# COS30015 IT Security

## Week 12

**Presented by Dr Rory Coulter**

23 October 2024

# Acknowledgement of Country

We respectfully acknowledge the Wurundjeri People of the Kulin Nation, who are the Traditional Owners of the land on which Swinburne's Australian campuses are located in Melbourne's east and outer-east, and pay our respect to their Elders past, present and emerging.

We are honoured to recognise our connection to Wurundjeri Country, history, culture, and spirituality through these locations, and strive to ensure that we operate in a manner that respects and honours the Elders and Ancestors of these lands.

We also respectfully acknowledge Swinburne's Aboriginal and Torres Strait Islander staff, students, alumni, partners and visitors.

We also acknowledge and respect the Traditional Owners of lands across Australia, their Elders, Ancestors, cultures, and heritage, and recognise the continuing sovereignties of all Aboriginal and Torres Strait Islander Nations.

# 12 Week Recap

**Our journey across the semester, considering it’s a snapshot**

- Fundamental Concepts of Cyber Security
- Offensive and Defensive Security
- System and Converged Security
- Web, Cloud and Network Security (Distributed Applications)
- Malware and Vulnerabilities
- Digital Forensics and Incident Response
- Cryptography
- Human Factors in Cyber Security
- Cyber Law and Risk
- Privacy and Ethics in Cyber Security
- Emerging Trends in Cyber Security

# 12 Week Recap

## Unit Learning Outcomes

Evaluate security of client and server computer

Plan security audits

Critically analyse the concepts of social engineering and physical security

Use a variety of security-related tools to identify attacks and mitigate attacks

Evaluate authentication and encryption systems

Research issues in IT Security

# 12 Week Recap

## Graduate Outcomes

Communication skills

Teamwork skills

Digital Literacies

# 12 Week Recap

## Thank you

- ★ Yicun Tian ★
- Tutoring team
- Prof Jun Zhang
- Students

# Assignment 2

# Emerging Trends in Cyber Security

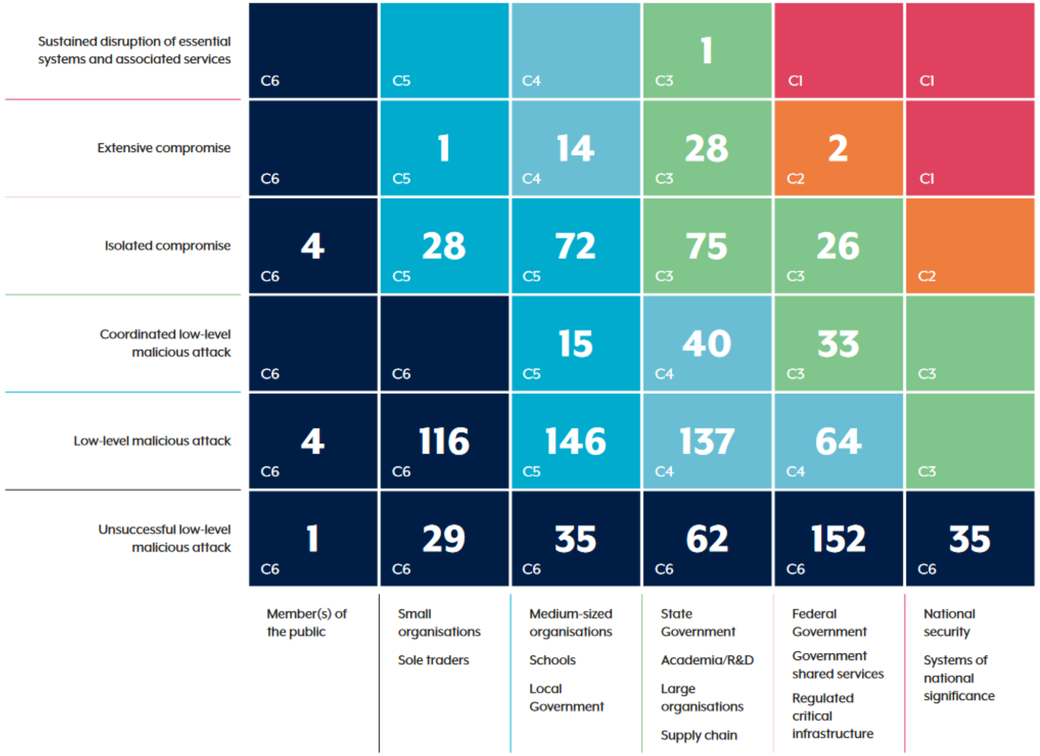
# Threat Landscape

SWINBURNE UNIVERSITY OF TECHNOLOGY

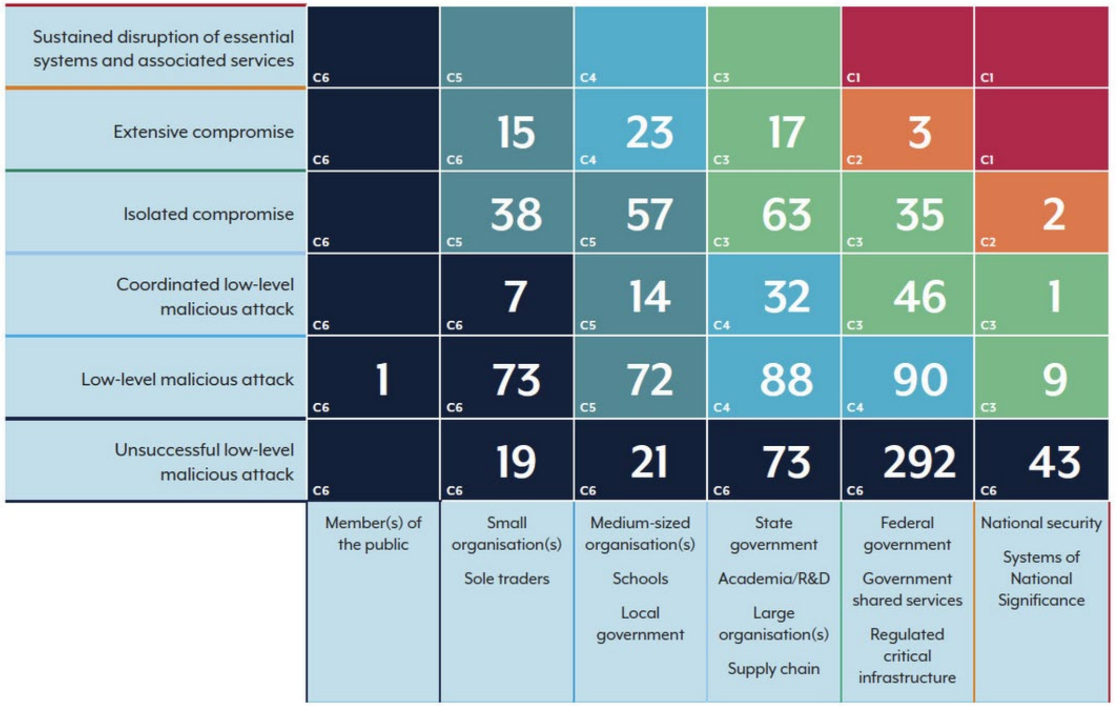
# Incident Severity

**Threats, motivations and TTPs are ever evolving and the attack(s) continuous**

2021 – 2022 & 2022 – 2023 (Its well assumed threats keep continuing to rise)



| | Member(s) of the public | Small organisations<br>Sole traders | Medium-sized organisations<br>Schools<br>Local Government | State Government<br>Academia/R&D<br>Large organisations<br>Supply chain | Federal Government<br>Government shared services<br>Regulated critical infrastructure | National security<br>Systems of national significance |
|---|---|---|---|---|---|---|
| Sustained disruption of essential systems and associated services | C6 | C5 | C4 | 1<br>C3 | C1 | C1 |
| Extensive compromise | C6 | 1<br>C5 | 14<br>C4 | 28<br>C3 | 2<br>C2 | C1 |
| Isolated compromise | 4<br>C6 | 28<br>C5 | 72<br>C5 | 75<br>C3 | 26<br>C3 | C2 |
| Coordinated low-level malicious attack | C6 | C6 | 15<br>C5 | 40<br>C4 | 33<br>C3 | C3 |
| Low-level malicious attack | 4<br>C6 | 116<br>C6 | 146<br>C5 | 137<br>C4 | 64<br>C4 | C3 |
| Unsuccessful low-level malicious attack | 1<br>C6 | 29<br>C6 | 35<br>C6 | 62<br>C6 | 152<br>C6 | 35<br>C6 |



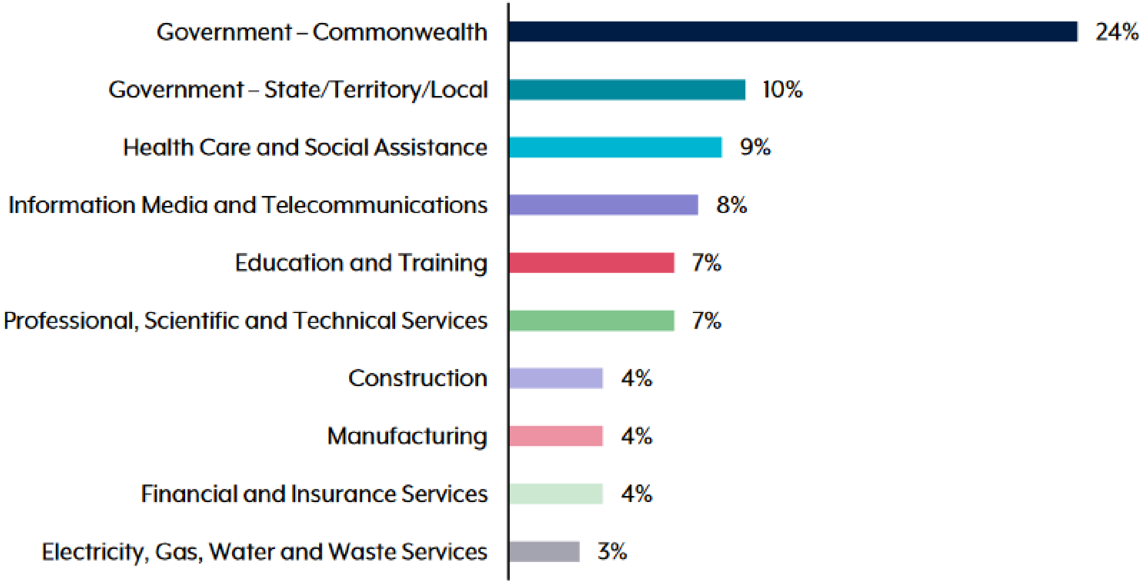
| | Member(s) of the public | Small organisation(s)<br>Sole traders | Medium-sized organisation(s)<br>Schools<br>Local government | State government<br>Academia/R&D<br>Large organisation(s)<br>Supply chain | Federal government<br>Government shared services<br>Regulated critical infrastructure | National security<br>Systems of National Significance |
|---|---|---|---|---|---|---|
| Sustained disruption of essential systems and associated services | C6 | C5 | C4 | C3 | C1 | C1 |
| Extensive compromise | C6 | 15<br>C6 | 23<br>C4 | 17<br>C3 | 3<br>C2 | C1 |
| Isolated compromise | C6 | 38<br>C5 | 57<br>C5 | 63<br>C3 | 35<br>C3 | 2<br>C2 |
| Coordinated low-level malicious attack | C6 | 7<br>C6 | 14<br>C5 | 32<br>C4 | 46<br>C3 | 1<br>C3 |
| Low-level malicious attack | 1<br>C6 | 73<br>C6 | 72<br>C5 | 88<br>C4 | 90<br>C4 | 9<br>C3 |
| Unsuccessful low-level malicious attack | C6 | 19<br>C6 | 21<br>C6 | 73<br>C6 | 292<br>C6 | 43<br>C6 |

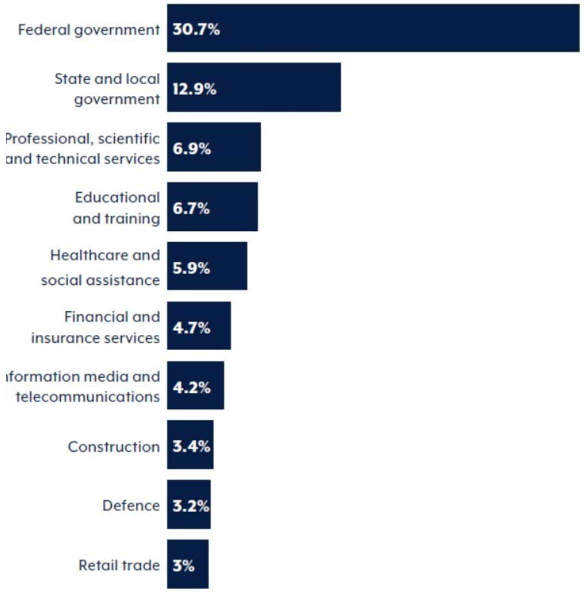
SOURCE: https://www.cyber.gov.au/sites/default/files/2023-03/ACSC-Annual-Cyber-Threat-Report-2022_0.pdf & https://www.cyber.gov.au/about-us/view-all-content/reports-and-statistics/asd-cyber-threat-report-july-2022-june-2023

# Incident Severity

## Threats, motivations and TTPs are ever evolving and the attack(s) continuous

2021 – 2022 & 2022 - 2023

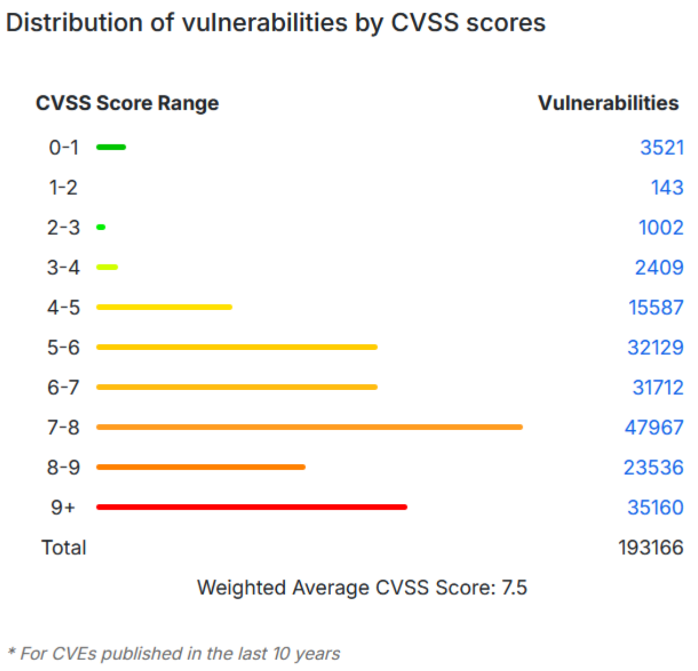




SOURCE: https://www.cyber.gov.au/sites/default/files/2023-03/ACSC-Annual-Cyber-Threat-Report-2022_0.pdf & https://www.cyber.gov.au/about-us/view-all-content/reports-and-statistics/asd-cyber-threat-report-july-2022-june-2023

# Vulnerabilities

**Constant search for zero-day vulnerabilities and establishing an exploit**

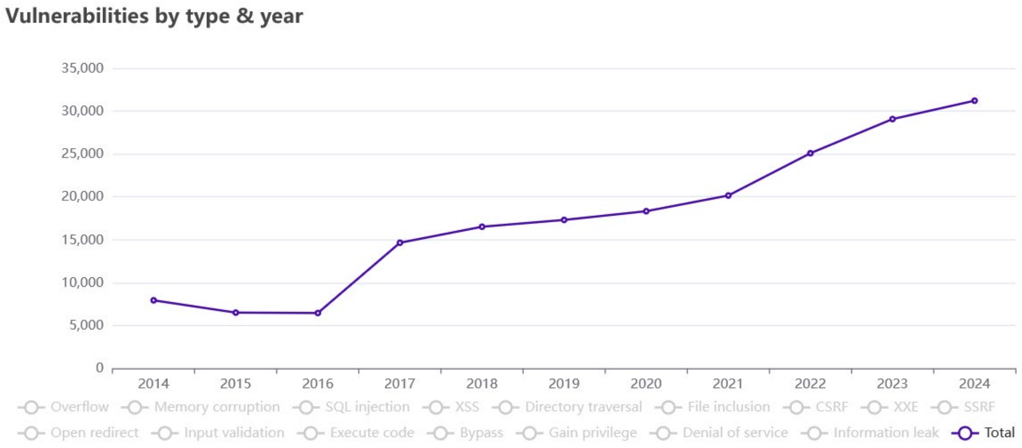


Distribution of vulnerabilities by CVSS scores

| CVSS Score Range | Vulnerabilities |
|---|---|
| 0-1 | 3521 |
| 1-2 | 143 |
| 2-3 | 1002 |
| 3-4 | 2409 |
| 4-5 | 15587 |
| 5-6 | 32129 |
| 6-7 | 31712 |
| 7-8 | 47967 |
| 8-9 | 23536 |
| 9+ | 35160 |
| Total | 193166 |

Weighted Average CVSS Score: 7.5

** For CVEs published in the last 10 years*



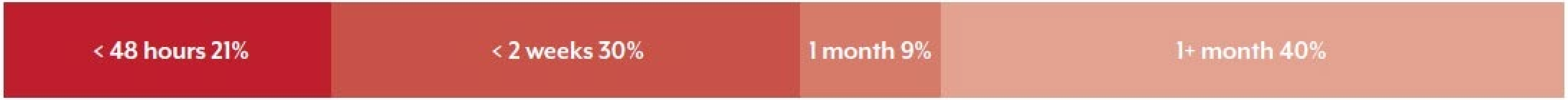
Vulnerabilities by type & year

SOURCE: https://www.cvedetails.com/

# Vulnerabilities

## According to the ACSC’s 2022 – 2023 threat report

- *“1 in 5 vulnerabilities was exploited within 48 hours of a patch or mitigation advice being released”*
- *“half of the vulnerabilities were exploited within 2 weeks of a patch or mitigation advice being released”*
- *“2 in 5 vulnerabilities were exploited more than one month after a patch or mitigation advice was released”*



SOURCE: https://www.cyber.gov.au/sites/default/files/2023-03/ACSC-Annual-Cyber-Threat-Report-2022_0.pdf & https://www.cyber.gov.au/about-us/view-all-content/reports-and-statistics/asd-cyber-threat-report-july-2022-june-2023

# Artificial Intelligence

SWINBURNE UNIVERSITY OF TECHNOLOGY

# Current AI Challenges

## Offensive and Defensive Perspectives

Offensive

- Phishing material
- Deep fake voice and video
- Poisoned datasets
- Write malicious code
- Data privacy (data submitted as a part of a request and in training)

Defensive

- Identify patterns and unique log entries
- Model typical user behaviour or traffic patterns
- Pre-emptive block suspicious behaviour

# Future AI Challenges

## For when offensive or kinetic attacks happen

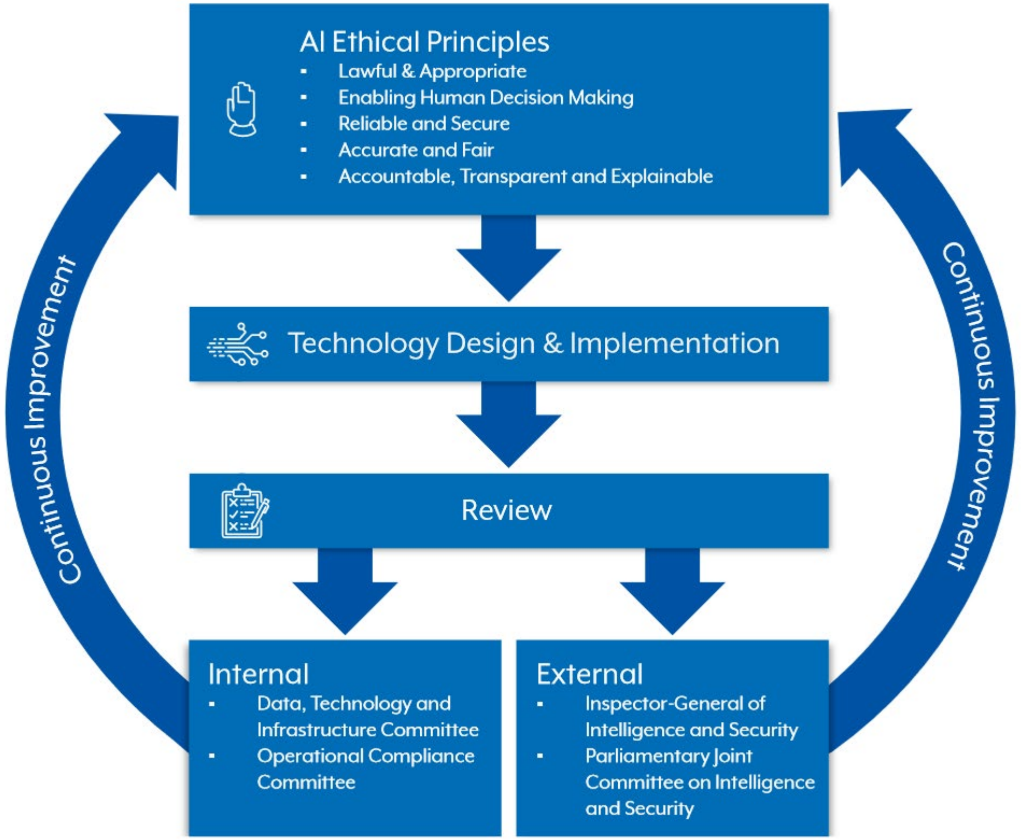
AI models performing attack campaign activities

- Automated access, compromise and objectives fulfilled
- Mis & Disinformation poisoning
- Bulk intelligence processes (and what if the data is wrong to begin with outside of an attack generally)

# Ethical AI

## One of many frameworks

Uniquely from a cyber security perspective



### AI Ethical Principles

- Lawful & Appropriate
- Enabling Human Decision Making
- Reliable and Secure
- Accurate and Fair
- Accountable, Transparent and Explainable

Technology Design & Implementation

Review

### Internal

- Data, Technology and Infrastructure Committee
- Operational Compliance Committee

### External

- Inspector-General of Intelligence and Security
- Parliamentary Joint Committee on Intelligence and Security

Continuous Improvement

Continuous Improvement

SOURCE: https://www.asd.gov.au/sites/default/files/2023-03/Ethical%20AI%20in%20ASD%20Framework.pdf

# TTPs

SWINBURNE UNIVERSITY OF TECHNOLOGY

# Common TTPs

**Spanning multiple incidents, common TTPs observed, but also easily mitigated against**

Covering

- Initial access
- Execution
- Persistence
- Privilege escalation
- Defence evasion
- Credential access
- Discovery
- Lateral movement
- Collection
- Command and control
- Exfiltration
- Impact

SOURCE: https://www.cyber.gov.au/about-us/advisories/summary-tactics-techniques-and-procedures-used-target-australian-networks

# Common TTPs (cont.)

**Spanning multiple incidents, common TTPs observed, but also easily mitigated against**

- Initial access
    - T1190 – Exploit Public-Facing Application
    - T1078 – Valid Accounts
    - T1193 – Spearphishing Attachment
    - T1189 – Drive-by Compromise
- Execution
    - T1059 – Command-Line Interface
    - T1086 – PowerShell
    - T1064 – Scripting
    - T1106 – Execution through API
    - T1204 – User Execution
    - T1504 – PowerShell Profiles
- Persistence
    - T1060 – Registry Run Keys / Startup Folder
    - T1100 – Web Shell
    - T1108 – Redundant Access
    - T1504 – PowerShell Profiles
- Privilege escalation
    - T1068 – Exploitation for Privilege Escalation
- Defence evasion
    - T1099 – Timestomp
    - T1070 – Indicator Removal on Host
    - T1107 – File Deletion
    - T1045 – Software Packing
    - T1158 – Hidden Files and Directories
- Credential access
    - T1003 – Credential Dumping
    - T1056 – Input Capture
    - T1081 – Credentials in Files
    - T1110 – Brute Force

SOURCE: https://www.cyber.gov.au/about-us/advisories/summary-tactics-techniques-and-procedures-used-target-australian-networks

# Common TTPs (cont.)

**Spanning multiple incidents, common TTPs observed, but also easily mitigated against**

- Discovery
    - T1007 – System Service Discovery
    - T1016 – System Network Configuration Discovery
    - T1018 – Remote System Discovery
    - T1033 – System Owner/User Discovery
    - T1046 – Network Service Scanning
    - T1049 – System Network Connections Discovery
    - T1082 – System Information Discovery
    - T1083 – File and Directory Discovery
    - T1087 – Account Discovery
    - T1135 – Network Share Discovery
    - T1482 – Domain Trust Discovery
- Lateral movement
    - T1021 – Remote Services (RDP, SSH)
    - T1077 – Windows Admin Shares
    - T1134 – Access Token Manipulation
    - T1080 – Tainted Shared Content
- Collection
    - T1005 – Data from Local System
    - T1039 – Data from Network Shared Drive
    - T1056 – Input Capture
    - T1074 – Data Staged
    - T1114 – Email Collection
    - T1213 – Data from Information Repositories
- Command and control
    - T1071 – Standard Application Layer Protocol

SOURCE: https://www.cyber.gov.au/about-us/advisories/summary-tactics-techniques-and-procedures-used-target-australian-networks

# Common TTPs (cont.)

**Spanning multiple incidents, common TTPs observed, but also easily mitigated against**

- Exfiltration
  - T1002 – Data Compressed
  - T1022 – Data Encrypted
  - T1048 – Exfiltration Over Alternative Protocol
  - T1041 – Exfiltration Over Command and Control (C2) Channel
- Impact
  - T1486 – Data Encrypted for Impact

SOURCE: https://www.cyber.gov.au/about-us/advisories/summary-tactics-techniques-and-procedures-used-target-australian-networks

# Close

SWINBURNE UNIVERSITY OF TECHNOLOGY

# From Here

## Advice

Try Hack Me, Offensive Security, etc.

CTFs

Bug Bounties

Cyber advisories

Meetups

Self-motivated projects

Cyber Security Honours

Masters Degree

Doctor of Philosophy

# Thank You

**COS30015 Academic Team, 2024**