BREACH BELOW THE SURFACE: A CYBER ESPIONAGE SIMULATION

BY DIVIJ BHAW

& ORLANDO MORRIS-JOHNSON

Rockingham Kwinana Chamber Of Commerce

ACKNOWLEDGEMENT TO COUNTRY

WHO ARE WE?

Emu Exploit is Australia's leading CTF hacking team, based in Perth and founded in 2021. We excel in cybersecurity challenges and foster community through technical workshops.

TODAY'S PRESENTERS:

Orlando (q3st1on)	Div (</Div>)
• **Professional/Student**	• **Professional/Student**
• **CTF Player**	• **CTF Player**
• **Forklift Certified**	• **Ceramics Expert**

OVERVIEW

1. SETTING THE SCENE: DISCUSSING IMPACTS AND TRENDS
2. INTRODUCING THE ACTORS AND SCENARIO
3. THE HACKERS' OBJECTIVES
4. TECHNICAL DEMO
5. WHAT WENT WRONG
6. ASSESSING THE DAMAGE
7. KEY TAKEAWAYS: PROACTIVE MEASURES

SETTING THE SCENE

CYBER ATTACKS: FINANCIAL, IP, AND SECURITY RISKS

OAIC Notifiable Data Breaches Report: January to June 2024

- 527 breaches reported — highest in 3.5 years, up 9% from the previous 6 months
- 63% of breaches affected SMBs with 100 or fewer individuals

IBM Cost of a Data Breach Report 2024

- Avg. breach cost: $4.26M AUD
- 5.7% increase from 2023

SANS 2024 Top Attacks and Threats Report

- Surge in the deployment of zero-day vulnerabilities with 70% malware surge signaling rising threats.

EVOLVING CYBER LANDSCAPE AND TRYING TO KEEP UP

The Australian Cyber Security Centre ‘s Annual Cyber Threat Report for 2023-24

- “The threat environment continues to evolve, driven by increasing geopolitical tension and strategic competition.”

Foreign Interference Risks Nation-states are engaging in a range of hostile cyber activities, including:

- Influence or coercion
- Espionage
- Pre-positioning for future disruptive attacks

“Nation-states are exploring AI to enhance cyber operations.”

- Enabling rapid vulnerability discovery and automated exploits and intrusions.

THE ACTORS

HACKER GROUP APT720 - MOLVANÎA MONGOOSE

- **Molvanîa, a fictional post-Soviet state,** is known as "the birthplace of the whooping cough" and home to Europe’s oldest nuclear reactor.
- Despite being landlocked, it **seeks nuclear submarine technology via corporate espionage.**
- Molvanîa threatens Emutopia’s security while **remaining its largest trade partner.**

REPCO PRIME

- REPCO PRIME, a leading global defense manufacturer, They secured a $**350 billion Nuclear submarine deal with Emutopia**.
- They **trust local contractors** have met regulatory DISP Cyber Security Standards .

JIM'S SHIP BUILDING

- Jim’s Shipbuilding is subcontracted to install and maintain air conditioning in the Submarines.
- Its Cyber Security Team **is understaffed and underfunded.**
- Their corporate IT services **are misconfigured and non-compliant.**

REPCO PRIME
DEFENSE COMPANY

JIM’S SHIP BUILDING

MOLVANÎA MONGOOSE'S OBJECTIVES

MOLVANÎA MONGOOSE OPERATIONAL OBJECTIVES

1. Data Exfiltration

Molvanîa aims to steal confidential sub schematics and ransom Jim’s Shipbuilding by defacing its site.

2. Lateral Movement Towards REPCO PRIME

Molvanîa wants to pivot from Jim’s Shipbuilding to REPCO PRIME , targeting larger contractors.

3. Sabotage

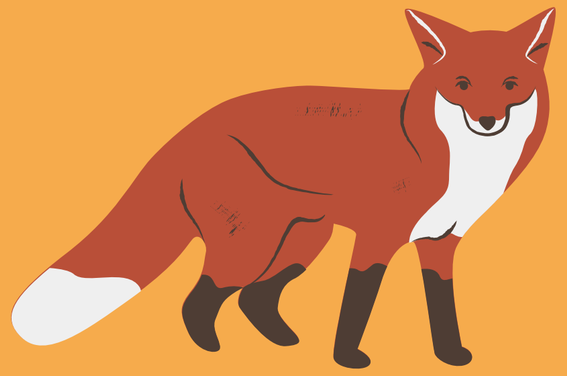
Molvanîa wants to sabotage submarine systems by altering specs or planting defects, risking Emutopia’s naval security.

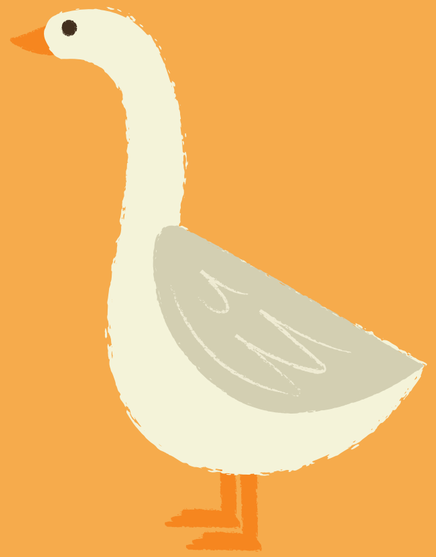
JIM'S SHIP MAKING

HACKED ?

ATTACK CHAIN DEMO

(TECHNICAL PROCESS)





WHAT DID THE MOLVANĬAN HACKERS STEAL?

WHAT DID THEY STEAL?

Submarine Blueprints & Technical Specifications

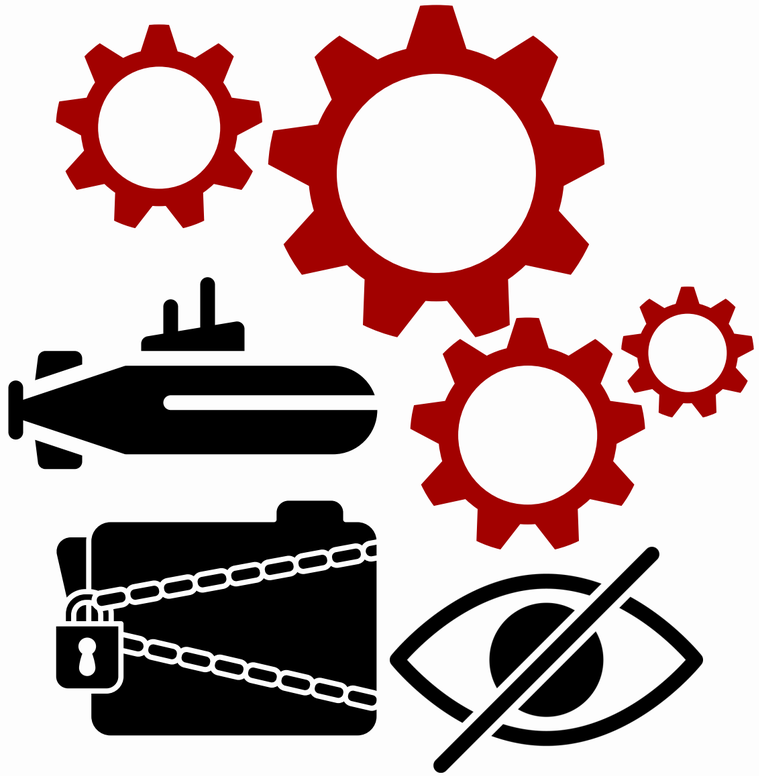
- Confidential REPCO PRIME sub schematics: structure, propulsion, materials.
- Secret engineering, stealth, and sonar evasion techniques.

Research & Development

- Innovations in submarine technology and blueprints for future naval defense projects.

Supply Chain & Logistics Data

- Internal records on submarine component suppliers, delivery schedules, and procurement details.



WHAT DID THEY STEAL?

Access Credentials & Network Security

- Stolen login details from Jim’s Ship Building employees.

Financial Records

- Bank statements, payroll info, and defence project budgets.

Communication & Internal Correspondence

- Emails, contracts, and messages revealing confidential negotiations between Jim’s Ship Building and REPCO PRIME

WHAT WENT WRONG ?

WHAT WENT WRONG ?

Poor Internal Security

- Weak passwords and poor credential management.

Lack of Network Segmentation

- Critical systems (e.g. print server, website, Windows server) are all interconnected.

No Security Auditing

- No monitoring, auditing, or threat detection in place.

Outdated Software & Patch Management

- Unpatched and open systems increased exposure to known vulnerabilities.

ESSENTIALLY, THEY WERE NOT MINDFUL OF THEIR SECURITY.

JIM'S SHIP BUILDING & REPCO PRIME'S DOWNFALL

Financial Impact

- Regulatory fines, penalties, and contract terminations.
- Stock price drop and supply chain delays causing major financial damage.

Reputation Damage

- Loss of trust from clients, partners, and government bodies.
- Negative media coverage and future contract risks due to security concerns.

Strategic & National Security Risk

- Doubts over reliability in critical sectors, affecting long-term defence and government partnerships.

WHAT HAPPENED TO JIM'S SHIP BUILDING

LATEST NEWS

JIM'S SHIPYARD BANKRUPTED AMID DATA BREACH SCANDAL

BREAKING NEWS

REPCO PRIME CEO dodges data breach questions in parliamentary hearing as stock prices plummet

PROACTIVE APPROACH TO CYBER DEFENSE

Visibility & Threat Awareness

- Continuously monitor systems (EDR, SIEM, NDR) for anomalies.

Testing & Response Readiness

- Conduct red, blue, and purple team exercises, and automate incident response playbooks.

Human & Supply Chain Resilience

- Train staff with awareness programs and enforce strong identity practices

Secure Architecture & Prevention

- Implement network segmentation and least privilege access.

WHY INVESTING IN CYBERSECURITY THREAT HUNTING ?

STATE-SPONSORED ATTACKERS OFTEN EVADE DETECTION AND STAY HIDDEN FOR MONTHS.

Threat hunting takes a proactive approach, actively searching for hidden threats like APTs that bypass traditional detection.

Reduce breach impact

- Detect early, contain threats, minimise damage.

Fill visibility gaps

- Uncover threats hidden from traditional tools.

Enhance incident response

- Streamline investigations, accelerate informed response actions.

WHAT HAPPENED TO MOLVANÎA'S NUCLEAR SUBMARINE PROGRAM

GLORY TO MOLVANÎA

THANK YOU

- RKCC
- CYBER WEST
- EMU EXPLOIT

SLIDES + VIDEO:

EMU.TEAM/RKCC

FIND US AT: (HTTPS://EMU.TEAM)

/ - @EMUEXPLOIT

DIV (</DIV>)

ORLANDO (Q3ST1ON)

NEXT UP: DISP

Rockingham Kwinana Chamber Of Commerce