RANSOMWARE Simulation with Detection & Response

Cybersecurity 2025/2026

Alessandro Modelli
ID: 0001145565

PROJECT OVERVIEW

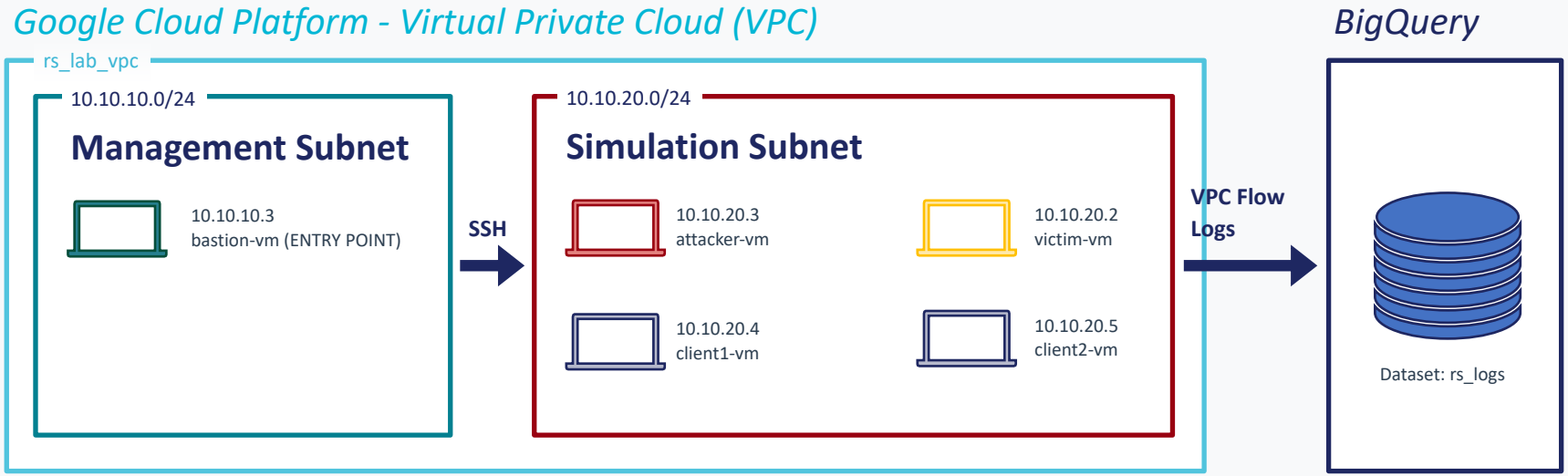
Objective

Design and implement a controlled ransomware simulation on Google Cloud Platform and evaluate the effectiveness of a network-based detection system with automated response measures.

Key Goals

- Reproduce typical ransomware behavior (encryption + exfiltration)
- Build an isolated cloud infrastructure with network logging
- Analyze network flows to identify anomalous patterns
- Implement automated detection and containment measures

INFRASTRUCTURE ARCHITECTURE



Key Infrastructure Features

- VPC Flow Logs enabled on simulation subnet (5-seconds log aggregation)
- Restrictive firewall rules (SSH only via bastion)
- Automatic log export to BigQuery
- 5 VMs total: 1 bastion + 4 simulation instances

SIMULATION SCENARIO

1

“Standard” Traffic Generation Setup

HTTP traffic generation between client1-vm, client2-vm, victim-vm (20 min duration, ~10s intervals)

2

Attacker Setup

Server on attacker-vm listening on port 8080 for data exfiltration

3

Ransomware Script

Python script encrypts **target files** (746 MB total) and exfiltrates to attacker

Target files: 250 dummy files (.txt, .csv, .pdf, .jpg, .png) inside victim-vm

SIMULATION EXECUTION

01

VPC Flow Logs activation

Activation of the configuration of VPC Flow Logs to collect all the logs

gcp-fl-simulation-subnet-europe-west8

02

HTTP server execution

Execution of Python servers on client VMs (port 8080) in background

client1-vm, client2-vm

03

HTTP traffic generation

Execution of Python script on client1-vm, client2-vm, victim-vm to generate HTTP requests in background

httpGen.py

Duration

~ 20 minutes

SIMULATION EXECUTION

04

Exfiltration server execution

Execution of server on attacker-vm listening for file exfiltration

server.py

5 minutes interval to register regular traffic

05

Ransomware execution

Execution of the ransomware script on the target folder

ransomware.py

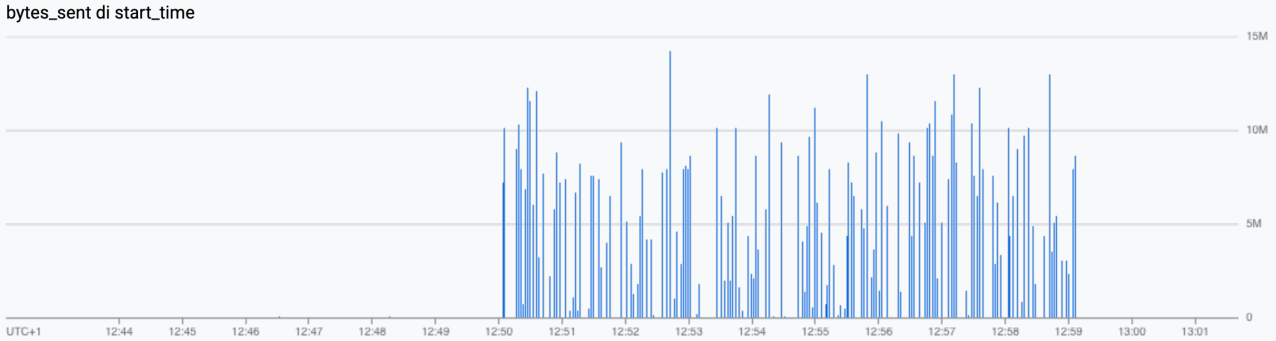
Duration

~ 20 minutes

LOG ANALYSIS & ANOMALY DETECTION

Data Processing Pipeline

- VPC Flow Logs collection → BigQuery export
- Created flattened view for efficient SQL querying
- Filtered external Google IPs (reduced 1409 → 704 log entries)
- Traffic analysis based on bytes_sent



Noticeable spike 12:50 - 12:59 UTC+1

LOG ANALYSIS & ANOMALY DETECTION

Data Processing Pipeline

- Traffic destination ports analysis
- “Standard” Traffic vs Ransomware Traffic)

“Standard” Traffic

- Max bytes_sent: 39.7 KB on other ports
- Port 8080: < 20 KB of bytes_sent
- Traffic type: HTTP Requests
- Duration: Continuous

Ransomware Traffic

- Max bytes_sent: ~150MB+ on port 8080
- Port 8080: 1.5 GB of bytes_sent
- Traffic type: File uploads
- Duration: ~9 minutes

DETECTION SYSTEM DESIGN

Detection Thresholds

- Time window: 1 minute
- Minimum events: 5 flows per window
- Minimum bytes_sent: 25 KB per flow

Detection Logic

- BigQuery query scans last 4 minutes of flow logs
- Groups flows into 1-minute windows by (src_vm, dest_vm, dest_port)
- Filters out low-volume traffic (< 25 KB)
- Triggers alert when threshold exceeded → automated response

Result: Successfully identified ransomware activity from 12:50 to 12:59 UTC

RESPONSE MEASURES DESIGN

ISOLATION

- EGRESS Firewall rule

  Dynamic creation of a new firewall rule to deny all TCP traffic on the identified port.

TERMINATION

- Compromised VM shutdown

  Shutdown of identified instance to interrupt any script execution

Automated Response Workflow

AUTOMATED DETECTION AND RESPONSE SYSTEM

Automated Workflow

FINAL RESULTS

WITHOUT vs WITH AUTOMATION

Simulation 1

- NO detection and response system

9m 03s
Attack duration
12:50 - 12:59

250/250
Exfiltrated files
100%

No containment measures
Complete data exfiltration

Simulation 2

- Automated detection and response system

3m 46s
Attack duration
16:10 - 16:14

98/250
Exfiltrated files
~40%

Detection every 2 minutes
Partial data exfiltration
Automated ISOLATION and TERMINATION

KEY FINDINGS & INSIGHTS

Network Analysis is Effective

VPC Flow Logs successfully identified ransomware data exfiltration patterns based on volume and frequency anomalies

Automation Reduces Impact

Automated detection and response system interrupted exfiltration limiting damage to 40% of target data

Real-Time Monitoring Essential

2-minute scheduler interval provided near real-time detection

Multi-Layer vs Single-Layer response

Combining firewall isolation + VM shutdown ensures complete containment while only firewall isolation does not interrupt the script execution

CONCLUSIONS

This project demonstrates that network-based detection can effectively identify and mitigate ransomware attacks in cloud environments

Key success factors:

- Comprehensive logging (VPC Flow Logs)
- Efficient anomaly detection thresholds
- Automated response mechanisms

Thank you for your attention