responses to emerging threats.
- **Safeguarding Stakeholders:** Tracks compromised information to minimize the impact of potential breaches.

5. Executive Monitoring

- **Leadership Protection:** Safeguards executives by tracking impersonations, deepfake content, and personally identifiable information (PII) leaks across social media, dark web platforms, and cybercrime forums.
- **Deepfake Detection and Takedown:** Utilizes advanced AI technology to identify and remove manipulated media in real-time, protecting the reputation and integrity of key personnel.

6. Physical Security Intelligence

- **Comprehensive Threat Management:** Provides real-time updates to proactively address potential physical threats and ensure the safety of assets and personnel.
- **Centralized Oversight:** Effortlessly manage security across multiple locations, including offices and warehouses, from a unified platform.

7. Cloud Security Posture Management (CSPM)

- **Cloud Security Enhancement:** Offers continuous monitoring of cloud environments, identifying misconfigurations and ensuring compliance with security policies.

8. Takedown and Disruption

- **Fraud Prevention:** A powerful tool for combating online fraud and cybercrime, ensuring malicious content is promptly removed.

9. BotShield

- **Intelligence on Compromised Hosts:** Provides detailed insights into infected devices within your network that communicate with known command-and-control infrastructures.

10. Vulnerability Management

- **Real-Time Risk Evaluation:** Advanced scanning and remediation strategies give organizations a comprehensive view of exploitable vulnerabilities.

11. Third Party Risk Management (TPRM)

- **Secure Collaborations:** Identifies and mitigates risks arising from third-party interactions, ensuring secure business operations.

12. Digital Forensics & Incident Response (DFIR)

- **Comprehensive Support:** Cyble provides digital forensics and incident response services to help businesses manage, mitigate, and recover from cybersecurity incidents.
- **Timely Remediation:** Aids in reducing downtime and ensuring continuity post-incident.

Enhancing Cybersecurity in the ANZ Region with Cyble's Advanced Solutions

Cyble offers a suite of cybersecurity products tailored to address the unique challenges faced by organizations in the Australia and New Zealand (ANZ) region:

CYBLE VISION	**Cyble Vision:** Cyble Vision is an award-winning, AI-powered cyber threat intelligence platform that enhances organizational security through real-time intelligence and threat detection. It offers comprehensive features, including Attack Surface Management, Brand Intelligence, Cyber Threat Intelligence, Dark Web Monitoring, Executive Monitoring, Physical Security Intelligence, Cloud Security Posture Management, Takedown and Disruption, BotShield, Vulnerability Management, Third Party Risk Management, and Digital Forensics & Incident Response. These capabilities empower organizations in the ANZ region to proactively address emerging threats and safeguard their digital assets in an increasingly complex cyber threat landscape.
CYBLE HAWK	**Cyble Hawk:** A specialized threat detection and intelligence platform designed for federal bodies, law enforcement agencies, and regulatory organizations. Cyble Hawk provides insights into cybercrime activities relevant to national security, offers detailed information on threat actors targeting critical infrastructure, and delivers immediate notifications of emerging threats.
ODIN by CYBLE	**Odin by Cyble:** An advanced internet-scanning tool offering real-time threat detection and cybersecurity insights. Odin covers over 4 billion IPs to identify vulnerabilities, provides detailed host information—including data on IP addresses, hostnames, and locations—and allows for scanning and examination of digital certificates.
AmIBreached Powered by CYBLE	**AmIBreached:** A dark web search engine that enables consumers and organizations to identify, prioritize, and mitigate dark web risks. AmIBreached accesses over 150 trillion records from various breaches and forums, offers real-time monitoring with immediate alerts on compromised data, and provides a user-friendly interface for easy monitoring and management.
THE CYBER EXPRESS	**The Cyber Express:** A cybersecurity news platform providing current news, in-depth insights, and a wealth of knowledge on cybersecurity matters. The Cyber Express covers a wide range of topics, including cyber threats, vulnerabilities, and data breaches; offers expert analysis from skilled journalists and researchers; and provides educational content on cybersecurity auditing and compliance.

By leveraging these solutions, ANZ organizations can enhance their cybersecurity posture, proactively address emerging threats, and safeguard their digital assets in an increasingly complex cyber threat landscape.

About Cyble

Cyble Inc. is a cybersecurity company specializing in dark web monitoring and threat intelligence services. Cyble leverages proprietary AI-based technology to help enterprises, federal bodies, and individuals stay ahead of cybercriminals. The company is known for its expertise in tracking cyber threats, data breaches, and other malicious activities.

See Cyble in Action

10080 North Wolfe Road, Suite SW3-200, Cupertino, CA 95014 | contact@cyble.com | +1 888 673 2067