Incident Response Simulation

April 13th, 2025

Nijat Ismayilov

Contents

1. Introduction

Incident response is a critical process in cybersecurity, ensuring that organizations can effectively detect, contain, and recover from security breaches. This document details a simulated incident response scenario where an organization experiences a security breach.

The objective of this exercise is to evaluate the organization’s response to the incident, identify gaps, and recommend improvements for future security incidents.

2. Incident Response Process

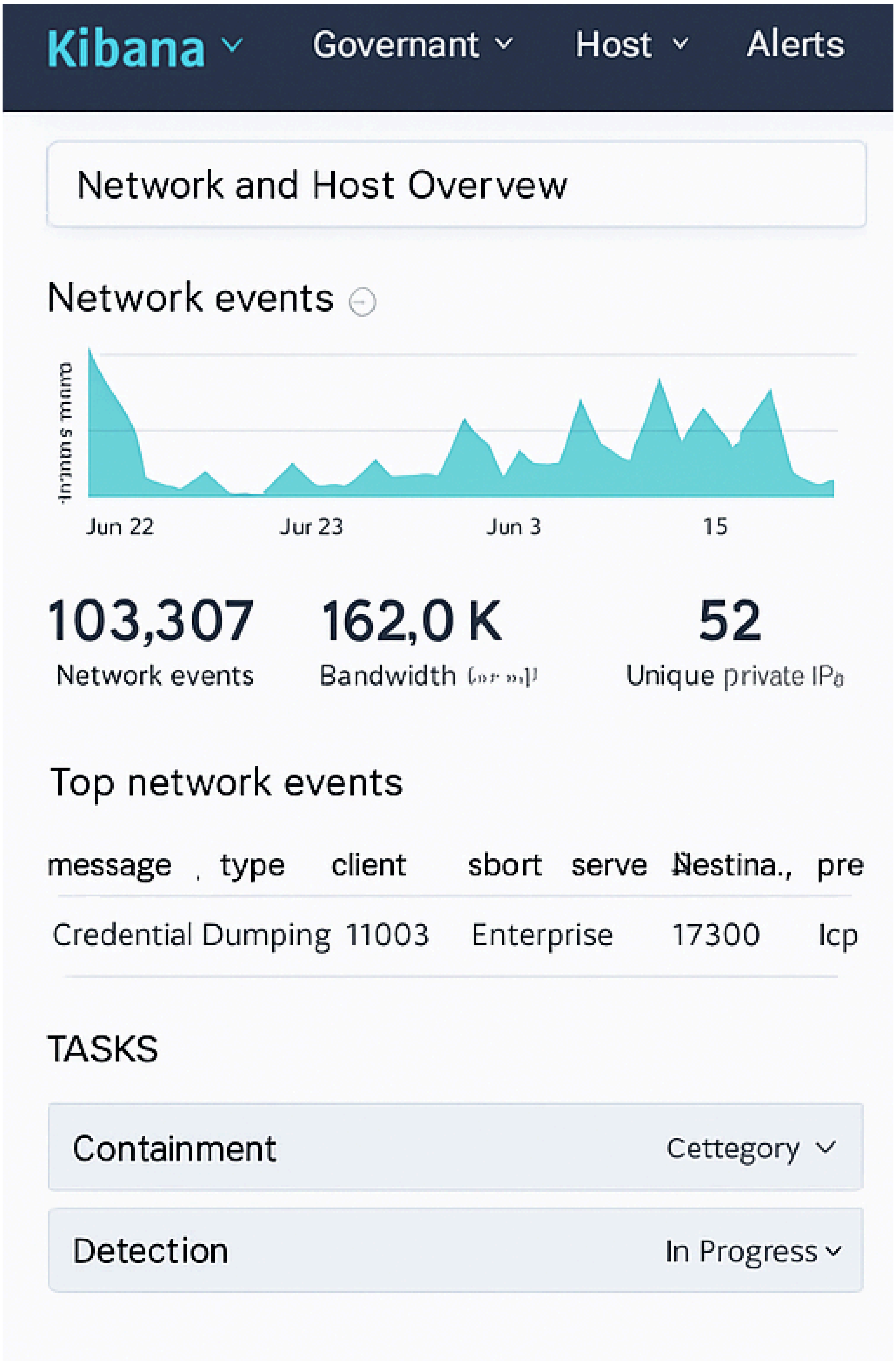
The **Incident Response Lifecycle** consists of six major phases:

2.1. Preparation

- Establishing an incident response plan
- Implementing monitoring and logging solutions
- Training employees on security best practices

2.2. Identification

- Detecting abnormal activity using logs and alerts
- Analyzing logs with **ELK Stack** to confirm a security breach



Network and Host Overvew

Network events

103,307
Network events

162,0 K
Bandwidth [illegible]

52
Unique private IPs

Top network events

message	type	client	sbort	serve	Nestina.,	pre
Credential Dumping		11003	Enterprise		17300	Icp

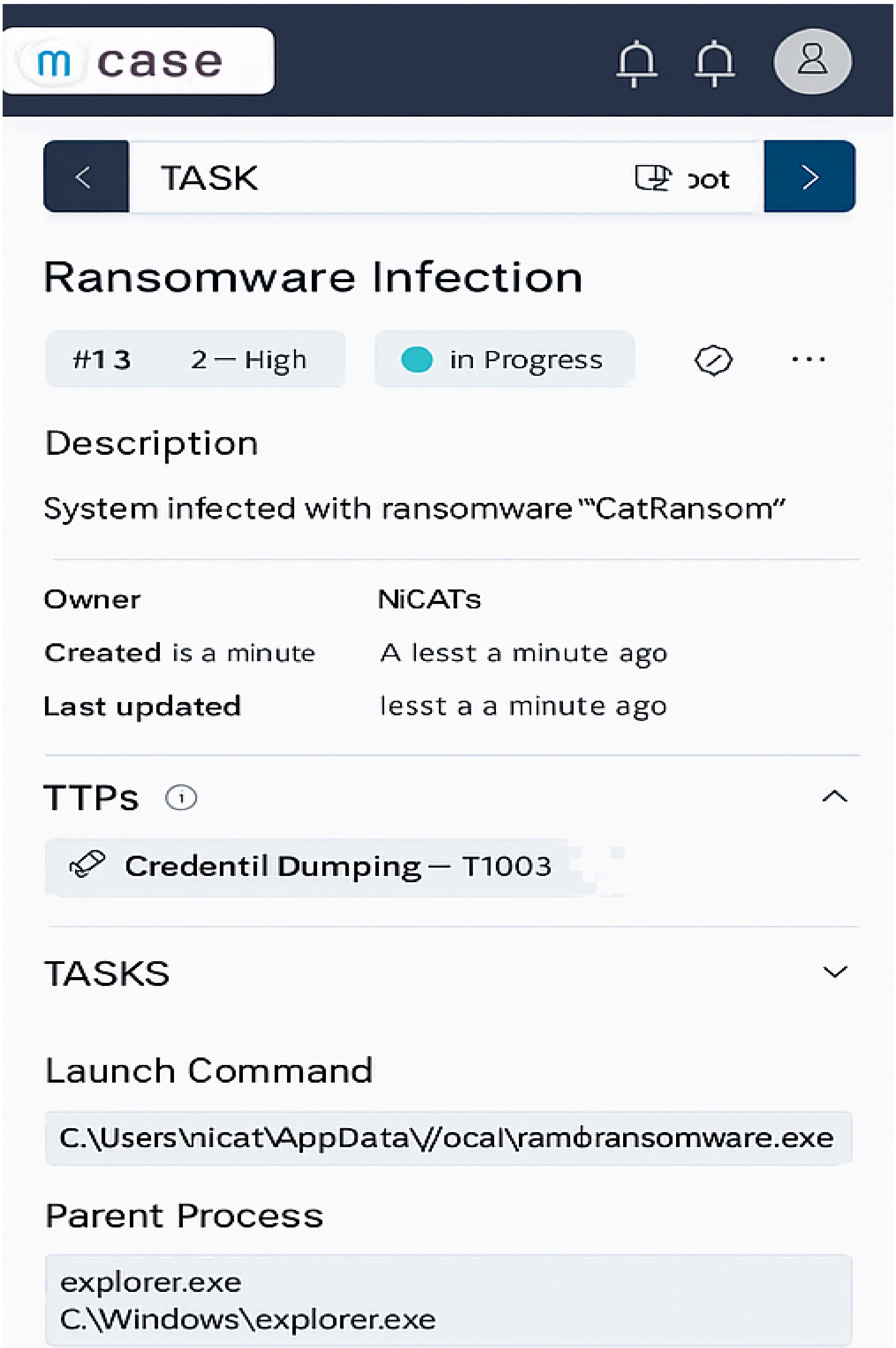
TASKS

Containment — Cettegory

Detection — In Progress

2.3. Containment

- Isolating affected systems to prevent further spread
- Blocking malicious network traffic using firewalls and endpoint security solutions



Ransomware Infection

#13 2 — High

● in Progress

Description

System infected with ransomware "CatRansom"

Owner	NiCATs
Created is a minute	A lesst a minute ago
Last updated	lesst a a minute ago

TTPs

Credentil Dumping — T1003

TASKS

Launch Command

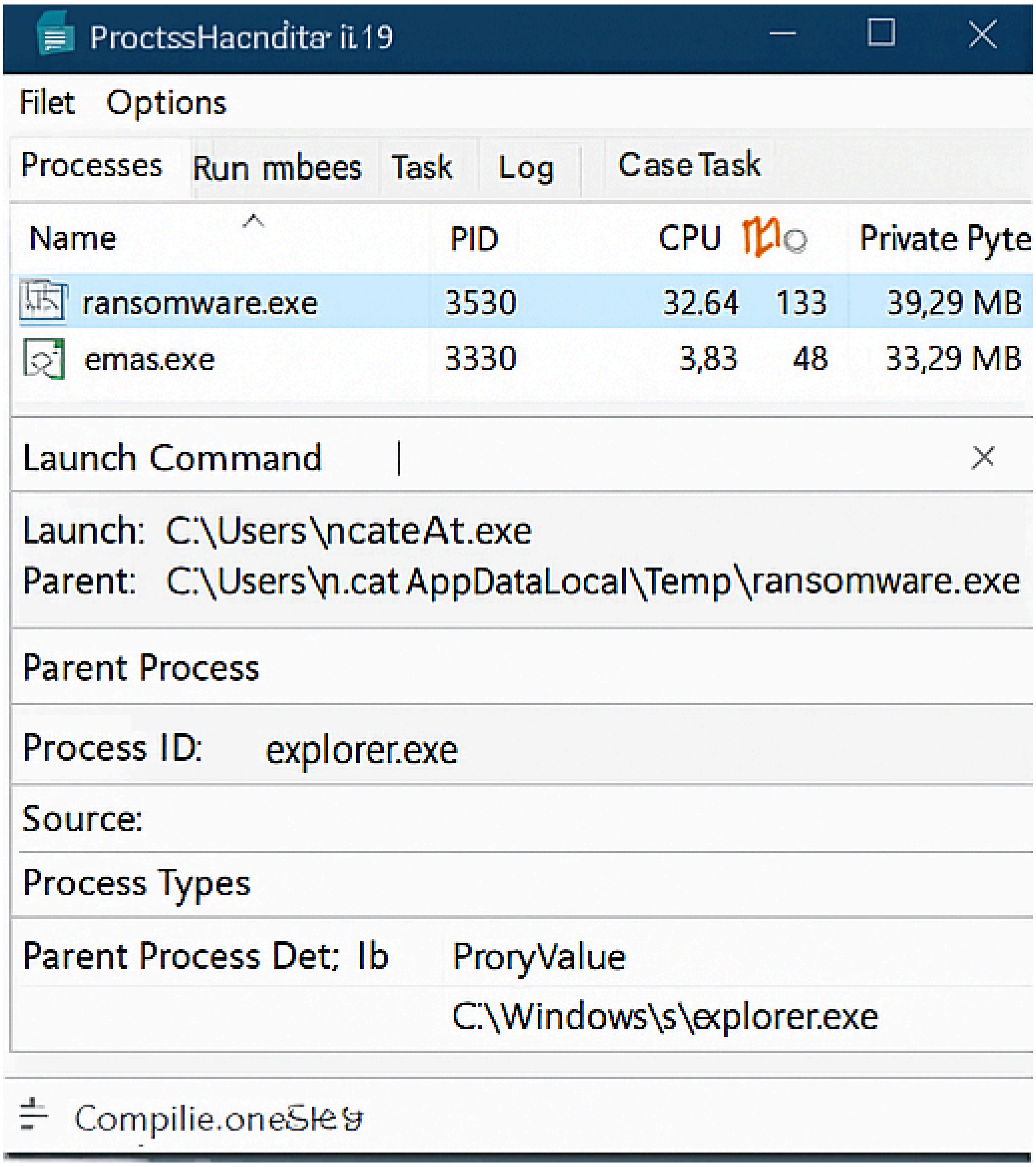
```
C.\Users\nicat\AppData\/ocal\ramɸransomware.exe
```

Parent Process

```
explorer.exe
C.\Windows\explorer.exe
```

2.4. Eradication

- Removing malware or unauthorized access
- Conducting forensic analysis to trace the attack vector



Name	PID	CPU		Private Pyte
ransomware.exe	3530	32.64	133	39,29 MB
emas.exe	3330	3,83	48	33,29 MB

Launch Command

Launch: C:\Users\ncateAt.exe
Parent: C:\Users\n.cat AppDataLocal\Temp\ransomware.exe

Parent Process

Process ID: explorer.exe

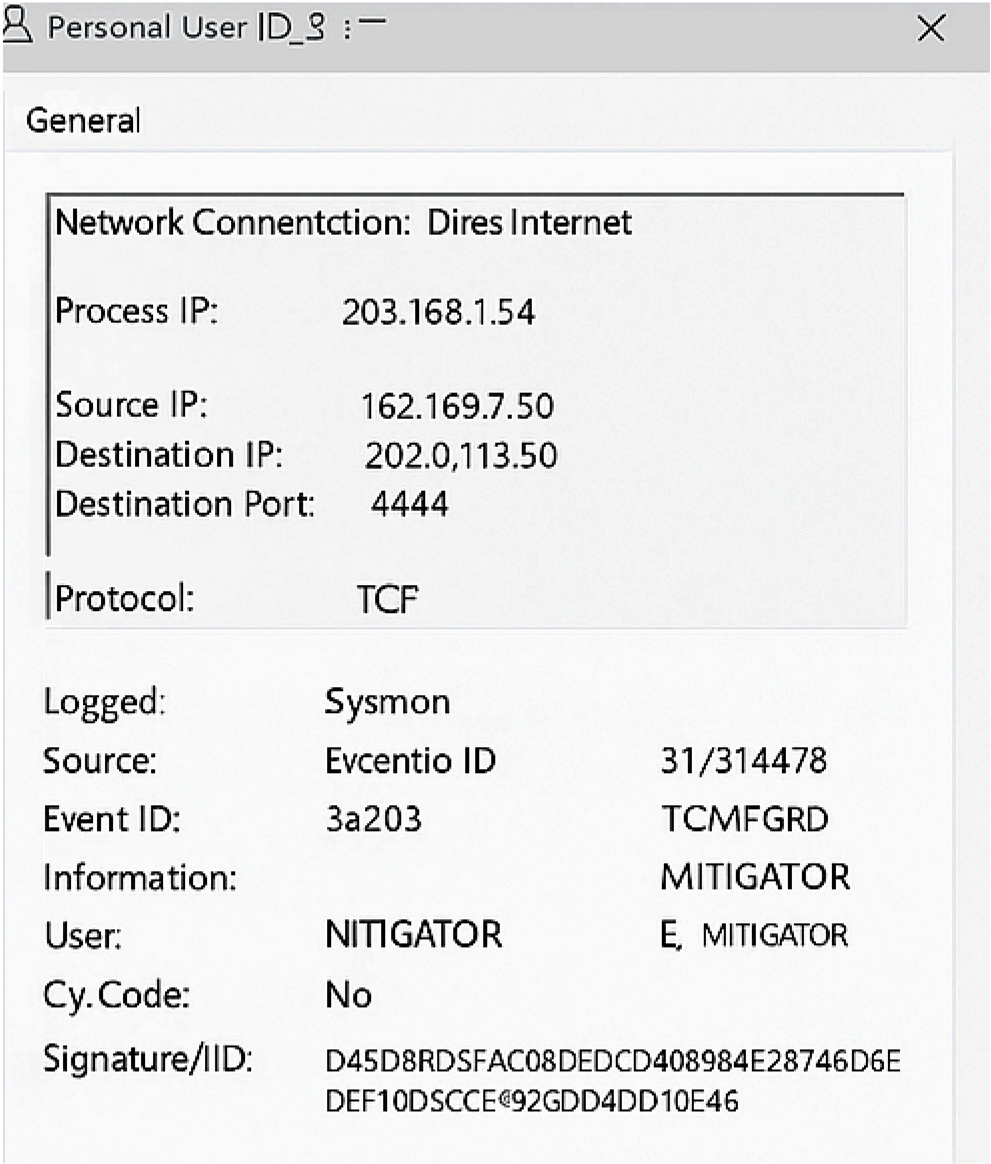
Source:

Process Types

Parent Process Det; Ib ProryValue
C:\Windows\s\explorer.exe

2.5. Recovery

- Restoring systems from secure backups
- Monitoring for any signs of reinfection



Network Connentction: Dires Internet

Process IP: 203.168.1.54

Source IP: 162.169.7.50

Destination IP: 202.0,113.50

Destination Port: 4444

Protocol: TCF

Logged:	Sysmon	
Source:	Evcentio ID	31/314478
Event ID:	3a203	TCMFGRD
Information:		MITIGATOR
User:	NITIGATOR	E, MITIGATOR
Cy.Code:	No	
Signature/IID:	D45D8RDSFAC08DEDCD408984E28746D6E DEF10DSCCE@92GDD4DD10E46	

2.6. Lessons Learned

- Reviewing logs and incident response steps
- Updating security policies to prevent future breaches

3. Simulation Scenario

In this simulation, the organization experienced a **ransomware attack** targeting internal file servers. Suspicious activities were detected by **SIEM (Security Information and Event Management) tools**, triggering an investigation.

The attacker exploited a **phishing email** to gain initial access, followed by **lateral movement** within the network. Sensitive files were encrypted, and a ransom note appeared demanding payment in cryptocurrency.

4. Implementation and Findings

During the incident response process, the following findings were observed:

- The phishing email contained a **malicious attachment** that delivered a **Remote Access Trojan (RAT)**.
- The attacker used **PowerShell scripts** to escalate privileges and execute ransomware payloads.
- **Network logs showed unusual outbound traffic** to an external IP, indicating data exfiltration attempts.

By analyzing logs in **ELK Stack** and coordinating response efforts in **TheHive**, we successfully contained the attack and prevented further damage.

5. Recommendations

To enhance incident response capabilities, the following improvements are recommended:

1. **Improve Employee Training**: Conduct regular **phishing awareness training** to reduce human errors.

2. **Enhance Logging & Monitoring**: Utilize **SIEM tools like ELK Stack** to detect threats earlier.

3. **Implement Stronger Access Controls**: Enforce **multi-factor authentication (MFA)** to prevent unauthorized access.

4. **Regular Backup Strategy**: Ensure **offline backups** are available to restore data in case of ransomware attacks.

6. Conclusion

The **Incident Response Simulation** successfully demonstrated how to detect, contain, and recover from a ransomware attack. By leveraging **ELK Stack**, **TheHive**, and forensic analysis, we mitigated the impact and strengthened the organization's security posture.

This exercise highlights the importance of continuous improvement in incident response strategies to protect against evolving cyber threats.