Cymbal Security Incident Report

Contents

[Executive Summary 2](#_Toc177561130)

[Investigation 3](#_Toc177561131)

[Response 4](#_Toc177561132)

[Recommendations 5](#_Toc177561133)

# Executive Summary

After detecting some unusual activity in cloud systems, the security team conducted an investigation to discover that the company has suffered a significant security breach across networks, applications, and data storage repositories. As part of this breach, attackers gained unauthorised access to sensitive information including customer personal information and credit card details.

The incident began with the infection of a virtual machine (VM) with malware. The VM was vulnerable to attack due to misconfigurations that allowed the attacker to establish a connection.

Furthermore, the VM had been created with a default service account, which had full access to cloud APIs. This posed a significant risk for privilege escalation, which ultimately occurred when the attacker gained access to this account.

Leveraging this compromised account, the attacker gained access to all other services, and began targeting sensitive customer data. The attacker was able to query, save and exfiltrate customer credit card data via cloud storage, specifically exploiting further misconfigurations in storage bucket policies.

# Investigation

A comprehensive investigation uncovered the following details regarding the incident:

1. Malware

Analysis confirmed the presence of known malware on the VM. The specific type of malware gave insight as to the techniques and motivations of the attacker, namely password theft and data exfiltration.

1. Unauthorised access

The VM was required to be publicly accessible, but had open SSH and RDP services. Network traffic analysis and access logs provided evidence indicating the attacker’s entry point. The attacker established a connection to the infected VM using these services and a stolen password.

1. Privilege escalation

The attacker leveraged the compromised VM to gain access to critical resources. The VM had been setup using a default service account, which had full access to Google Cloud APIs. The service account’s managed user key was retrieved by the attacker on the VM, which was then used to gain further access to sensitive resources. Moving laterally, the attacker was able to begin specifically targeting resources containing customer data.

1. Data exfiltration

Analysis confirmed the exfiltration of customer credit card data, location data and customer names. This was made possible via use of BigQuery to find and retrieve customer data. The results of the these queries was then output to a text file, which was stored in a Storage Bucket. This bucket had previously been setup as publicly accessible and without uniform-bucket level access policies applied. Once the file was stored there, the attacker later retrieved this data remotely.

# Response

The following actions were taken to contain, eradicate and recover from the incident:

1. Isolate the VM

The compromised VM cc-app-01 was immediately isolated from the network. This limited the spread of the attack and prevented further unauthorised access.

1. Restriction of services

Firewall rules were updated to restrict SSH and RDP access to the VM. This minimised the risk of further exploitation through these services.

1. Storage bucket policies

All public access to storage buckets was removed and uniform bucket-level access was applied. This minimised the risk of further data exfiltration through this service.

1. Restore from snapshot

The VM was restored using a trusted snapshot taken prior to the incident. This restored the VM to a clean and secure state.

1. Security configuration review

A full review of security policies and implemented configurations was conducted across all systems to identify any other potential misconfigurations or vulnerabilities in systems. Any issues were identified and rectified promptly.

1. Increased monitoring

Further enhancements were made to monitoring capabilities such as real-time log analysis and prompt alerting for unauthorised access attempts and suspicious activities based on this incident.

# Recommendations

Based on the investigation and response to this particular incident, the following recommendations are made to improve the company’s cybersecurity practices:

1. Regular risk assessments

Perform regular risk assessments to identify potential security risks and vulnerabilities. This includes assessing systems and policies in accordance with best and latest practices.

1. Implement MFA

Implement MFA for all accounts. This layer of security greatly reduces the risk of unauthorised access.

1. Implement the Principle of Least Privilege

The principle of least privilege mandates that accounts only have access to the necessary permissions to fulfil their role. Review and update account permissions regularly to ensure that accounts do not have unnecessary access to services they do not require.

1. Penetration Testing

Conduct regular penetration testing to identify and assess vulnerabilities. This allows vulnerabilities to be addressed prior to actual security incidents.