Module 3 - Execution Phase: Operation 'AEGIS SHIELD'

Course: Advanced Cyberwarfare Programme

Course Code: ACW904-ASSIGNMENT-M3-V1.0

Instructor Name: Aminu Idris

Date: Oct 29, 2025

Version 1.0

Table of Content

COMMAND LOG: OPERATION AEGIS SHIELD

WATCH COMMANDER:
DATE: Oct 29, 2025

[Inject 1 // 08:30Z]

Orientation: Initial Delivery attempt identified via suspicious email attachment (Q4_Manifests_Urgent.xlsm) sent to logistics personnel. This aligns with IRON VORTEX TTPs and represents the Delivery phase of the Cyber Kill Chain.
Decision & Command: [MONITOR] logistics subnet traffic for signs of exploitation or lateral movement.
Tasking: Analyst-1 (Network Analyst)
Rationale: Applying the OODA loop, this is the Observe/Orient phase. Monitoring enables early detection of follow-on exploitation and positions resources for rapid containment. No immediate disruption is warranted until further indicators emerge.

[Inject 2 // 09:15Z]

Orientation: Confirmed Exploitation and Installation on host EMP-WS-1138. EDR alert shows powershell.exe launched by EXCEL.EXE, attempting to download from external IP 185.141.25.234.
Decision & Command:
[ISOLATE HOST] EMP-WS-1138
[BLOCK IP/DOMAIN] 185.141.25.234
Tasking: Specialist-1 (Incident Responder) for isolation, Analyst-1 (Network Analyst) for firewall block
Rationale: Under ROE A (Active Defense), containment is critical to prevent adversary control and lateral movement. Blocking the IP severs the initial C2 channel. This is the Decide/Act phase of the OODA loop.

[Inject 3 // 09:45Z]

Orientation: Host EMP-WS-1138 is making periodic encrypted outbound connections to 185.141.25.234 over port 443. Captured binary indicates active C2 communication—Command & Control phase confirmed.
Decision & Command:
[REQUEST MALWARE ANALYSIS] on captured binary
[REPORT & ESCALATE] to OPCOM-CYBER
Tasking:
Specialist-2 (Malware Reverse Engineer)
Watch Commander (self) for escalation

Rationale: ROE C mandates reporting confirmed adversary infrastructure. Malware analysis supports the secondary mission objective and ROE D (Preservation of Evidence). This is a strategic intelligence opportunity.

[Inject 4 // 10:30Z]

Orientation: Adversary is conducting internal reconnaissance from EMP-WS-1138, targeting network shares and attempting access to CM-DB-01—the Cargo Manifest Database. This marks the Actions on Objectives phase.

Decision & Command:

[REQUEST FORENSICS] on EMP-WS-1138

[MONITOR] CM-DB-01 network logs

Tasking:

Specialist-1 (Incident Responder) for forensic imaging

Analyst-1 (Network Analyst) for monitoring

Rationale: Protecting critical infrastructure takes precedence. Forensics preserves host state for intelligence while monitoring ensures real-time visibility. This balances containment with evidence preservation per ROE D.

[Inject 5 // 11:30Z]

Orientation: Malware analysis confirms IRON VORTEX attribution. Three hardcoded C2 domains identified:

- sysupdate.northlandia-cdn[.]com
- content-delivery.northlandia-cdn[.]com
- api.cloud-services.northlandia-cdn[.]com

Decision & Command:

[BLOCK IP/DOMAIN] all three domains

[REPORT & ESCALATE] to OPCOM-CYBER

Tasking:

Analyst-1 (Network Analyst) for domain blocking

Watch Commander (self) for escalation

Rationale: ROE C requires immediate reporting of adversary infrastructure. Blocking these domains prevents fallback C2 channels and strengthens network resilience (ROE A). This completes the intelligence cycle.

FINAL SITUATIONAL REPORT (SITREP)

TO: OPCOM-CYBER
FROM: TACCOM-CYBER, Watch Commander, Watch Team Delta
SUBJECT: FINAL SITREP: IRON VORTEX INTRUSION ON POSEIDON NETWORK
DATE/TIME: Oct 29, 2025 / 12:00 ZULU

1. SUMMARY

This incident included the POSEIDON Maritime Logistics Network being targeted by an intrusion attempt from the IRON VORTEX threat actor. The adversary used a spear phishing campaign to distribute a malicious Excel macro, which compromised at least one workstation (EMP-WS-1138). The threat was stopped before it was able to accomplish its stated goal of connecting to the Cargo Manifest Database (CM-DB-01), due to the containment, isolation, and escalation that were appropriately conducted in a timely manner. The network is up and running now, and we were able to protect some key assets.

2. INCIDENT TIMELINE & ACTIONS TAKEN

Time (Z)	Kill Chain Phase	Event	Defensive Action(s)	Outcome
08:30	Delivery	Spear-phishing email with malicious Excel attachment detected.	Initiated [MONITOR] of logistics subnet traffic.	Early detection; positioned resources for rapid response.
09:15	Exploitation / Installation	Host EMP-WS-1138 executed malicious PowerShell, downloading from 185.141.25.234.	[ISOLATE HOST] EMP-WS-1138; [BLOCK IP/DOMAIN] 185.141.25.234.	Contained compromised host; severed adversary's initial foothold.
09:45	Command & Control (C2)	Periodic encrypted outbound connections confirmed; binary captured.	[REQUEST MALWARE ANALYSIS] on binary; [REPORT & ESCALATE] to OPCOM-CYBER.	Preserved evidence; escalated intelligence to higher command.
10:30	Actions on Objectives	Reconnaissance from EMP-WS-1138 targeting Cargo Manifest Database (CM-DB-01).	[REQUEST FORENSICS] on compromised host; [MONITOR] CM-DB-01 network logs.	Protected critical asset; preserved forensic evidence for later analysis.

11:30	Intelligence Gathering	Malware analysis confirmed IRON VORTEX attribution; three C2 domains extracted.	[BLOCK IP/DOMAIN] all three domains; [REPORT & ESCALATE] to OPCOM-CYBER.	Secondary mission objective achieved; adversary infrastructure neutralized.

3. CURRENT NETWORK STATUS

The threat has been eradicated and all critical infrastructure assets are still secure and operational. The overall operational impact is minimal and limited to the quarantine of a single infected workstation.

Asset / Segment	Status	Operational Impact
EMP-WS-1138 (Compromised Host)	Isolated from the network; pending full remediation and eradication.	Contained successfully; no further adversary activity observed.
Cargo Manifest Database (CM-DB-01)	Secure and uncompromised.	High-value target defended; no data exfiltration or corruption detected.
Vessel Tracking System (VTS-SRV-01)	Fully operational.	No disruption to maritime situational awareness.
Port Operations Server (PO-SRV-01)	Fully operational.	No impact to crane/container scheduling or port throughput.
Public-Facing Web Server (WEB-SRV-01)	Unaffected.	No adversary interaction detected.
Employee Workstations (General)	149 unaffected; 1 isolated (EMP-WS-1138).	Minimal operational impact; logistics staff reassigned temporarily.
Network Perimeter (Firewall / IDS)	Updated with blocks for IP 185.141.25.234 and three C2 domains.	Strengthened defenses; adversary C2 infrastructure neutralized.

4. GATHERED INTELLIGENCE (SECONDARY OBJECTIVE)

Category	Details
Threat Actor	IRON VORTEX
Delivery Method (TTPs)	Spear-phishing emails with malicious Excel macro attachment (.xlsm)

Exploitation / Installation (TTPs)	Execution of powershell.exe by EXCEL.EXE to download payload from external IP
Persistence / C2 (TTPs)	Custom loader establishing encrypted C2 heartbeat every 90 seconds
Actions on Objectives (TTPs)	Internal reconnaissance targeting network shares and high-value database (CM-DB-01)
C2 IP Address (IOC)	185.141.25.234
C2 Domains (IOCs)	- sysupdate.northlandia-cdn[.]com - content-delivery.northlandia-cdn[.]com - api.cloud-services.northlandia-cdn[.]com

5. RECOMMENDATIONS

1. Block all known C2 infrastructure (IP 185.141.25.234 and the three domains) at the national level through your intrusion prevention systems (IPS) and DNS filters to prevent adversary fallback operations.
2. Disseminate information regarding IRON VORTEX's phishing vector, custom loader, and C2 methodology to all national agencies to provide greater situational awareness and enable proactive defense.
3. Examine and update the mail gateway filtering rules to fix any misconfigurations that could result in dangerous attachments getting through mail gateway.
4. Perform red-team exercises throughout maritime logistics networks to confirm ability to respond, to enhance response tempo, and to assess coordination in the face of live threat scenarios.

AFTER-ACTION REVIEW (AAR)

This is a demonstration of the well-executed ACW Doctrinal C2 Framework and the strict conformance to the Rules of Engagement. A key event was the rapid containment of EMP-WS-1138 and the blocking of the malicious IP address immediately after Inject 2. This action prevented the adversary from establishing persistence and also safeguarded the Cargo Manifest Database from compromise. In addition, relaying confirmation of C2 infrastructure to OPCOM-CYBER escalated it in a timely manner, thus also accomplishing intelligence collection, and without operational delay.

The challenge I faced was how to walk ROE (A) Active Defense and (D) Preservation of Evidence (POE) on a very fine line. When the adversary started to stage, containment became more urgent than intelligence gathering to prevent destruction of critical national infrastructure. That remains a core tension at the command. In addition to emphasizing the intense resource requirements of malware reverse engineering, the analysis also underscored the imperative of faster intelligence flowing to future operations. Overall the drill reaffirmed the importance of

bold leadership, doctrinal compliance, and moral ownership of mission-essential systems in the heat of battle.

REFERENCES

Hutchins, E. M., Cloppert, M. J., & Amin, R. M. (2011). Intelligence-driven computer network defense informed by analysis of adversary campaigns and intrusion kill chains. Lockheed Martin Corporation. Retrieved from https://www.lockheedmartin.com

National Institute of Standards and Technology. (2020). NIST Special Publication 800-61 Revision 2: Computer Security Incident Handling Guide. U.S. Department of Commerce. https://doi.org/10.6028/NIST.SP.800-61r2

Rid, T., & Buchanan, B. (2015). Attributing cyber attacks. Journal of Strategic Studies, 38(1–2), 4–37. https://doi.org/10.1080/01402390.2014.977382

Stopford, M. (2020). Maritime economics (4th ed.). Routledge. https://doi.org/10.4324/9780429439397

U.S. Department of Defense. (2018). Department of Defense Cyber Strategy. Office of the Secretary of Defense. Retrieved from https://media.defense.gov