Final Report – Cymbal Bank Security Incident

Executive Summary

Cymbal Bank experienced a cloud security incident that exposed a limited amount of customer and transaction data. The investigation determined that the breach originated from a misconfigured Compute Engine virtual machine (VM) with open SSH and RDP ports and a Cloud Storage bucket that allowed public access. These weaknesses enabled an external attacker to connect remotely, move laterally through the environment, and access stored data.

Google Cloud Security Command Center (SCC) detected the abnormal activity and generated compliance alerts, allowing the Security Operations Team (SOC) to act quickly. The team contained the compromised assets, removed insecure configurations, and restored systems from trusted sources. No malware persistence or unauthorized users remained after remediation. This incident underscored the importance of continuous configuration monitoring, restricted network access, and prompt response coordination.

Investigation

The investigation focused on identifying how the attacker gained access, what actions were performed, and which data was affected.

- Malware infection: Evidence suggested the VM cc-app-01 was infected with remote-control malware that created outbound connections to external IP addresses.
- Unauthorized access: The attacker gained entry via open SSH (22) and RDP (3389) ports on a VM with a public IP address.
- Privilege escalation: The VM used a default service account with broad API permissions, which allowed the attacker to access additional cloud resources.
- Data exposure: A publicly accessible Cloud Storage bucket permitted unauthenticated reads, exposing sensitive customer information.
- Scope: No evidence was found of lateral movement into production databases or payment systems.

These results guided the response plan and confirmed the attacker leveraged cloud misconfigurations rather than exploiting unknown software vulnerabilities.

Response and Remediation

Containment and Eradication

- Stopped the compromised VM and created a forensic snapshot for evidence.
- Disabled and removed all overly permissive firewall rules (default-allow-ssh, default-allow-rdp, default-allow-icmp).
- Revoked all public permissions from Cloud Storage buckets and switched to Uniform Bucket-Level Access.
- Reviewed and restricted IAM permissions, removing unused accounts and excessive privileges.

- Implemented SCC policy enhancements to automatically flag and alert on public resources.

Recovery and Hardening

- Rebuilt the VM (cc-app-02) from a clean snapshot, with Secure Boot enabled and no public IP.
- Created a new firewall rule 'limit-ports' to allow SSH access only via Google IAP range (35.235.240.0/20).
- Enabled firewall logging on internal rules for better visibility.
- Conducted a PCI DSS 3.2.1 compliance review — confirming all high and medium findings were resolved.
- Monitored Cloud Logging and confirmed there were no further suspicious activities.

The coordinated containment and recovery restored secure operations within 24 hours of initial detection.

Recommendations and Future Prevention

- Continuous monitoring: Use SCC and Cloud Asset Inventory to automatically detect public resources, exposed ports, and IAM policy drift.
- Multi-factor authentication (MFA): Enforce MFA for all administrative and service accounts to reduce credential theft risks.
- Principle of least privilege: Regularly review IAM roles to ensure users and service accounts have only the permissions they need.
- Enhanced logging and alerting: Enable VPC Flow Logs and integrate Chronicle SIEM to centralize alerts and speed up incident detection.
- Incident response readiness: Conduct quarterly tabletop exercises to test playbooks and validate response coordination between security and operations teams.

Conclusion

The Cymbal Bank incident was successfully contained and resolved through rapid detection, disciplined response, and a focus on secure recovery. The organization's cloud environment now follows hardened configurations, improved access control, and continuous monitoring practices. The incident reinforced that strong identity management, minimal network exposure, and continuous compliance validation are essential to defending against evolving threats.

Prepared by: Jeferson Domingues Madureira

Title: Junior Cloud Security Analyst

Date: October 2025