# Security Incident Report

### **Table of contents**

[Security Incident Report 1](#_crlgmap8ym05)

[Table of Contents 1](#_u17i2fv460ug)

[Executive summary 2](#_c8wmvmx6j3to)

[Investigation 3](#_sgg8djay179y)

[Response and Remediation 4](#_bgoc8vygd0dj)

[Containment and eradication measures 4](#_kyhxcqk3n5c5)

[Recovery measures 4](#_givq0r4a9hwr)

[Recommendations 5](#_5hqs6q8ystb1)

# **Executive summary**

# **The data breaches evolved around Attackers gaining unauthorised access to sensitive customer information, including credit card data, and personal details. There was high severity around the Bucket, compute, Instance, and Firewall primarily as CymbalBank was finding problems with these resources.**

* **VPC Flow logs should be Enabled for every subnet VPC Network**: There are several low severity findings for Flow Logs disabled. This indicates that Flow Logs are not enabled for several subnetworks in the Google Cloud project used for this lab. This is a potential security risk because Flow Logs provide valuable insights into network traffic patterns, which can help identify suspicious activity and investigate security incidents.

**Basic roles (Owner, Writer, Reader) are too permissive and should not be used**: This medium severity finding indicates that primitive roles are being used within the Google Cloud environment. This is a potential security risk because primitive roles grant broad access to a wide range of resources.

* **An egress deny rule should be set**: This low severity finding indicates that no egress deny rule is defined for the monitored firewall. This finding raises potential security concerns because it suggests that outbound traffic is not restricted, potentially exposing sensitive data or allowing unauthorized communication.

# 

# 

# 

# 

# 

# 

# 

# **Investigation**

A comprehensive investigation was conducted to determine the nature and extent of the compromise. The following findings were identified:

1. **Malware infection**: Forensic analysis confirmed the presence of malware on the compromised VM. The specific type and variant of the malware were identified through in-depth analysis, providing insights into the attacker's techniques and potential motivations.

2. **Unauthorized access**: Evidence revealed that the attacker gained unauthorized access to the compromised VM by exploiting open RDP and SSH services. The access logs and network traffic analysis provided crucial insights into the attacker's entry point and their subsequent activities.

3. **Privilege escalation**: The forensic examination indicated that the attacker leveraged the compromised VM to escalate privileges and gain access to sensitive systems and resources. Through the exploitation of user and service account credentials, the attacker was able to move laterally within the network and target additional services; in particular gaining unauthorized access to BigQuery.

4. **Data exfiltration**: The forensic analysis confirmed the exfiltration of credit card information, including card numbers, user names, and associated locations. The attacker utilized a storage bucket with public internet access to initiate and facilitate the exfiltration, exporting the compromised data for later remote retrieval.

The findings provide valuable insights into the attack, enabling the incident response team to understand the attack vector, the attacker's actions, and the compromised data. These findings will serve as crucial evidence for further investigations, remediation efforts, and future cybersecurity enhancements.

# 

# **Response and remediation**

To effectively remediate the incident, a series of actions were taken in alignment with industry best practices. The following outlines the containment, eradication, and recovery measures implemented:

Cymbal Bank Junior staff were quickly able to respond through their inspection for-

PCI DSS 3.2.1 report - noticing it was needed to first gather information about the breach, fix the compute engine vulnerabilities, fix cloud storage bucket permissions, limit firewall port access, fix the firewall configuration and verify compliance throughout the process.

### **Containment and eradication measures**

1. Finding high-severity listing and identifying breaches
2. Removing public access to the storage bucket
3. Isolating compromised VM

### **Recovery measures**

1. shut down the vulnerable VM **cc-app-01**, and create a new VM from a snapshot taken before the malware infection.
2. Restoring the VM and creating a new VM snapshot
3. fixed the cloud storage permissions by revoking public access to the storage bucket and switching to uniform bucket-level access control. You also removed all user permissions from the storage bucket.
4. fixed the firewall rules by deleting the default-allow-ICMP, default-allow-RDP, and default-allow-ssh firewall rules, and enabling logging for the remaining firewall rules.
5. Compliance test

By implementing these measures, the security team successfully mitigated the immediate risks, removed the attacker's presence, and restored affected systems to a secure and operational state.

# **Recommendations**

This incident provided valuable lessons that can inform future cybersecurity practices and help prevent similar incidents. The following are recommendations that we suggest be implemented to mitigate similar attacks from happening in the future:

They are implementing network segmentation to successfully isolate parts of the network limiting future breaches and their severity.

Improving monitoring and logging - using tools like audit logging

Enhance endpoint security: using MFA for all remote access services

Enhancing employee awareness and training