Threat Hunting with Mitre Attack

By

Luekrit Kongkamon

Understanding Adversary Behaviour with MITRE ATT&CK

In cybersecurity, understanding how adversaries operate is crucial for effective defence. The MITRE ATT&CK® (Adversarial Tactics, Techniques, and Common Knowledge) framework can analyse recent cyber incidents affecting Australian universities.

MITRE ATT&CK is a globally recognized, living knowledge base that documents and categorizes the tactics, techniques, and procedures (TTPs) used by adversaries during cyberattacks. Developed and maintained by the MITRE Corporation, it provides a comprehensive framework for understanding how attackers achieve their objectives within a target environment.

Key elements of MITRE ATT&CK include:

- **Tactics (why)** represent the high-level adversarial goals or "why" an attacker might perform a certain action (e.g., Initial Access, Execution, Persistence, Lateral Movement). These are the categories that group specific techniques.
- **Techniques (how)** describe the specific "how" an attacker accomplishes a tactic (e.g., "Phishing" for Initial Access, "Command and Scripting Interpreter" for Execution). Each technique details a particular method of achieving a tactical goal.
- **Sub-techniques** provide more granular detail within a technique, allowing for a more precise understanding of an adversary's operational methods.
- **Procedures:** refer to the real-world observed applications of techniques by specific threat groups or malware, demonstrating how an adversary executes their objectives using specific techniques.

In this project, I applied the MITRE ATT&CK framework to investigate 3 high-profile cyber incidents affecting Australian universities.

Threat Hunting from Australian University Incidents

Background

Australian universities are prime targets for cyberattacks due to their valuable research, intellectual property, and extensive digital infrastructure. This report analyses three major incidents involving the Australian National University (ANU), Western Sydney University (WSU), and Queensland University of Technology (QUT), identifying attack vectors, techniques, impacts, and preventive strategies.

Incident 1: Australian National University (ANU) – Ransomware Attack (2025)

On February 2025, the Australian National University (ANU) was targeted by the notorious FSociety ransomware group. The attackers issued a chilling threat to leak sensitive university data unless a substantial ransom was paid, holding critical information hostage.

- **Initial Access**: The initial access into ANU's systems most likely originated from a sophisticated phishing campaign. This aligns directly with the MITRE ATT&CK technique ***T1566: Phishing***. Adversaries often craft highly convincing emails, sometimes impersonating trusted entities or internal departments, to trick recipients into clicking malicious links or opening infected attachments.
- **Privilege Escalation:** Once a foothold was established, the attackers moved swiftly to gain higher levels of control within the network. This often involves privilege escalation, a crucial step where attackers exploit vulnerabilities or misconfigurations to gain administrative rights.
- **Lateral Movement:** Following this, lateral movement was observed, specifically through Remote Desktop Protocol (RDP). The use of RDP (a common technique under ***T1021.001***: Remote Services: Remote Desktop Protocol) allows attackers to move from one compromised system to another, expanding their reach across the university's extensive digital infrastructure.
- **Execution:** PowerShell was also a key tool in the attack, indicating the use of ***T1059: Command and Scripting Interpreter***, specifically PowerShell, for executing commands, automating tasks, or deploying malicious scripts during various phases of the attack, including potentially for discovery or defence evasion.
- **Exfiltration:** Once deep within the network, the attackers executed their primary objective: data exfiltration and encryption. They infiltrated various systems across the campus, systematically exfiltrating sensitive data over HTTPS. This aligns with techniques under the Exfiltration tactic, such as ***T1041: Exfiltration Over C2 Channel*** or ***T1048: Exfiltration Over Alternative Protocol***, leveraging seemingly legitimate network traffic (HTTPS) to blend in.
- Impact: Finally, the ransomware payload was deployed, leading to the widespread encryption of files across the entire campus. This destructive action directly corresponds to MITRE ATT&CK technique ***T1486: Data Encrypted for Impact***, which falls under the Impact tactic.

The consequences for ANU were severe, resulting in significant operational disruption, widespread inaccessibility of systems, and considerable reputational damage. The full extent of the data exposure remains undisclosed, adding to the long-term implications.

Recommendations

- Email filtering and phishing awareness
- Disable/monitor PowerShell
- Deploy EDR and network segmentation
- Adopt Zero Trust access controls

Incident 2: Western Sydney University (WSU) – Credential Abuse & Data Leak (2023–2025)

Western Sydney University (WSU) experienced a prolonged and stealthy breach between 2023 and 2025, characterized by unauthorized access to its Single Sign-On (SSO) system. This incident highlights the critical vulnerability of identity and access management in large organizations.

- **Initial Access**: The attackers leveraged valid credentials, likely obtained through phishing campaigns targeting staff and students or through the reuse of passwords compromised in other breaches. The use of ***T1078: Valid Accounts*** is a cornerstone of this attack, enabling adversaries to bypass initial authentication layers and gain legitimate-looking access, making detection significantly harder.
- **Discovery:** Once authenticated, the attackers were able to move within WSU's cloud environment. They engaged in ***T1619: Cloud Discovery***, systematically mapping out cloud resources, identifying valuable data repositories, and understanding the cloud infrastructure configuration. This discovery phase is crucial for adversaries to locate their targets and plan their exfiltration strategy.
- **Exfiltration**: The culmination of the breach involved the exfiltration of a massive volume of sensitive data: 580TB of student and staff information. This aligns with ***T1537: Cloud Storage Object Discovery*** and ***T1567: Exfiltration Over Web Service or more broadly***, ***T1537: Cloud Exfiltration*** as cited. The compromised data was subsequently discovered on the dark web, affecting over 10,000 individuals.

Key contributing factors to the breach's long duration and significant impact included weak multi-factor authentication (MFA) enforcement and limited anomaly detection capabilities. Had stronger MFA been universally enforced and suspicious login patterns been actively monitored, the initial access and subsequent unauthorized activity could have been significantly curtailed or prevented

Recommendation

- Enforce MFA on all systems
- Deploy CASB tools
- Monitor SSO login behavior and session reuse
- Conduct periodic identity audits

Incident 3: Queensland University of Technology (QUT) – Ransomware via Print Spooler (2022)

On December 2022, Queensland University of Technology (QUT) suffered a ransomware attack that notably exploited the "PrintNightmare" vulnerability (CVE-2021-34527). This incident underscored the risks associated with unpatched systems and legacy services.

- **Initial Access**: The attack likely began with ***T1190: Exploit Public-Facing Application***, where attackers leveraged the critical PrintNightmare vulnerability on an accessible system. This vulnerability allows for remote code execution, providing the initial foothold into QUT's network.
- **Lateral Movement**: Once inside, attackers engaged in lateral movement, specifically utilizing ***T1021.002: Remote Services: SMB/Windows Admin Shares***. This technique involves using the Server Message Block (SMB) protocol, common for file sharing and network communication in Windows environments, to spread across internal systems. The exploitation of the Print Spooler service facilitated this movement and allowed for the deployment of the ransomware.
- **Impact**: The most visible sign of the attack was printers across the campus automatically printing ransom notes, a direct and impactful manifestation of the attack's final stage. This was followed by the encryption of files, disrupting IT services across the university. This action aligns with ***T1486: Data Encrypted for Impact***, a core technique under the Impact tactic.

The incident caused widespread disruption, affecting over 11,000 users. The exploitation of a known, patchable vulnerability highlights a critical lesson in cybersecurity: consistent and timely patching of systems is paramount.

Recommendations

- Patch management policy for critical CVEs
- Disable legacy services like Print Spooler
- Segment networks and isolate high-value assets

Lesson Learned

Each incident reveals key lessons for the higher education sector.

- The ANU ransomware attack emphasized the need for email security, user behaviour analytics, and endpoint controls to stop advanced persistent threats.
- WSU's credential abuse case illustrated the importance of strong identity and access management, particularly in federated cloud environments.
- QUT’s ransomware outbreak highlighted the risks of unpatched systems and the importance of removing unnecessary legacy services like the Print Spooler from critical infrastructure.

Recommendations for My University IT security Team

To strengthen My University’s cybersecurity posture, it is important to adopt a Zero Trust strategy that verifies every user and device before granting access, regardless of their location.

1. **Adopt Zero Trust Architecture**: Assume breach and verify every connection—user, device, and application.

2. **Enforce MFA Everywhere:** Apply multi-factor authentication to SSO, cloud apps, VPNs, and admin accounts.
3. **Invest in Detection & Response Tools**: Deploy SIEM/XDR for real-time alerts on suspicious login patterns, privilege escalation, and data movement.
4. **Vulnerability & Patch Management:** Automate patch rollout for high CVEs like PrintNightmare. Prioritize critical systems.
5. **Conduct Red Team/Blue Team Simulations:** Regularly test detection and incident response readiness.
6. **Identity Access Reviews:** Regularly audit user permissions and remove excessive privileges.
7. **Cybersecurity Awareness Training:** Mandatory training for staff and students on phishing, social engineering, and password hygiene.
8. **Cloud Security Monitoring with CASB**: Gain visibility into SaaS and cloud activity to prevent unauthorized data exfiltration.

Tools & Frameworks Used

- MITRE ATT&CK Framework
- Threat Intelligence Analysis
- CVE & Vulnerability Research
- Microsoft Defender, SIEM/XDR Concepts, CASB Principles
- Zero Trust Architecture (NIST & Microsoft Guidelines)