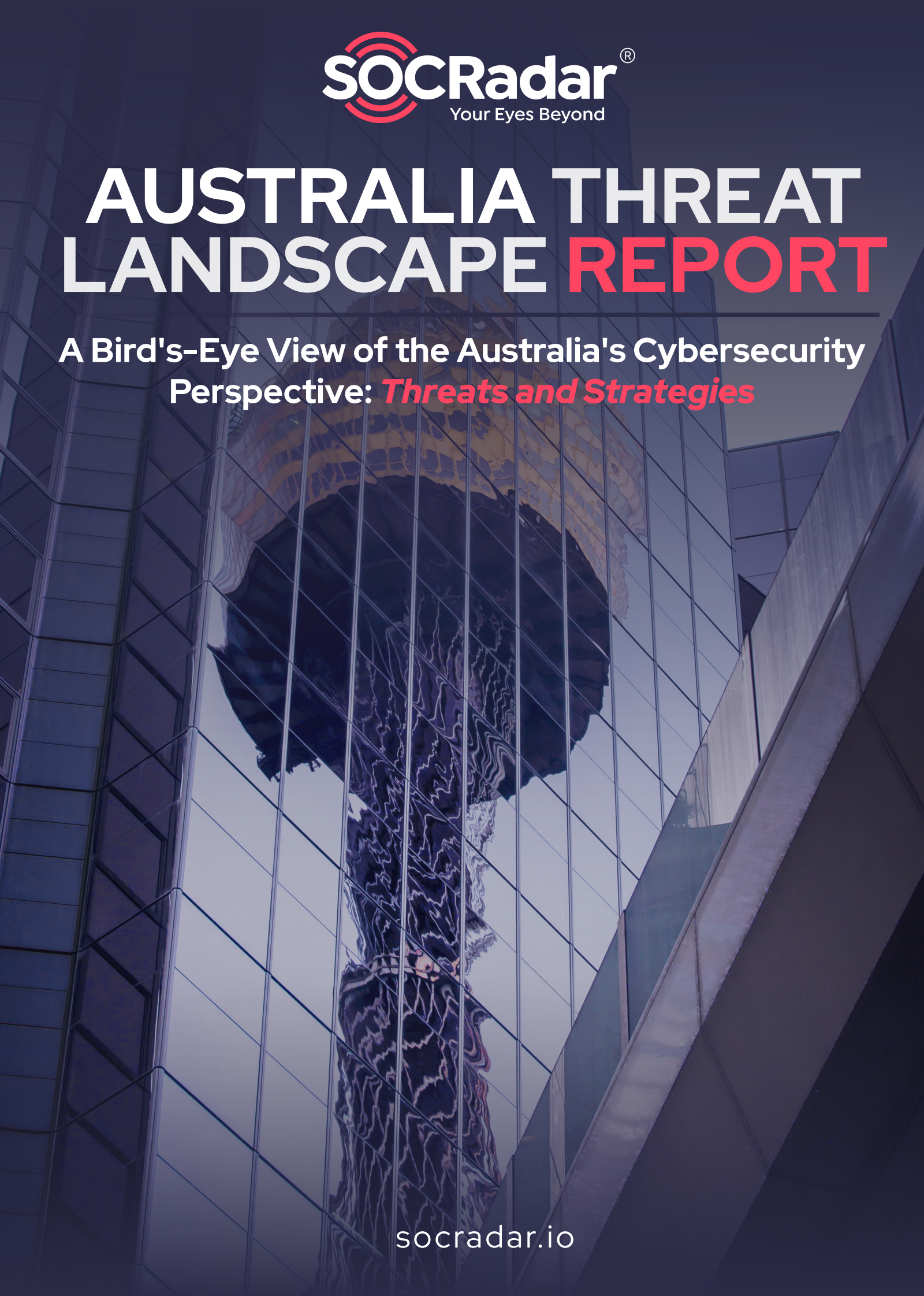
SOCRadar®
Your Eyes Beyond

AUSTRALIA THREAT LANDSCAPE REPORT

A Bird's-Eye View of the Australia's Cybersecurity Perspective: *Threats and Strategies*



socradar.io

Table of Contents

Executive Summary

In this comprehensive report, SOCRadar XTI analyzes the Australian cyber threat landscape, including dark web activities, ransomware attacks, phishing threats, and the impact of data breaches on the Australian government's cyber security measures. The report focuses on a time scope of 12 months between September 2022 and August 2023. The key findings are as follows;

1. **Dark Web Activities:** SOCRadar XTI platform identified 274 dark web posts mentioning Australia; most posts are related to data sharing and selling. The most targeted industries are Electronic Shopping and Mail Order Houses, Information, Finance and Insurance, and Retail Trade.

2. **Ransomware Attacks:** 76 ransomware attacks and 22 ransomware groups targeting Australian organizations were observed. Information, Healthcare and Social Assistance, Professional Scientific and Technical services are the most targeted industries.

3. **Phishing Threats:** The potential phishing domains impersonating Australian organizations listed on the SOCRadar XTI platform increased according to the previous 12-month term. Most of these domains are secured by HTTPS.

4. **Data Breaches:** Large-scale data breaches affected a remarkable portion of the Australian population, particularly in the last part of 2022 and early 2023. In response to the major data breaches, the Australian government took crucial steps such as aggravating legal penalties and began discussing a new cyber security strategy.

Introduction

Australia, as one of the leading economies in the Asia Pacific region, has seen a concerning rise in cyber-attacks against the country's critical infrastructure in recent years. According to the Australian Bureau of Statistics, more than two in 10 businesses (22%) experienced a cyber security attack during the 2021-22 financial year, compared to almost one in 10 (8%) in 2019-20. The Australian Government's online cybercrime reporting tool, ReportCyber, received over 76,000 cybercrime reports during the same period; this marked an increase of approximately 13% from the previous year.

Cyber-attacks on Australia continued to be effective, and Australia has been the victim of significant cyber-attacks, especially in the last part of 2022, the beginning of this report time scope. High-profile incidents impacting businesses across critical sectors such as telecommunication, healthcare, finance, and government. SOCRadar XTI has recorded various cyber-attacks suffered by Australian organizations, and notable threat actors' malicious activities targeted Australia.

By raising awareness about the specific cyber challenges facing Australia, this report aims to help Australian organizations better protect themselves against these evolving threats and provide insight into the decisive actions undertaken by the Australian government.

Timeline of Significant Cybersecurity Incidents in Australia

Optus Breach

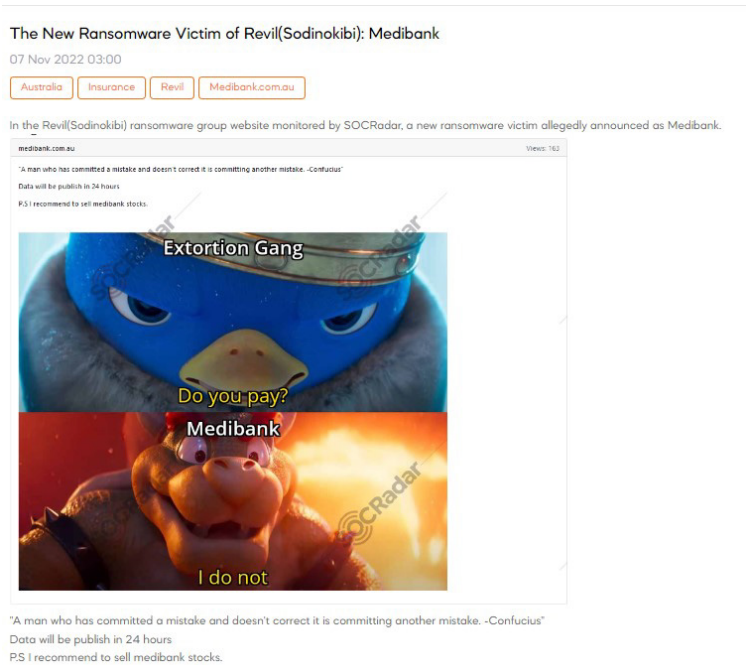
In September 2022, one of Australia's largest telecommunications companies, Optus, suffered a data breach, affecting approximately 9.7 million current and former customers. The breach exposed customers' personal information, including names, addresses, birthdates, phone numbers, e-mail addresses, and, in some cases, passport and driver's license numbers.

2.1 million of Optus's customers' identity documents and 37,000 Medicare ID numbers - government identification numbers that could be used for accessing medical records- had been stolen as part of the breach.

On September 20, Optus's technical team noticed and investigated suspicious activity on its network. The next day, it was identified that Optus's systems had sustained a data breach, and regulators were informed. On September 22, the company went public with the data breach.

Medibank

On October 13, 2022, Medibank announced a cyber-attack resulting in a data breach. Medibank, one of Australia's largest private health insurance providers, was breached by a ransomware group with ties to the defunct REvil gang, and nearly 500,000 Australian Medibank customers, along with almost 20,000 international customers, were affected. Following the breach, 9.7 million present and past customer details, including service provider names and codes associated with diagnosis and procedures, have been compromised.



Ransomware victim announcement for Medibank

Timeline of Significant Cybersecurity Incidents in Australia

Latitude

On March 16, Latitude Financial Services disclosed a data breach resulting from a cyber-attack that was detected with unusual activity on the company's systems, causing the company to shut down internal and customer-facing systems.

During the cyber-attack, the threat actor could steal employee login credentials and use them to steal personal customer information from two service providers.

Latitude Financial reported that the network breach had led to a "large-scale data theft affecting 14 million customers (past and present) and applicants across Australia and New Zealand".

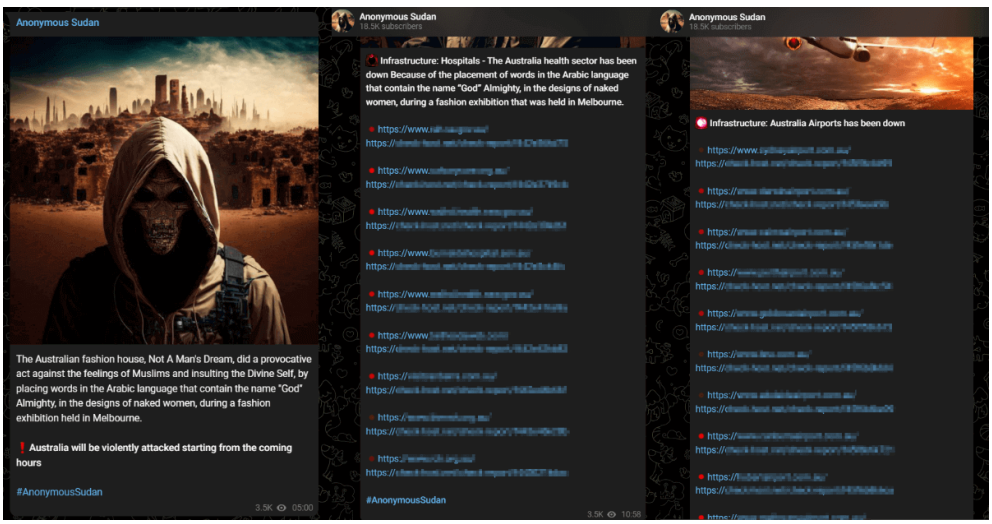
The company posted in a statement about the breach that the stolen data included:

- approximately 7.9 million Australian and New Zealand driver's licenses number
- approximately 53,000 passport numbers
- 100 customers' monthly financial statement
- approximately 6.1 million records dating back to at least 2005

#OpAustralia

Australia faced a campaign in March because of some clothing displayed at the Melbourne Fashion Festival. On March 24, Anonymous Sudan shared a post on their Telegram channel that expressed anger towards the Festival and threatened to launch cyber-attacks against Australia. Following the announcement on Telegram, various Australian organizations, including hospitals, universities, and airports, have been targeted by cyber-attacks.

Also, Australia has reported receiving cyber-attacks from around 38 malicious groups from different regions.



Anonymous Sudan's announcement of a cyber-attack on Australia

Timeline of Significant Cybersecurity Incidents in Australia

Warning Over Tax Season Phishing Scams

The Australian Taxation Office (ATO) shared a warning about a significant increase in SMS and e-mail scams. Scammers are impersonating the ATO, encouraging people to click on fraudulent links. The ATO emphasizes that it never sends SMS or e-mails with links to log into online services.

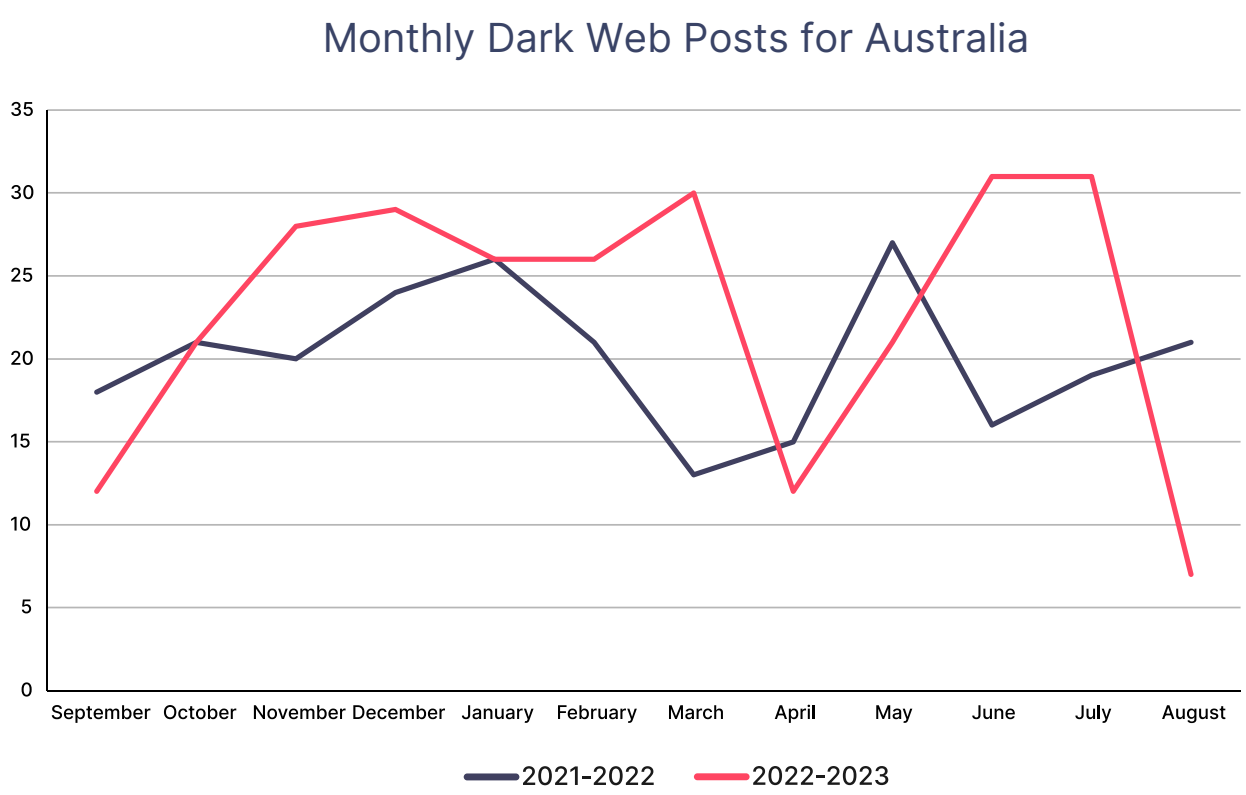
Australian Taxation Office X (Formerly known as Twitter) announcement

Dark Web Radar: A Deep Dive into Australia-Related Activities

Monthly Posts

Within the report's time scope, **274** dark web posts associated with Australia were detected. Compared to the previous 12 months, in which **241** dark web posts were detected, it is seen that malicious activities targeting Australia on underground platforms have increased.

The graph below illustrates the monthly distribution of the detected dark web posts.



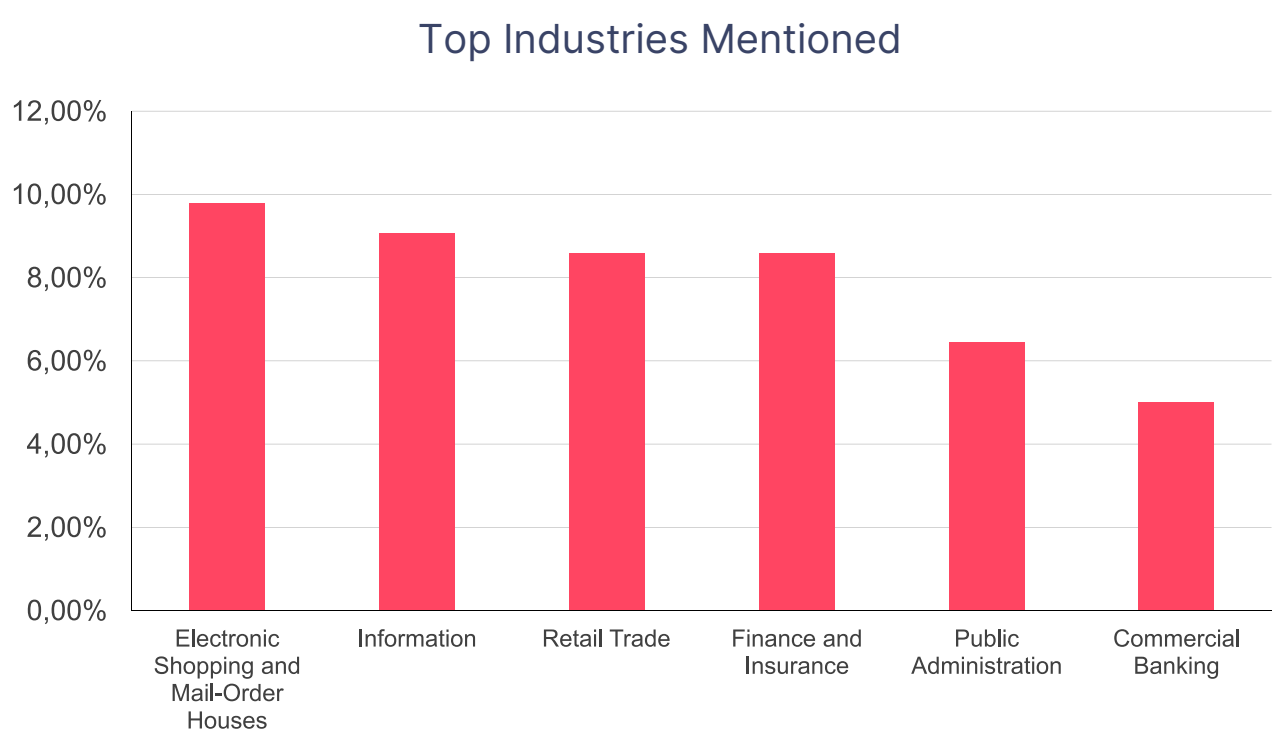
Dark Web Radar: A Deep Dive into Australia-Related Activities

Top Targeted Industries on Dark Web

Based on the analysis of Australia-related dark web posts by industries;

"Electronic Shopping and Mail-Order Houses" is the most frequently mentioned industry, with a rate of **9.79%** of all posts. "Information" is a close second at **9.07%**. "Retail Trade" and "Finance and Insurance" both represent **8.59%,** "Public Administration" mentions **6.44%,** and "Commercial Banking" mentions **5.01%** of posts.

These outputs highlight the most attractive and potentially vulnerable industries on the dark web.

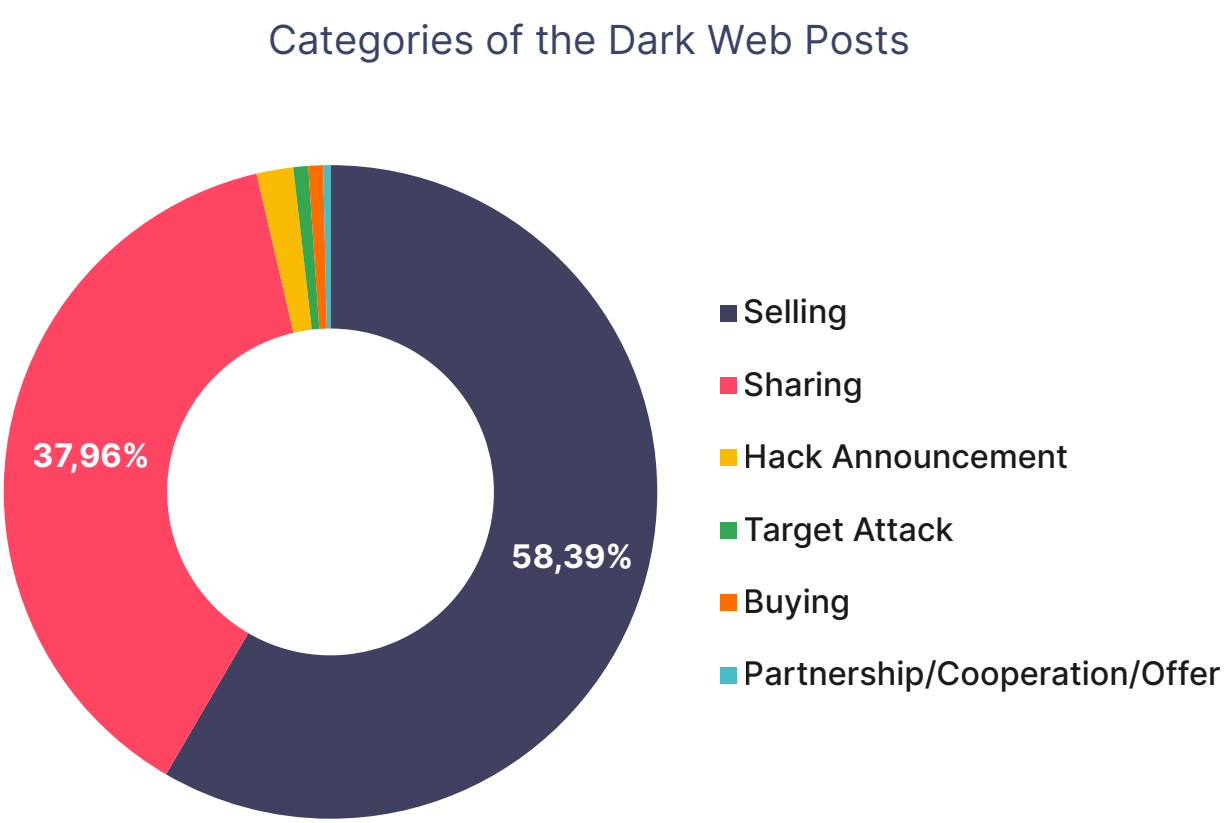


Dark Web Radar: A Deep Dive into Australia-Related Activities

Categories of Posts

Based on the analysis of Australia-related dark web posts by their categories;

Most posts, at **58.39%,** revolve around Sharing (data for free), with Selling (data for sale) following closely at **37.96%.** Other topics like Hack Announcements, Buying, Target Attacks, and Partnership/Cooperation/Offer are significantly less common, with a total **3.65%** rate, showing that the bulk of these posts focused on information exchange or transactional purposes.

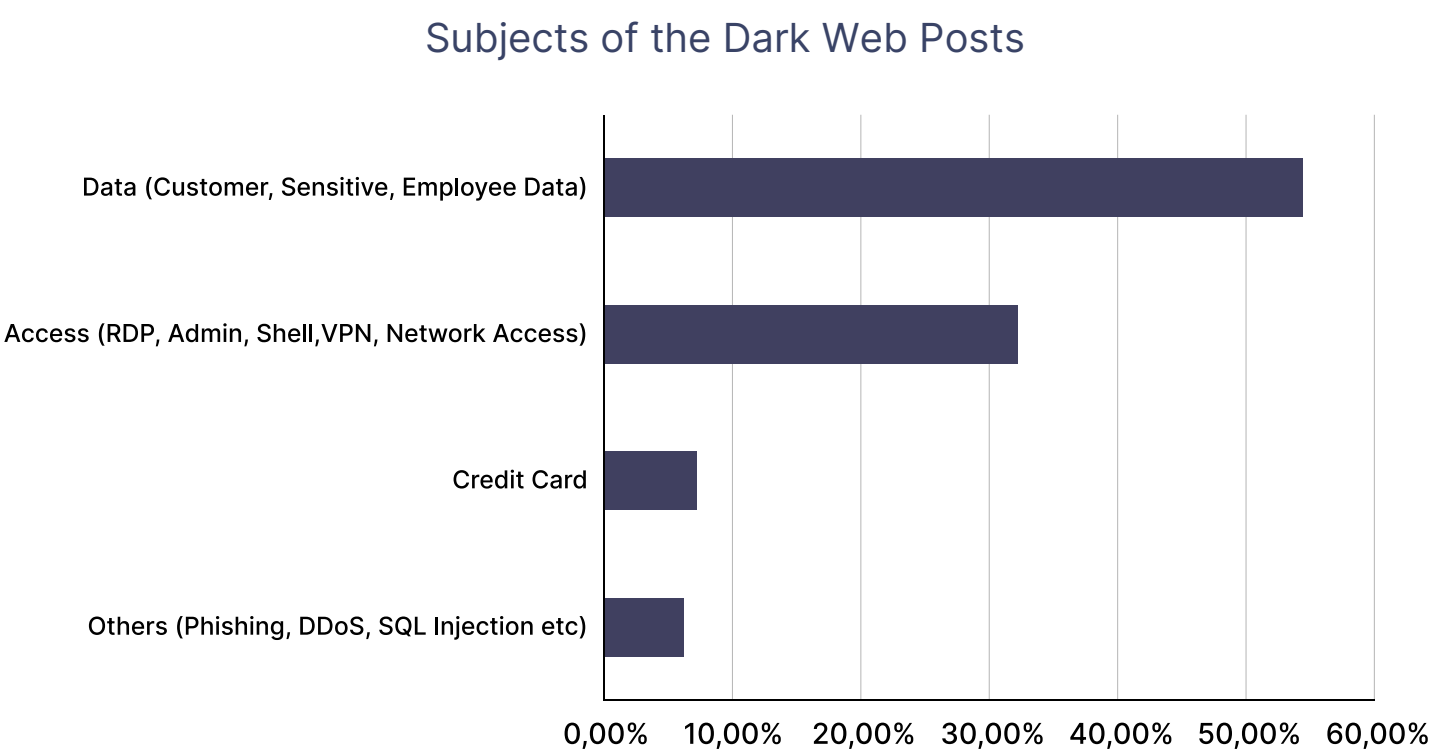


Dark Web Radar: A Deep Dive into Australia-Related Activities

Subjects of Posts

Based on the analysis of Australia-related dark web posts by their subject matter;

Over **50%** of the posts allege data/database leak that contains customer, employee, and sensitive data. More than **30%** of the posts include access details for the Admin portal, RDP, VPN, Shell, and Network, which can be used during the initial stages of a cyber-attack. So they give valuable insights into future cyber-attacks.



Dark Web Radar: A Deep Dive into Australia-Related Activities

Post Authors

It was observed that **274** dark web posts were distributed among **201** unique post owners. Consequently, even the most active post owner's contribution does not surpass 2%. Within this context, it's evident that there hasn't been any post author specifically targeting Australia.

Recent Events

Sep 11
2023

Unauthorized Admin Access Sale is Detected for an Australian E-Commerce Company

In a hacker forum monitored by SOCRadar, an unauthorized admin access sale is detected allegedly belongs to an e-commerce company that operates in Australia

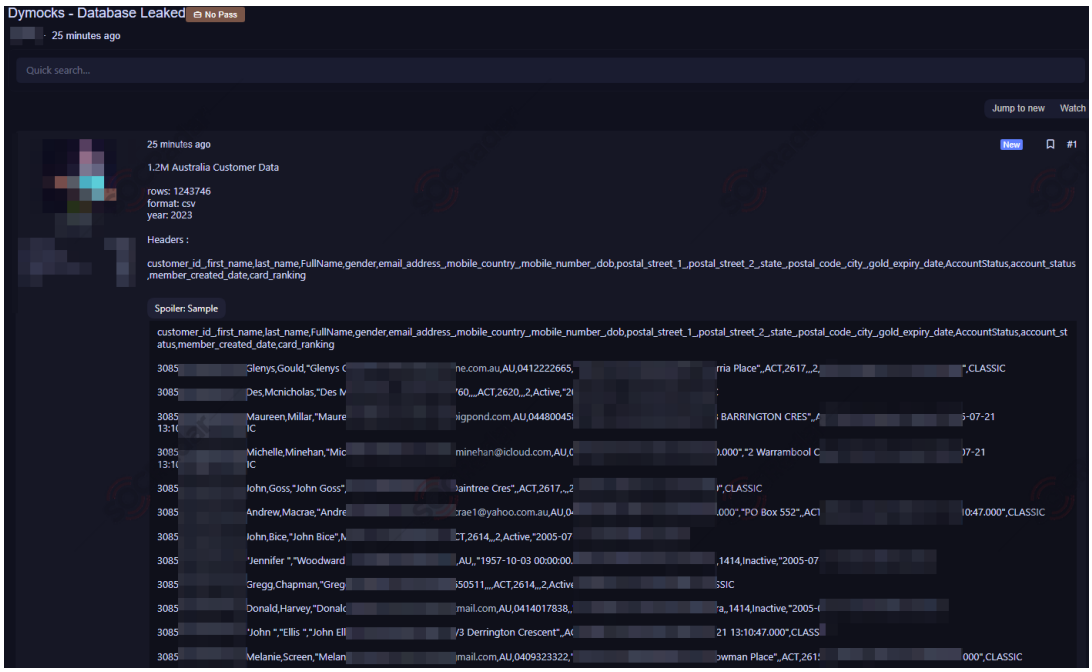
Dark Web Radar: A Deep Dive into Australia-Related Activities

Recent Events

Sep 8 2023

Database of Dymocks is Leaked

In a hacker forum monitored by SOCRadar, a new alleged database leak is detected for Dymocks (1.2M Australia Customer Data)



Sep 8 2023

Unauthorized RDP Access Sale is Detected for an Australian Company

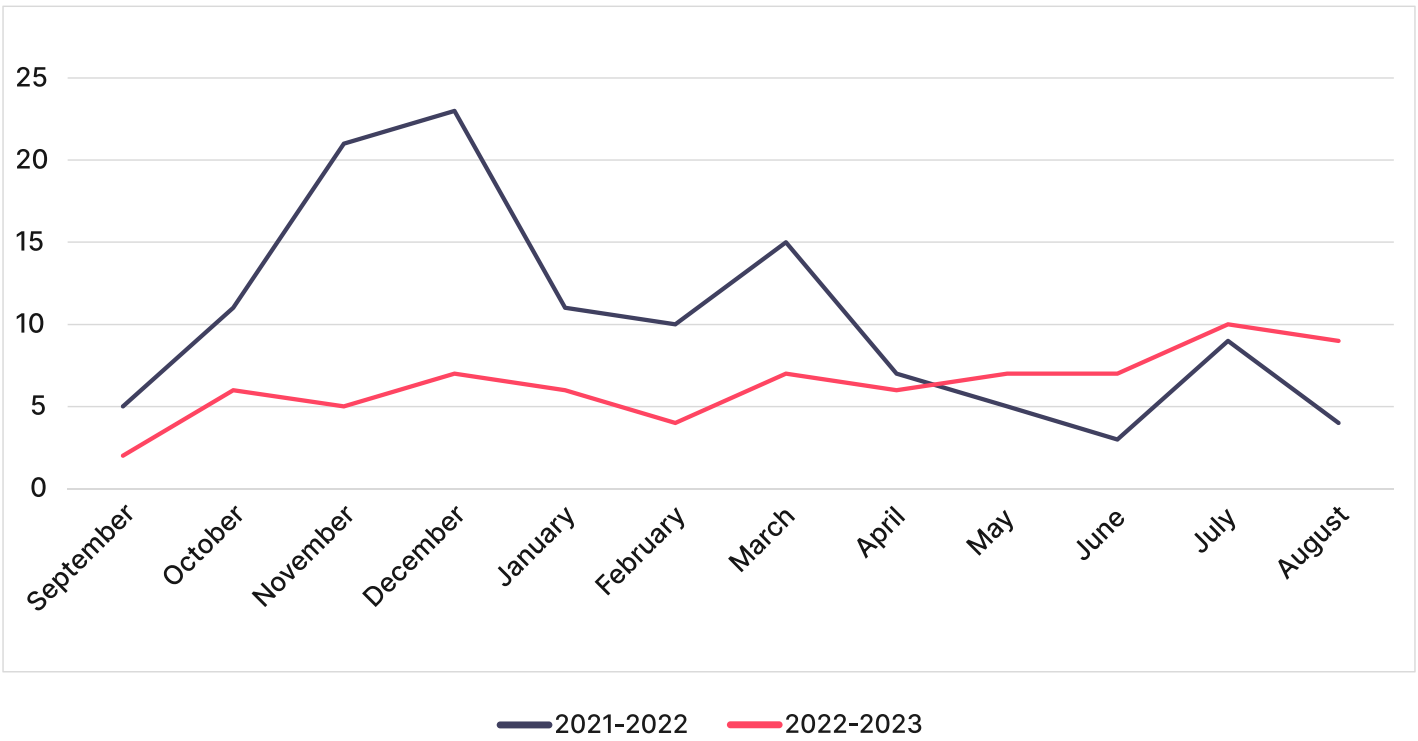
In a hacker forum monitored by SOCRadar, an unauthorized RDP access sale is detected that allegedly belongs to a company that operates in Australia.

Analyzing Ransomware Threat Landscape of Australian Organizations

Trends in Ransomware Attacks

Within the report's time scope, **76** ransomware incidents targeting Australia were detected. Compared to the previous 12 months, in which **124** ransomware incidents were detected, it is seen that Australia's appeal has significantly decreased **(38.7%)** in the ransomware ecosystem.

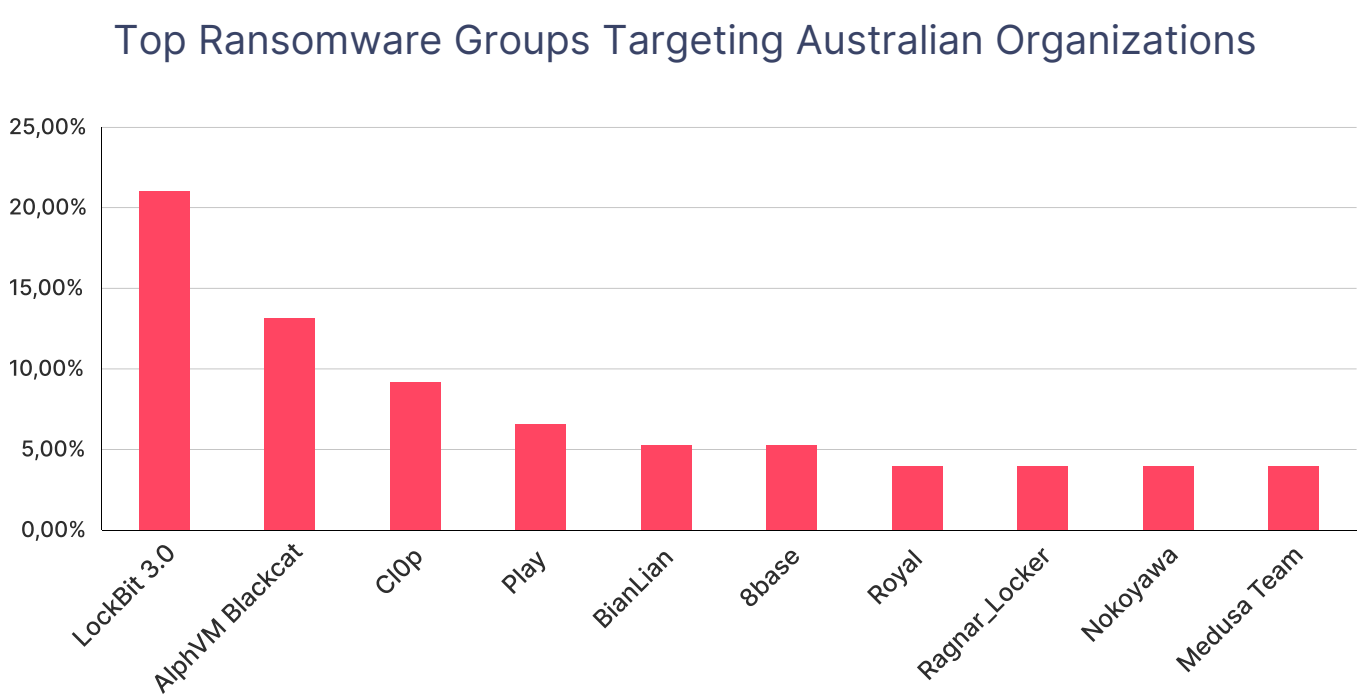
The graph below illustrates the monthly distribution of the ransomware incidents.



Analyzing Ransomware Threat Landscape of Australian Organizations

Prominent Ransomware Groups

22 ransomware groups targeting Australian organizations were observed during the report time scope. The well-known ransomware group "LockBit" accounts for **21.05%** of detected ransomware attacks. "AlphVM / Blackcat" contributed **13.16%**, "Cl0p" **9.21%,** and "Play" **6.58%.**

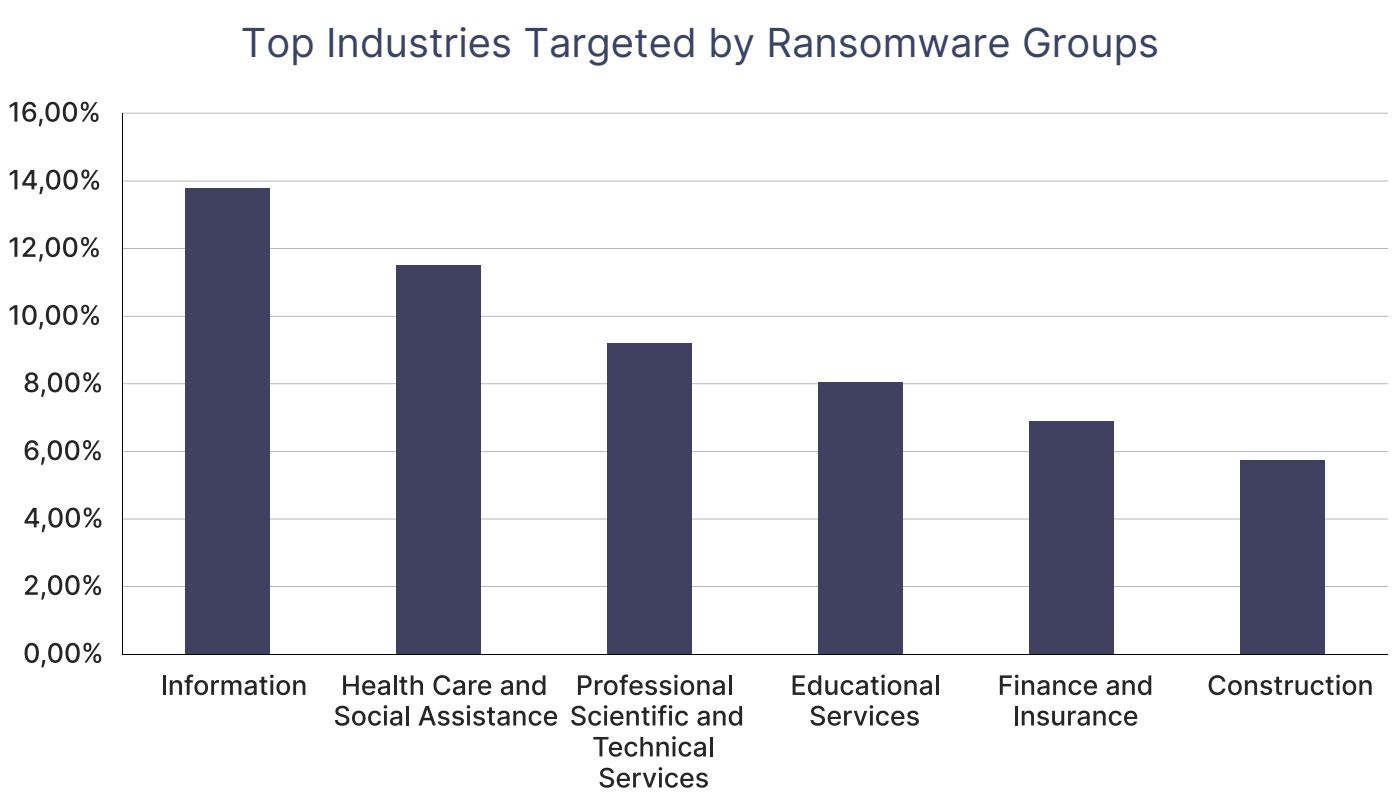


Analyzing Ransomware Threat Landscape of Australian Organizations

Industries Under Siege

Based on the analysis of Australia-related ransomware incidents by industries;

''Information'' was the most frequently targeted industry, with **16.7%** of all posts. ''Health Care and Social Assistance'' followed by **11.49%,** 'The Professional, Scientific, and Technical Services' at **9.20%,** with ''Educational Services'' at **8.05%** of the posts.

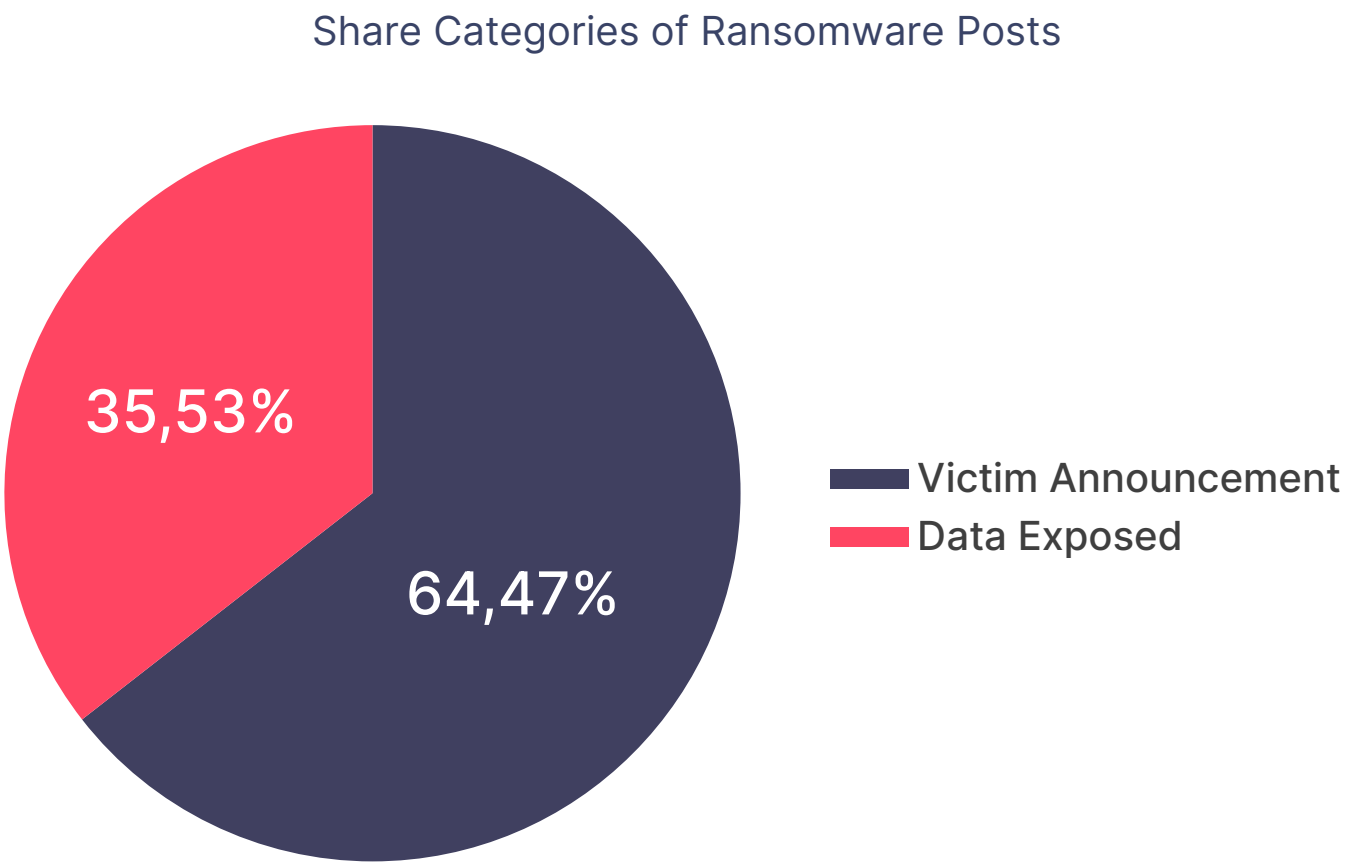


Analyzing Ransomware Threat Landscape of Australian Organizations

Categorizing Ransomware Posts

Based on the analysis of Australia-related ransomware posts by their categories;

The majority of the posts, **64.47%,** were Victim Announcements, while Data Exposed posts constituted **35.53%.** Many of these attacks are announced through shares on ransomware groups' own blogs and leak sites, highlighting the critical role of monitoring such platforms for early threat detection.



Analyzing Ransomware Threat Landscape of Australian Organizations

Recent Events

Sep 10 2023

The New Ransomware Victim of Rhysida: Core Desktop

In the Rhysida ransomware group website monitored by SOCRadar, a new ransomware victim allegedly announced as Core Desktop.

Sep 6 2023

The New Ransomware Victim of Akira: Energy One

In the Akira ransomware group website monitored by SOCRadar, a new ransomware victim was allegedly announced as Energy One.

date	title	content
2023-09-06	Energy One	Energy One Limited provides various software products and services to wholesale energy, environmental, and carbon trading markets in the Asia-Pacific, the United Kingdom, and Europe. The company will provide you all with its 77GB data where you will find information on their projects with big business names, financial documents, contracts, and HR information as well.

Sep 5 2023

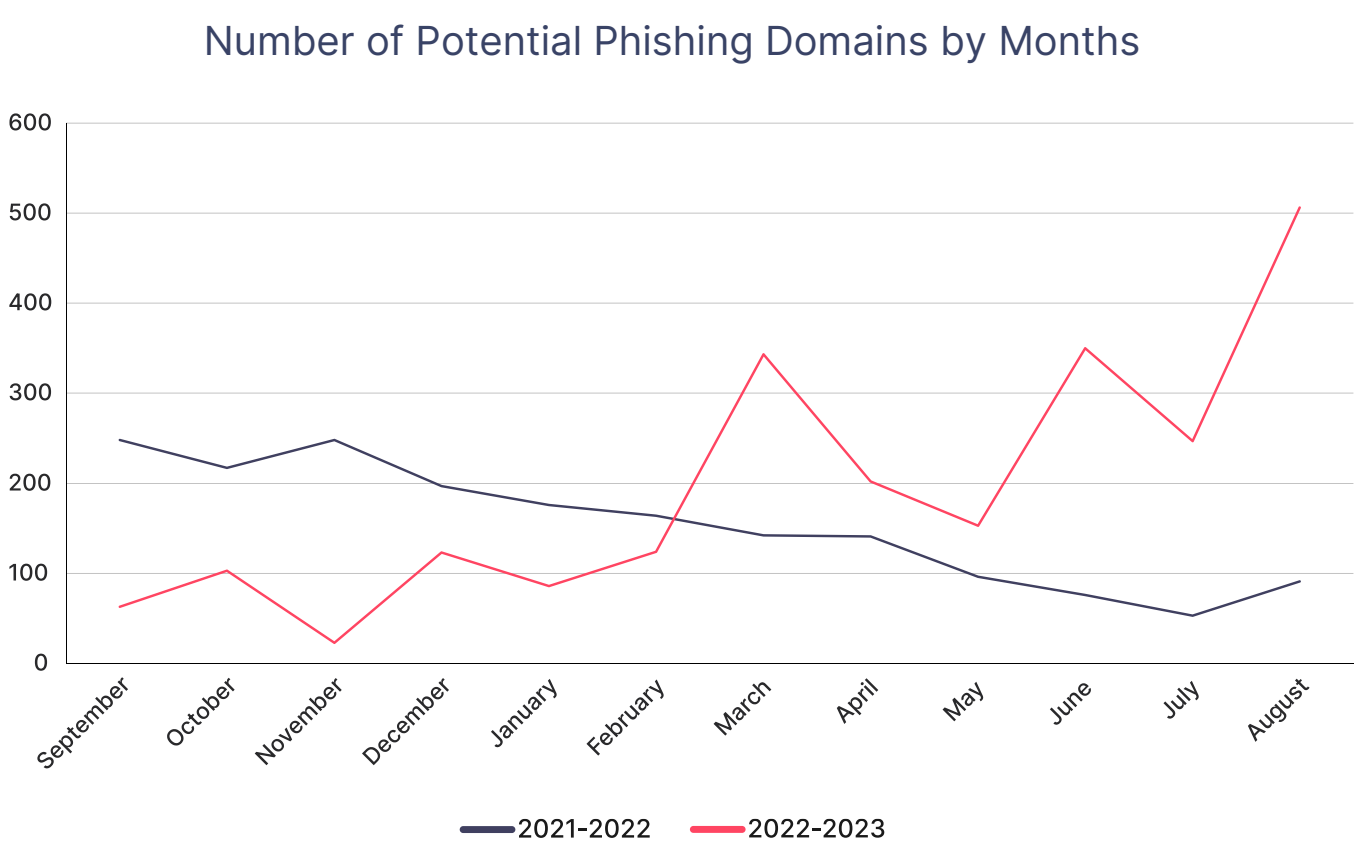
Cactus Ransomware Group Leaked of MINEMAN Systems

In the Cactus ransomware group website monitored by SOCRadar, new data leaks detected allegedly belong to MINEMAN Systems.

Deceptive Domains: Unpacking the Phishing Threats against Australian Organizations

Escalation in Phishing Domain Registrations

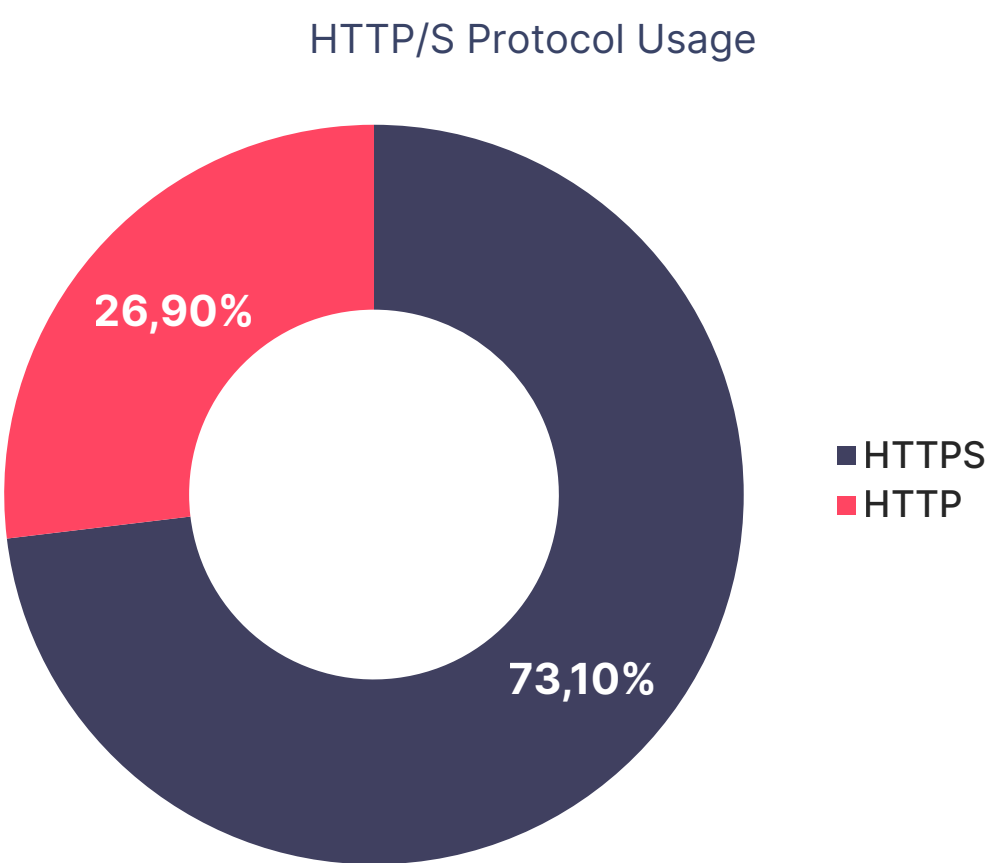
From September 2022 to August 2023, 2,323 potential phishing domains impersonating Australian organizations were listed on the SOCRadar XTI platform. In the previous 12-month term, a total of 1,849 domains were recorded. The threat is substantial, as evident in the increase of potential phishing domains.



Deceptive Domains: Unpacking the Phishing Threats against Australian Organizations

Misuse of SSL/TLS Protocols by Phishing Domains

Analysis of the usage of SSL/TLS protocols by the potential phishing domains, emerges a concerning trend. A significant **73.10%** of these domains used HTTPS, while the remaining **26.90%** opted for HTTP. It's important to note that threat actors often misuse HTTPS to lend a false sense of security to their potential victims. The presence of the padlock icon next to the website address can deceive users into believing that the website is secure and authentic, making them more likely to share sensitive data.



Deceptive Domains: Unpacking the Phishing Threats against Australian Organizations

Recent Events

May 29
2023

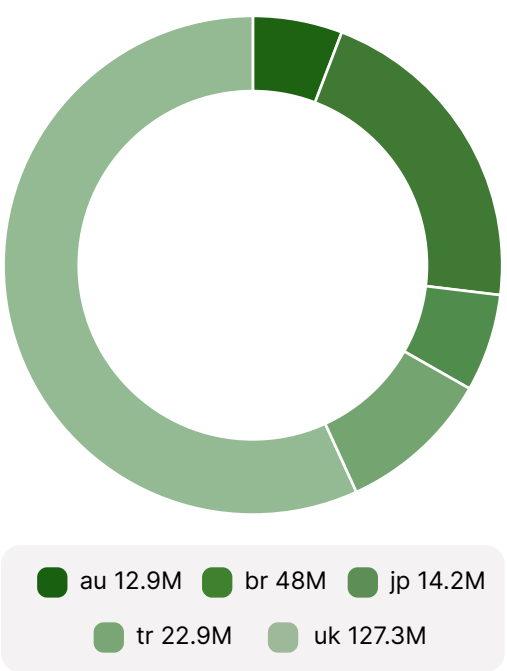
Phishing Page Sale is Detected for the Westnet

In a hacker Telegram channel monitored by SOCRadar, a new phishing page sale is detected for Westnet, an Australian telecommunication company.

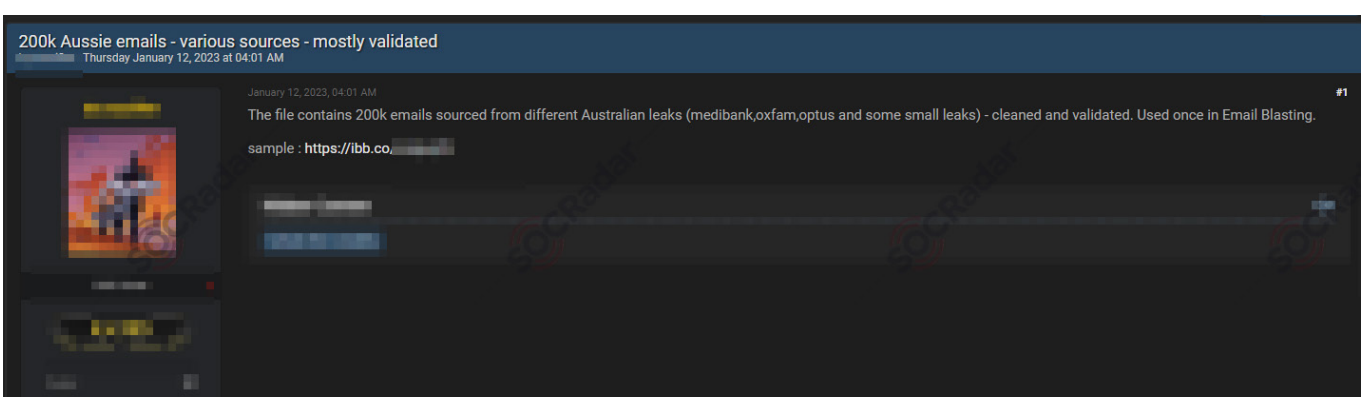
A Deep Dive into Data Breaches: Australian Government's Response

Data breaches have been more prevalent in recent years in Australia. There is a concerning rise in cyber-attacks against the country's critical infrastructure, such as healthcare,telecommunication, and finance, and massive data breaches due to them. Australia (au) is in fifth place among the Most Frequent E-mail Domain Countries on the SOCRadar XTI Platform breach data set.

SOCRadar XTI Platform: Most Frequent E-mail Domain Countries



Those massive data breaches affected millions of Australians and significantly impacted the country's cyber security landscape. Breaches also resulted in millions of Australians' personal information being published on the dark web; many people were concerned about privacy and security.



Alleged database leak from different Australian leaks (Medibank,Oxfam,Optus and some small leaks)

A Deep Dive into Data Breaches: Australian Government's Response

The Optus, Medibank, and Latitude breaches, which occurred one after the other in a short period of 6 months and were the most significant data breaches in Australian history, prompted the government to take action.

At the end of 2022, the Australian Parliament passed key privacy reforms under the Privacy Legislation Amendment. The Australian Government has announced, introduced, and delivered legislation in just over a month. According to The Privacy Legislation Amendment, the civil penalty will increase from $2.2 million to the greater of the following:

- A $50 million;
- 30% of adjusted turnover for the period;
- Three times the financial gain of the misuse of data.

Australia's Security of Critical Infrastructure Act 2018 (SOCI Act) was updated, and the revised SOCI Act became effective on February 17, 2023. The new critical infrastructure definition expands the scope of previously established critical infrastructure sectors and identifies 'data storage and process' as one of the 11 critical infrastructure sectors.

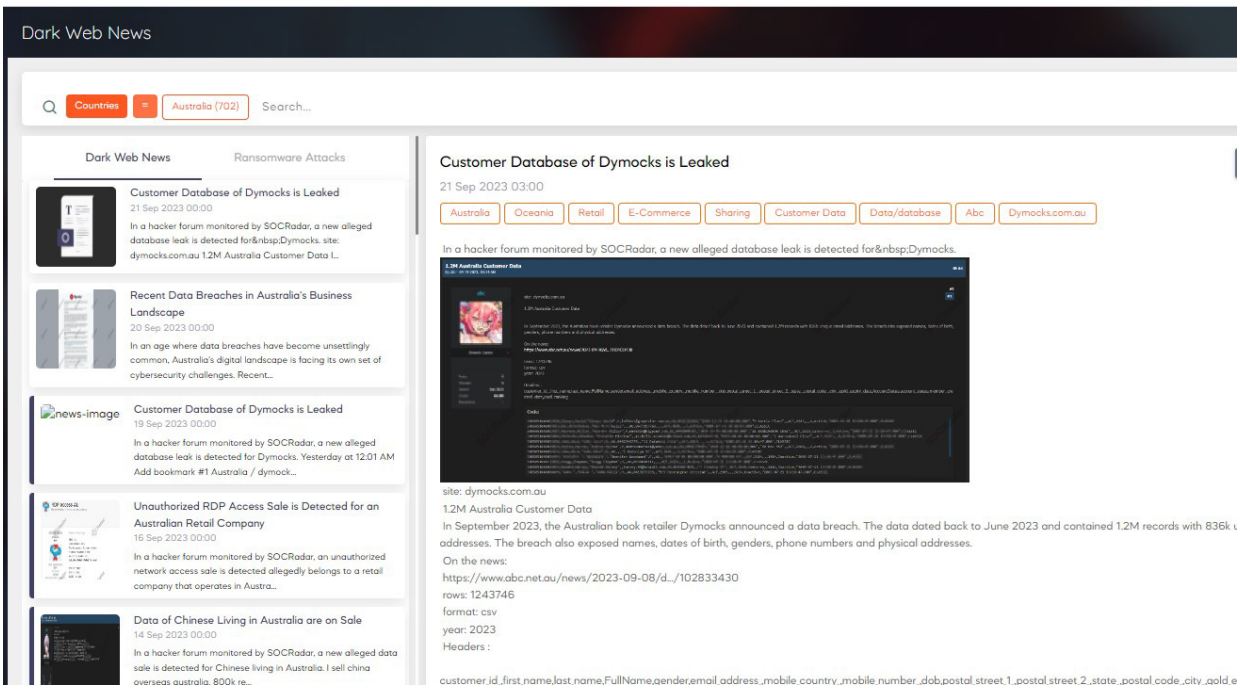
In December 2022, Australia's cyber security authority announced the establishment of the 2023-2030 Australian Cyber Security Strategy, which will help the government realize its vision of making Australia the most cyber-secure nation in the world by 2030. In February 2023, Australia released a discussion paper seeking views on how the government can reach its opinions on how the 2023–2030 Australian Cyber Security Strategy can help the government realize its objectives under the 2023-2030 Australian Cyber Security Strategy.

Lessons Learned: Key Takeaways and Strategic Recommendations

Australian organizations' cyber threat landscape is constantly evolving and becoming more sophisticated. In such circumstances, it is essential to learn from the analyzed threat landscape and to develop strategic roadmaps based on these insights. This is crucial for enhancing resilience levels and safeguarding operational integrity. Here are five key outcomes from SOCRadar analysis:

1. Maintain awareness of the evolving cyber threat landscape

The increased number of posts about Australia on the dark web shows that the cyber threat landscape is rapidly expanding. Organizations need to stay on top of these changes to have proactive measures on their security plans as necessary. Businesses can access real-time data on new threats from the dark web using SOCRadar XTI's Dark Web News module, keeping them one step ahead of cybercriminals.

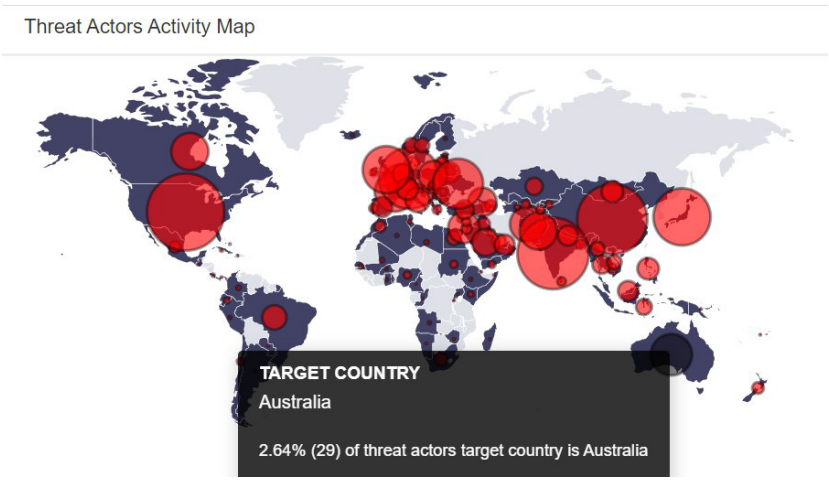


SOCRadar XTI platform Dark Web News Module

Lessons Learned: Key Takeaways and Strategic Recommendations

2. Focus Extended Threat Intelligence Solutions

Many threat actors target almost all industries in Australia with the numerous TTPs they use. In such a comprehensive threat environment, an extended threat intelligence solution that can provide a wide range of services, from detecting threat actors targeting your region, country, and industry and their TTPs to discovering digital assets and exploitable vulnerabilities within your organization, can be beneficial. SOCRadar XTI offers comprehensive contextual and actionable intelligence with External Attack Surface Management, Digital Risk Protection and Cyber Threat Intelligence solutions.

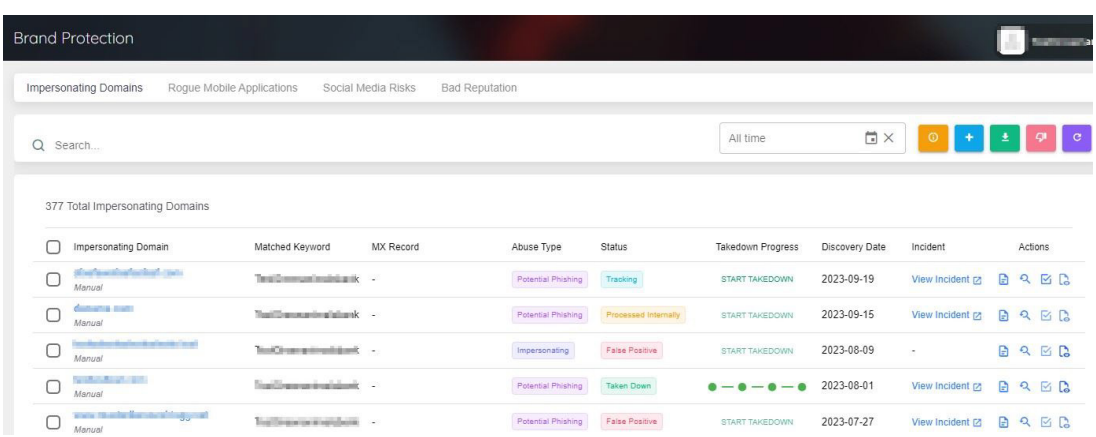


SOCRadar XTI Platform Threat Actor/Malware Module

Additionally, SOCRadar's XTI solutions can guide in identifying potential phishing domains and raising awareness of the latest phishing tactics. Also, against the phishing attempts, SOCRadar provides takedown capabilities in four distinct areas:

- Impersonating Domain Takedown
- Impersonating Social Media Account Takedown
- Rogue Mobil Application Takedown
- GitHub Repository (Critical Data) Takedown

The takedown process can be triggered easily by clicking the ''Start Takedown'' button placed on the takedown Progress column under the 'Brand Protection' and ''Surface Web Monitoring'' modules.



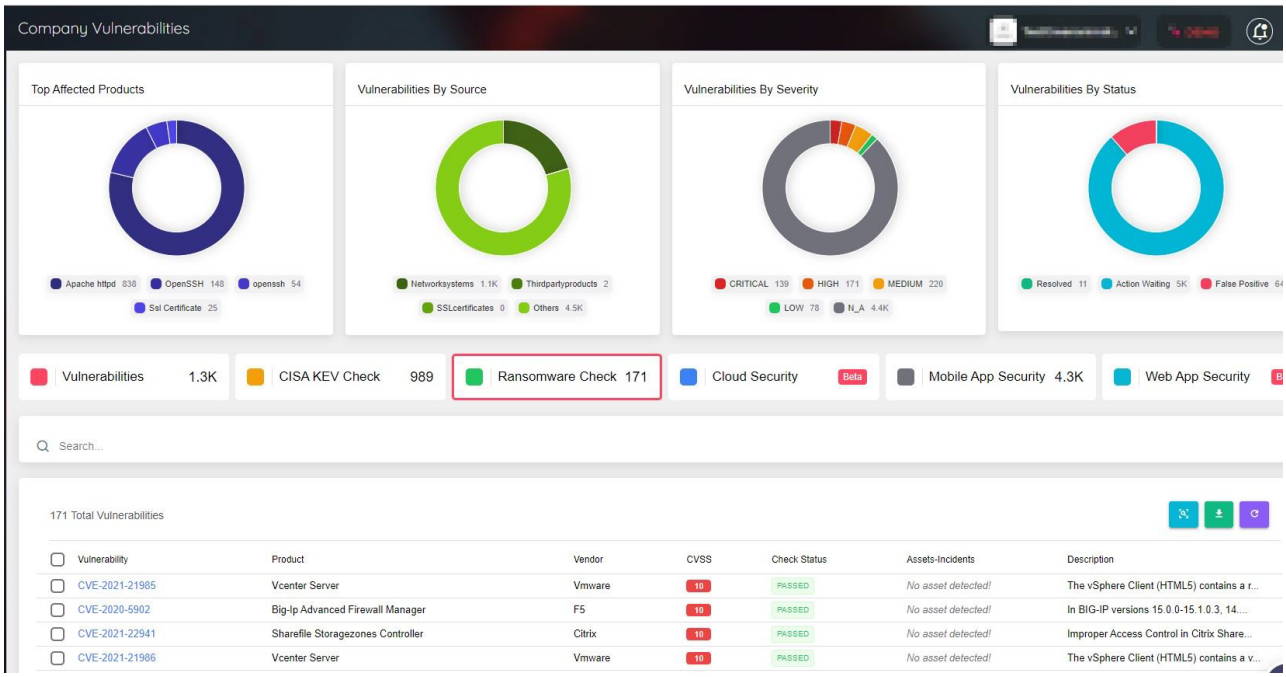
SOCRadarXTI Platform provides takedown process request just one click

Lessons Learned: Key Takeaways and Strategic Recommendations

3. Stay vigilant against ransomware

Ransomware is still a severe threat to Australia, as is the rest of the world. It's crucial to have strong security measures and a strong reaction strategy against ransomware attacks. SOCRadar XTI can guide businesses to identify potential ransomware threats and develop an effective response plan.

Knowing the vulnerabilities that ransomware groups often exploit and being prepared for them is one of the primary methods against ransomware attacks. SOCRadar XTI platform scans all the external assets considering the vulnerabilities most commonly used by ransomware groups via the 'Ransomware Check' feature under the 'Company Vulnerabilities' module.



SOCRadar XTI Company Vulnerabilities Module, Ransomware Check Feature

Who is SOCRadar®?

Your Eyes Beyond

As an Extended Threat Intelligence (XTI) platform and inventor of the concept, SOCRadar's approach effectively integrates Threat Intelligence, Digital Risk Protection, and External Attack Surface Management (EASM). Adapting proactive security with a hacker mindset, we aim to help security teams to detect blindspots before attackers.

The shortage of cybersecurity experts is a growing problem worldwide. All companies around the world must use resources efficiently to provide adequate cyber security with their limited resources. Automated security solutions offer precisely the opportunity that corporations are looking for. With its AI-powered automation technology. **With providing protection against threats for more than 12.000+ companies from 157 countries, SOCRadar has become an extension of SOC teams from every industry.**

SOCRadar provides extended cyber threat intelligence (XTI) that combines: **"Cyber Threat Intelligence, Digital Risk Protection, and External Attack Surface Management Services."** SOCRadar provides the actionable and timely intelligence context you need to manage the risks in the transformation era.

12.000
Free Users

Dark Web Monitoring: SOCRadar's fusion of its unique dark web recon technology with the human analyst eye further provides in-depth insights into financially-targeted APT groups and the threat landscape.

Protecting Customers' PII: Scan millions of data points on the surface, deep and dark web to accurately identify the leakage of your customers' Personally Identifiable Information (PII) in compliance with regulations.

Credit Card Monitoring: Enhance your fraud detection mechanisms with automation speed by identifying stolen credit card data on popular global black markets, carding forums, social channels, and chatters.

360-Degree Visibility: Achieve digital resilience by maintaining internet-facing digital asset inventory. Significantly accelerate this process by automated discovery, mapping, and continuous asset monitoring.

GET ACCESS 12 MONTHS FOR FREE

Gartner Peer Insights™ 4.9/5

Contact Us info@socradar.io +1 (571) 249-4598 651 N Broad St, Suite 205, Middletown, DE 19709