Assignment 3.1: Intelligence Triage and Response Report

Joshua A. Wortz

University of San Diego

CSOL-580

Dr Hollandsworth

03/16/2026

Section 1: Intelligence Triage

Initial Assessment

A comprehensive cyber campaign spanning 2021 to 2023 has been identified, targeting government entities and critical infrastructure sectors worldwide. Technical analysis of these intrusions reveals a sophisticated array of attack vectors and Indicators of Compromise (IOCs). Primary deployment tools included CatB ransomware, which was utilized in high-profile attacks against the All India Institute of Medical Sciences (AIIMS) and the Presidency of Brazil in 2022 (Newsroom, 2024). Beyond standard ransomware, the threat actors leveraged legitimate dual-use encryption software, specifically Jetico BestCrypt and Microsoft BitLocker, to facilitate unauthorized data encryption (Newsroom, 2024). Technical artifacts identified within the environments include the China Chopper web shell, the DTrack backdoor, and custom malware families such as DoorMe and MGDrive, the latter of which includes a macOS variant known as Gimmick (Newsroom, 2024).

Based on the systemic impact on high-value targets—including the Presidency of Brazil and approximately 37 organizations within the U.S. manufacturing sector—this campaign is classified as Critical/High severity (Newsroom, 2024). This rating is justified by the targeting of foundational services like healthcare and government administration, which aligns with the high-impact categorization described in foundational risk analysis frameworks (CyberEdge Group, 2022).

Threat Actor Analysis

The campaign is attributed to two primary activity clusters. The first is ChamelGang, also known as CamoFei, which is a China-nexus group (Newsroom, 2024). The second cluster exhibits overlapping activity previously attributed to the Chinese hacking crew APT41 and the North Korean state-sponsored actor Andariel, evidenced by the shared use of the China Chopper web shell and the DTrack backdoor (Newsroom, 2024). These actors demonstrate varied objectives, including intelligence gathering, data theft, financial gain, information operations, and denial-of-service (DoS) attacks (Newsroom, 2024).

A critical trend in their strategy is the use of ransomware as the final stage of cyber-espionage operations. This tactic serves to cover their tracks by destroying forensic evidence and artifacts that could alert defenders to their presence, while simultaneously providing an opportunity for misattribution or plausible deniability (Newsroom, 2024). These groups use a "digital quartermaster" strategy, in which custom malware is supplied to distinct operational groups such as REF2924 and Storm Cloud, effectively blurring the lines between threat clusters through shared infrastructure (Newsroom, 2024).

Data Correlation & Evidence

Effective Security Operations (SecOps) rely on enriching SIEM and EDR alerts with real-time external context to identify associations between local events and known threat actor TTPs

(CyberEdge Group, 2022). Below are representations of the indicators security teams should hunt for within the environment:

Evidence 1: Sample Log Snippet (Web Server Access Log).

```
POST /scripts/default.aspx - 80 - 10.0.0.5 Mozilla/5.0+... - 200 0 0 15
```

(Note: This log identifies a potential China Chopper web shell execution via an unusual POST request to a scripts directory.)

Evidence 2: SIEM Alert Snippet (Unauthorized Encryption)

`Alert: BitLocker Drive Encryption Started | User: SYSTEM | Host: DC-01 | Process: C:\Windows\System32\BitLockerWizard.exe` *(Note: This alert triggers on the unexpected use of dual-use tools like BitLocker by a system process rather than a scheduled administrative task.)*

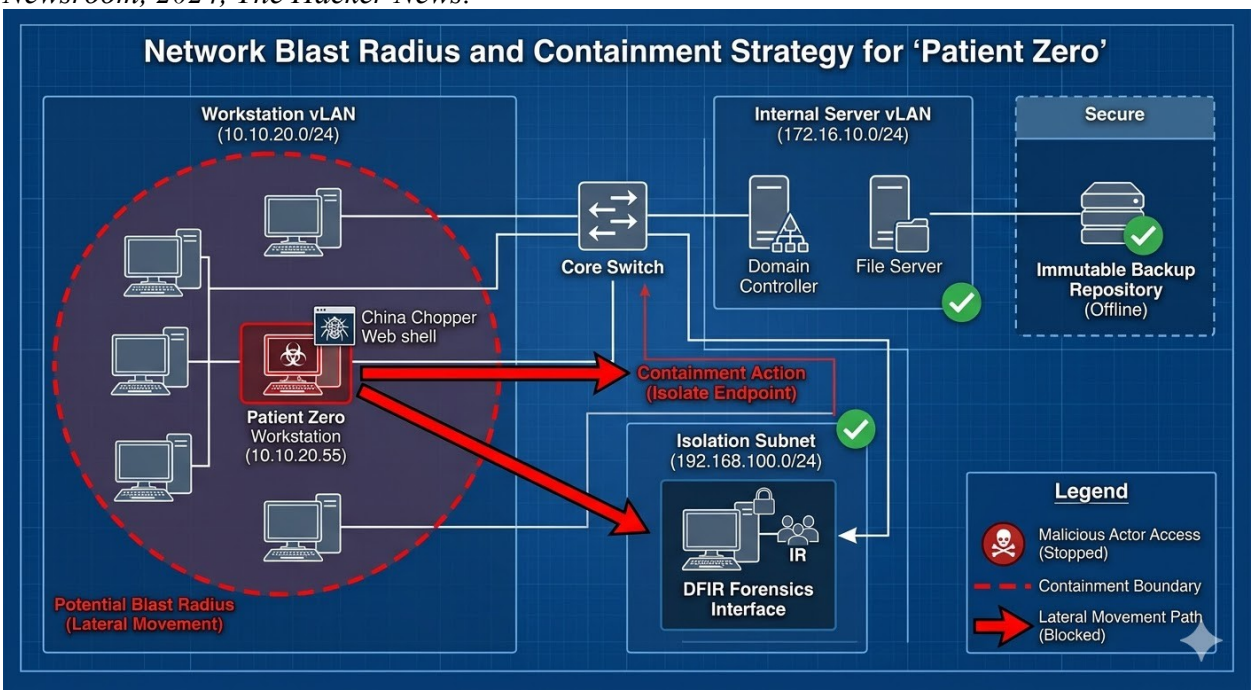
Section 2: Structured Incident Response Plan

Per industry best practices for intelligence-led response (CyberEdge Group, 2022), the following structured plan defines the phases of containment, eradication, and recovery.

Phase 1: Containment

- **Endpoint Isolation:** Immediately isolate any endpoints exhibiting artifacts of DTrack, China Chopper, or BeaconLoader from the production network (Newsroom, 2024).
- **Network Restriction:** Block all outbound traffic to Command and Control (C2) domains identified during triage to halt data exfiltration.
- **Blast Radius Visualization:**
  Figure 1.
  Network topology illustrating the potential blast radius of a China Chopper web shell infection and the subsequent containment action to an isolation subnet. Adapted from "Chinese and N. Korean Hackers Target Global Infrastructure with Ransomware," by

Newsroom, 2024, The Hacker News.



Phase 2: Eradication

- **Malware Removal:** Systematically remove custom backdoors such as DoorMe, MGDrive, and AukDoor from the environment (Newsroom, 2024).
- **Dual-Use Tool Restriction:** Strictly restrict administrative access to Jetico BestCrypt and Microsoft BitLocker through Group Policy Objects (GPOs) to prevent unauthorized use by threat actors (Newsroom, 2024).
- **Credential Reset:** Force a password reset for all administrative and service accounts that may have been compromised during the espionage phase of the attack.

Phase 3: Recovery

- **Immutable Restoration:** Rebuild impacted systems exclusively from offline, immutable backups (Newsroom, 2024). This is critical as threat actors use ransomware to destroy artifacts and evidence (Newsroom, 2024).
- **Forensic Validation:** Prior to bringing systems back online, perform a final forensic sweep to ensure no dormant persistence mechanisms remain.
- **Role Allocation:** SecOps Analysts perform rapid alert triage while Incident Responders execute technical remediation (CyberEdge Group, 2022).

Section 3: Mitigation Recommendations

To enhance long-term resilience, the organization must transition from a reactive posture to a proactive, intelligence-led security model.

1. **Intelligence Feed Integration:** Incorporate intelligence feeds directly into SIEM and EDR tools. This enables automatic enrichment of alerts with external context, speeding up the "Time to No" by allowing analysts to dismiss false positives and focus on genuine threats (CyberEdge Group, 2022).
2. **Proactive Process Preparation:** Prepare incident response workflows for common threats, such as state-sponsored ransomware, in advance. Proactively establishing these procedures reduces containment time and minimizes errors during high-pressure events (CyberEdge Group, 2022).
3. **Risk-Based Patching:** Adopt a vulnerability management strategy that prioritizes patching actively exploited vulnerabilities, such as those targeted by groups like ChamelGang and APT41, rather than attempting to patch all vulnerabilities indiscriminately (CyberEdge Group, 2022).

References

CyberEdge Group. (2022). *The intelligence handbook: A roadmap for building an intelligence-led security program* (4th ed.). Recorded Future; CyberEdge Press.

Gemini. (2026). *Network blast radius and containment strategy for 'Patient Zero'* [Infographic]. Google AI.

Newsroom. (2024, June 26). *Chinese and N. Korean hackers target global infrastructure with ransomware*. The Hacker News. https://thehackernews.com/2024/06/chinese-and-n-korean-hackers-target.html